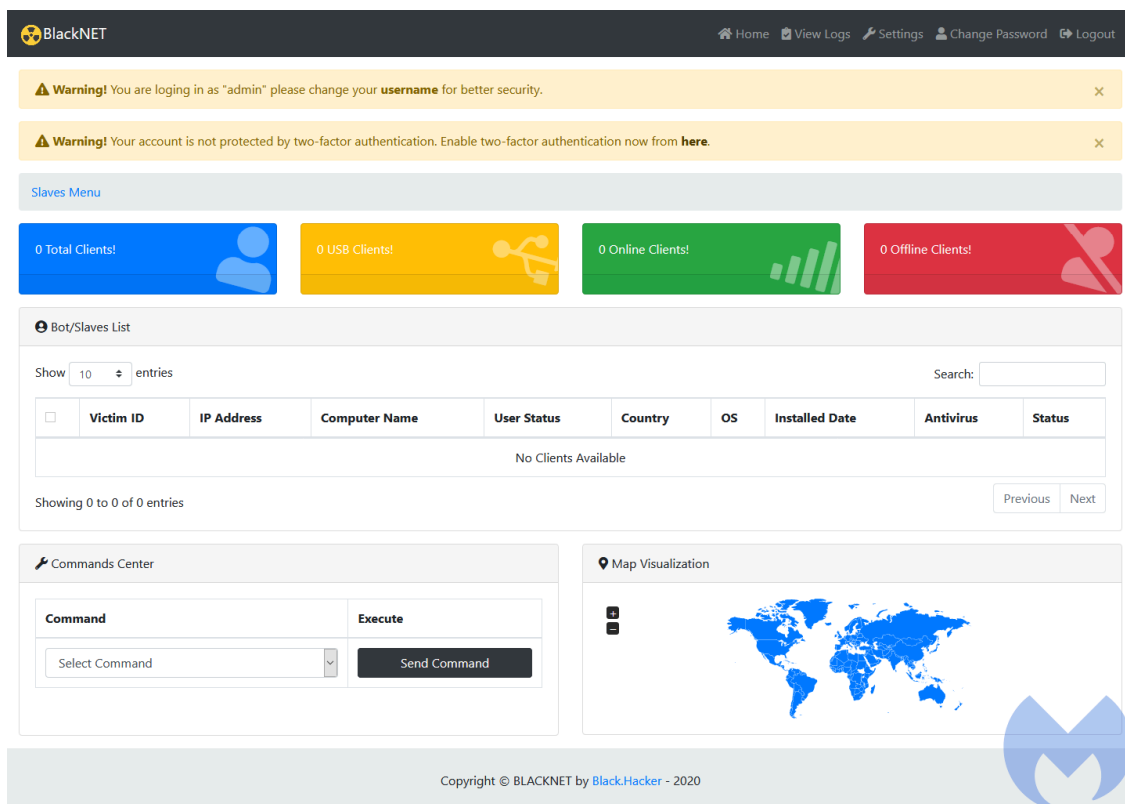


Fake "Corona Antivirus" distributes BlackNET remote administration tool | Malwarebytes Labs

By Threat Intelligence Team

Published: 2020-03-22 · Archived: 2026-04-05 20:05:27 UTC

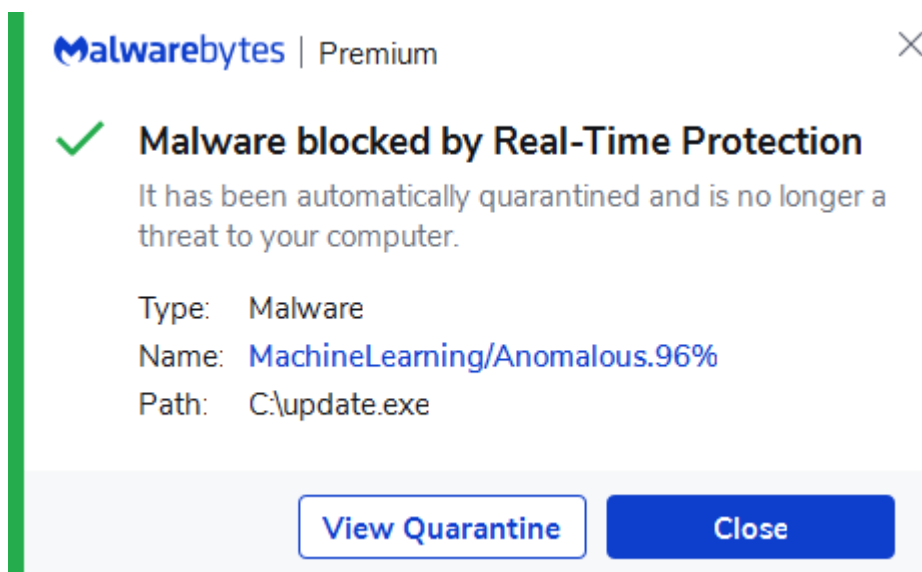


Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

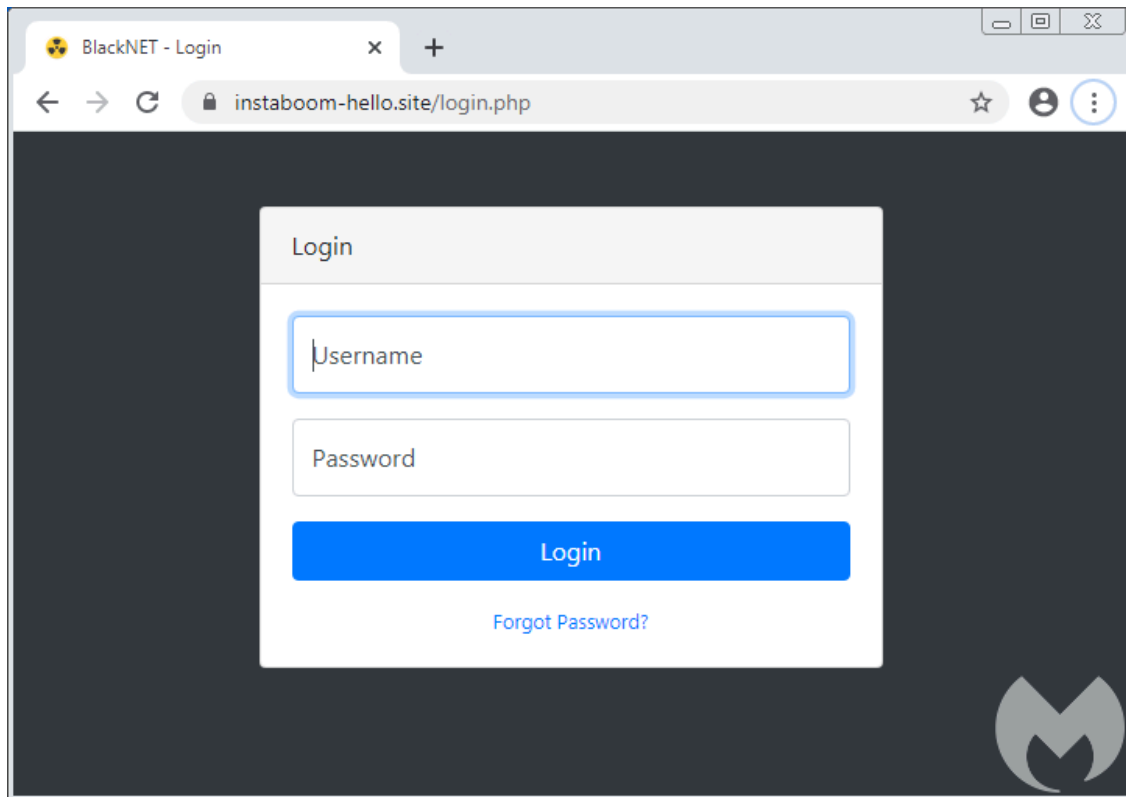
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

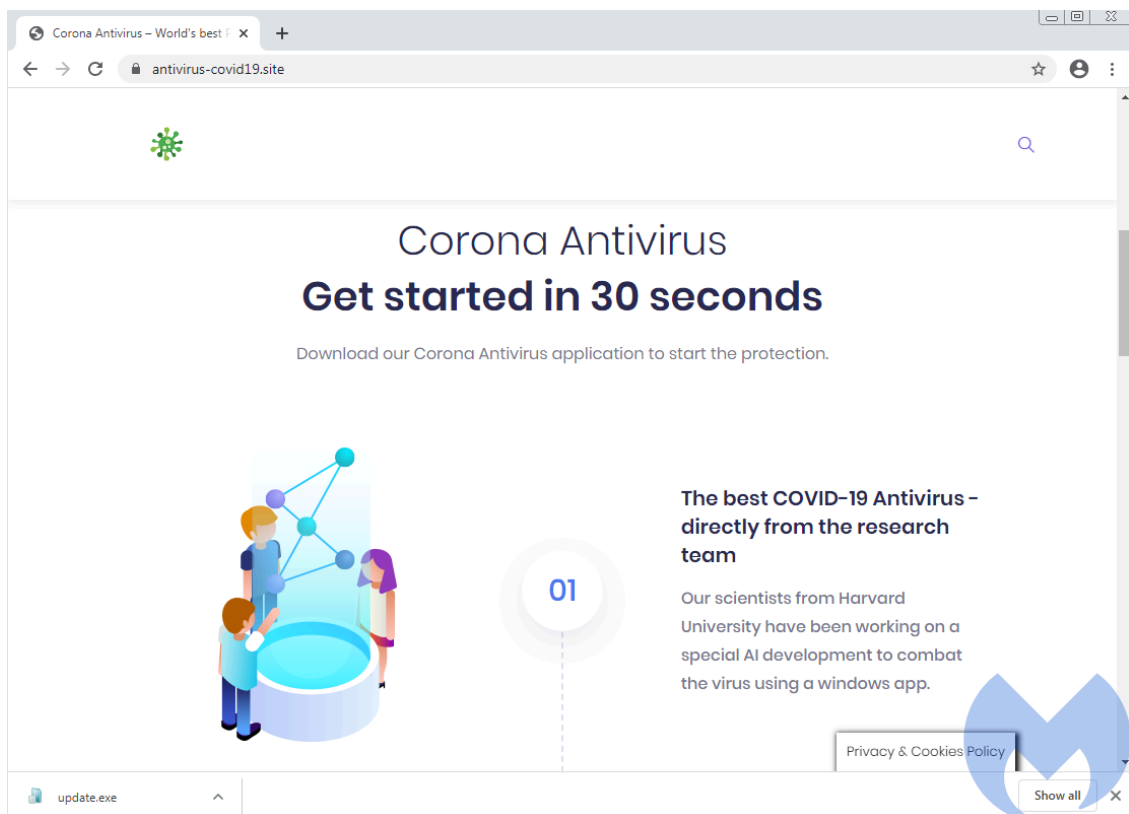
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

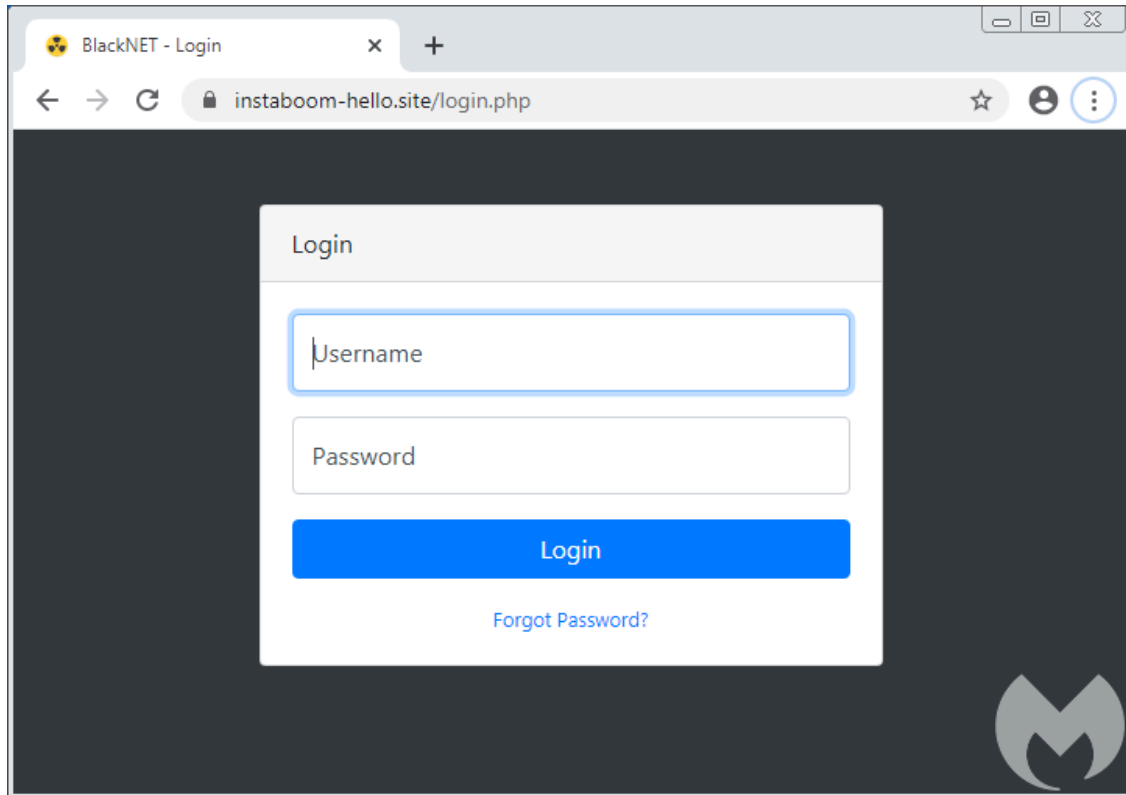


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

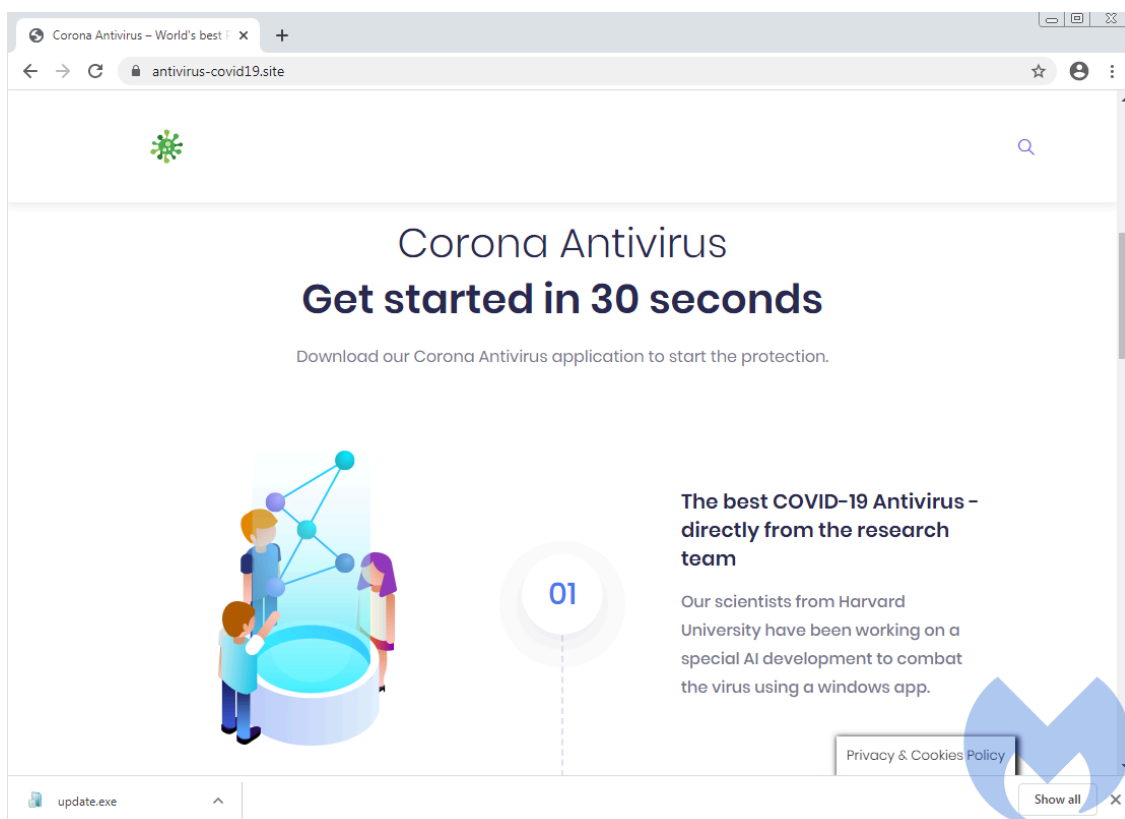
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

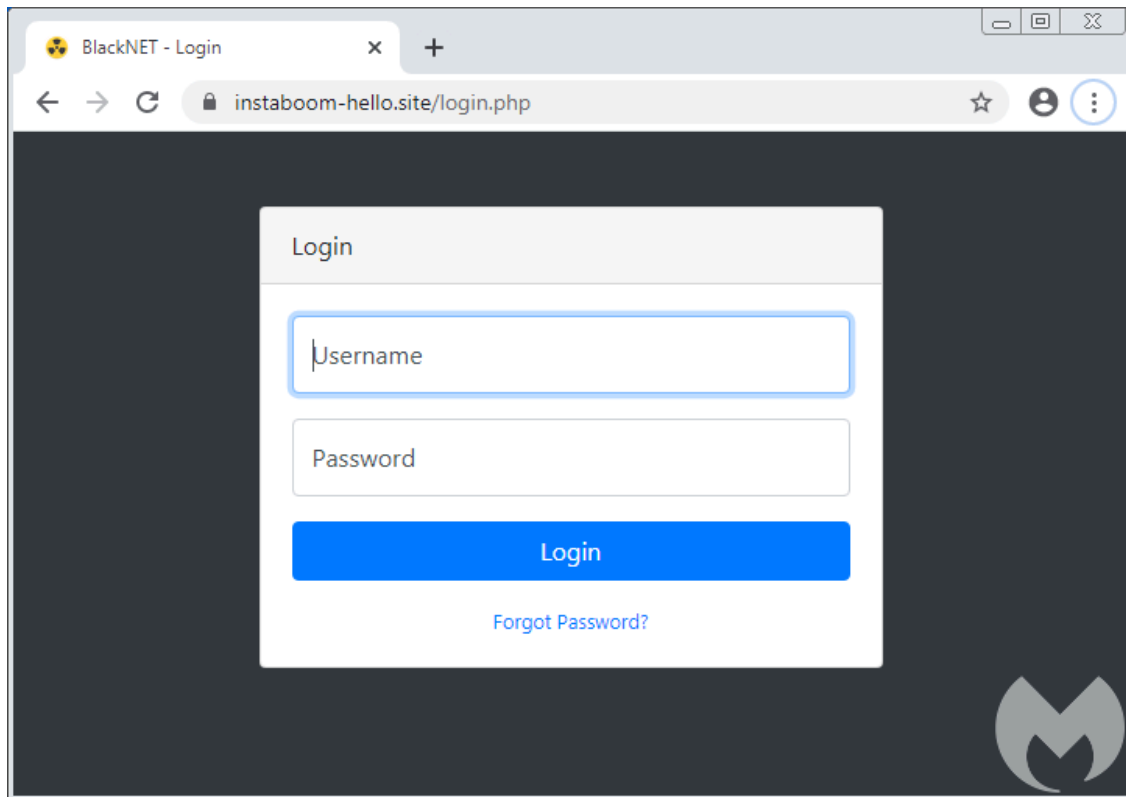


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[:]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[:]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

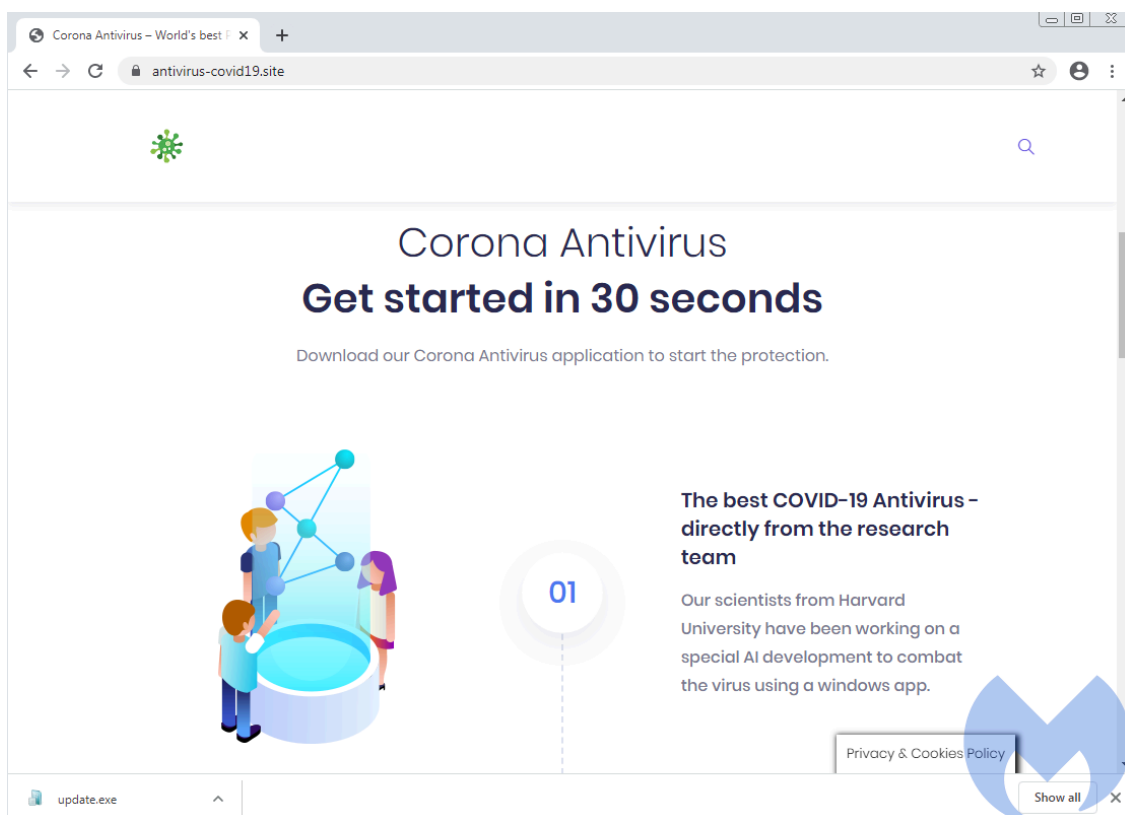
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

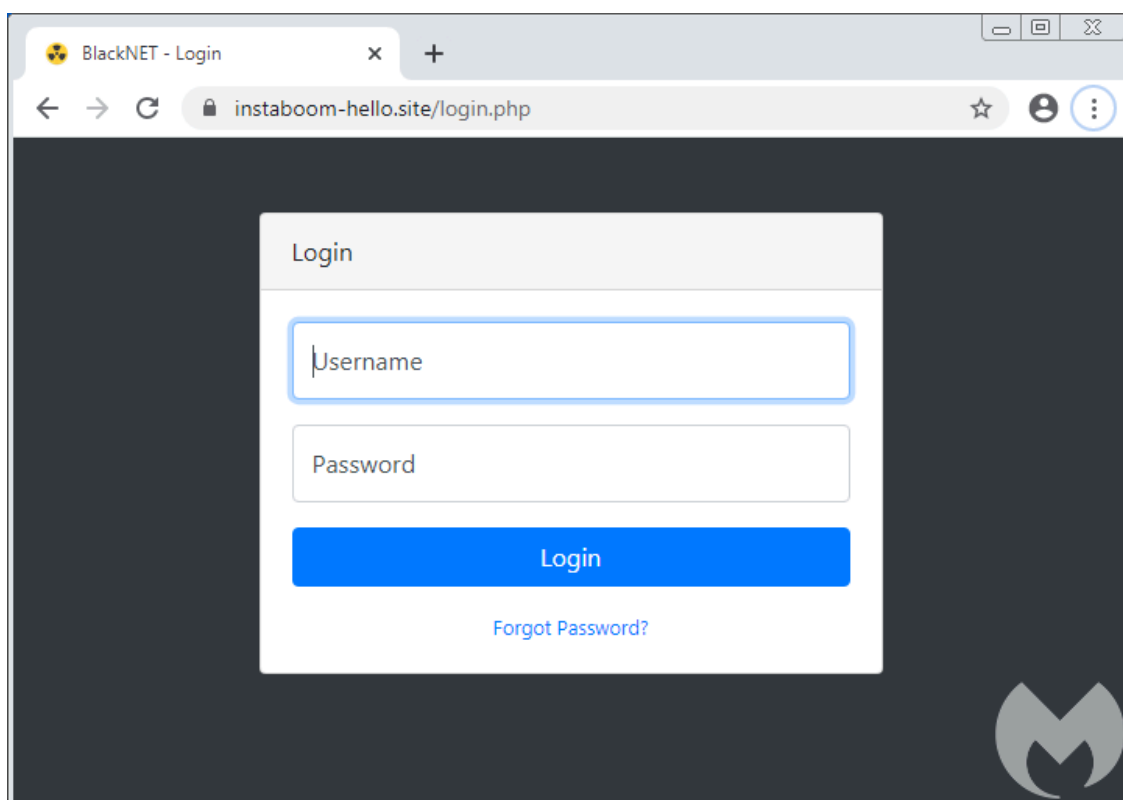
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

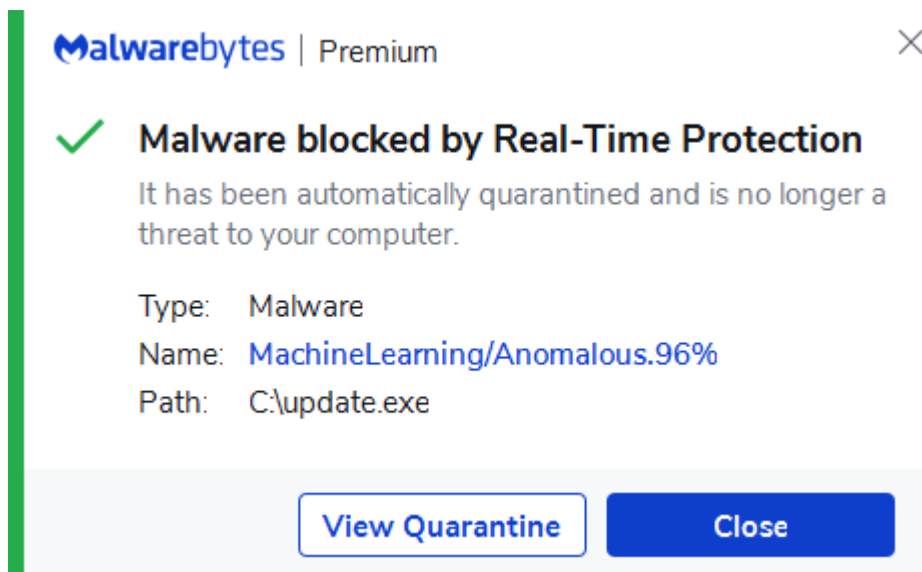
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

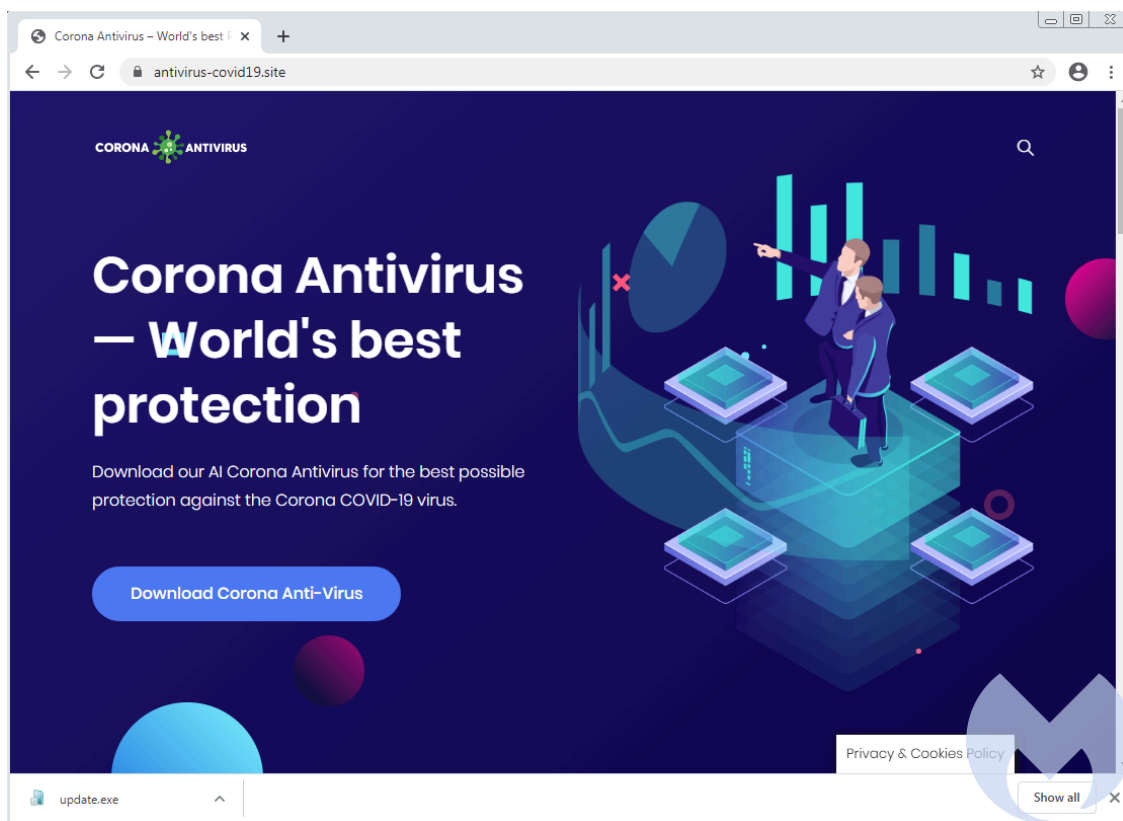
```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

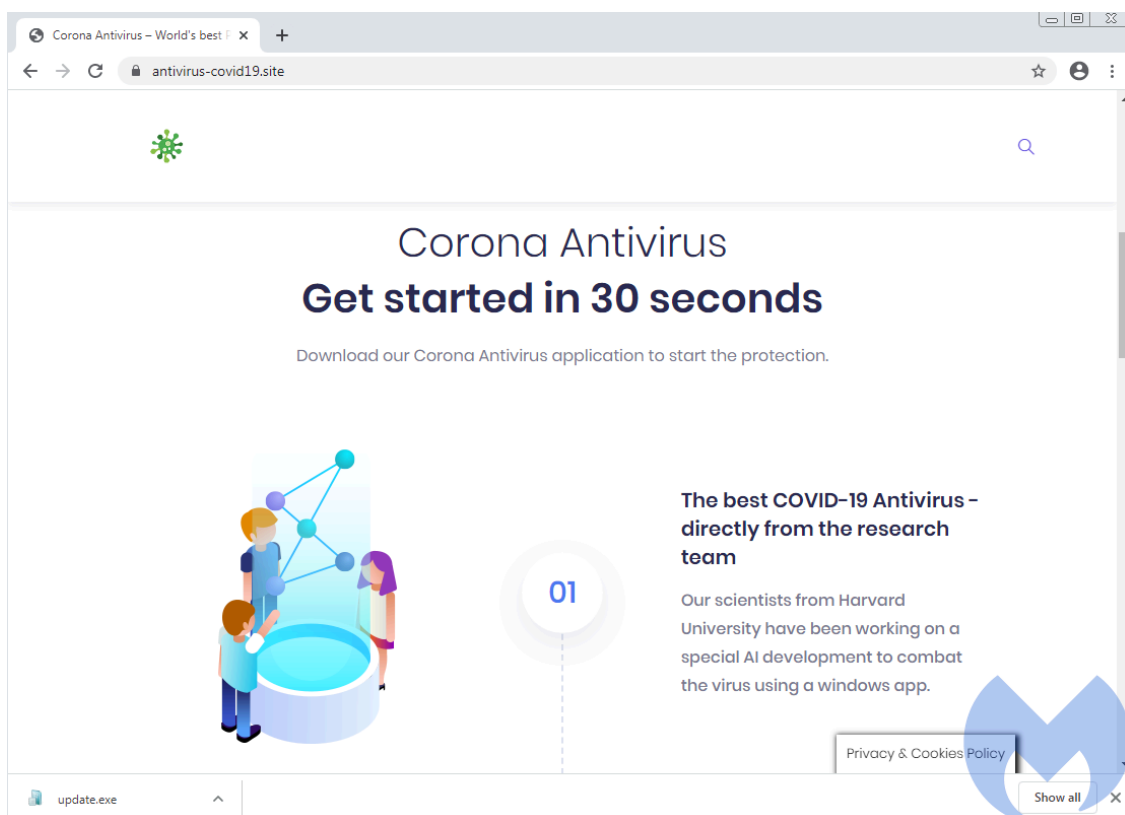
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

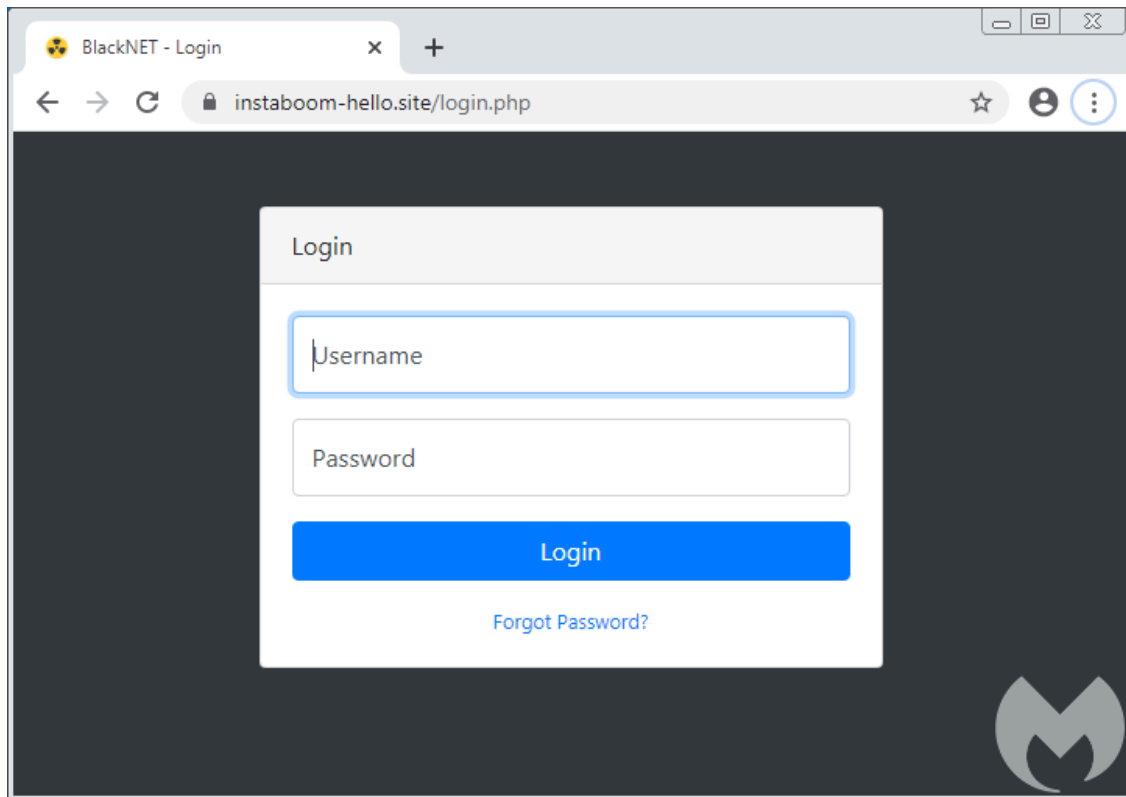


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

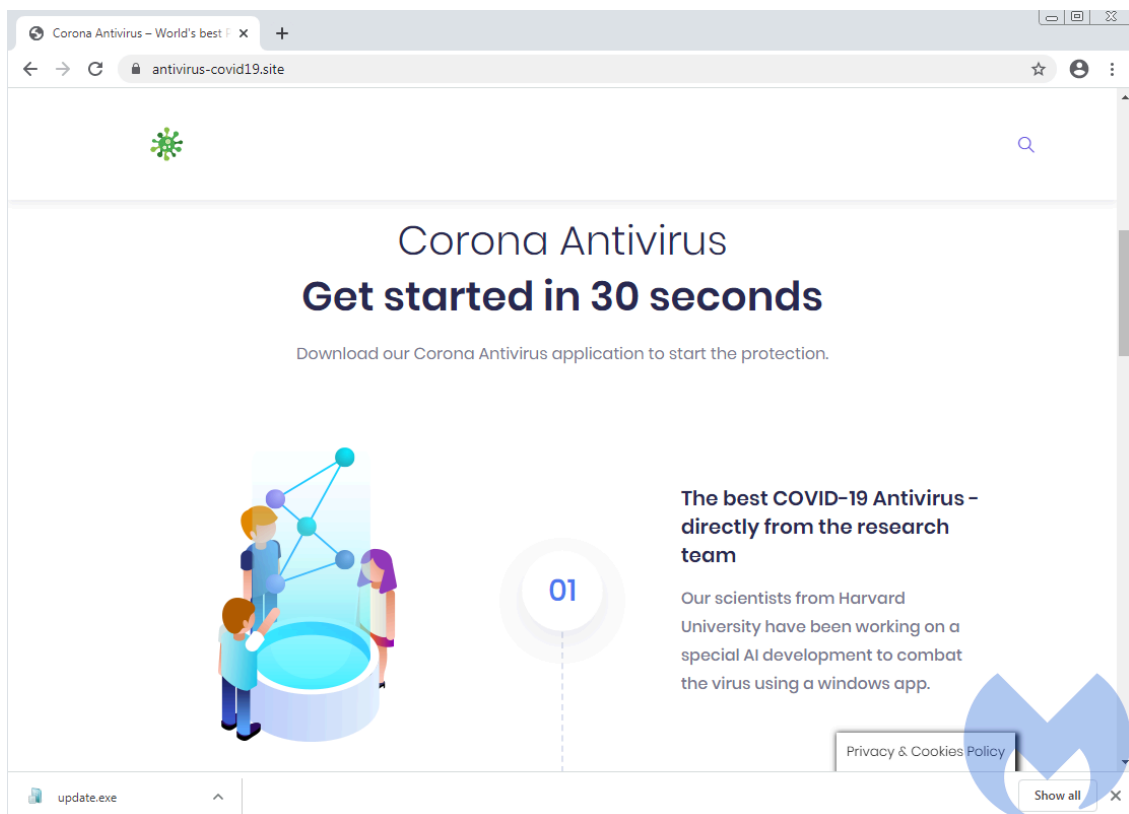
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

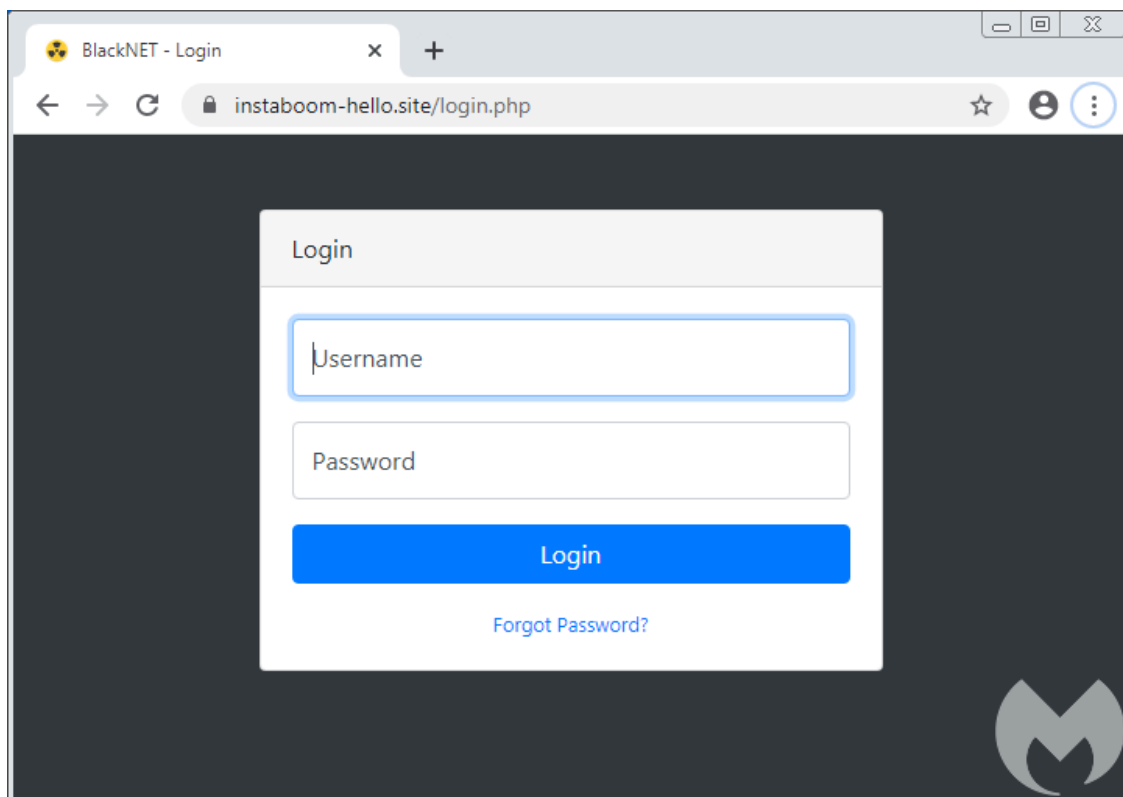


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

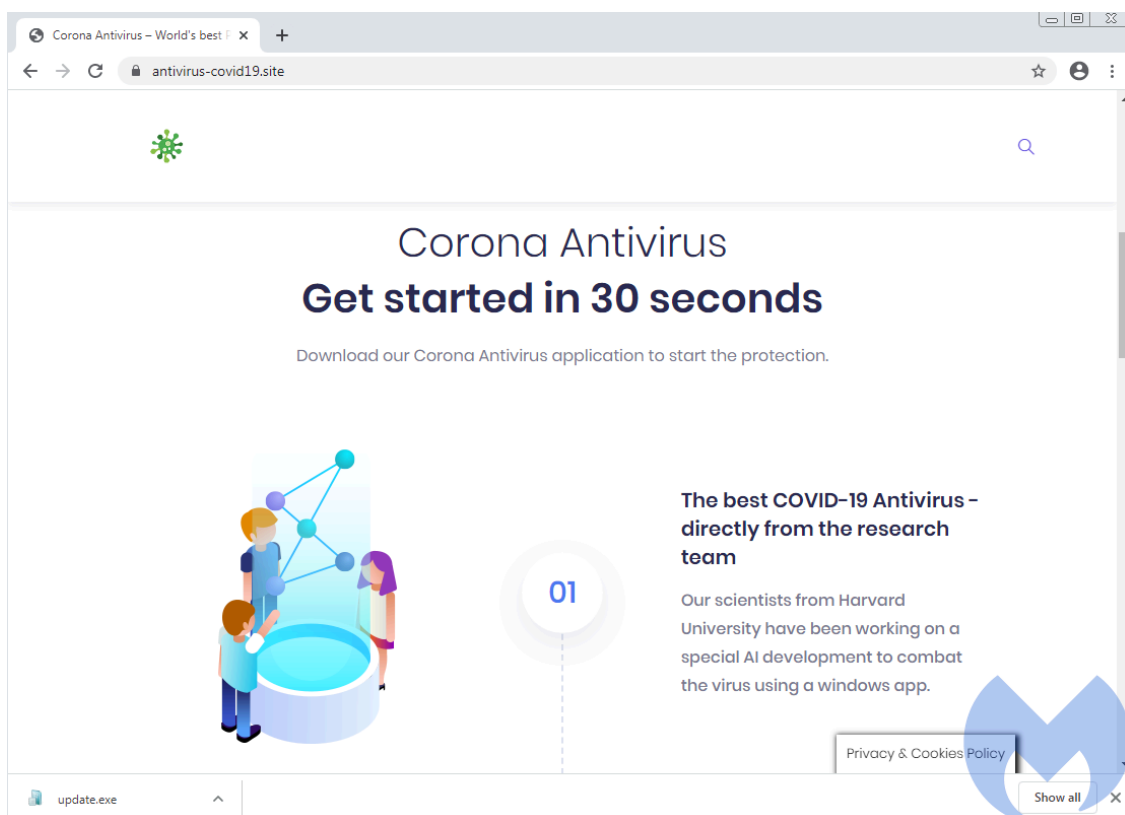
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

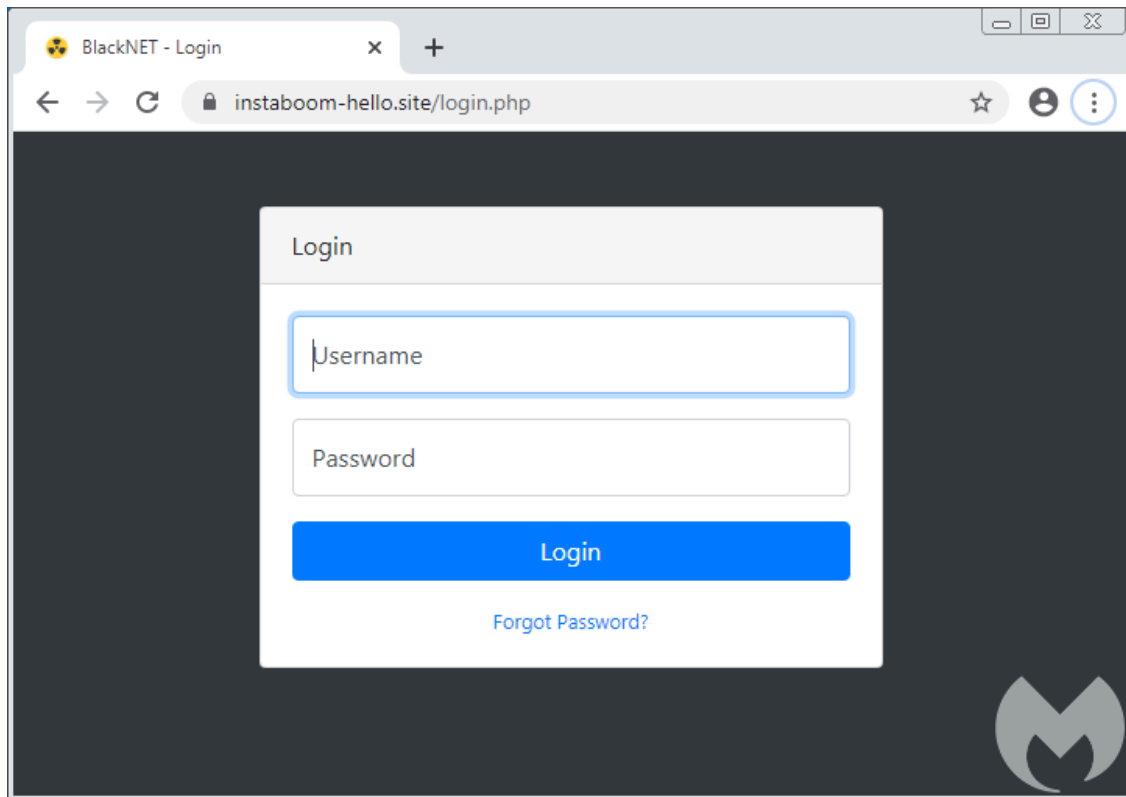


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main content area is divided into several sections. On the left, there's a 'Slaves Menu' with four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below this is the 'Bot/Slaves List' section, which includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. Further right is a 'Map Visualization' section showing a world map with a blue overlay. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

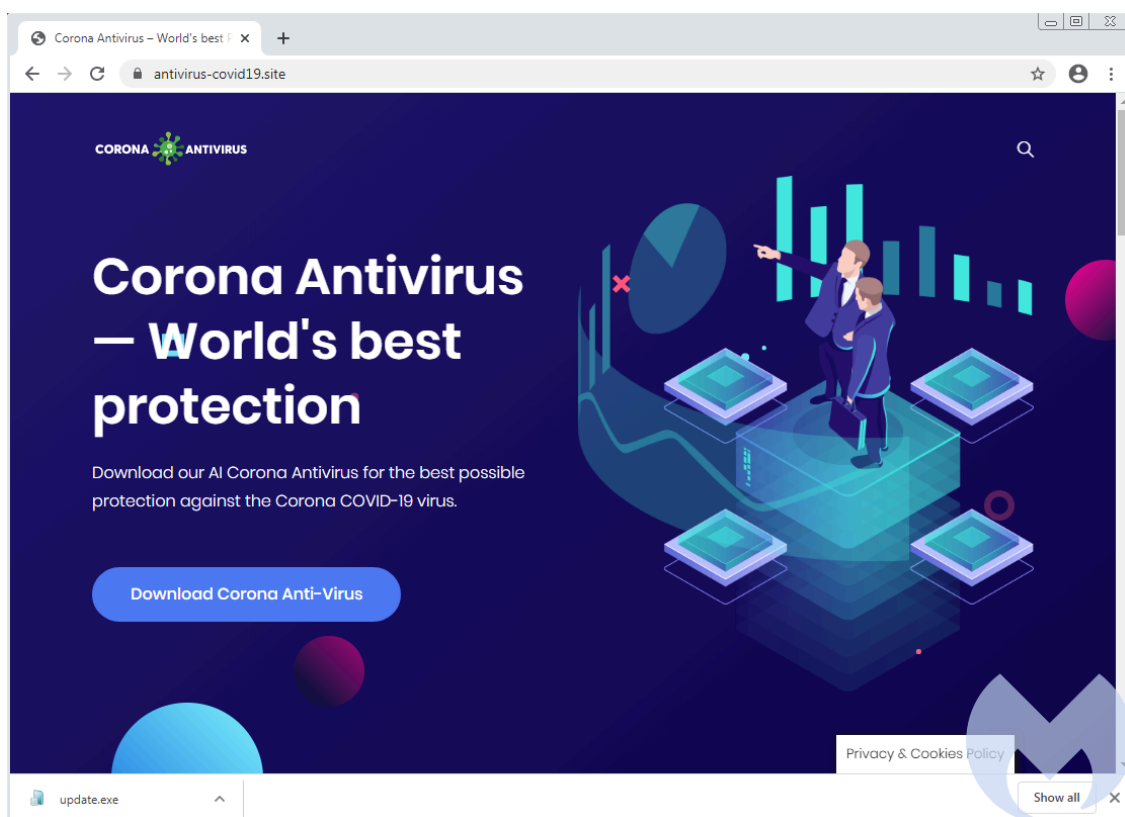
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

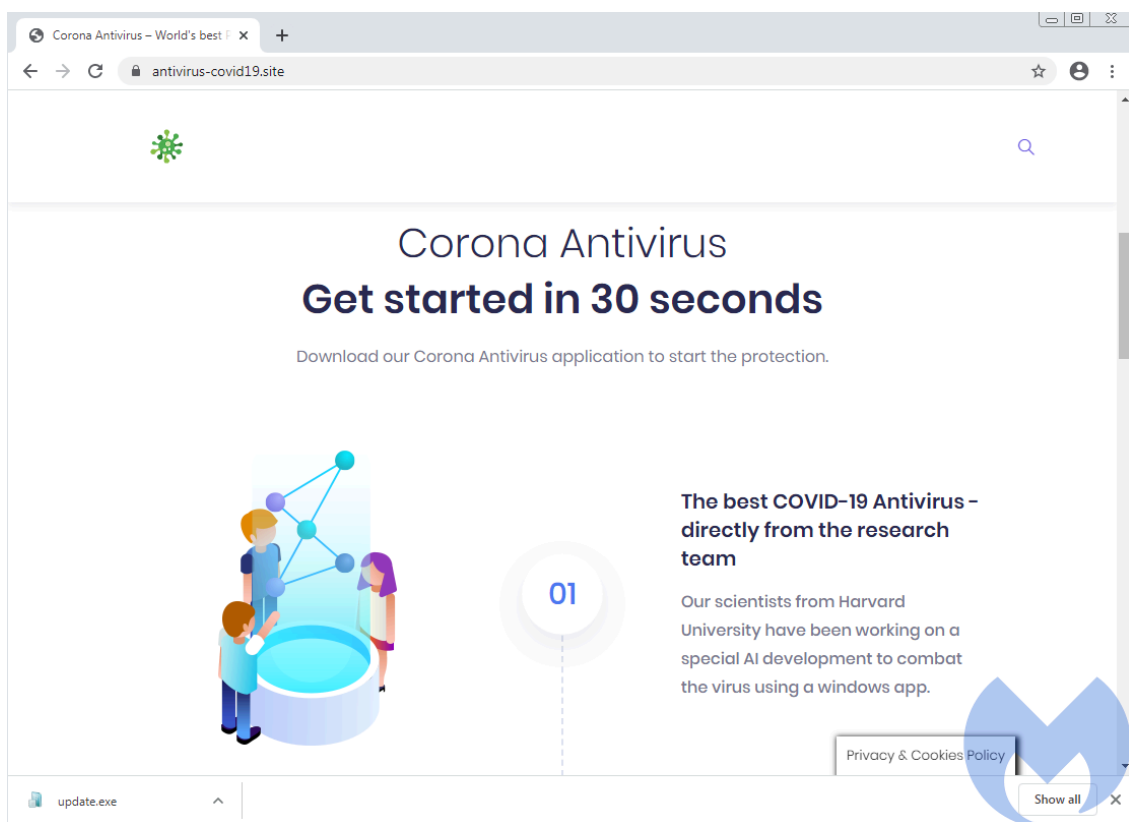
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

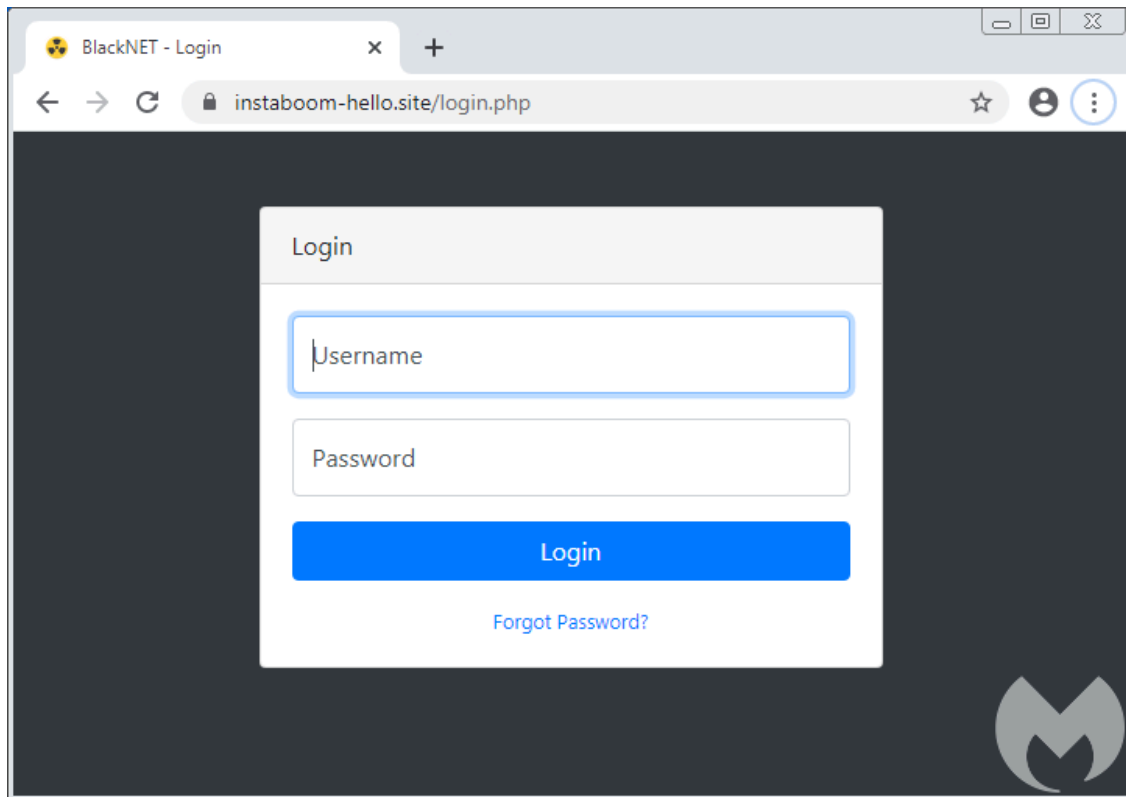


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

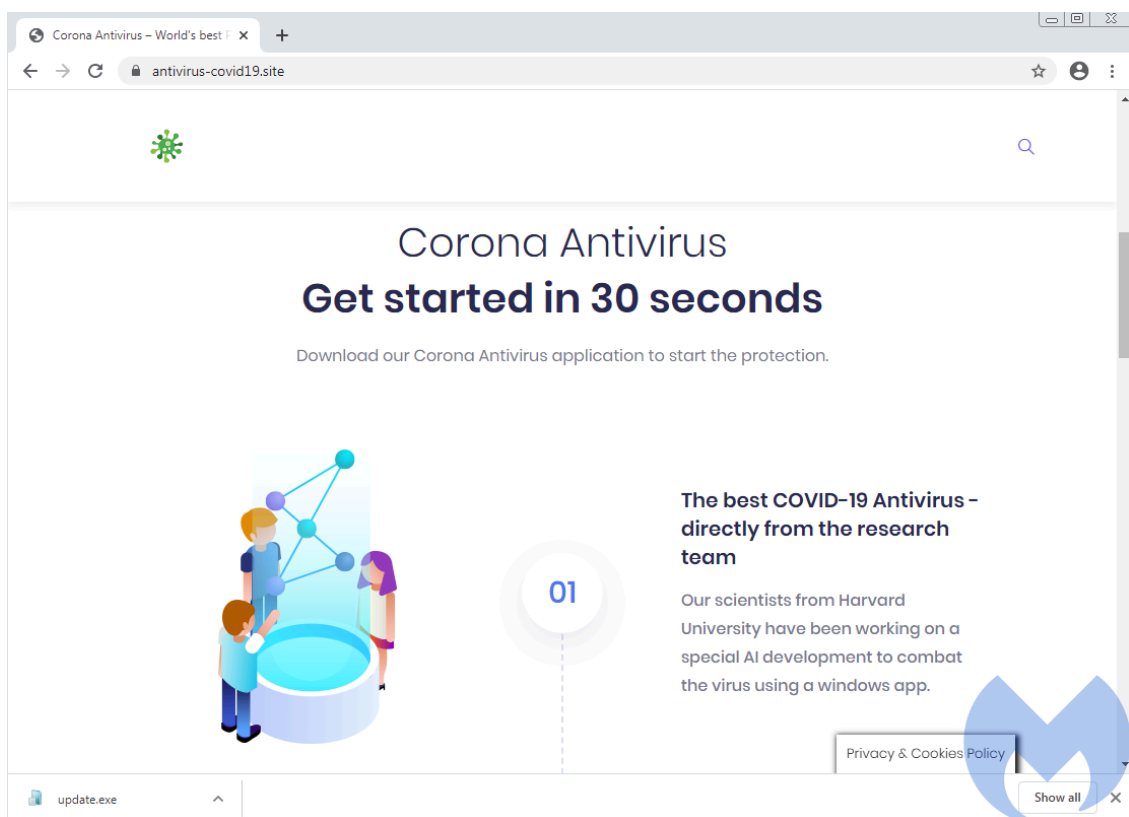
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes representing client statistics: 0 Total Clients (blue), 0 USB Clients (yellow), 0 Online Clients (green), and 0 Offline Clients (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots indicating client locations. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

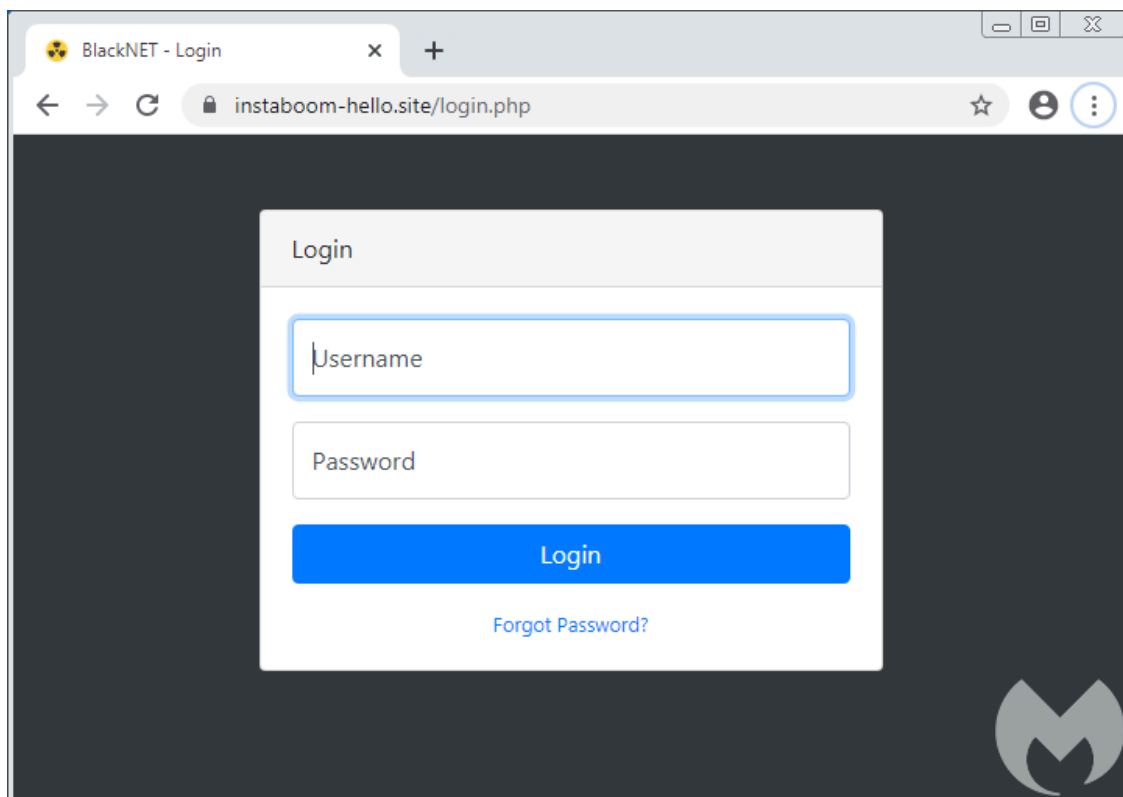
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

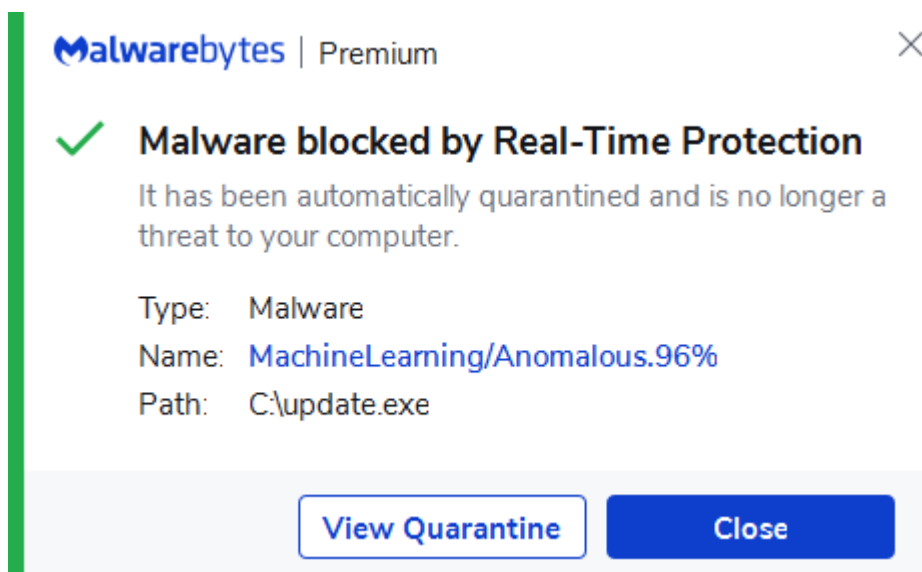
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

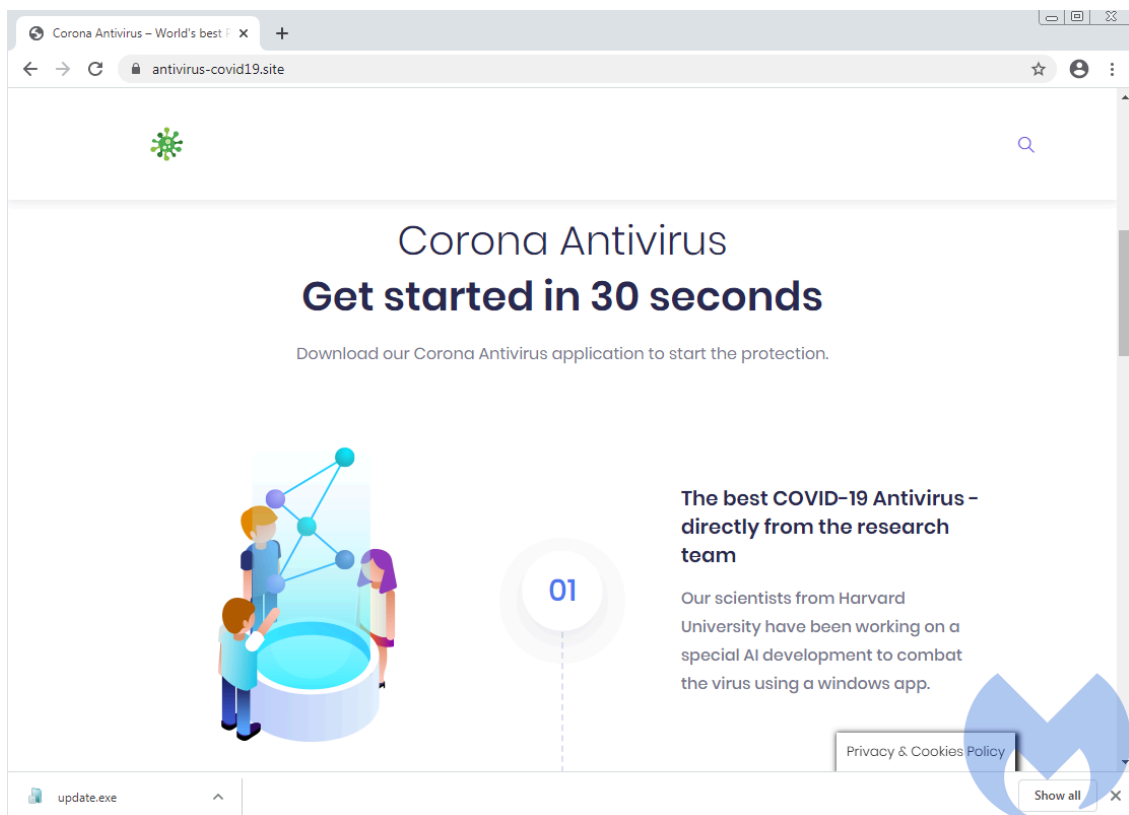
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

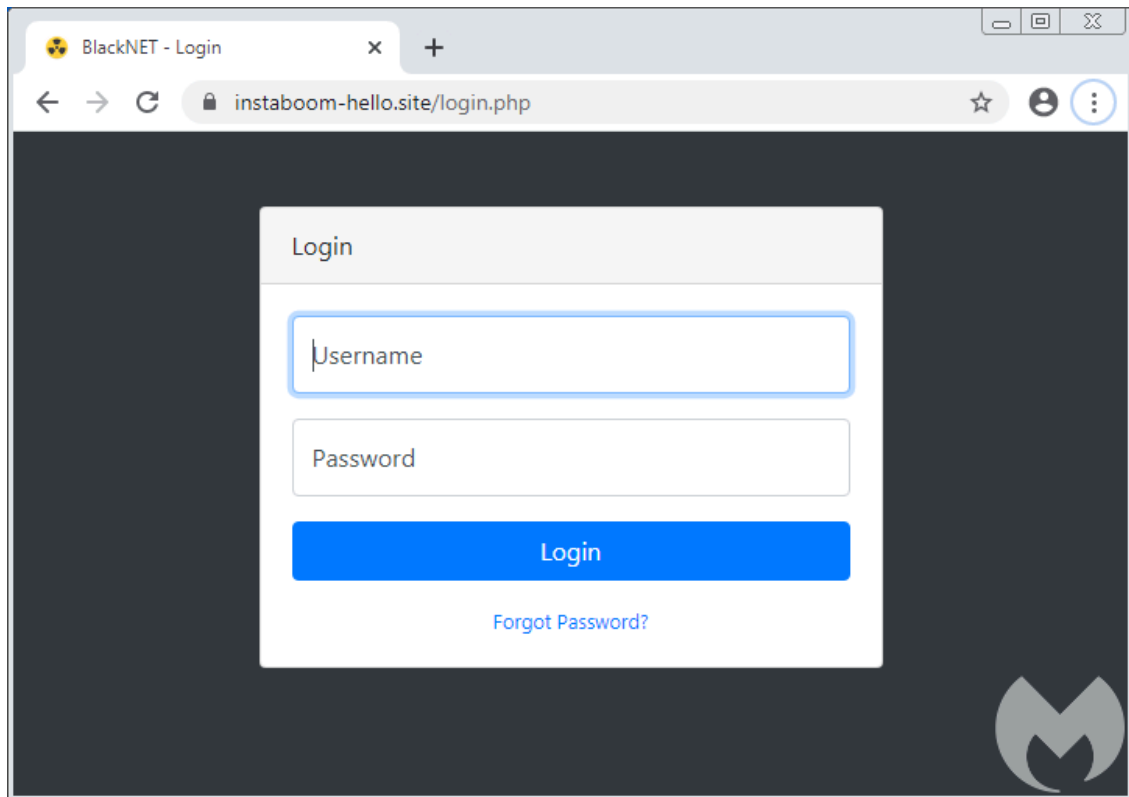


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

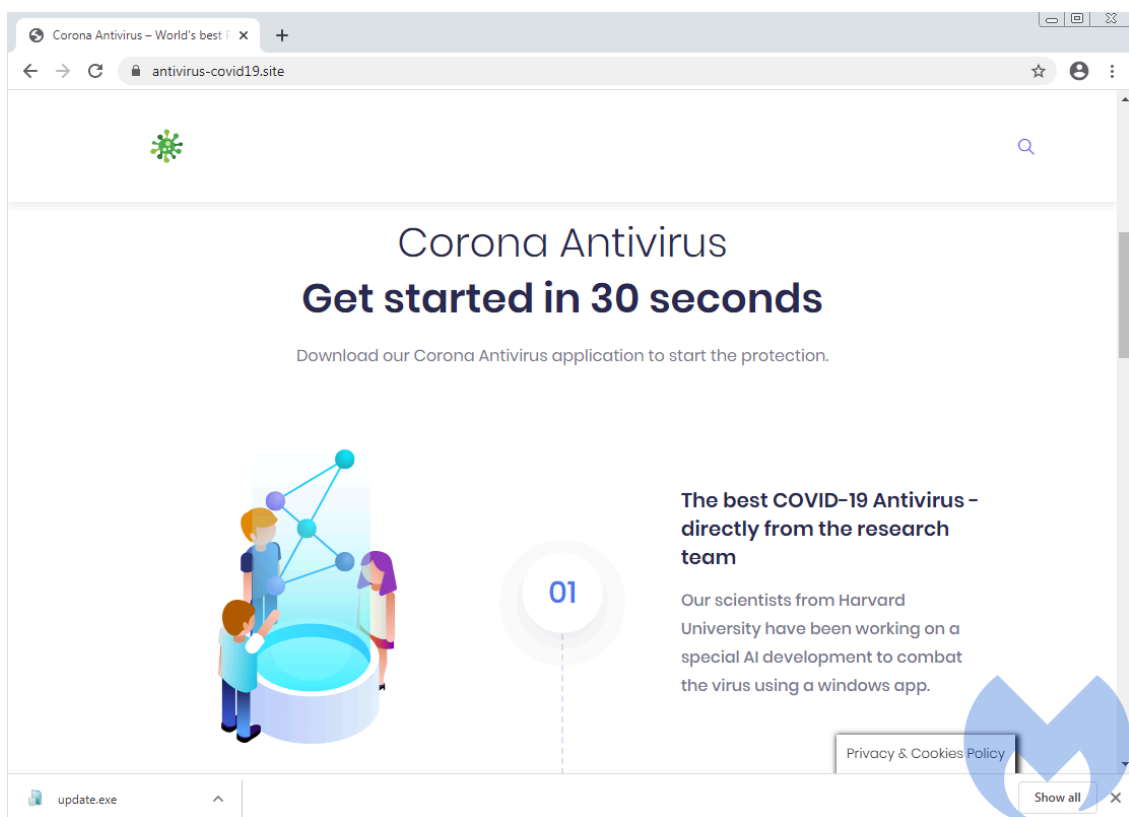
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

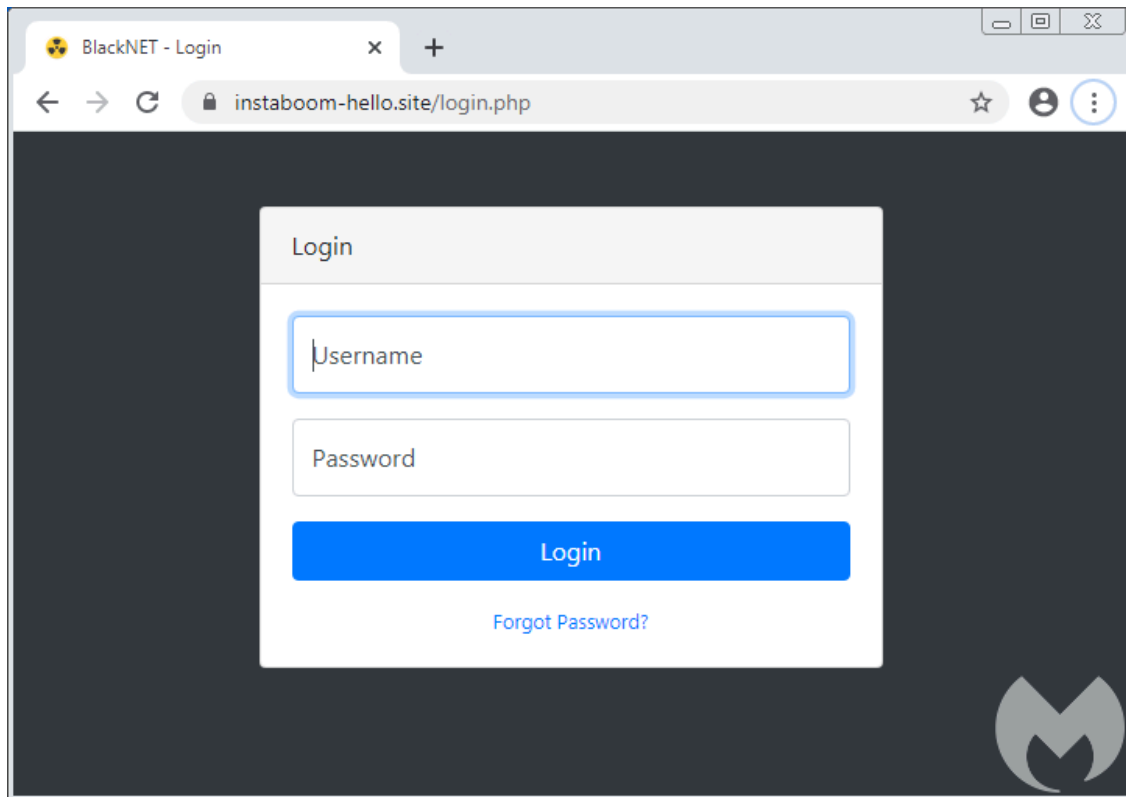


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

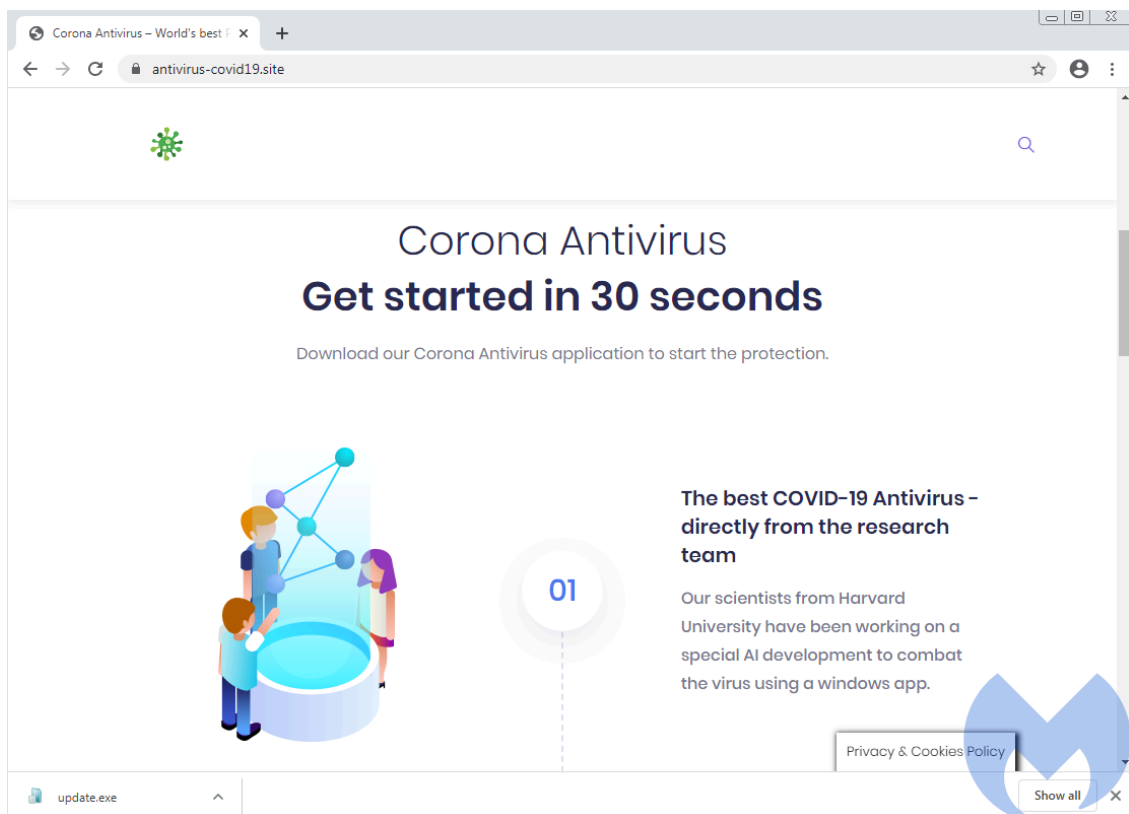
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

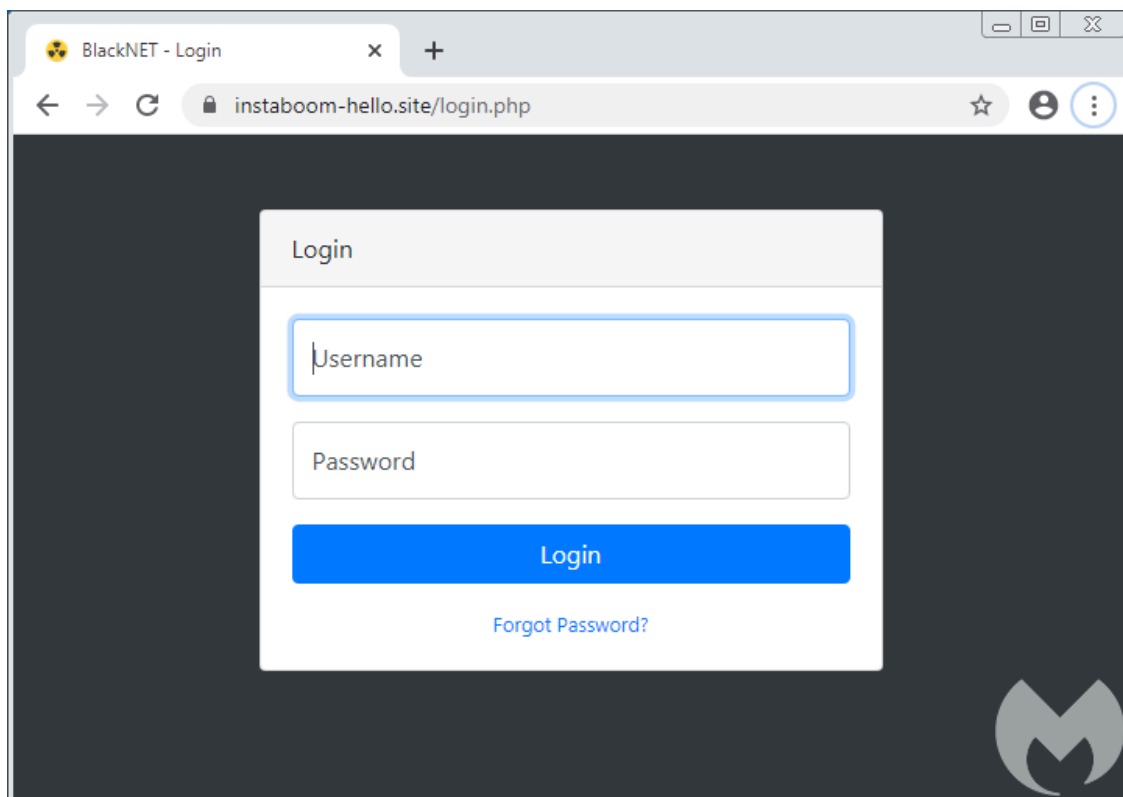


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

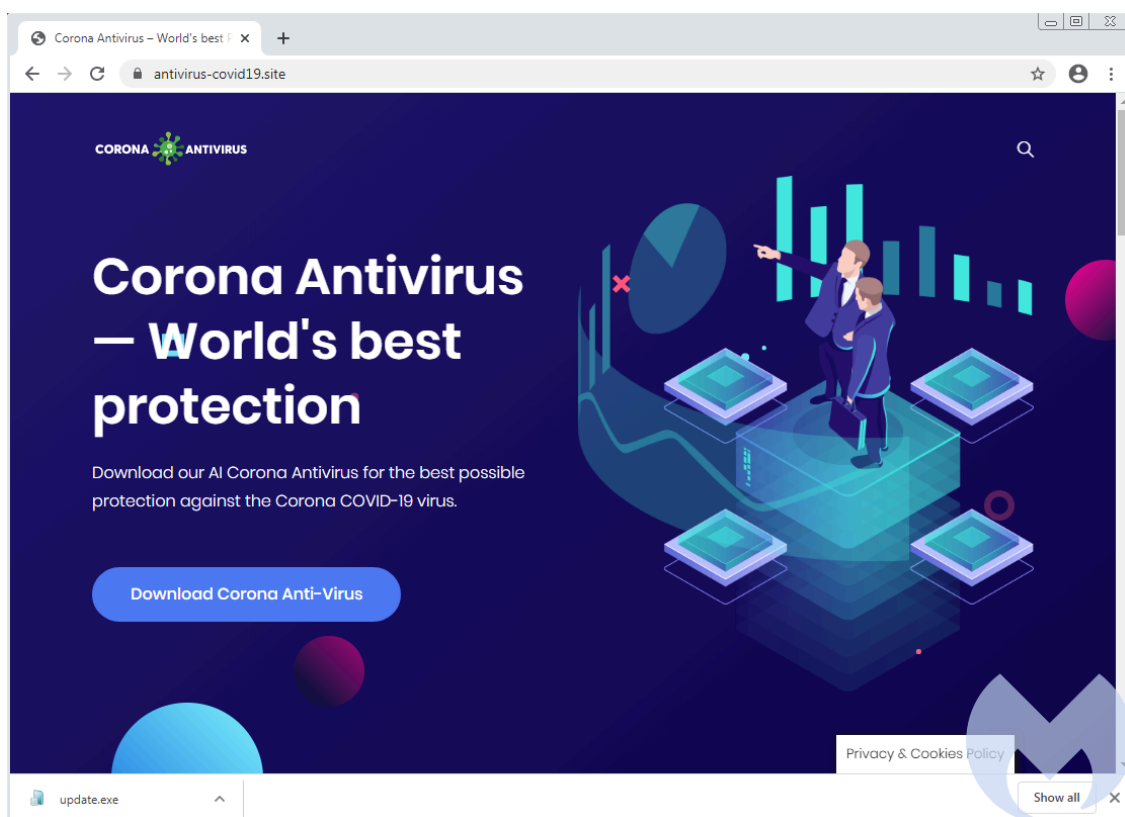
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

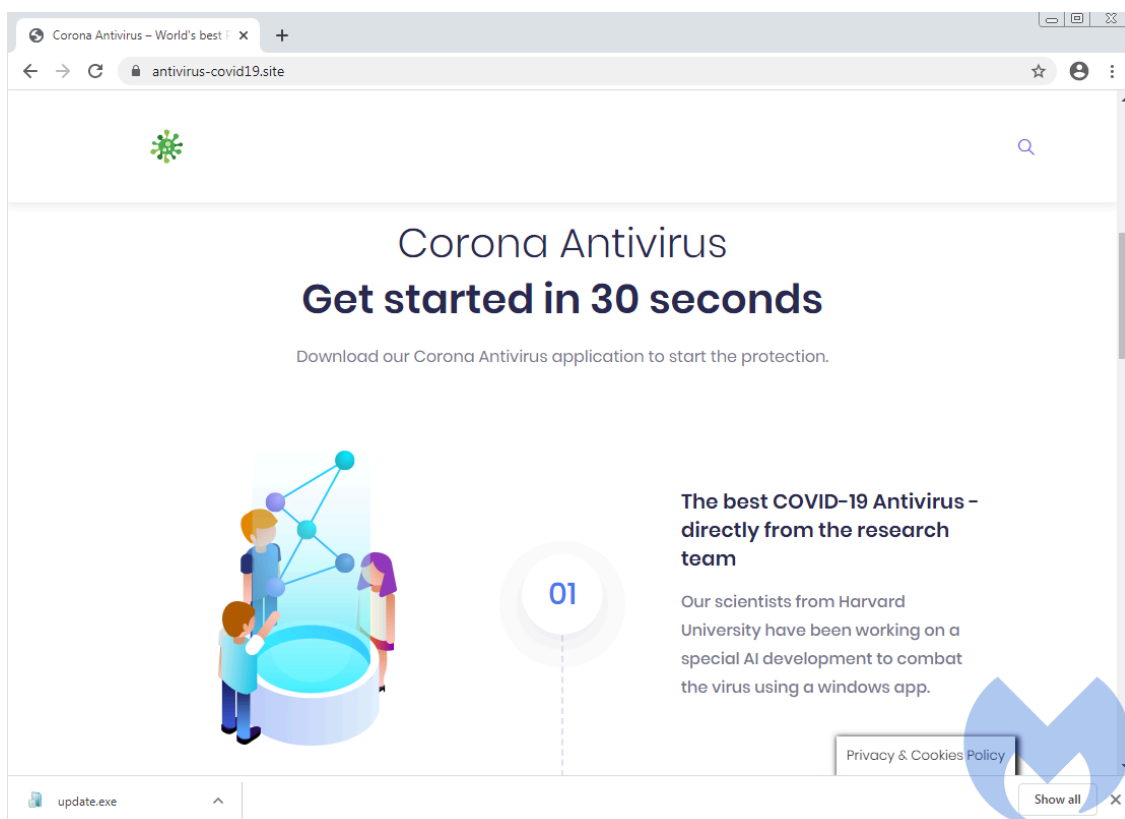
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

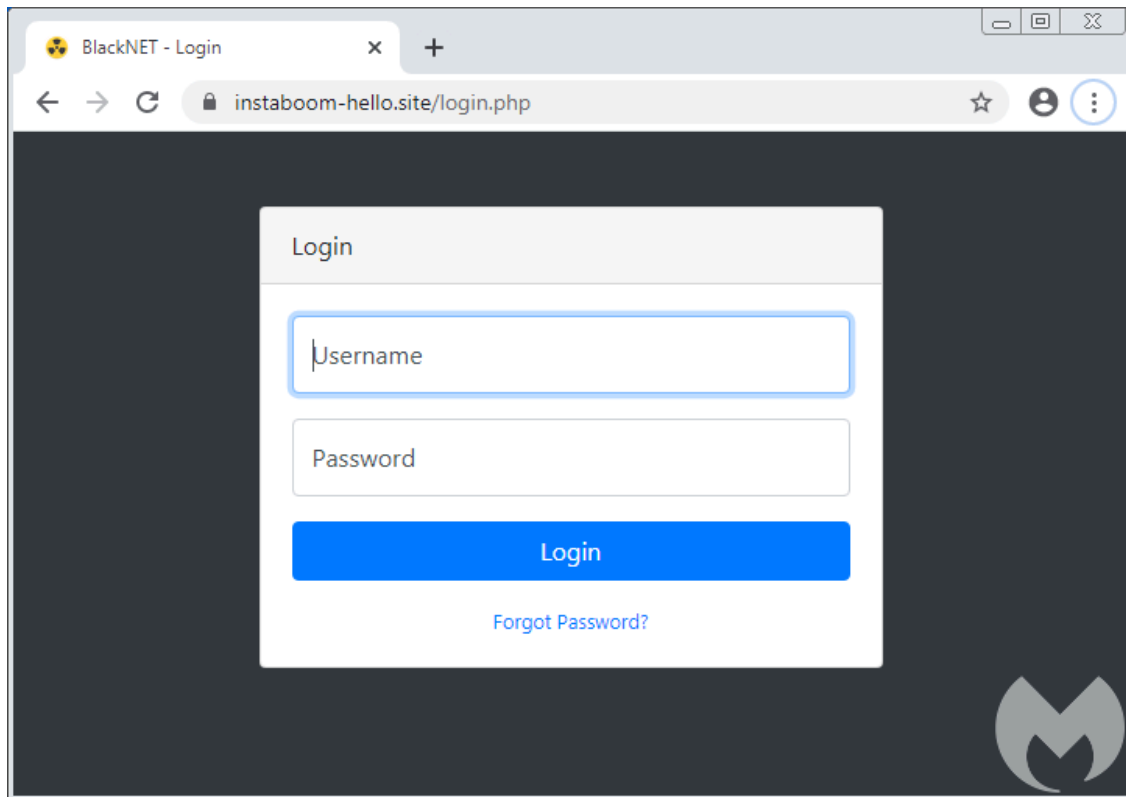


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

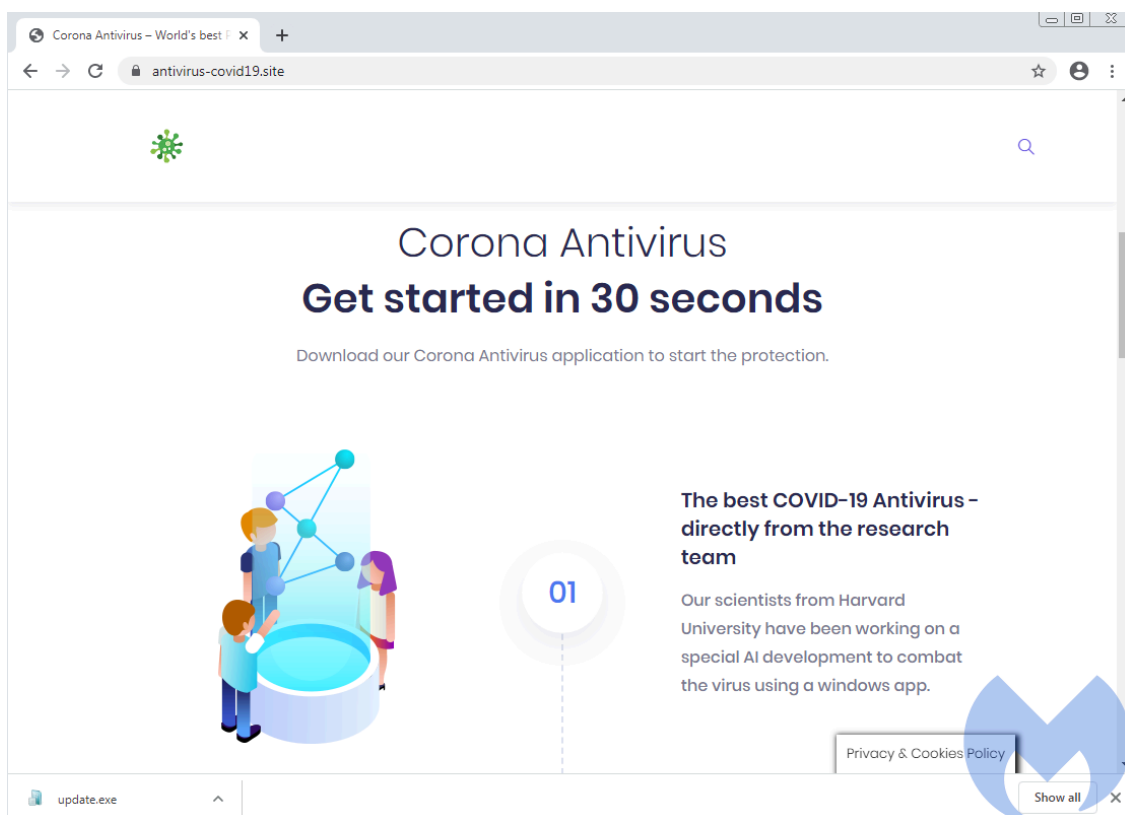
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

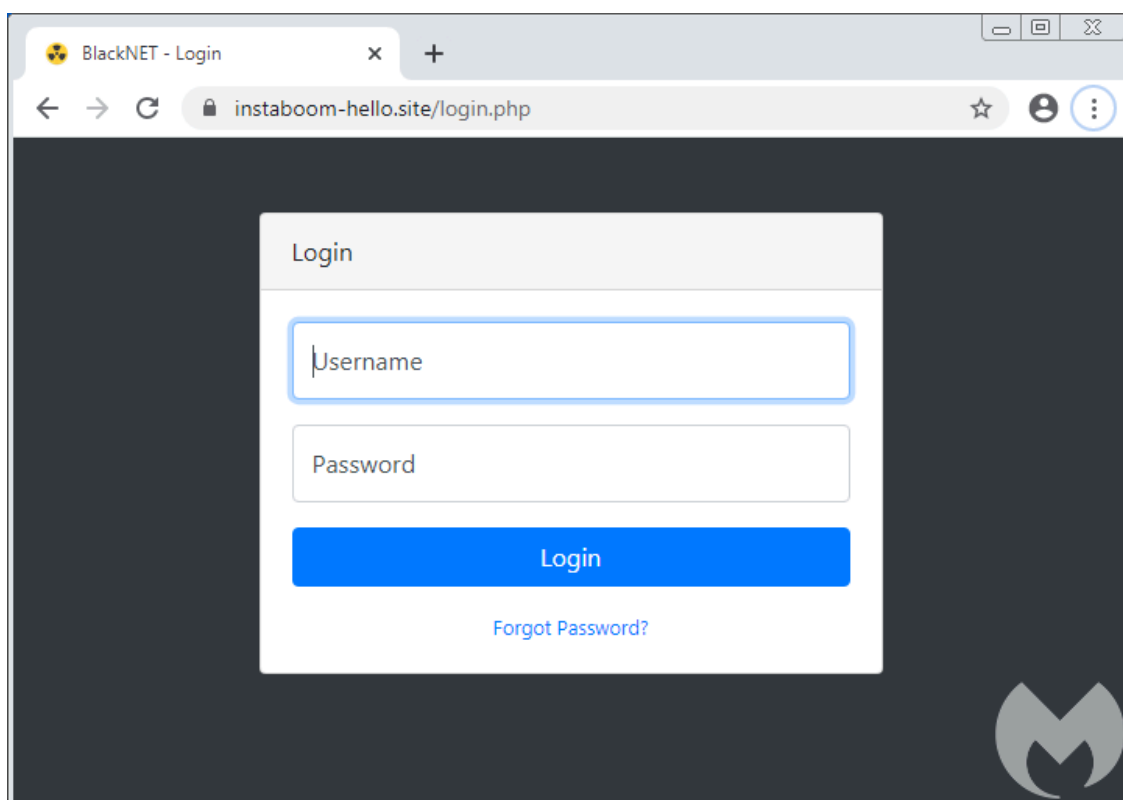
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

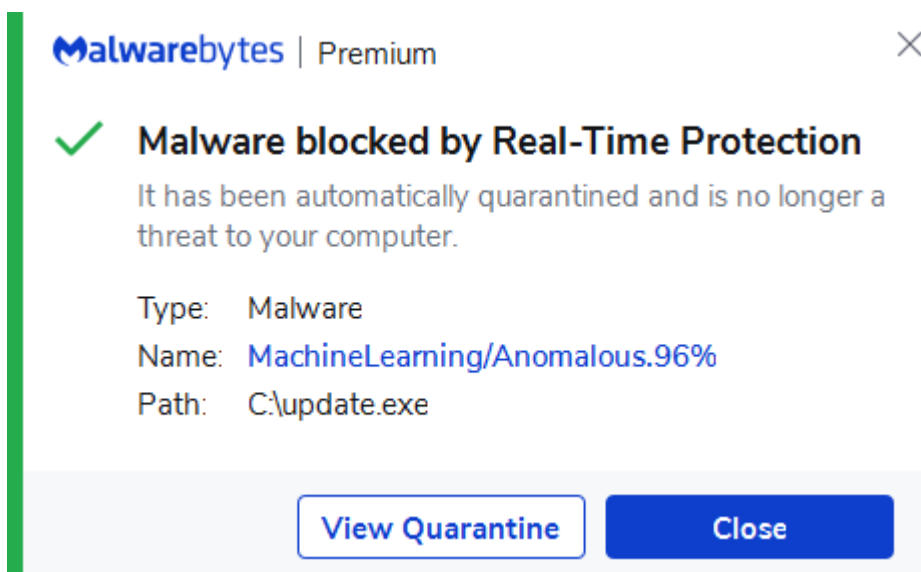
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

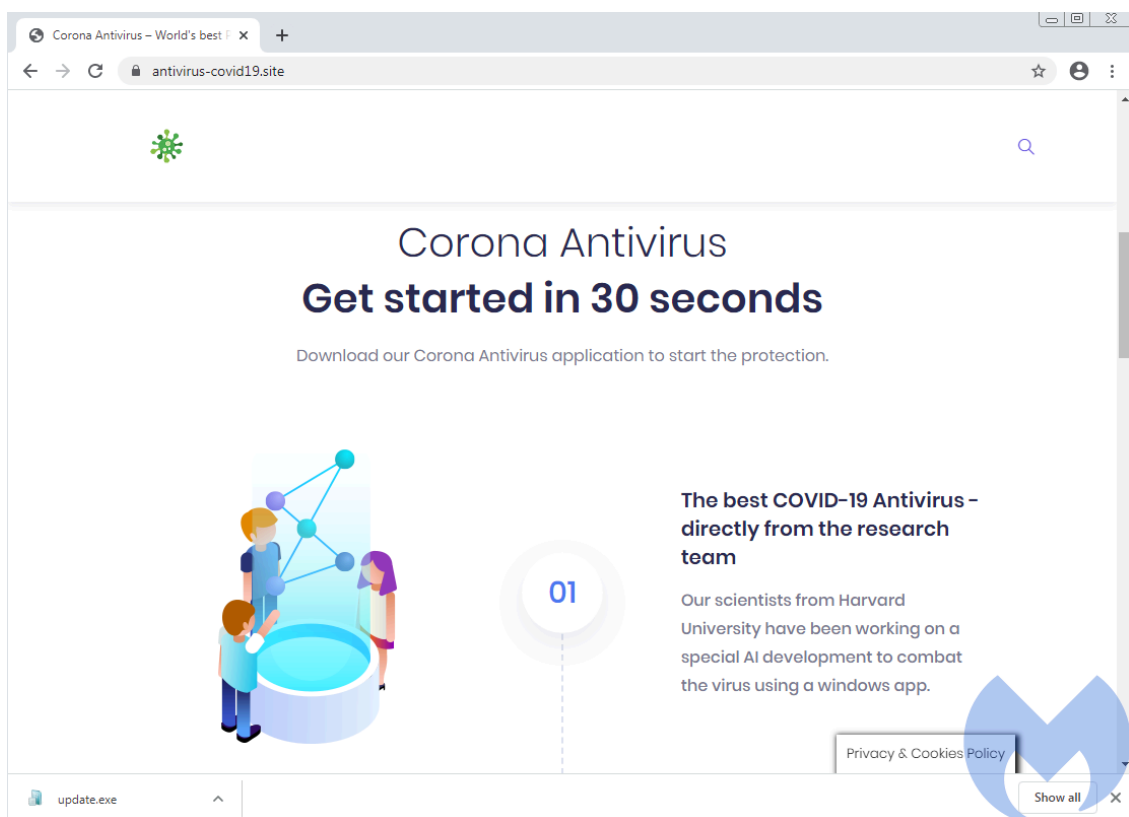
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

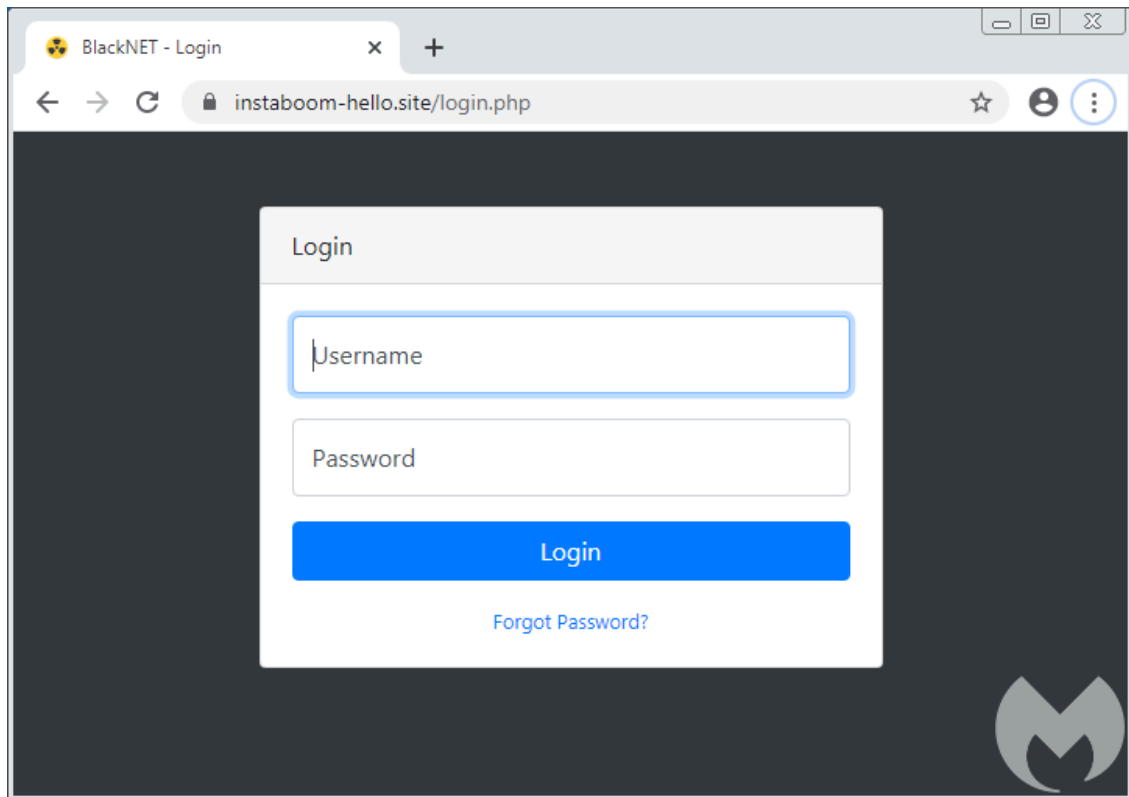


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

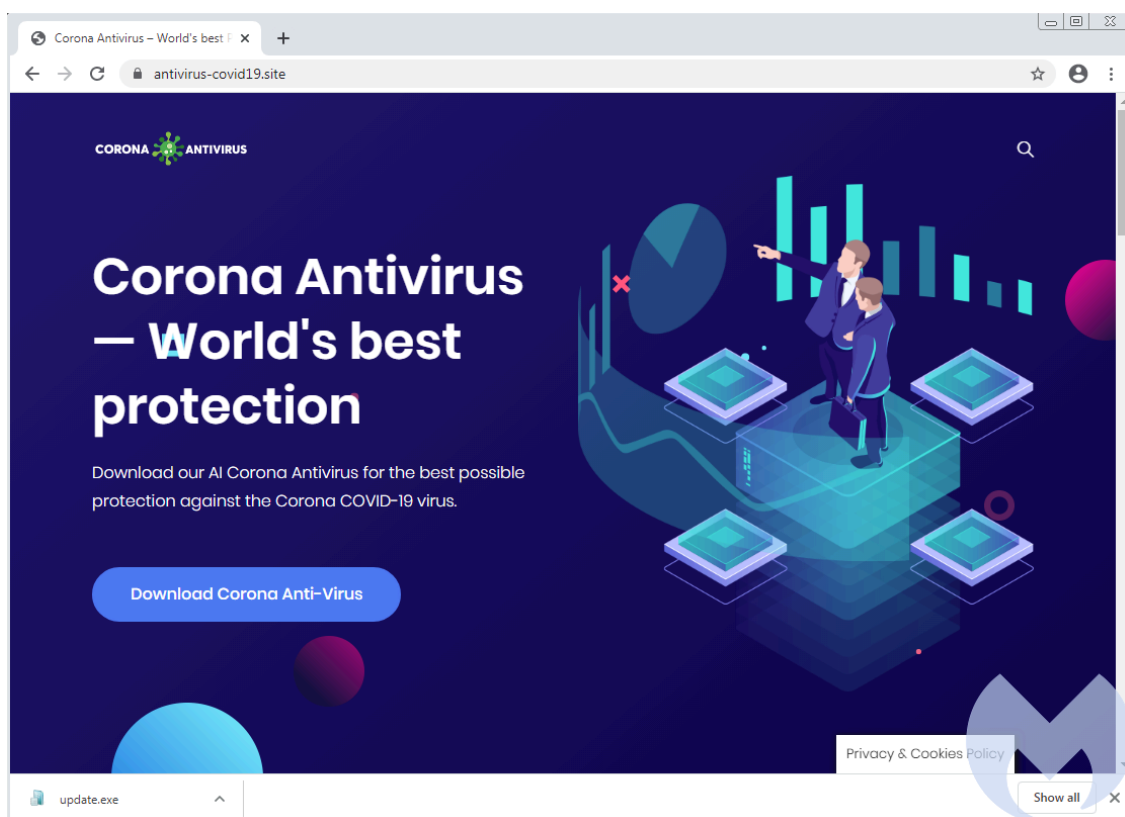
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

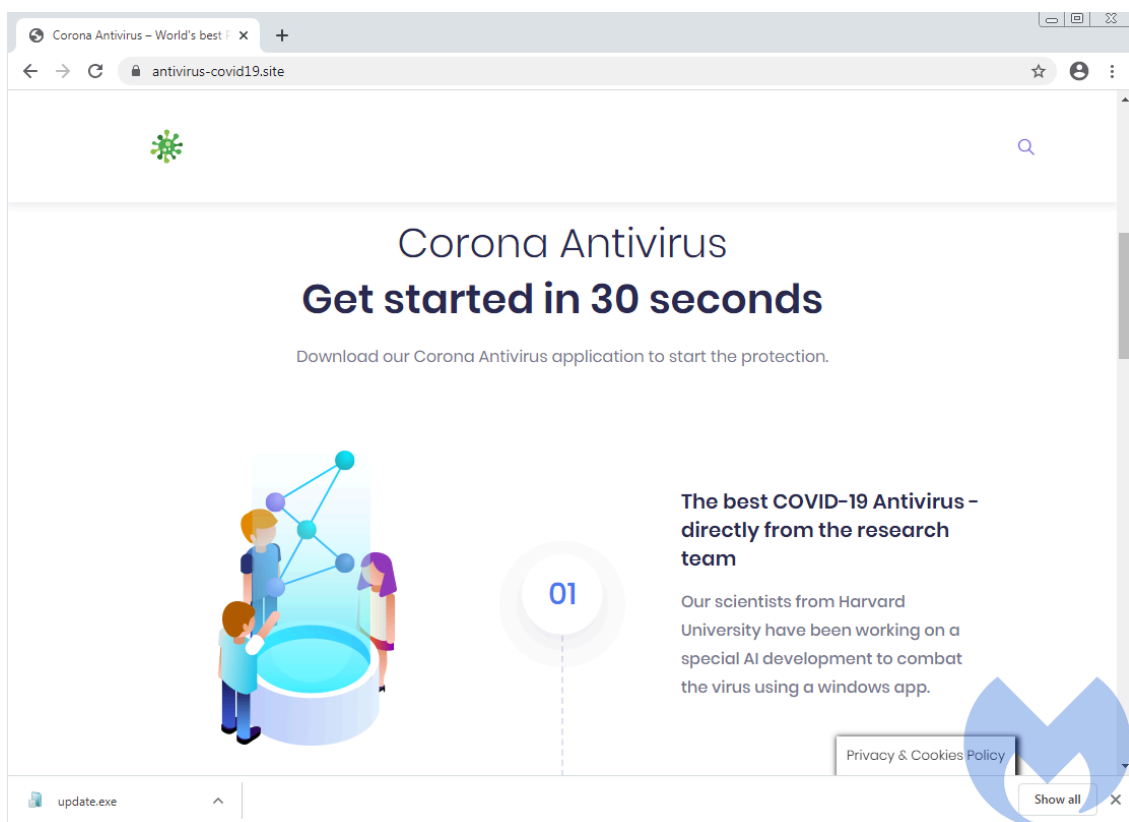
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

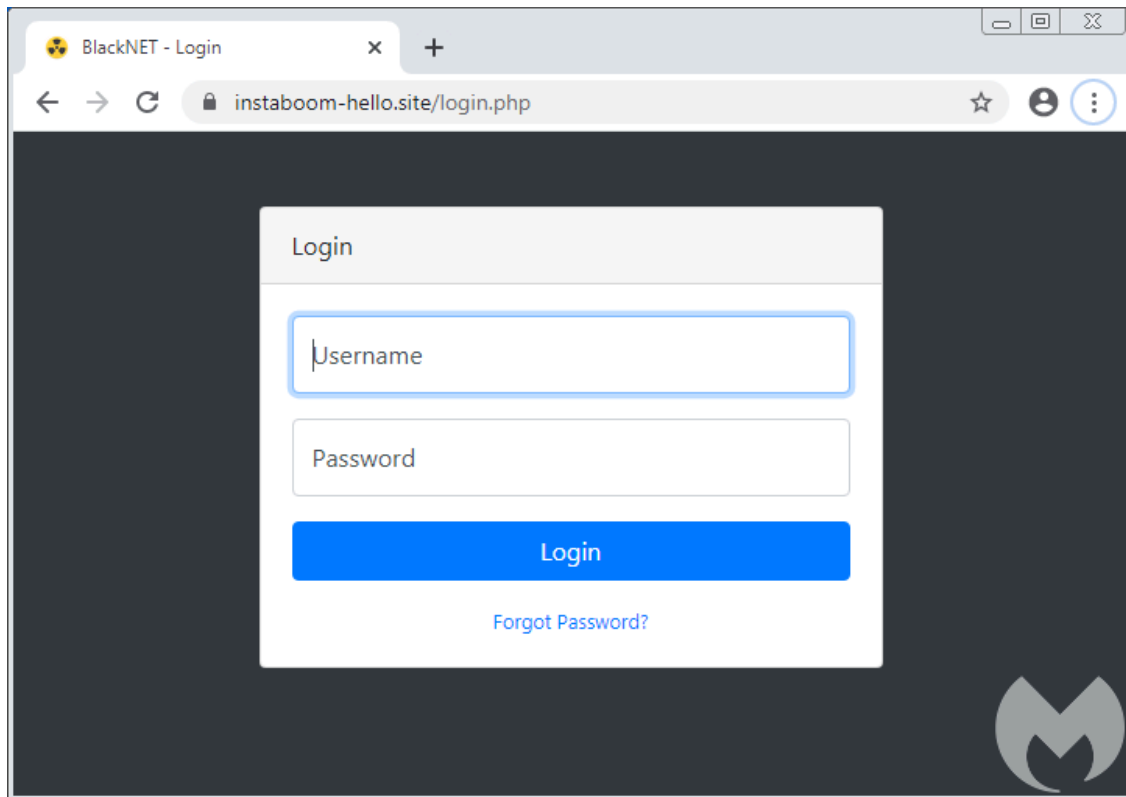


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

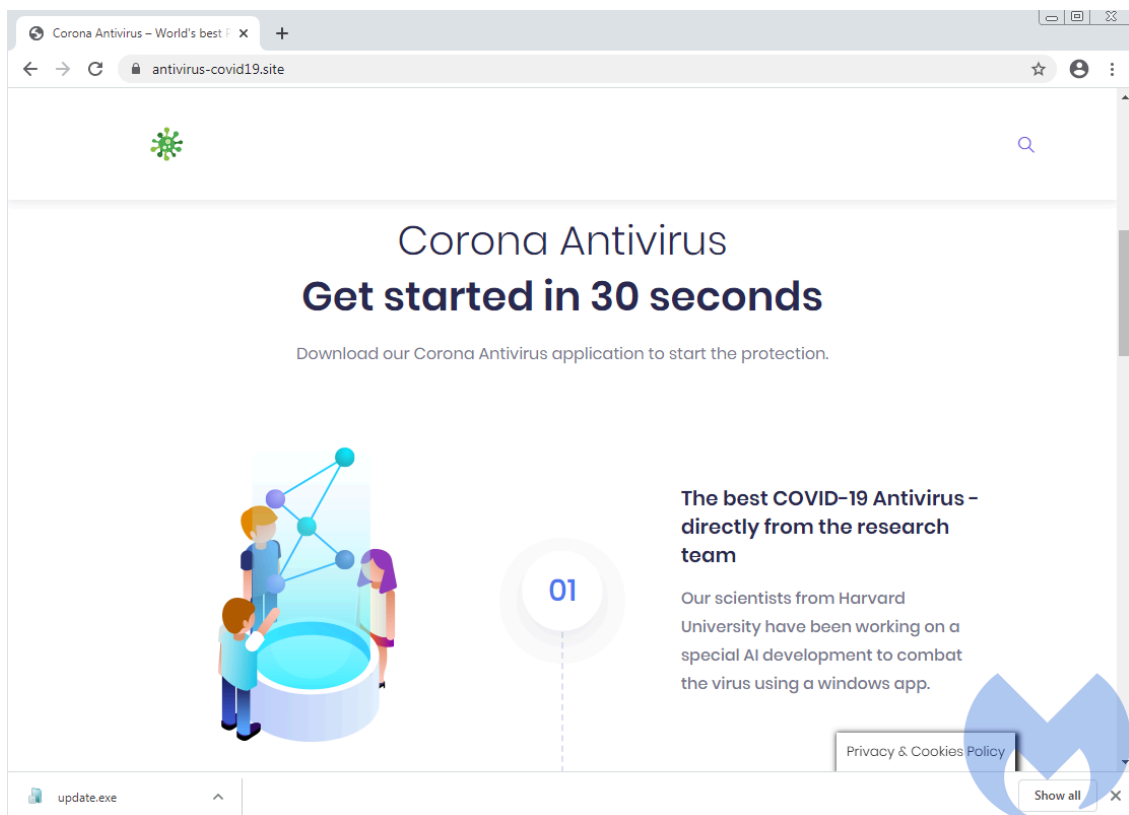
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

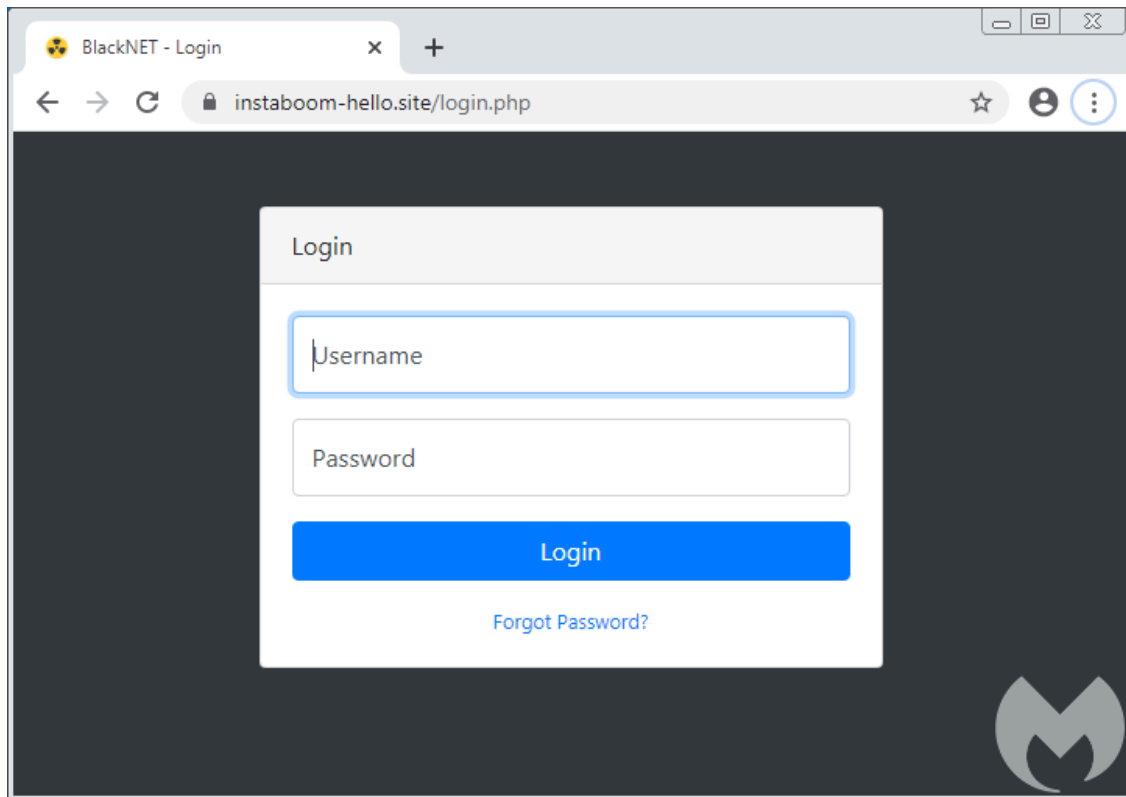


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

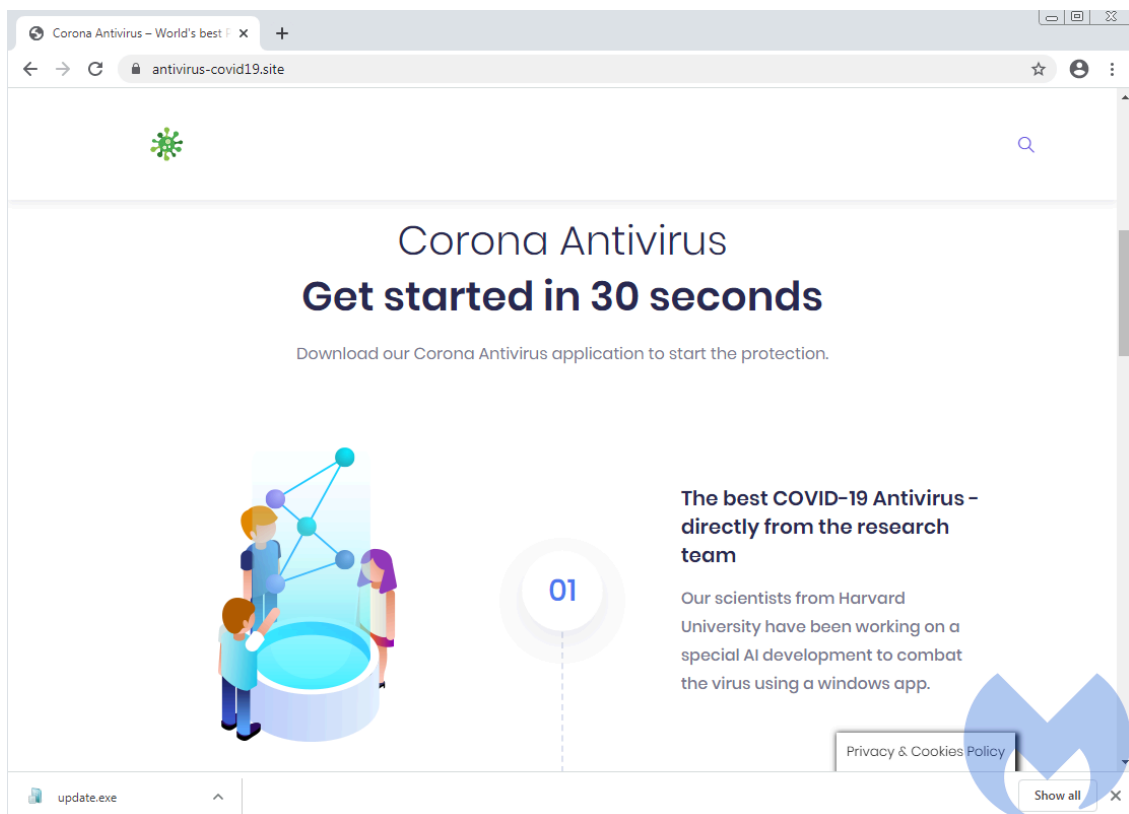
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

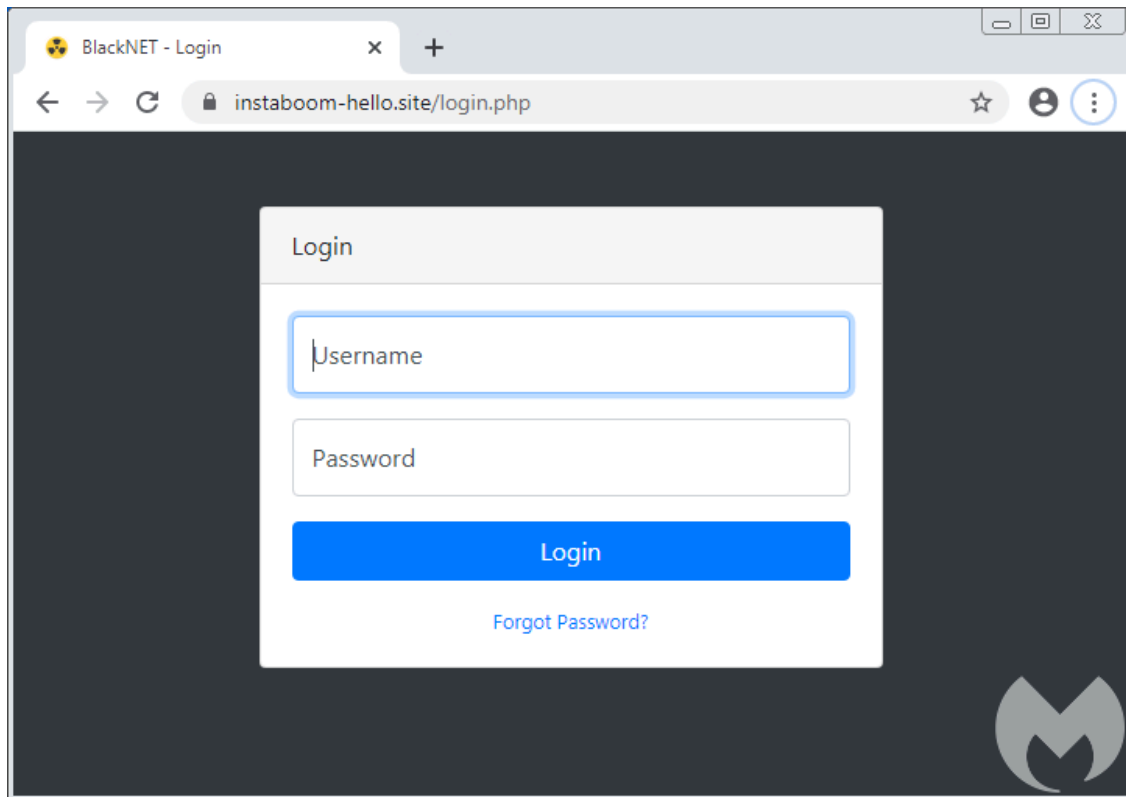


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

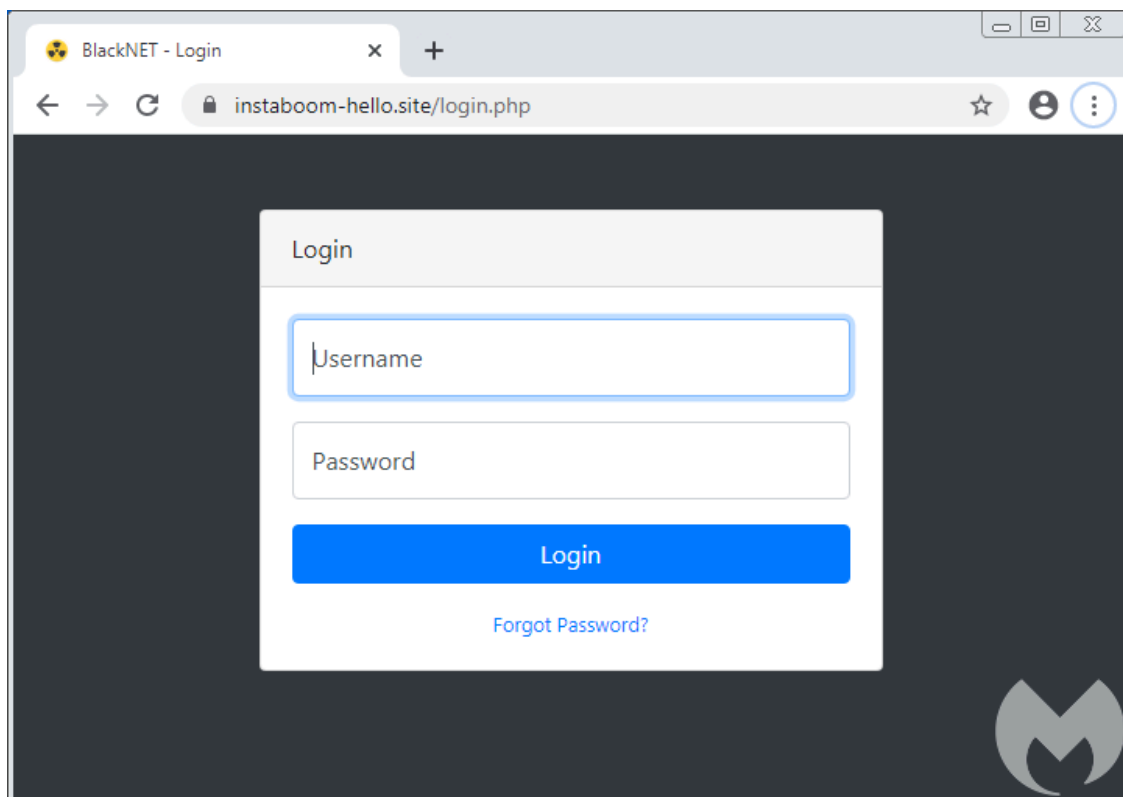
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

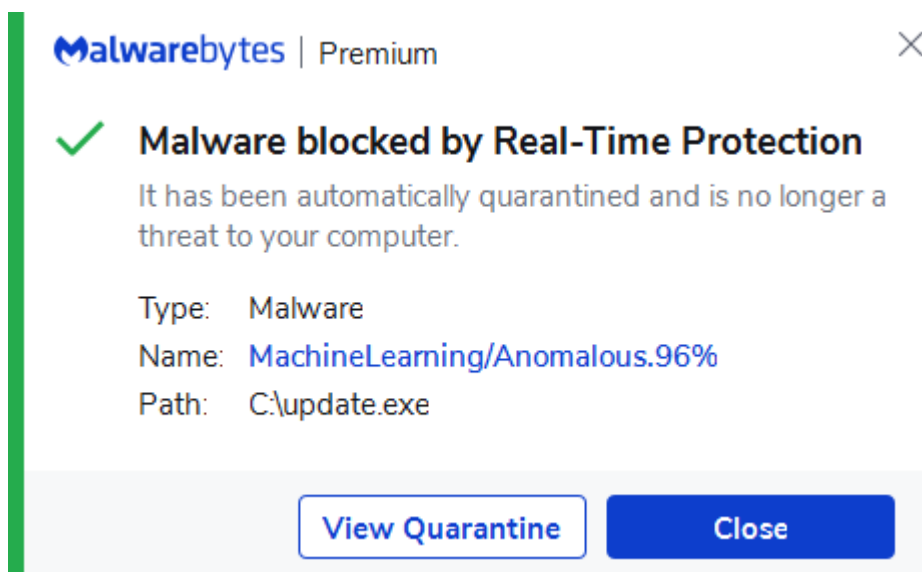
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

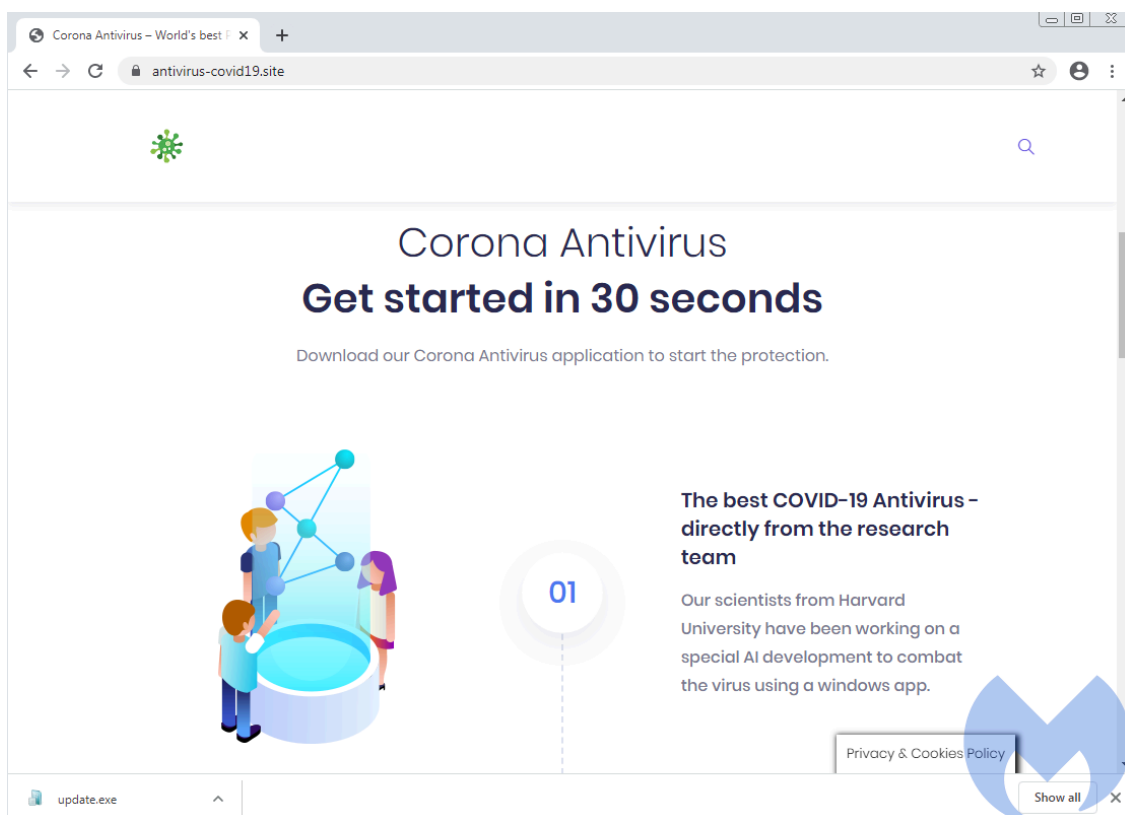
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

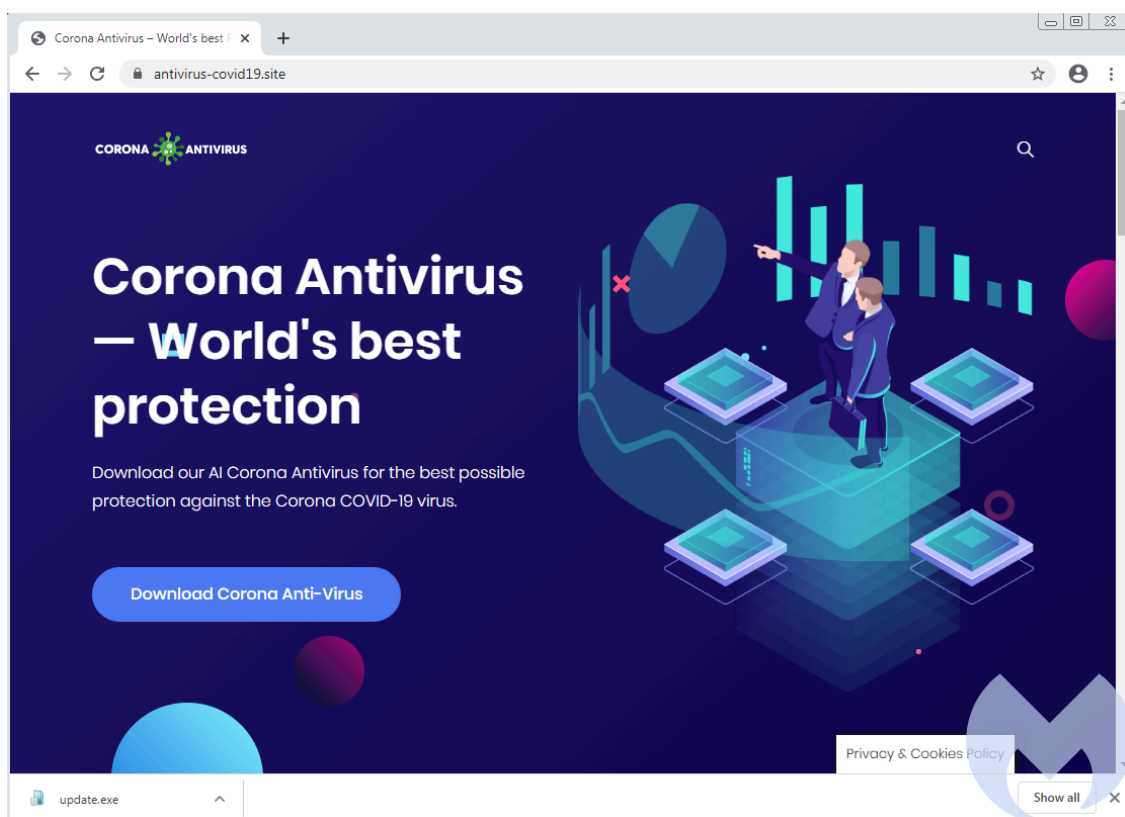
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

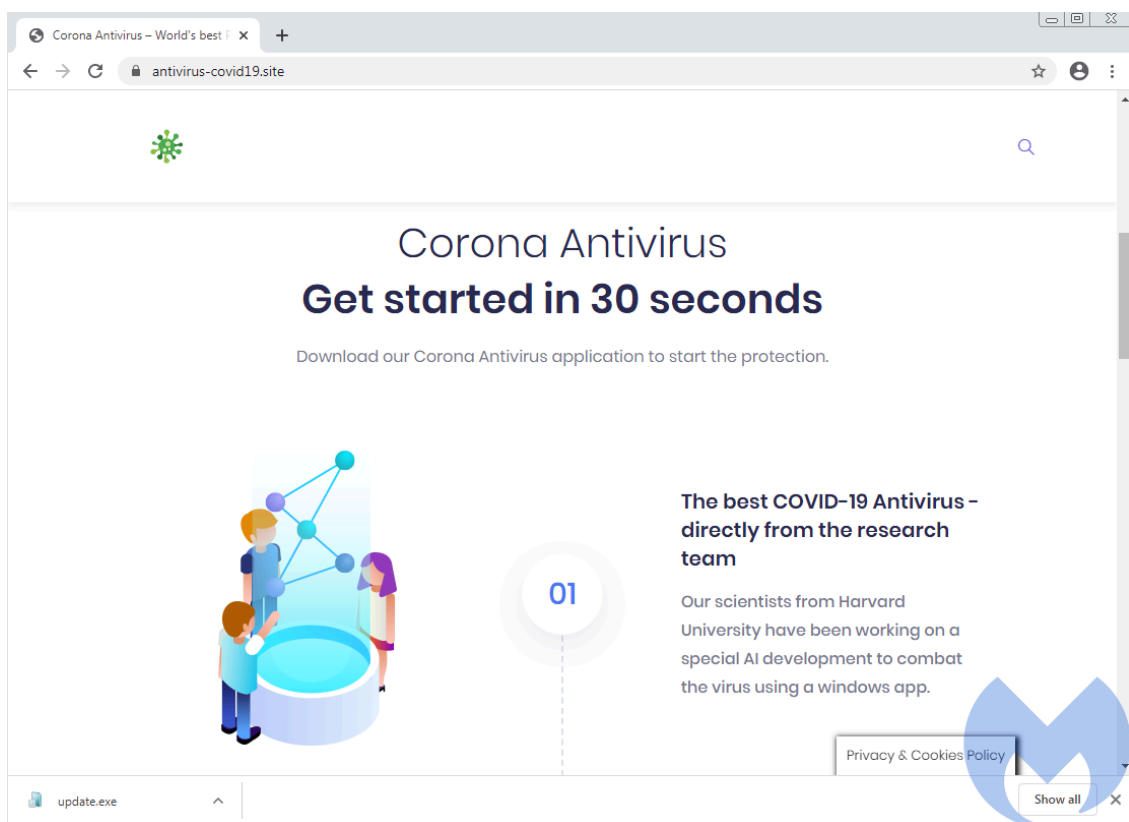
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

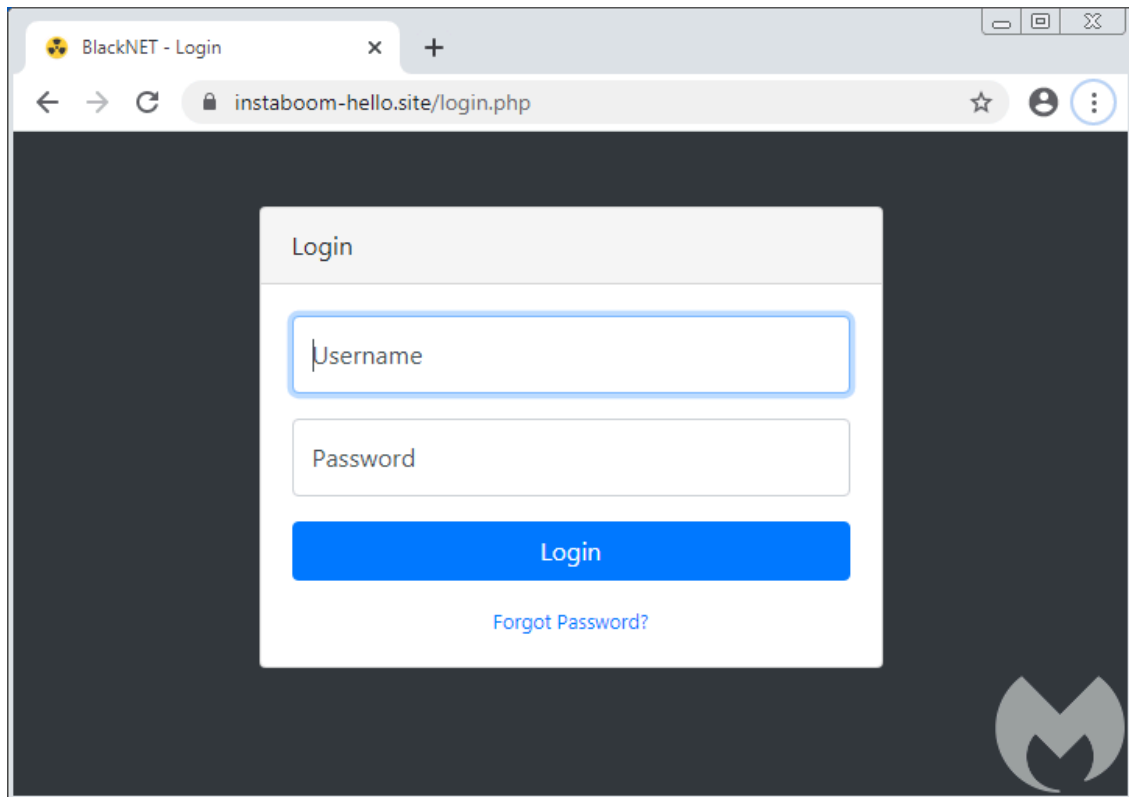


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

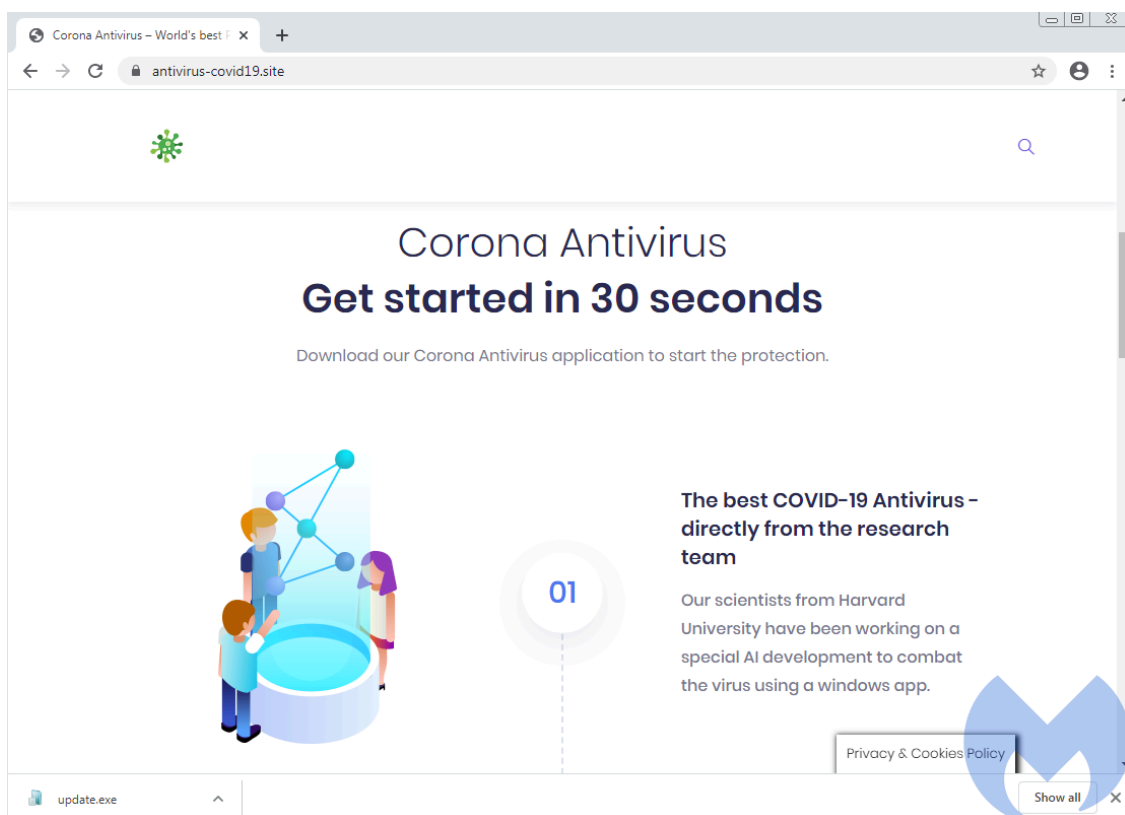
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

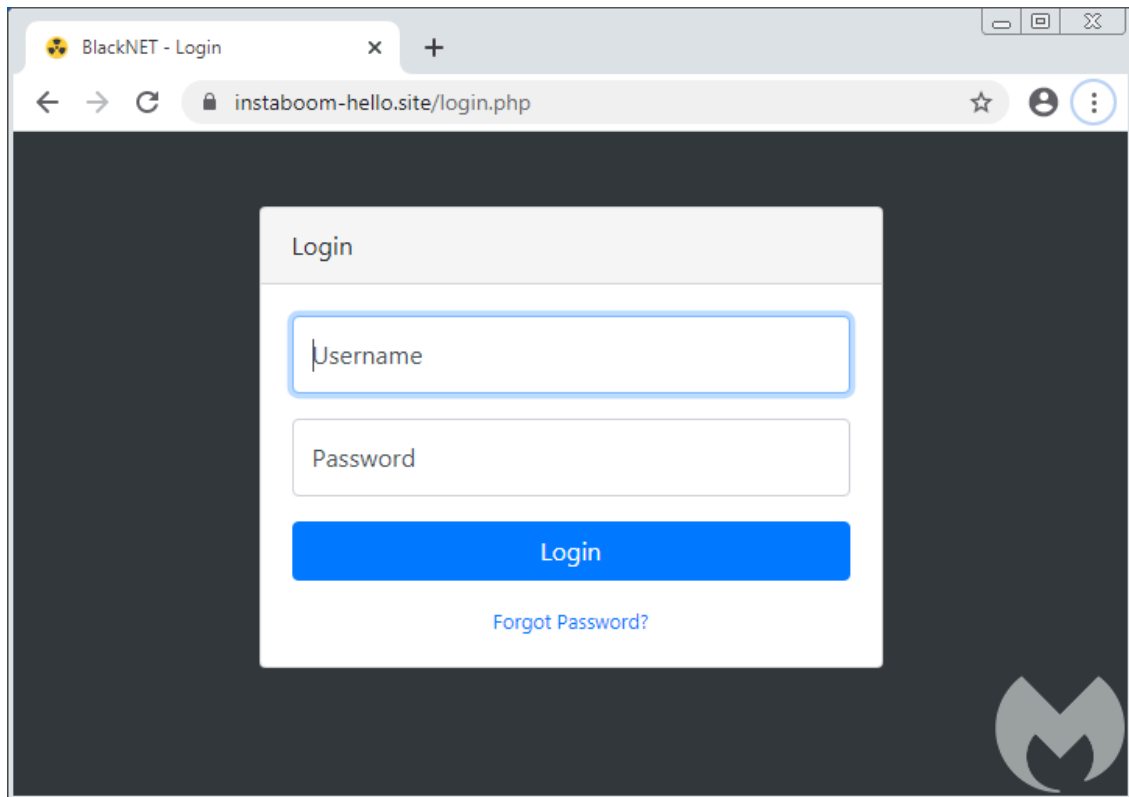


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue dot indicating a client location. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. The window has a green vertical bar on the left and a close button (X) in the top right corner. The main content area features a green checkmark icon and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

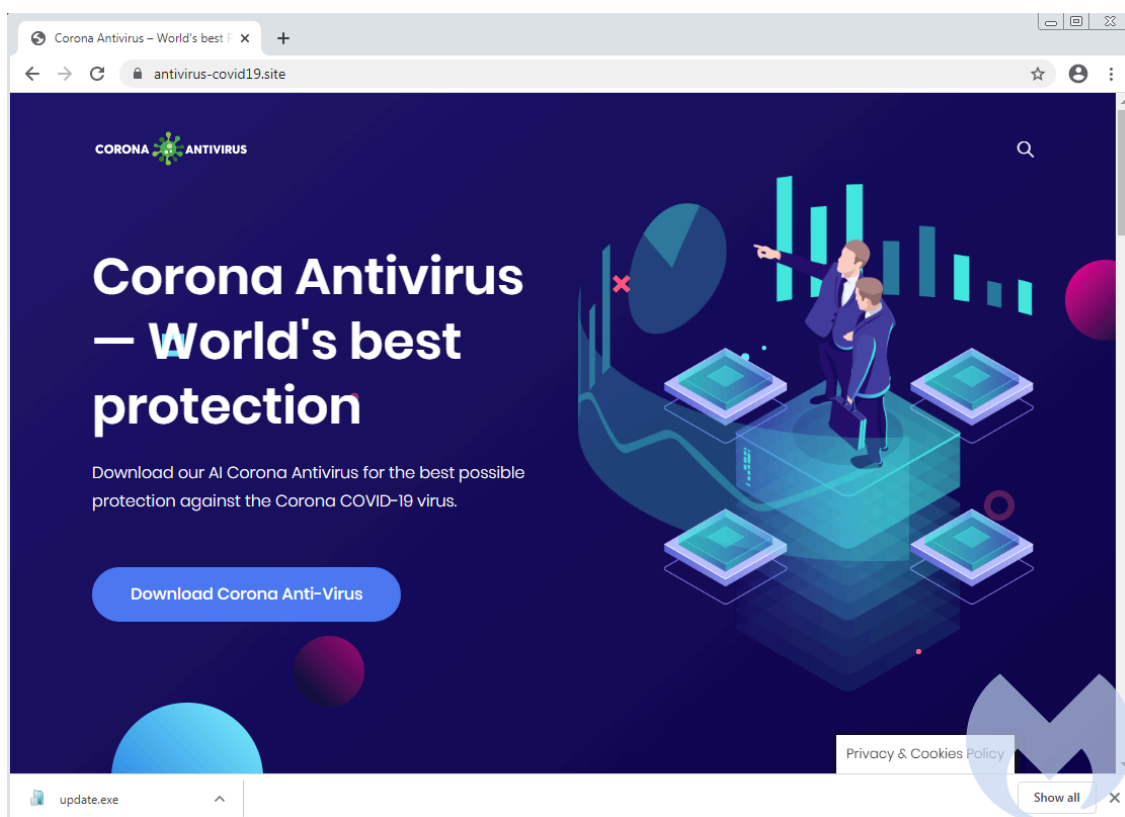
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

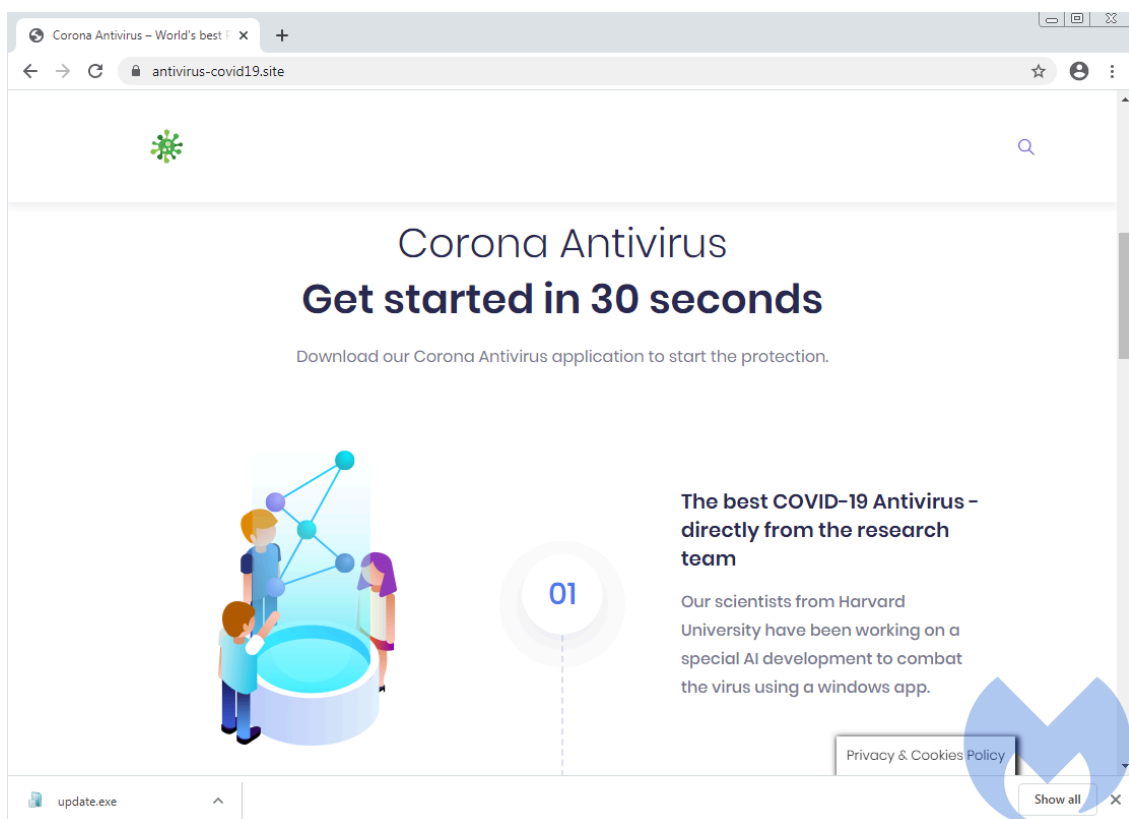
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

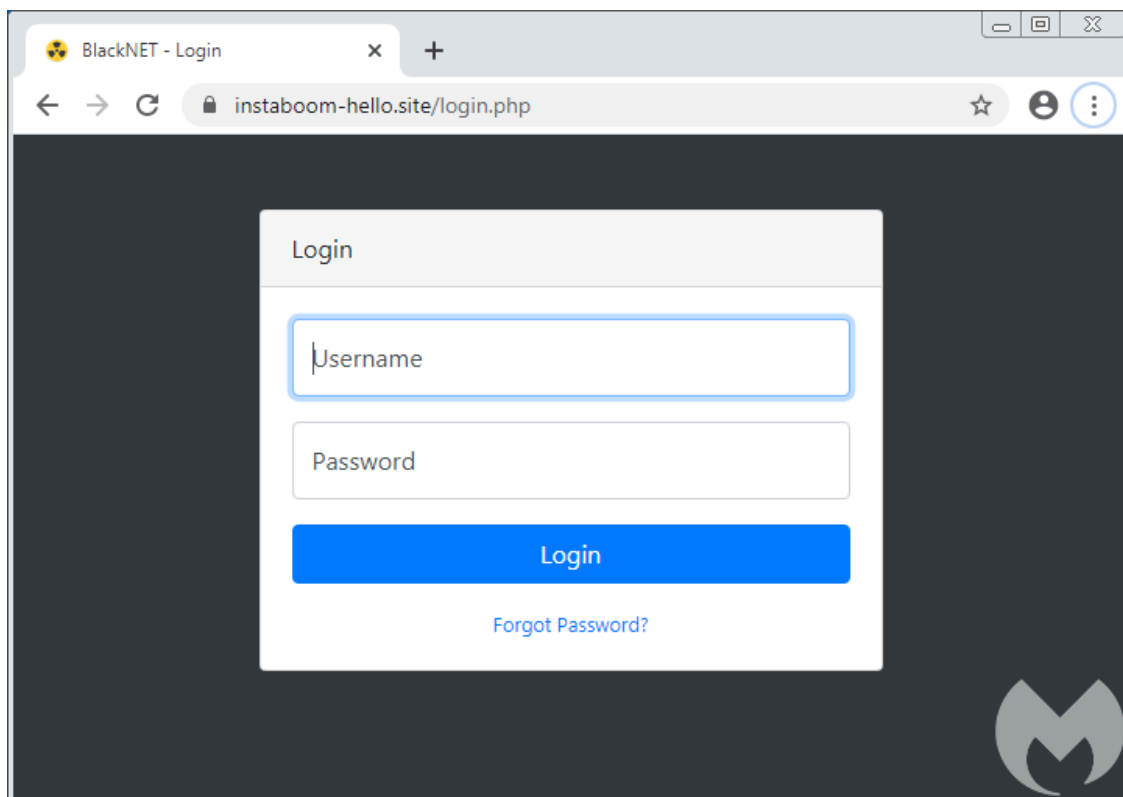
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

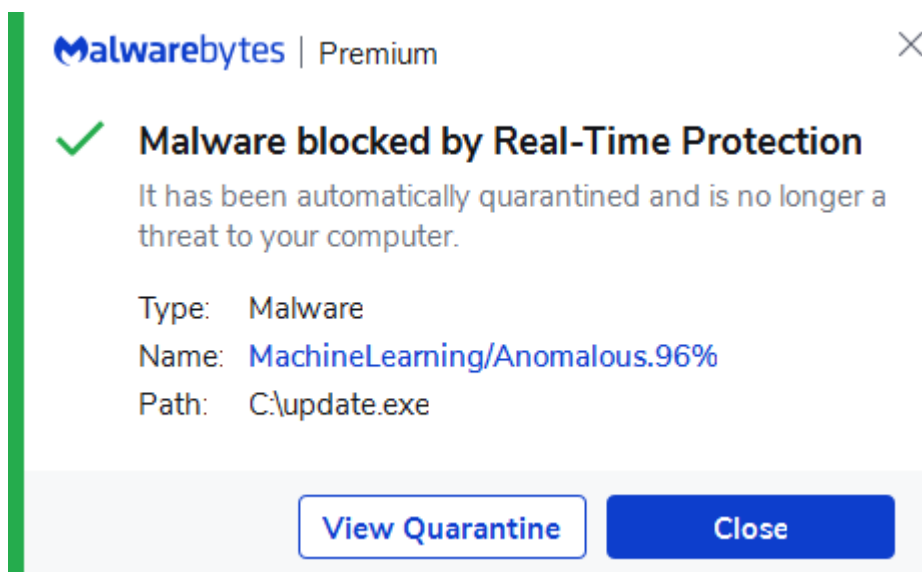
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

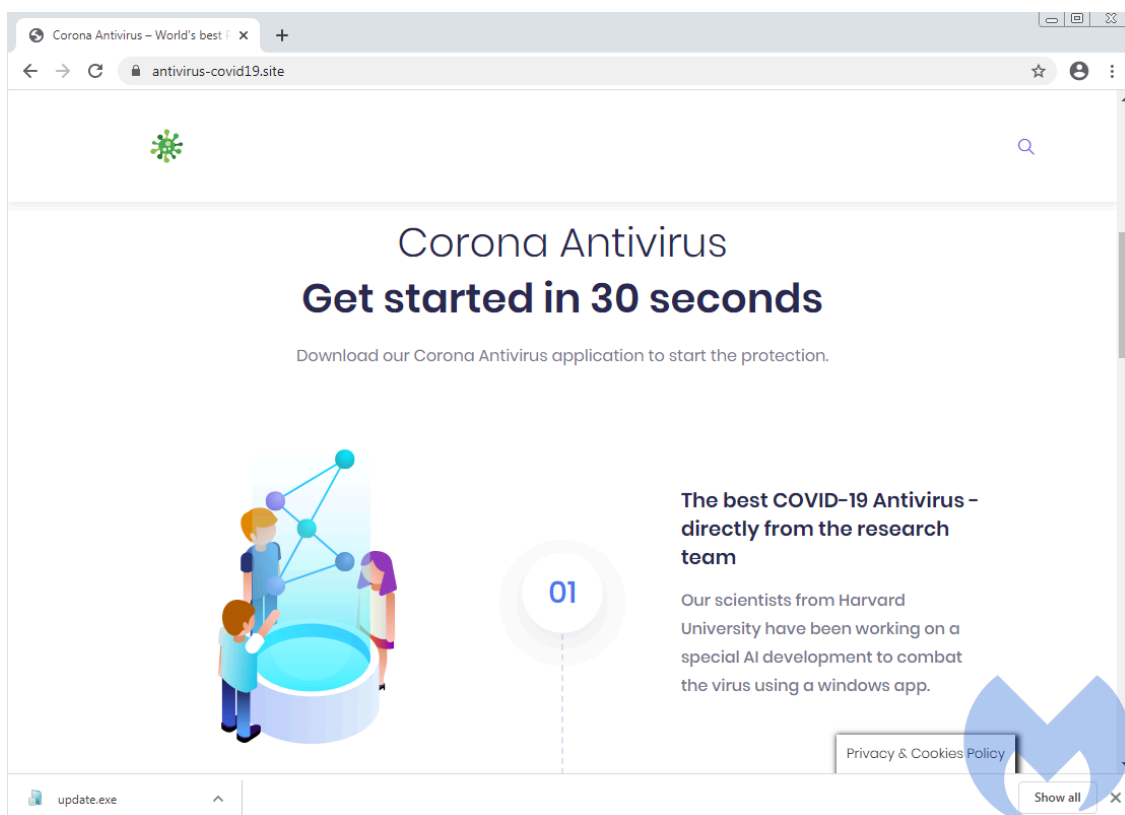
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

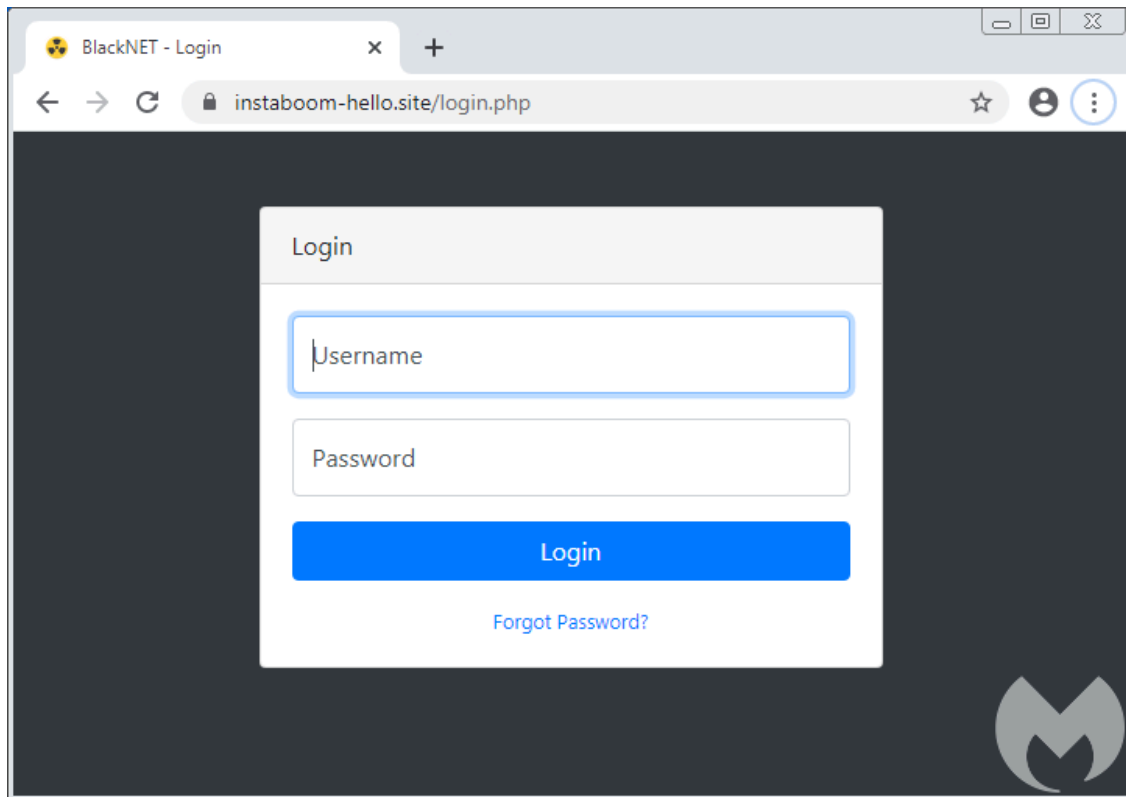



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

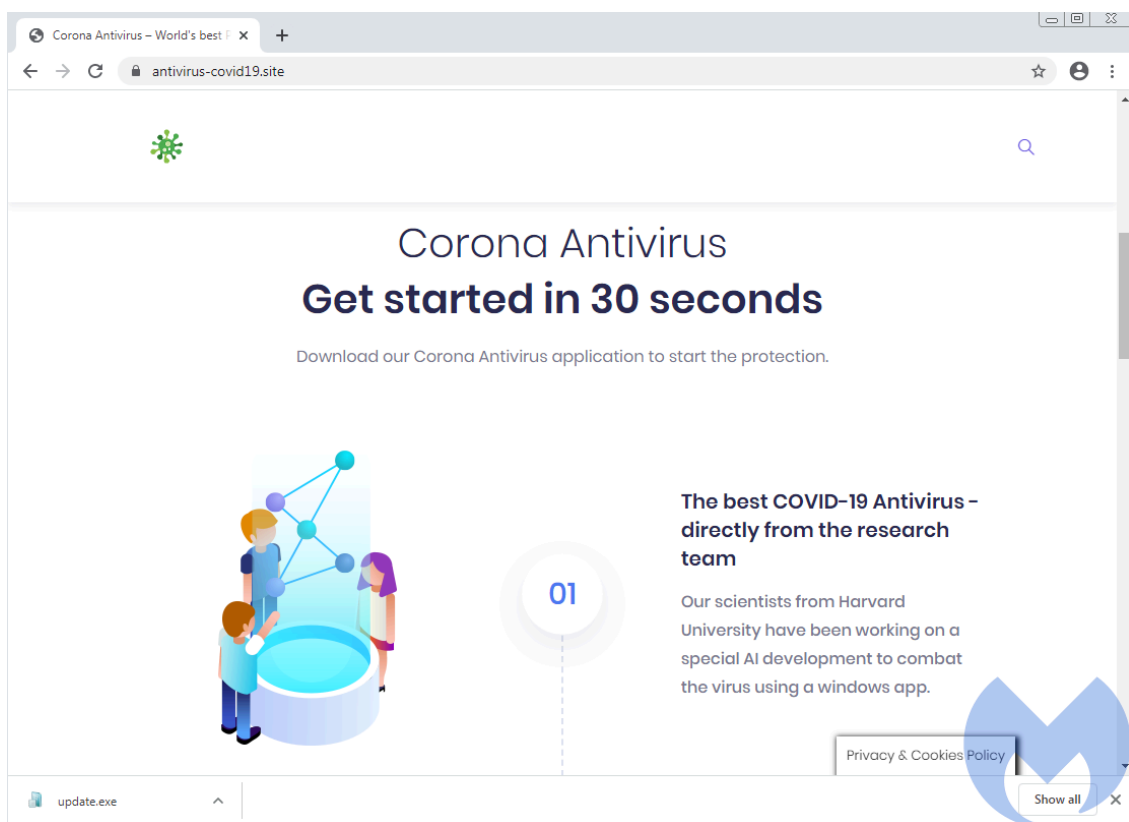
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

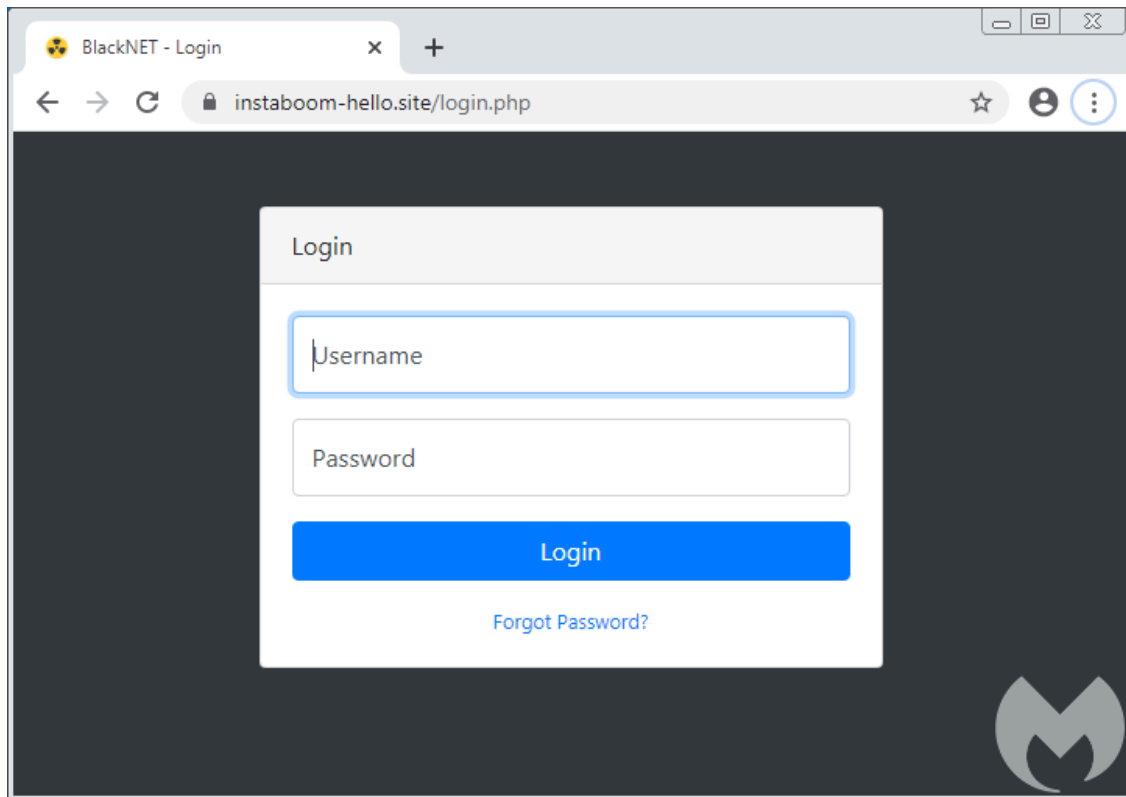


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

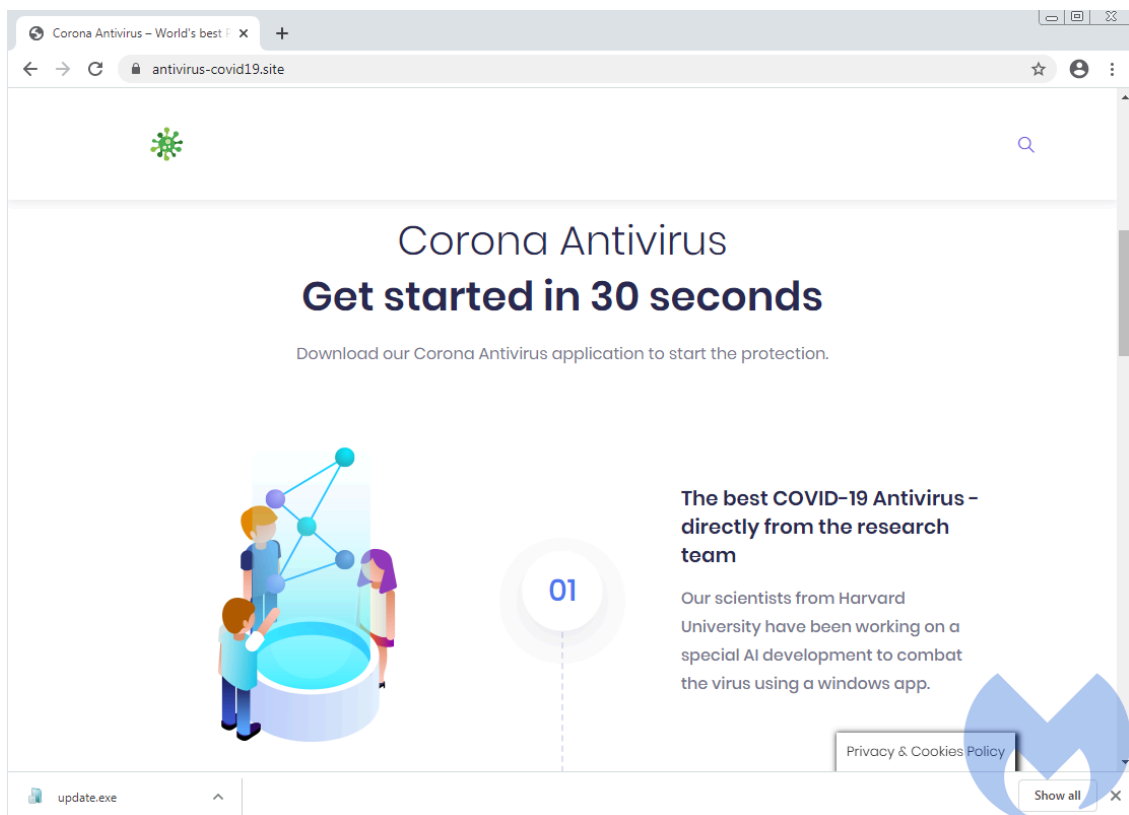
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

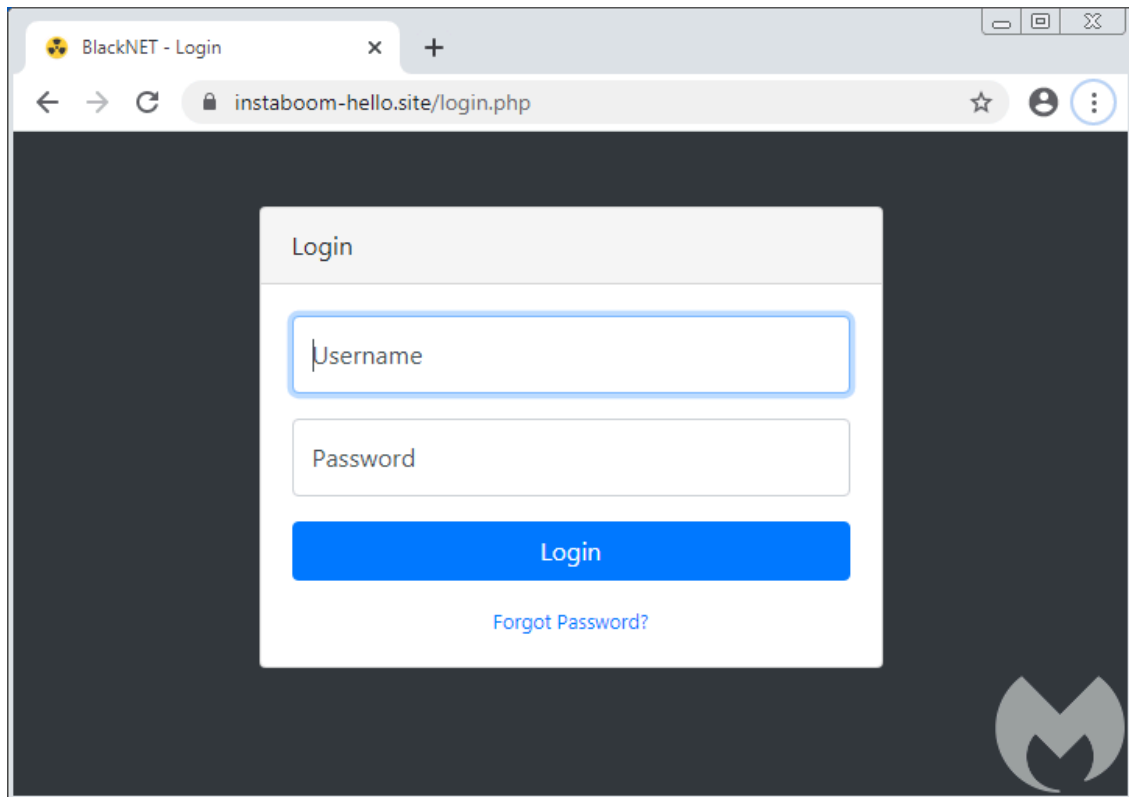


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

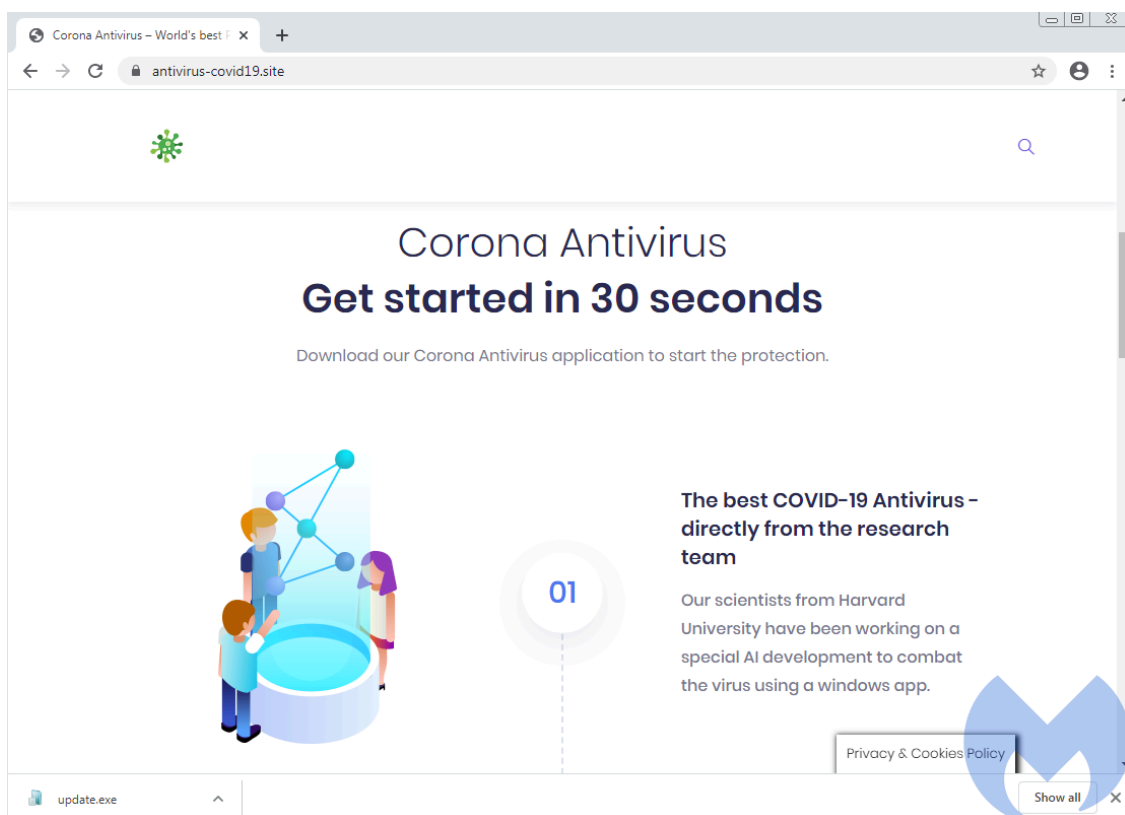
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

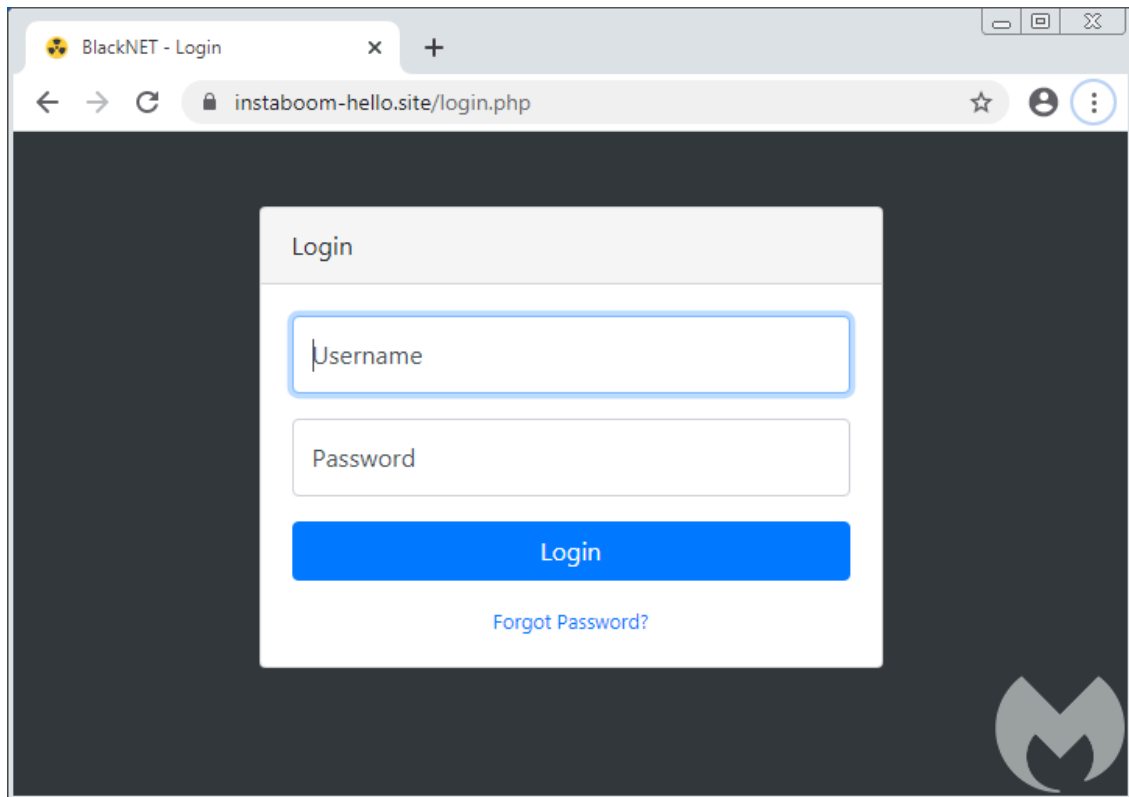


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

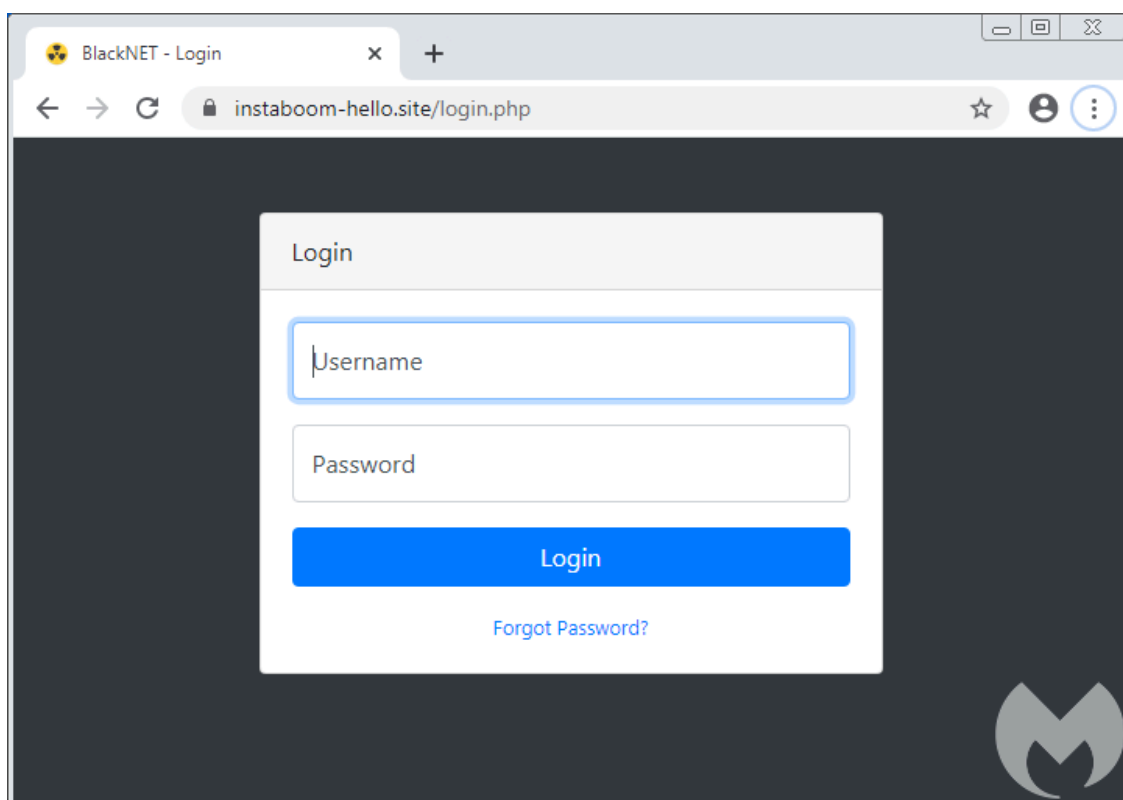
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

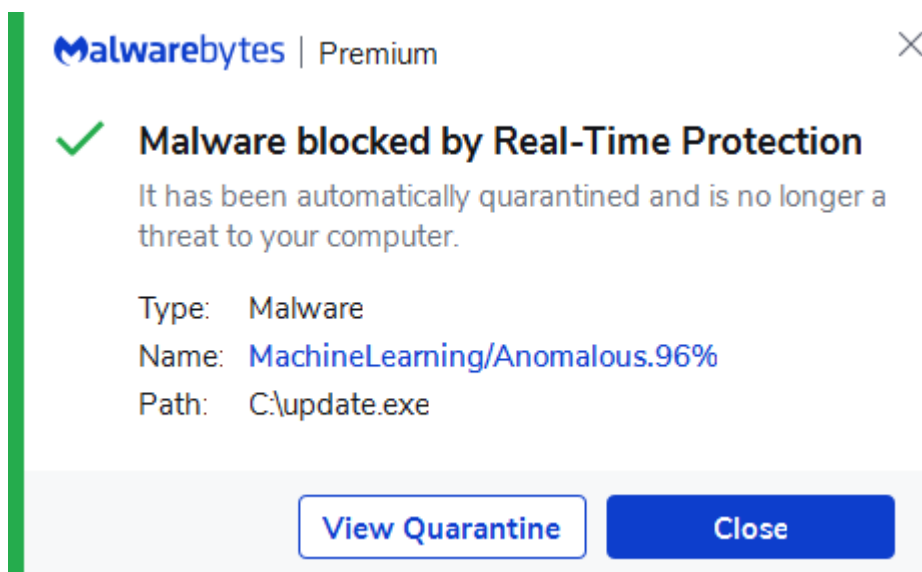
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

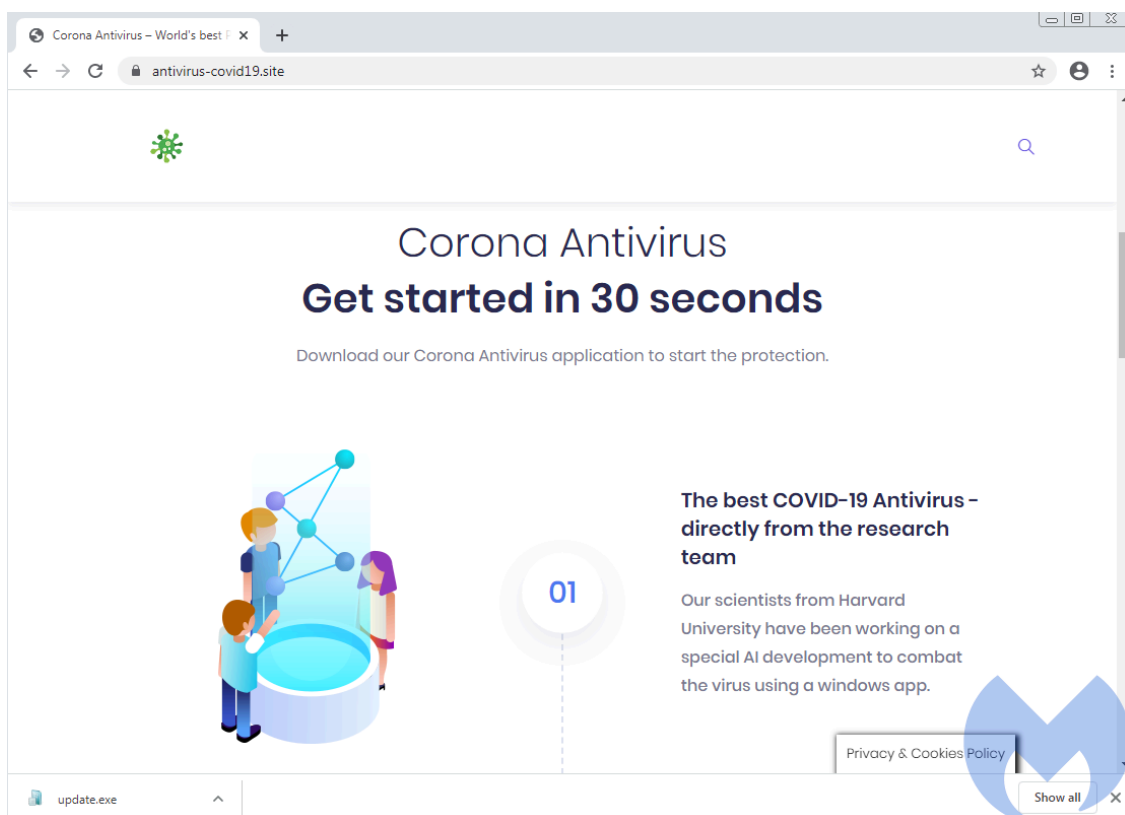
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

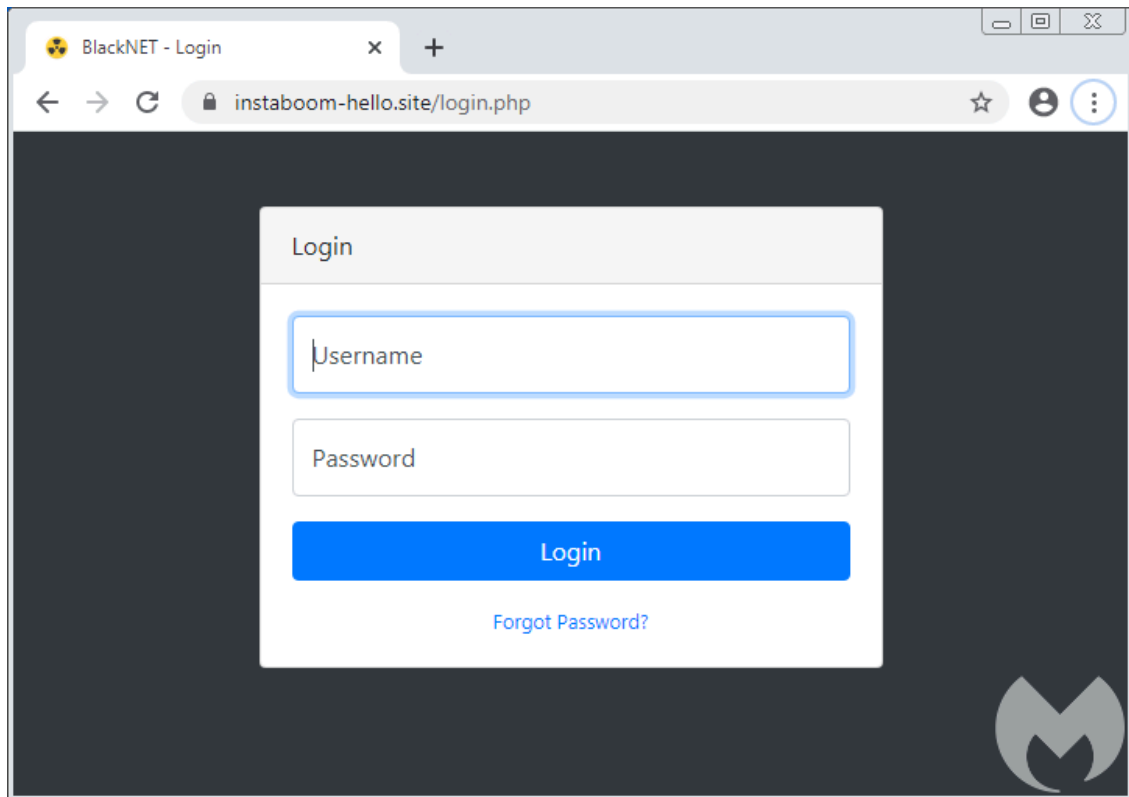


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

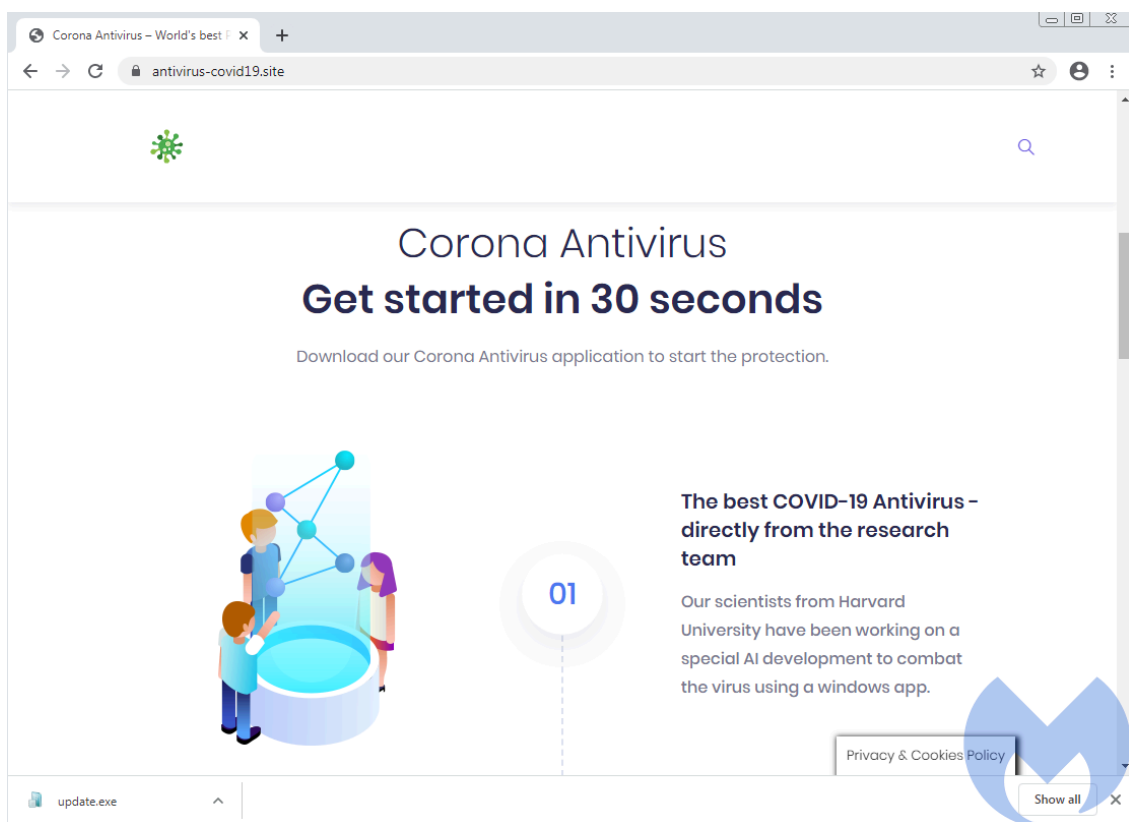
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

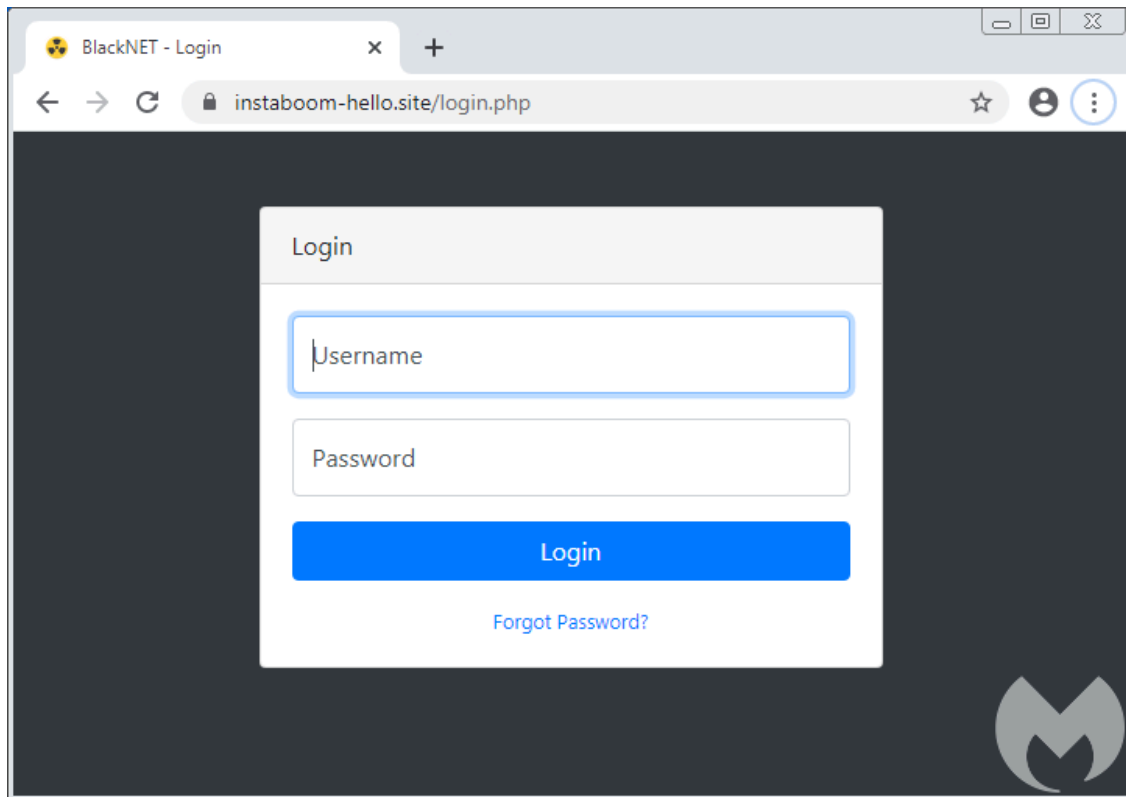


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

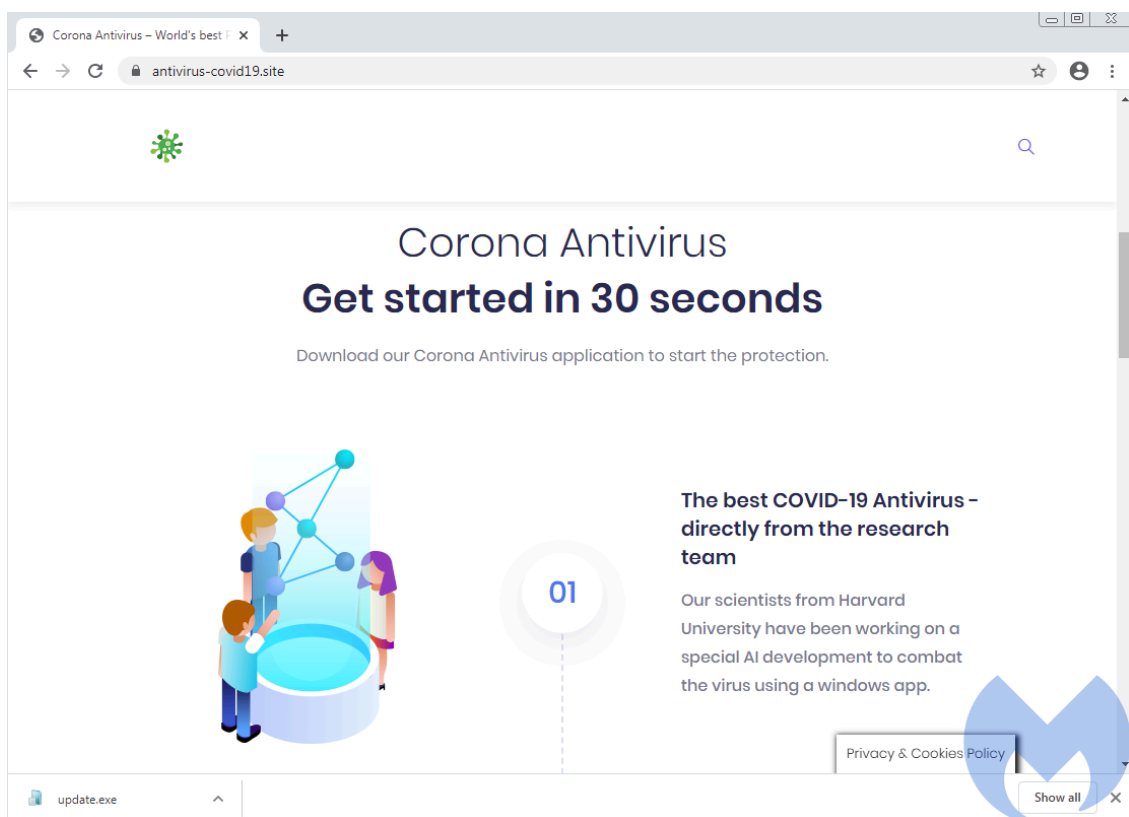
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

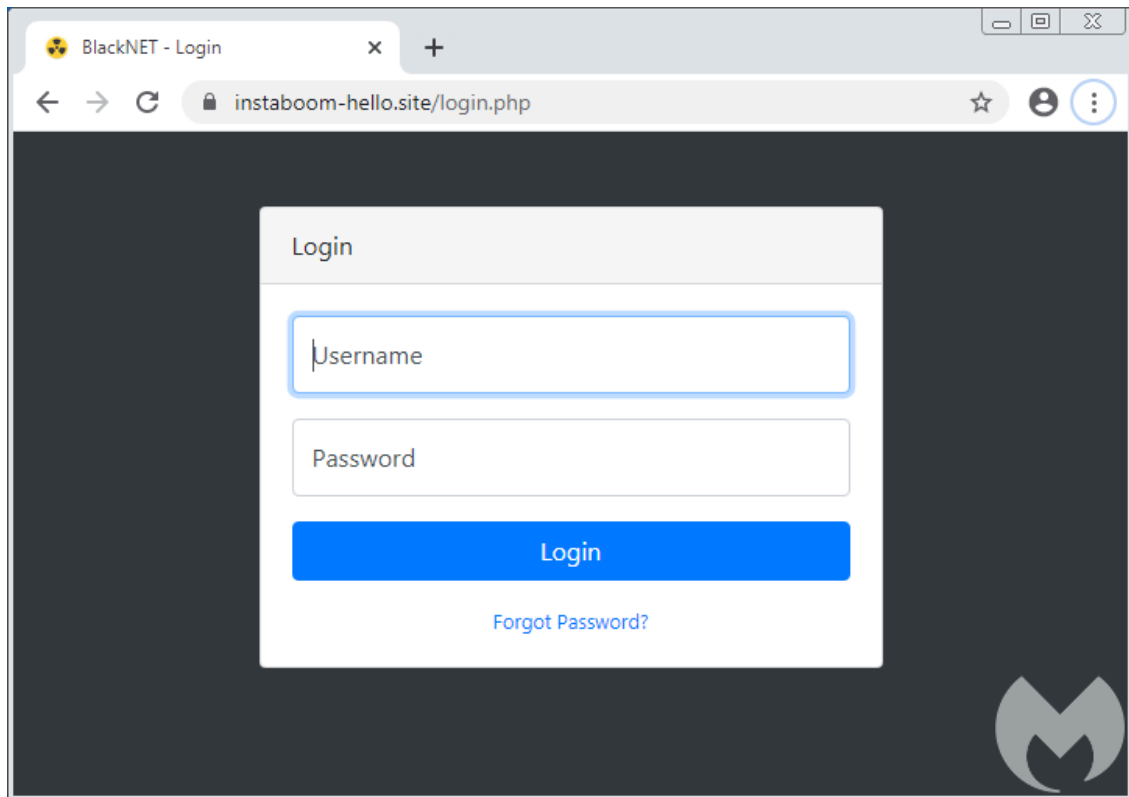


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Malwarebytes | Premium

✓ **Malware blocked by Real-Time Protection**

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: MachineLearning/Anomalous.96%

Path: C:\update.exe

View Quarantine Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

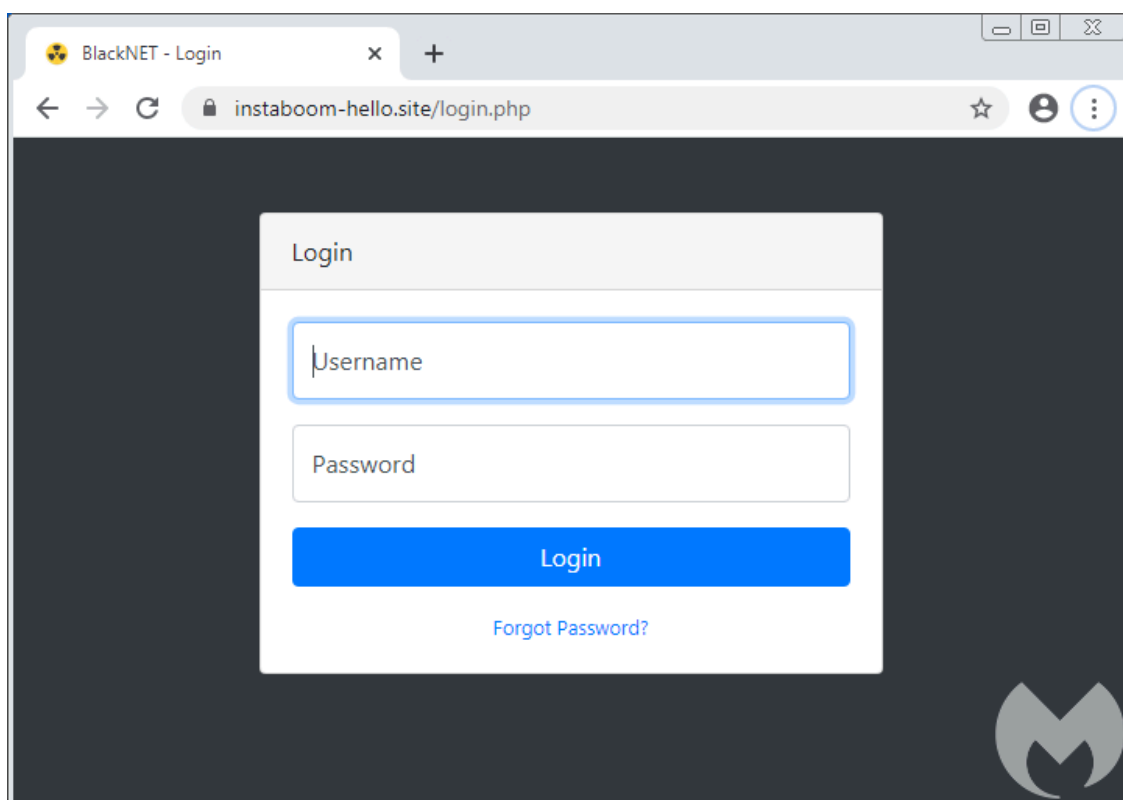
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

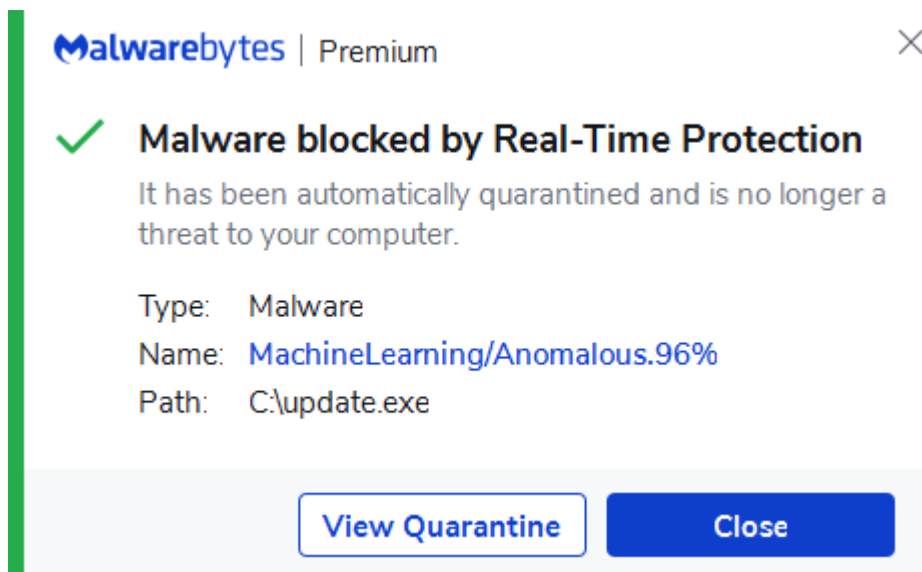
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

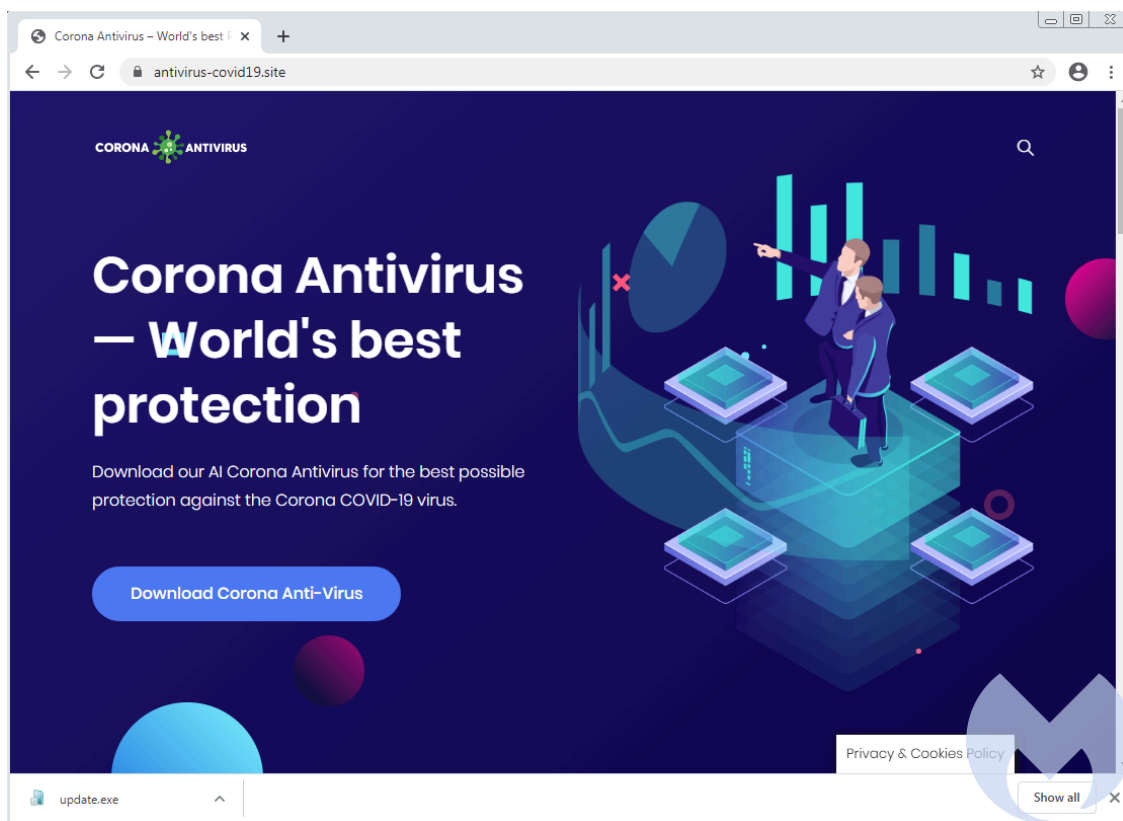
```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

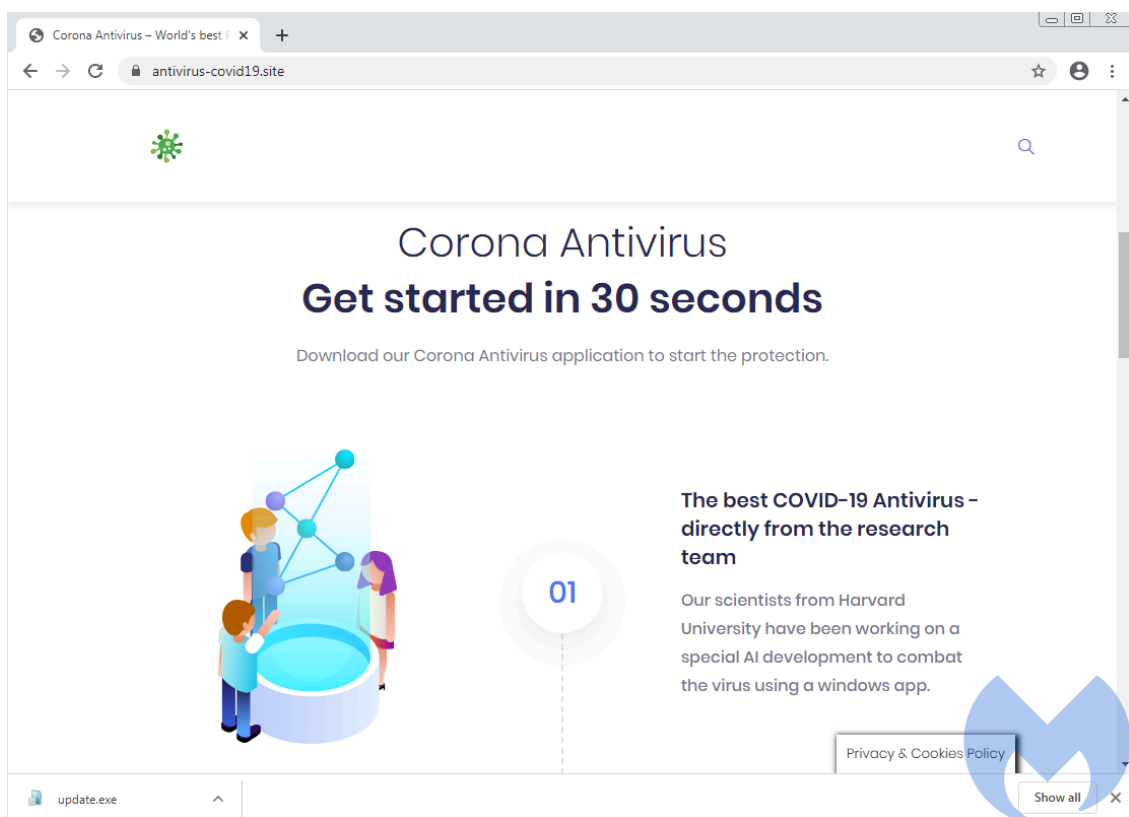
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

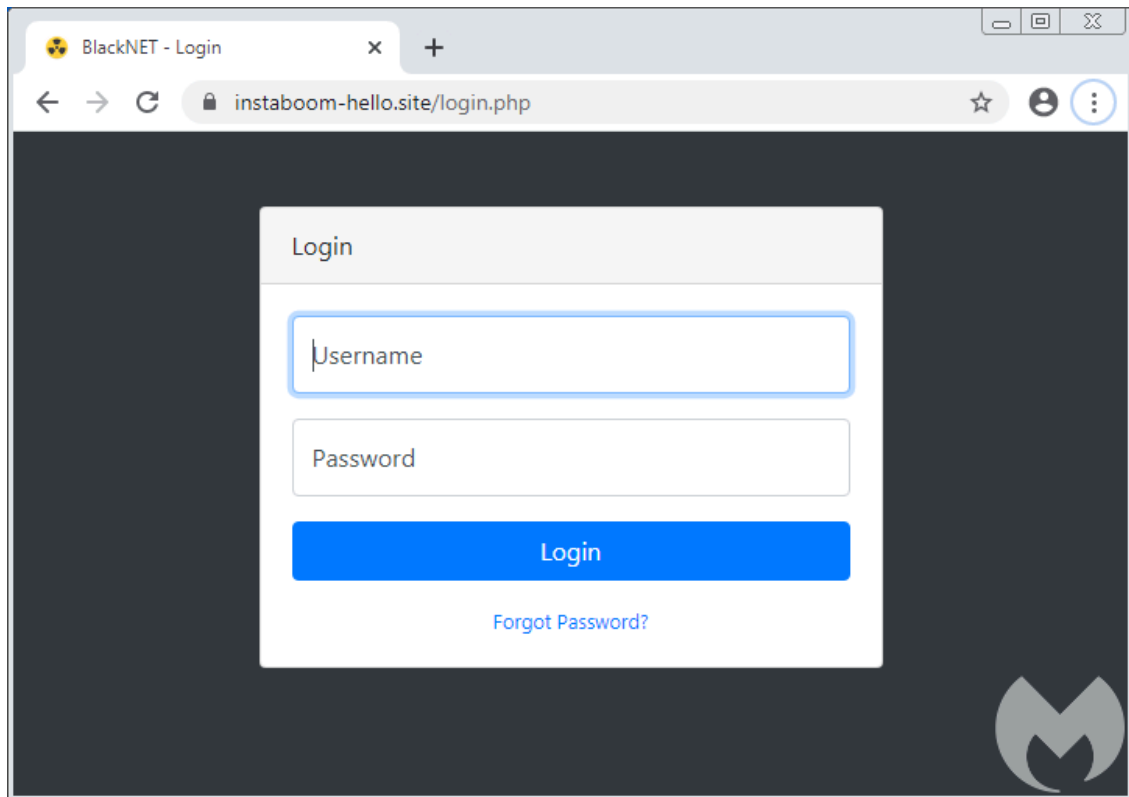


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Malwarebytes | Premium

✓ **Malware blocked by Real-Time Protection**

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: MachineLearning/Anomalous.96%

Path: C:\update.exe

View Quarantine Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

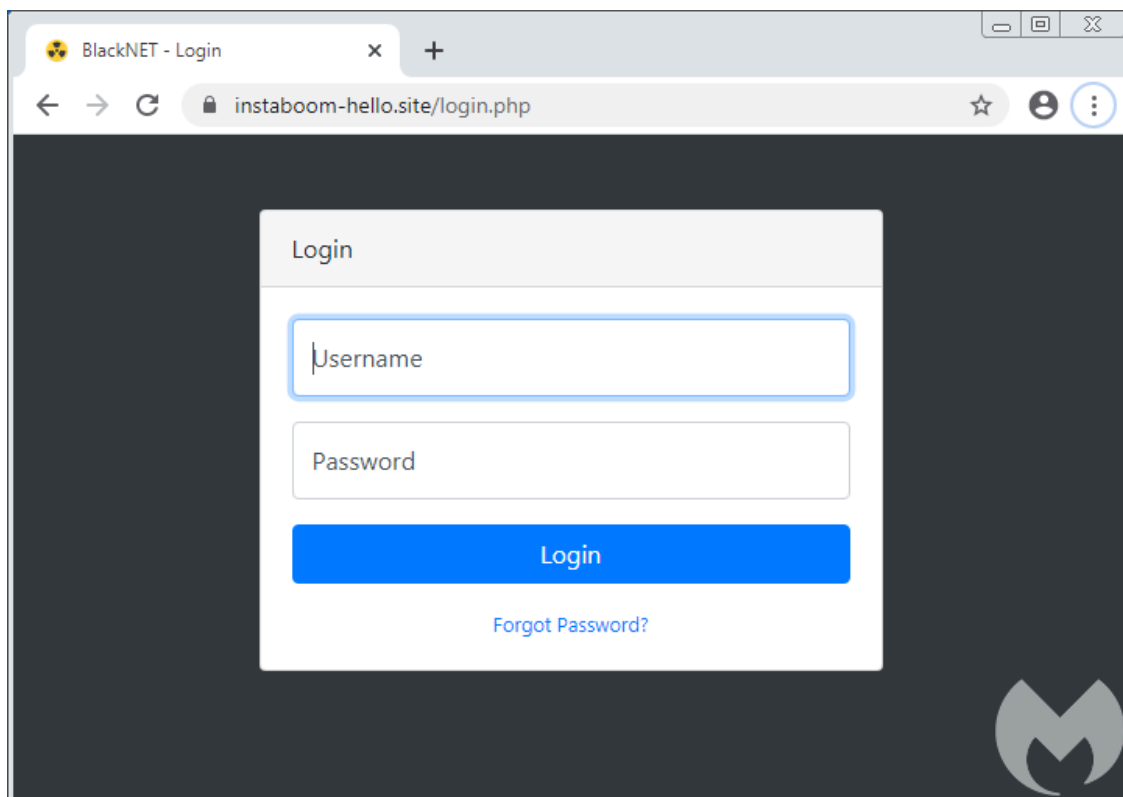
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

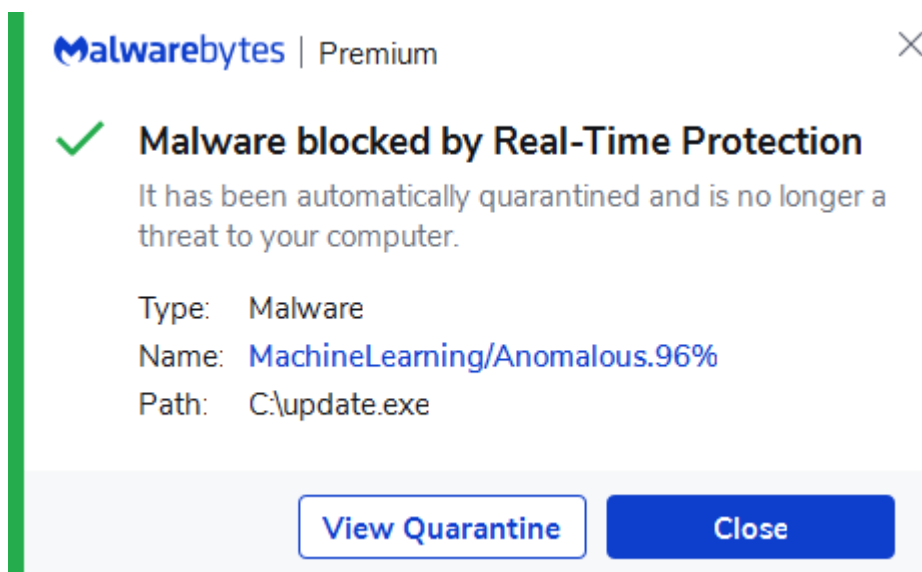
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

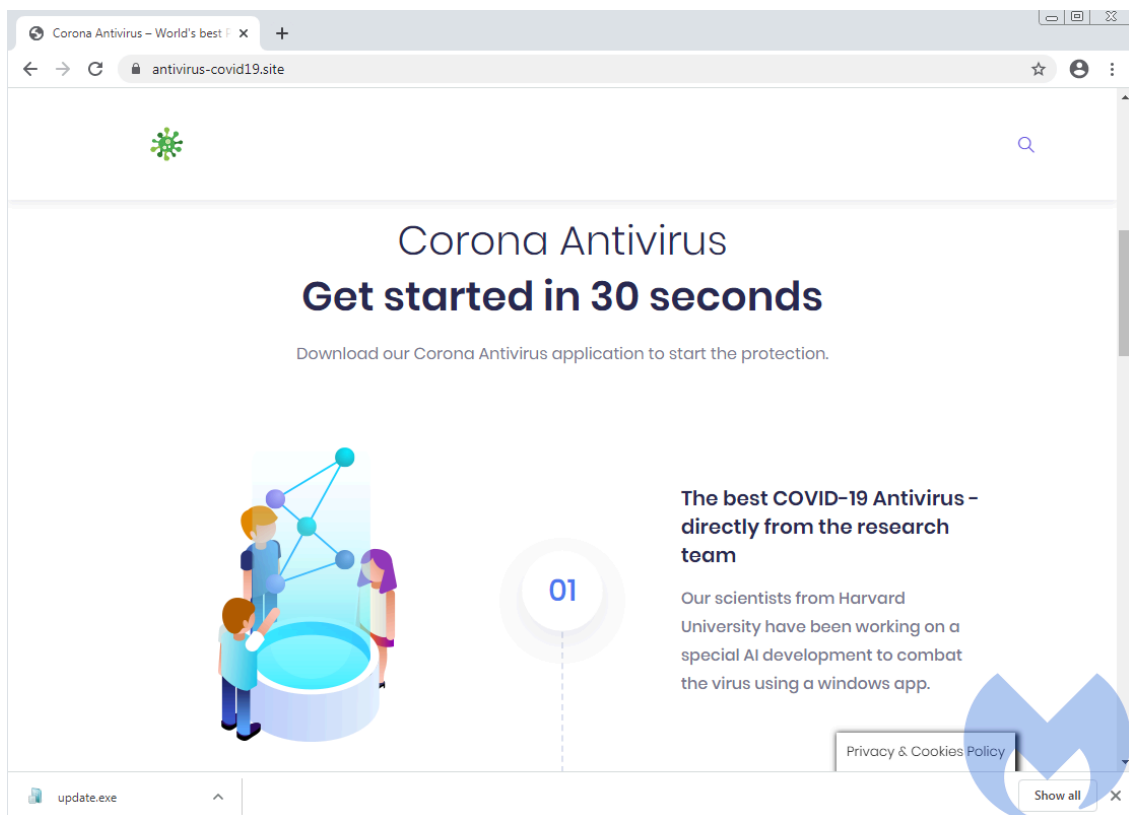
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

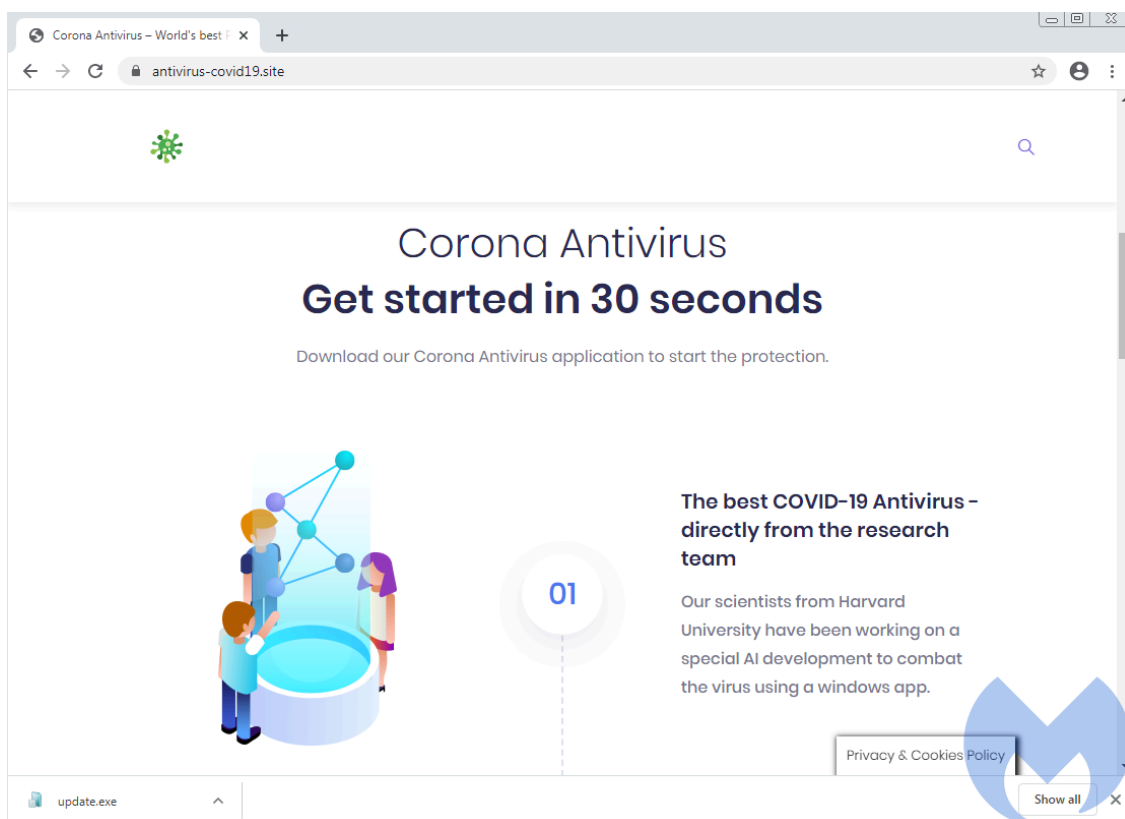
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

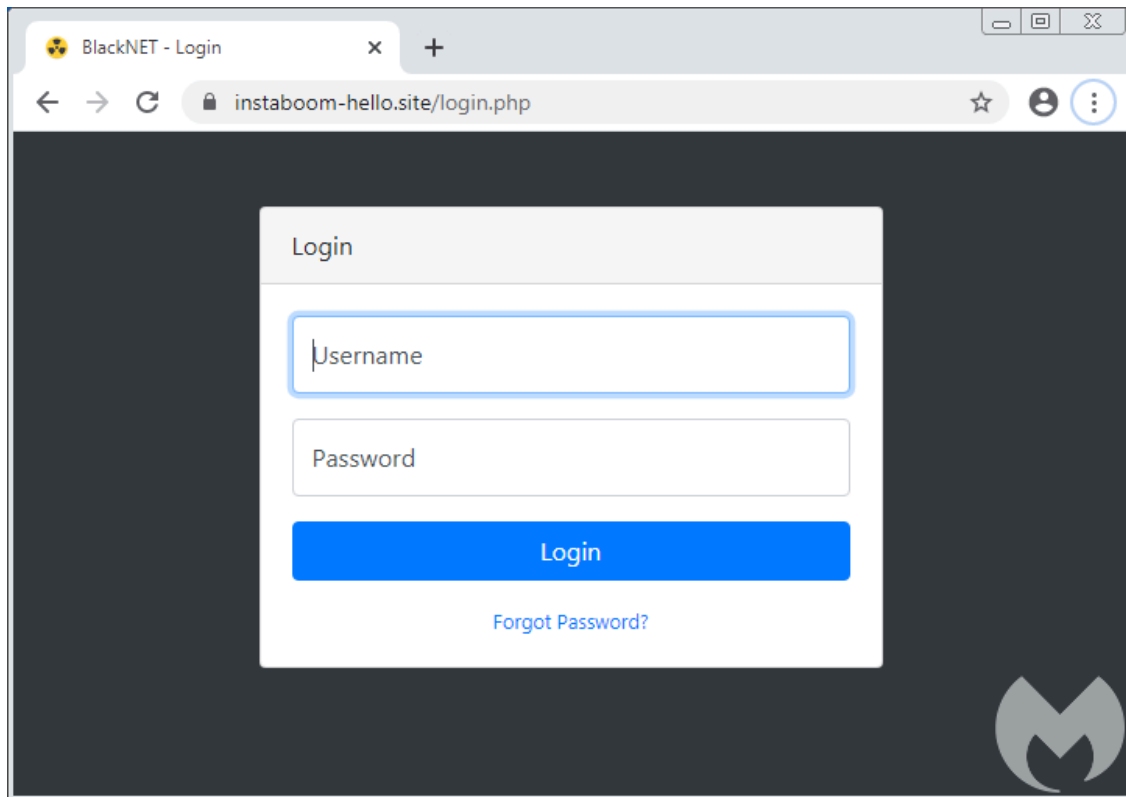


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

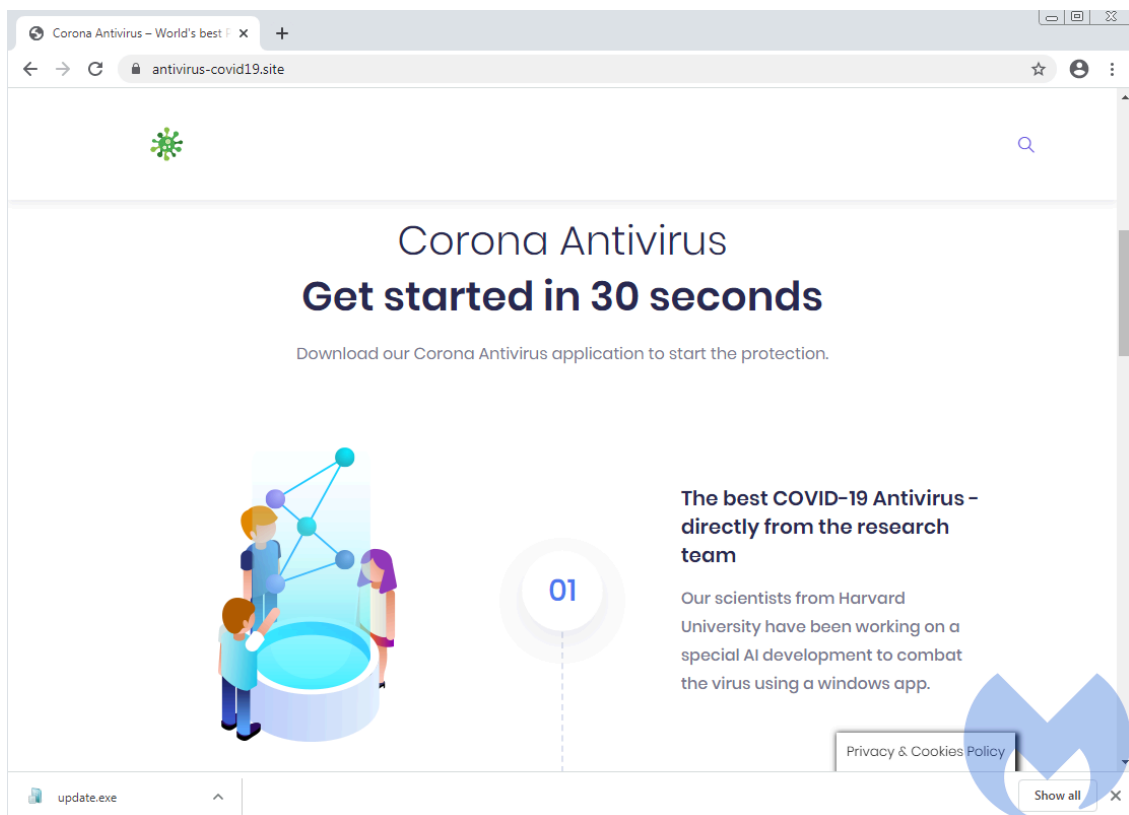
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

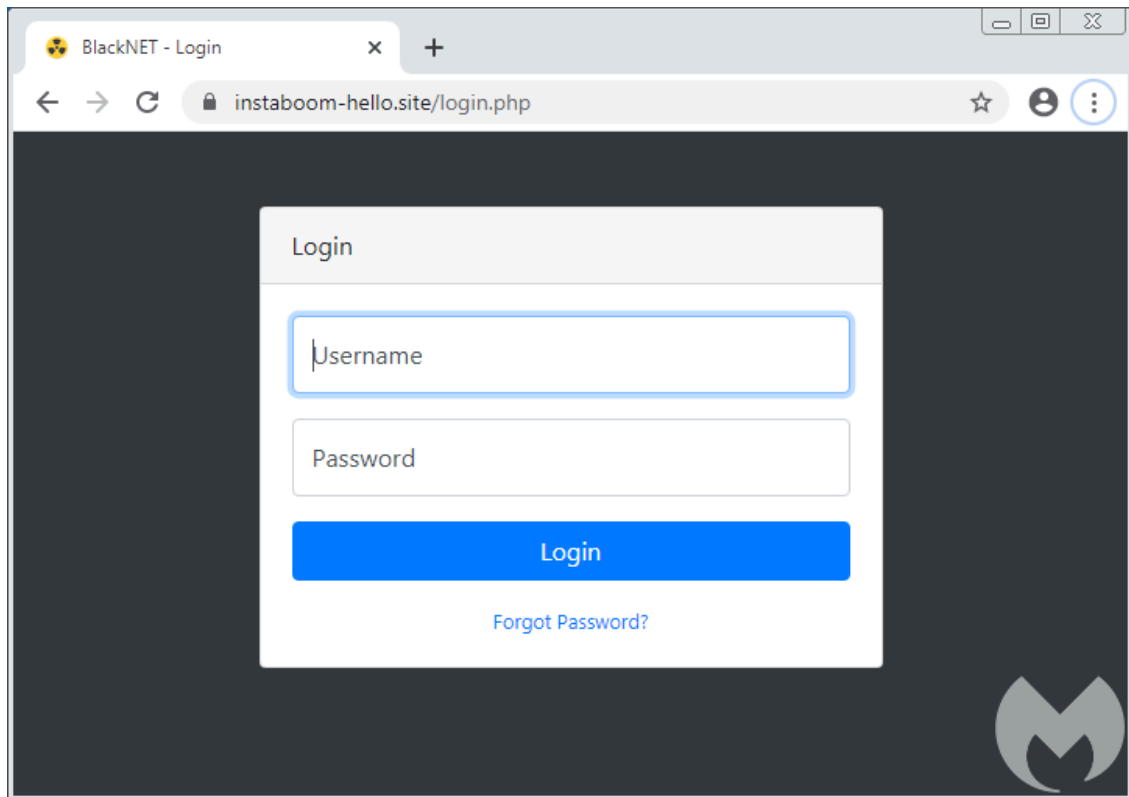


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

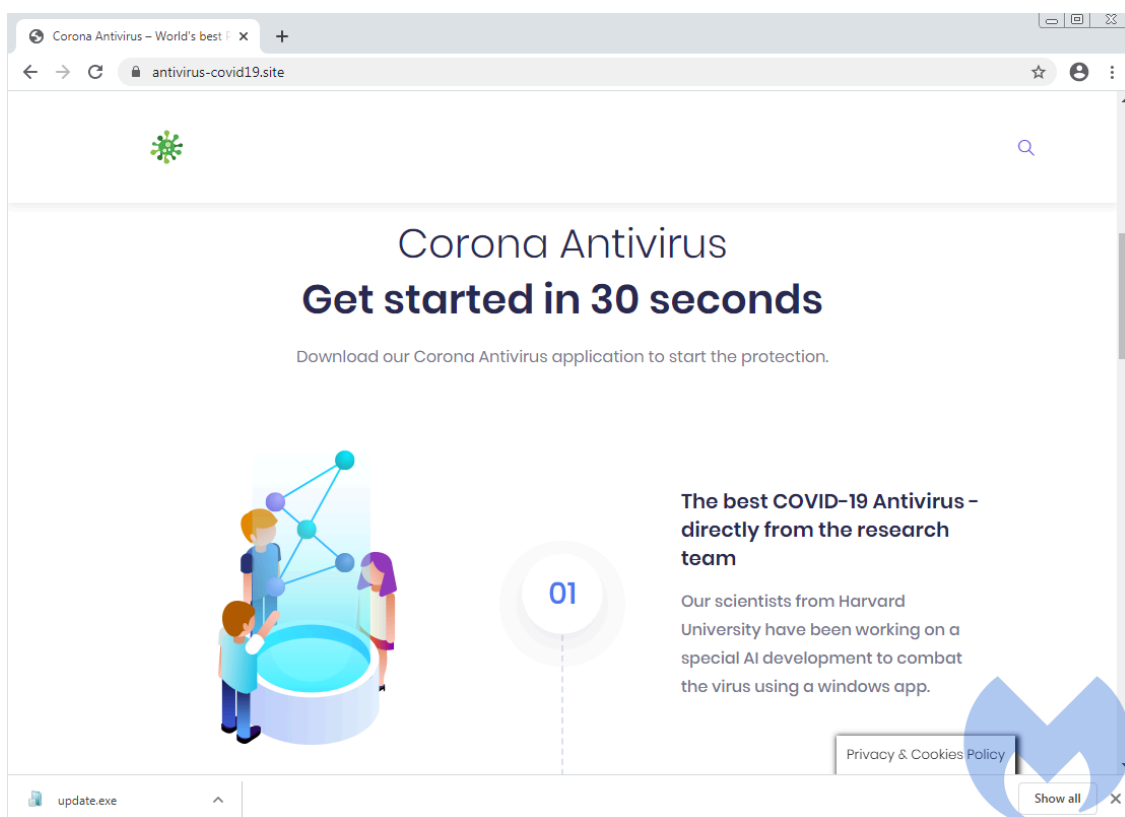
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

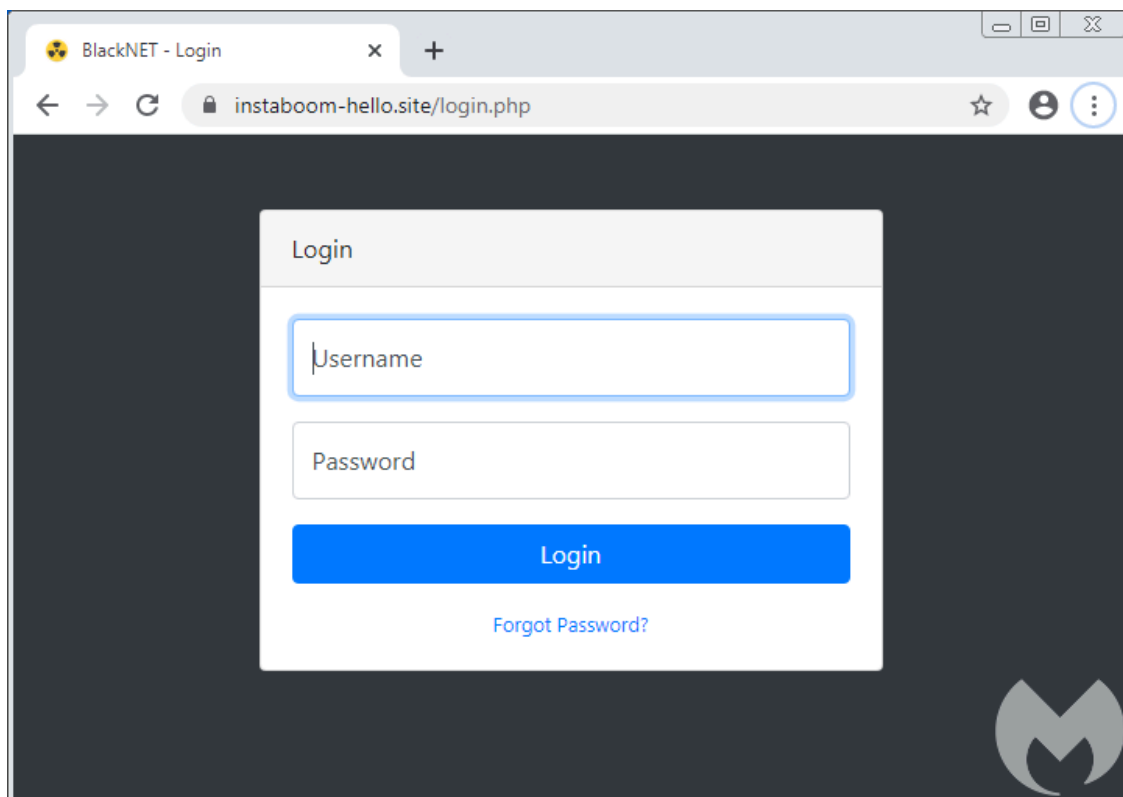


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

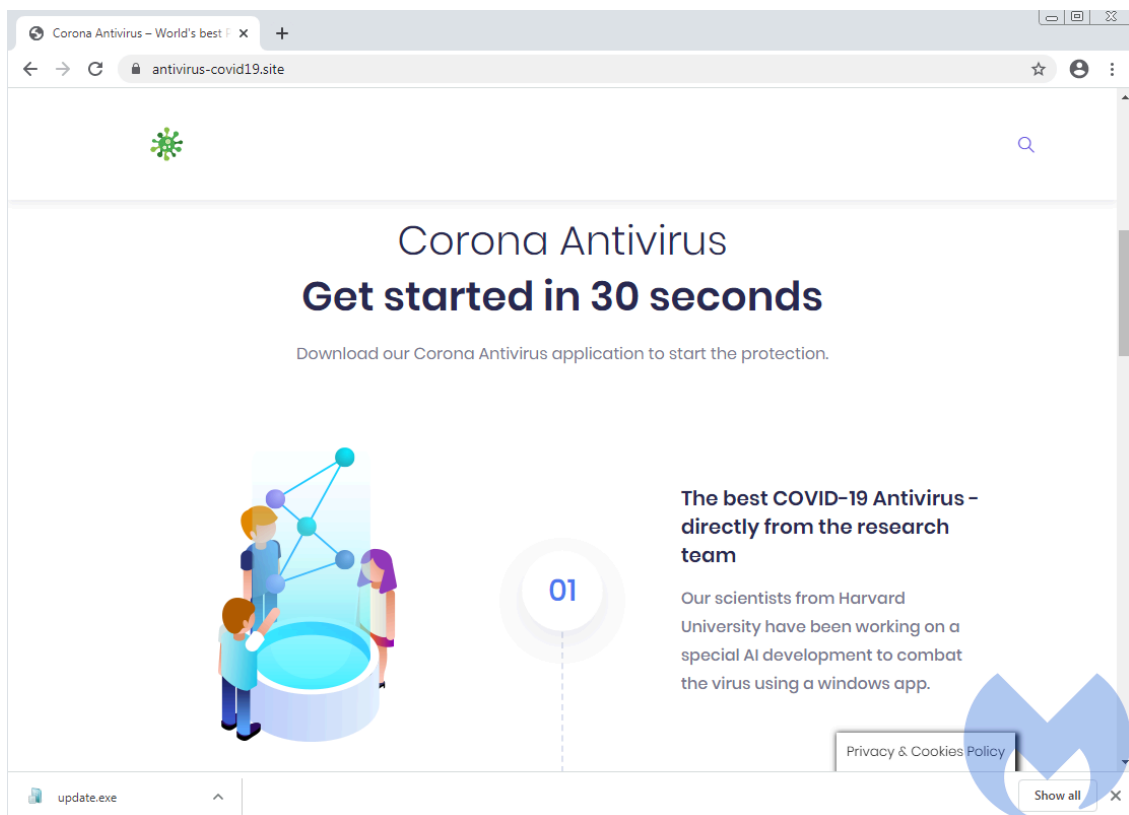
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

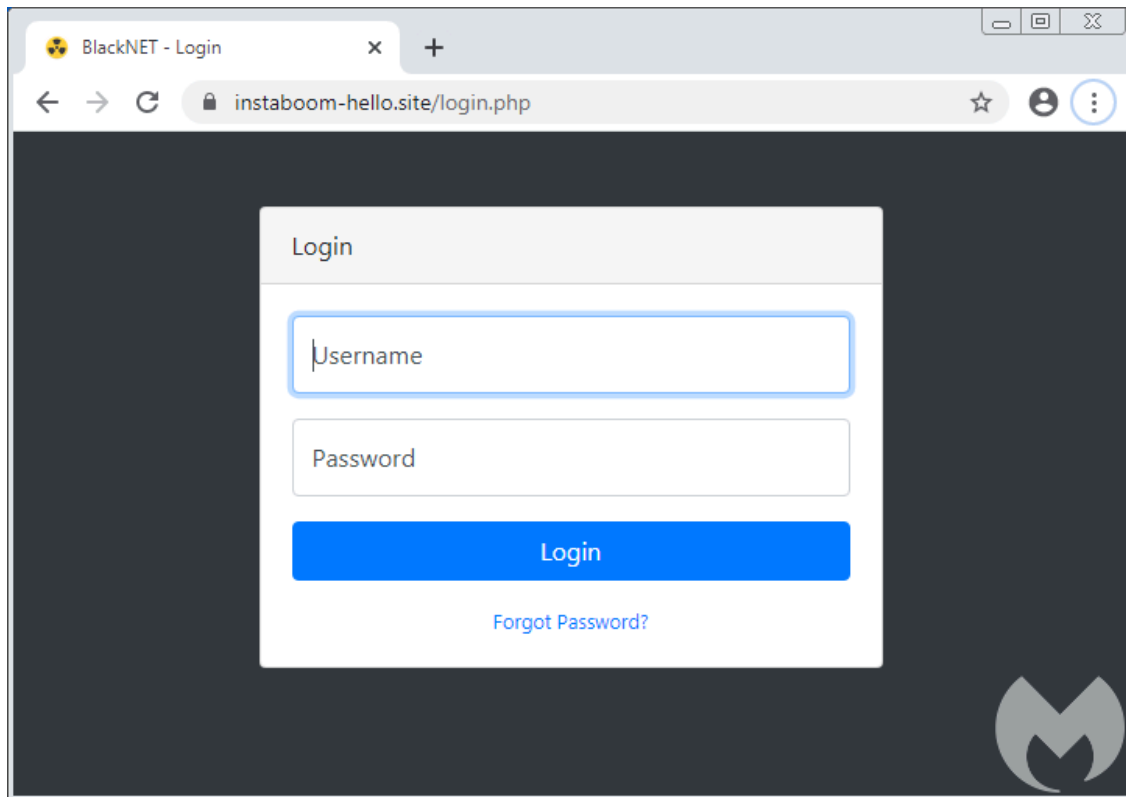


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

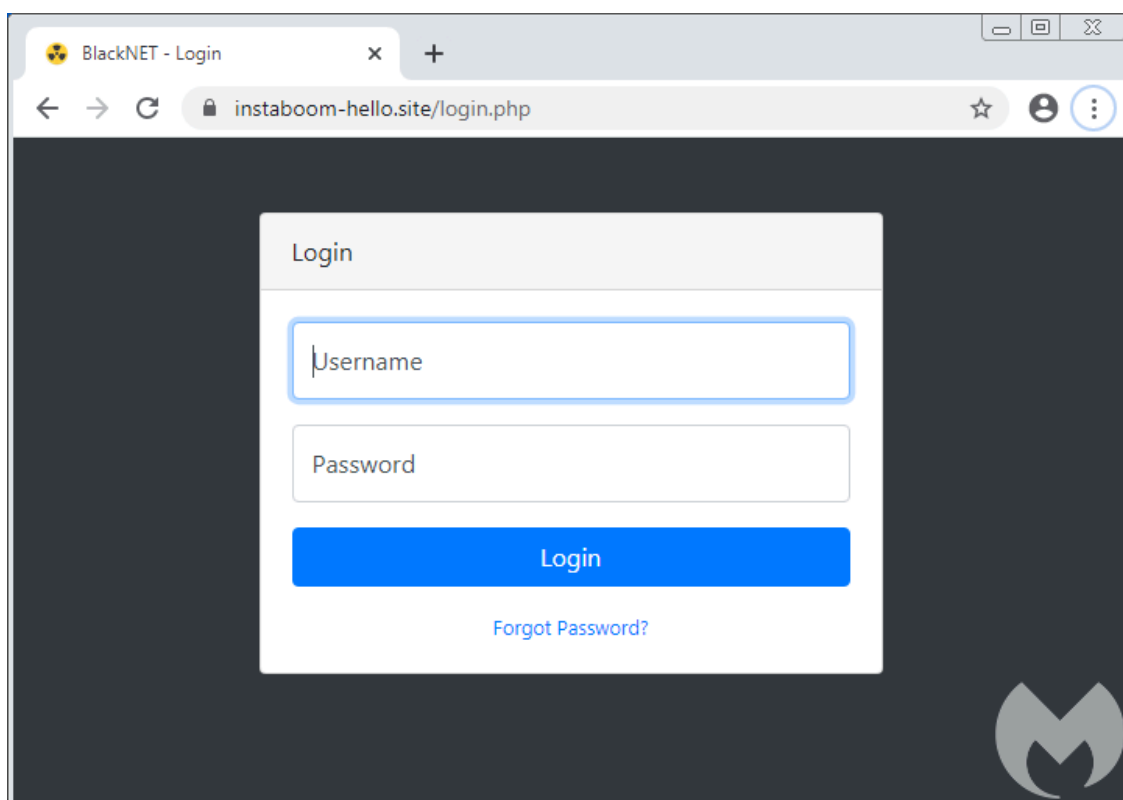
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

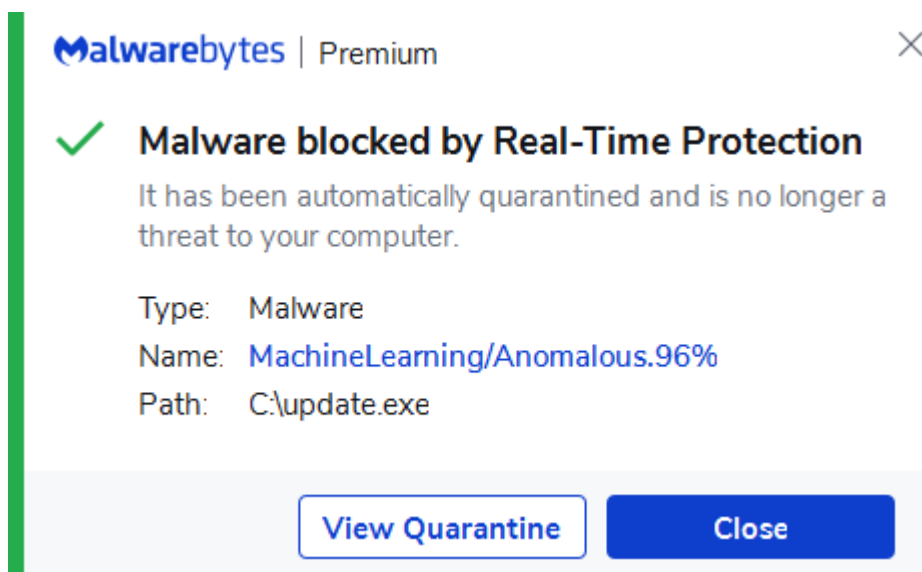
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

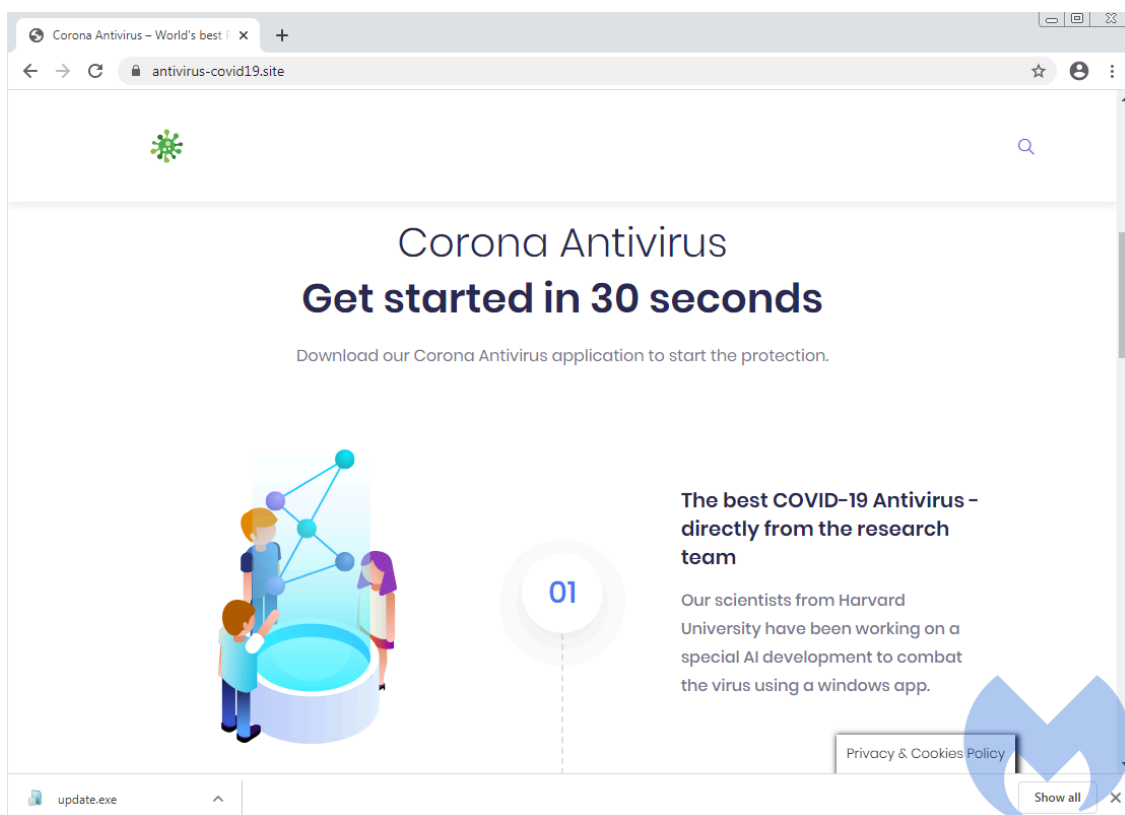
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

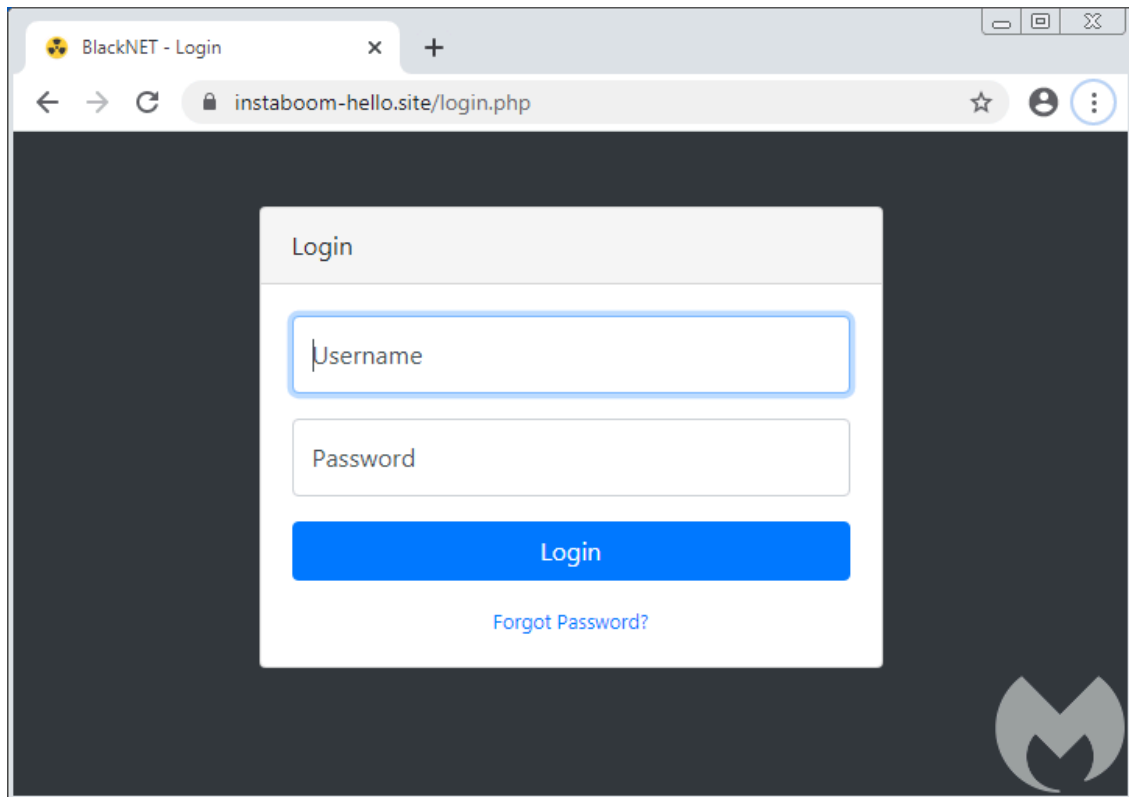


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

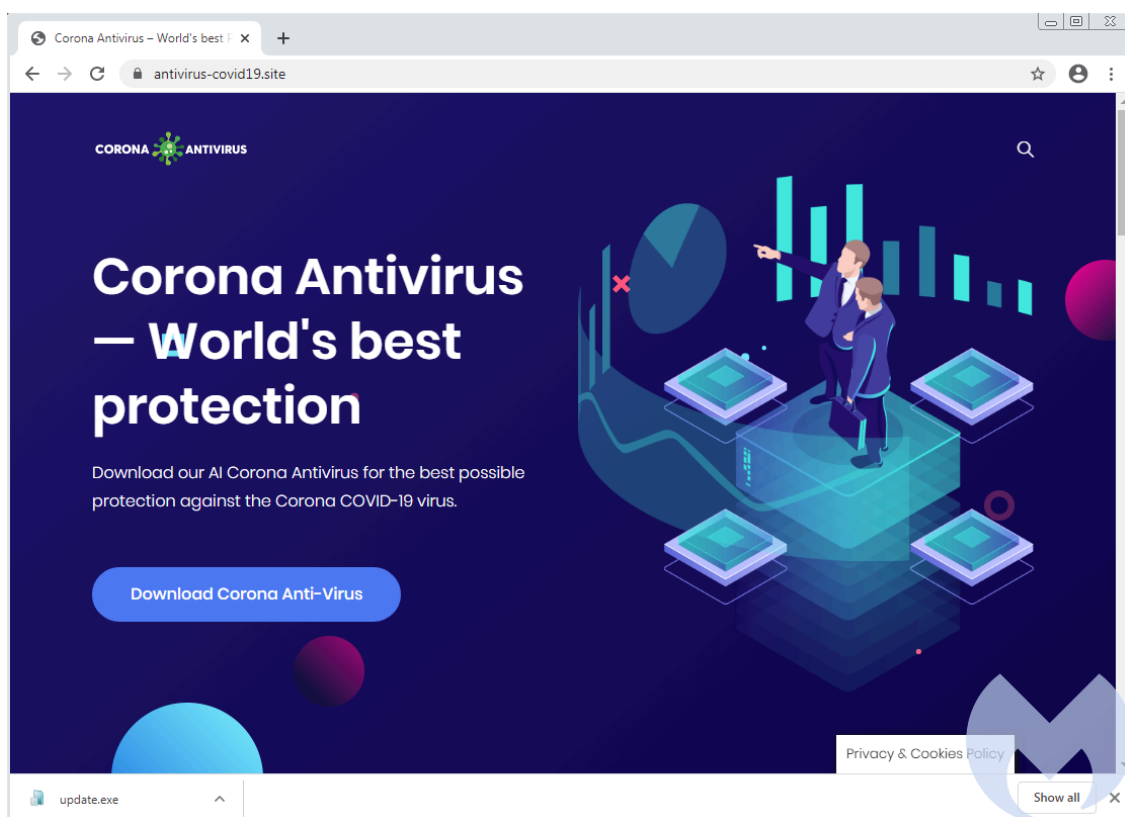
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

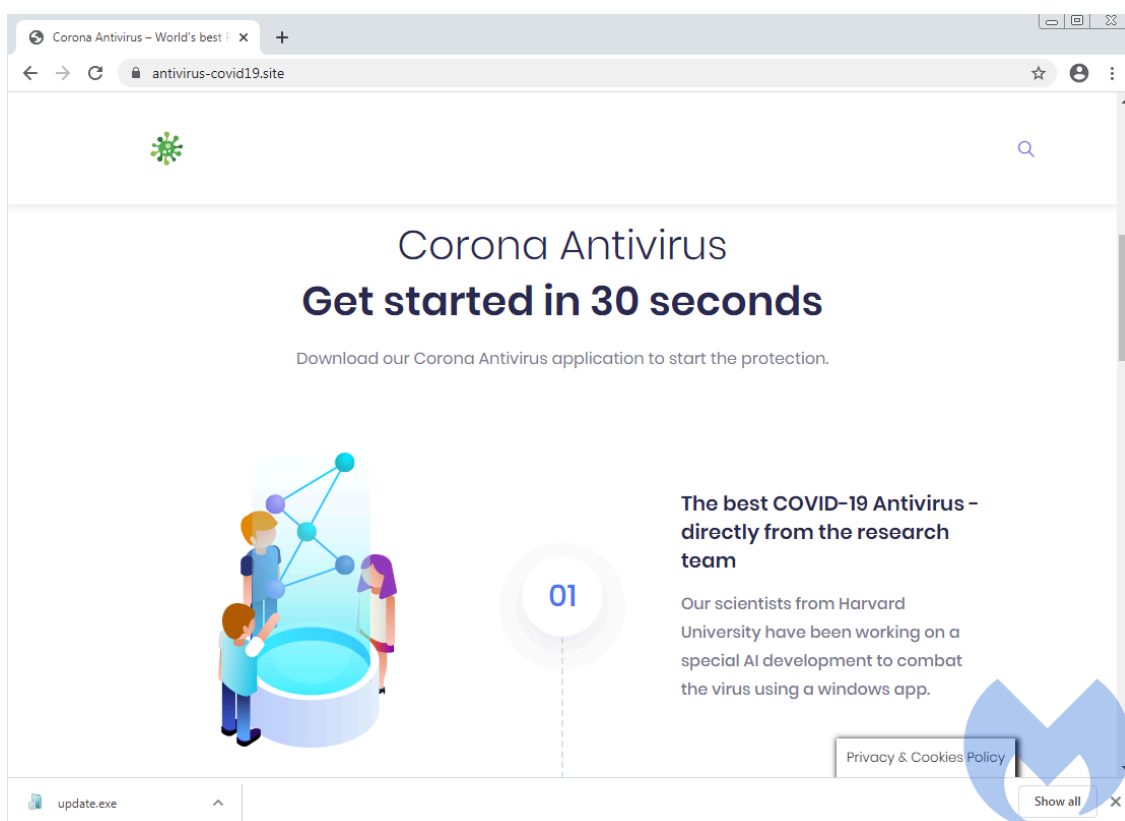
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

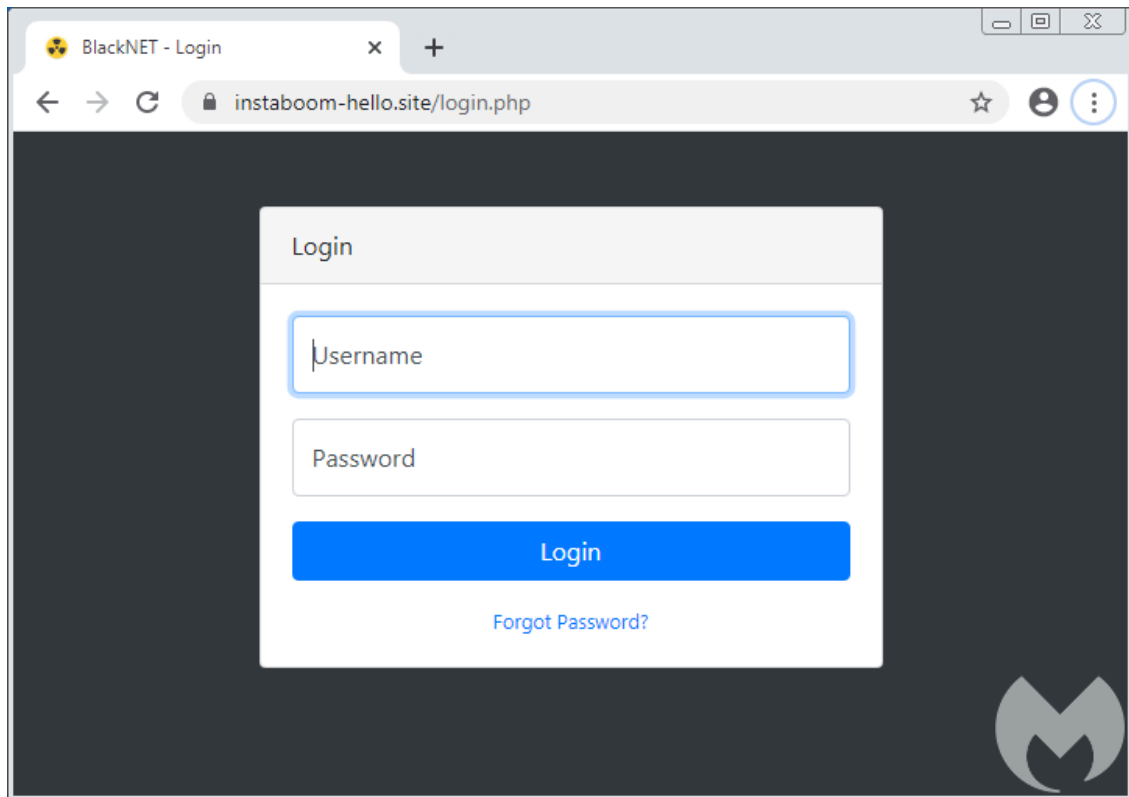


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET

Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Malwarebytes | Premium

✓ **Malware blocked by Real-Time Protection**

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: MachineLearning/Anomalous.96%

Path: C:\update.exe

View Quarantine Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

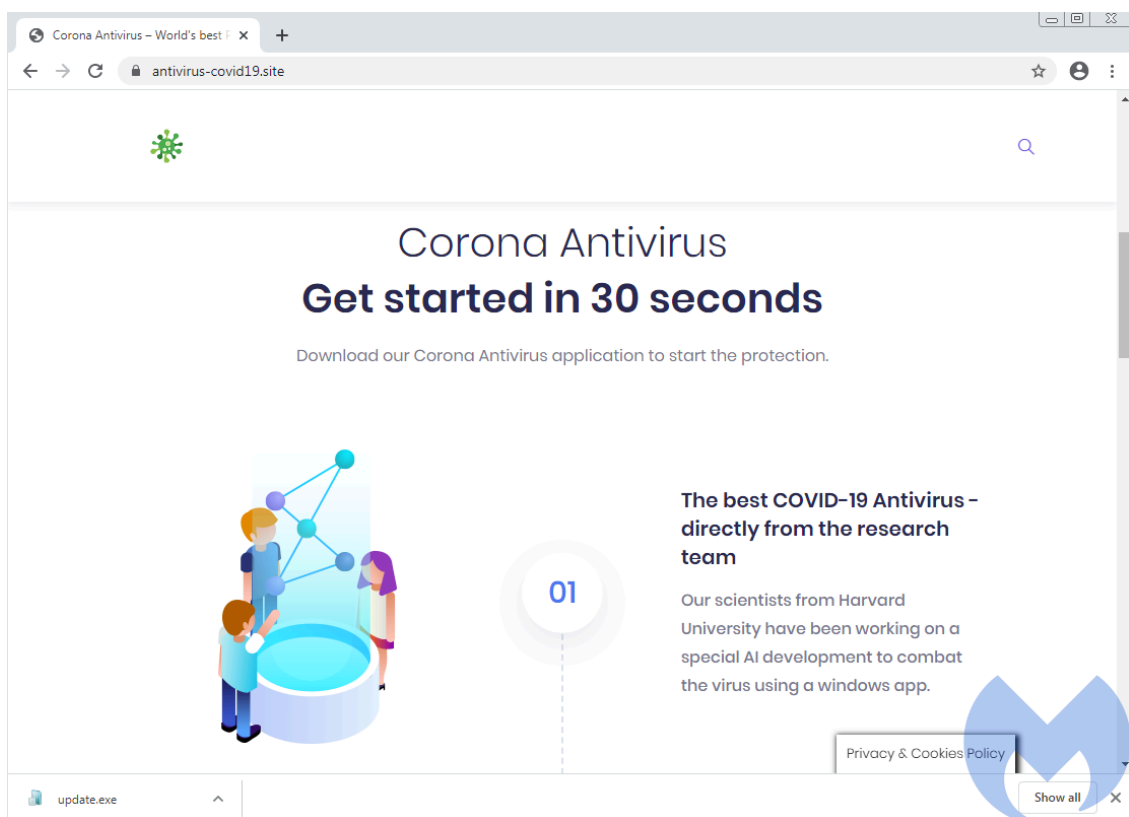
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

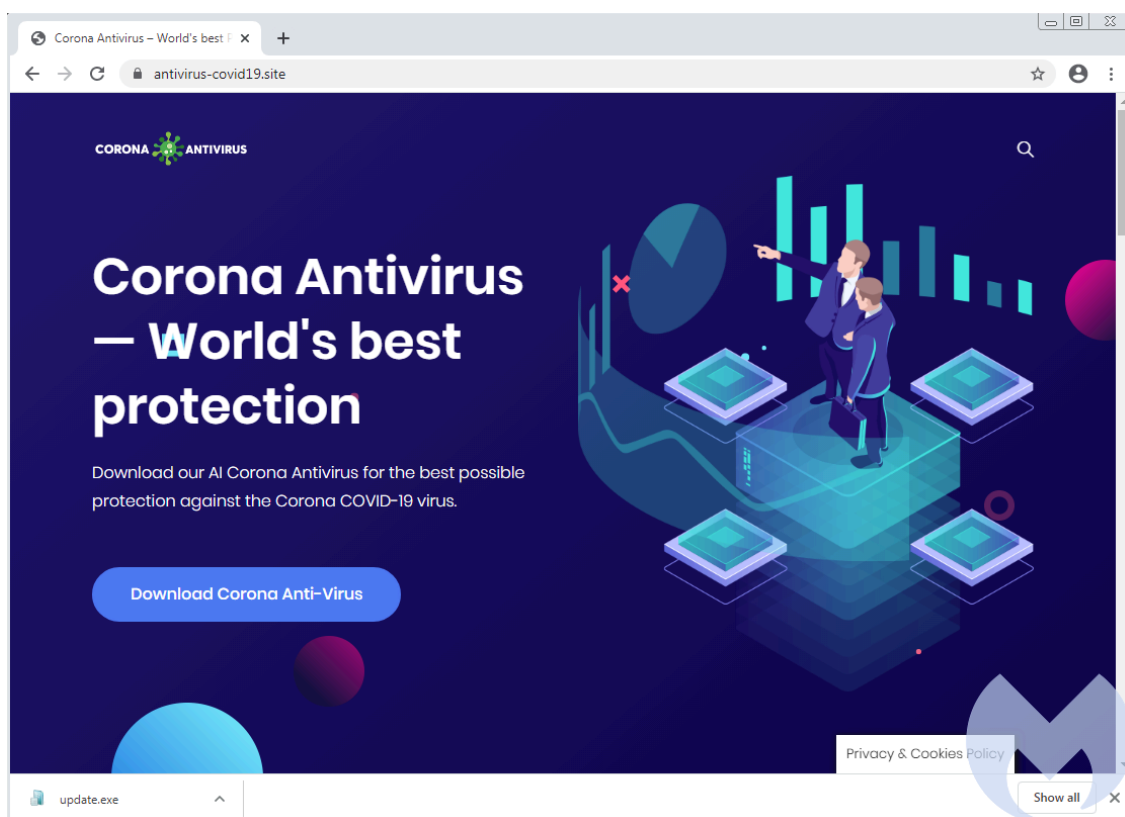
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

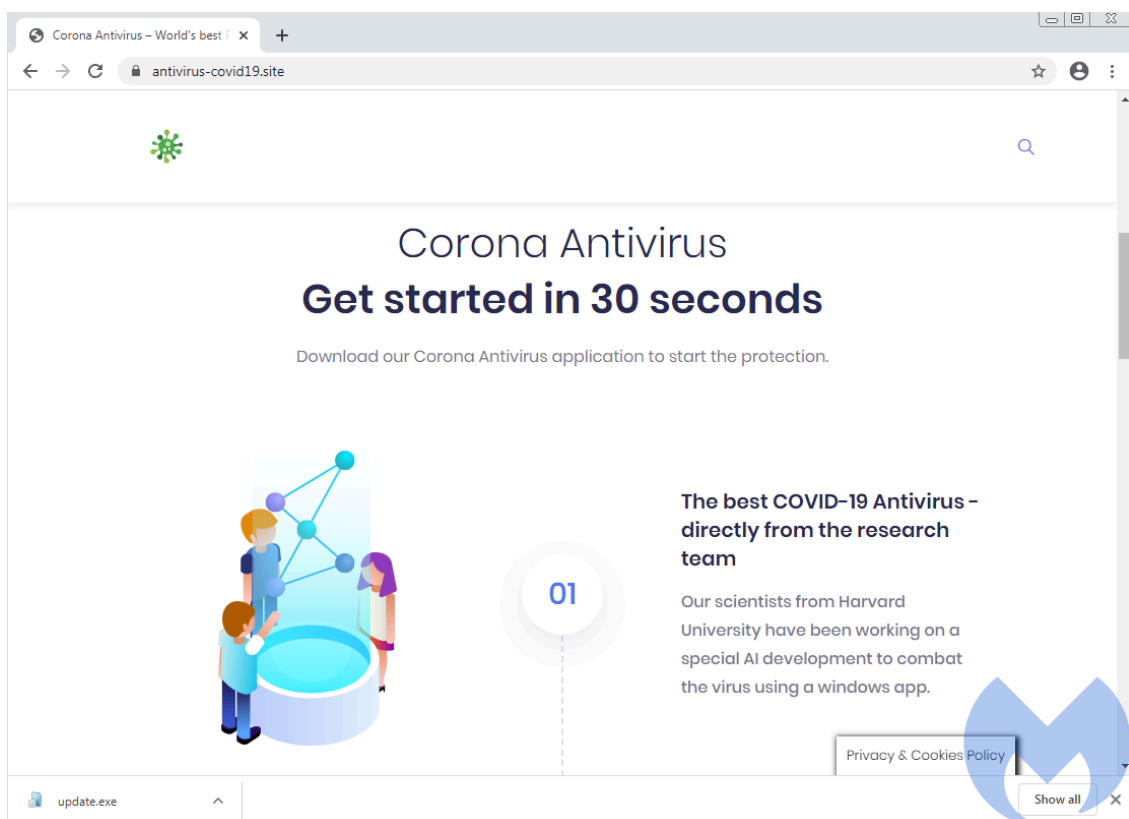
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

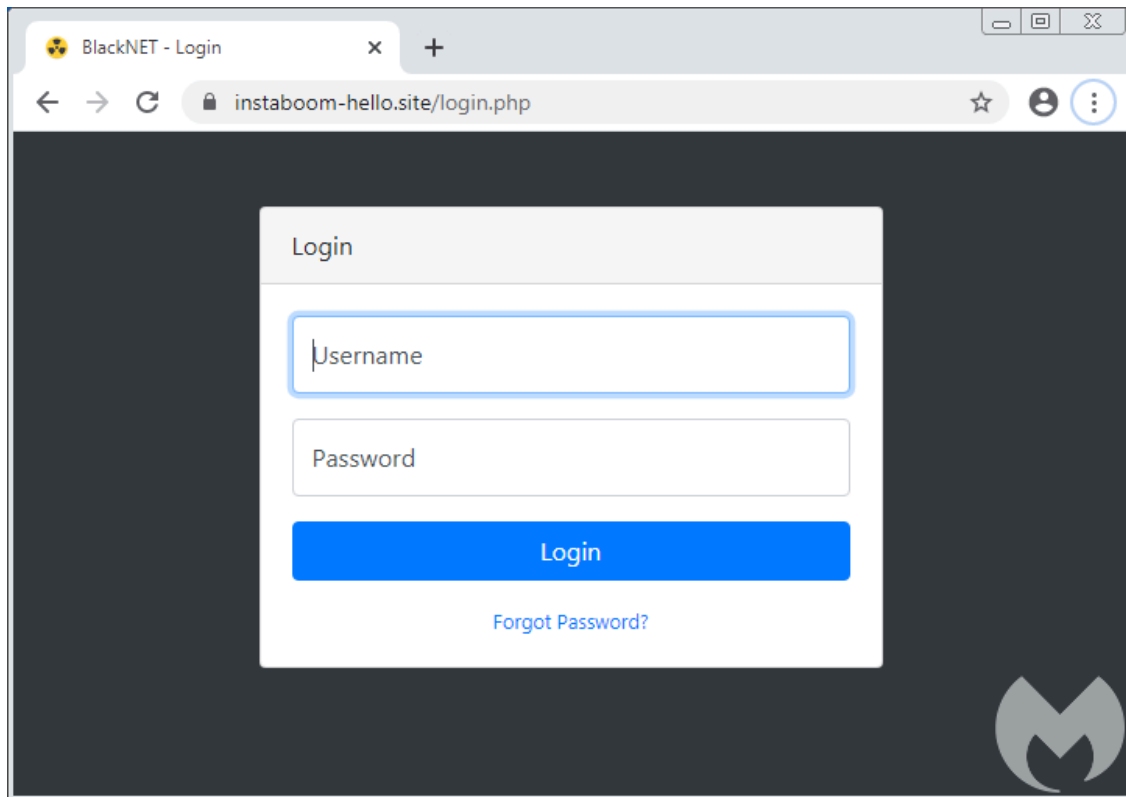


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

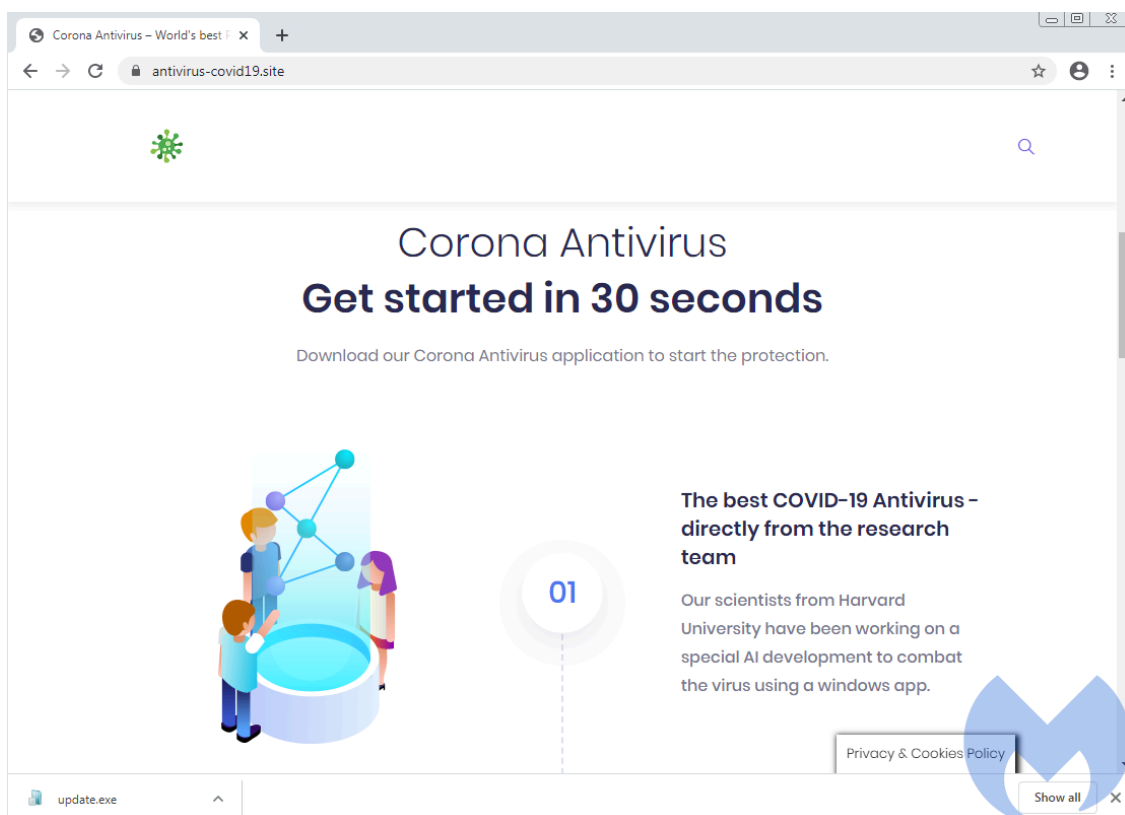
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

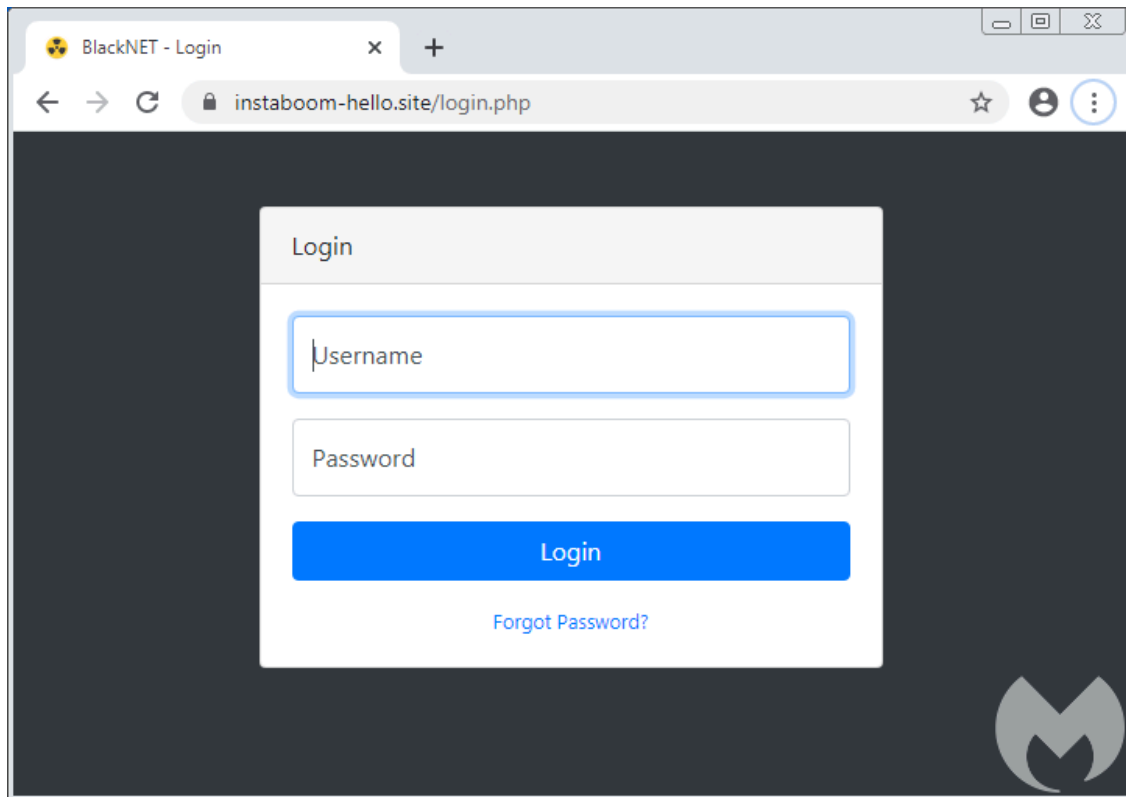


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

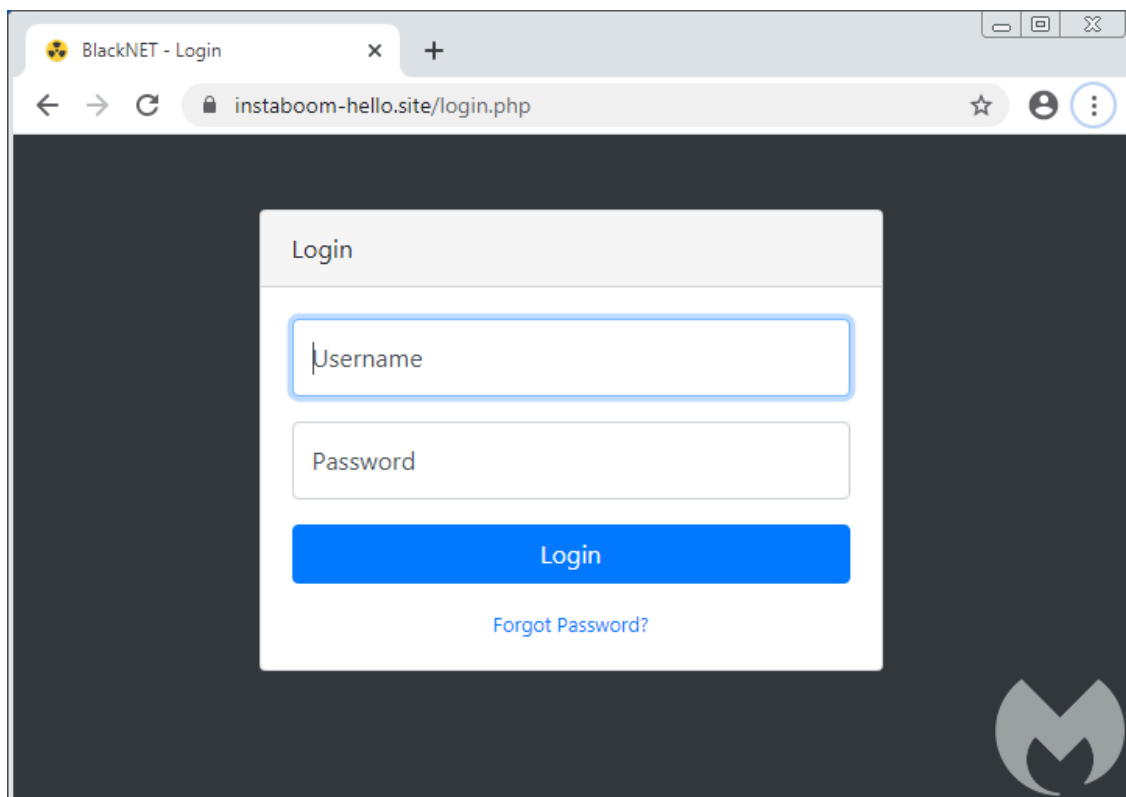
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

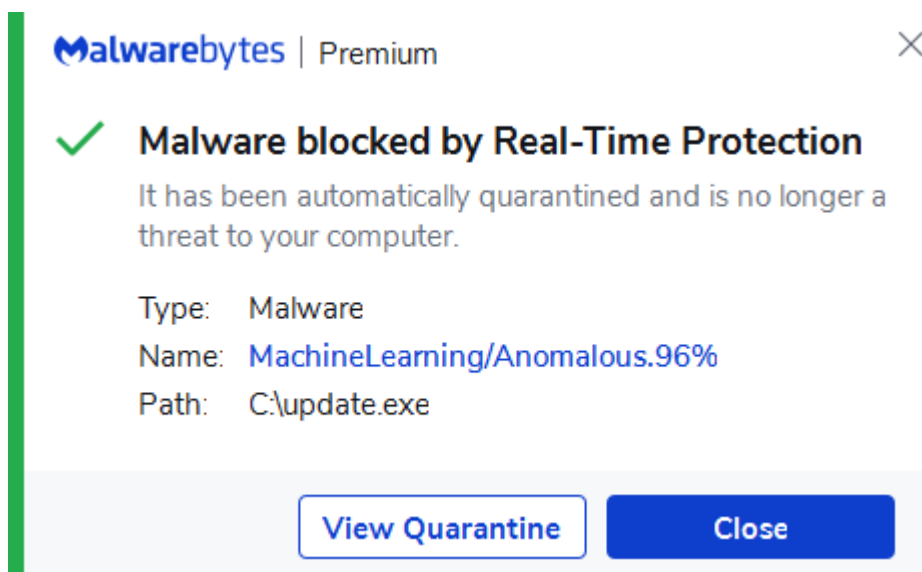
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

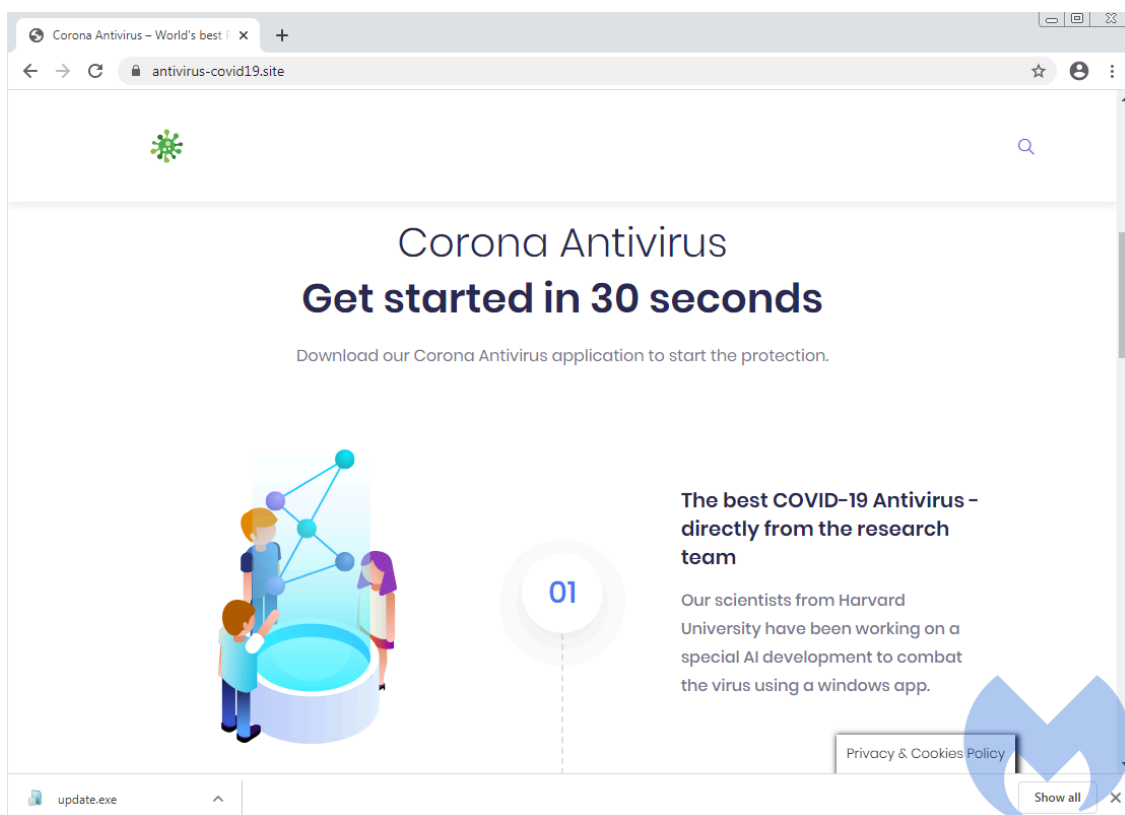
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

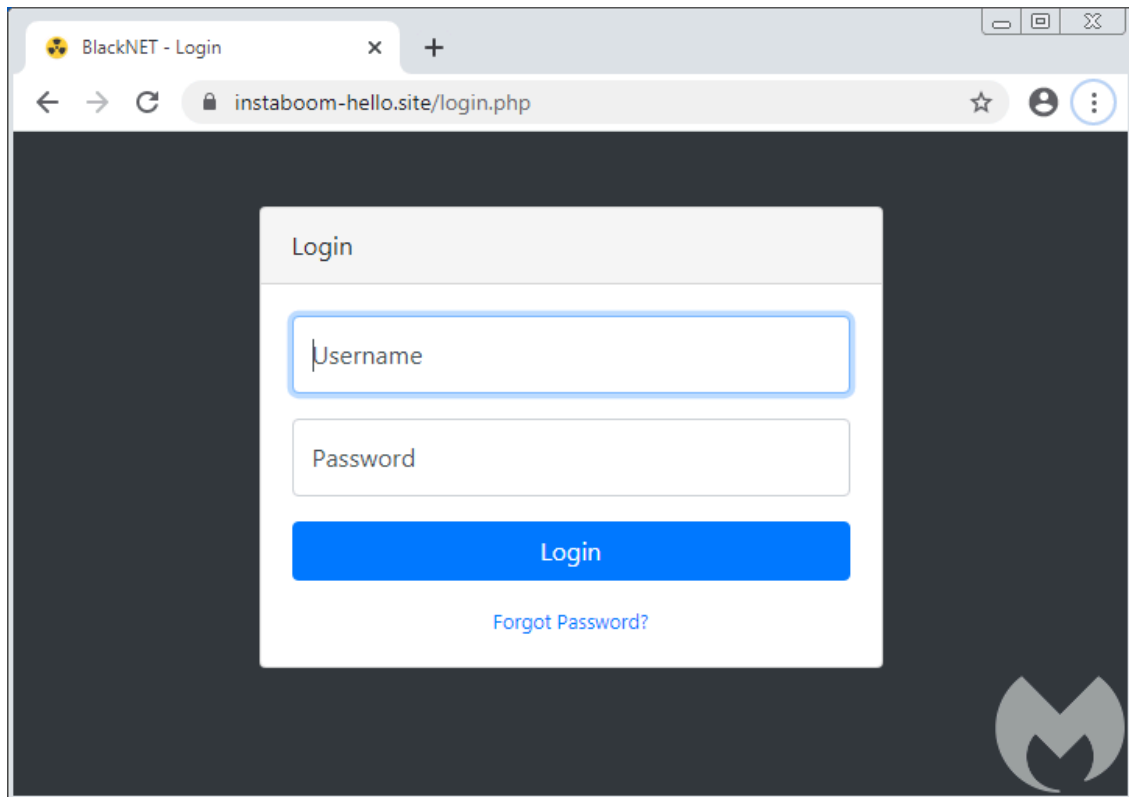


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

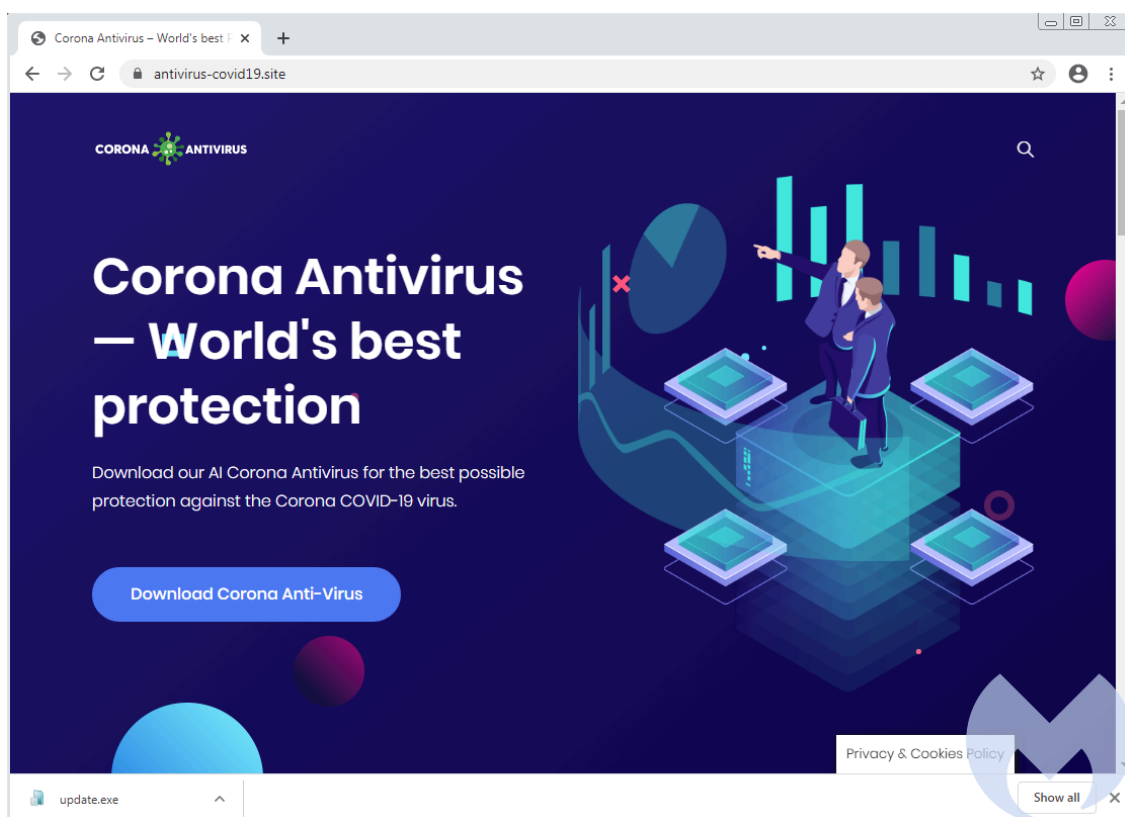
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

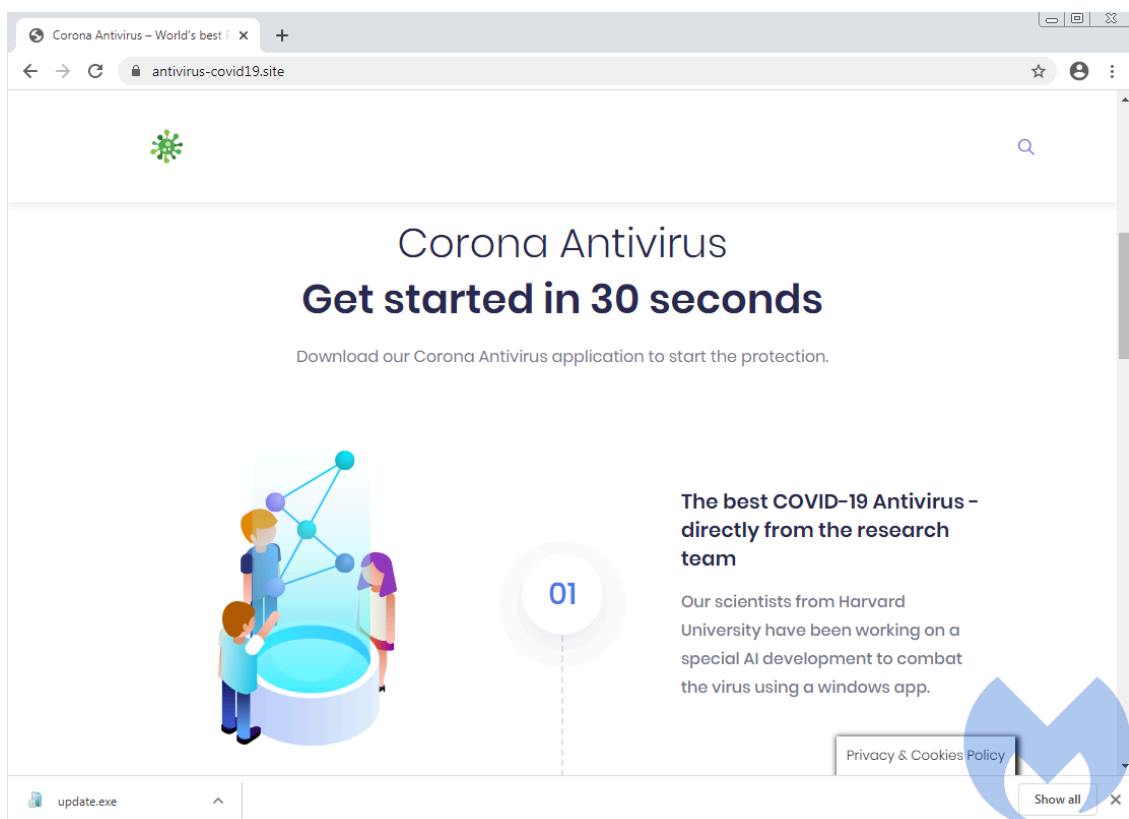
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

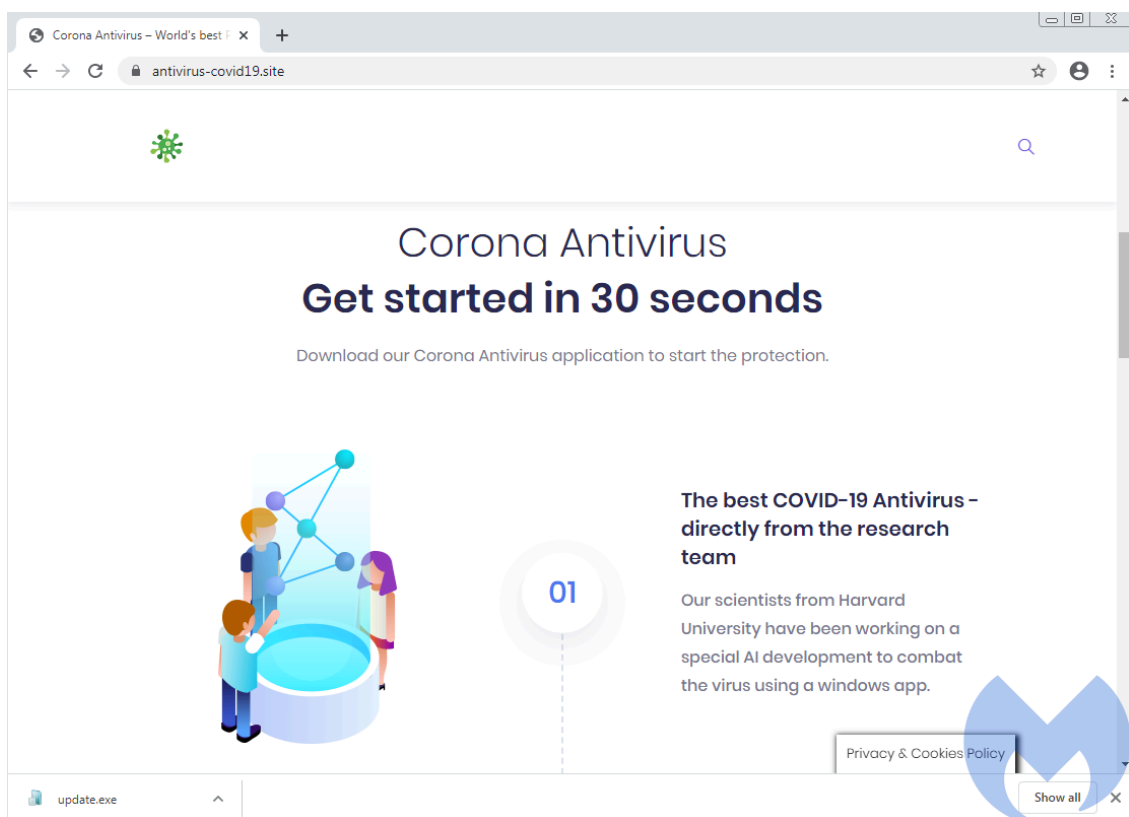
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

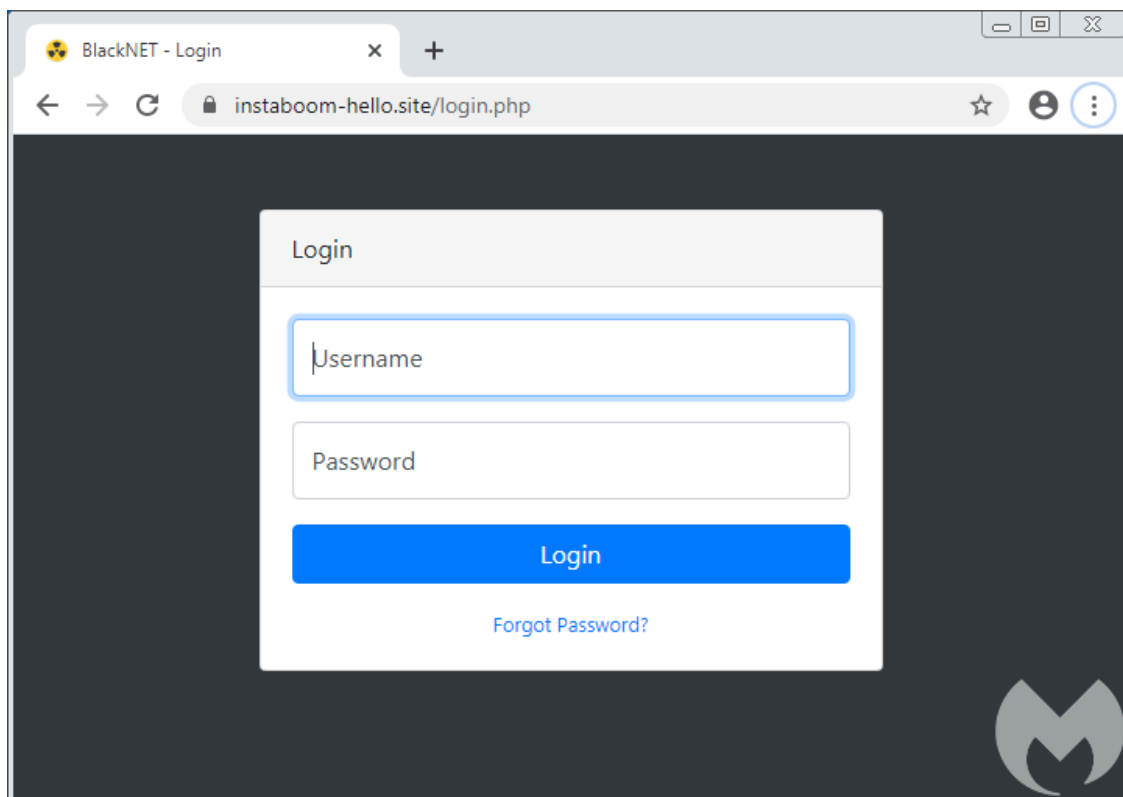
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

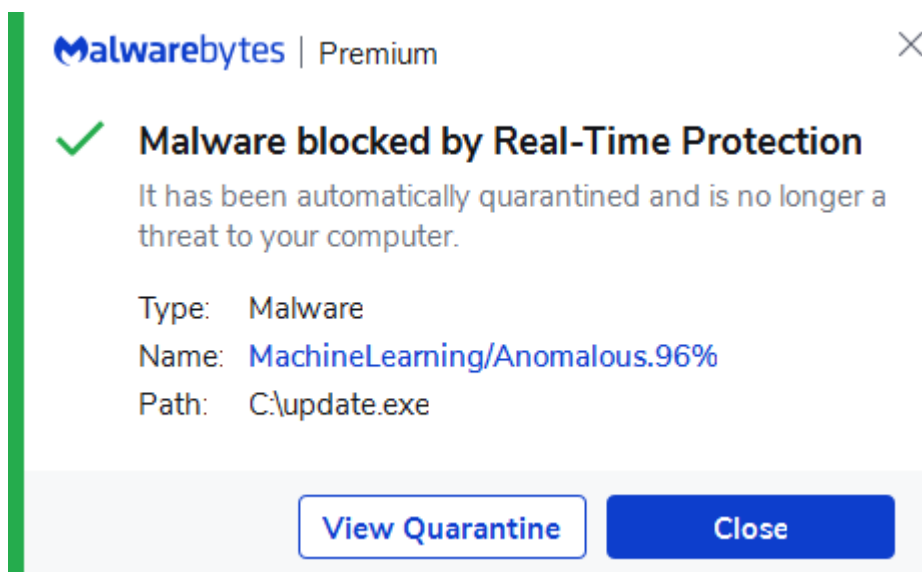
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a 'Select Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

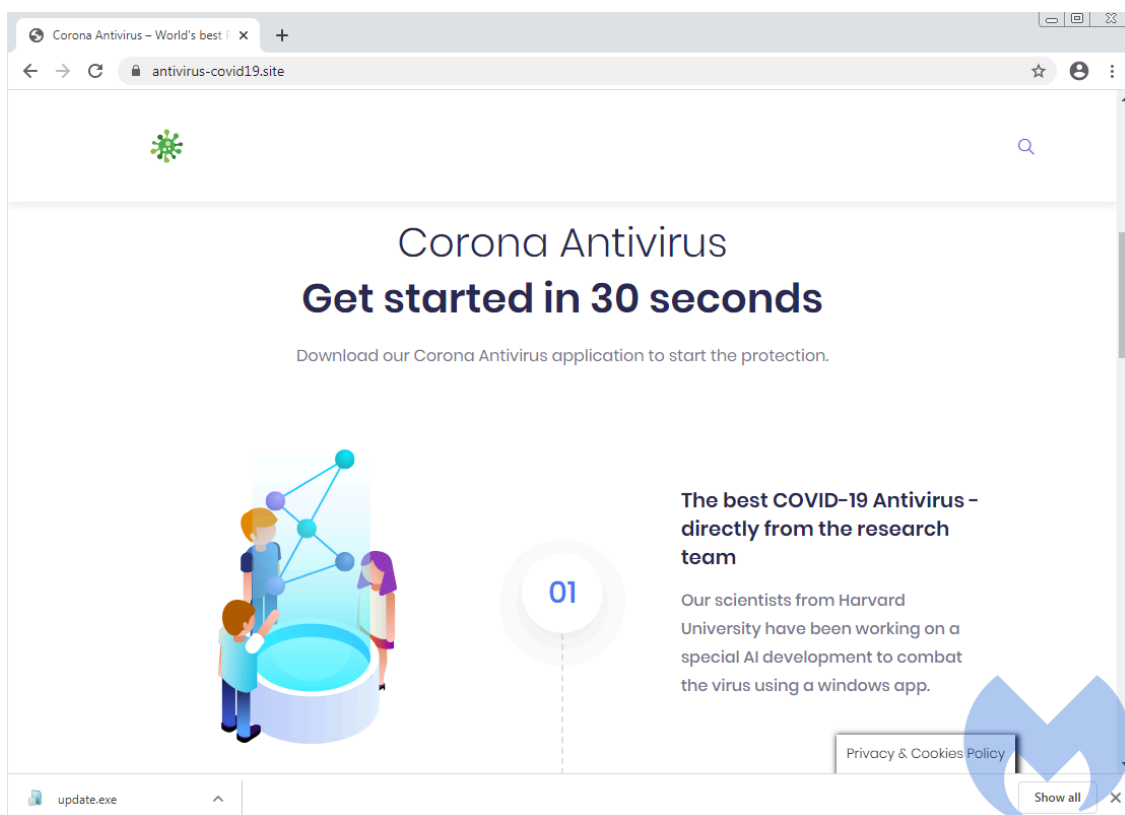
C2 panel

```
instaboom-hello[.]site
```




To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

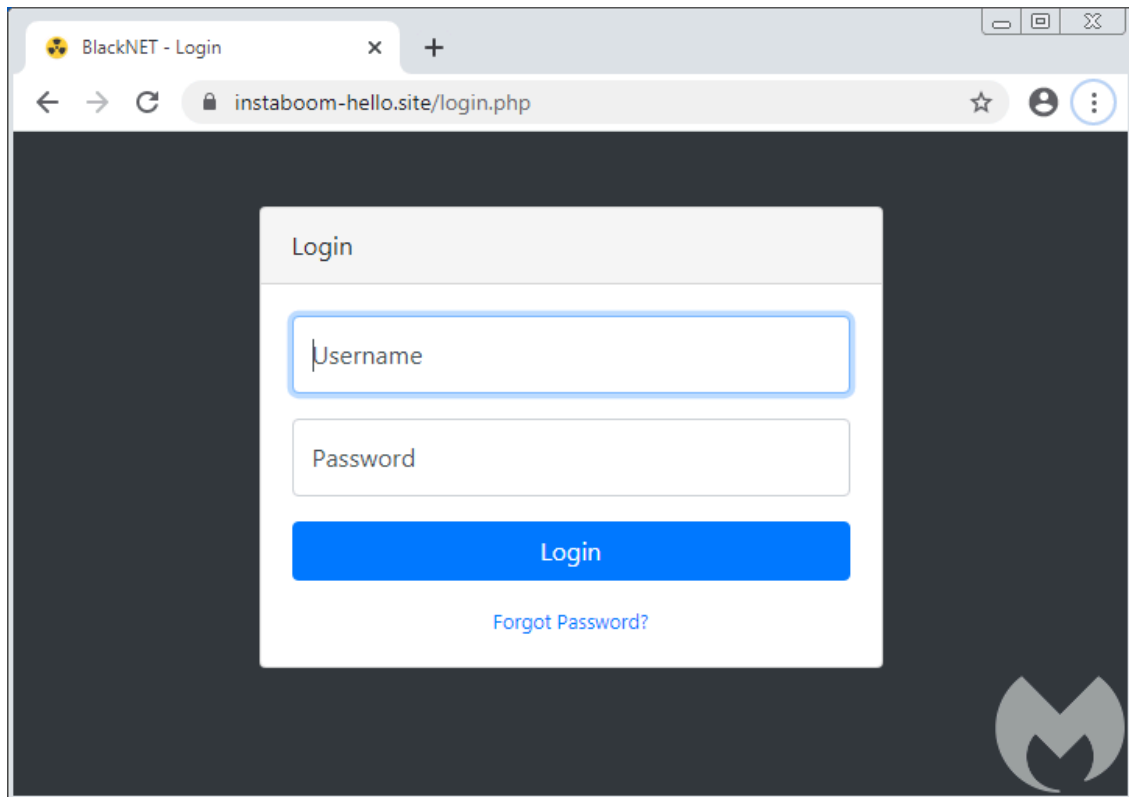


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

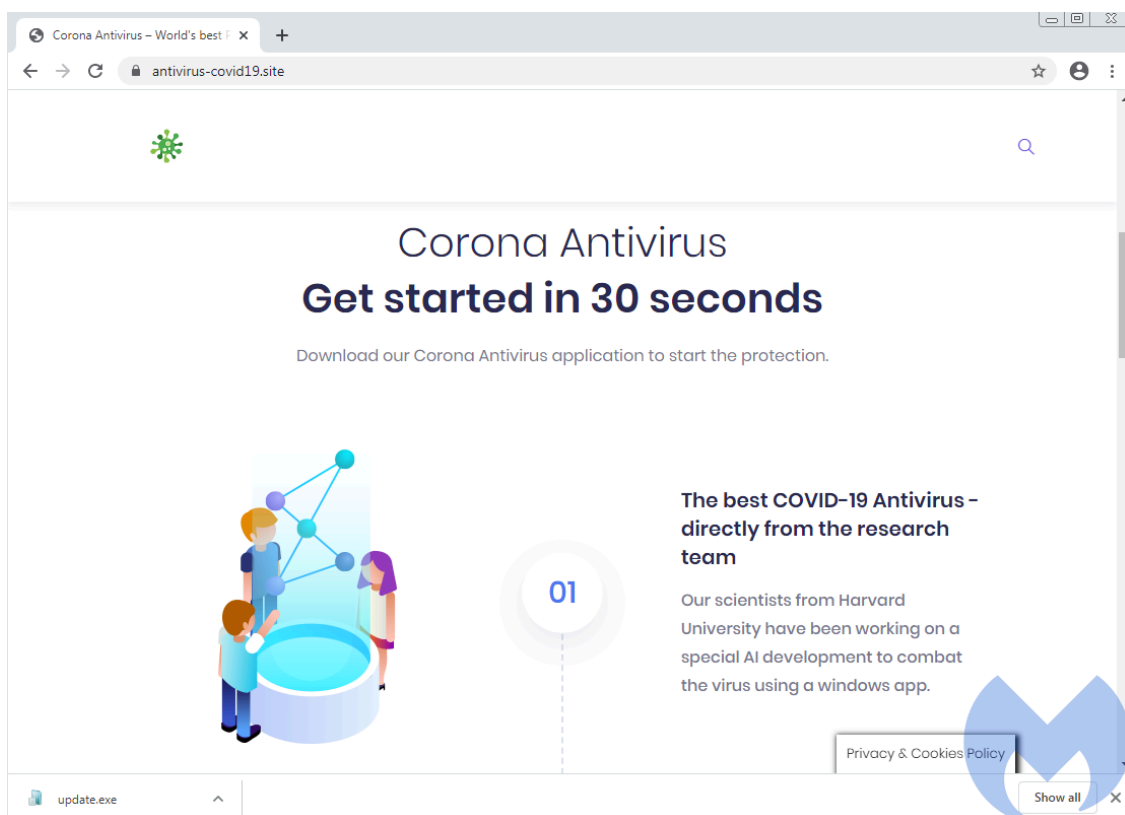
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

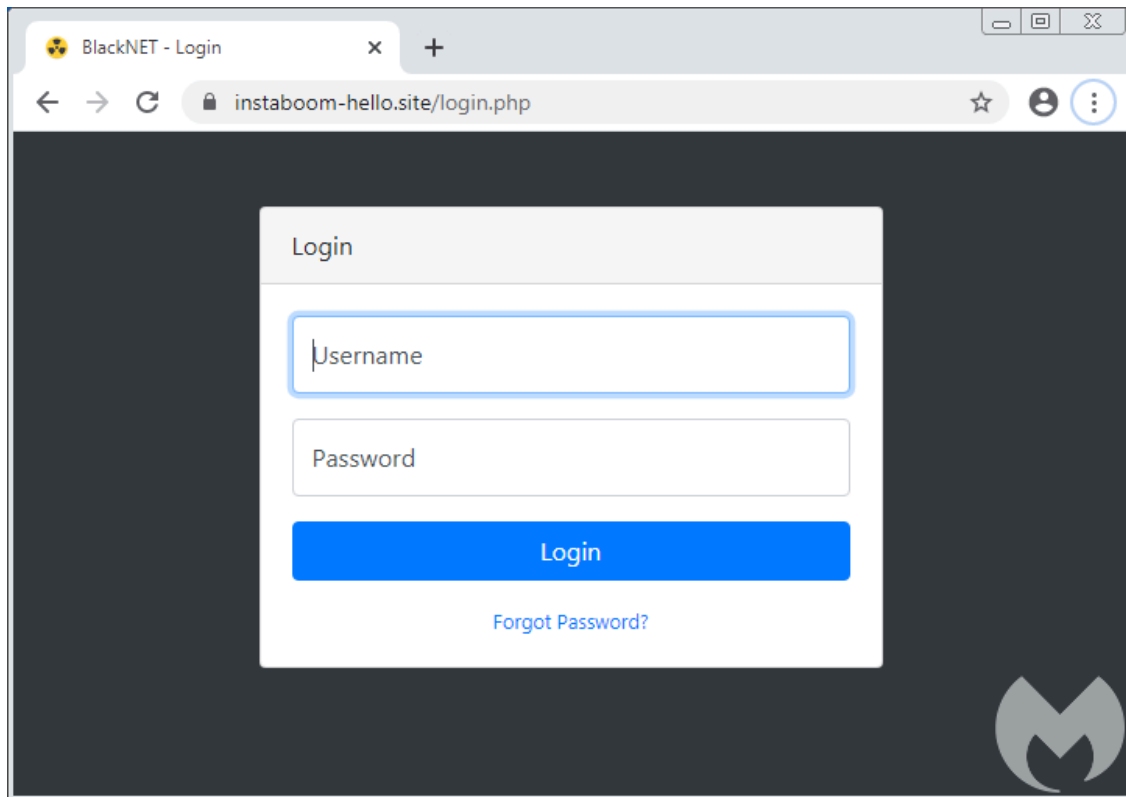


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

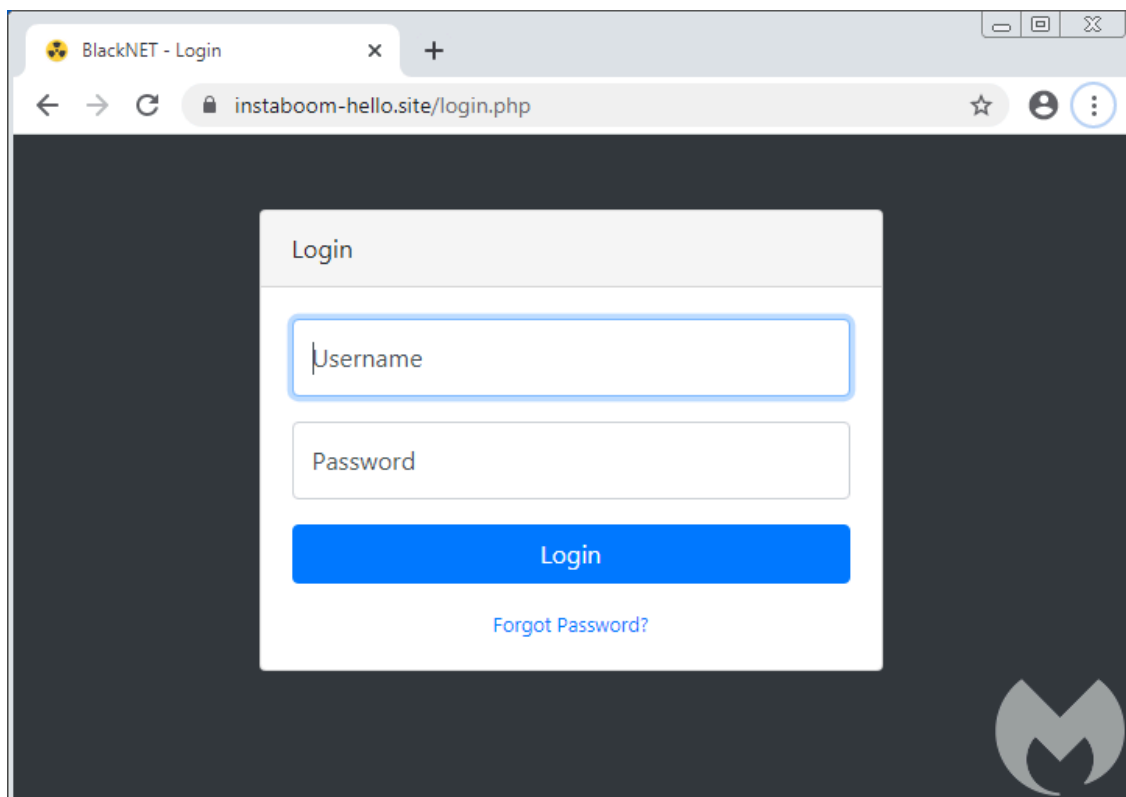
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

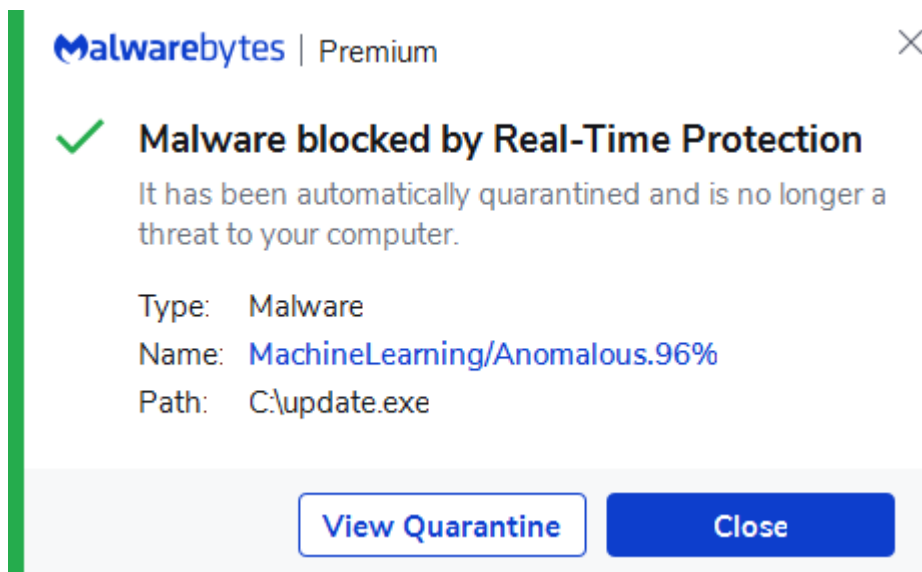
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

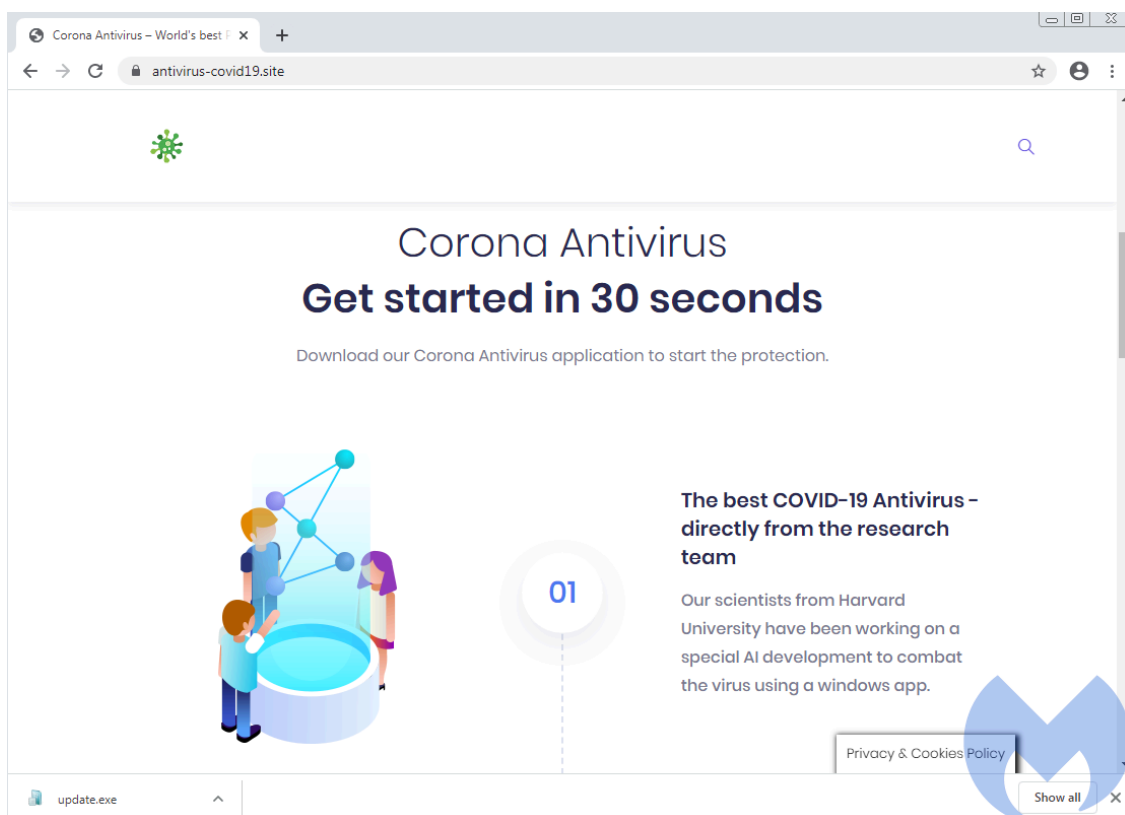
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

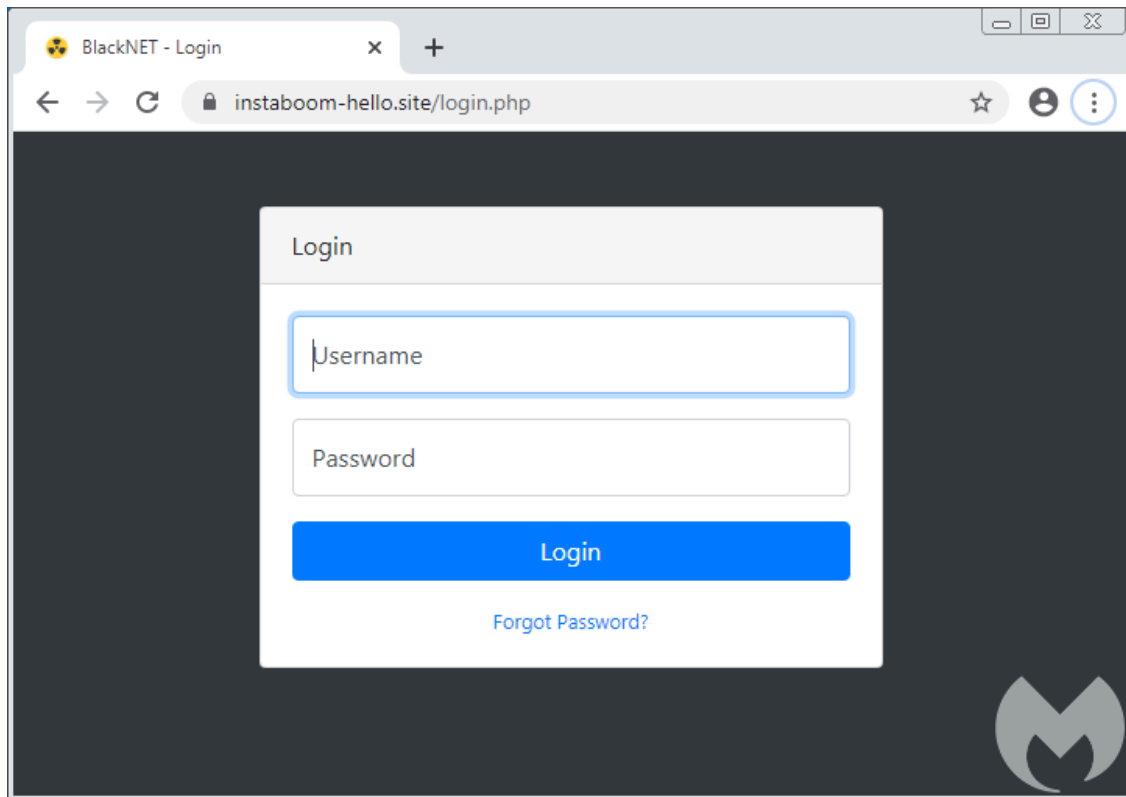


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

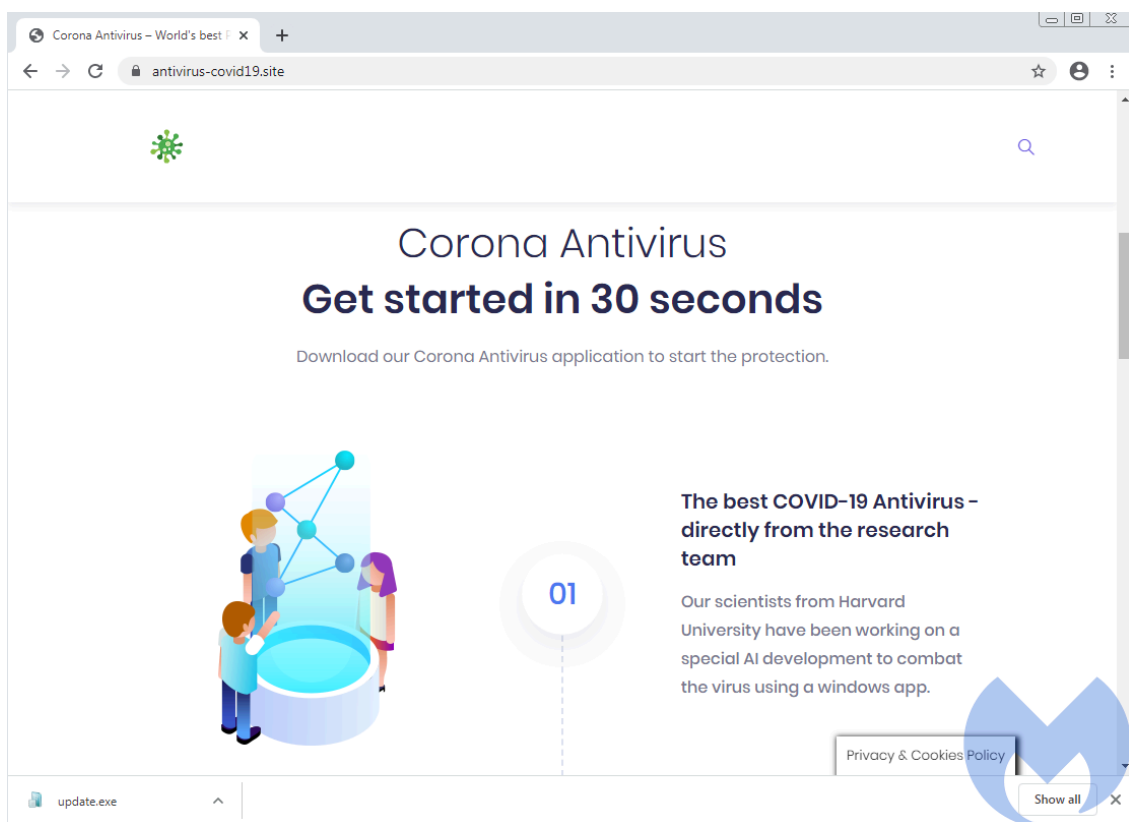
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

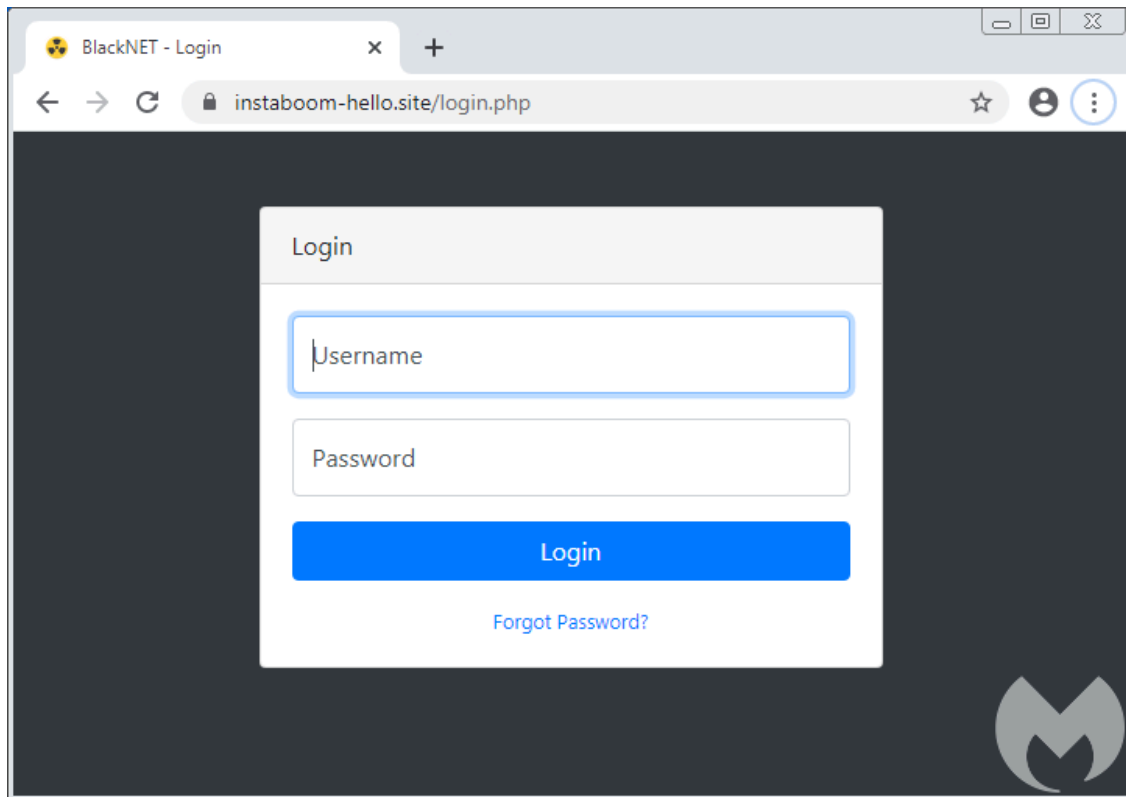


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

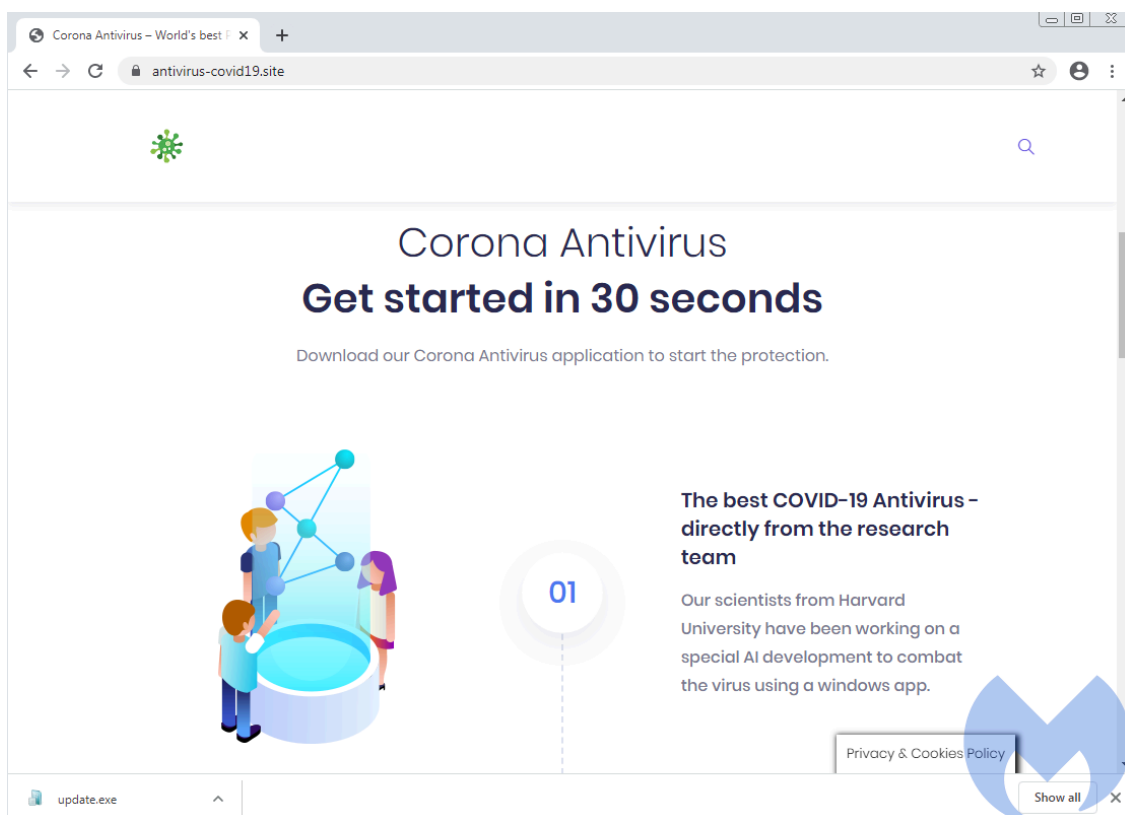
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

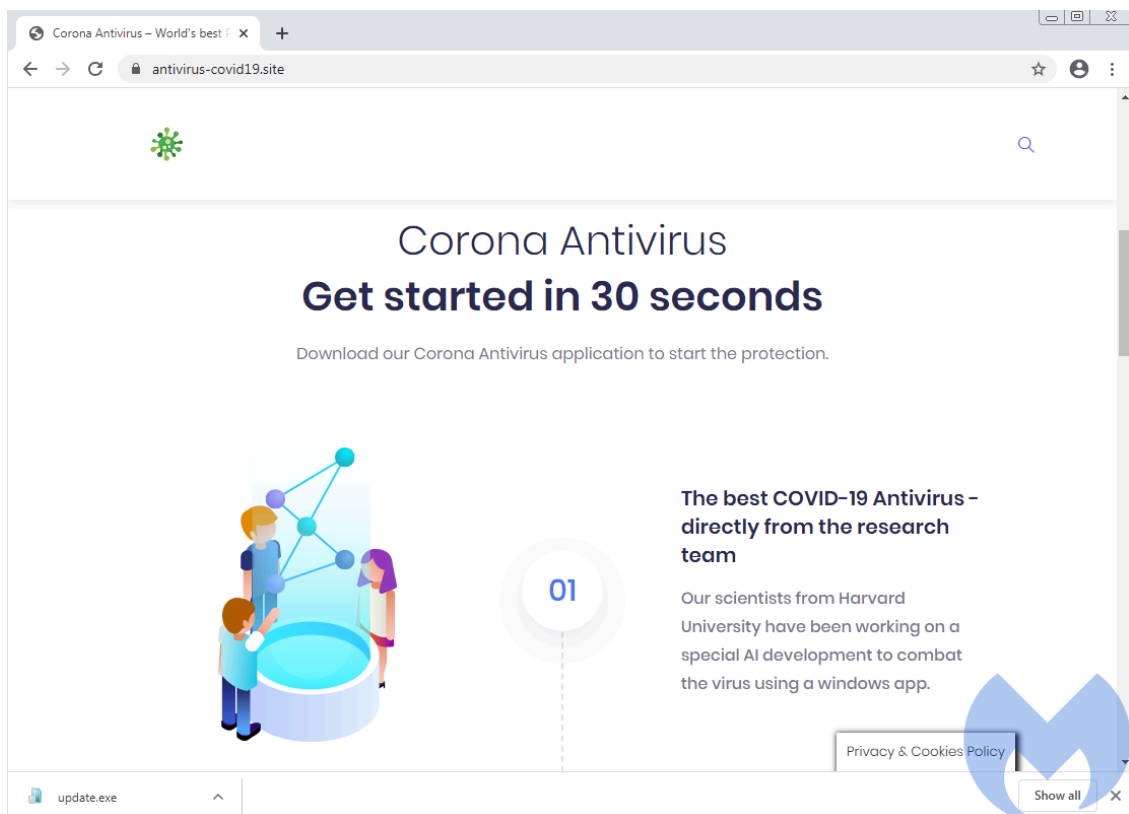
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

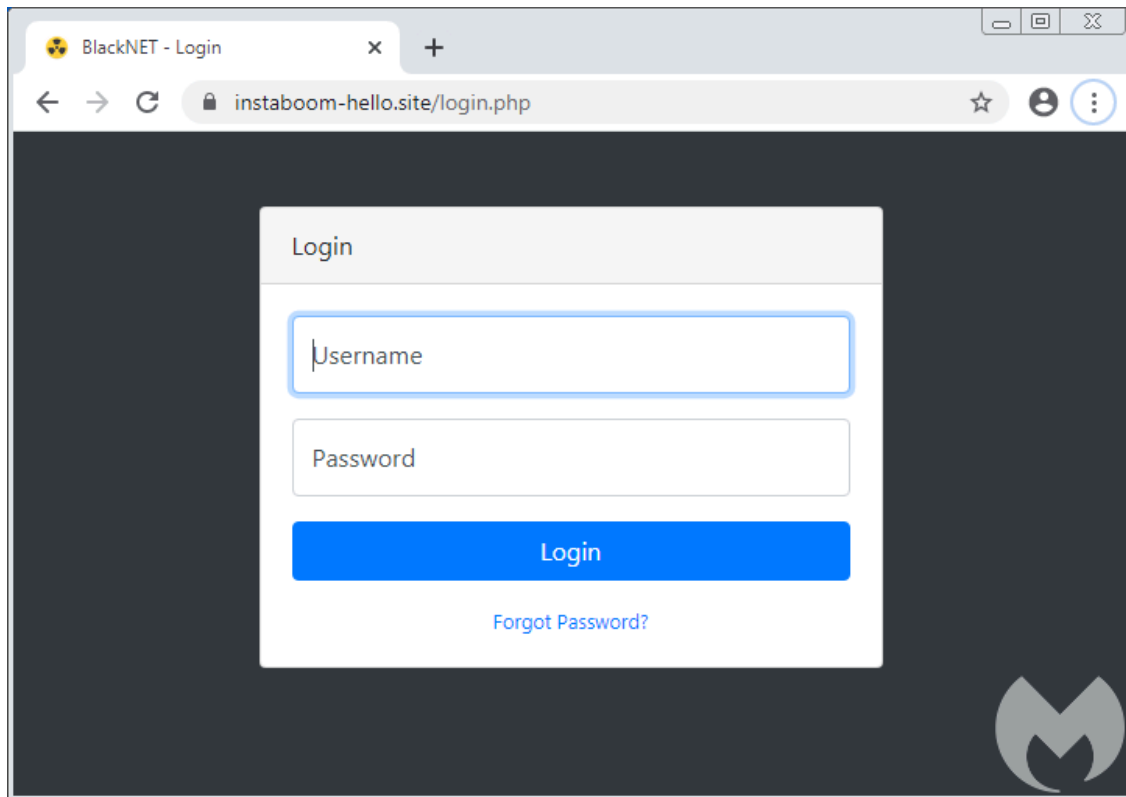


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

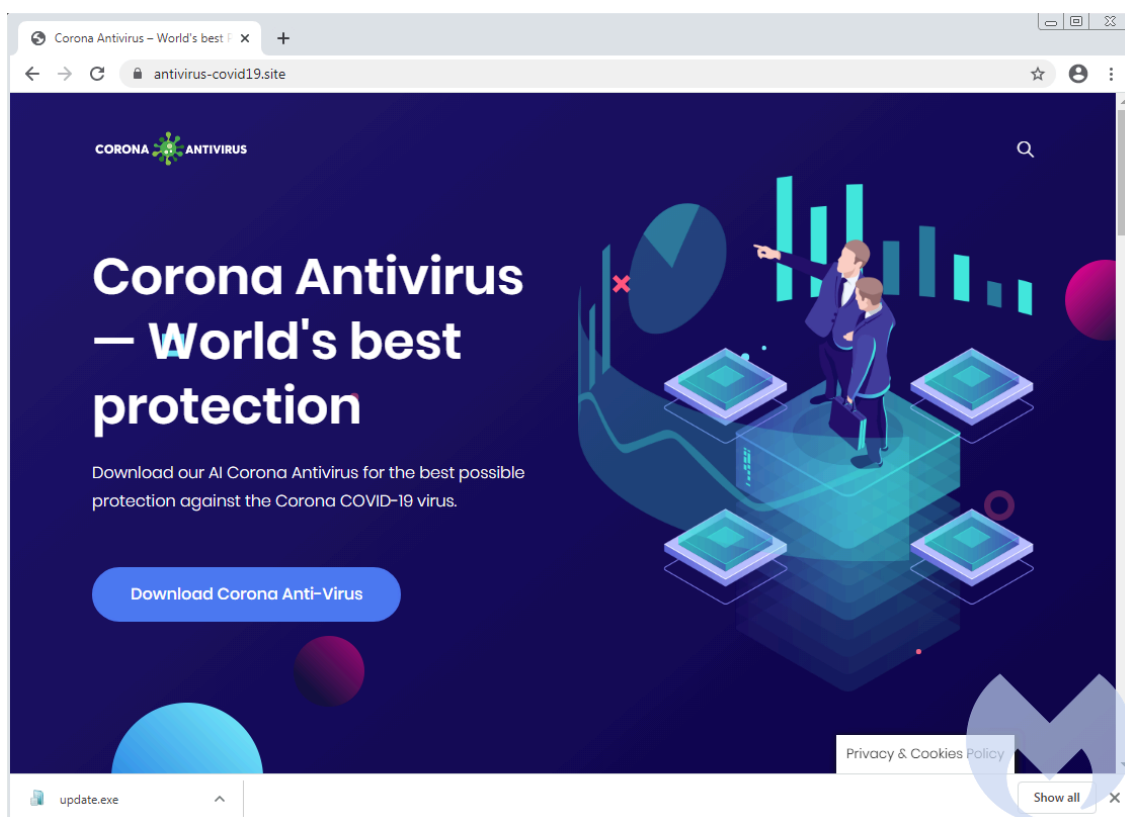
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

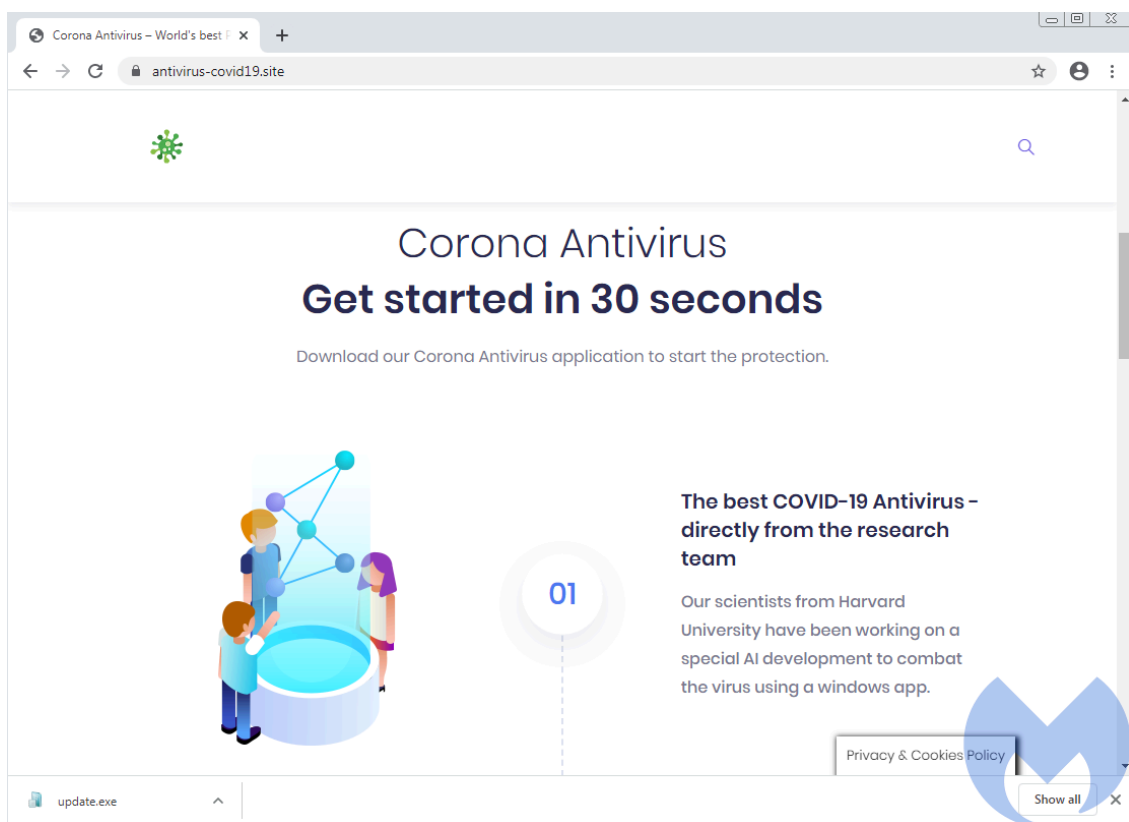
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

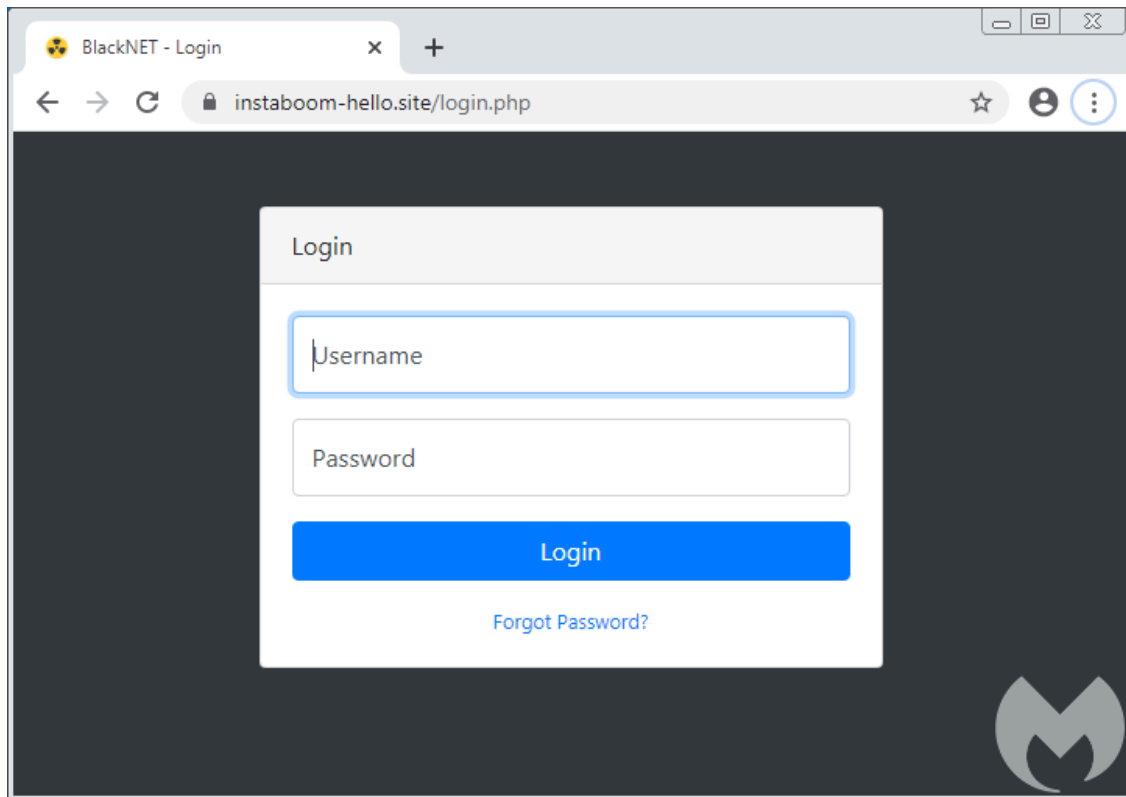


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

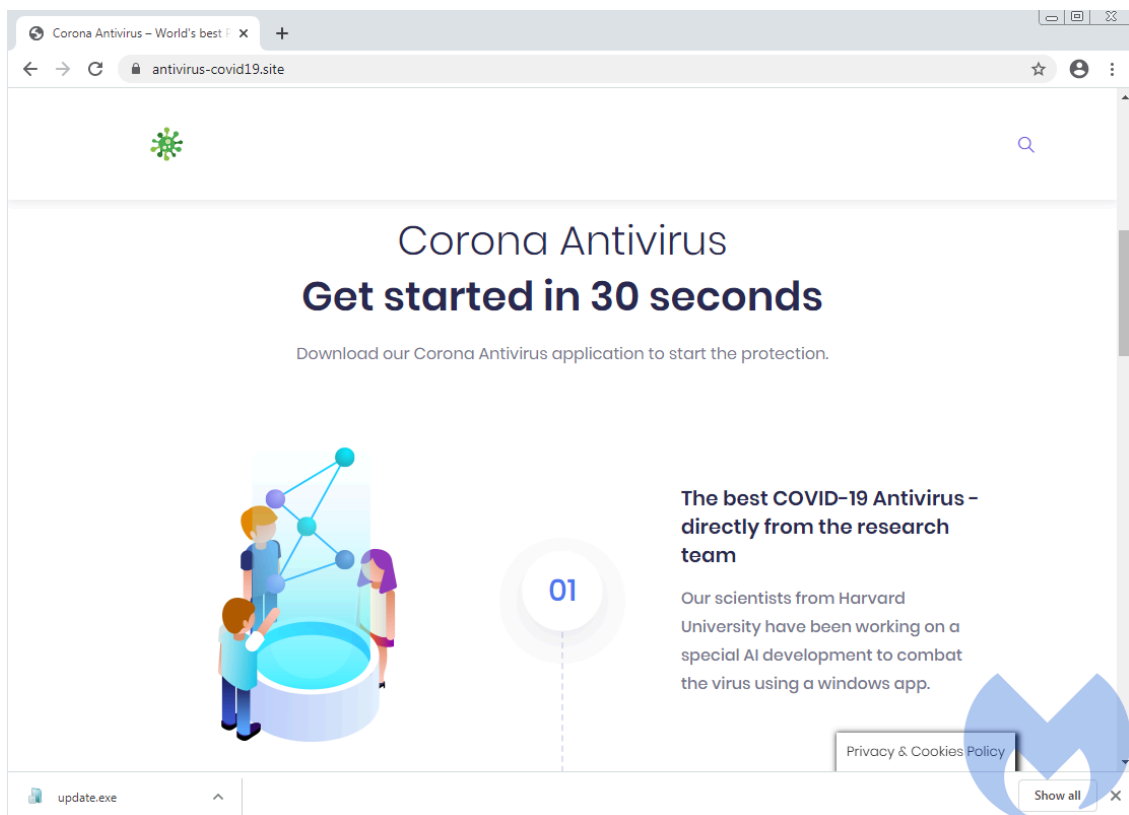
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

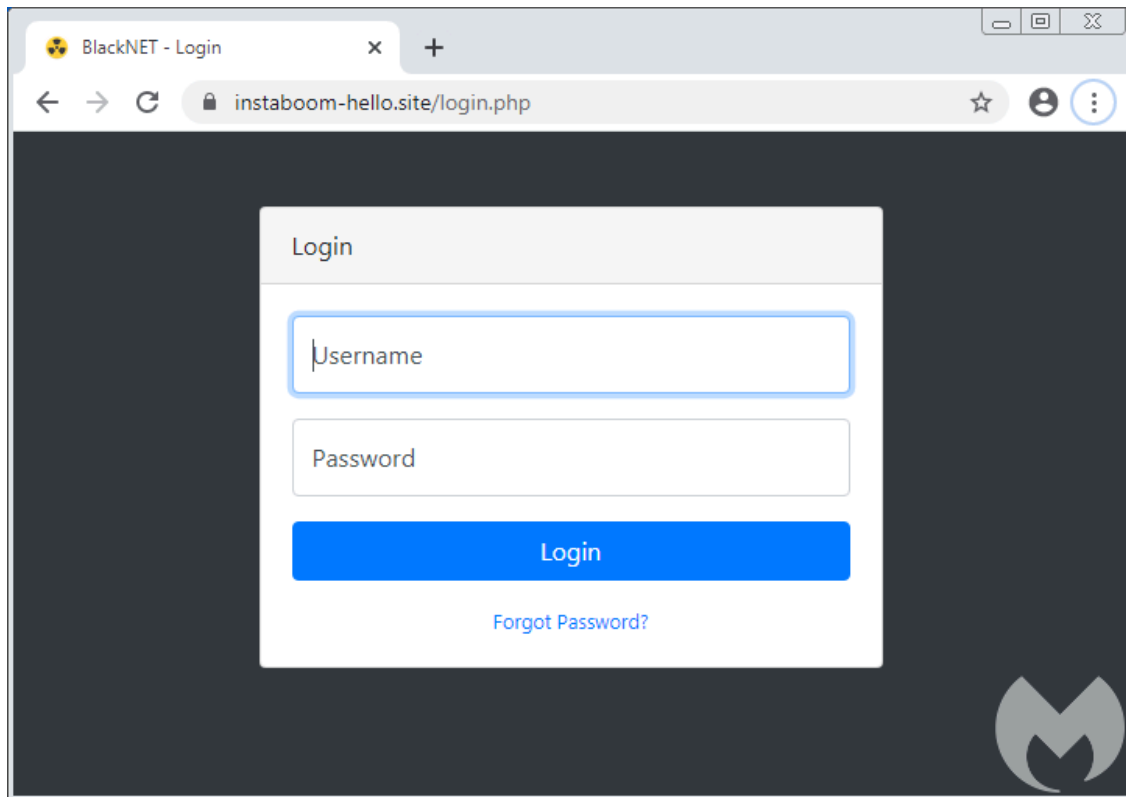


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table are 'Previous' and 'Next' buttons. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right of the commands center is a 'Map Visualization' showing a world map with a blue overlay. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

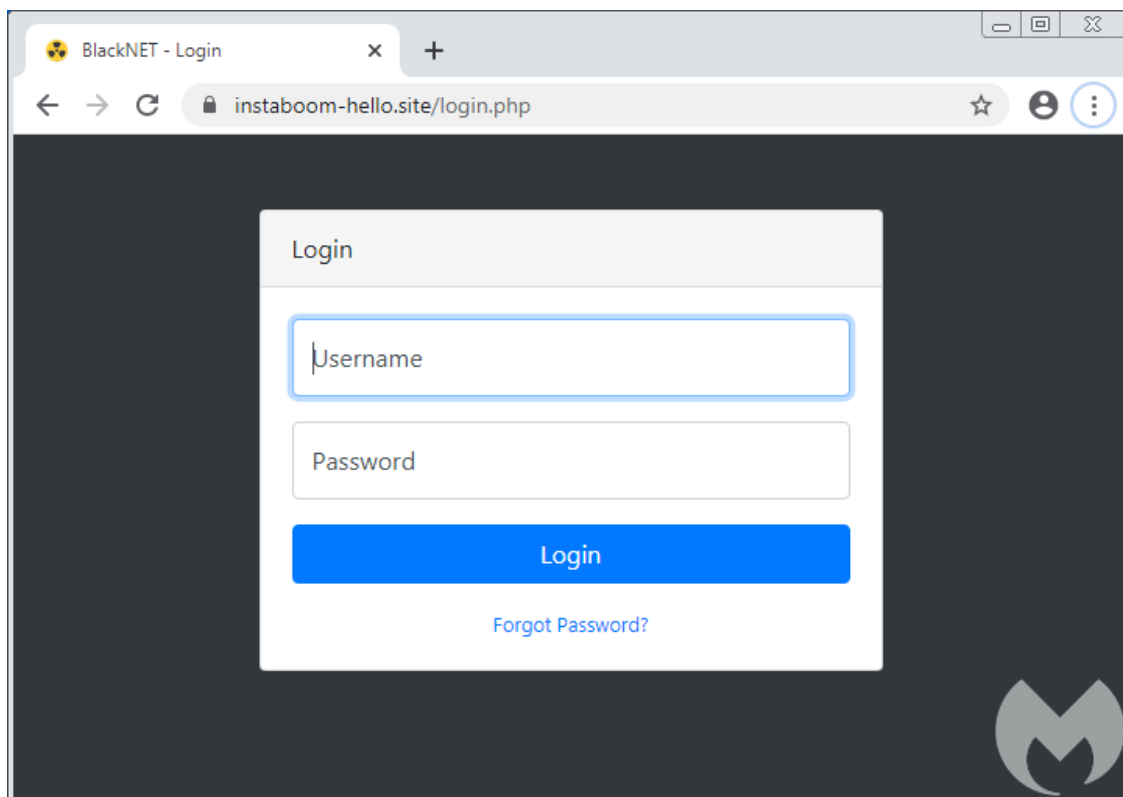
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

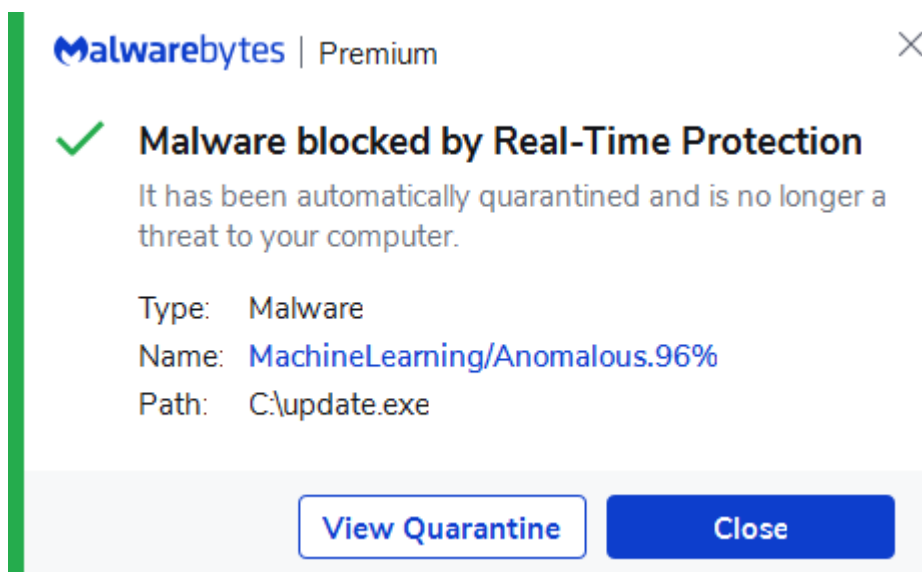
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

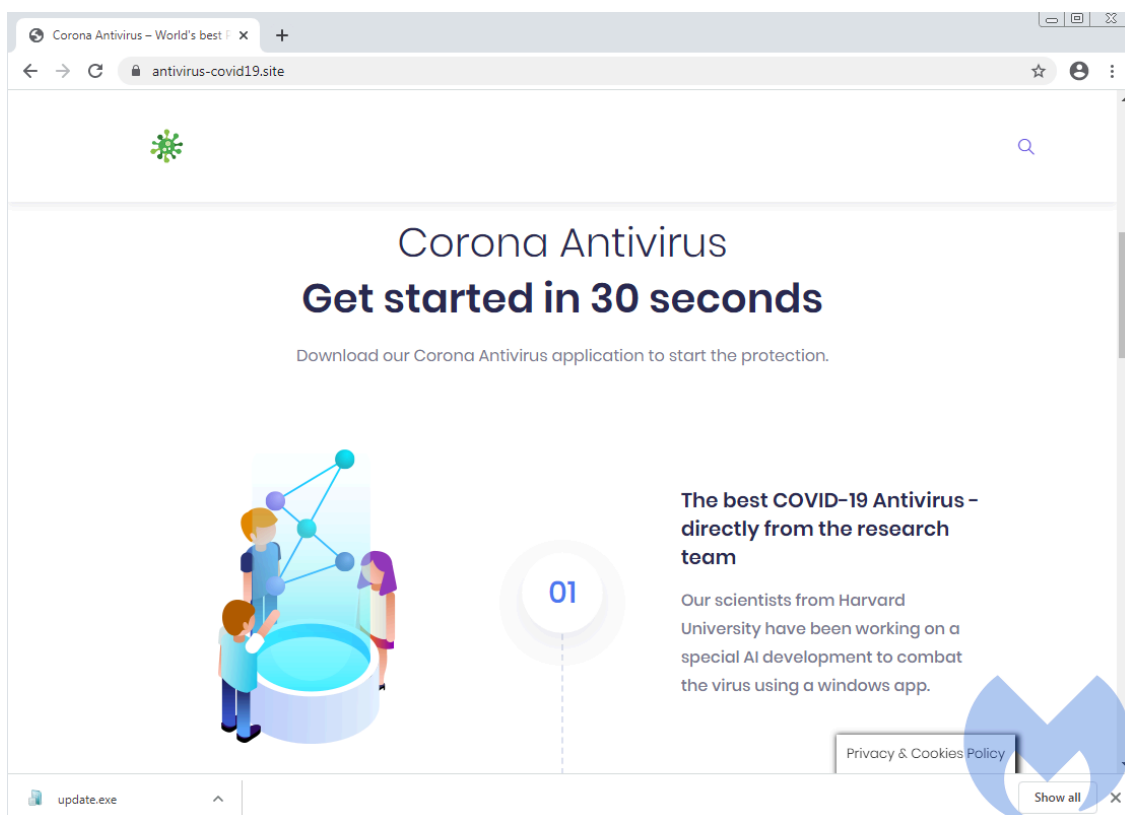
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

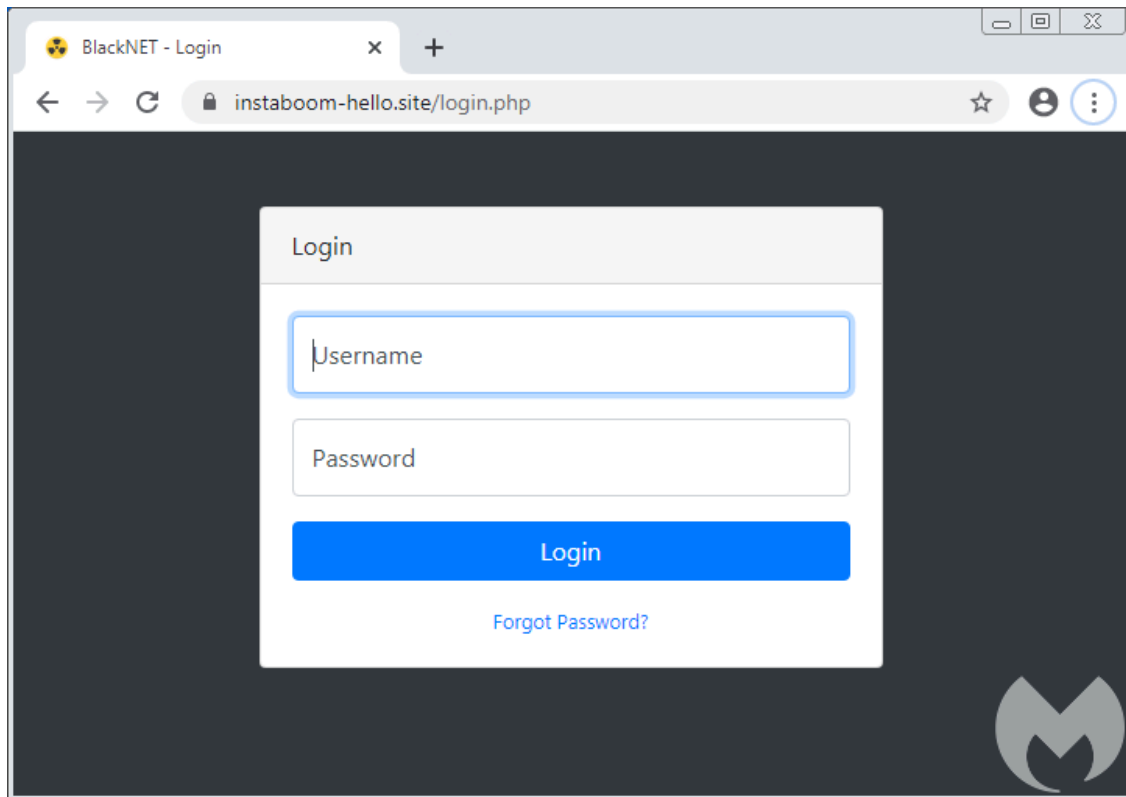


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue dot indicating a client location. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

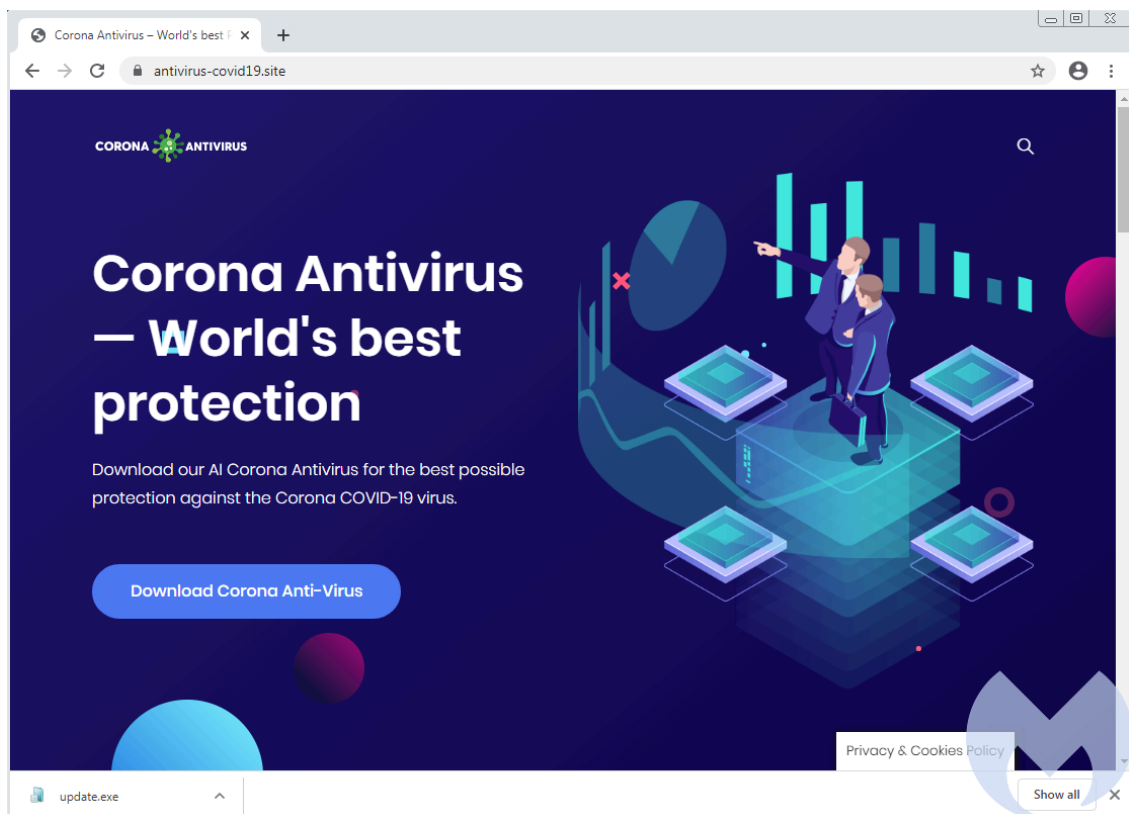
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

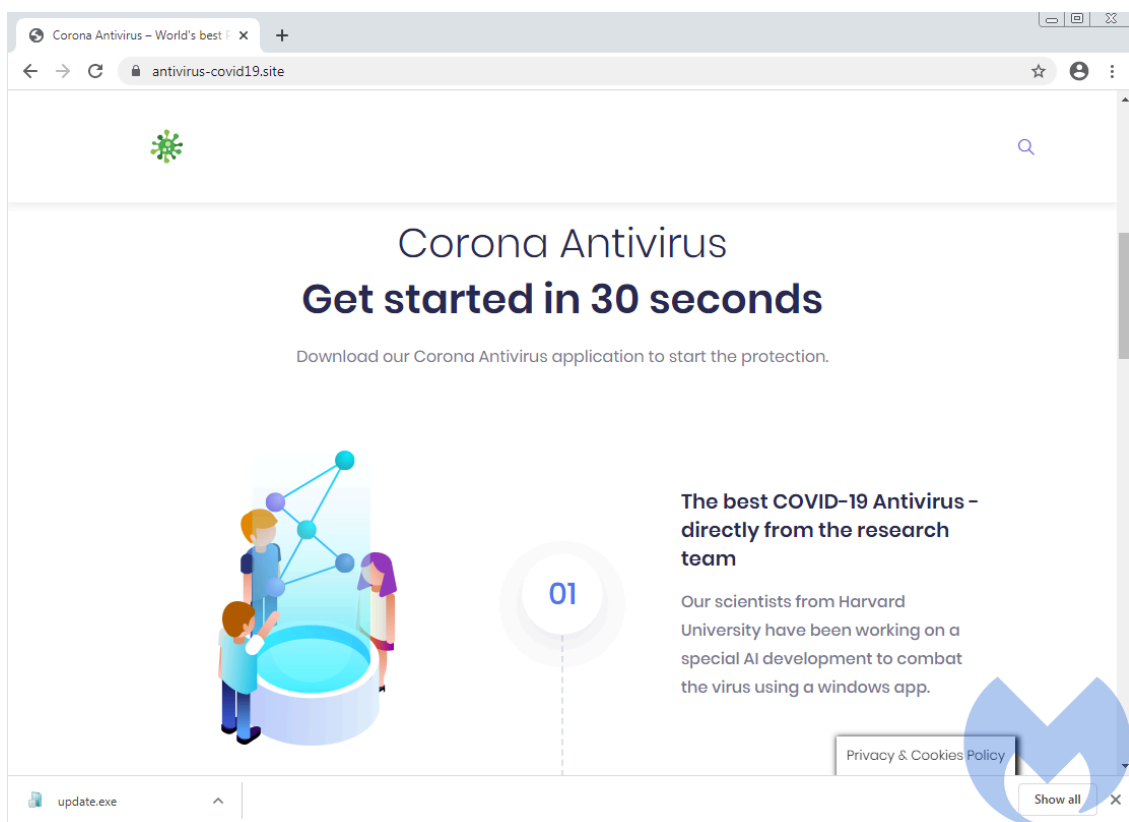
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

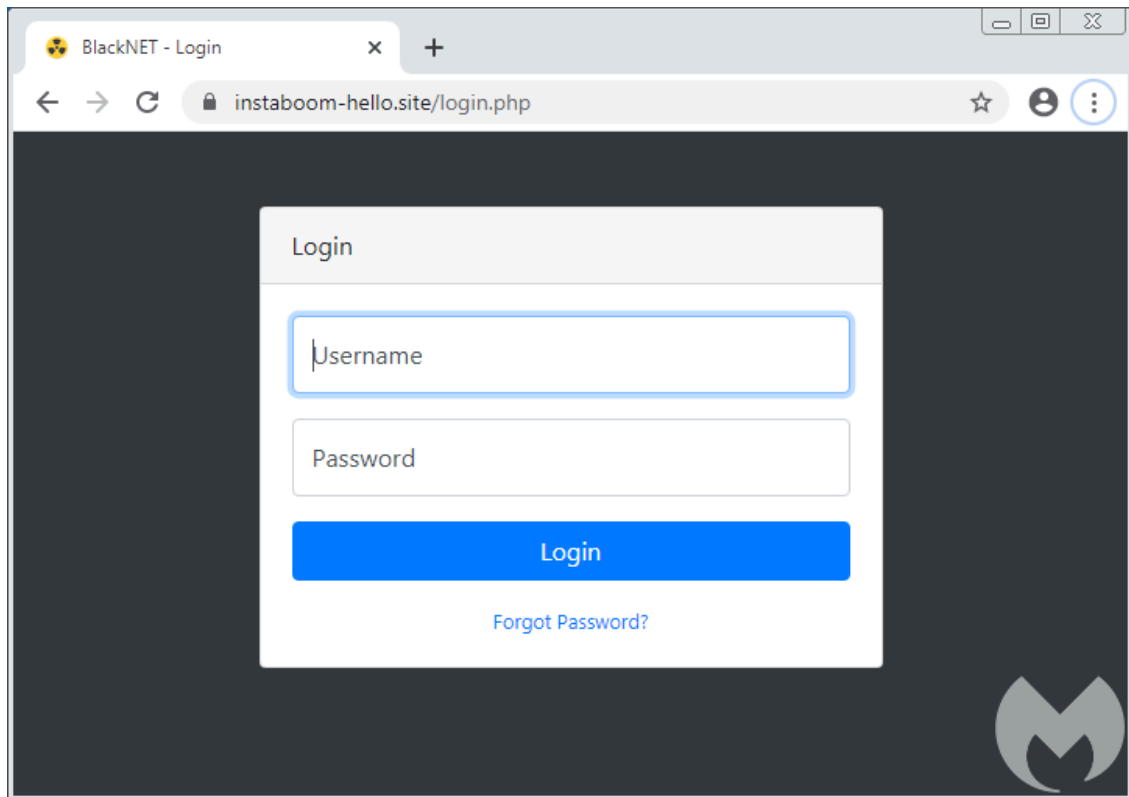


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

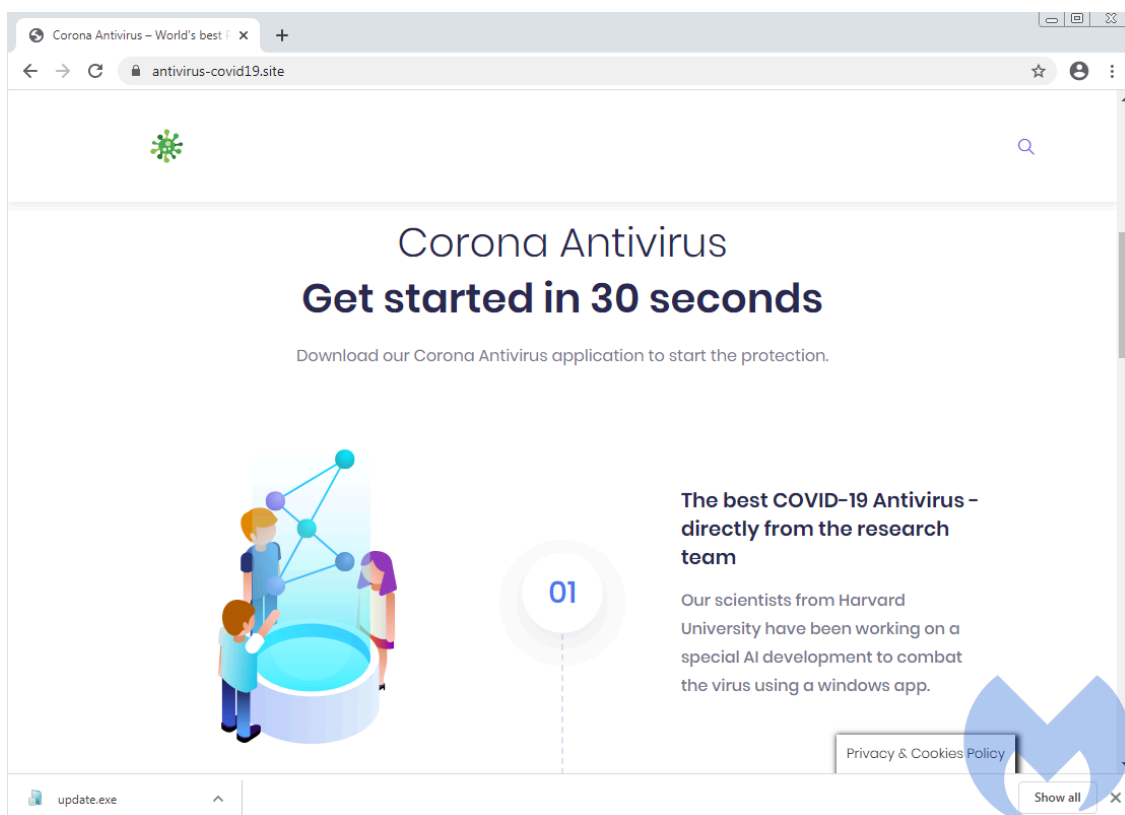
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

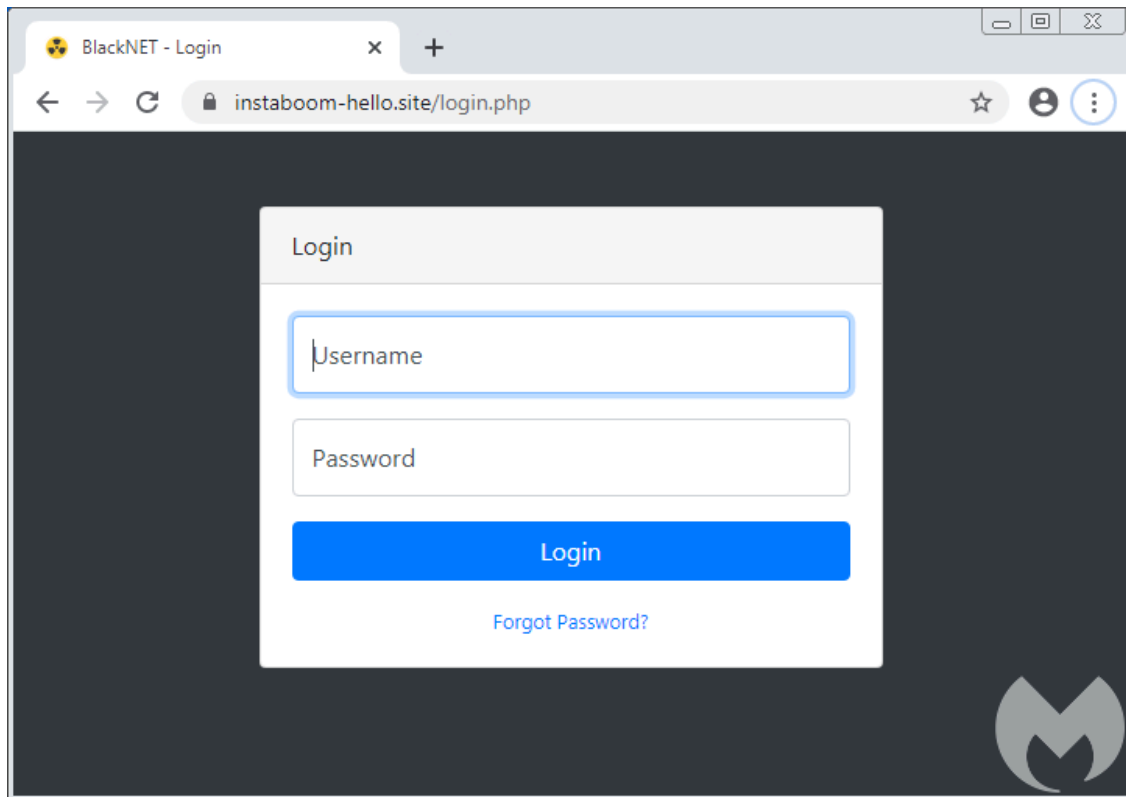


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

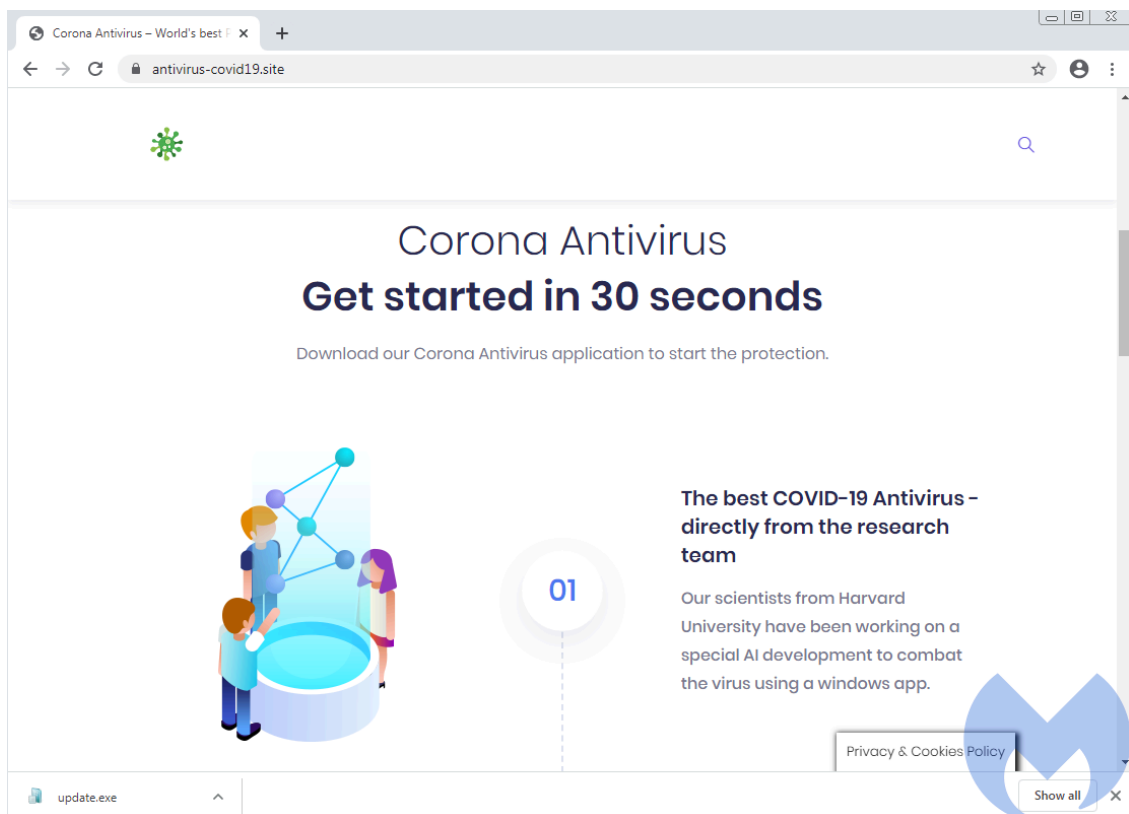
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

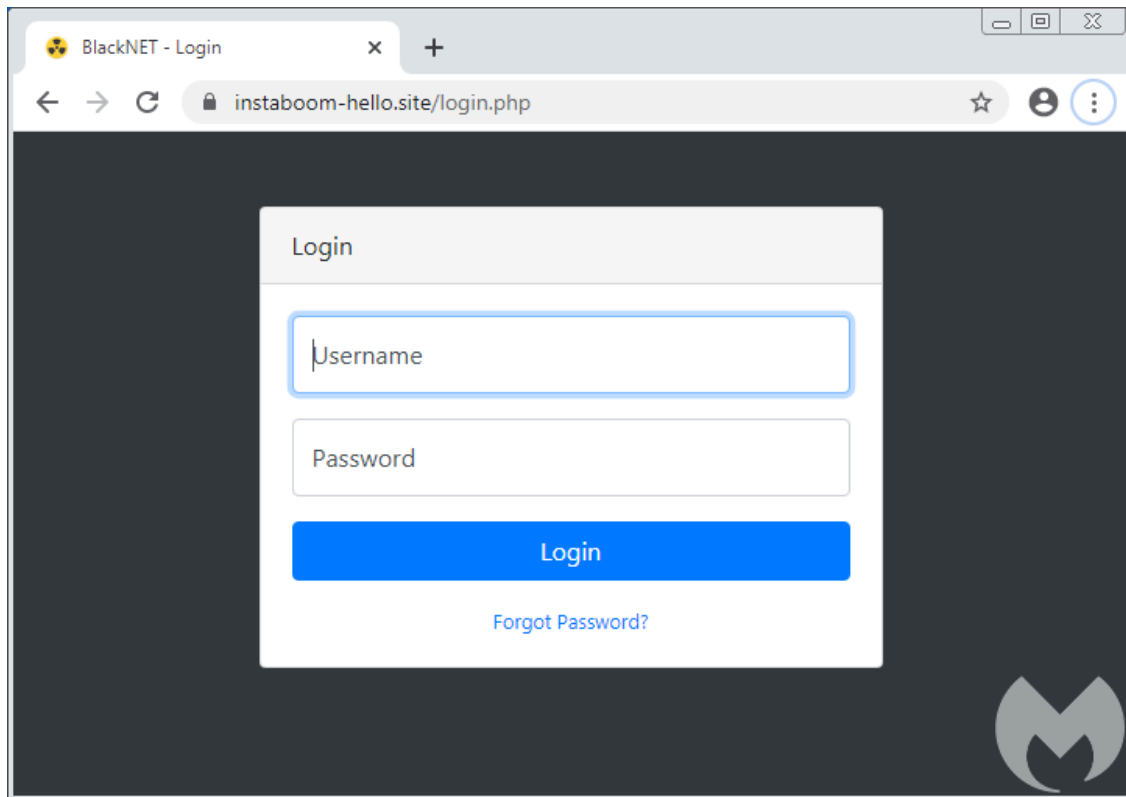


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. At the top left is the Malwarebytes logo and "Premium" text. At the top right is a close button (X). Below the header is a green checkmark icon followed by the text "Malware blocked by Real-Time Protection". Below this is a message: "It has been automatically quarantined and is no longer a threat to your computer." Below the message are three lines of information: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

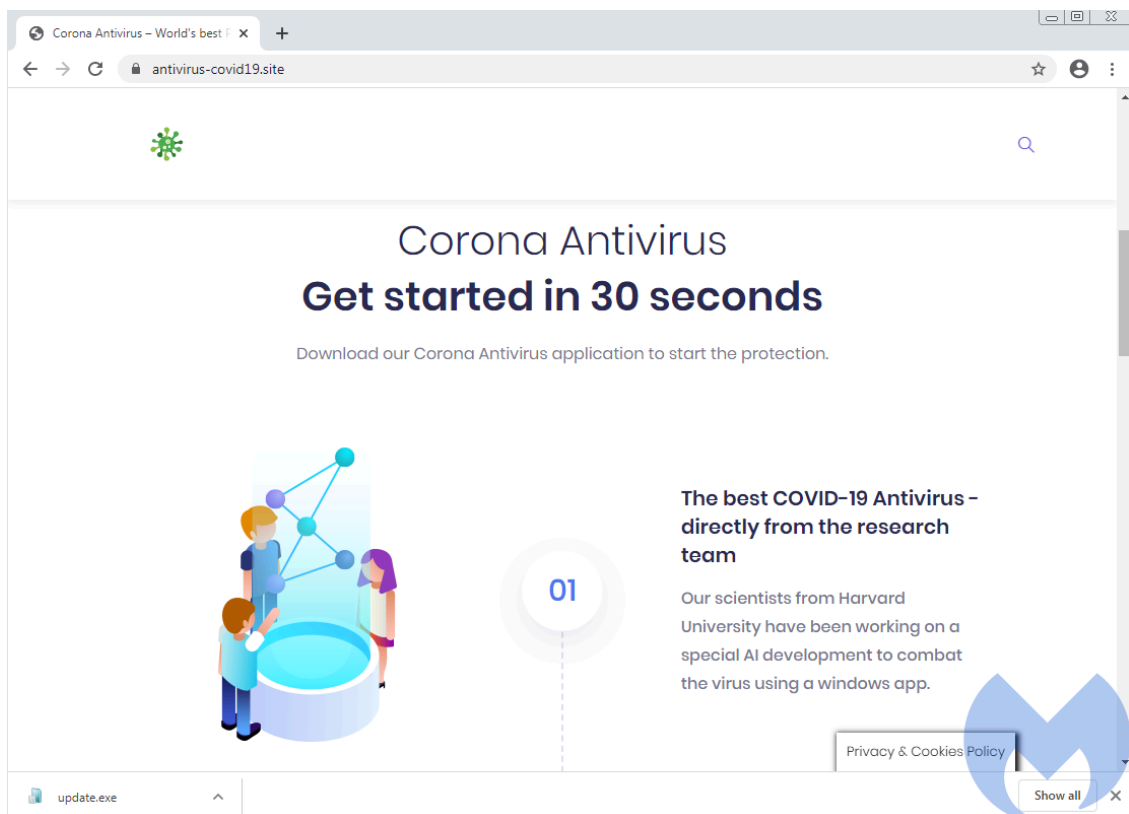
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

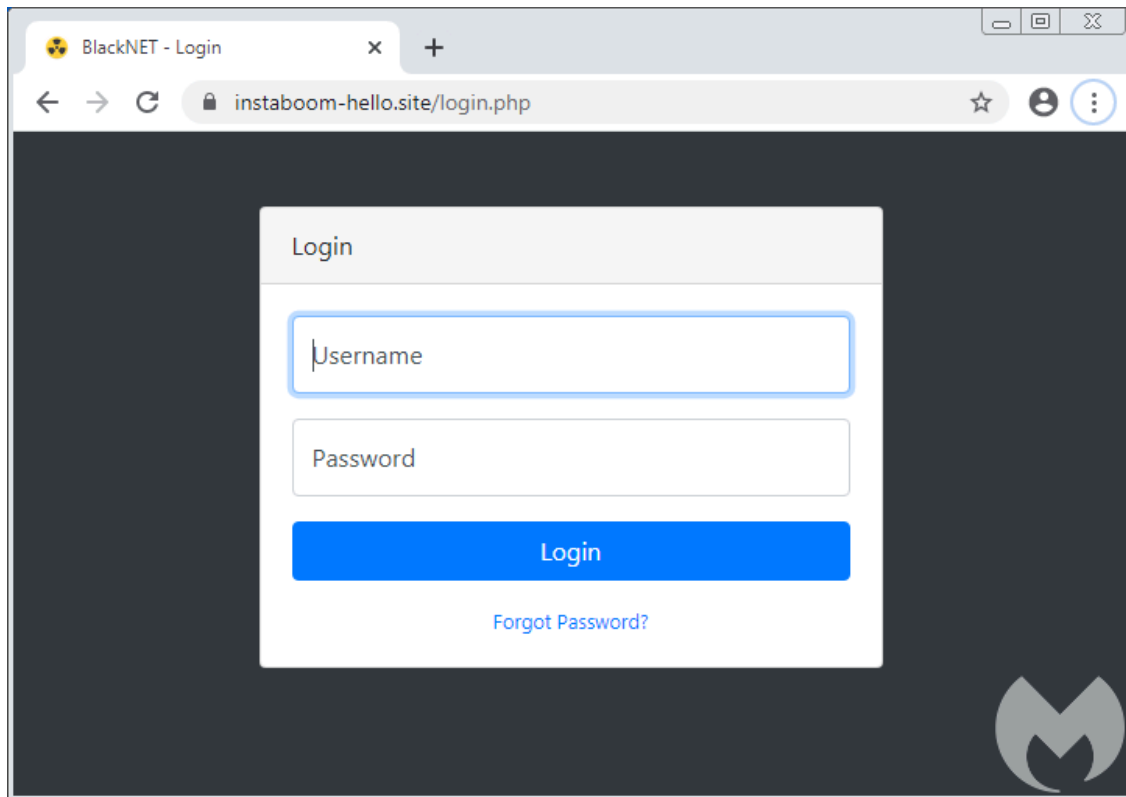


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

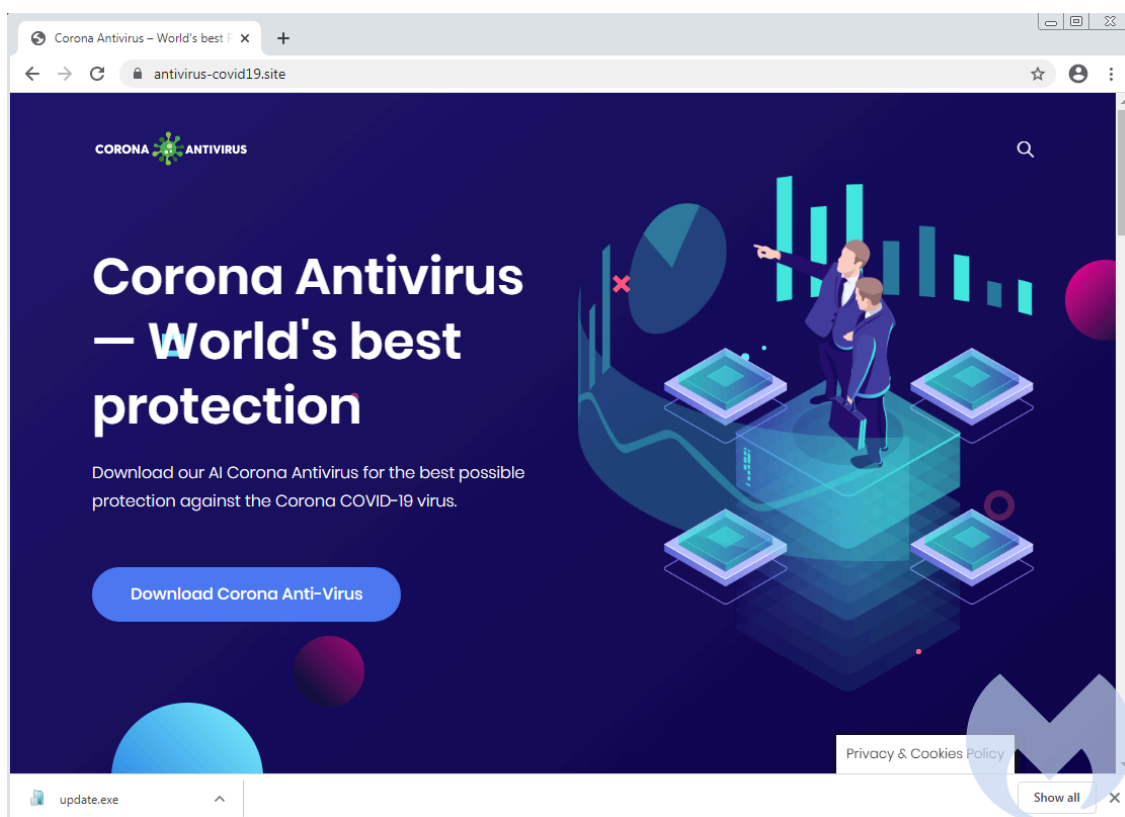
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

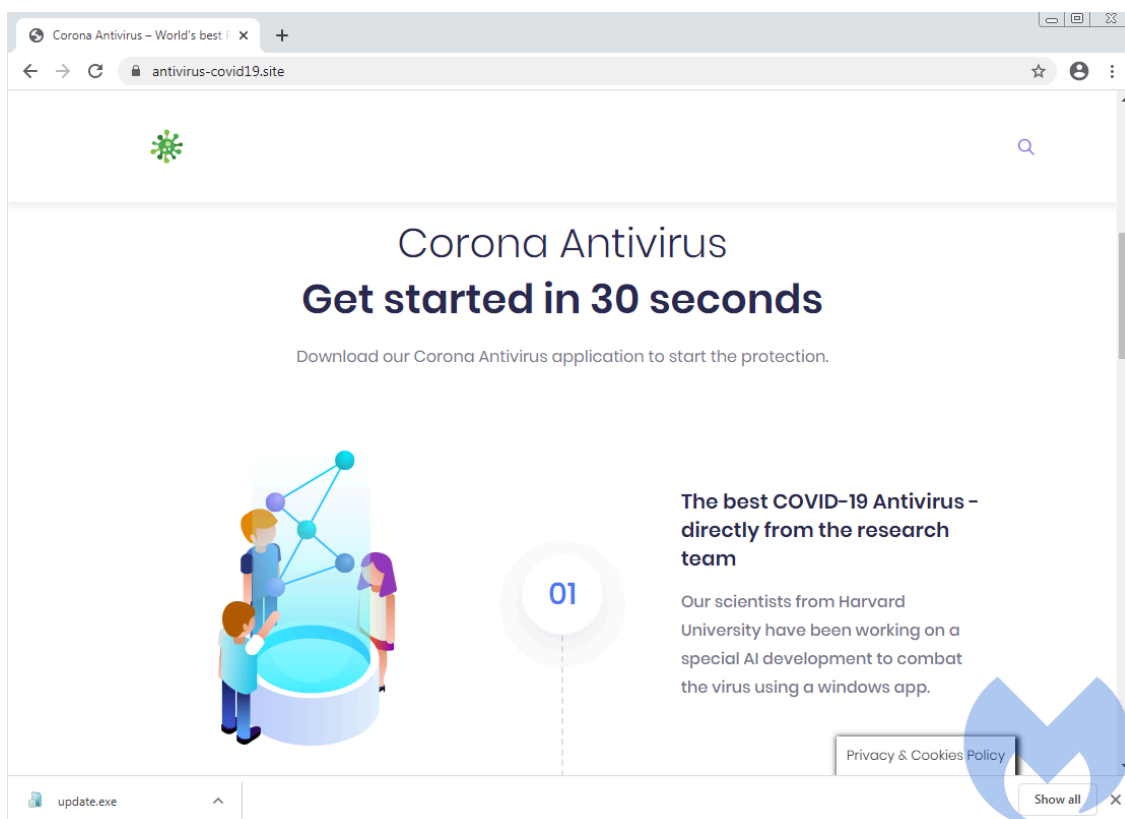
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

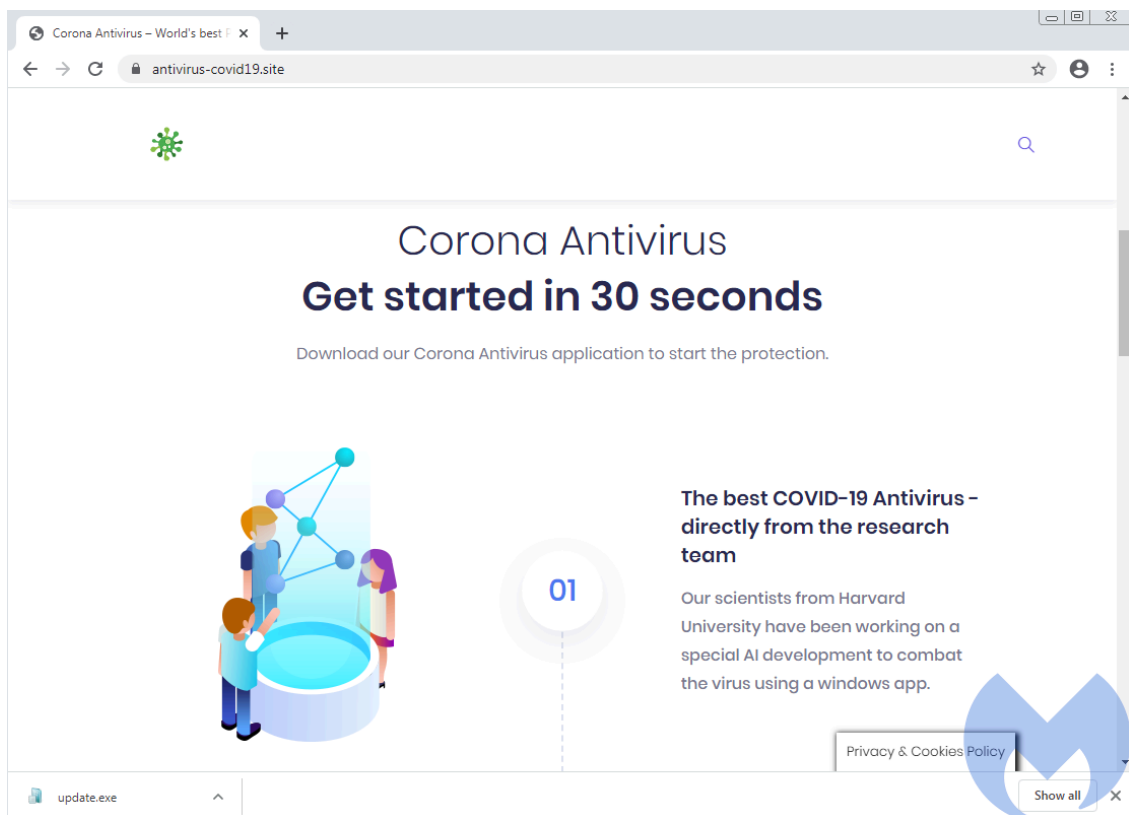
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

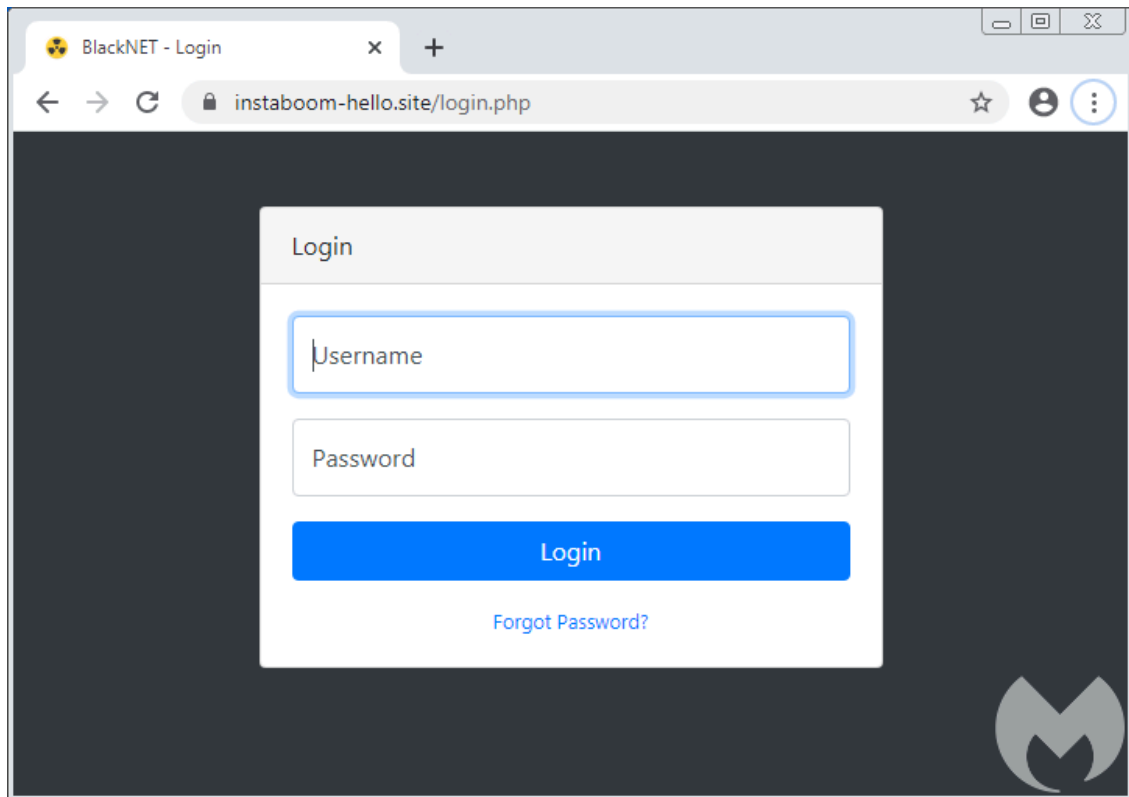


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

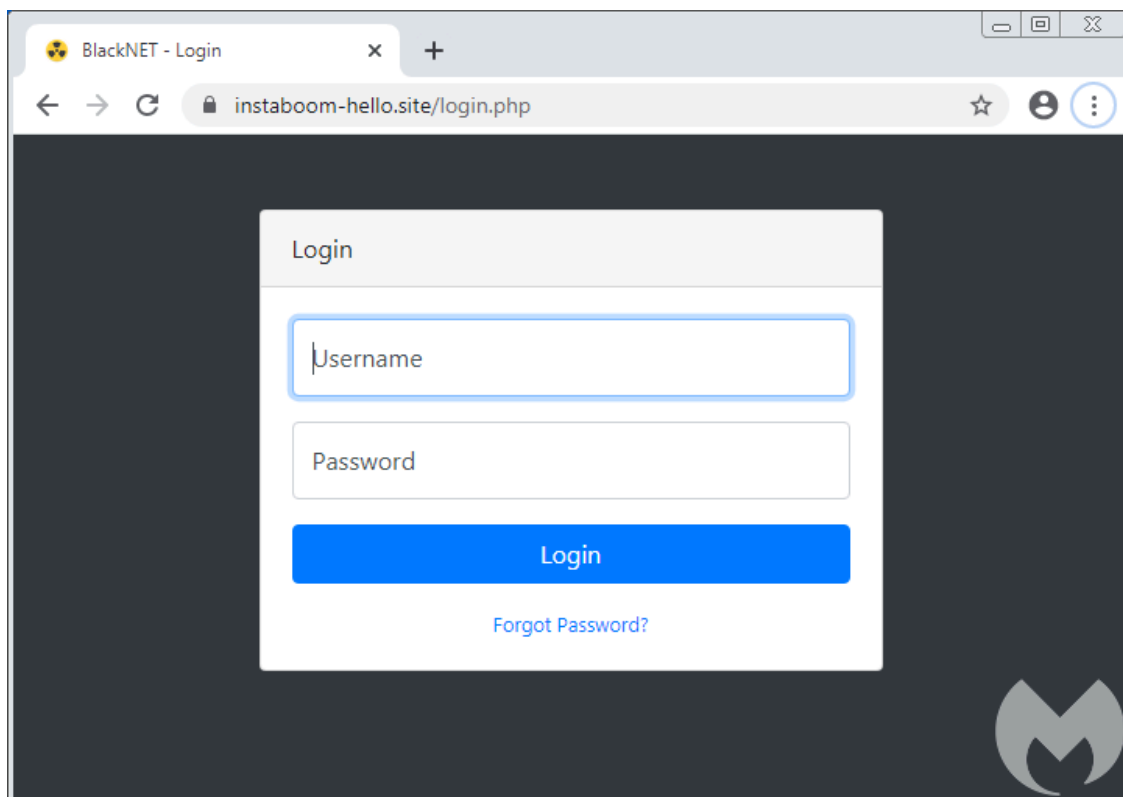
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

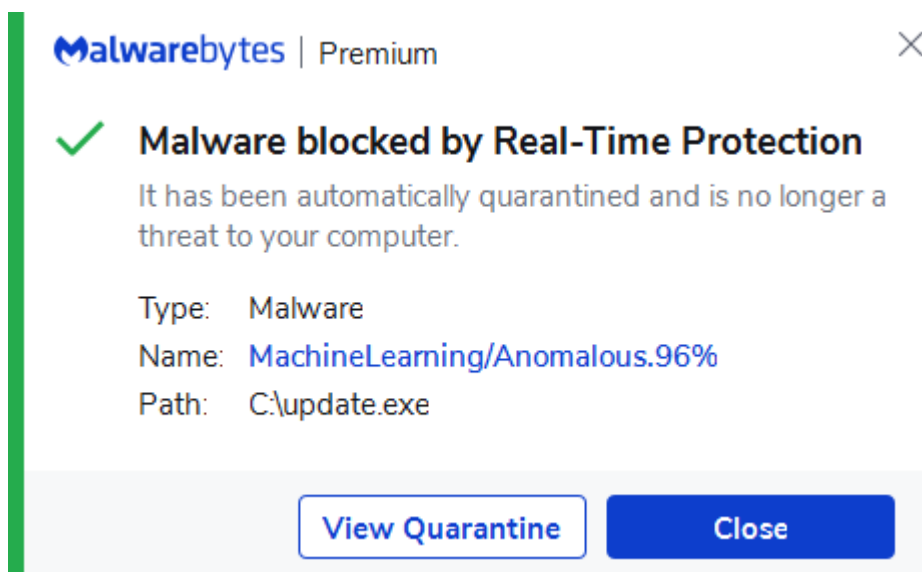
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

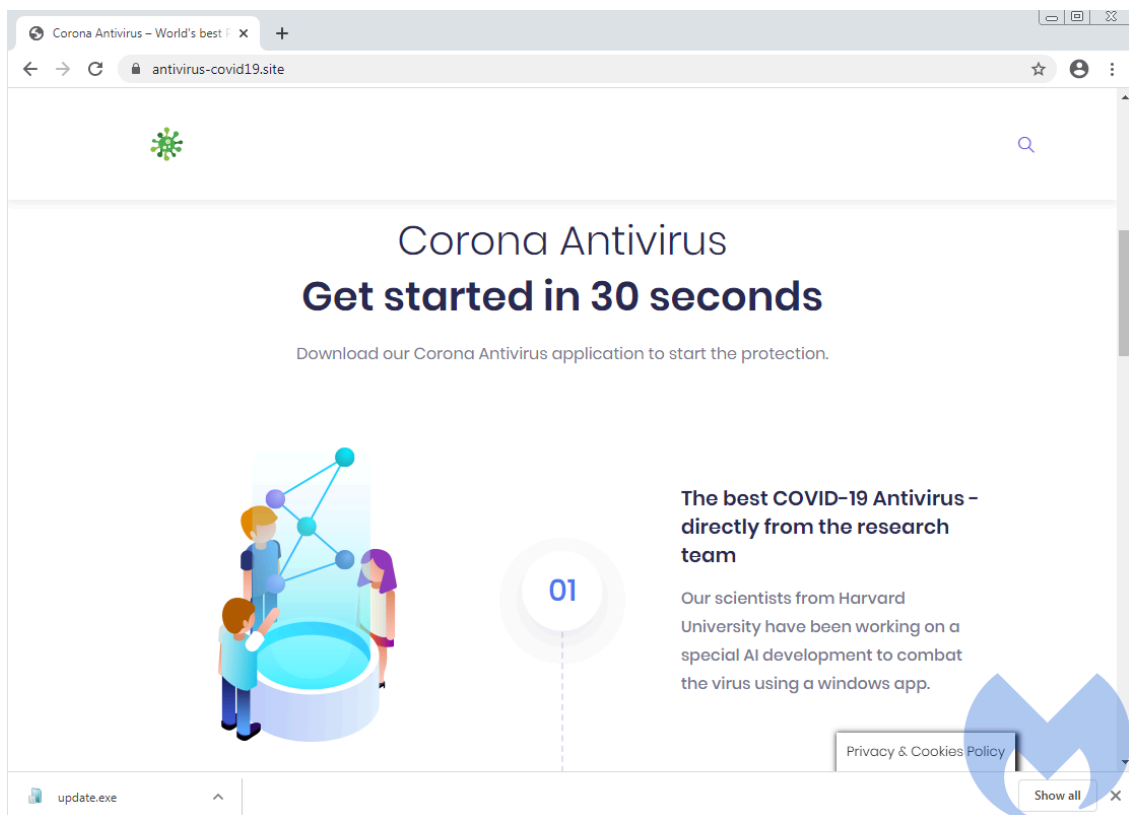
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

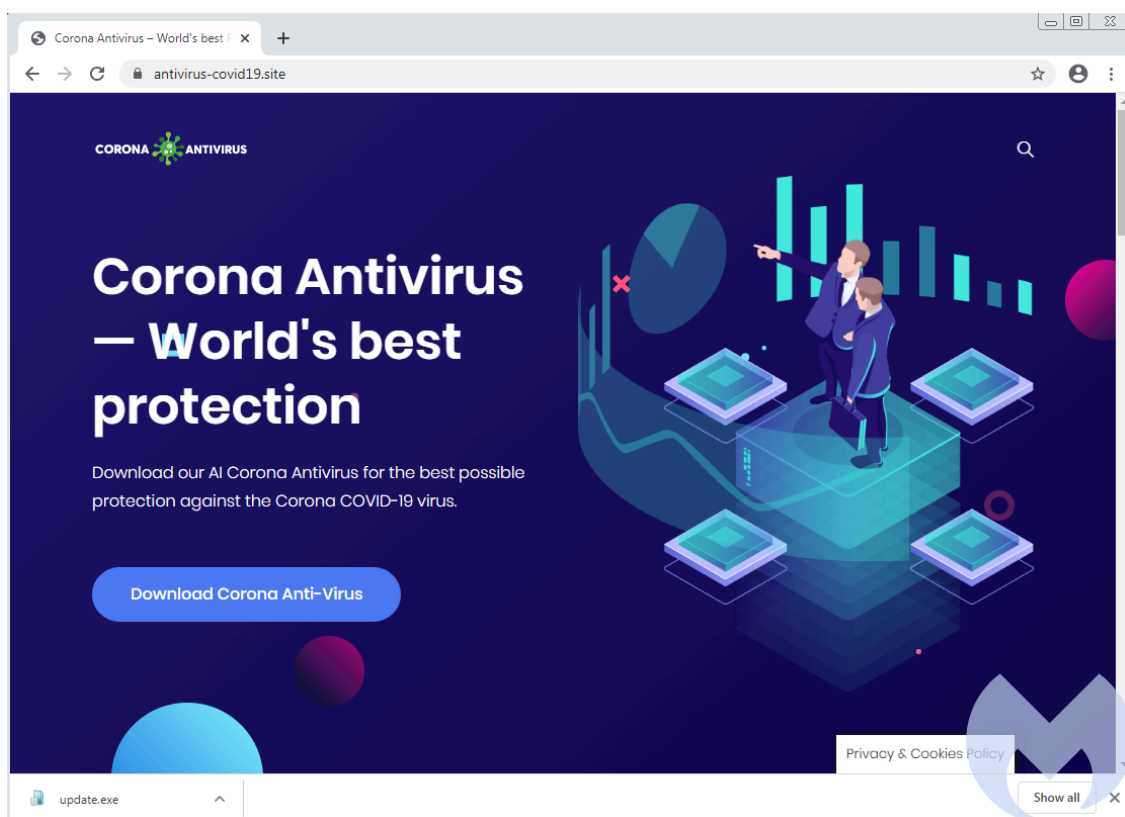
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

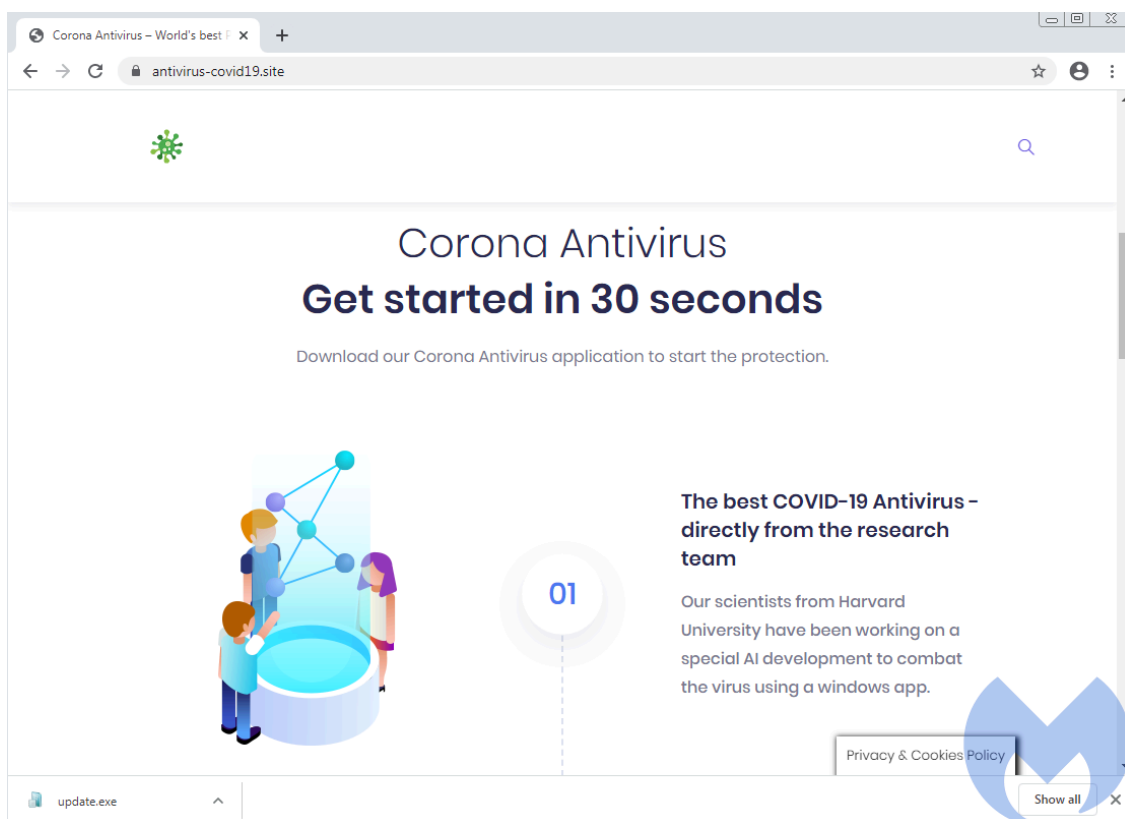
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

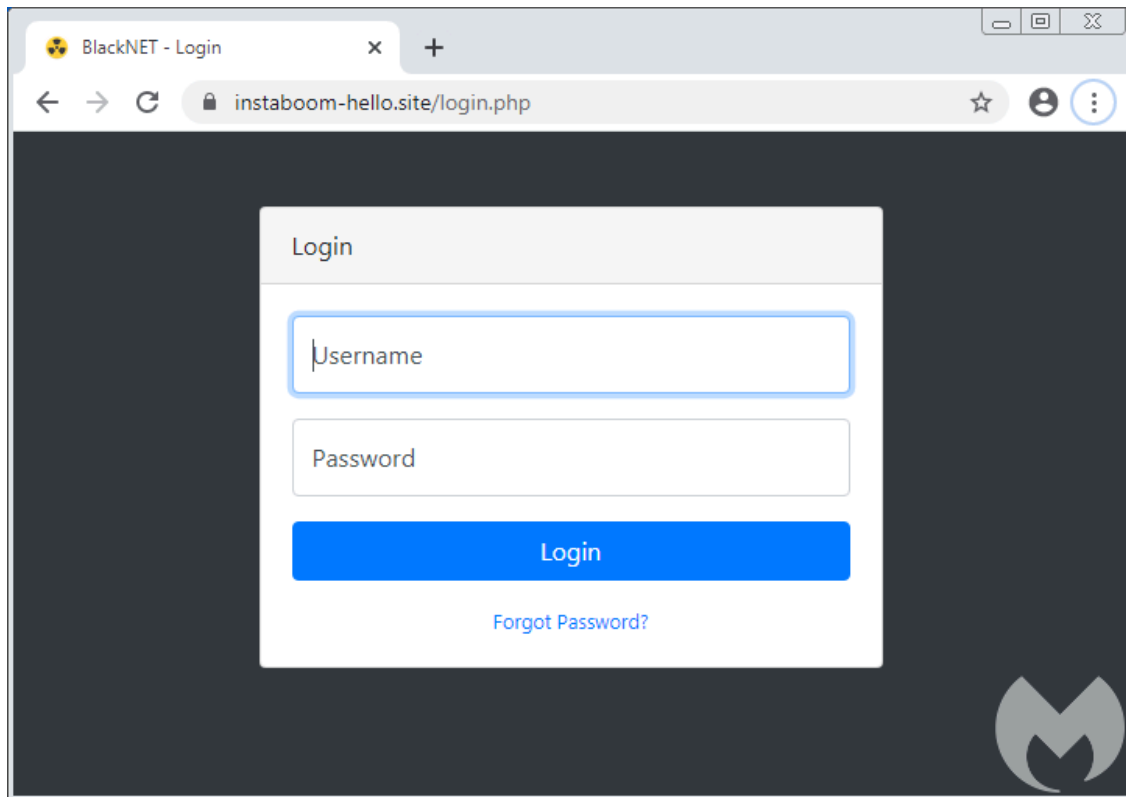


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

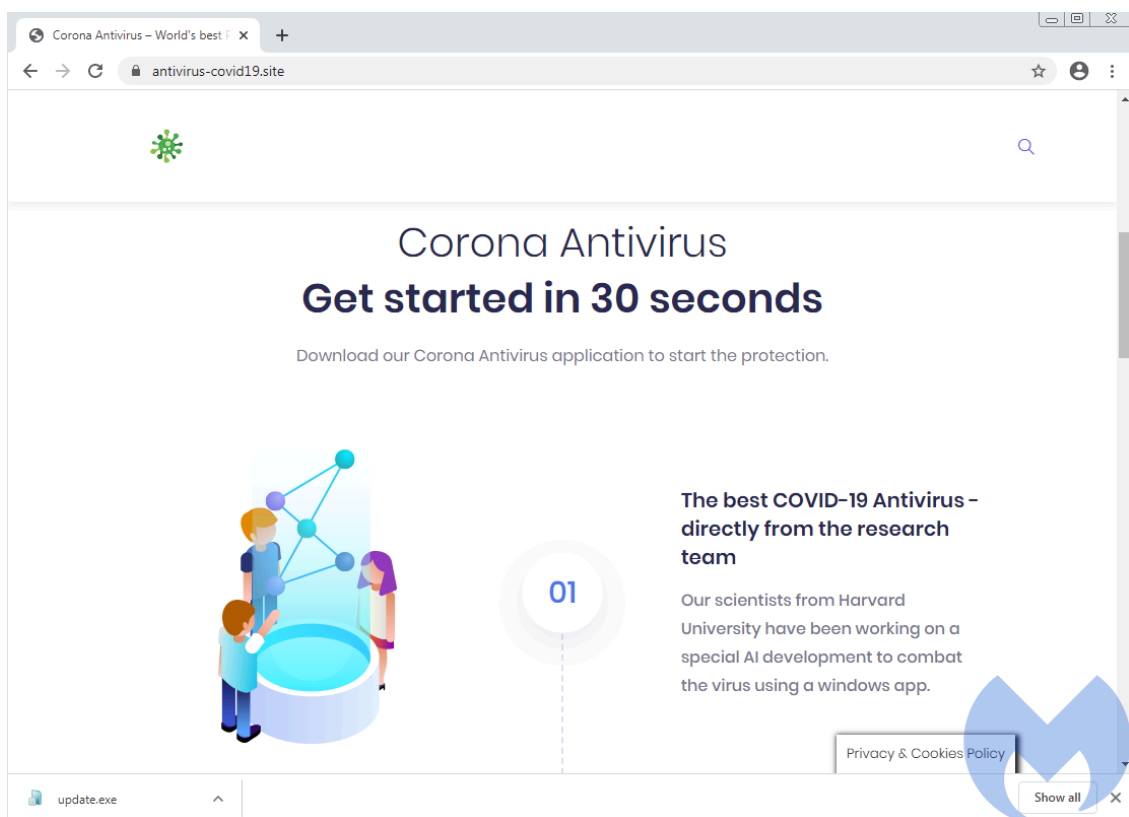
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

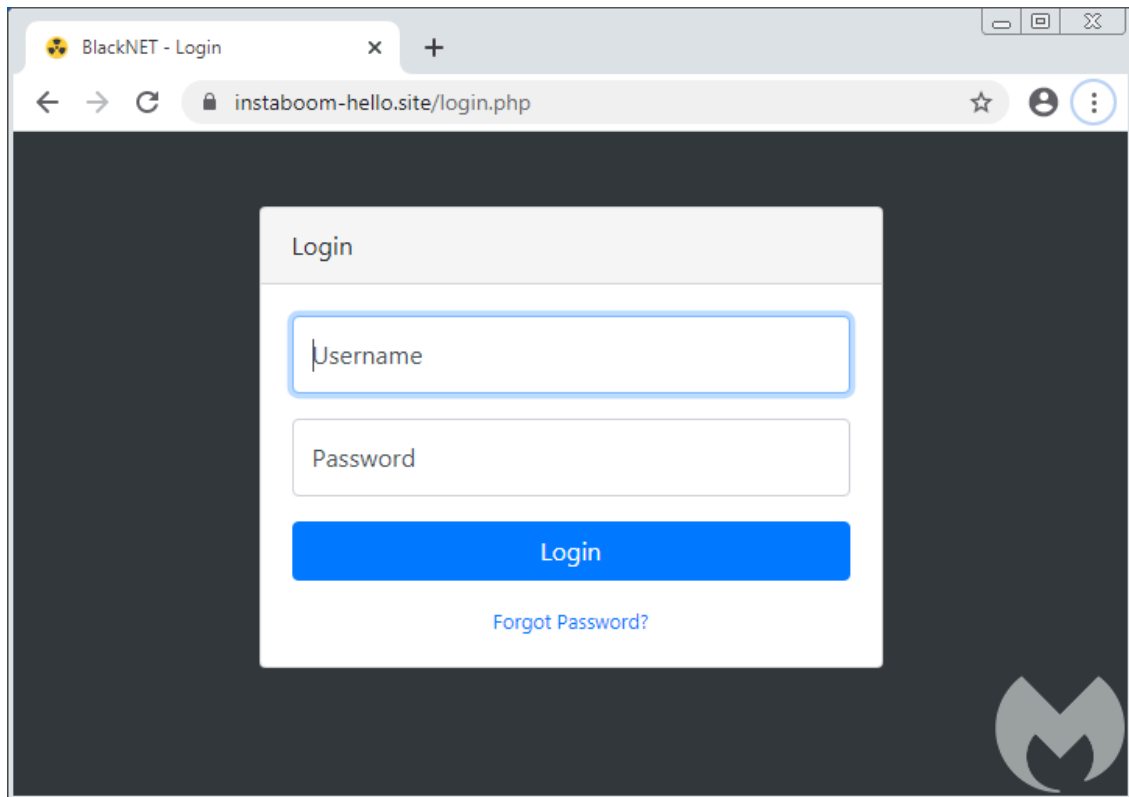


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

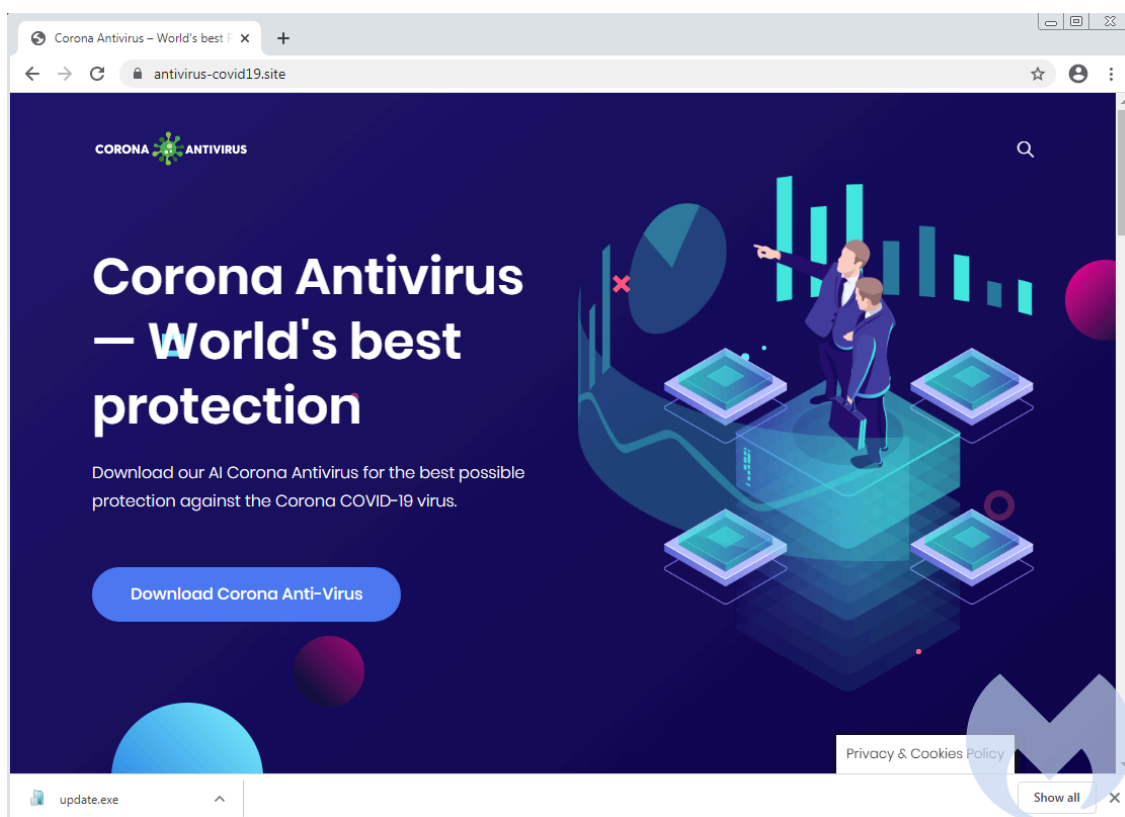
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

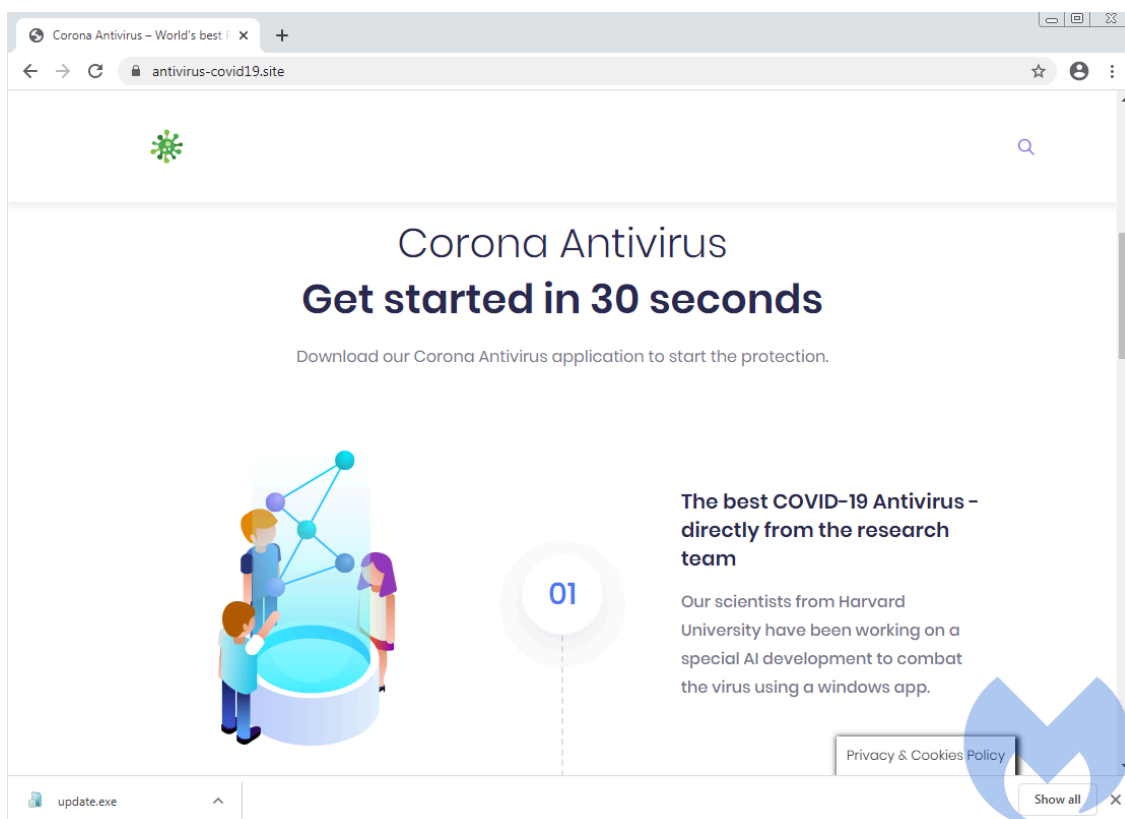
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

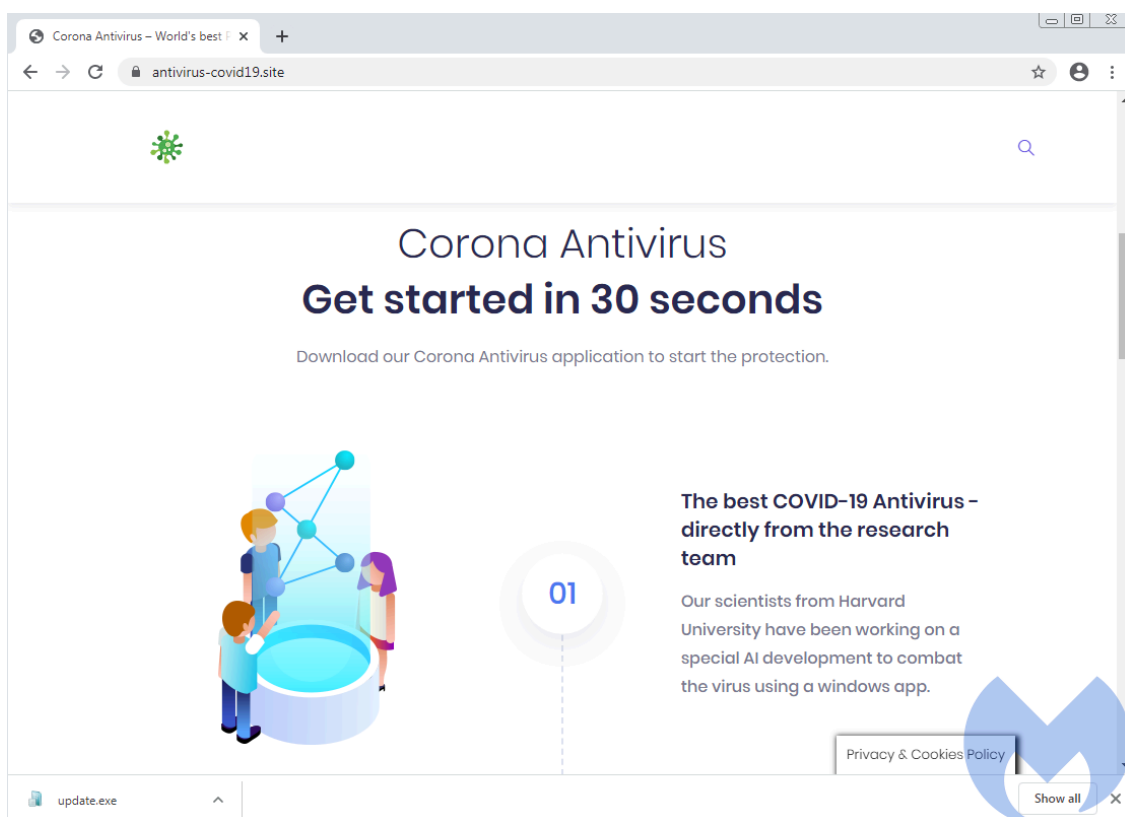
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

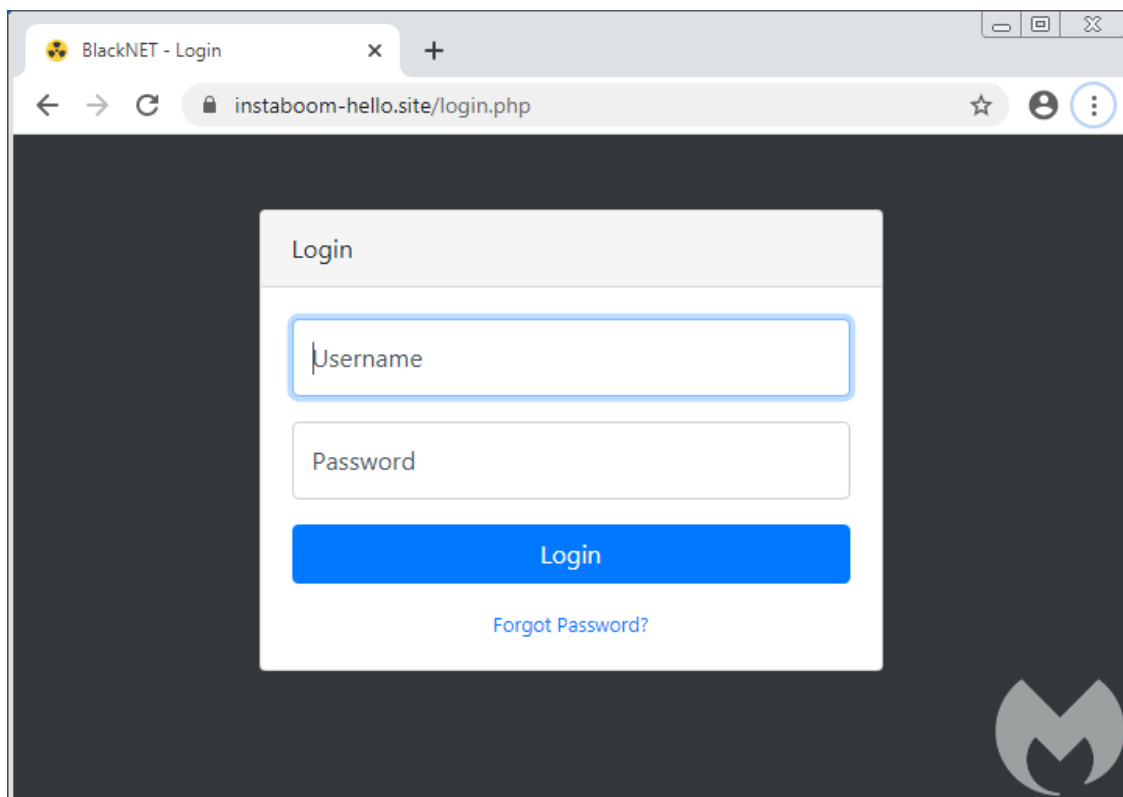


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

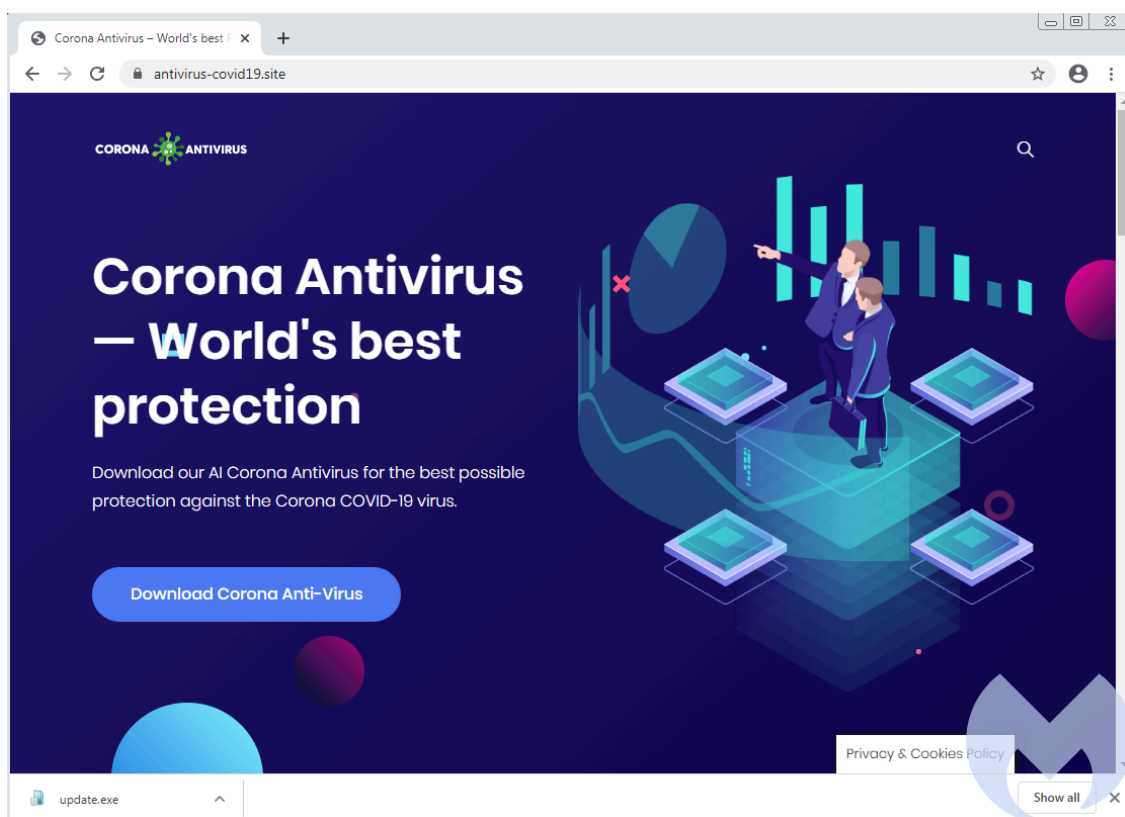
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

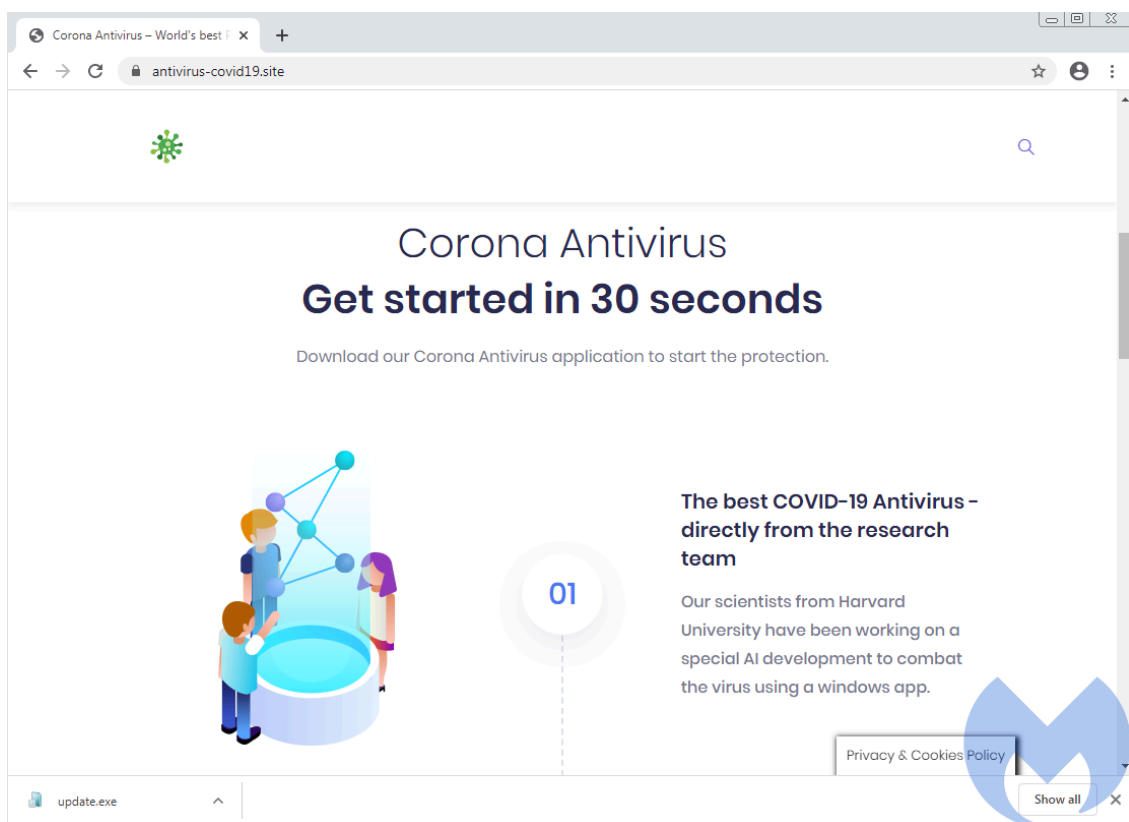
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

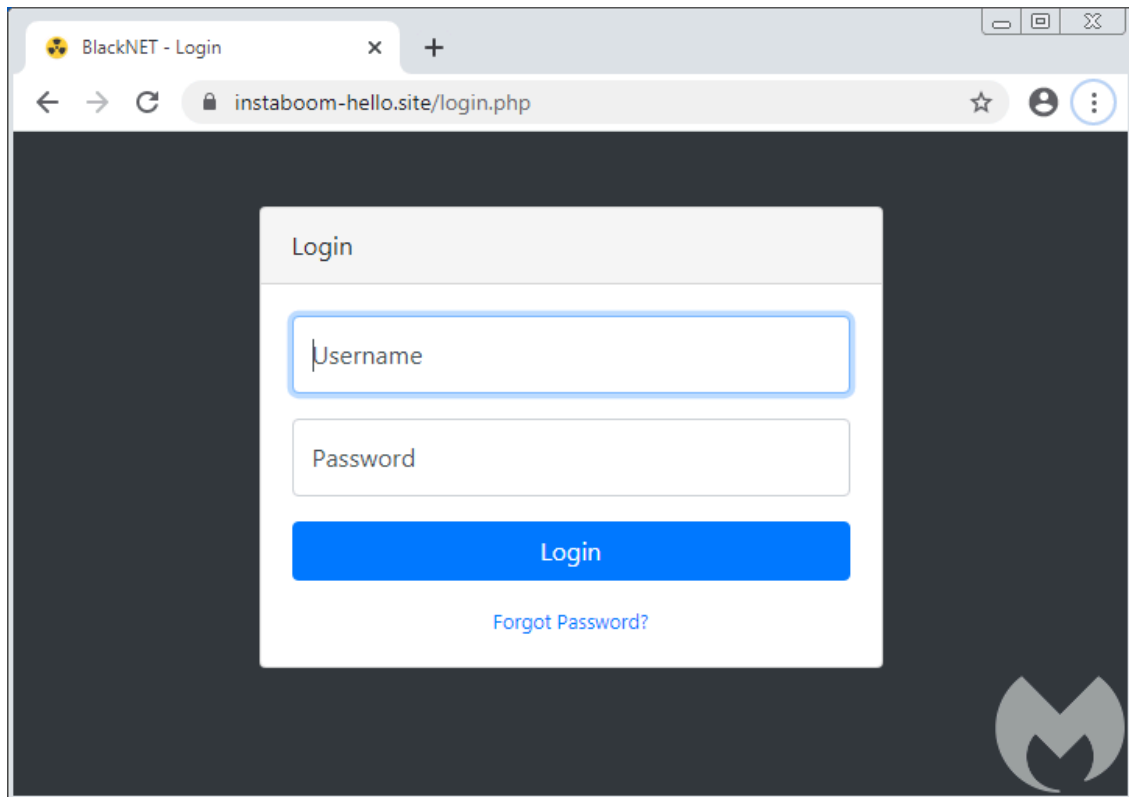


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features the Malwarebytes logo and 'Premium' text in the top left, and a close button (X) in the top right. A green checkmark icon is followed by the text 'Malware blocked by Real-Time Protection'. Below this, it states 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

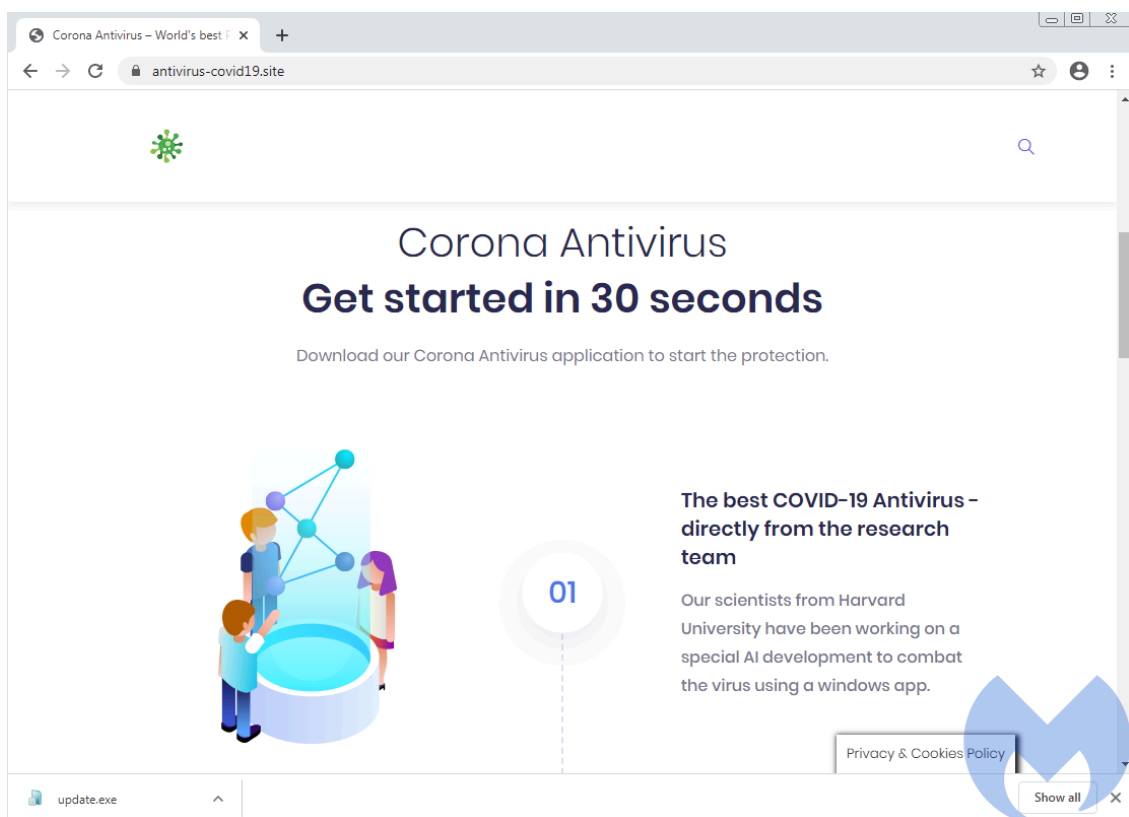
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

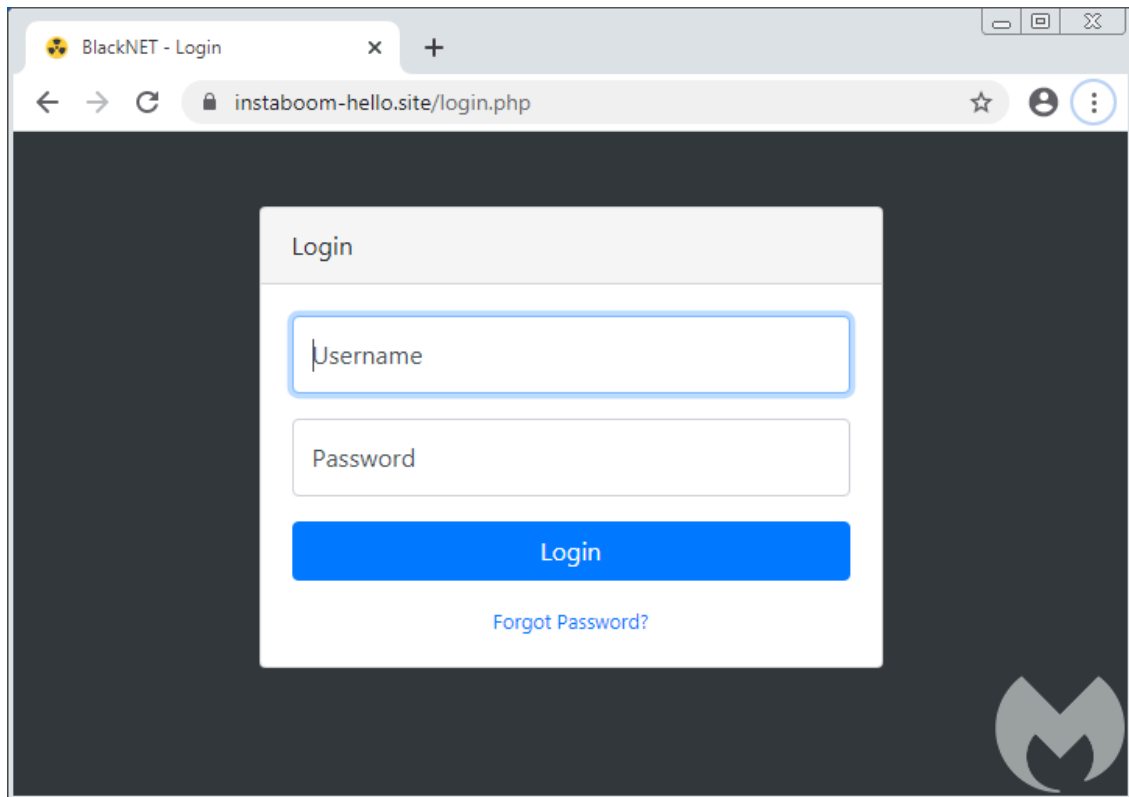


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

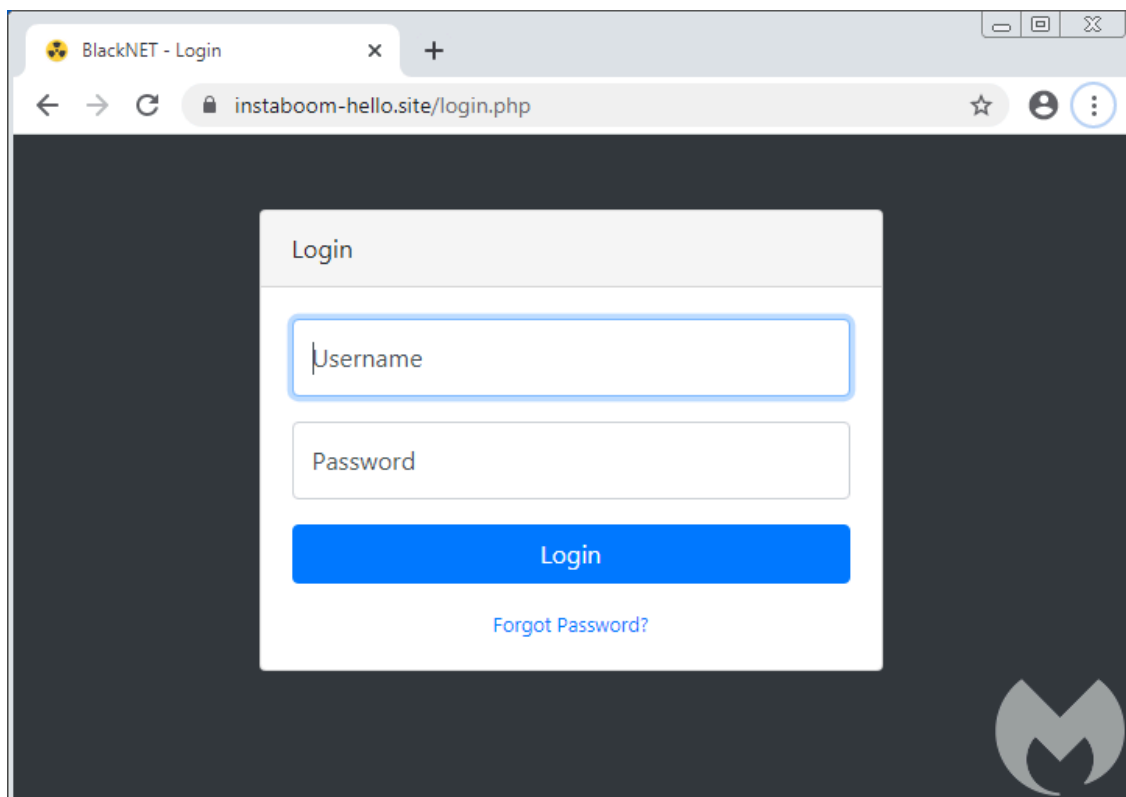
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

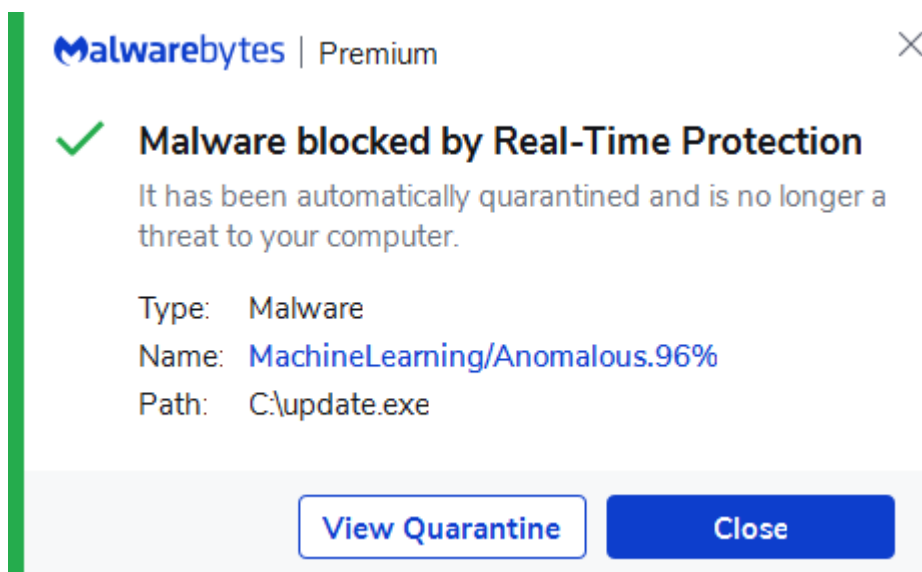
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

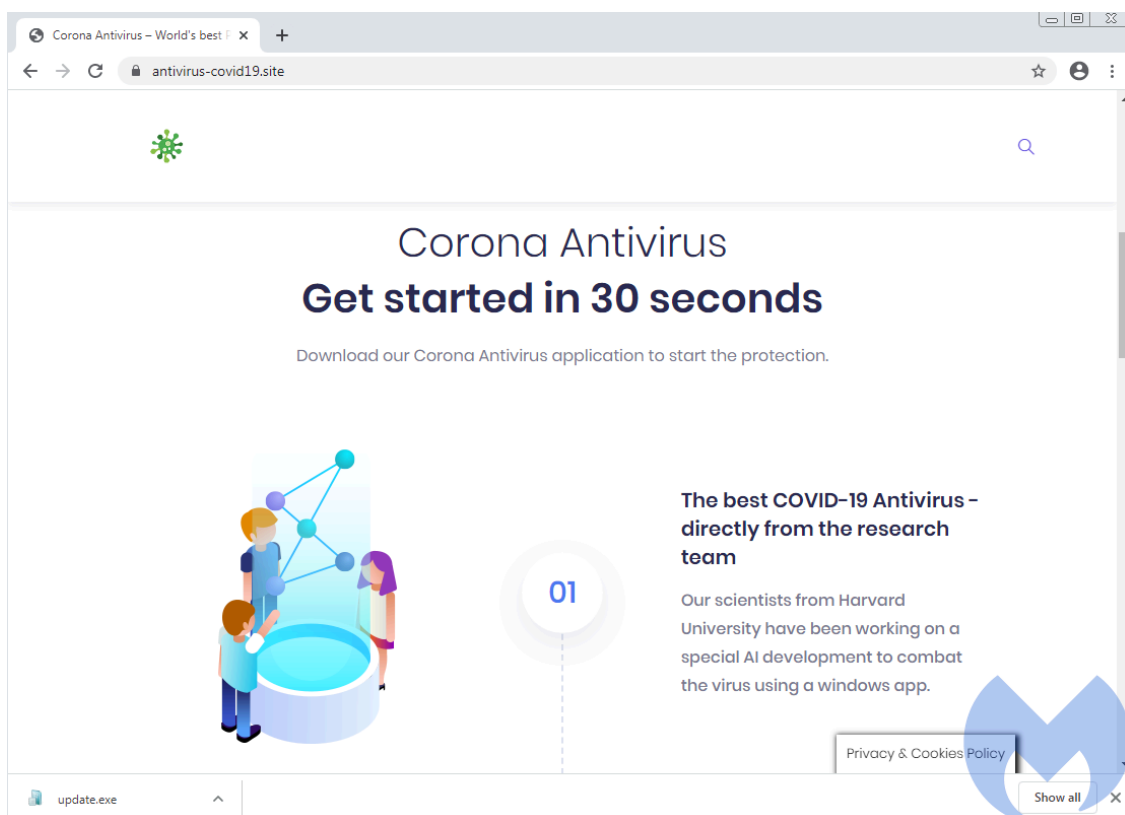
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

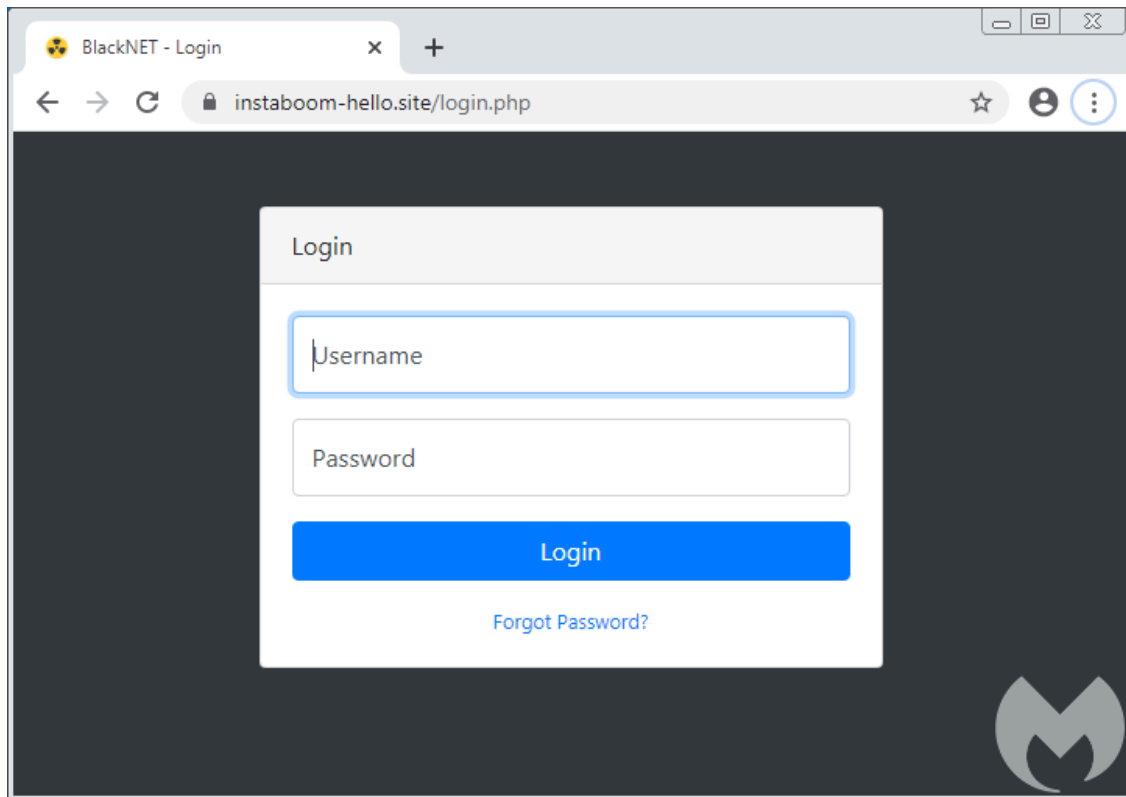


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

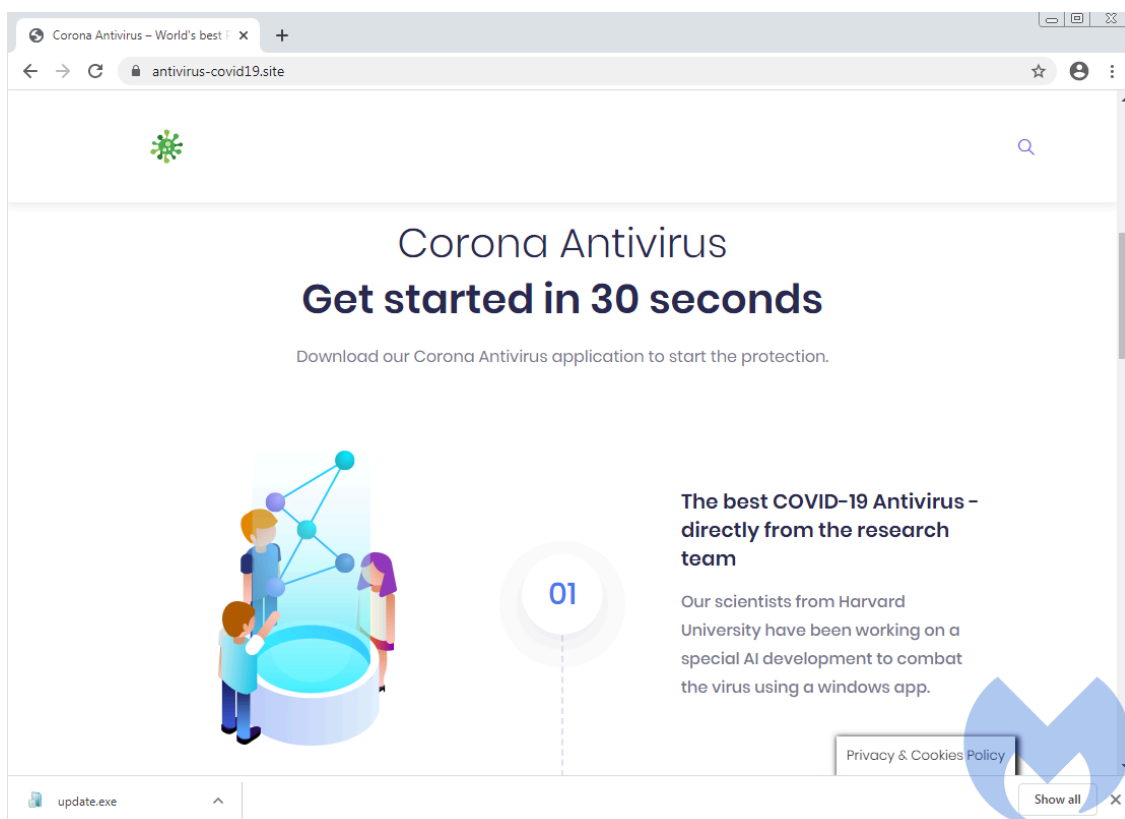
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

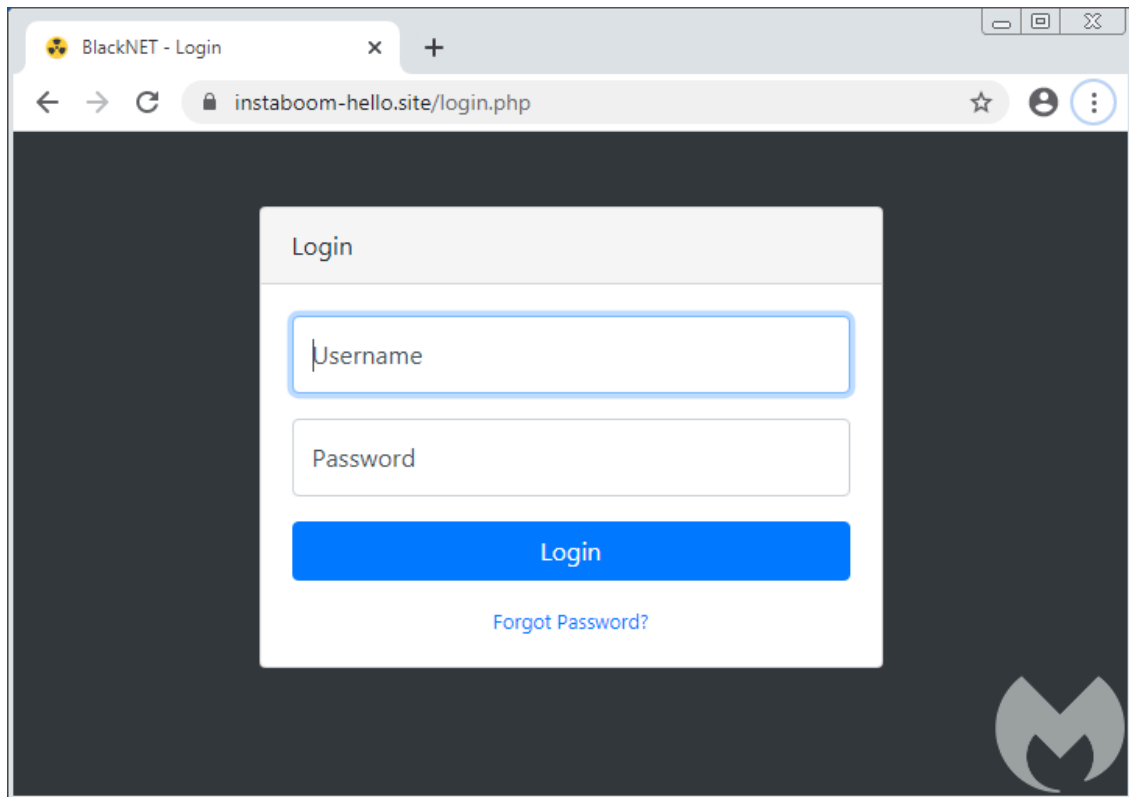


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

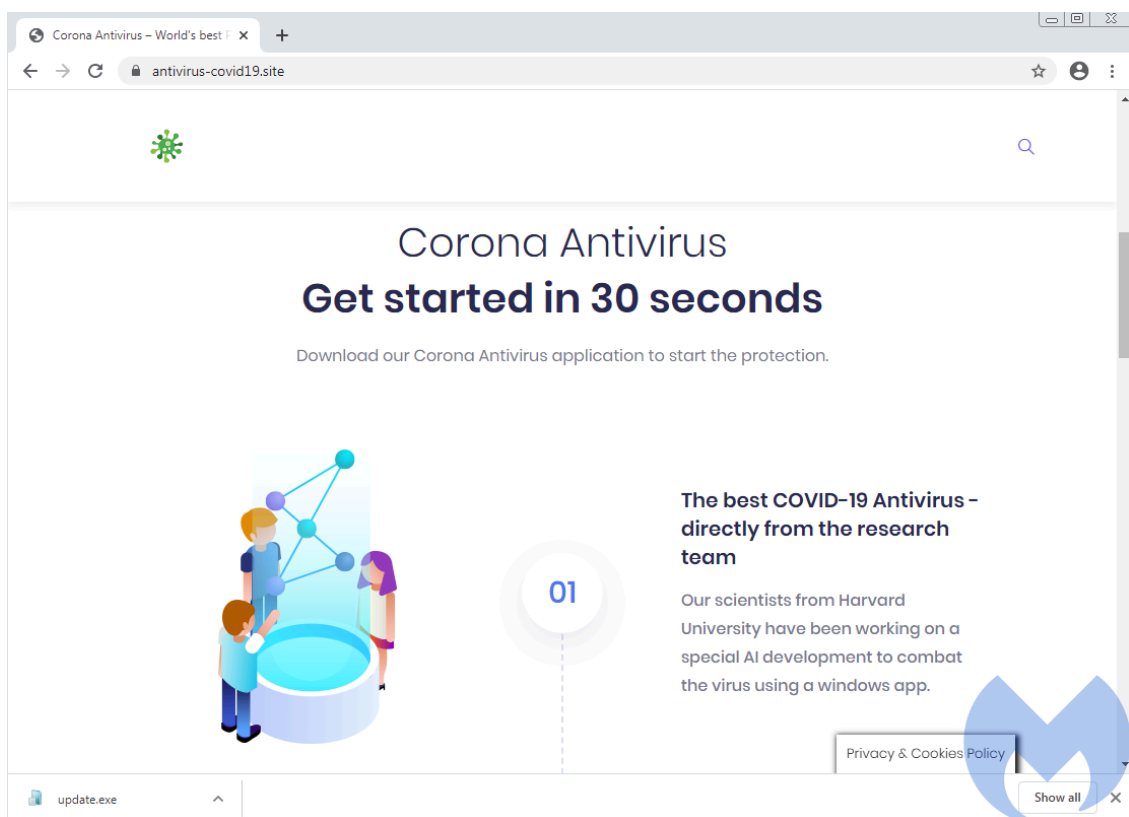
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

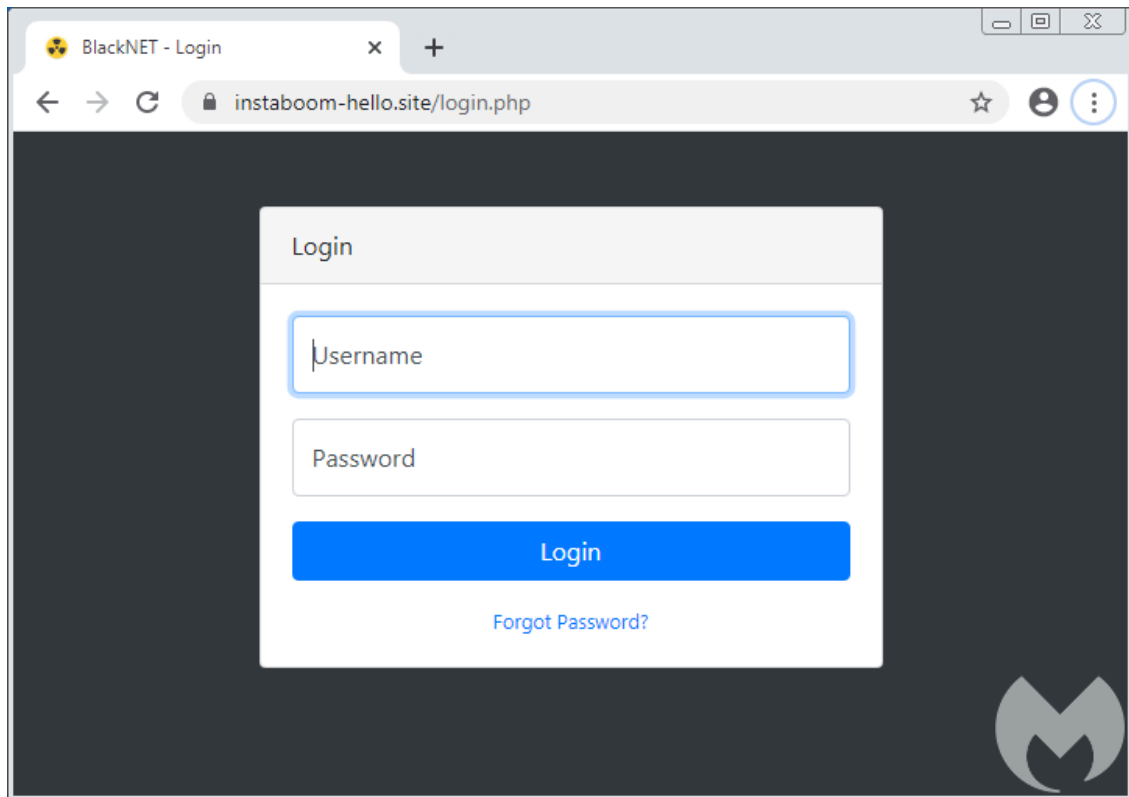


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

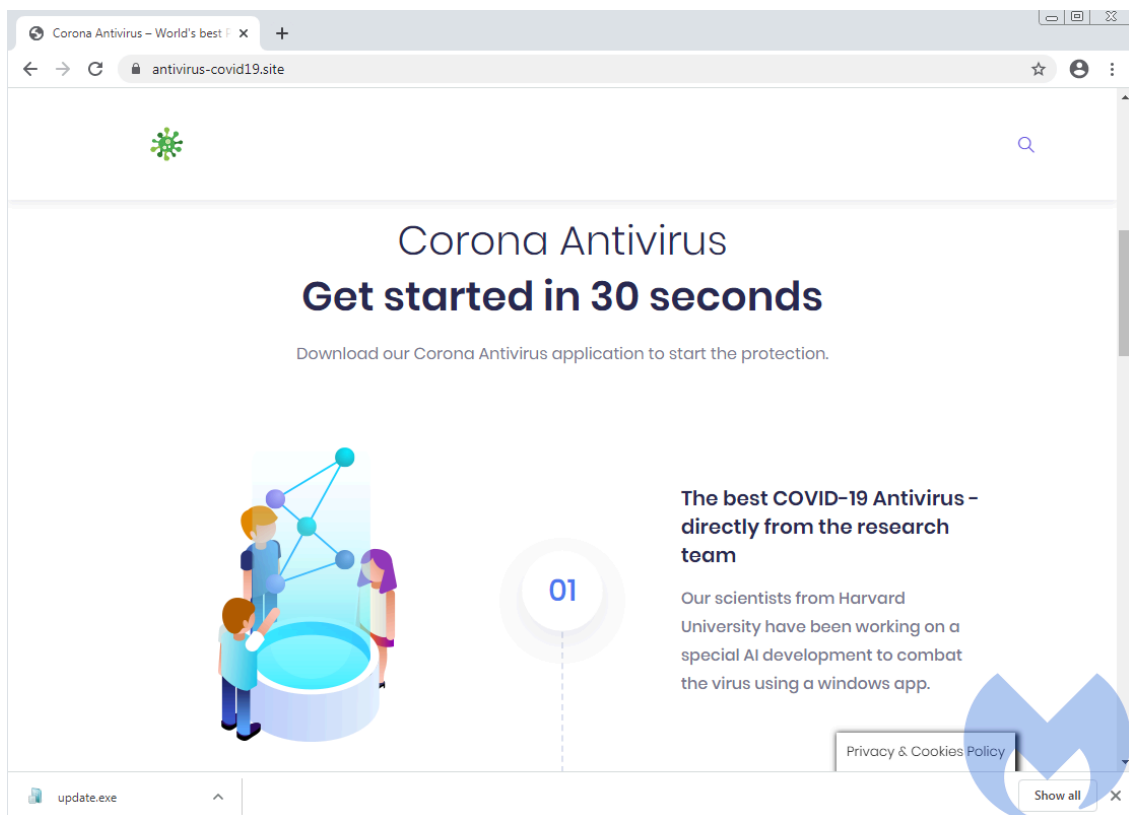
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

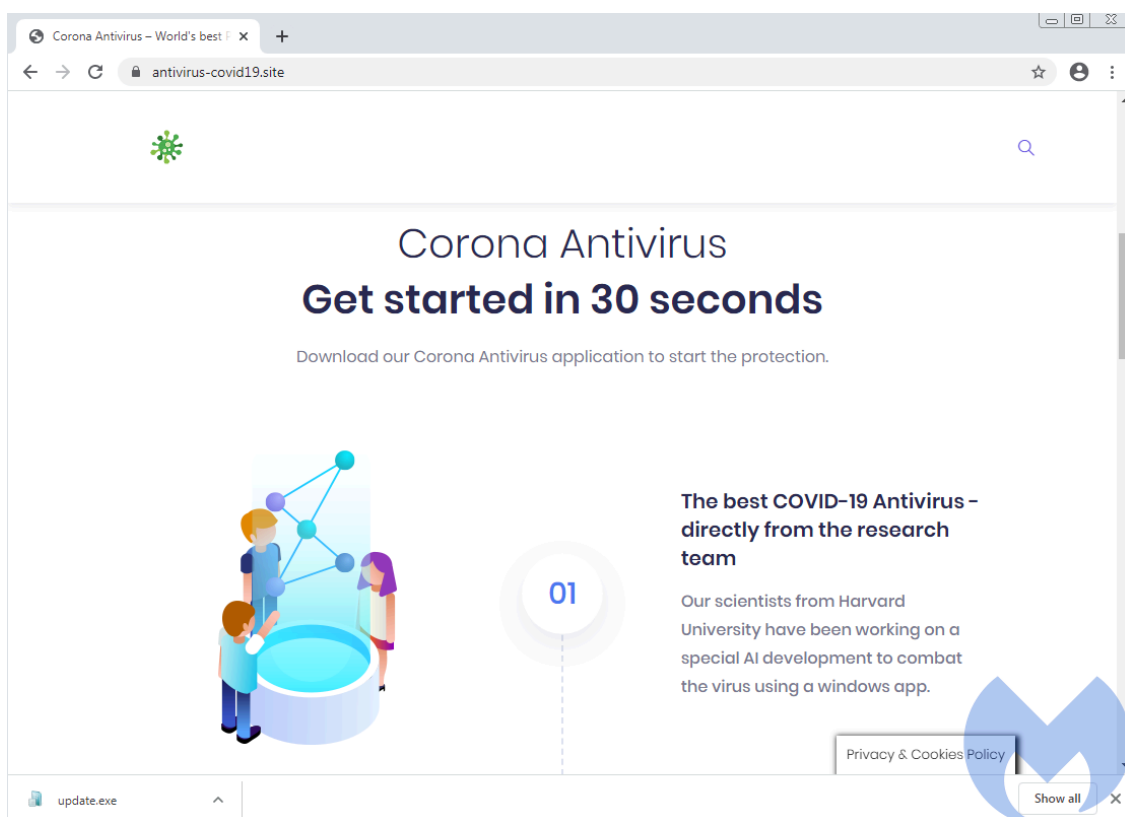
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

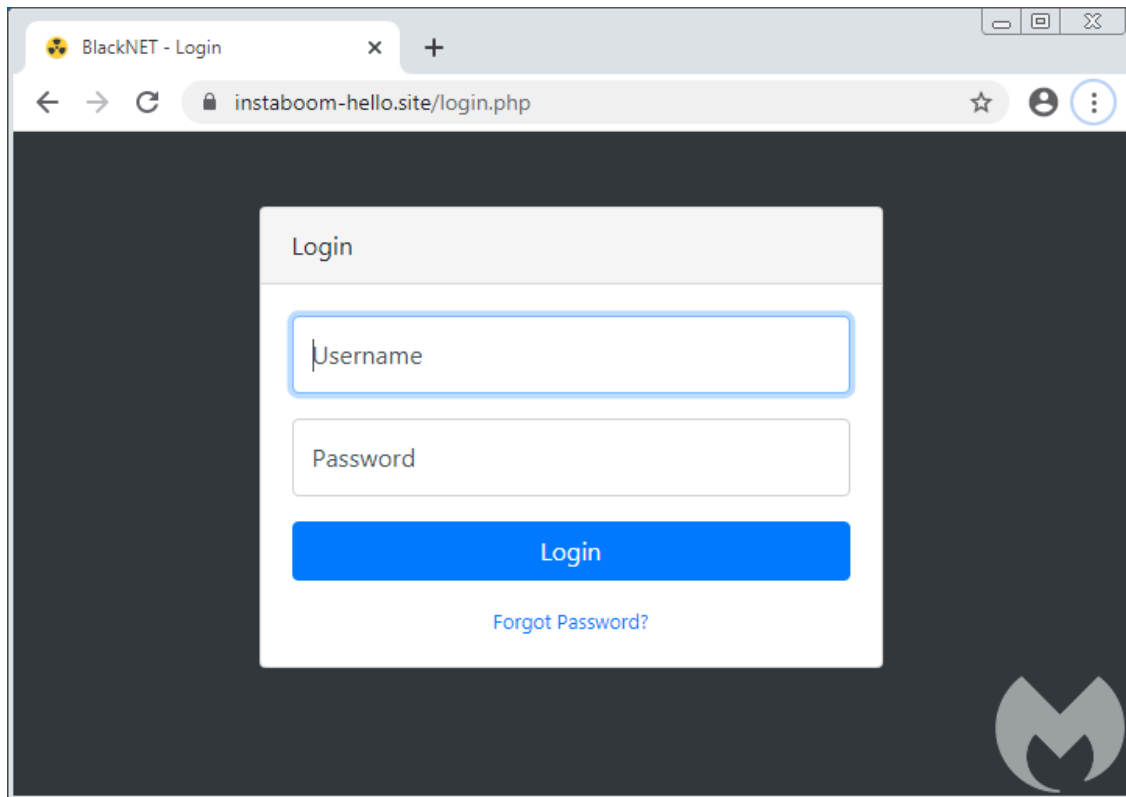


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue dot indicating a client location. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, it lists the details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

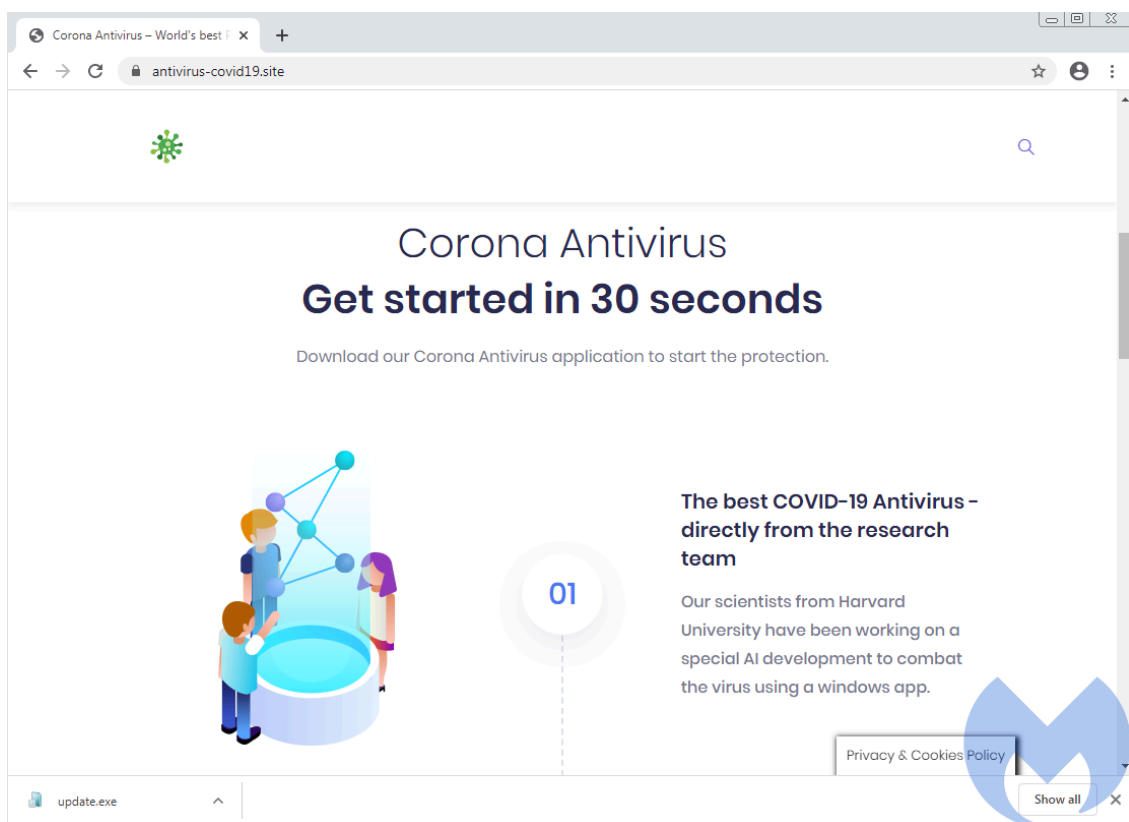
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

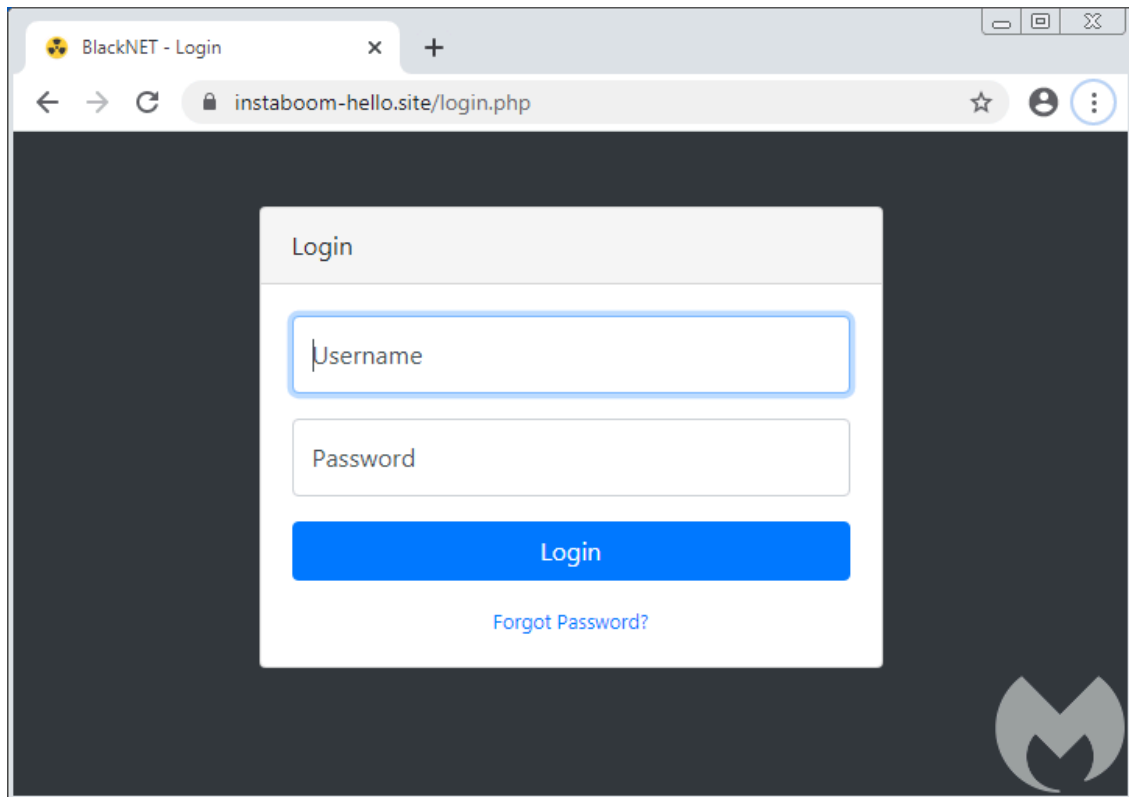


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

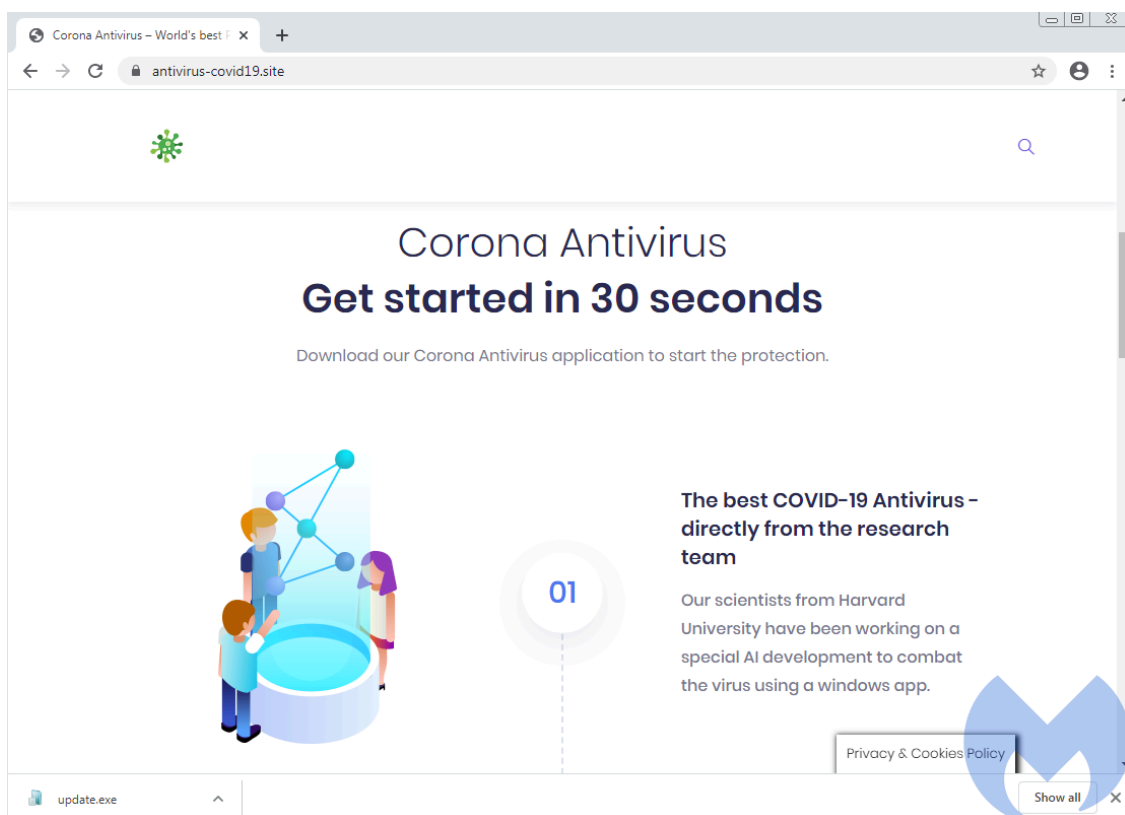
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

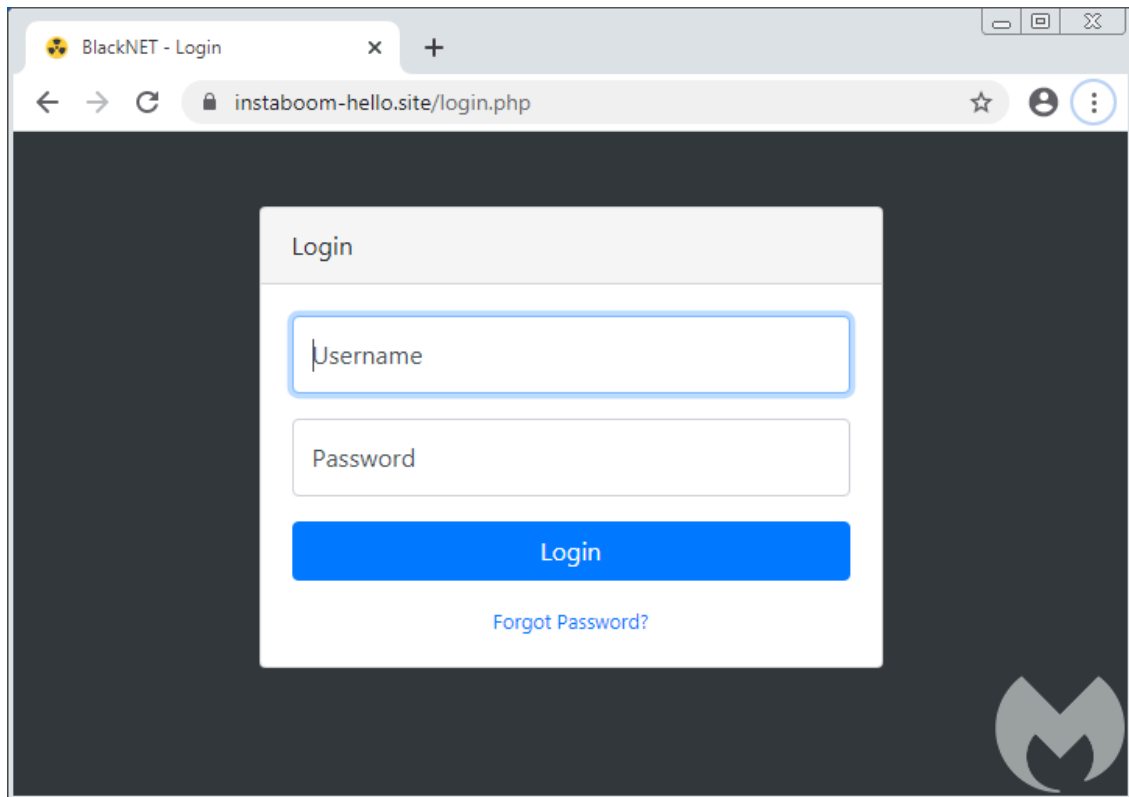


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

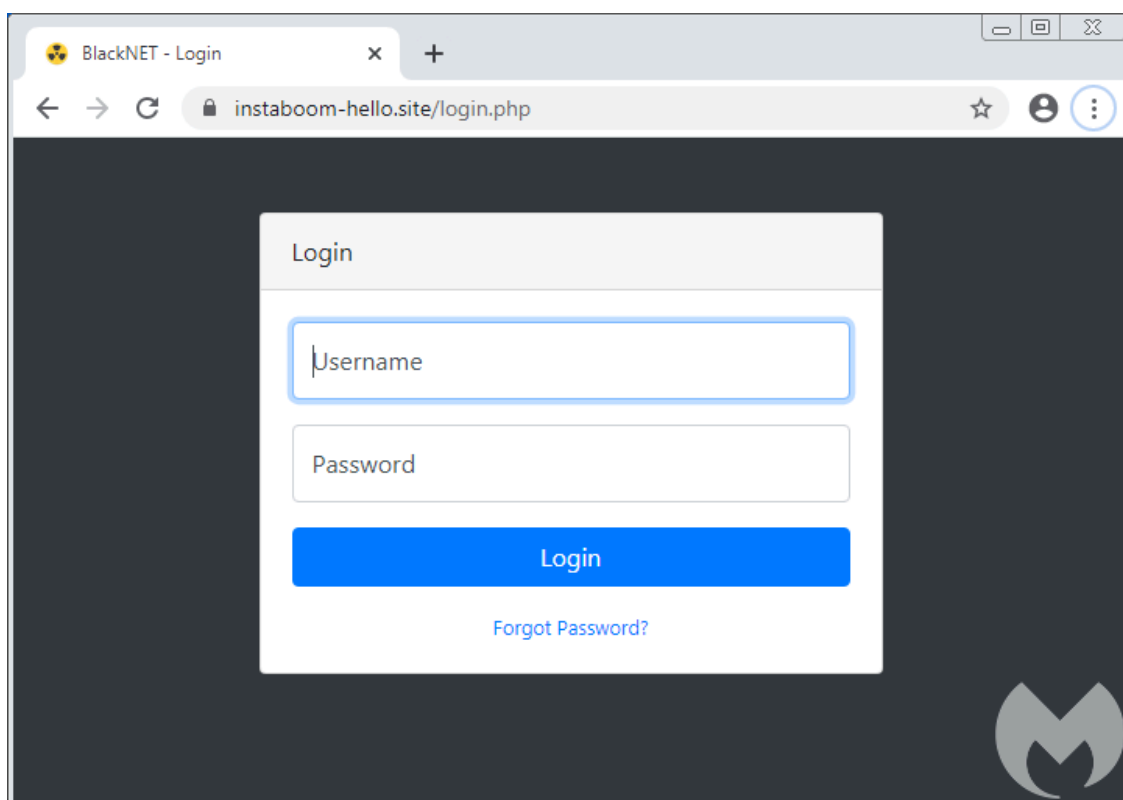
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

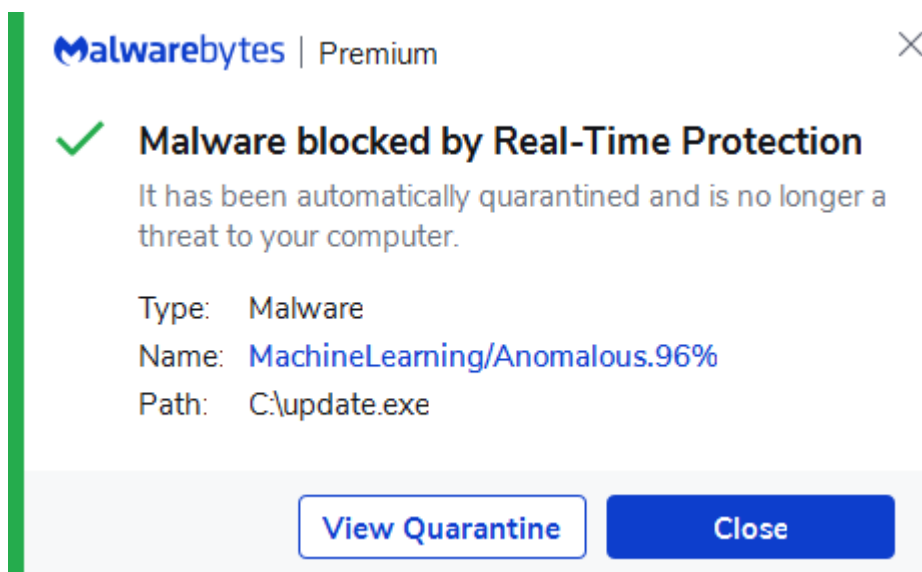
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

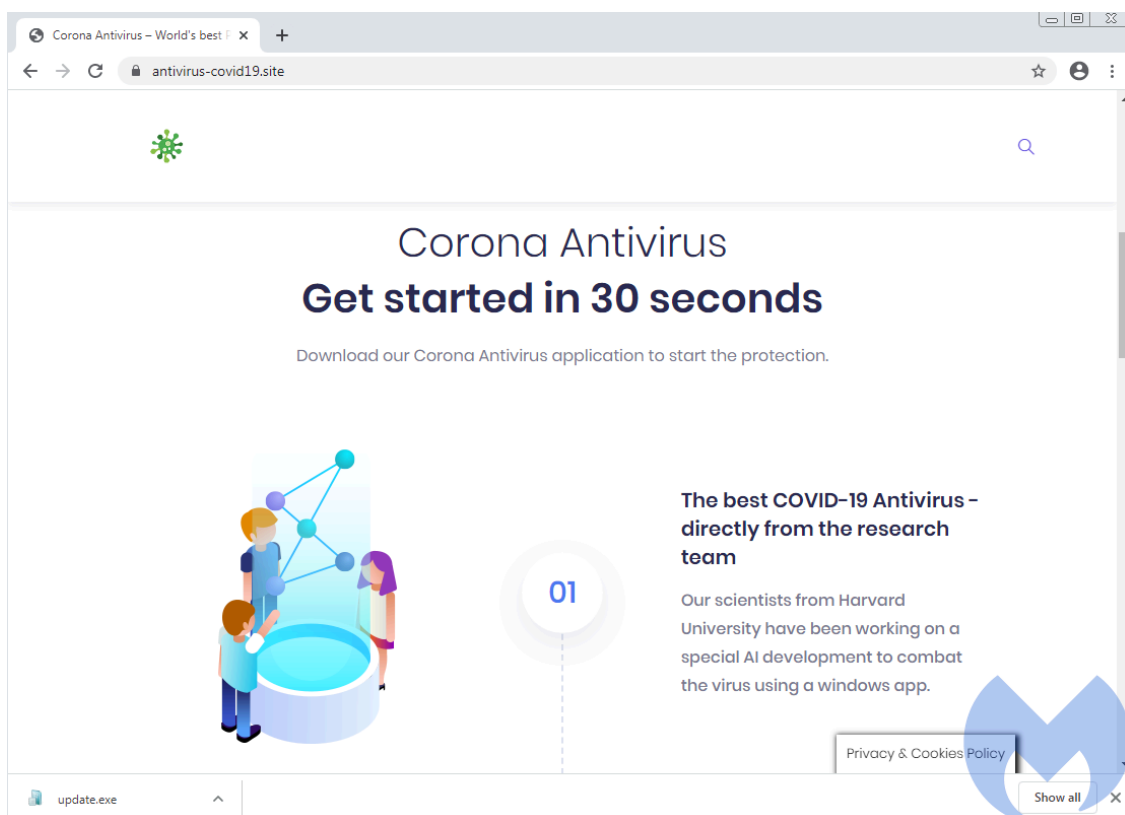
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

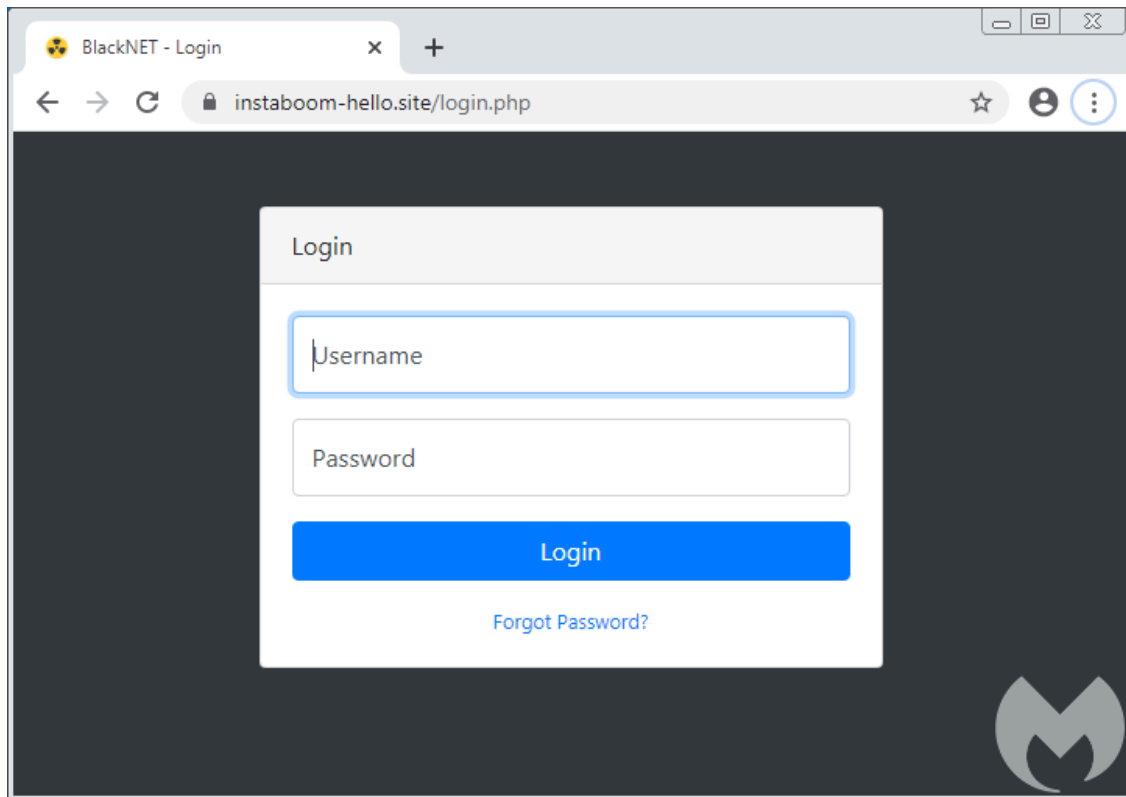


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

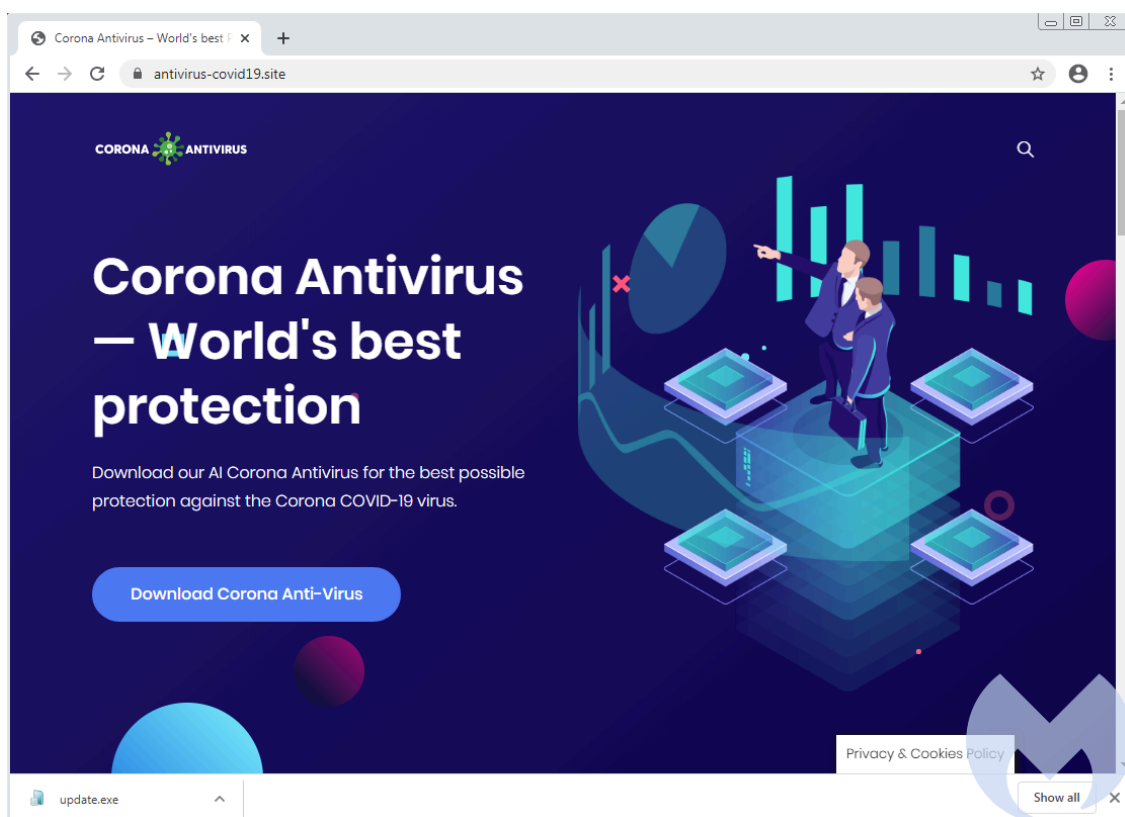
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

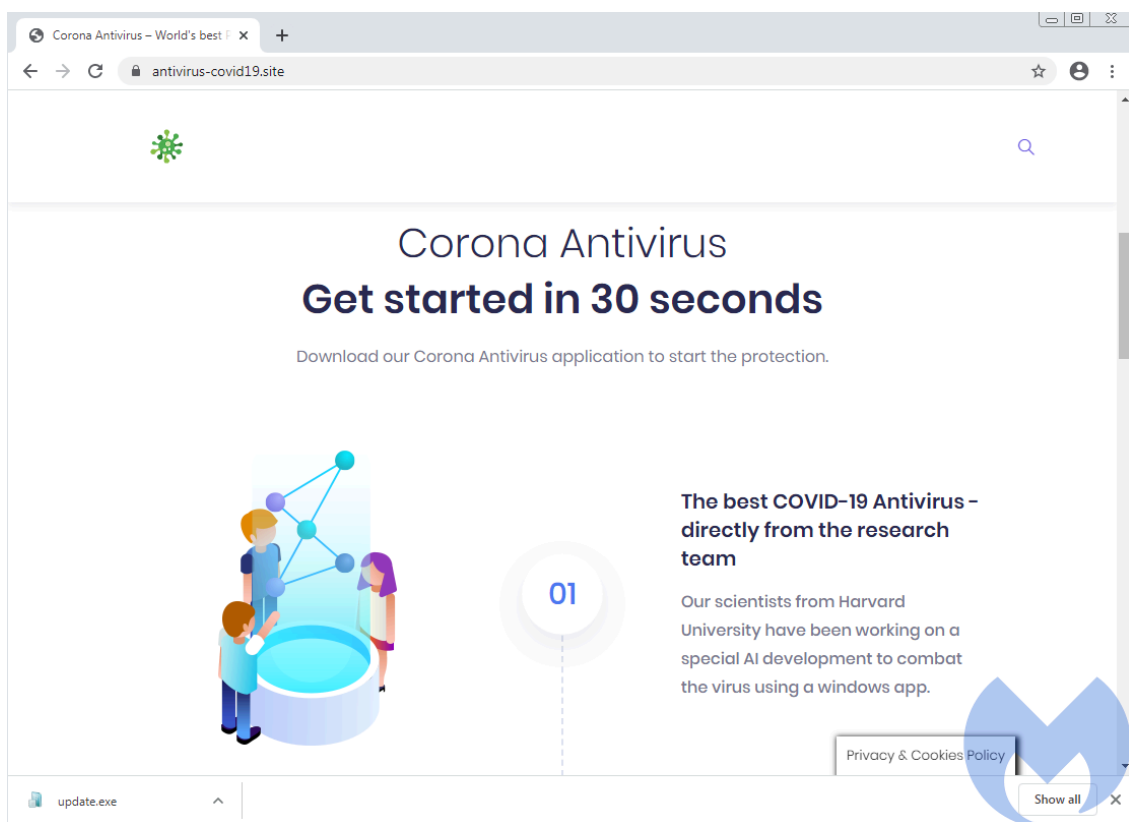
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

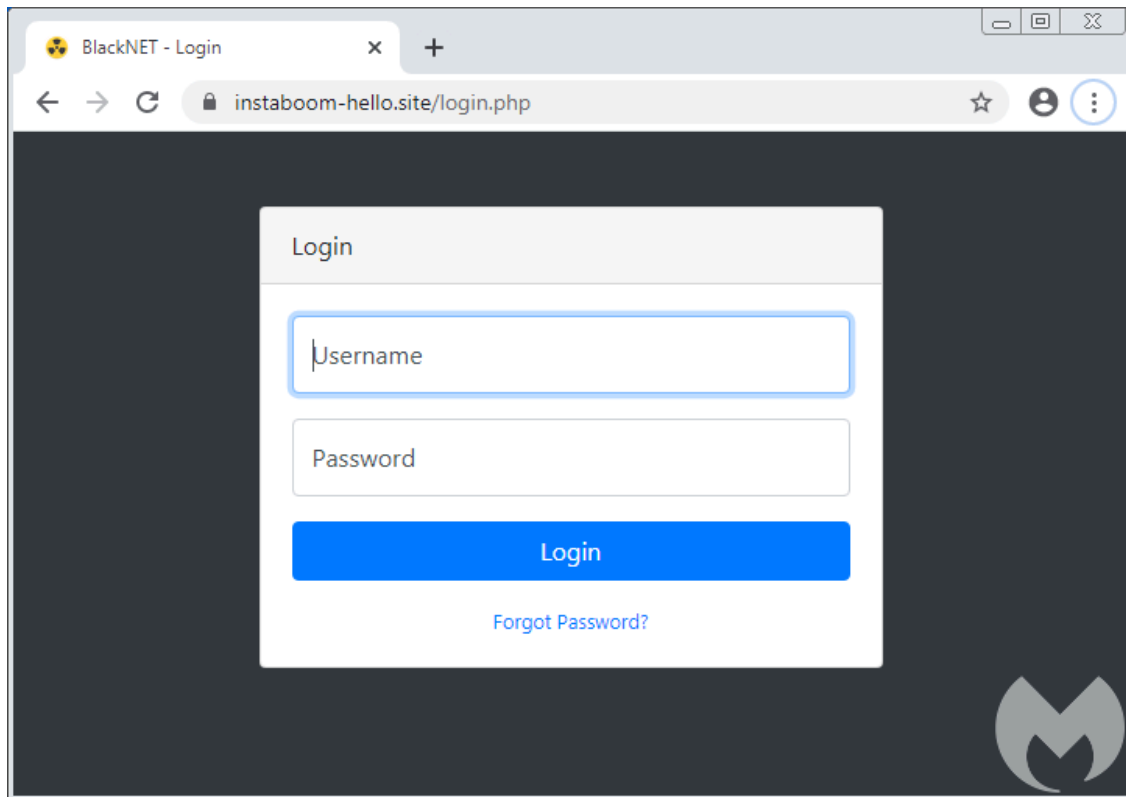


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[:]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[:]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a table showing columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the right of the table is a 'Map Visualization' showing a world map with blue markers. At the bottom left, there's a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

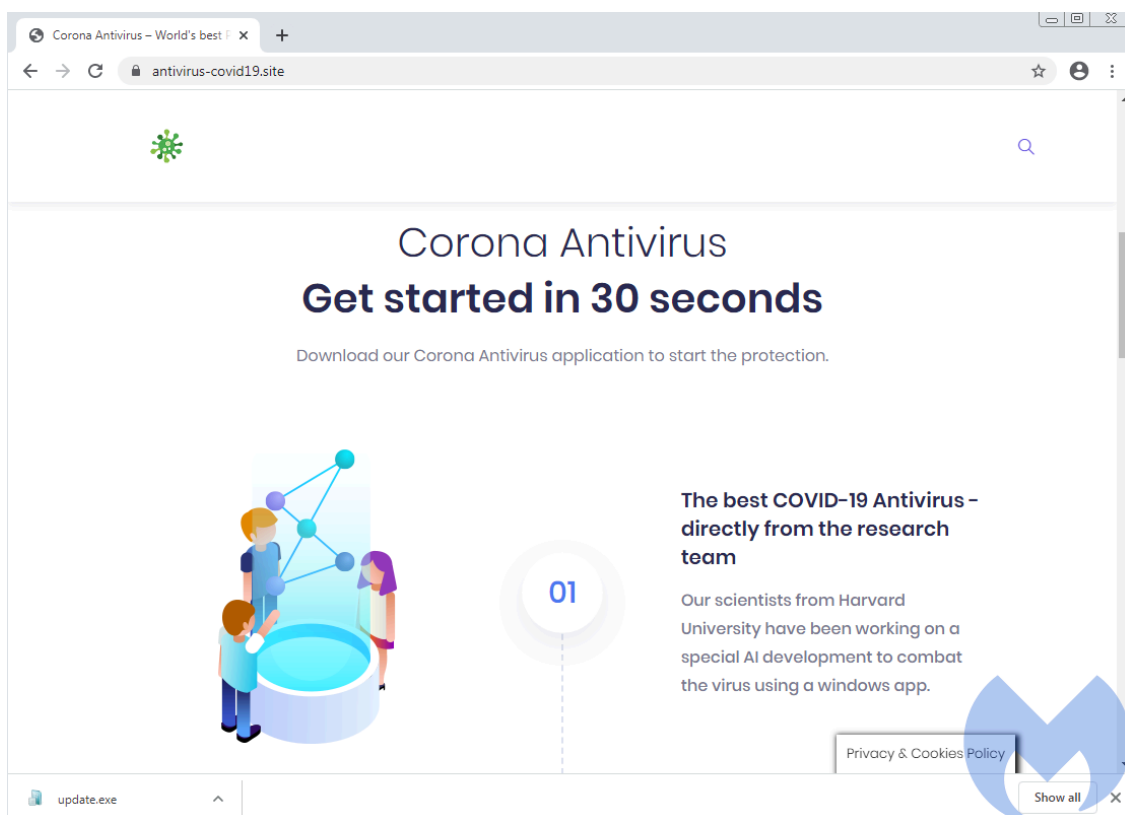
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

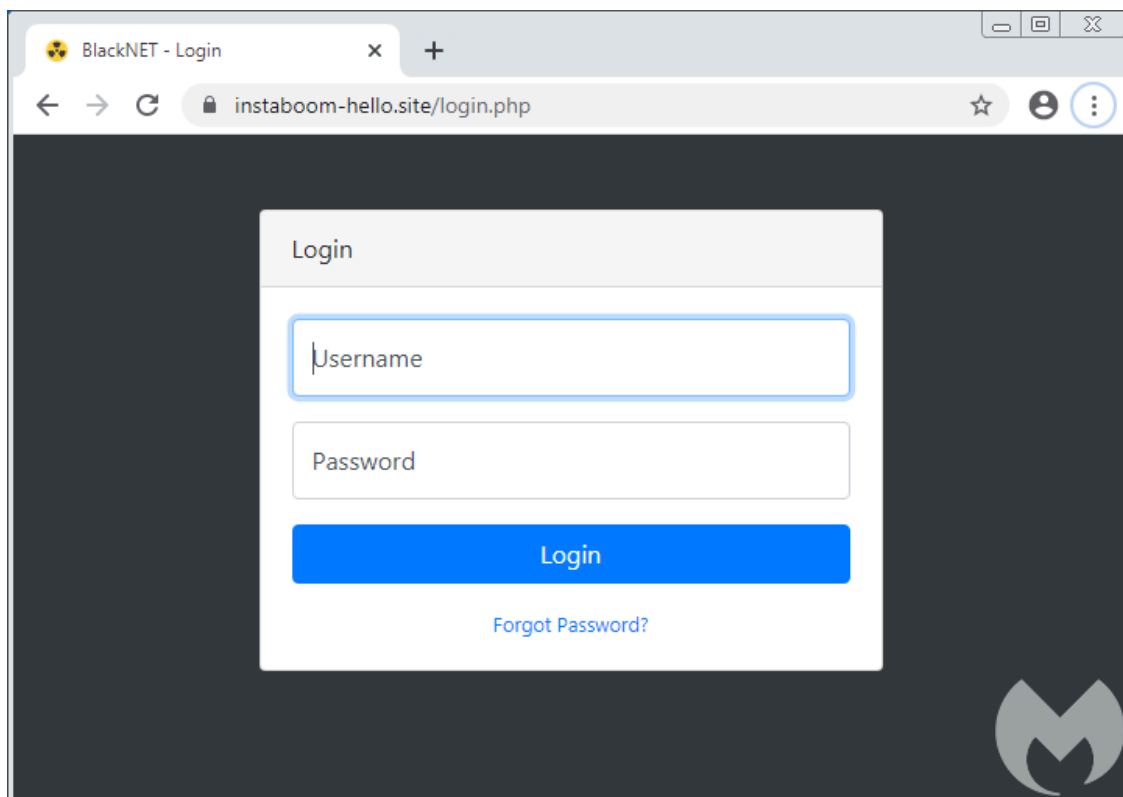
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

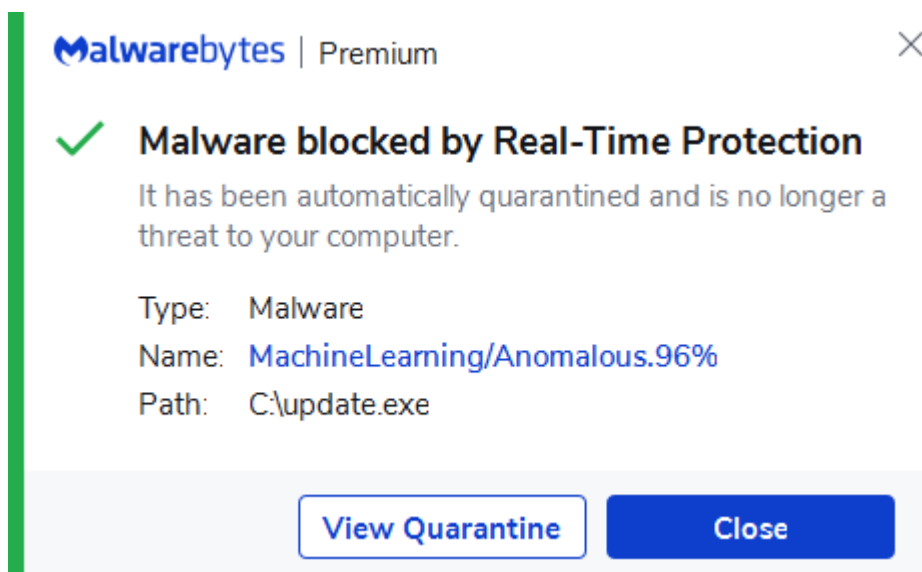
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

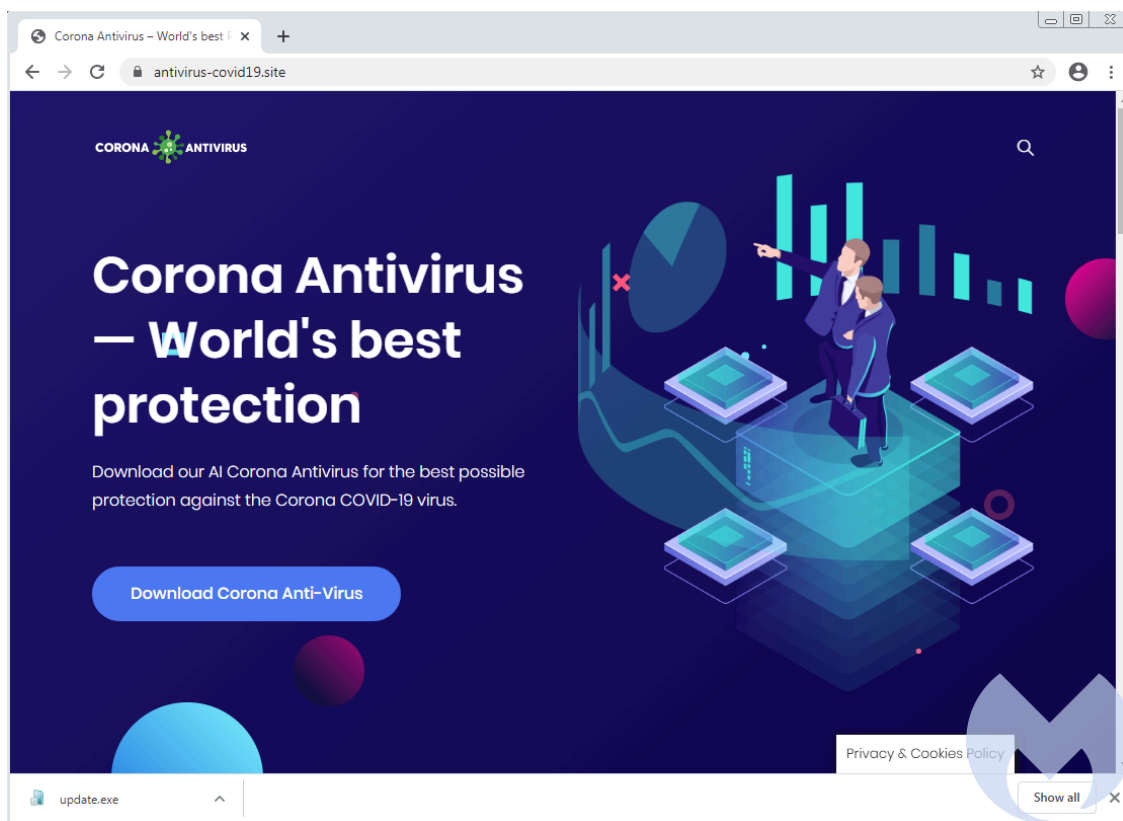
```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

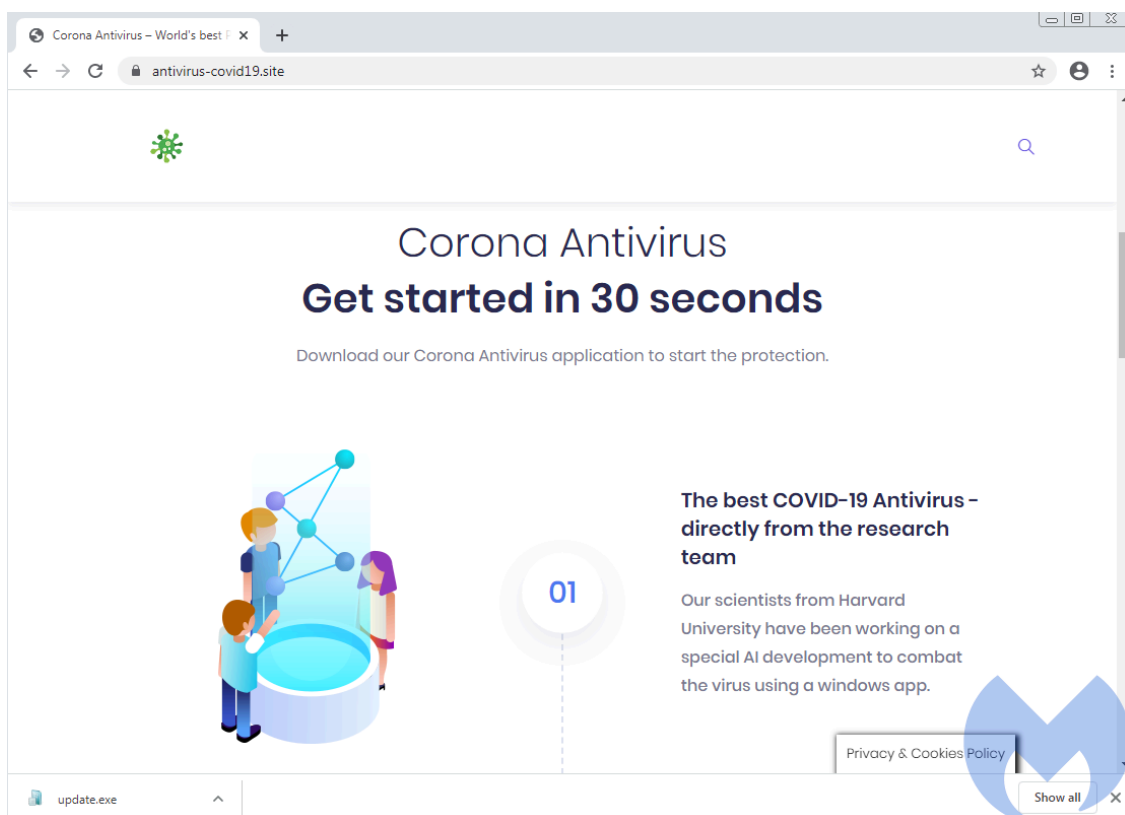
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

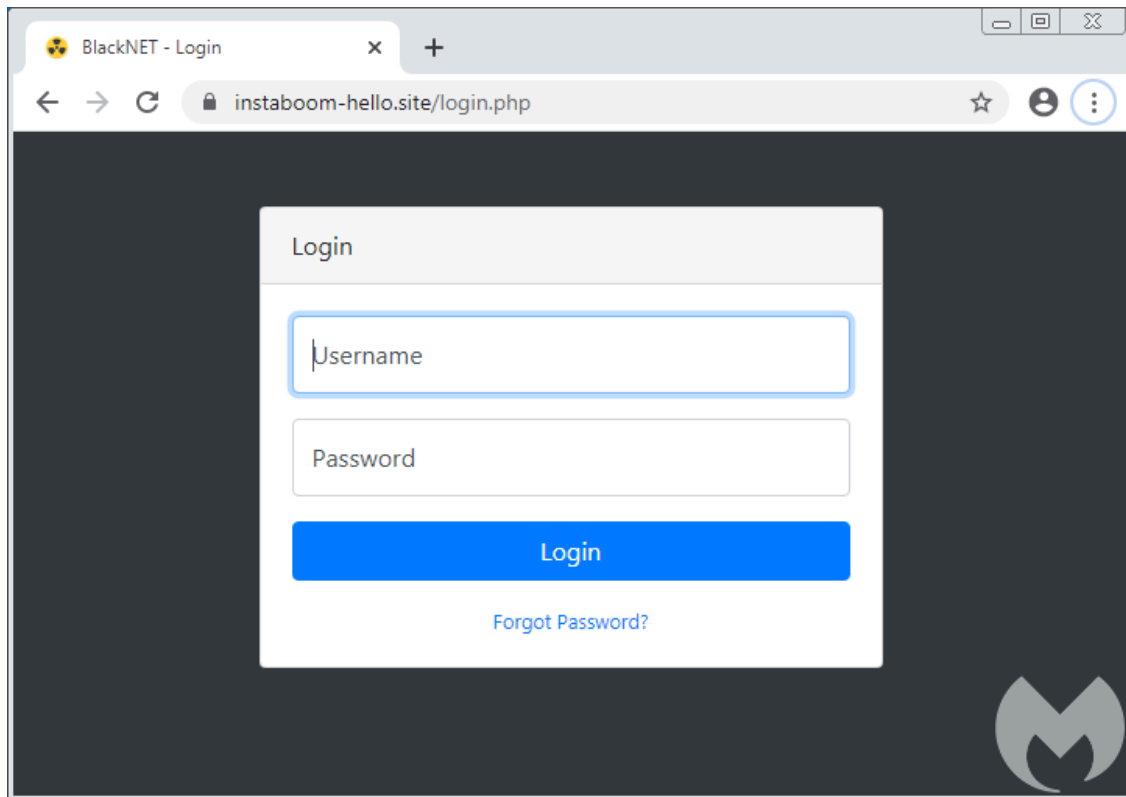


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. Further right is a 'Map Visualization' section showing a world map with a few blue dots indicating client locations. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

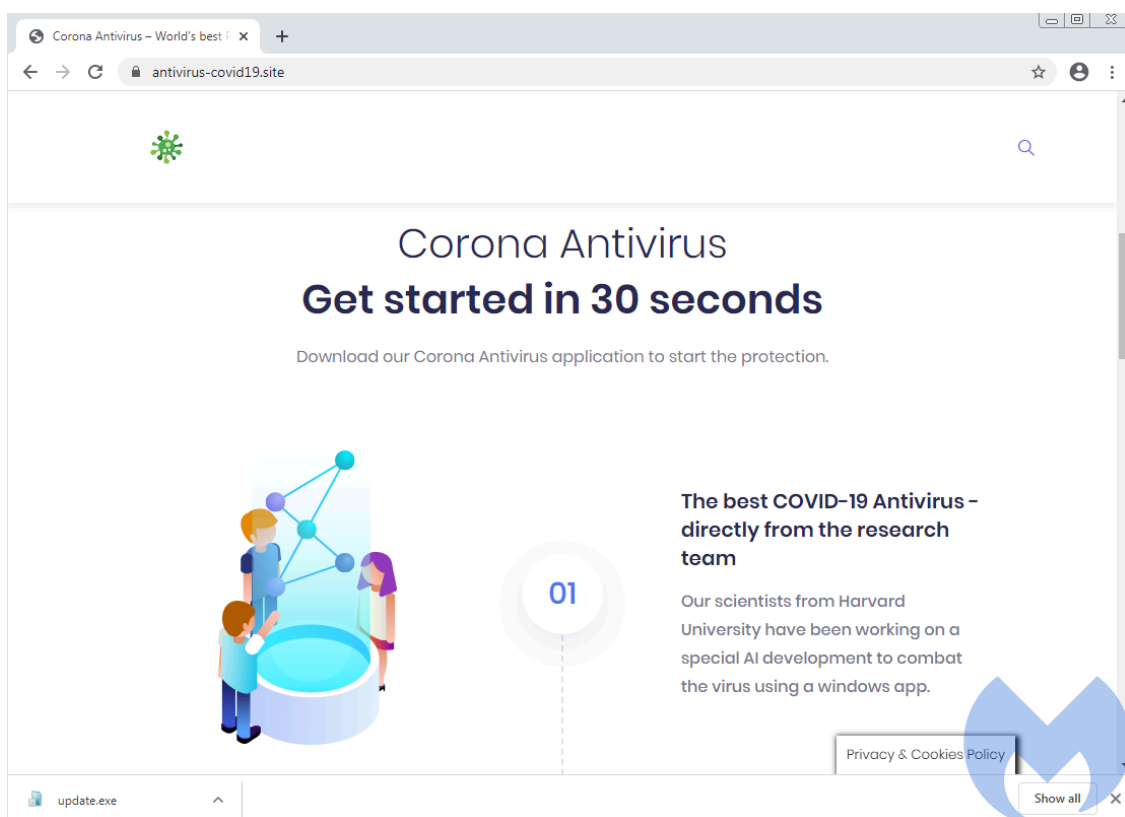
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

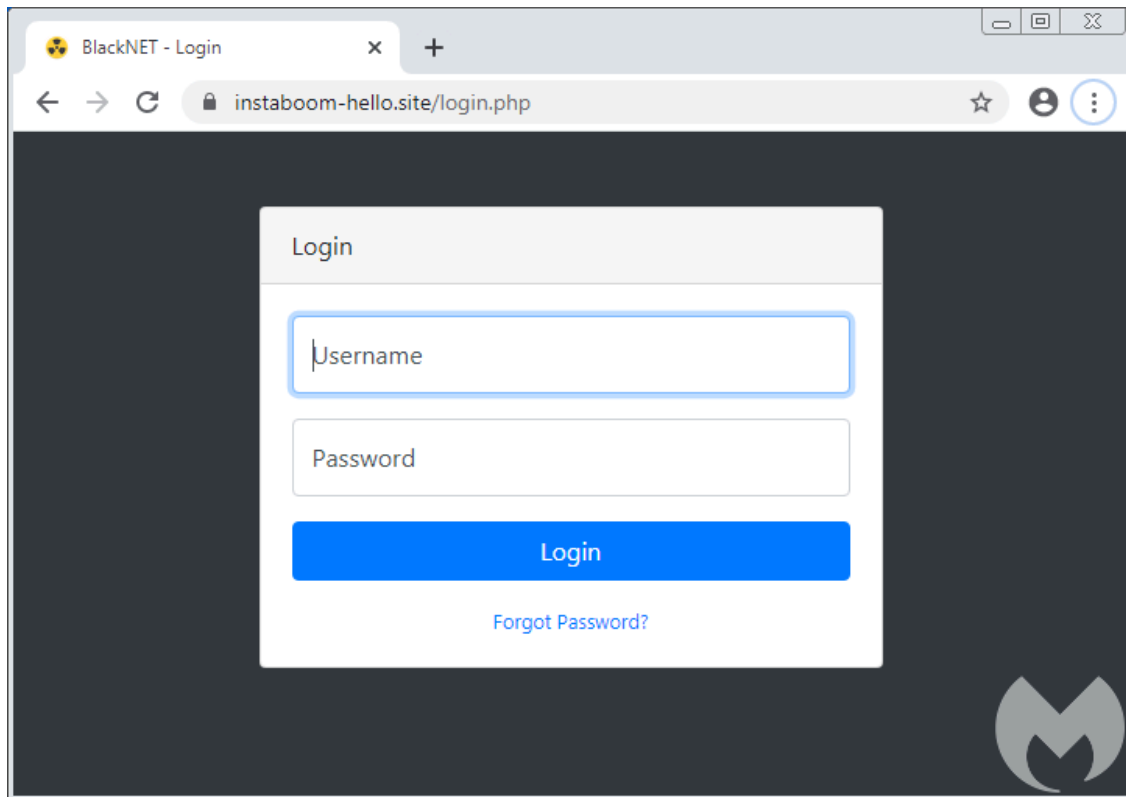


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

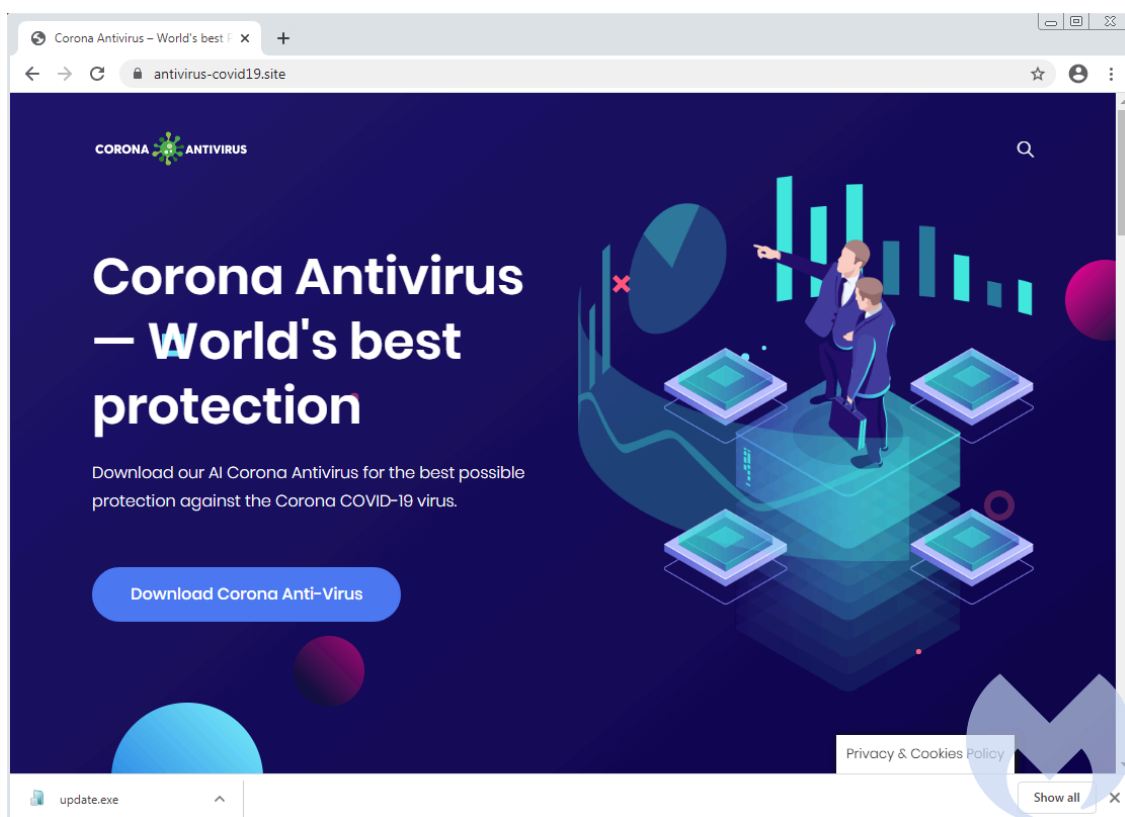
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

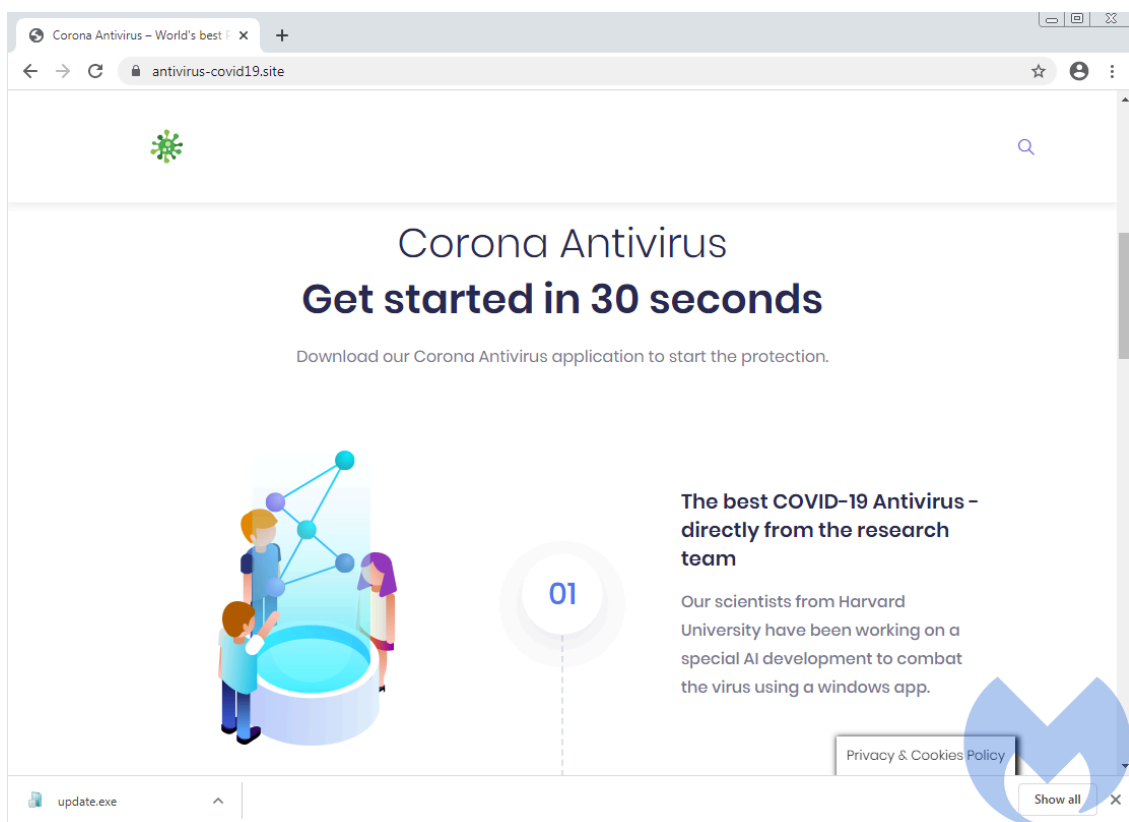
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

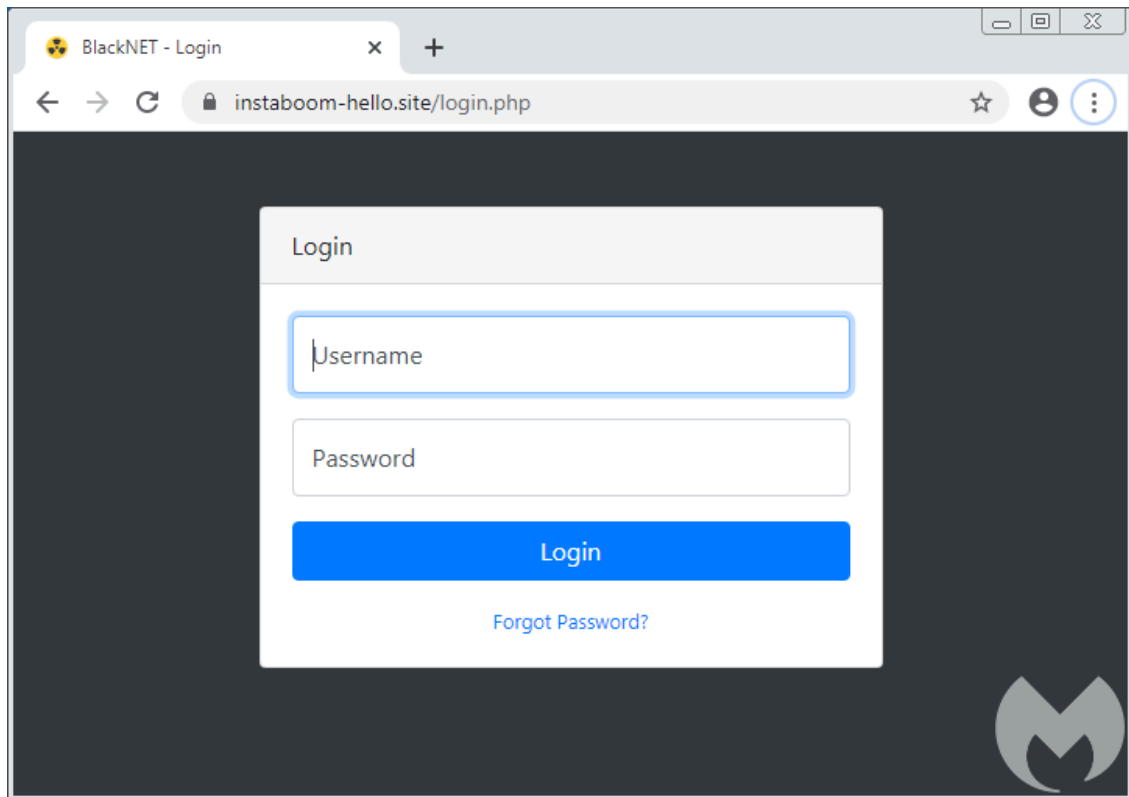


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

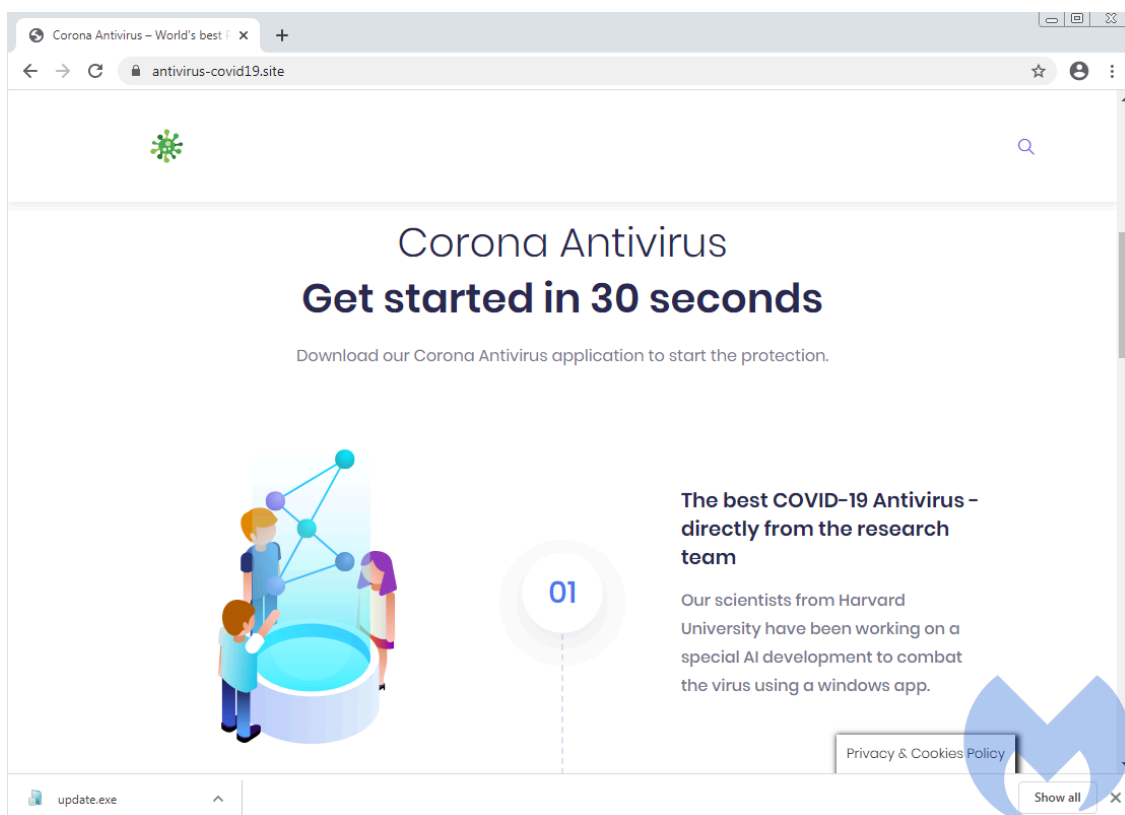
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

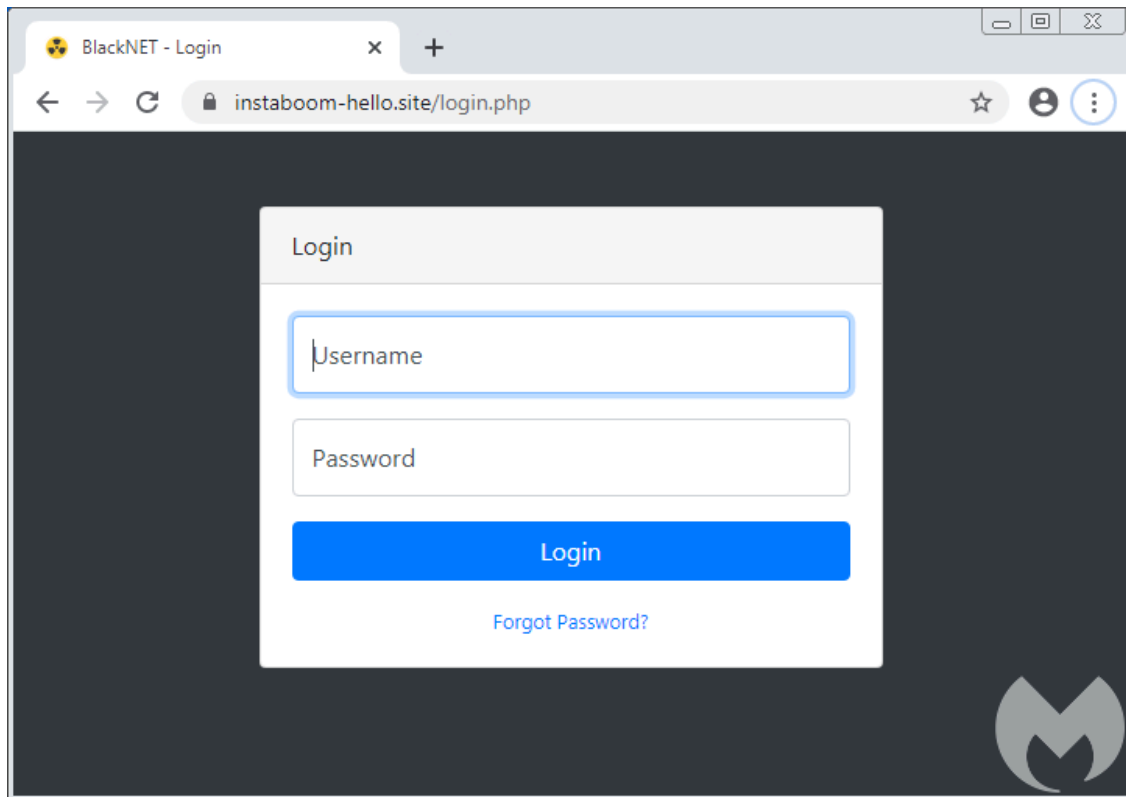


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a blue overlay. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

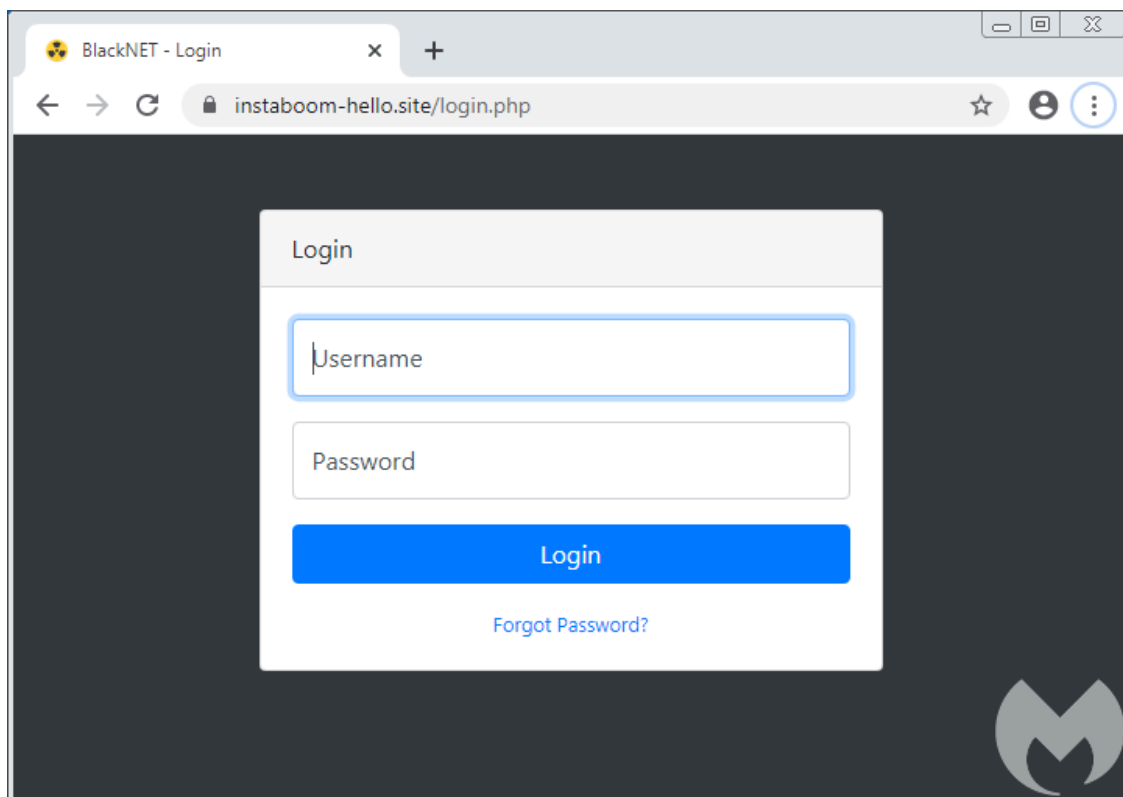
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET

Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

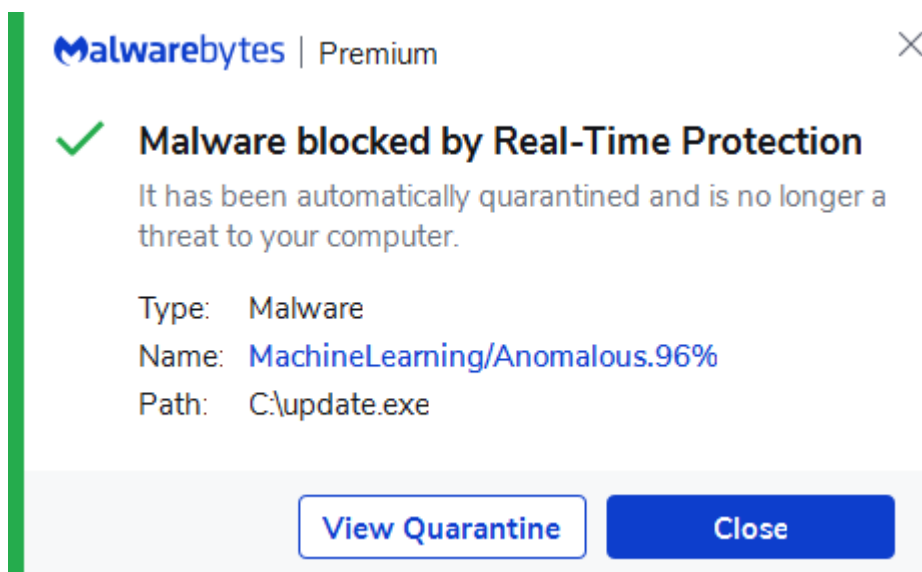
Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

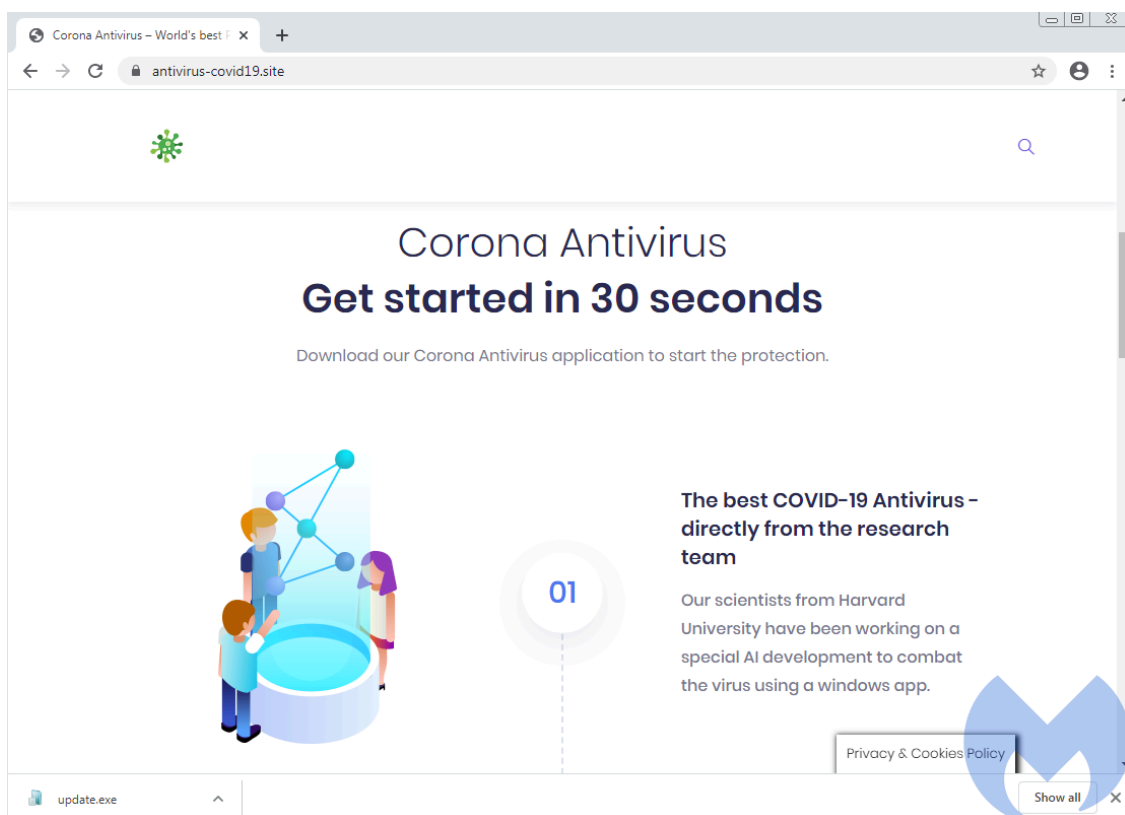
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

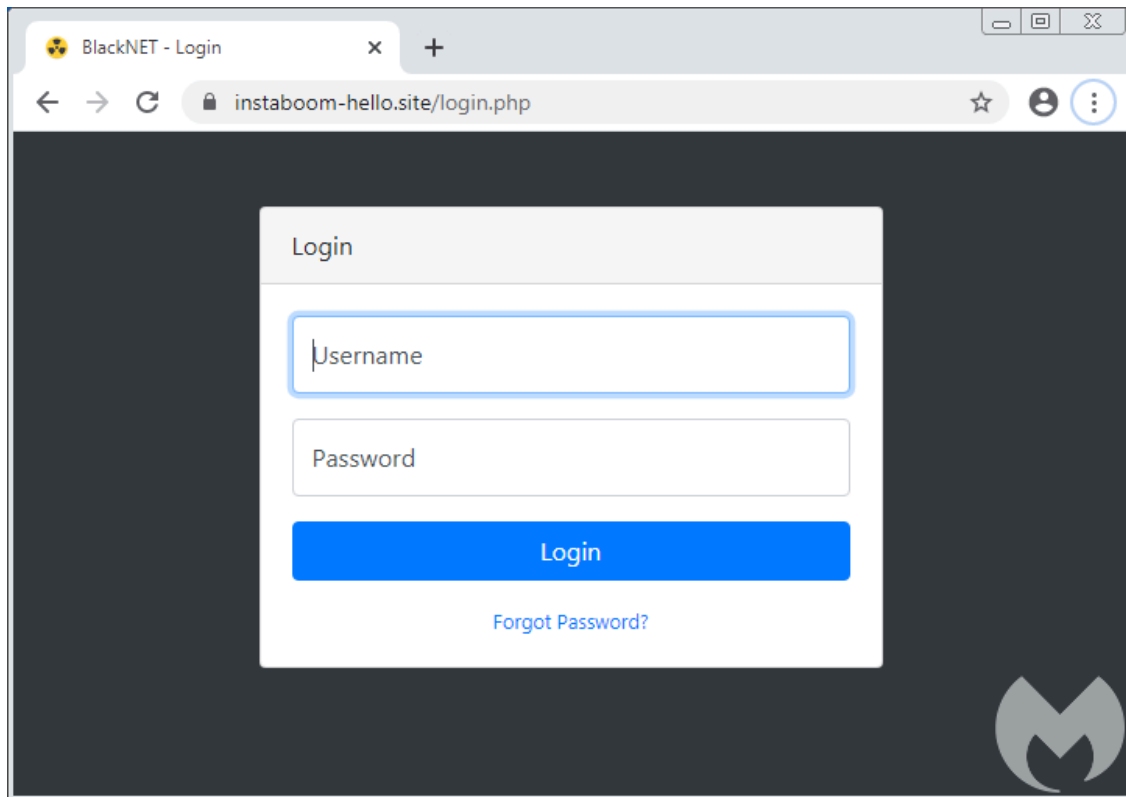


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

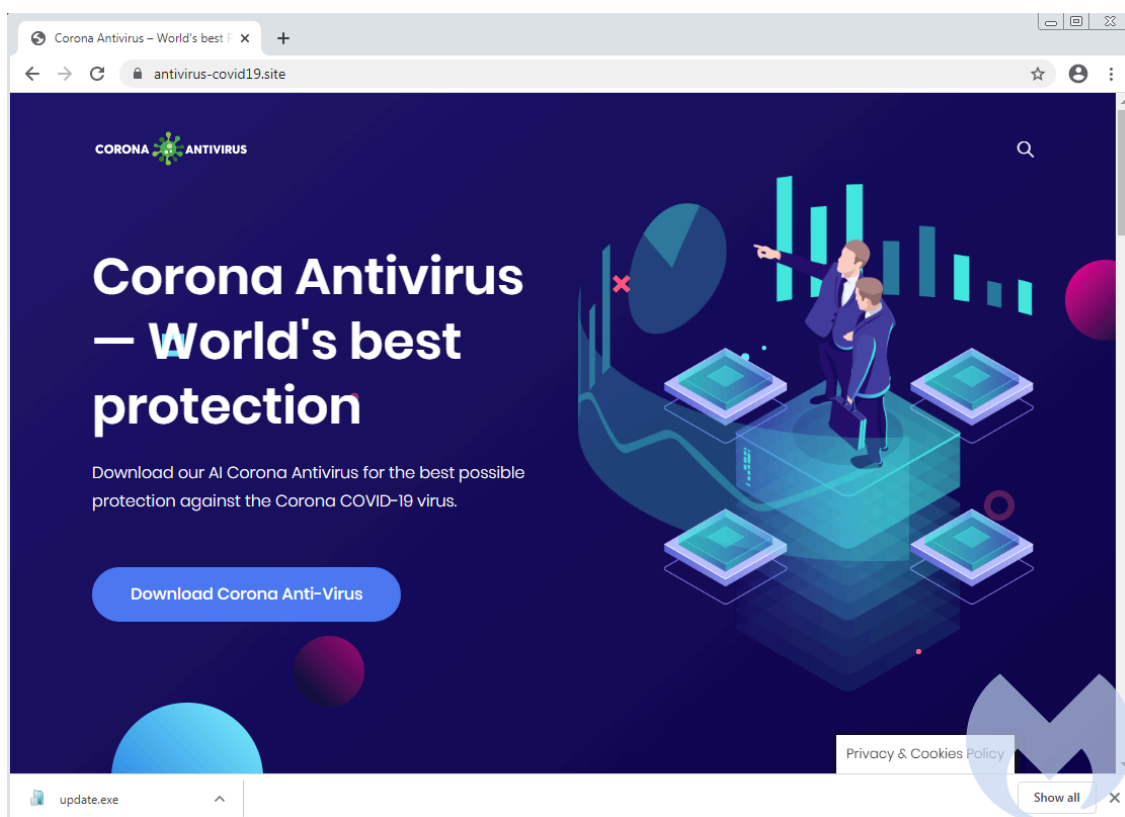
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

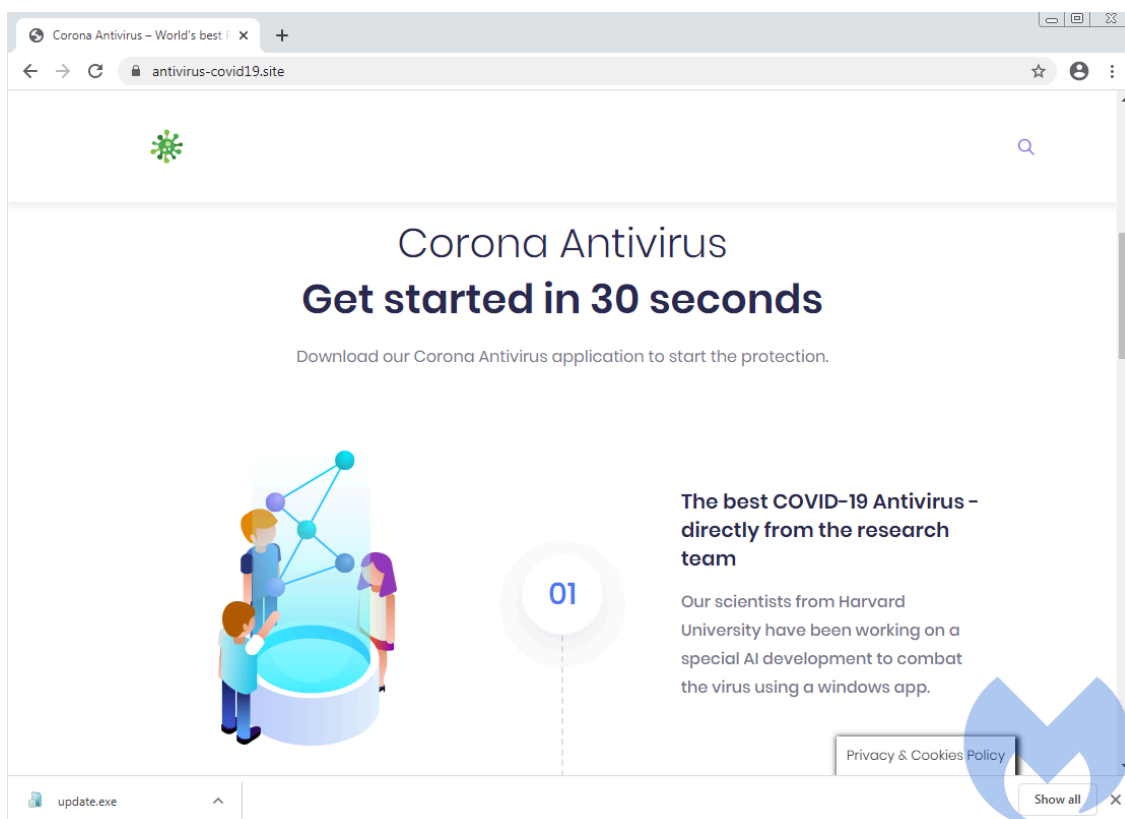
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

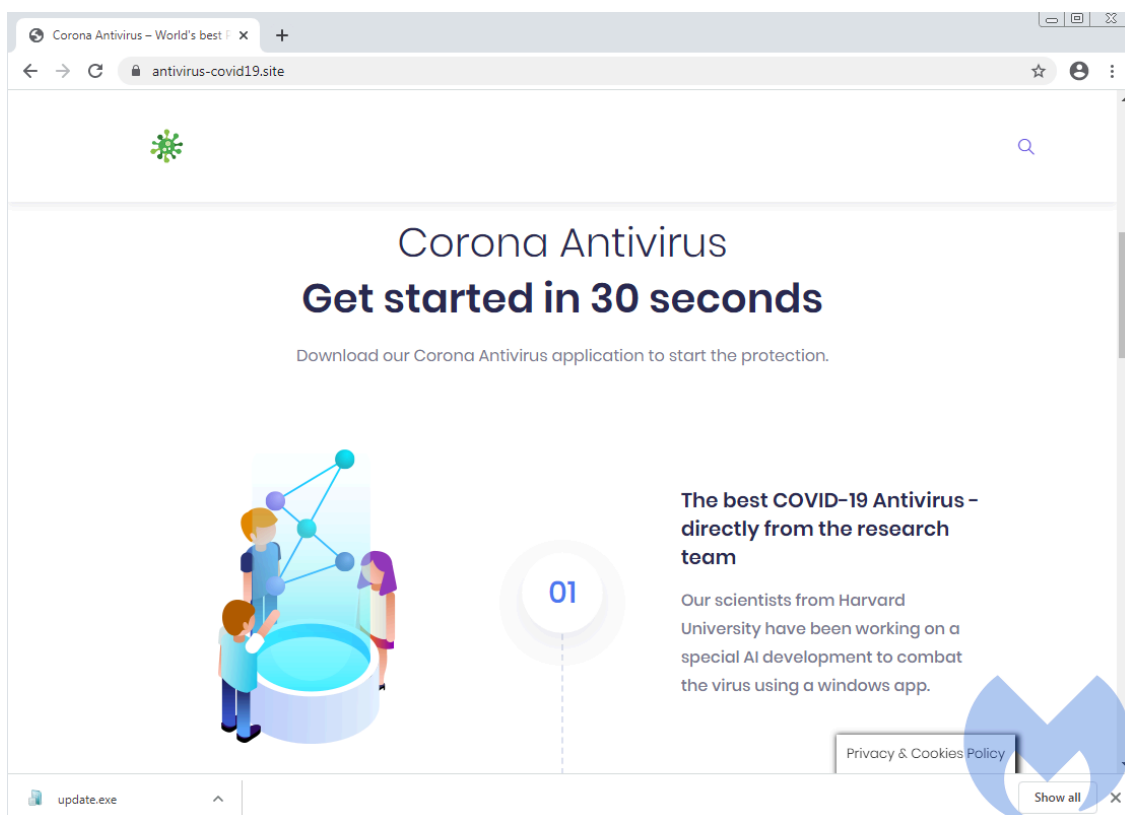
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

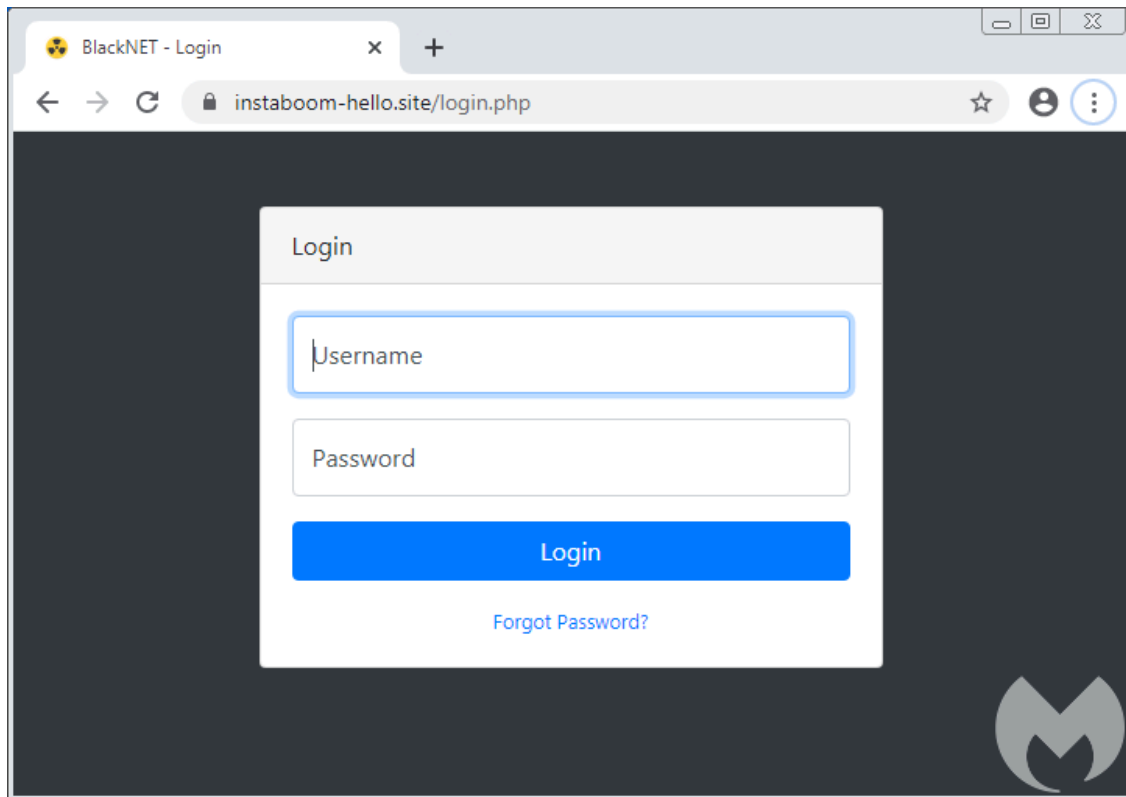


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

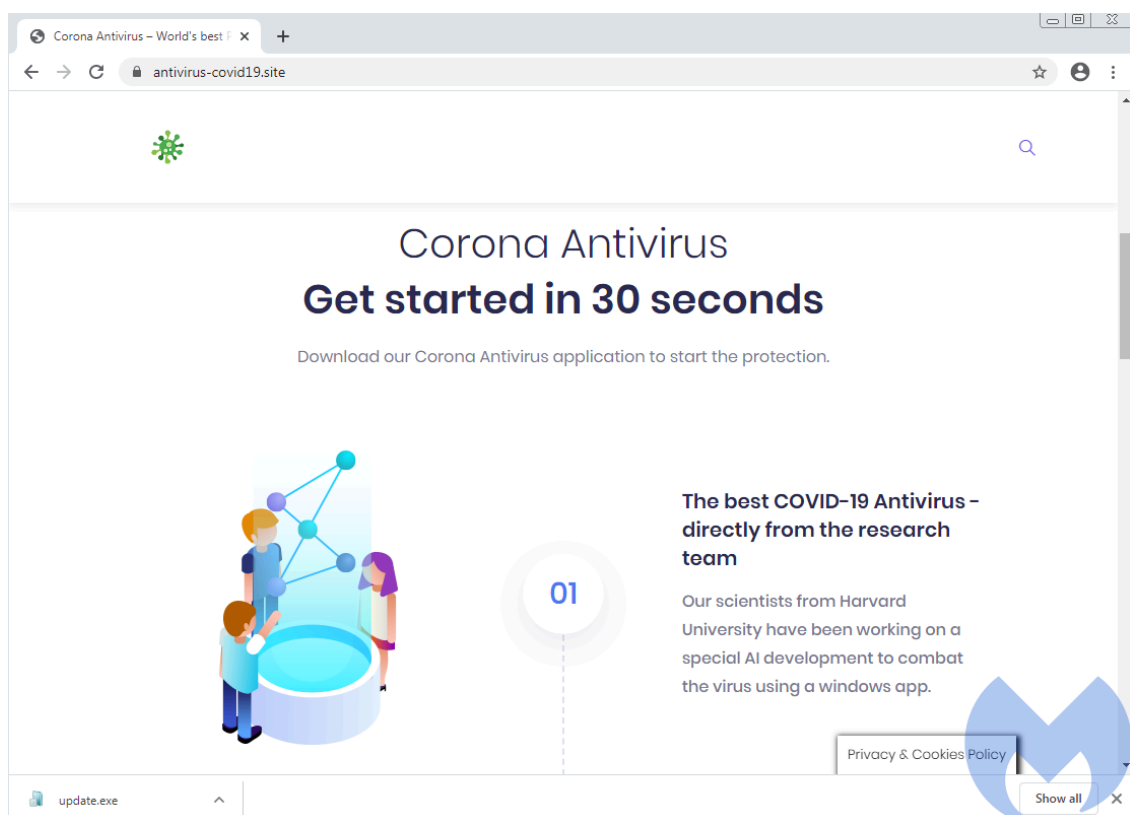
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

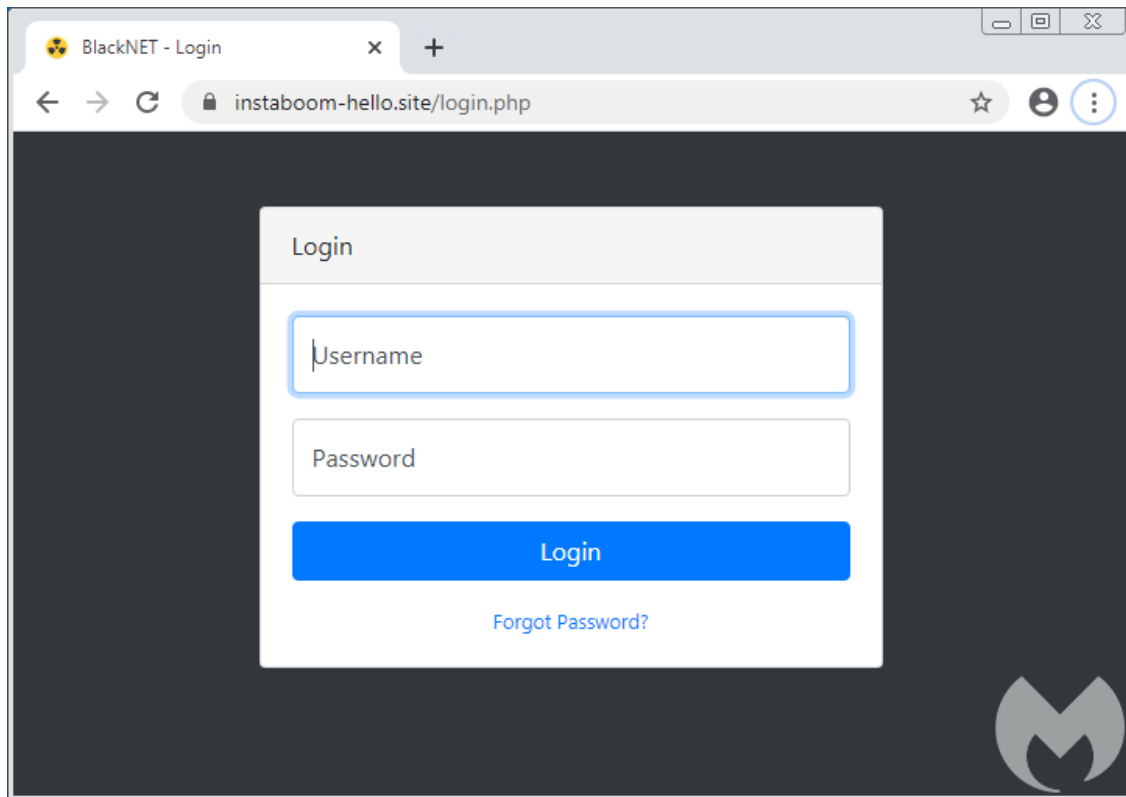


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

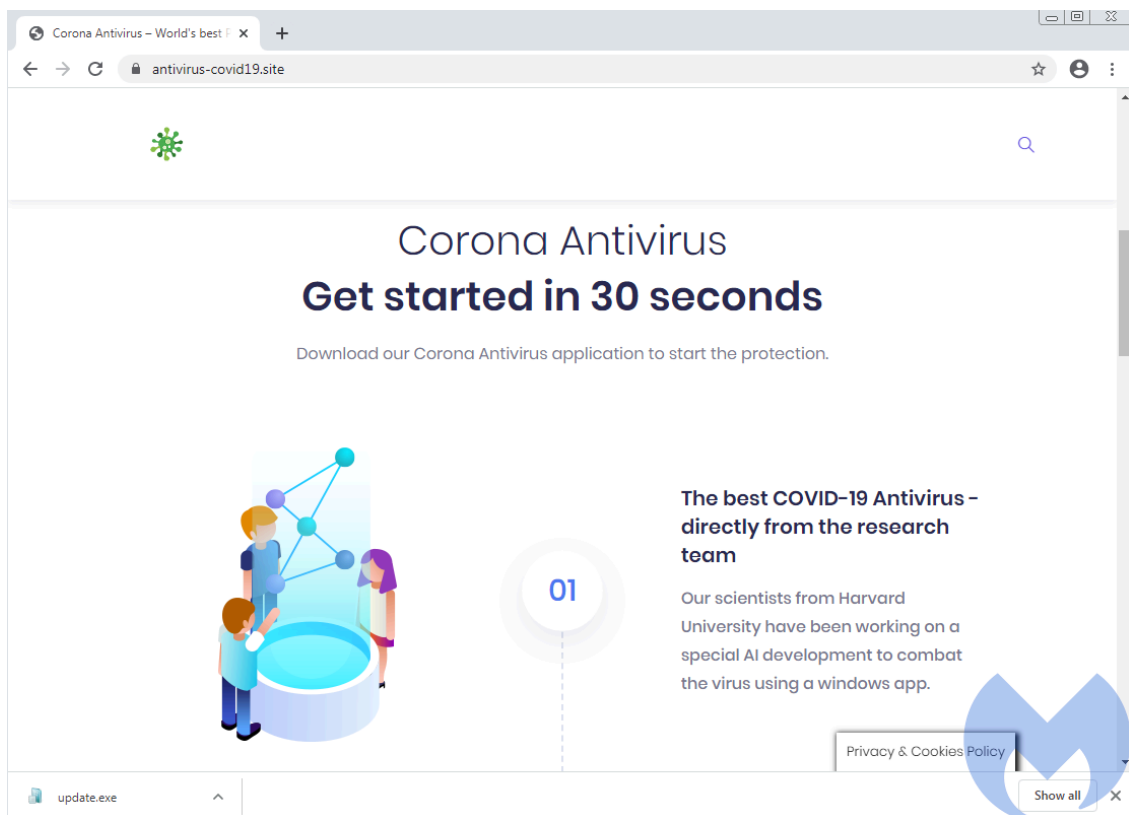
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

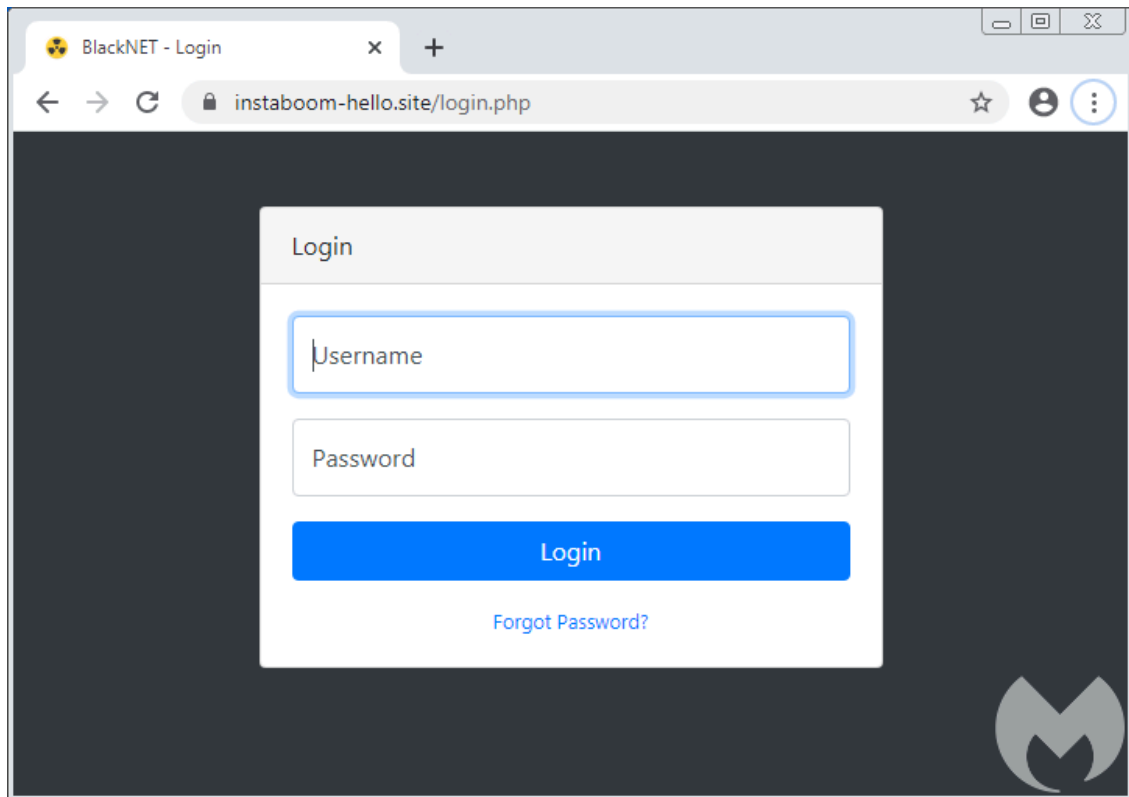


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

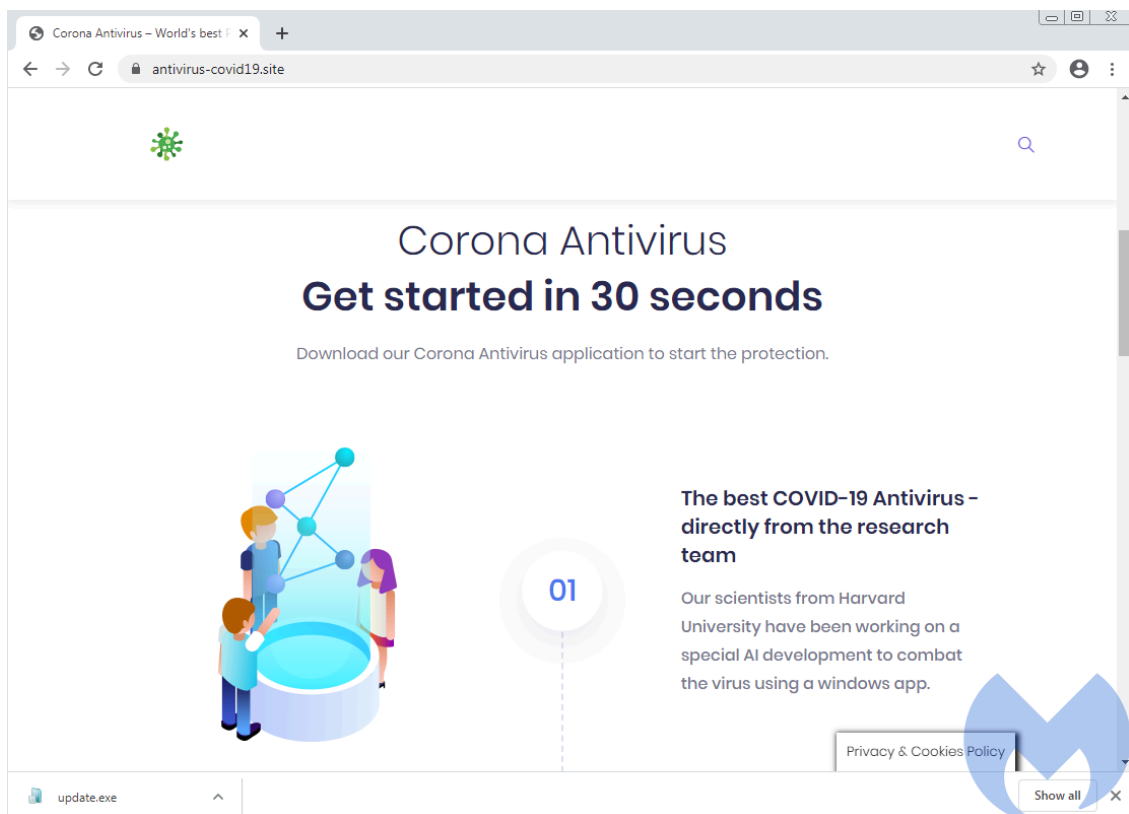
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

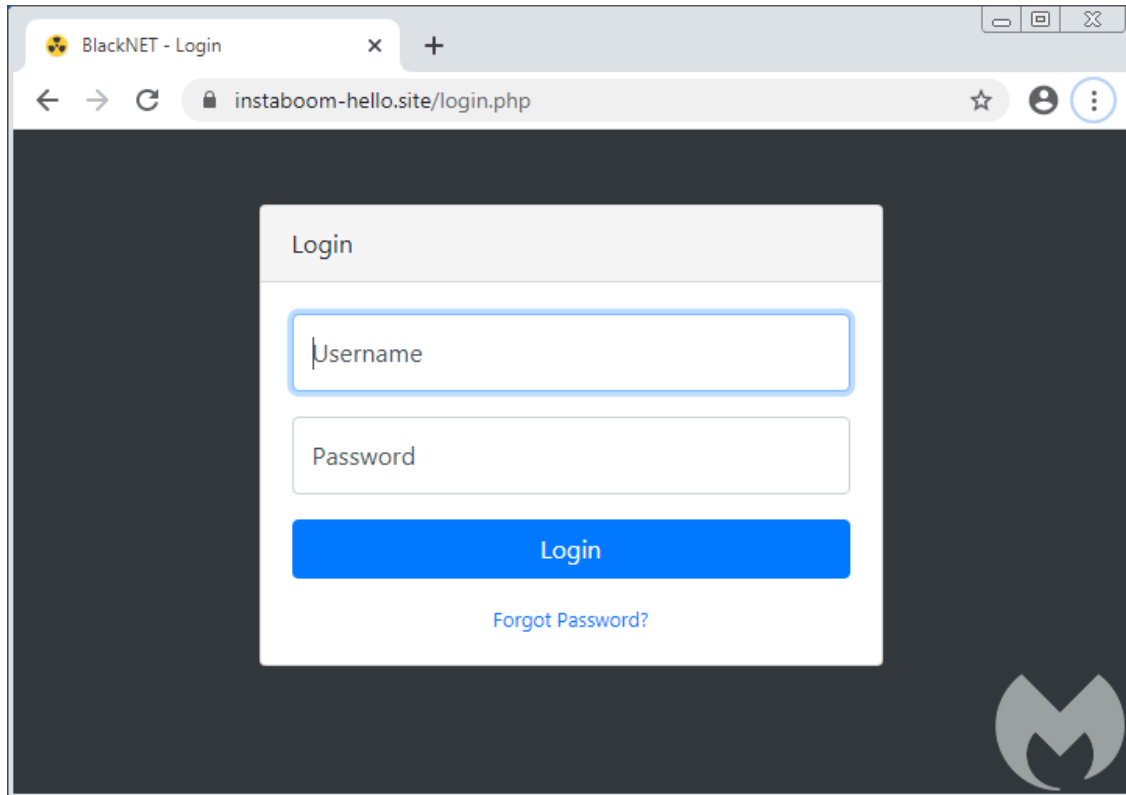


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

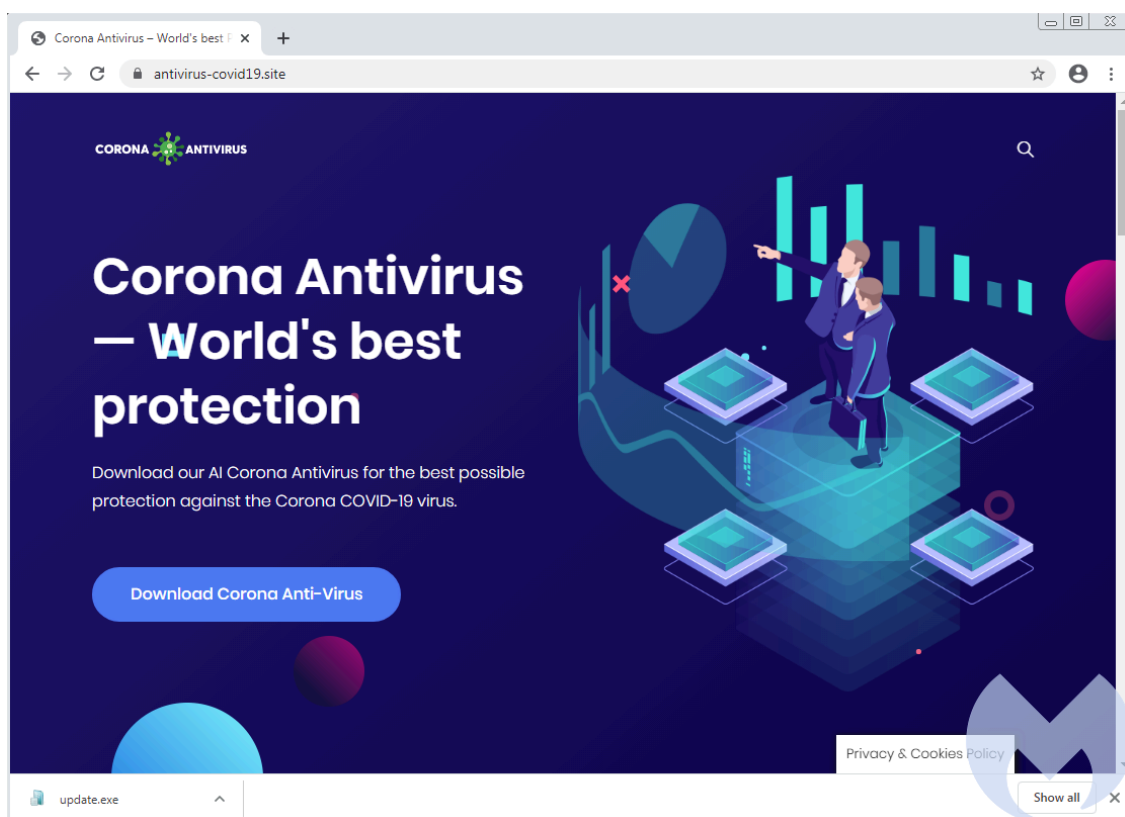
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

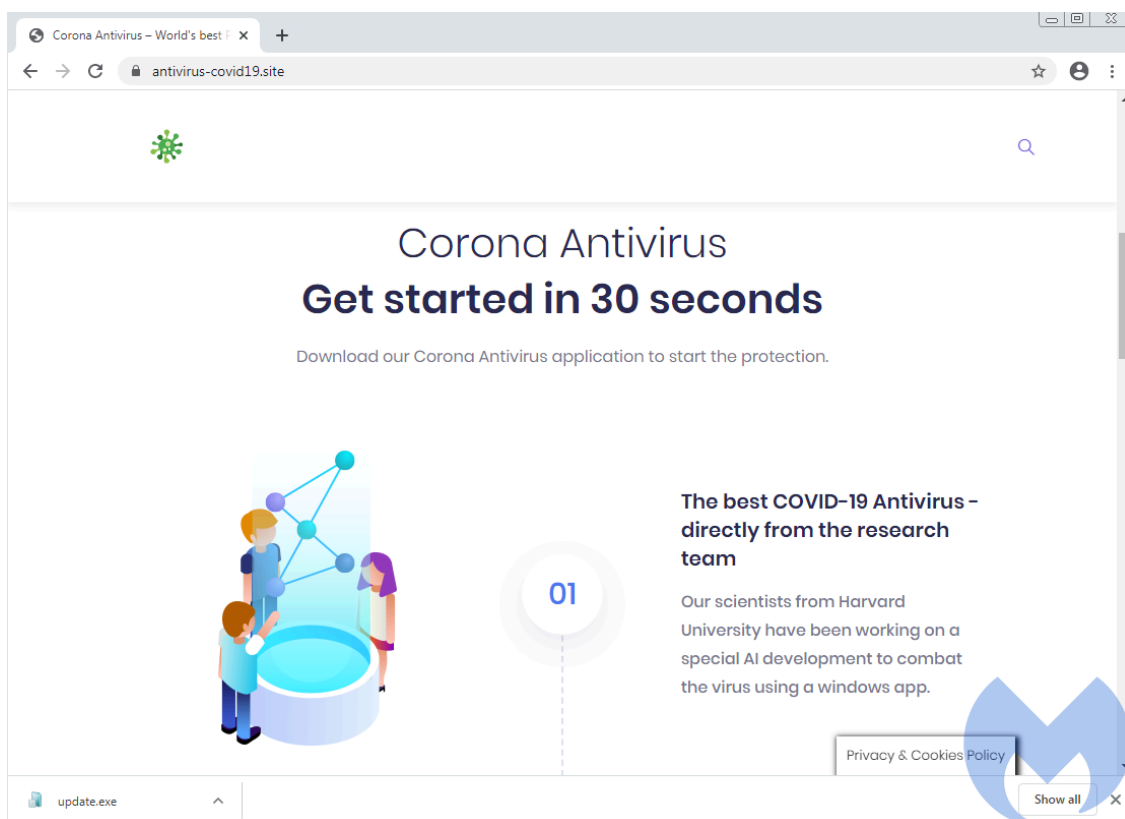
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

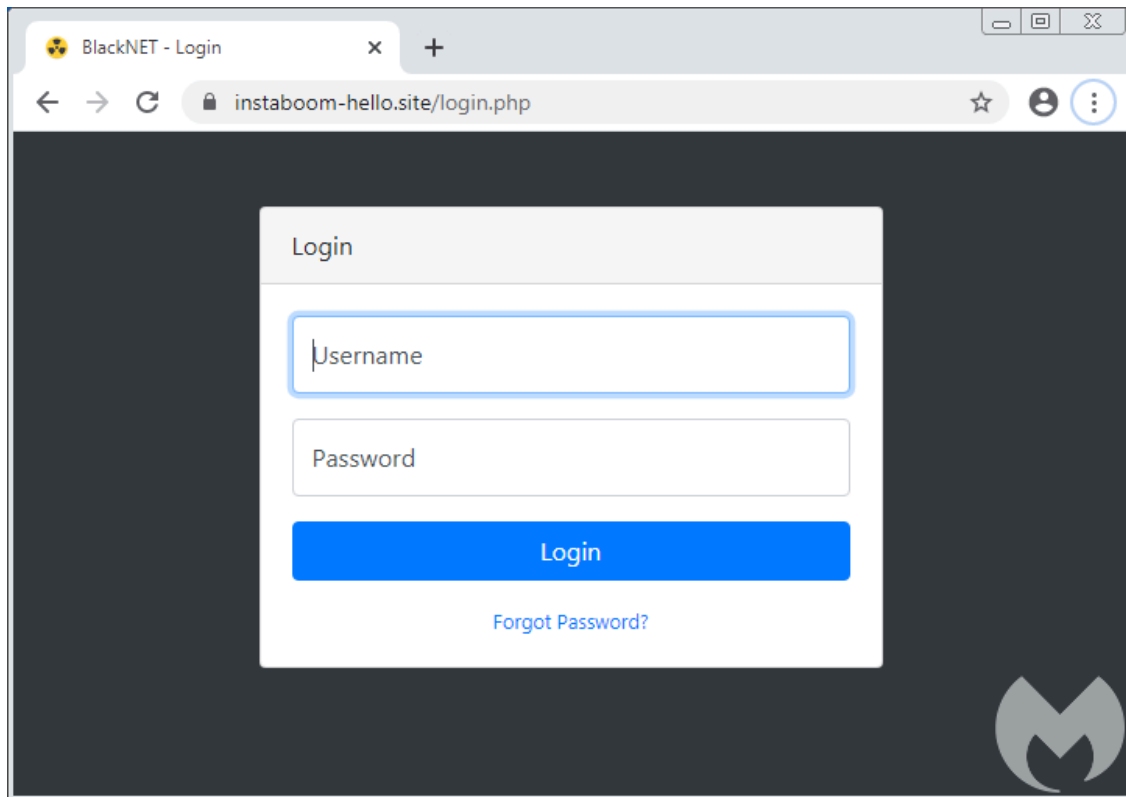


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

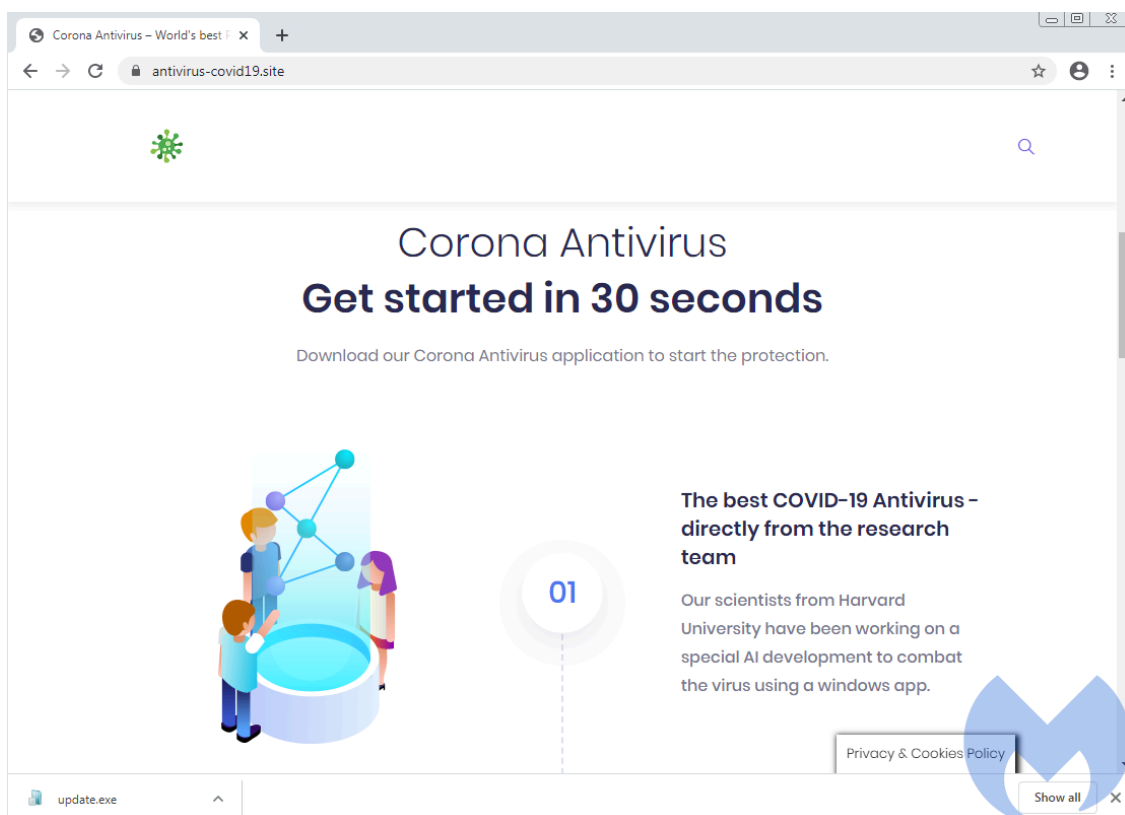
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

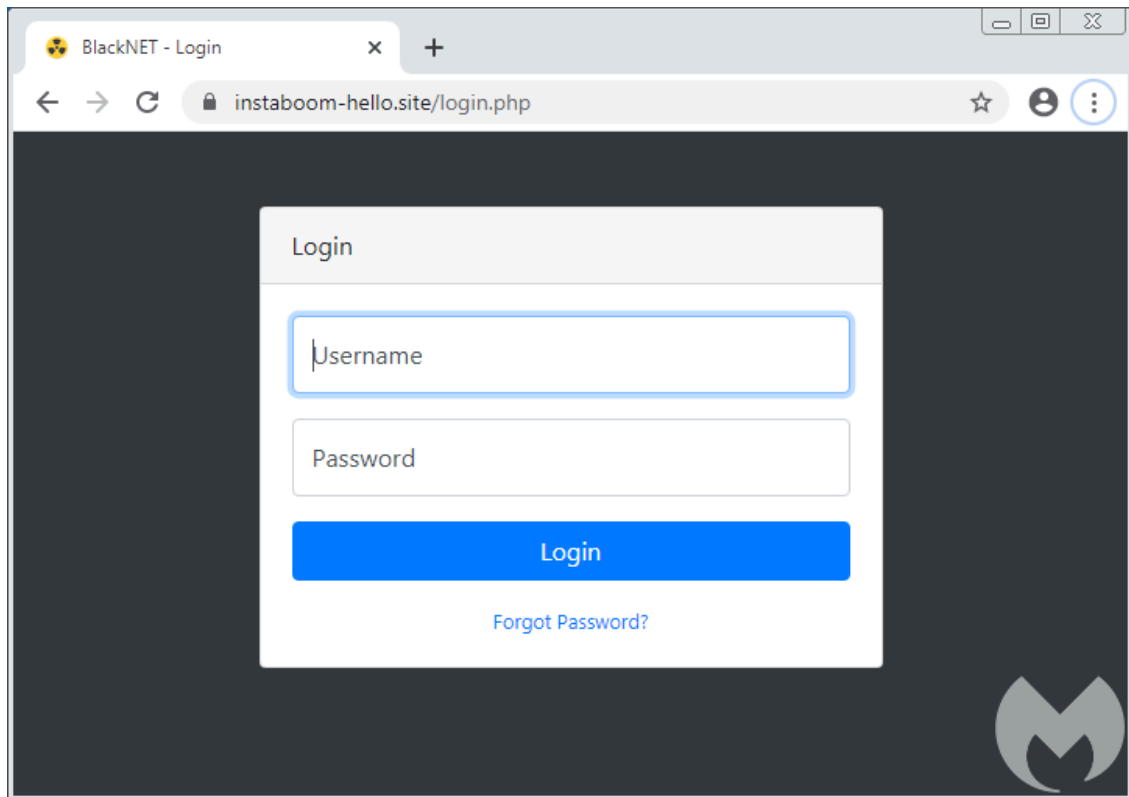


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this are two warning banners: one about logging in as 'admin' and another about two-factor authentication. The main content area has a 'Slaves Menu' with four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below the menu is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the right of the table are 'Previous' and 'Next' buttons. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right of the commands center is a 'Map Visualization' section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features the Malwarebytes logo and the word 'Premium' in the top left corner. A green checkmark icon is next to the heading 'Malware blocked by Real-Time Protection'. Below this, a message states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom of the window are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

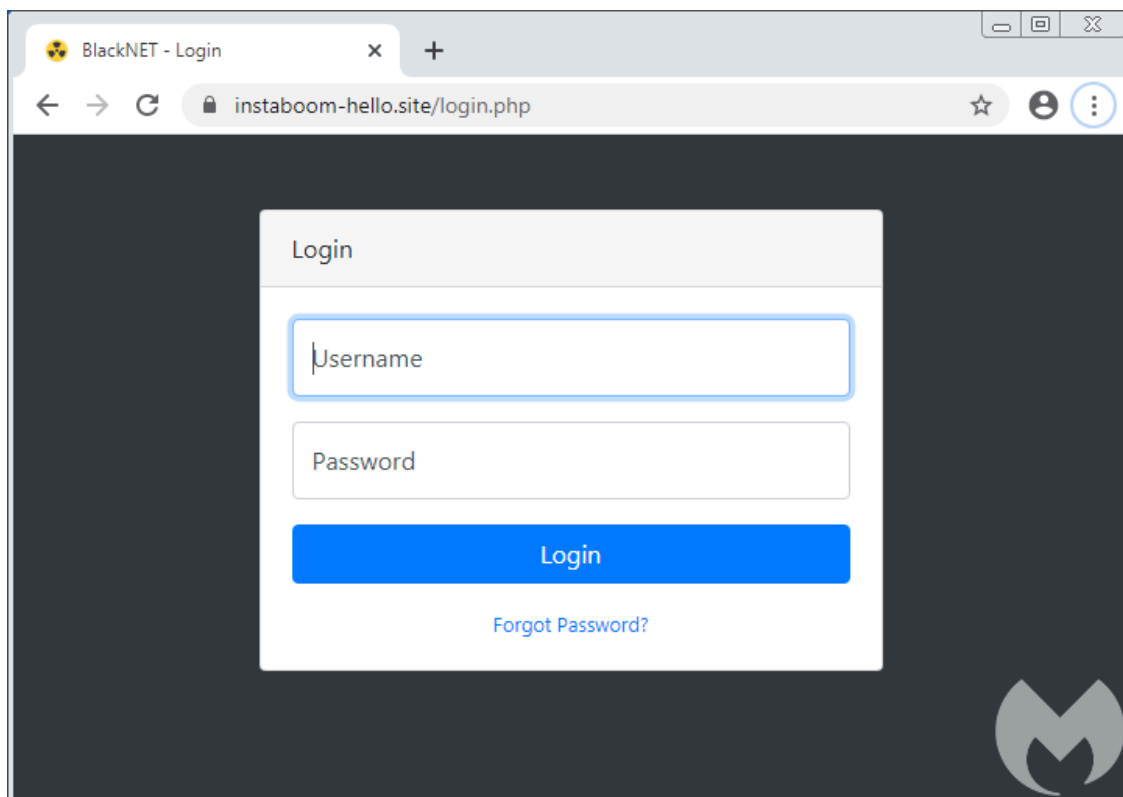
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

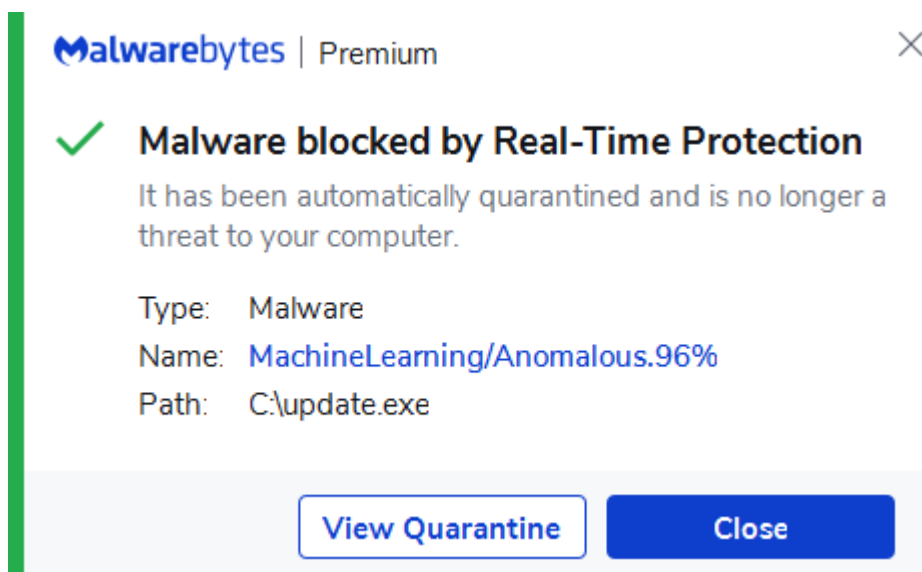
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

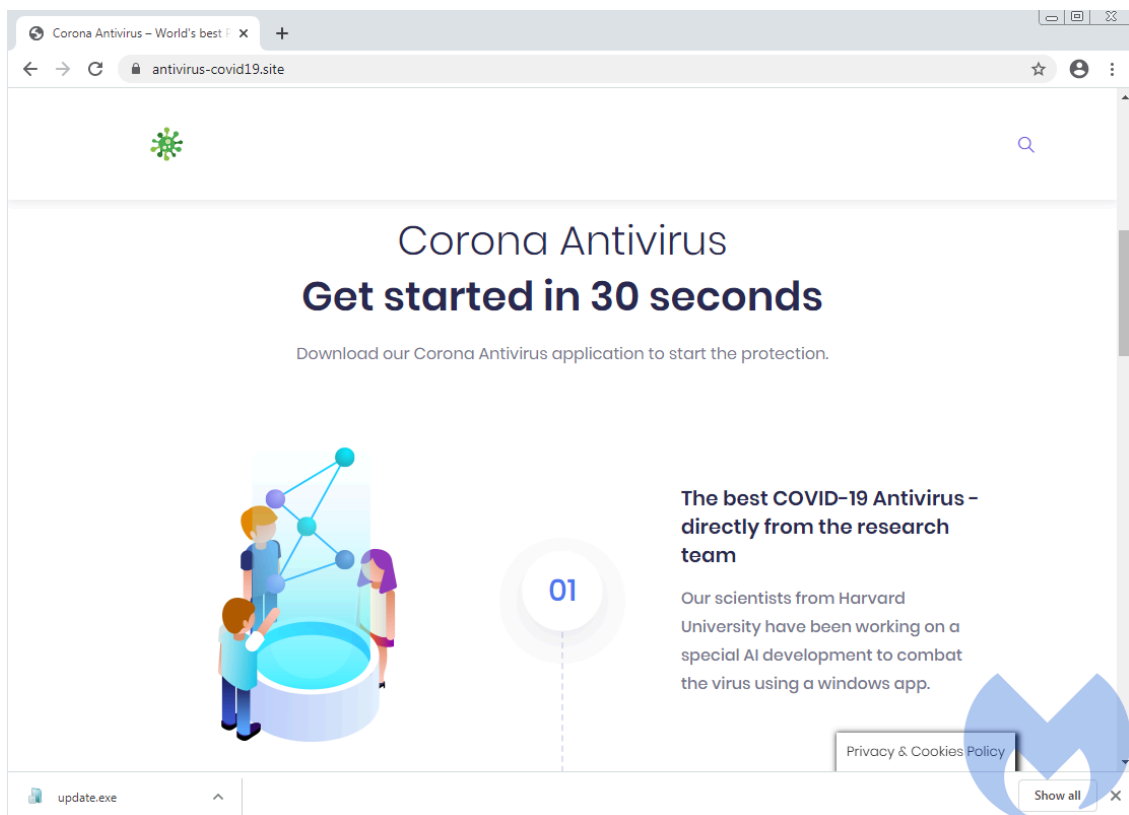
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

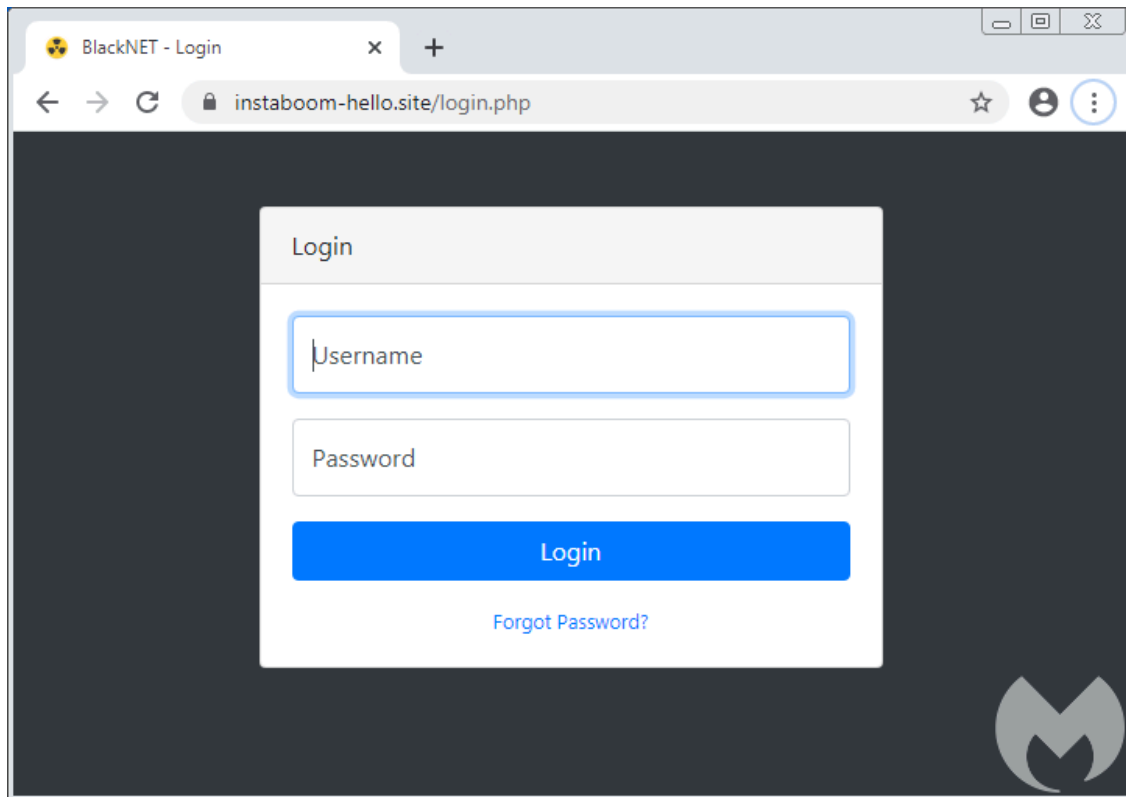


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

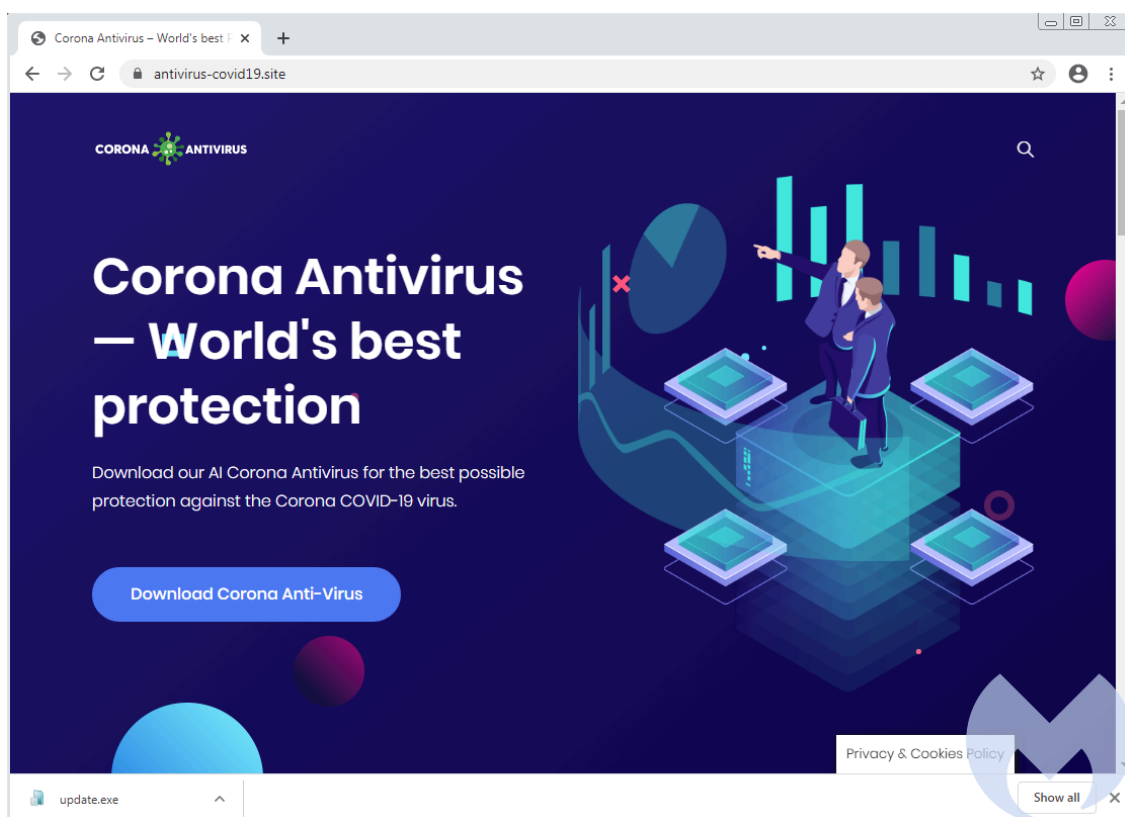
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

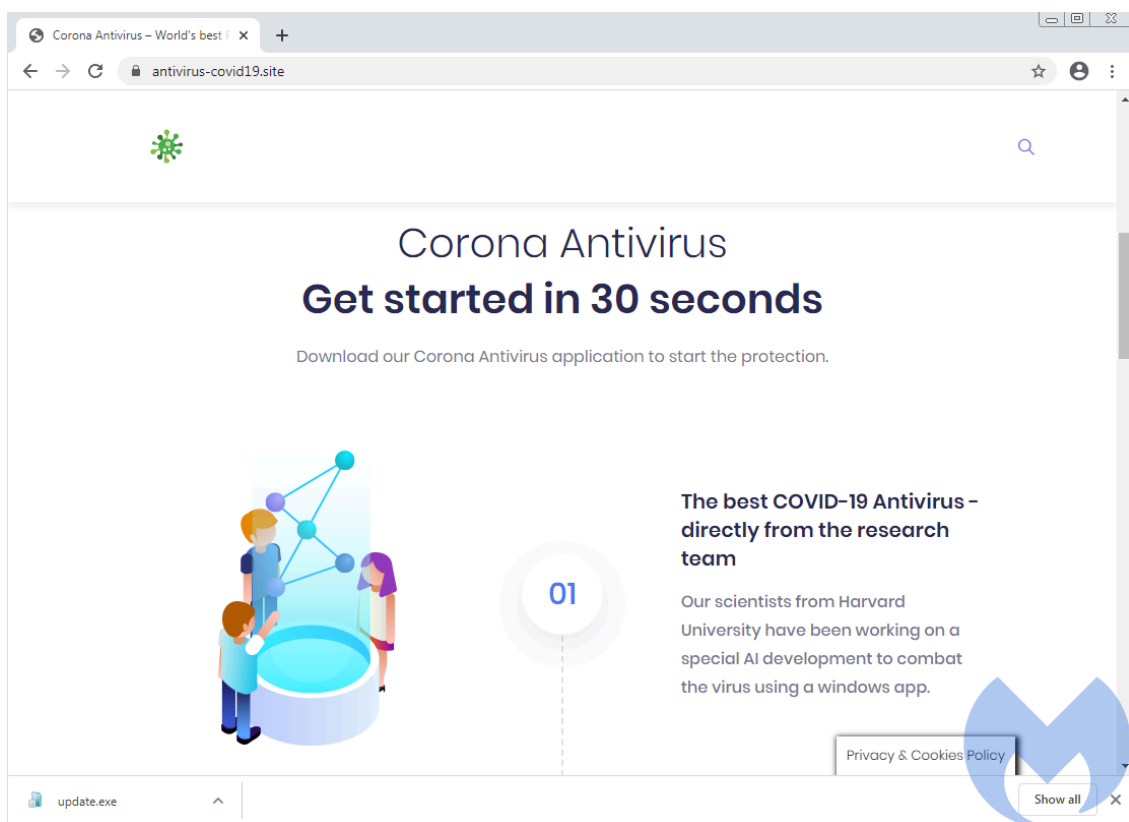
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

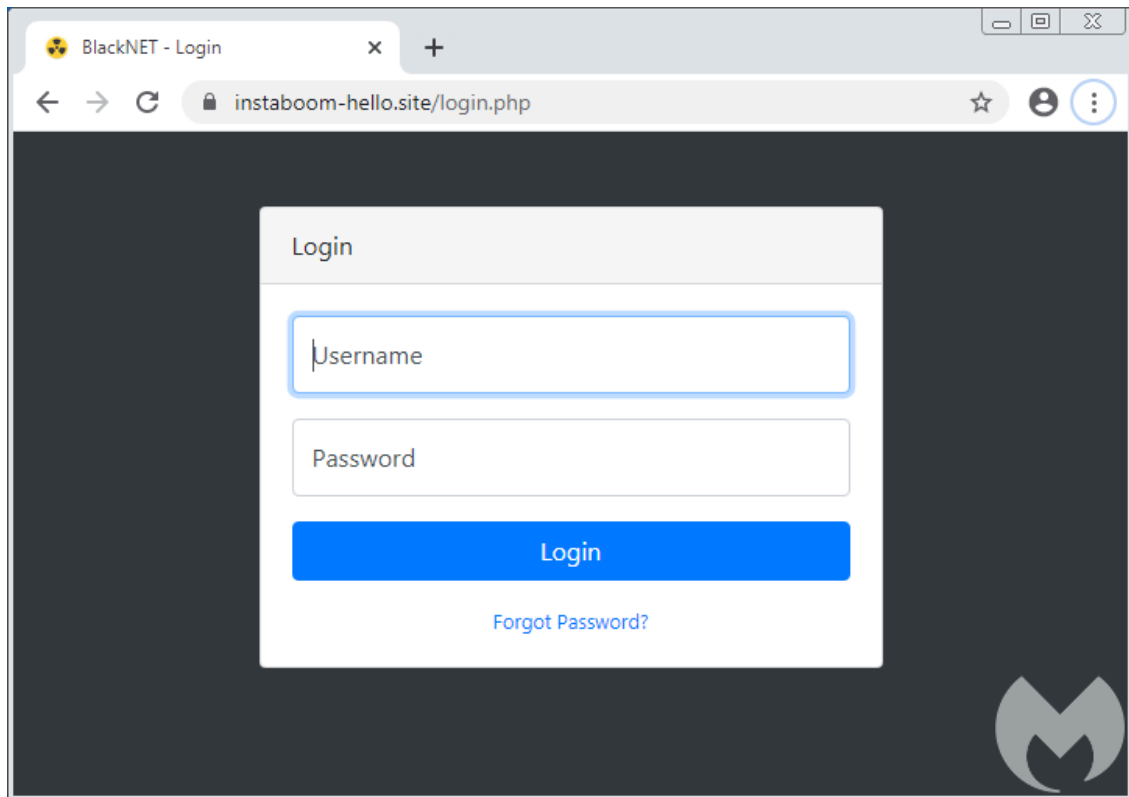


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

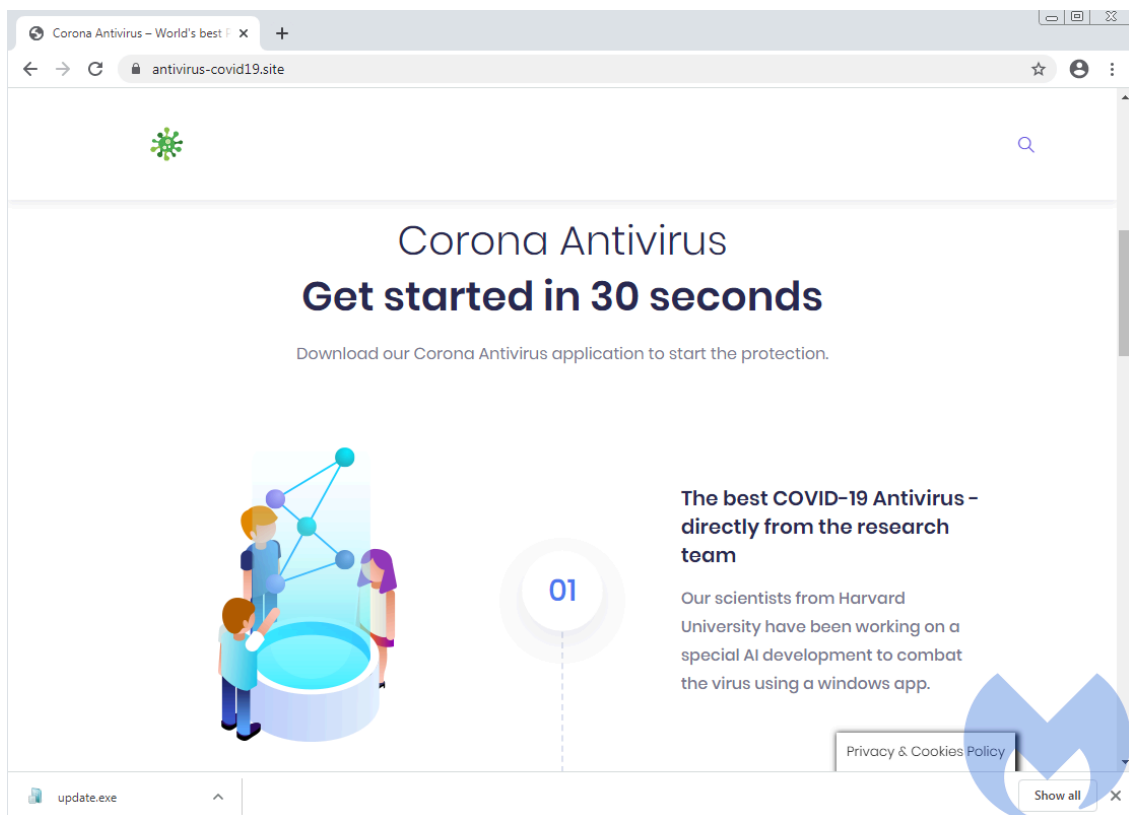
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

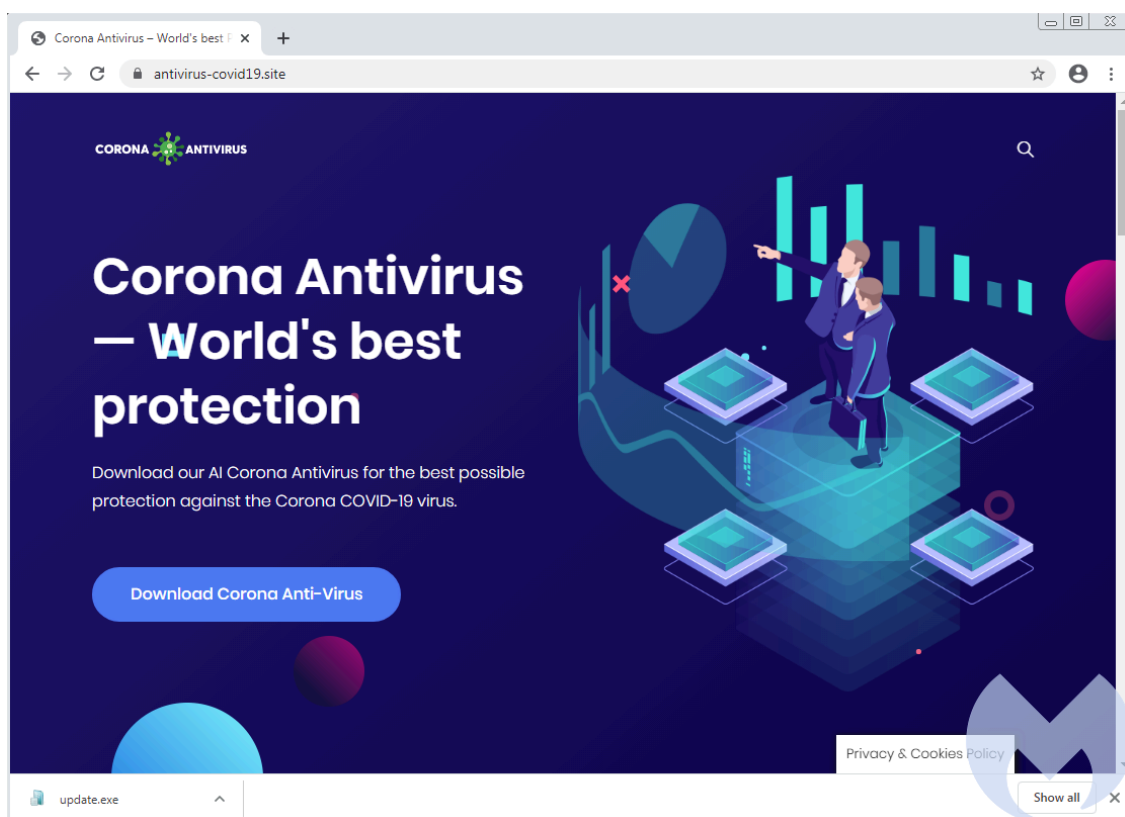
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

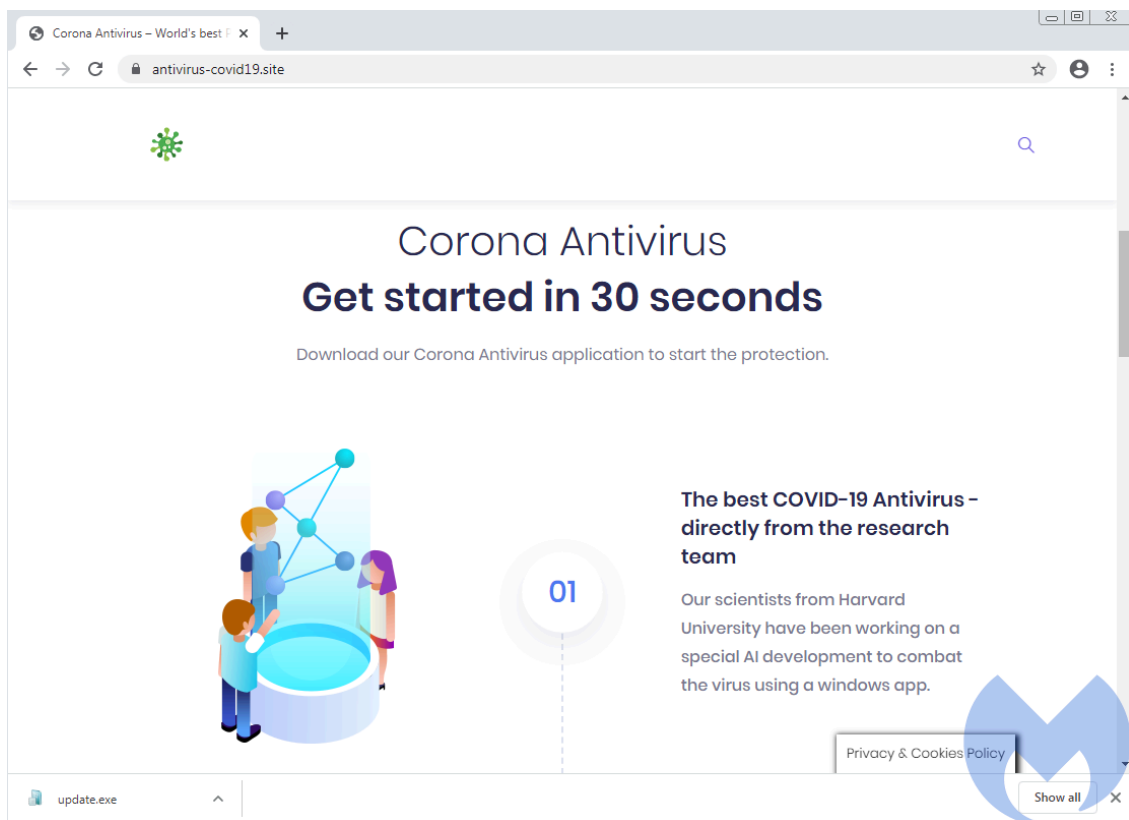
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

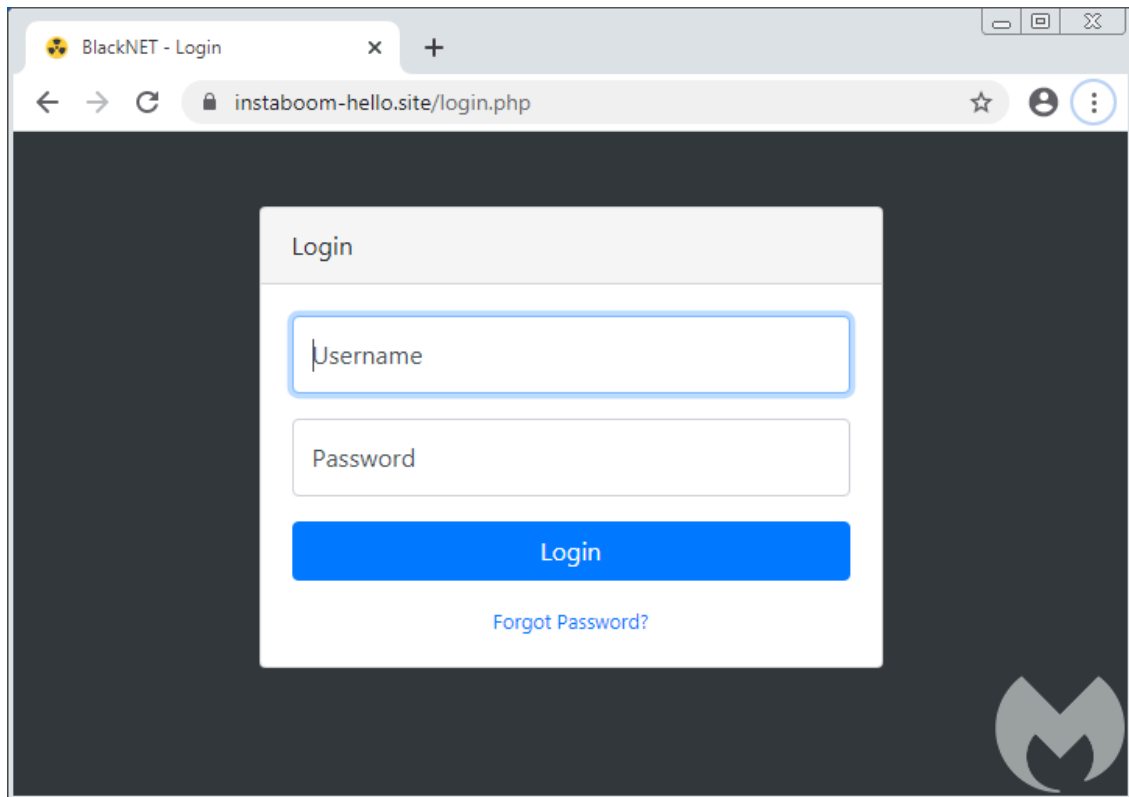


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

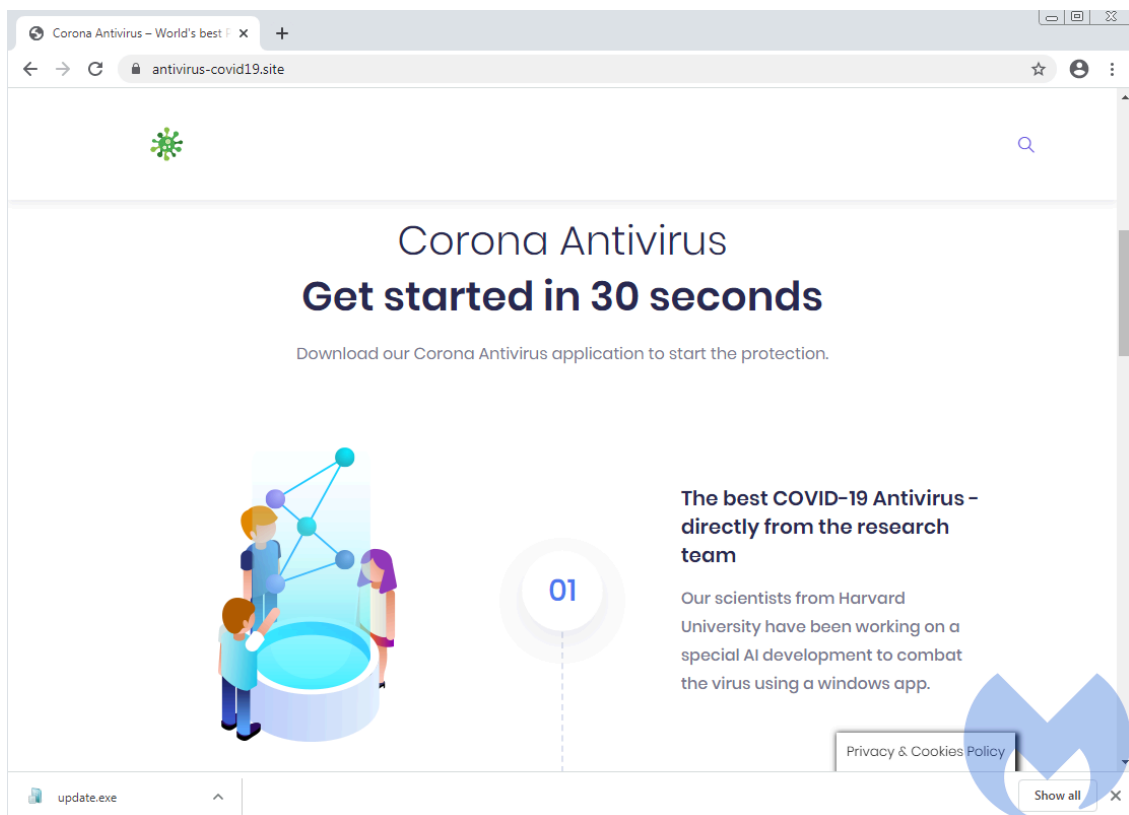
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

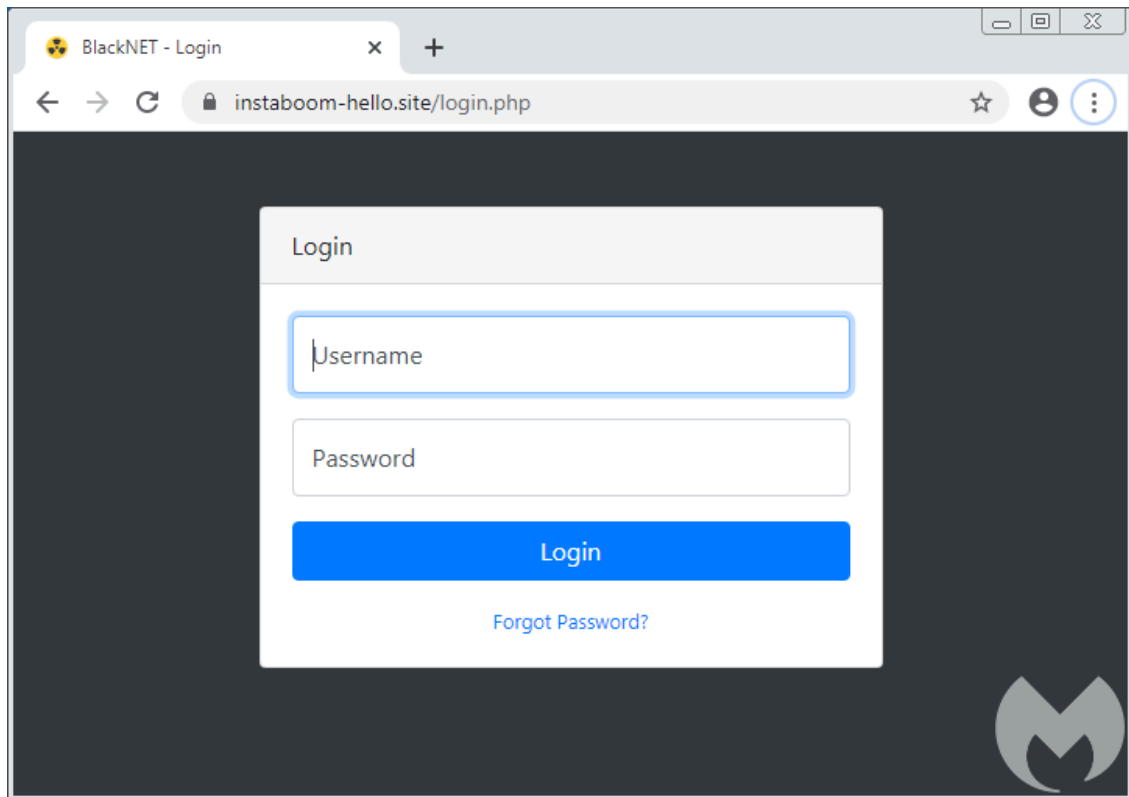


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

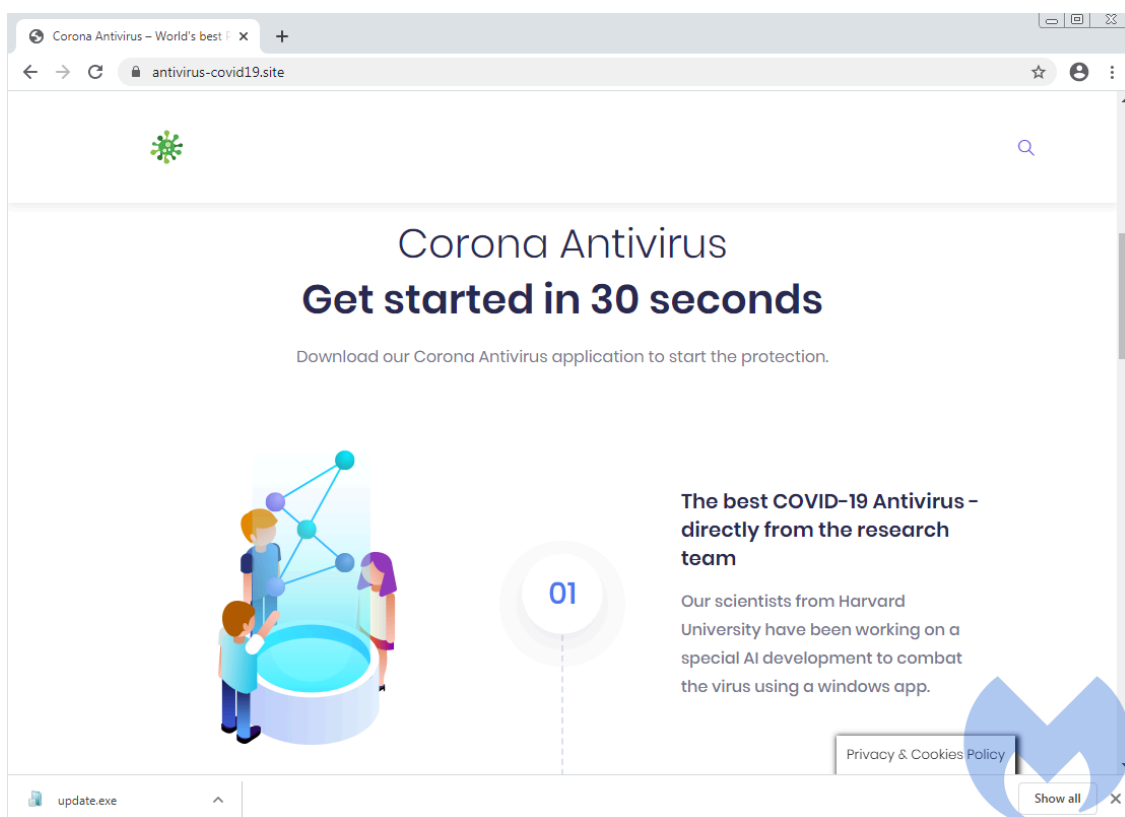
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

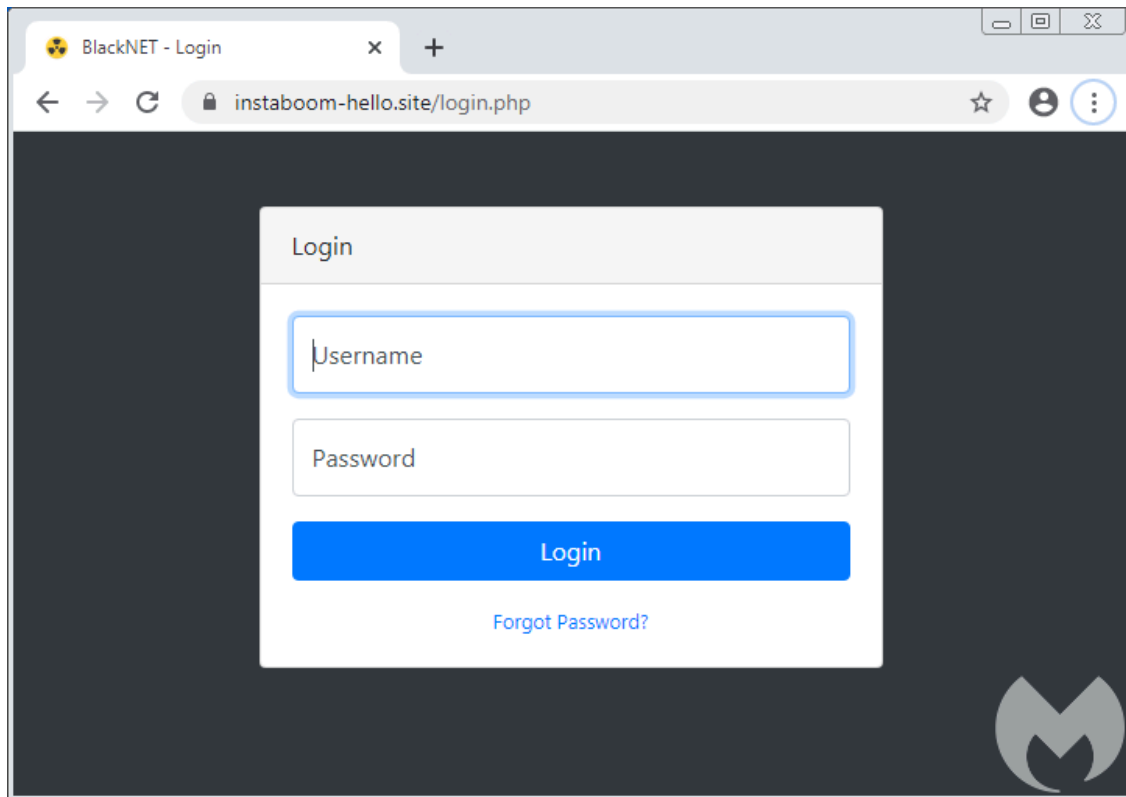


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

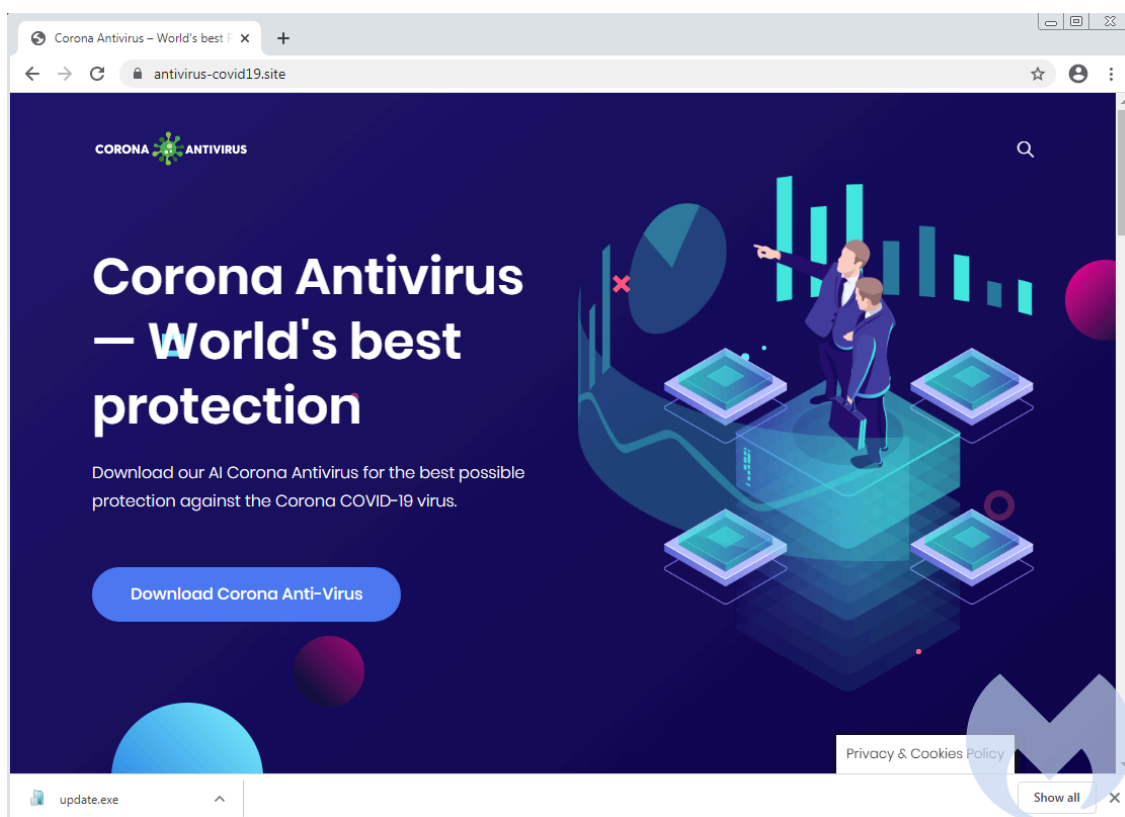
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

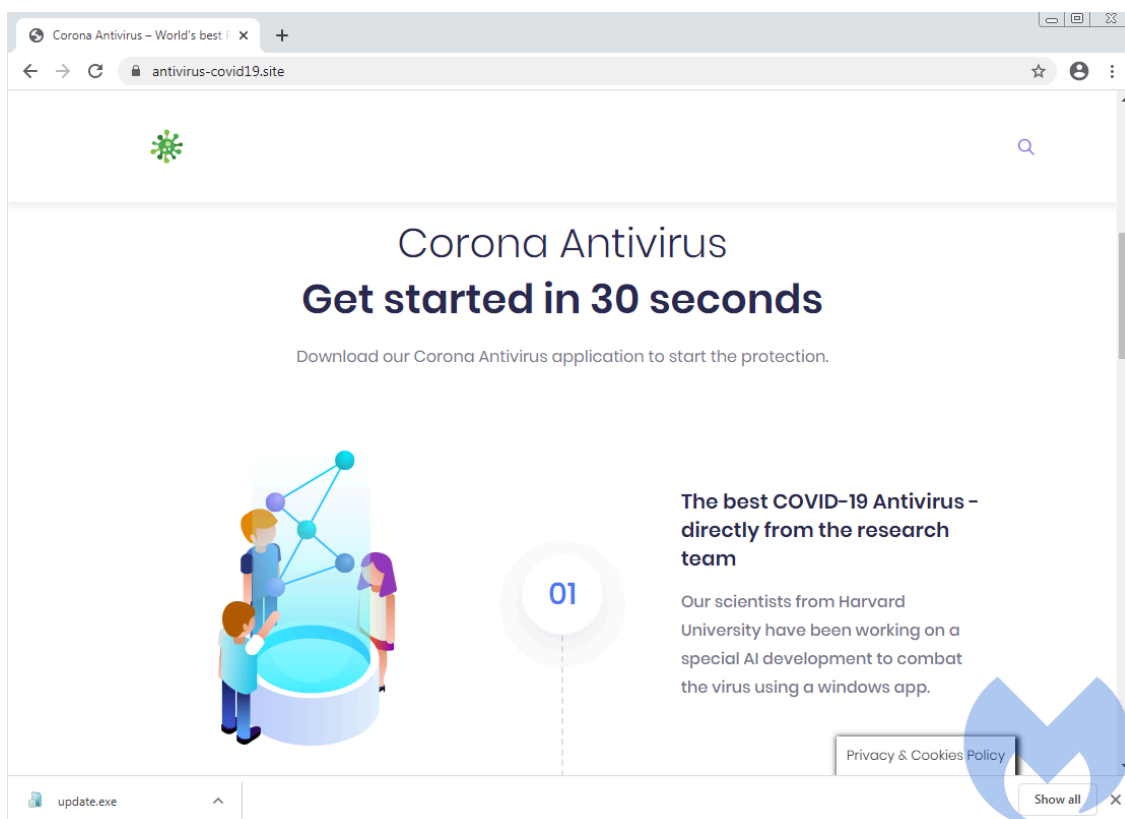
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

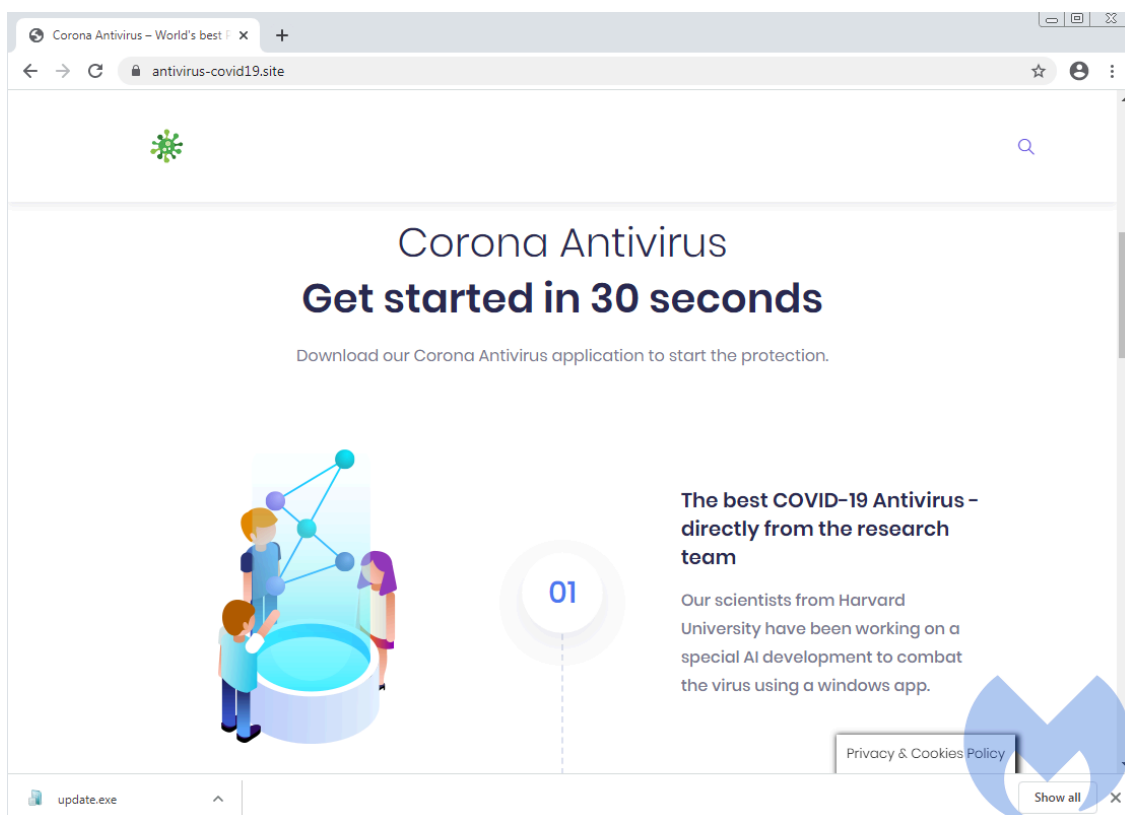
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

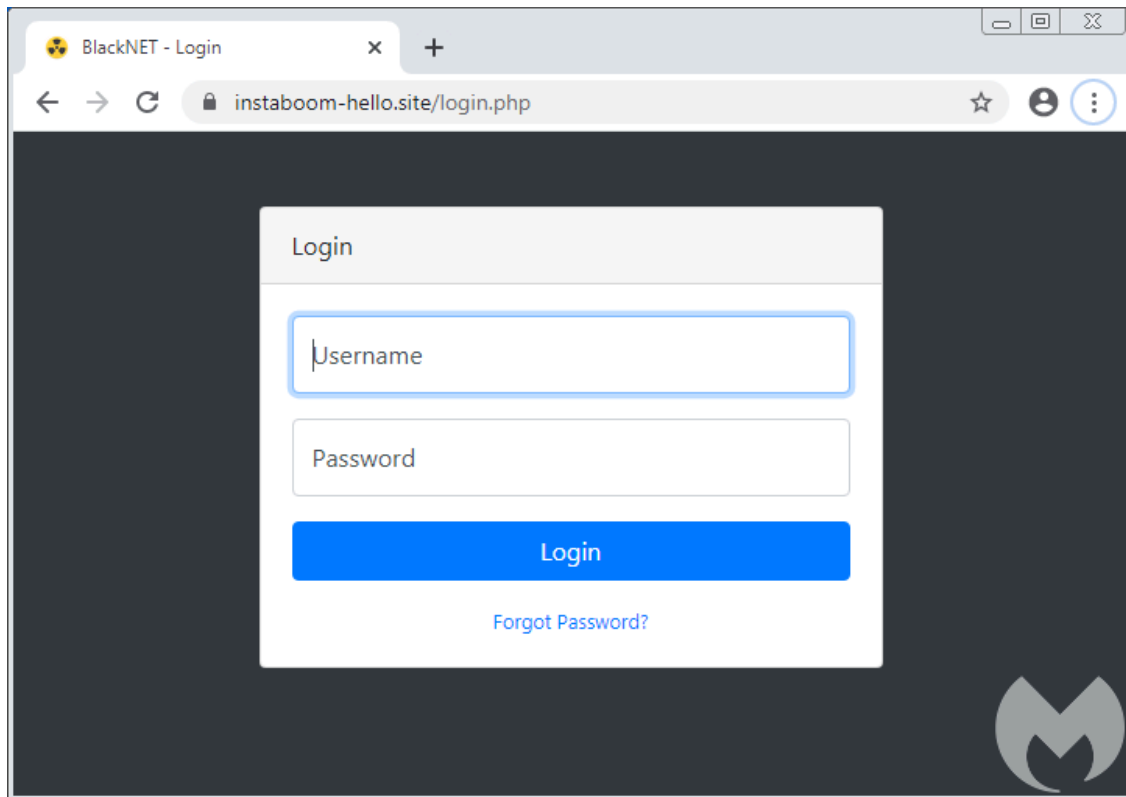


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

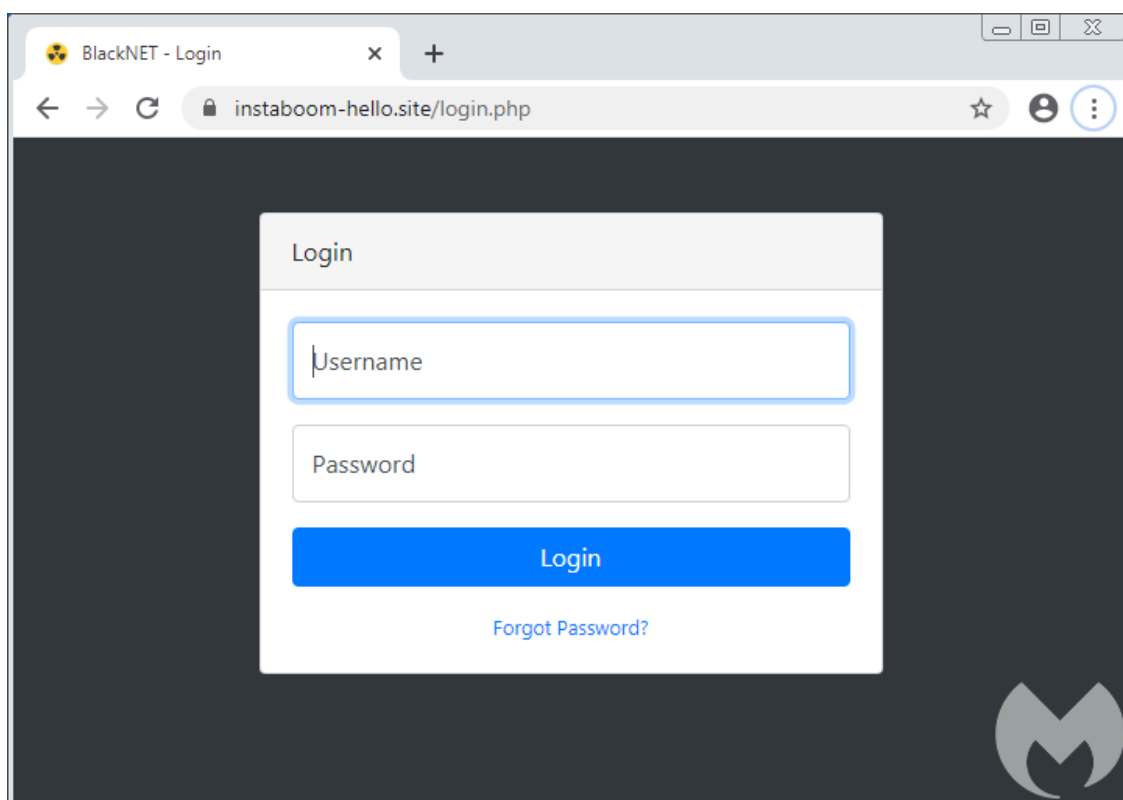
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

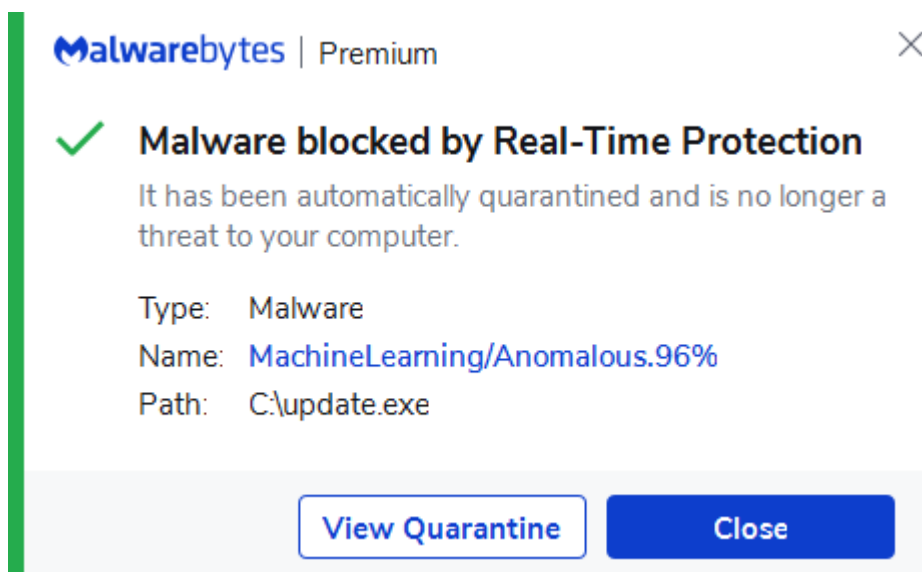
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

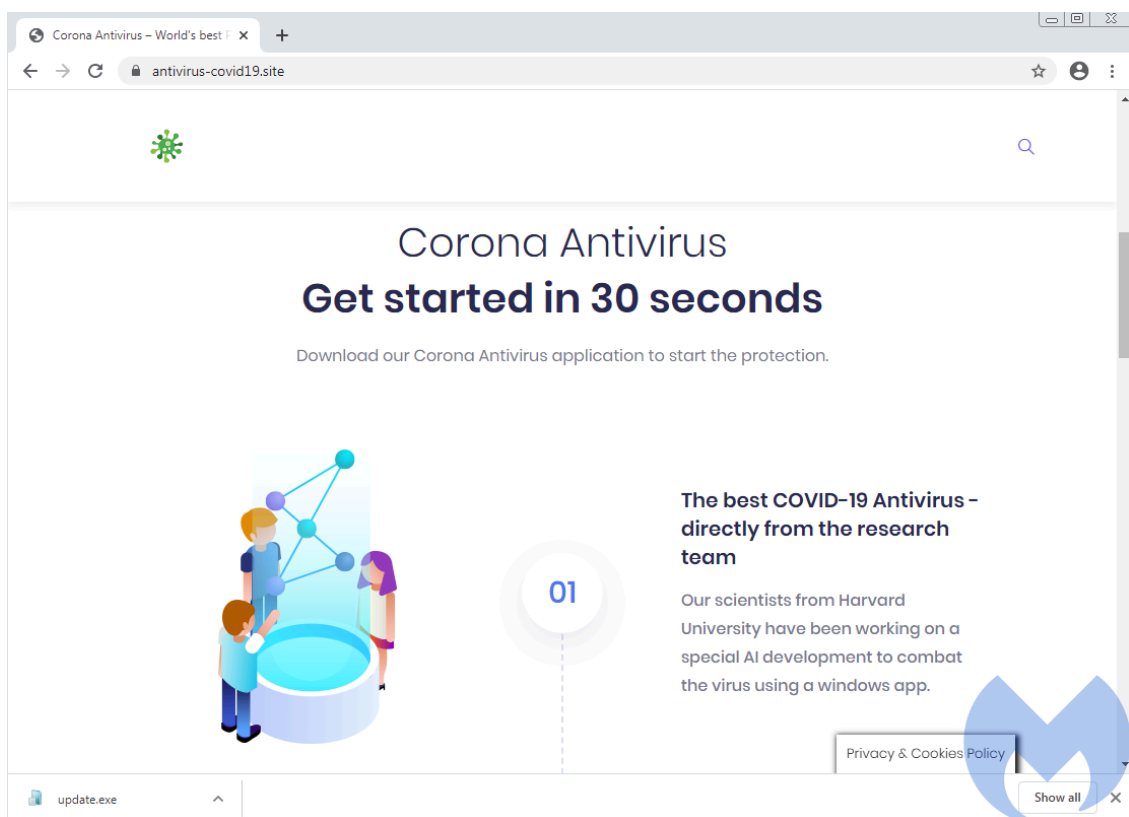
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

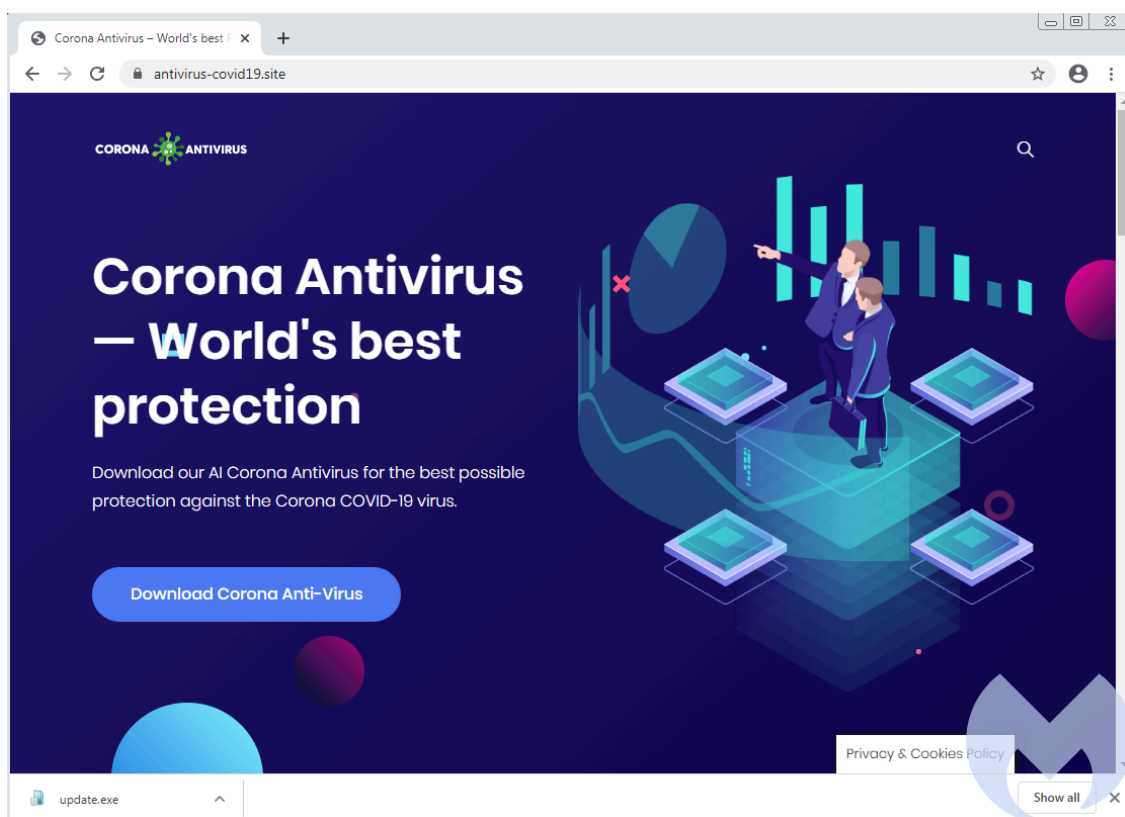
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

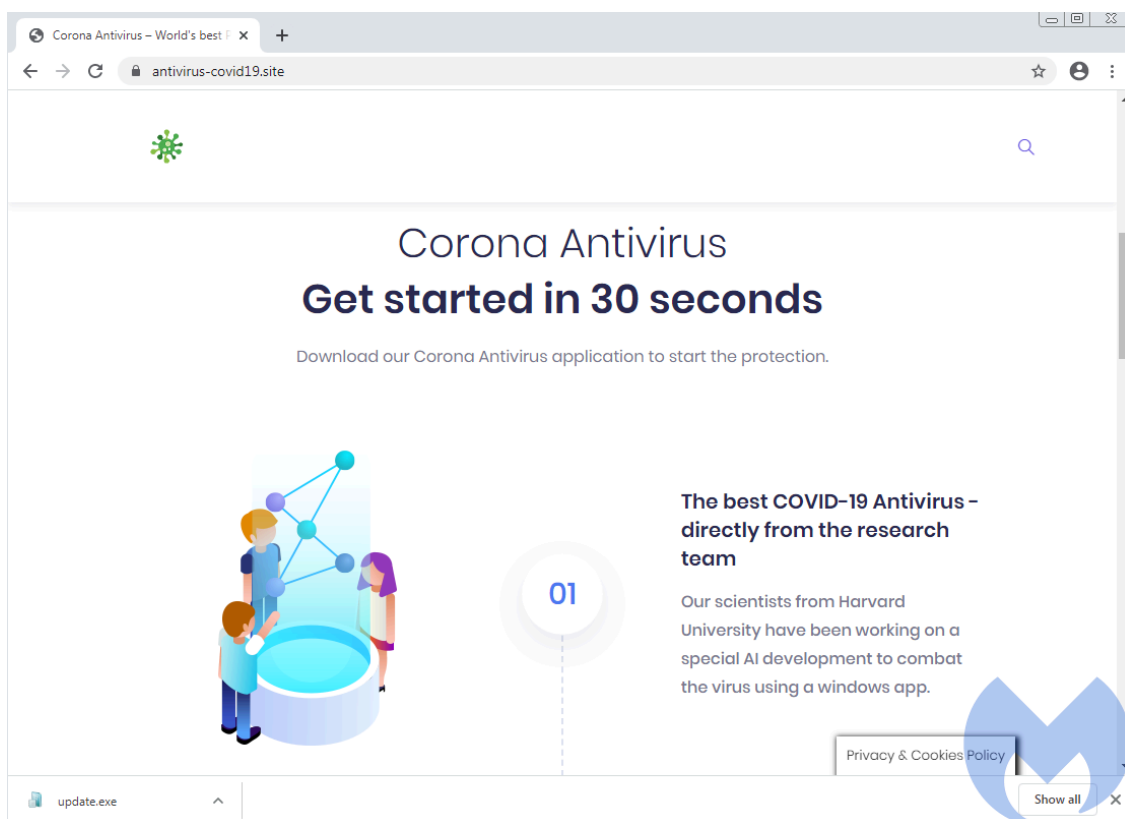
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

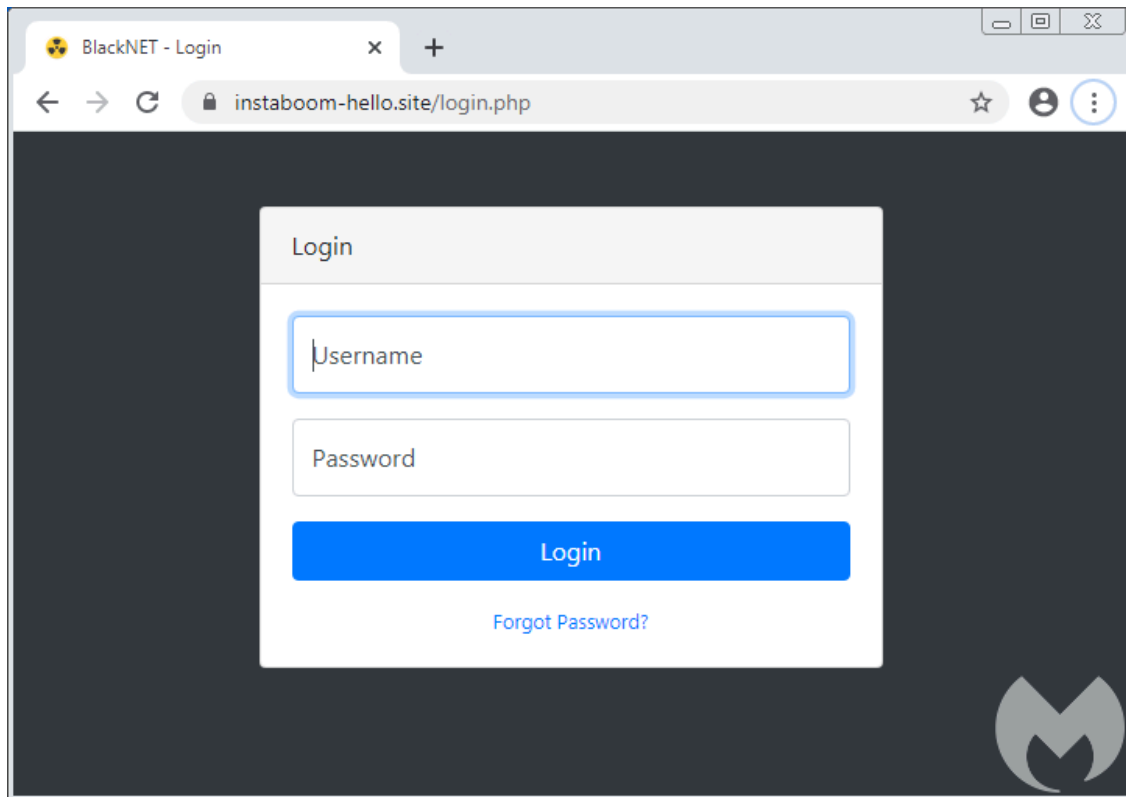


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

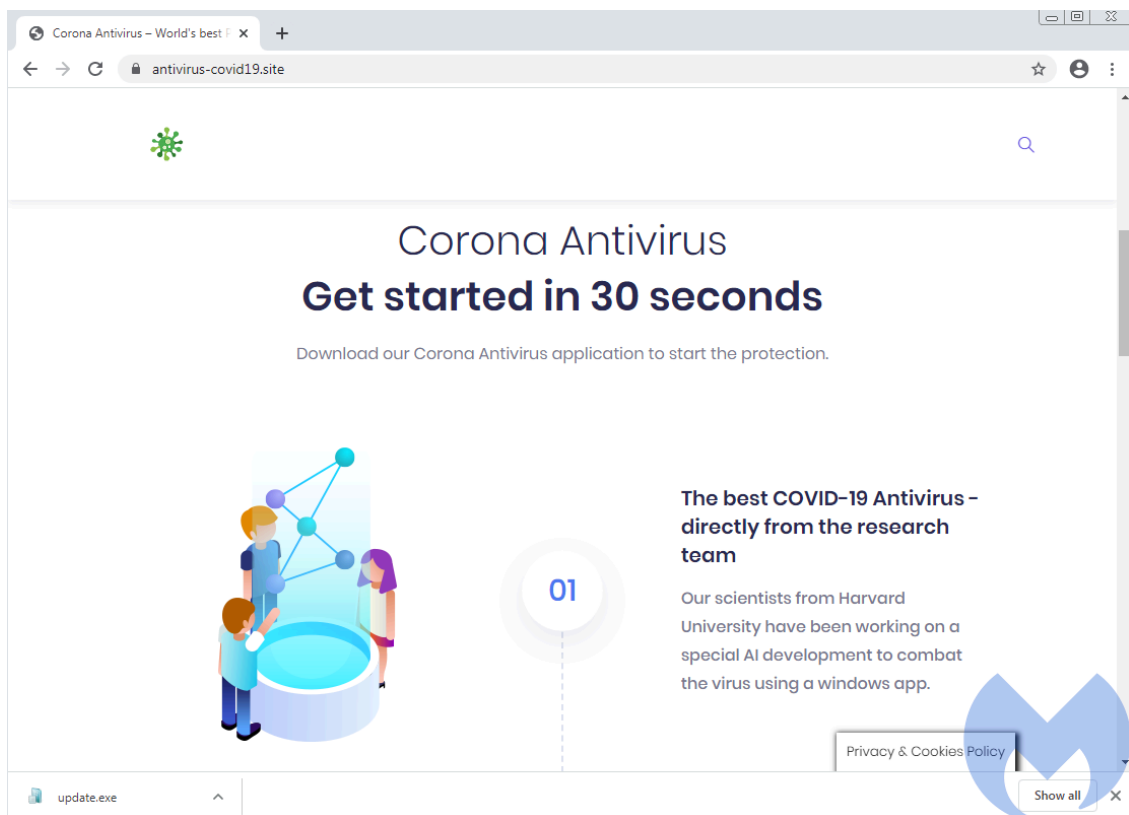
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

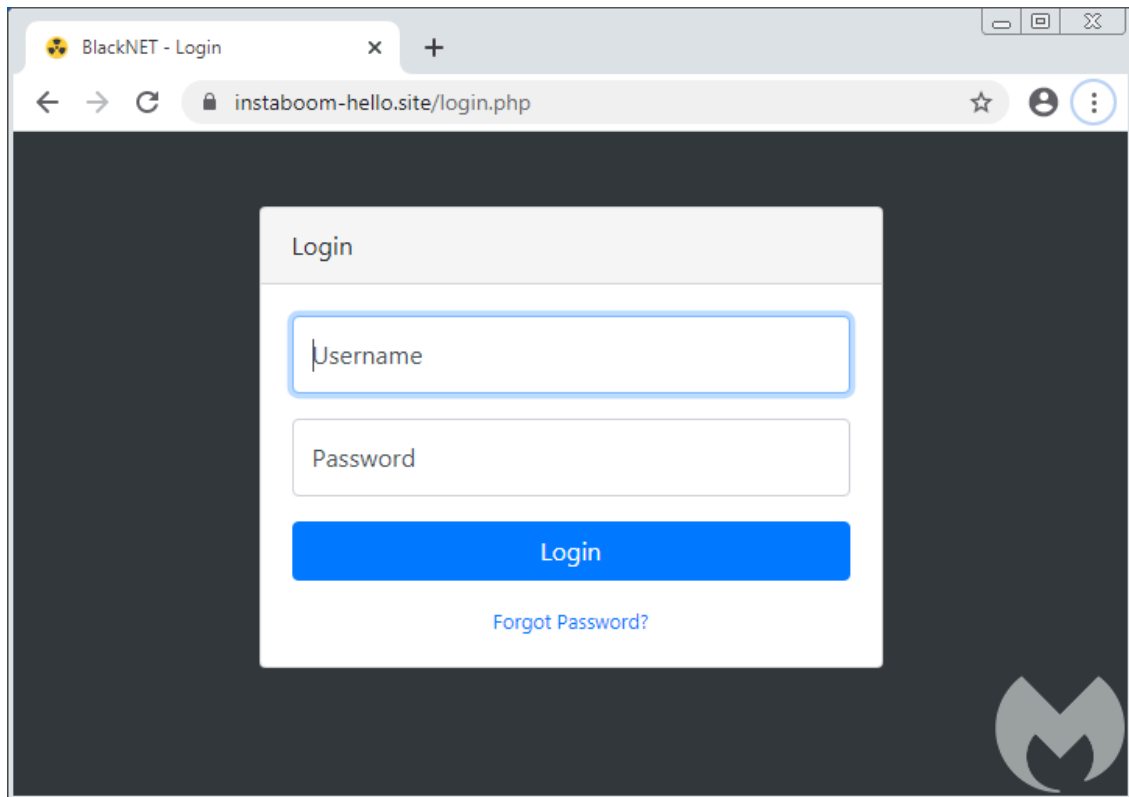


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. At the top left is the Malwarebytes logo and "Premium" text. At the top right is a close button (X). Below the header is a green checkmark icon followed by the text "Malware blocked by Real-Time Protection". Below this is a message: "It has been automatically quarantined and is no longer a threat to your computer." Below the message are three lines of information: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

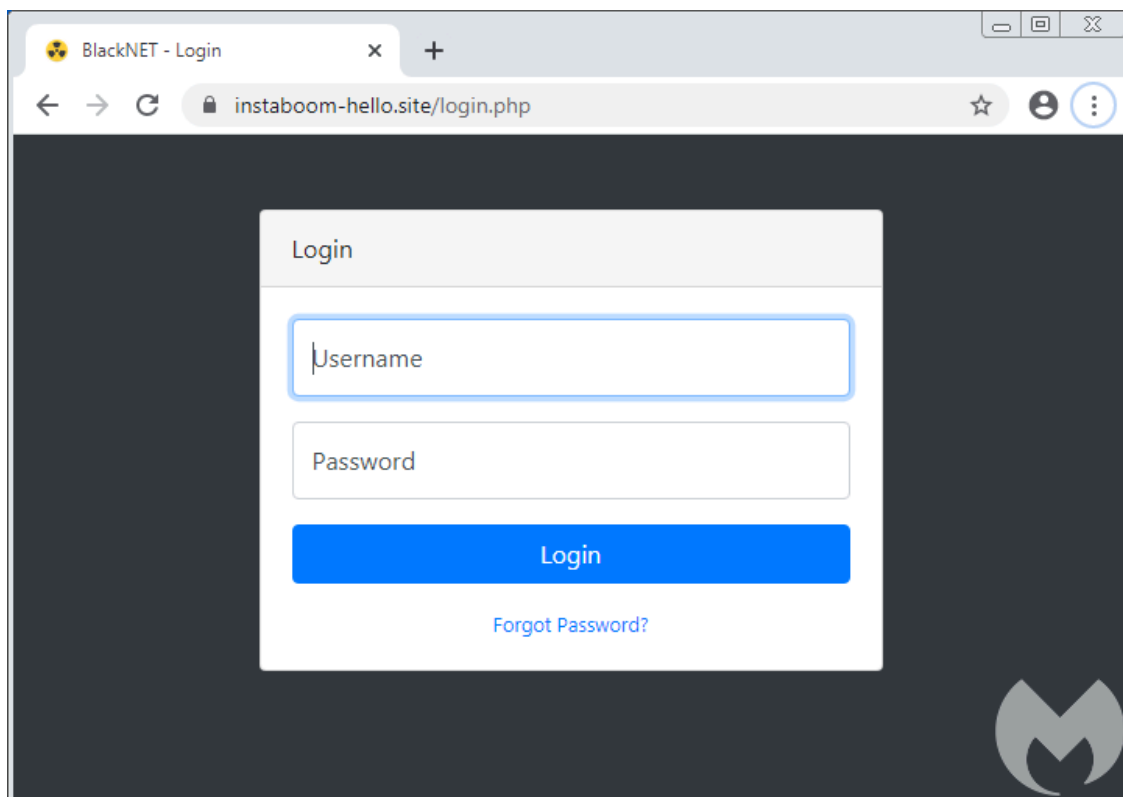
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

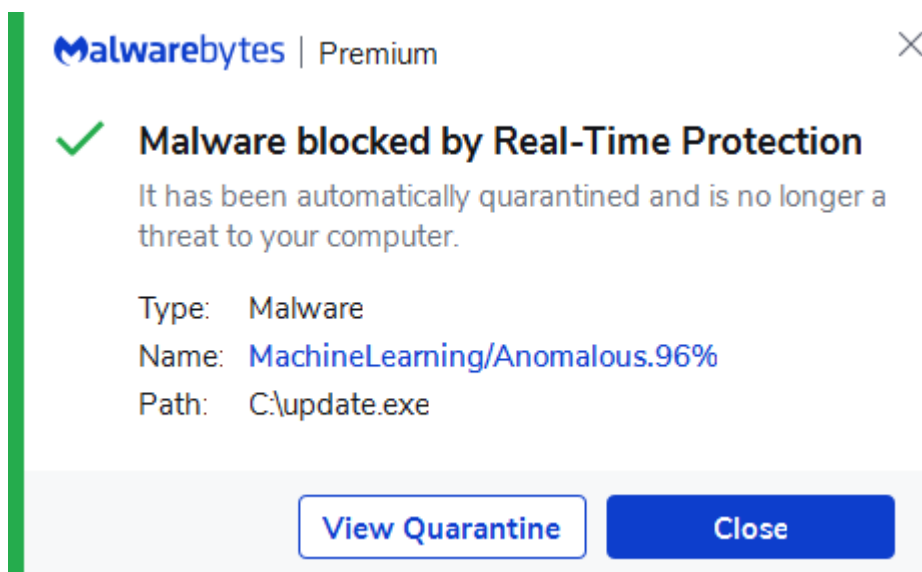
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

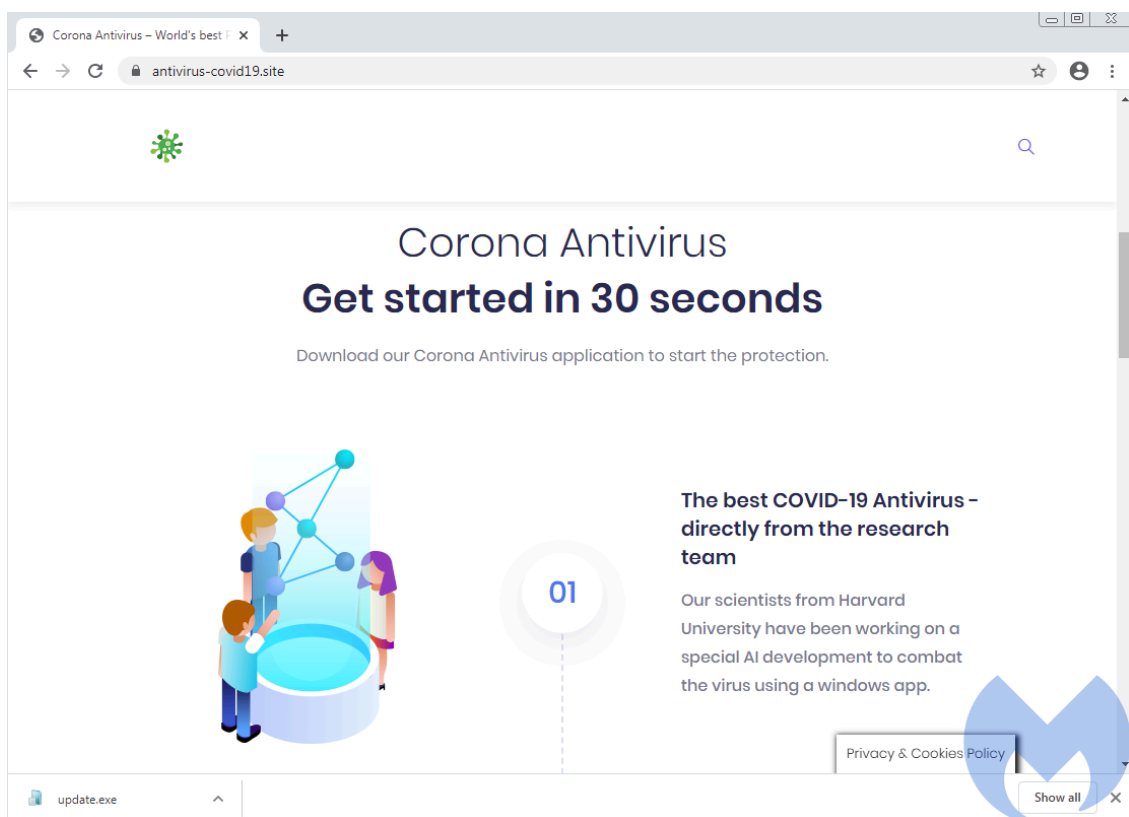
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

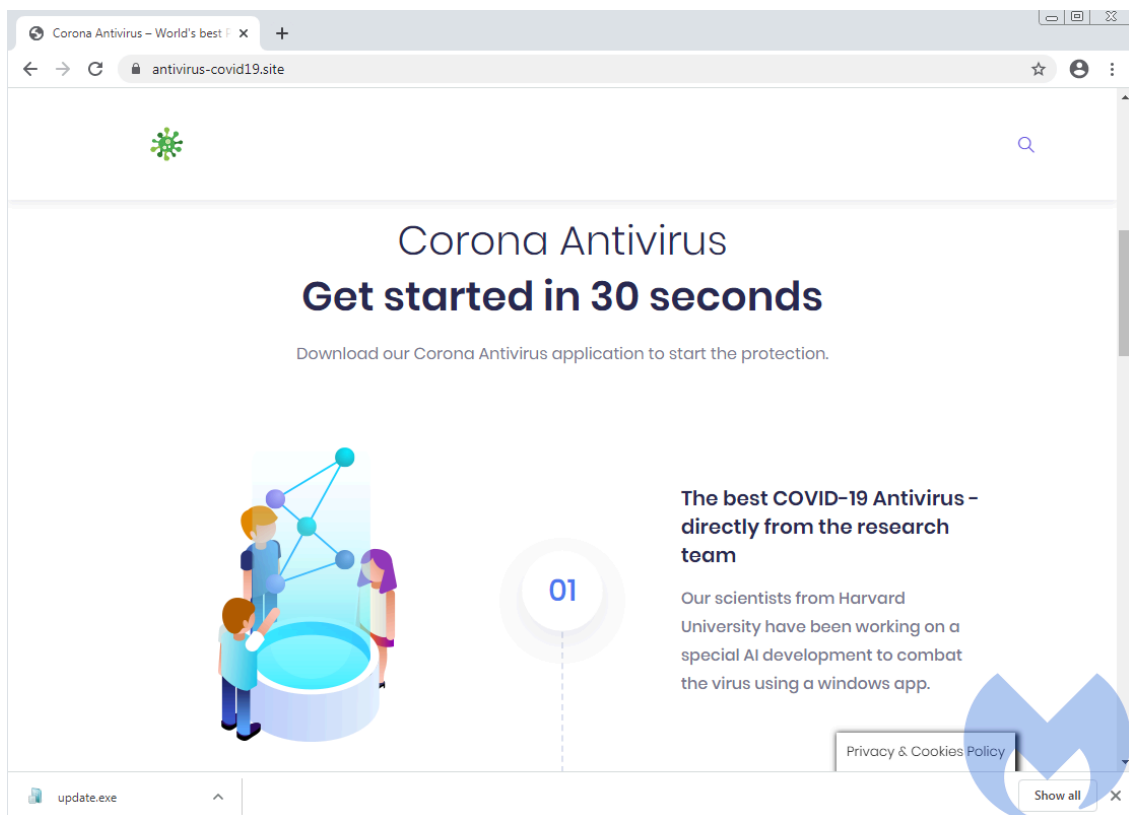
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

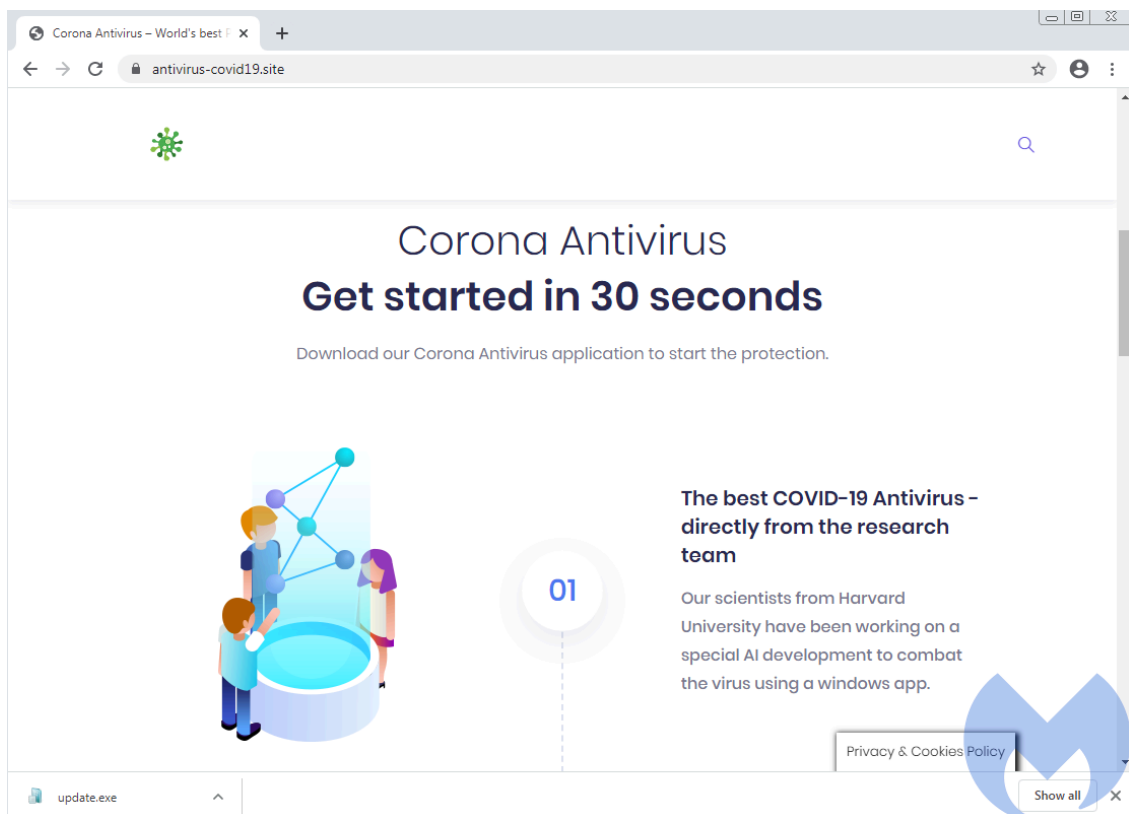
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

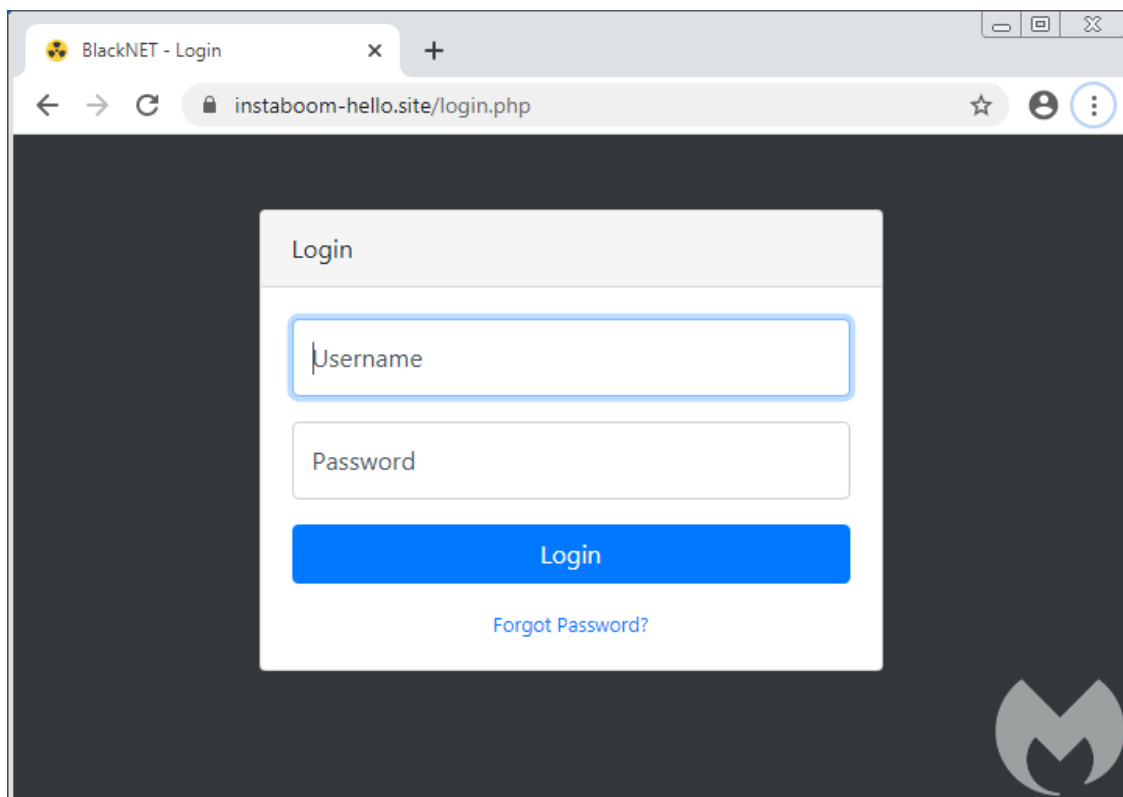


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

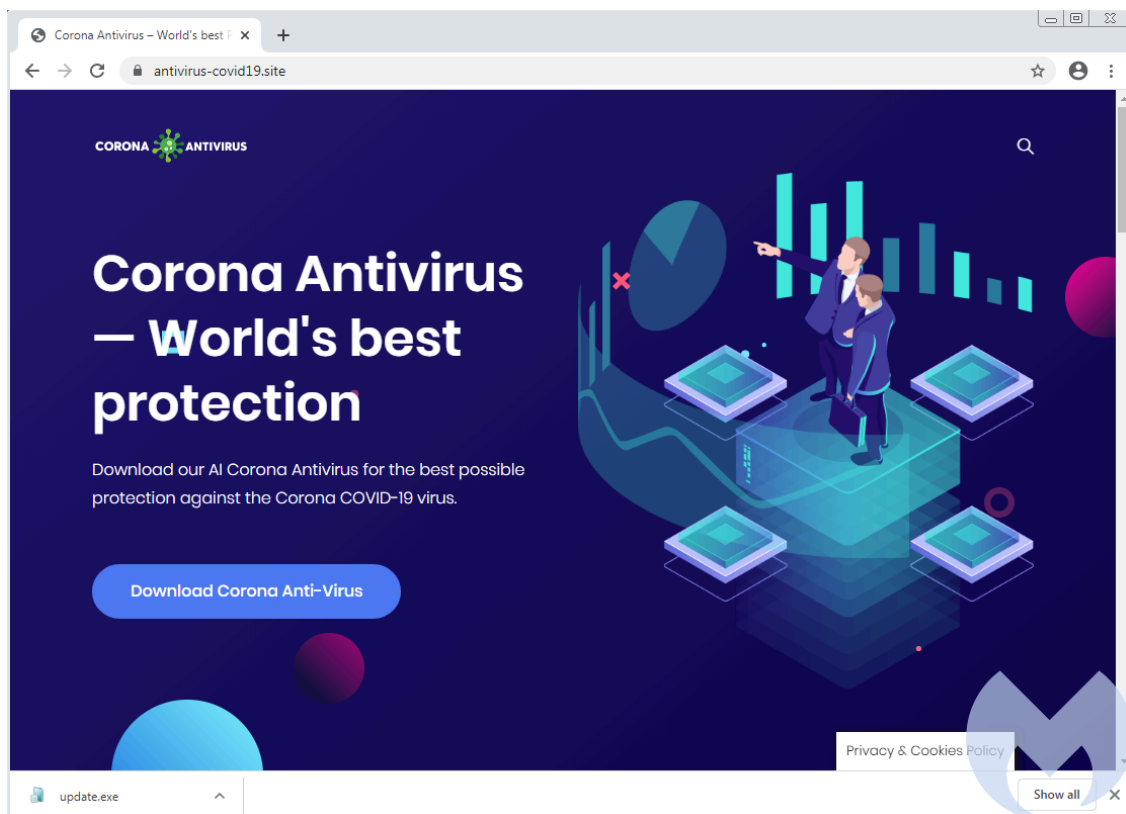
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

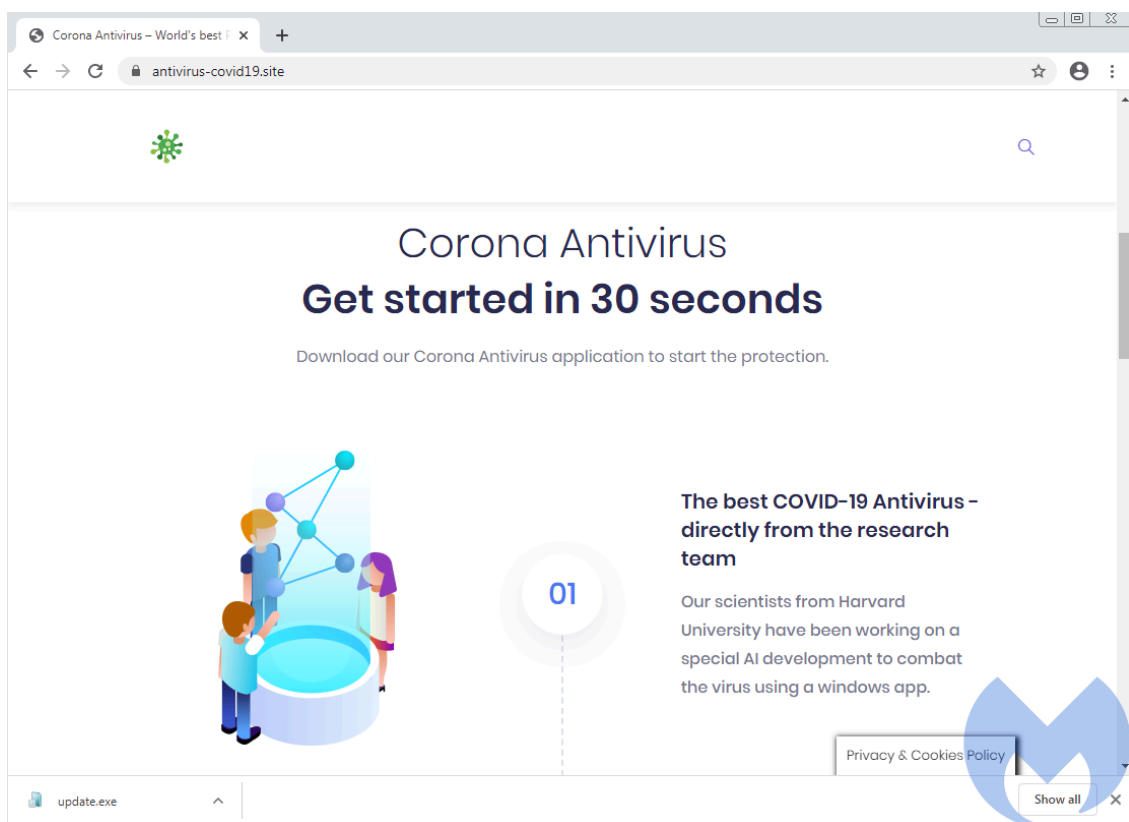
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

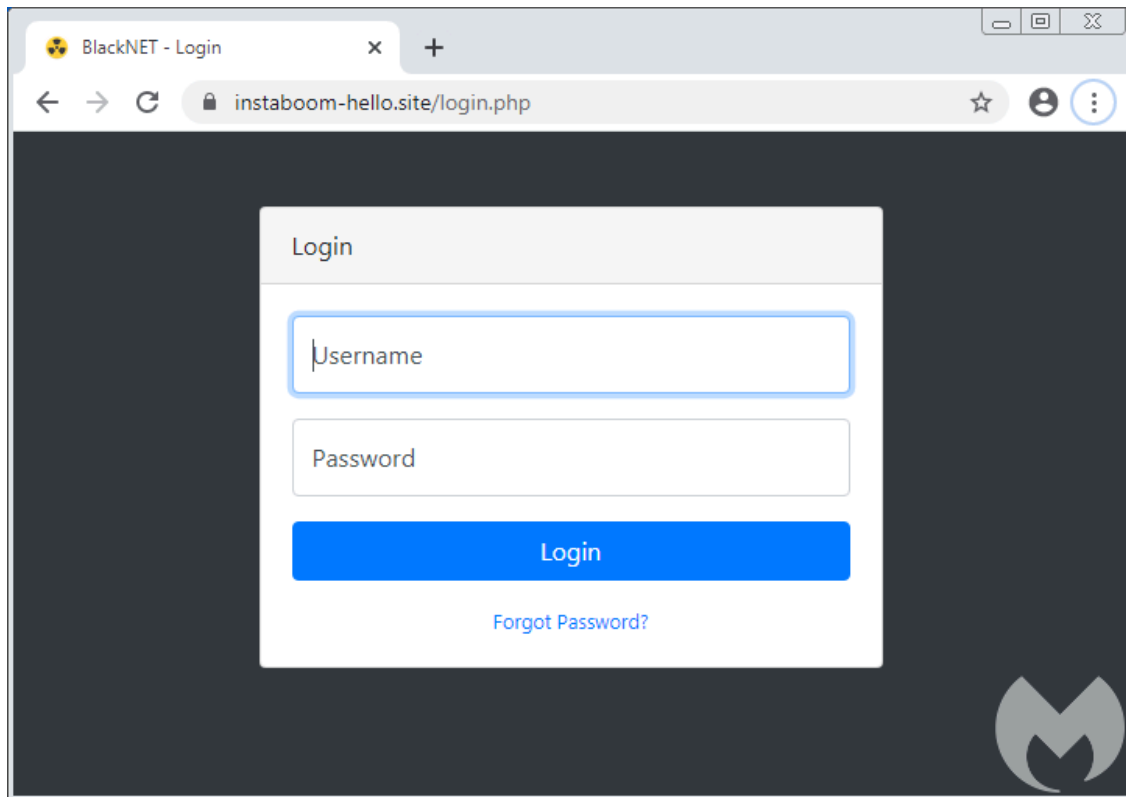


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

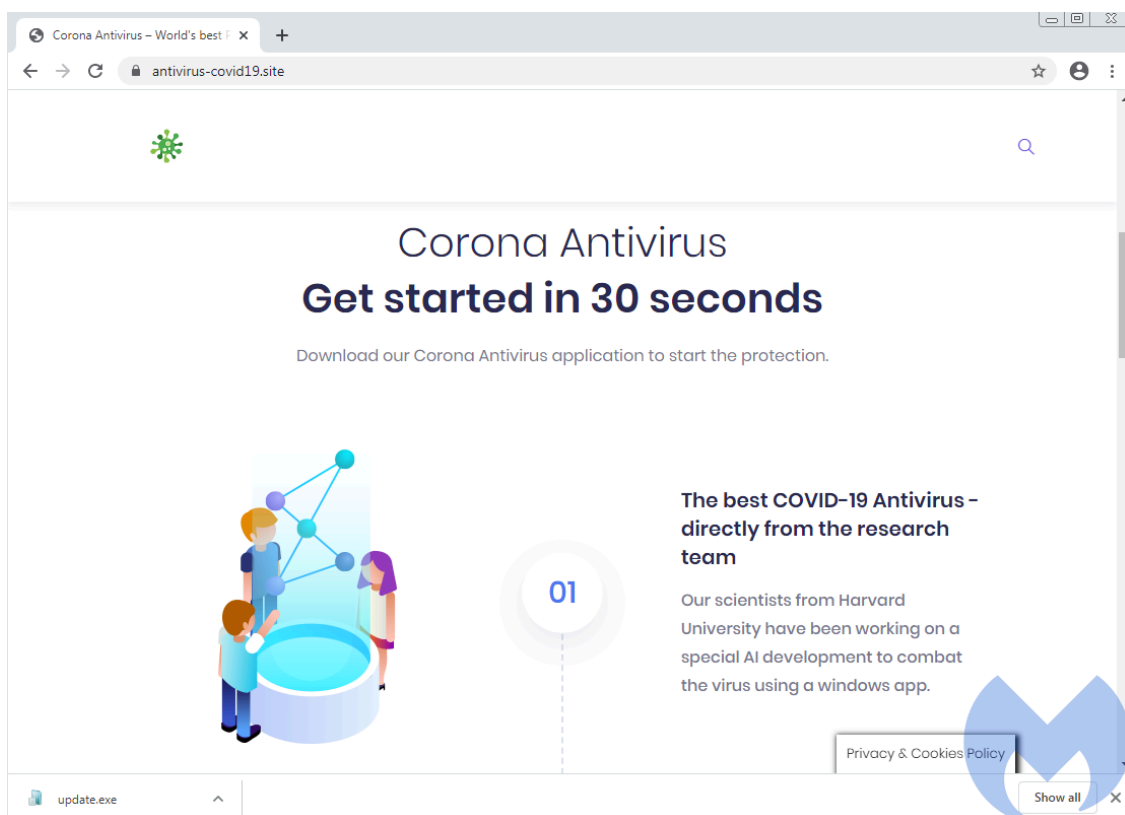
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

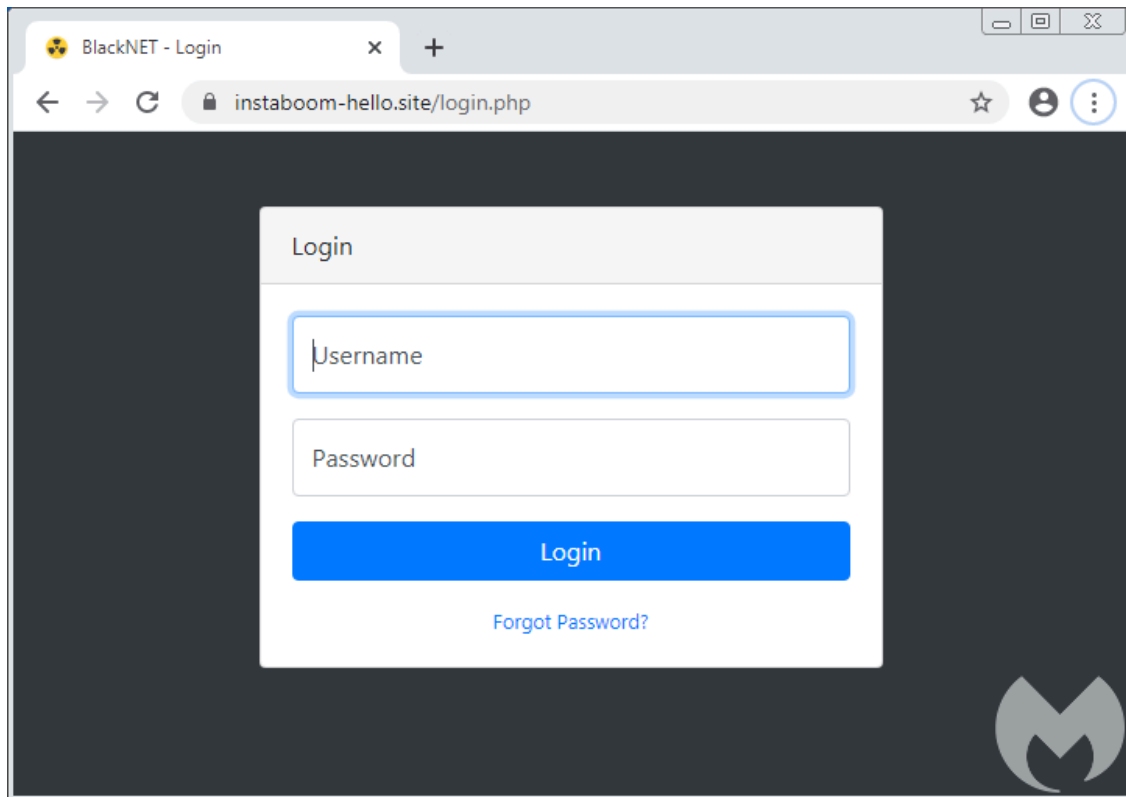


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

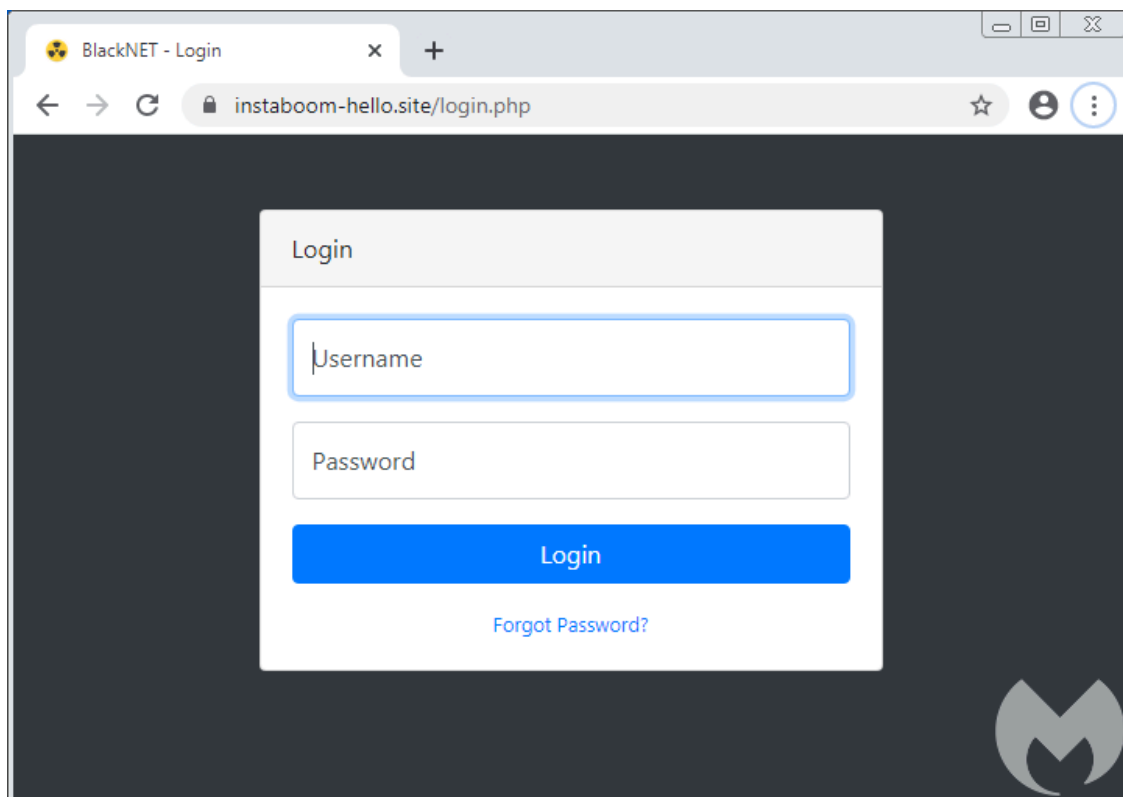
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

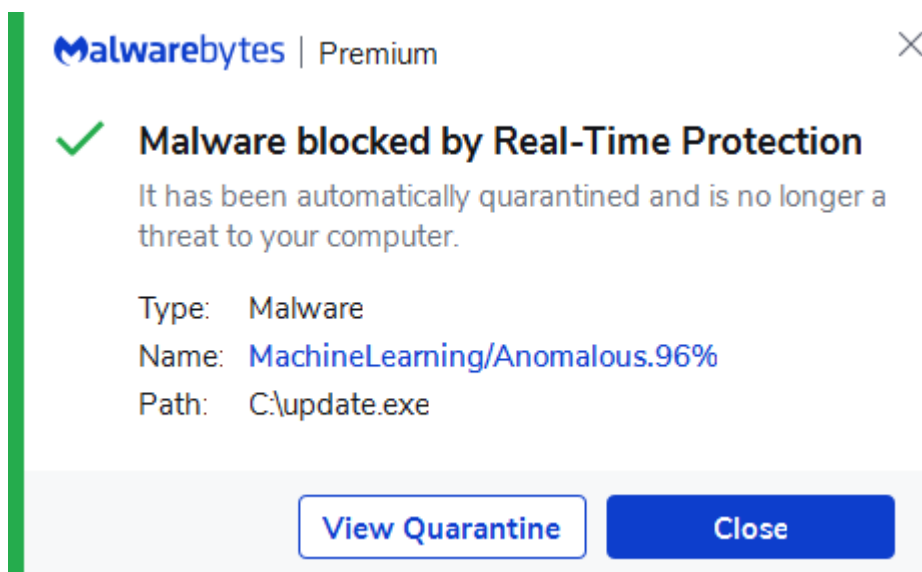
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

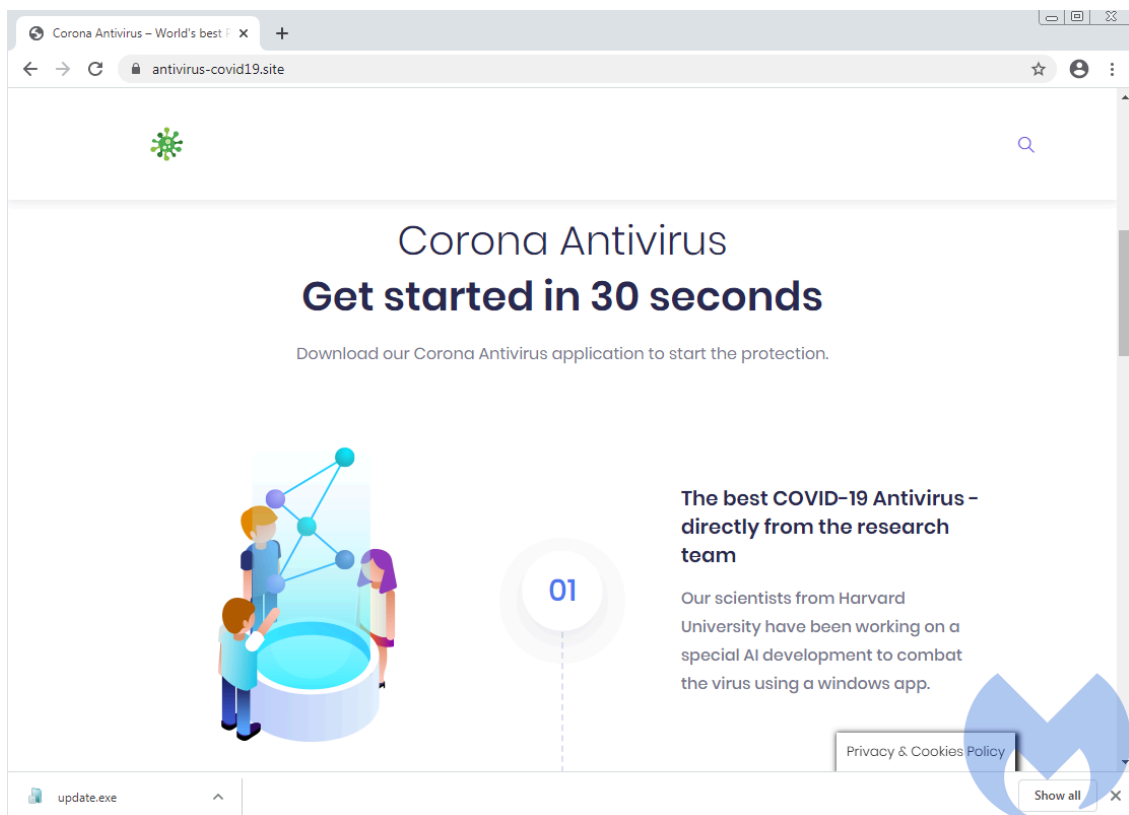
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

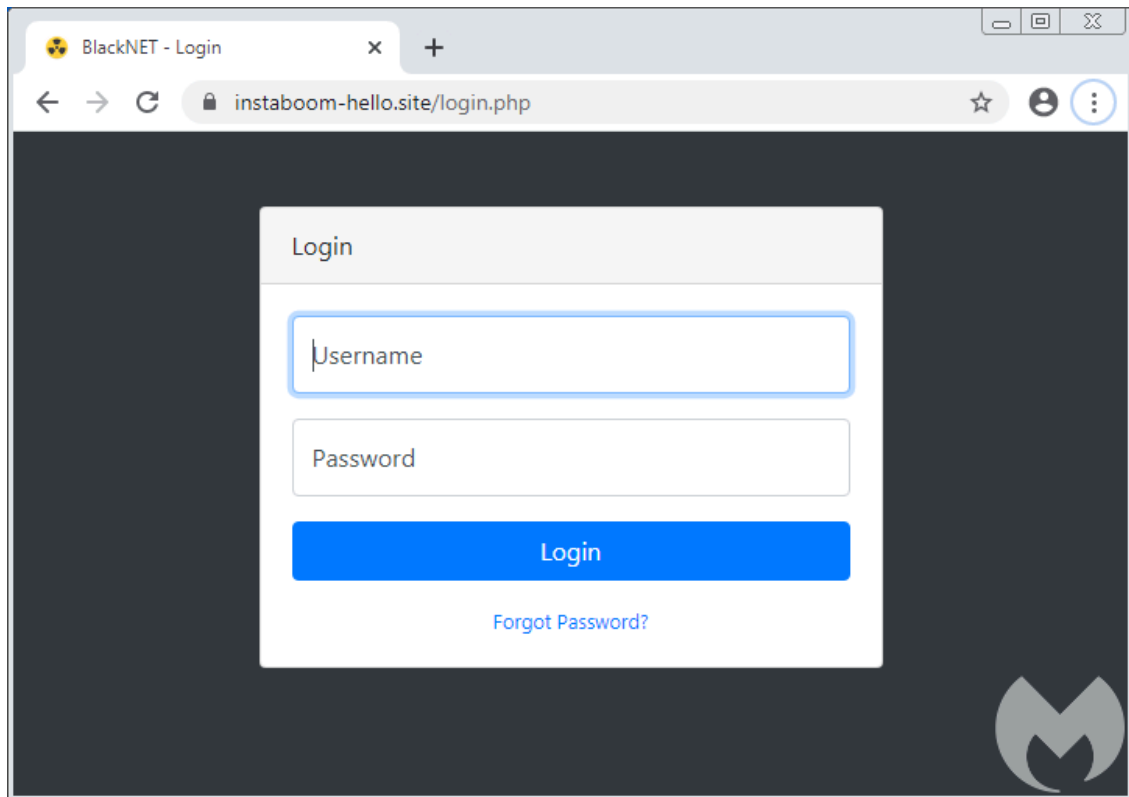


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

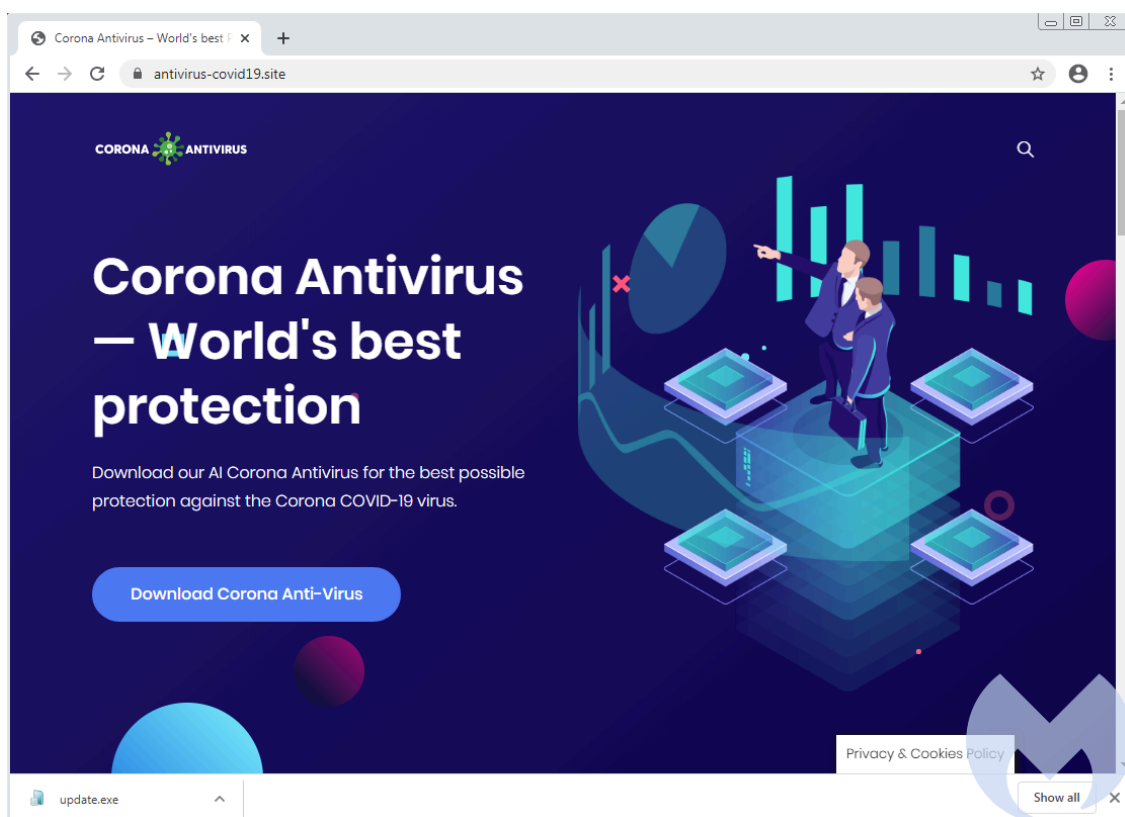
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

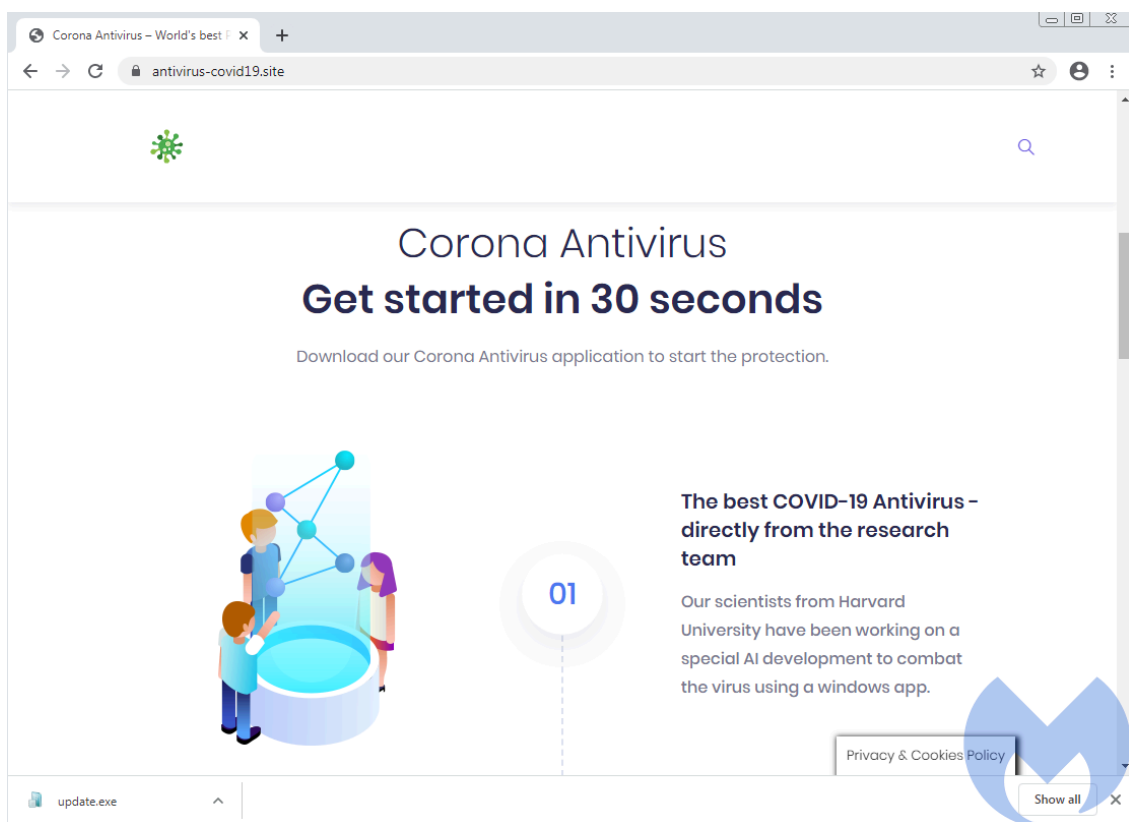
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

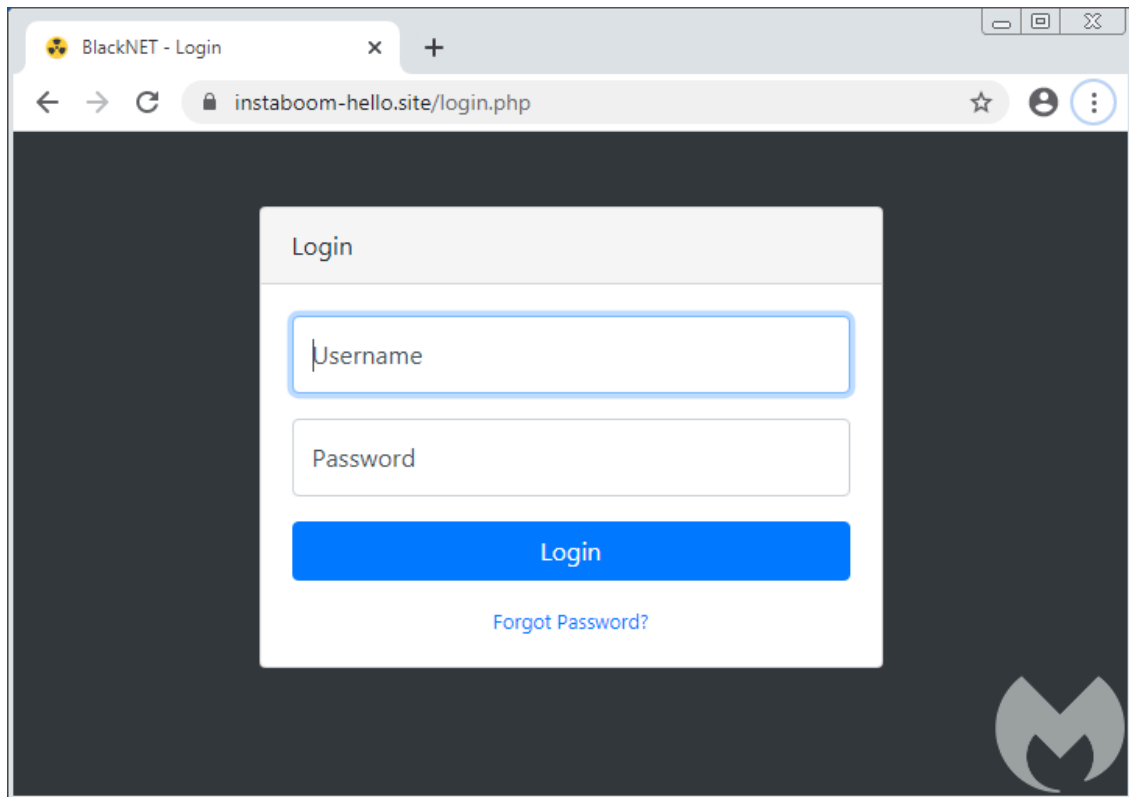


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

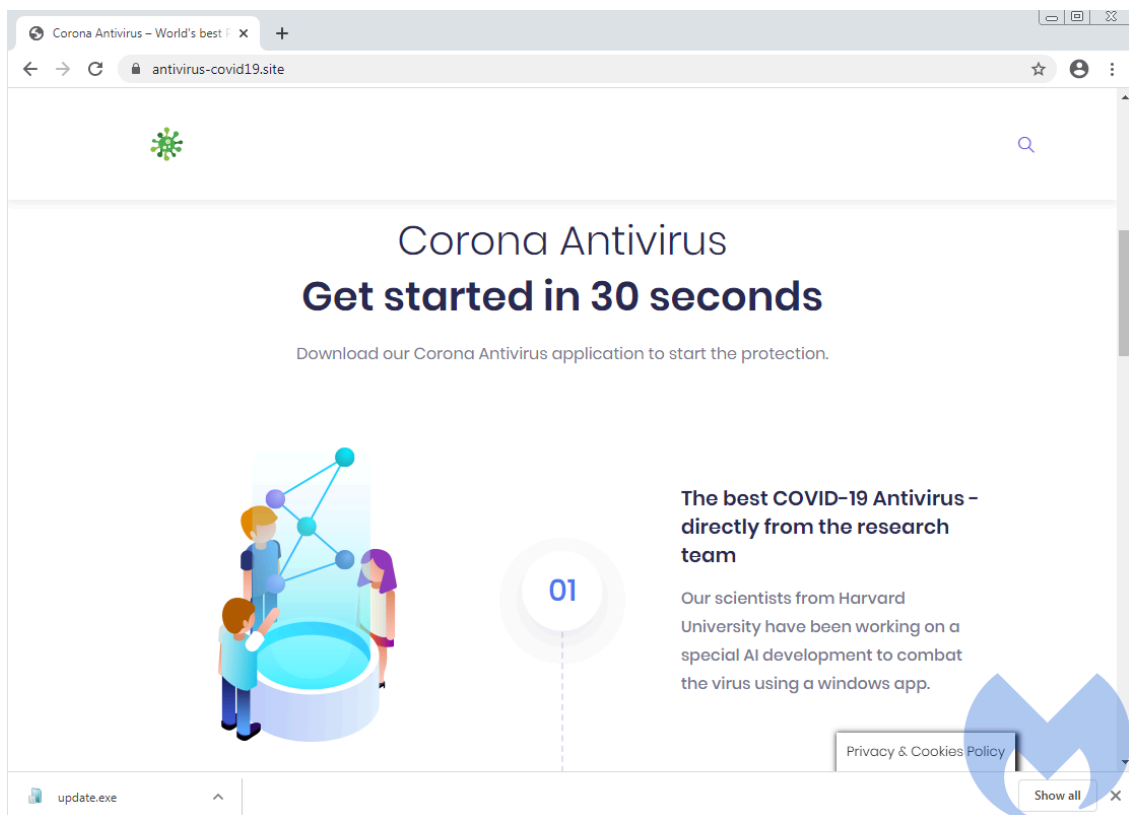
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

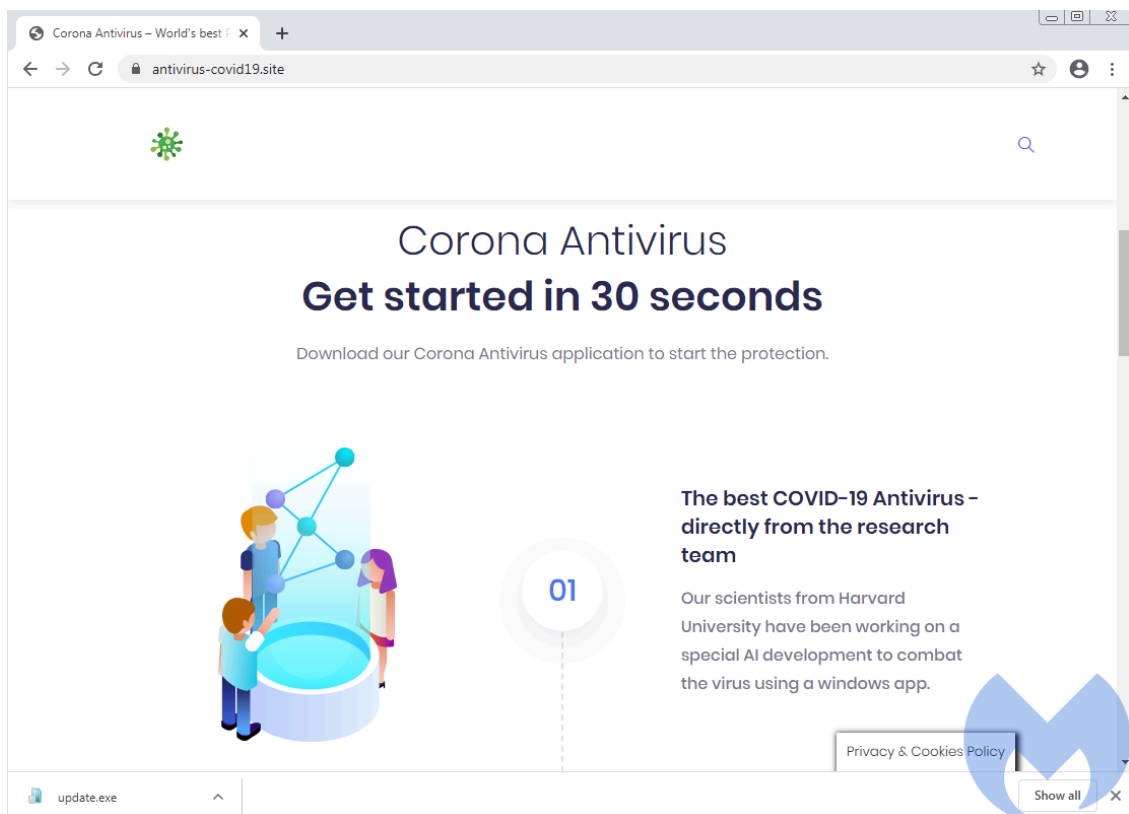
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

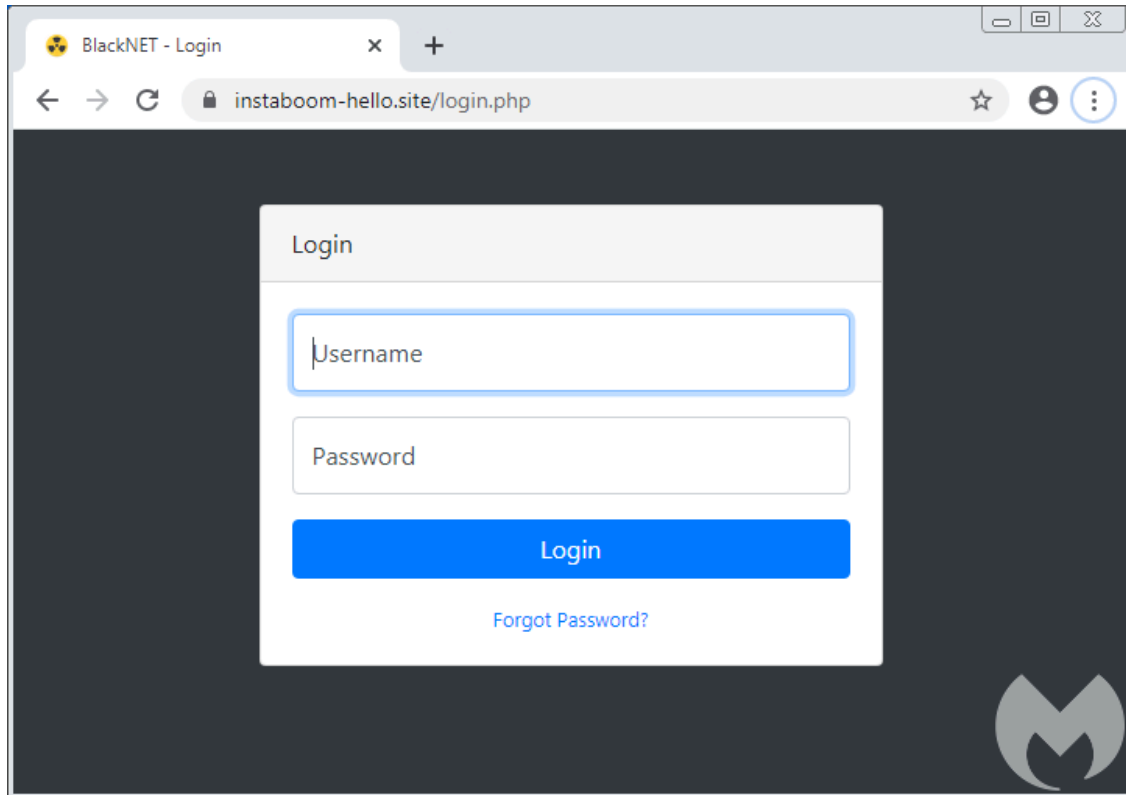


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

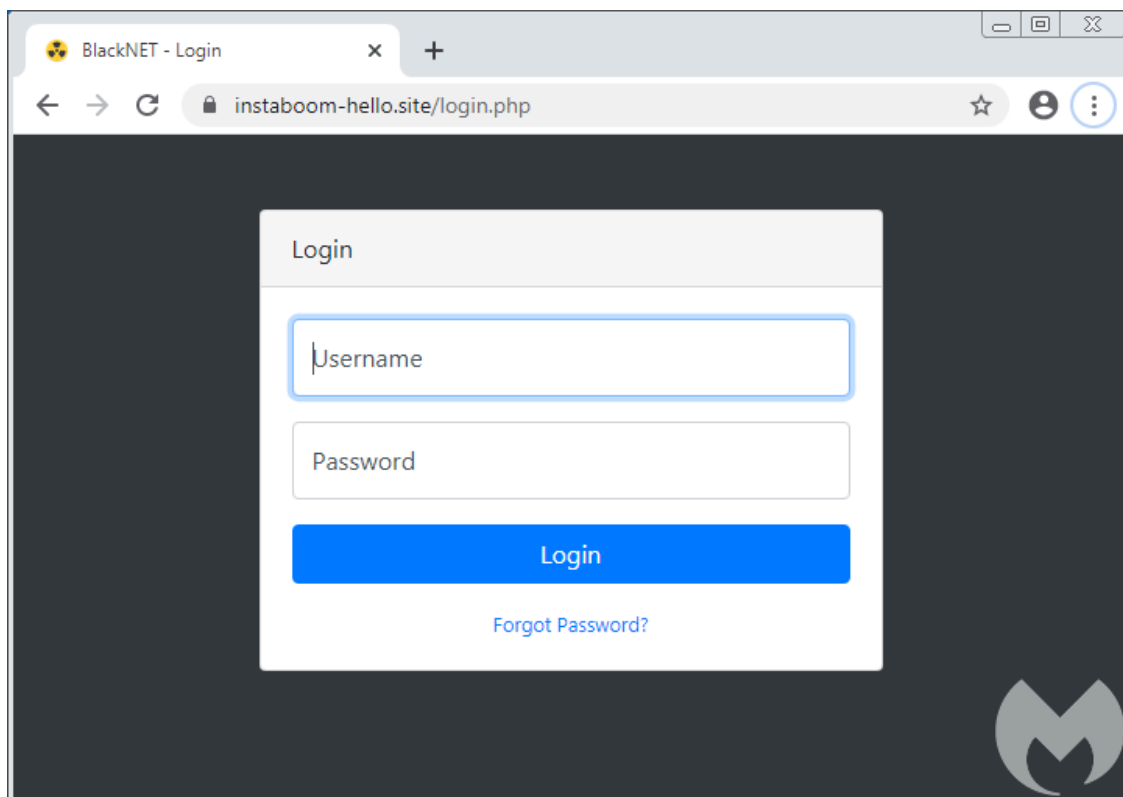
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

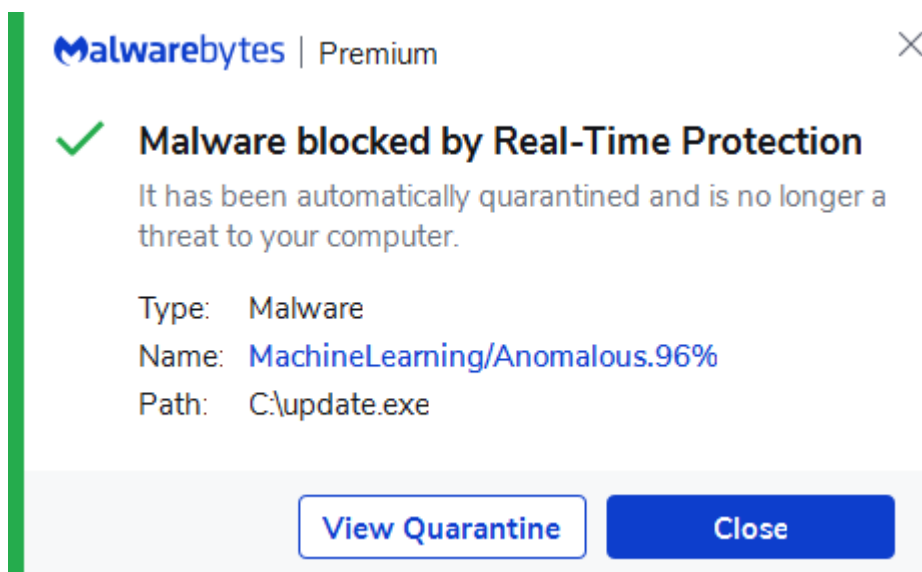
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

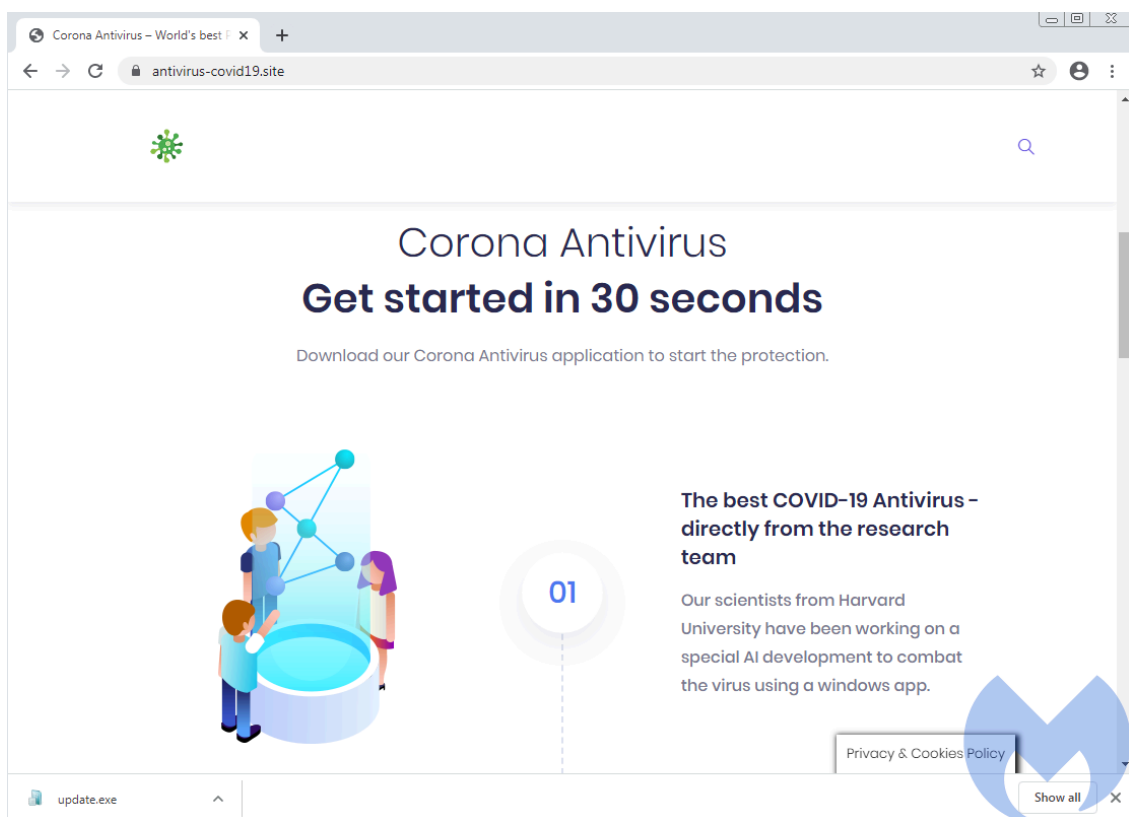
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

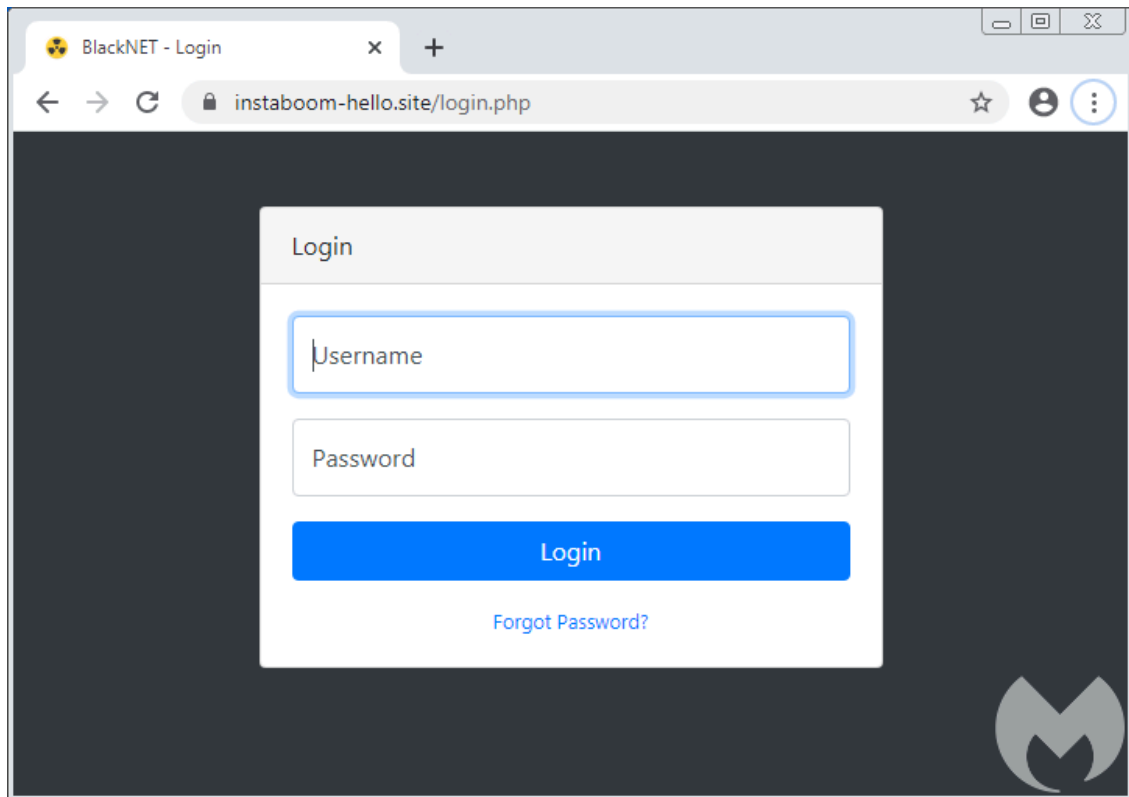


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

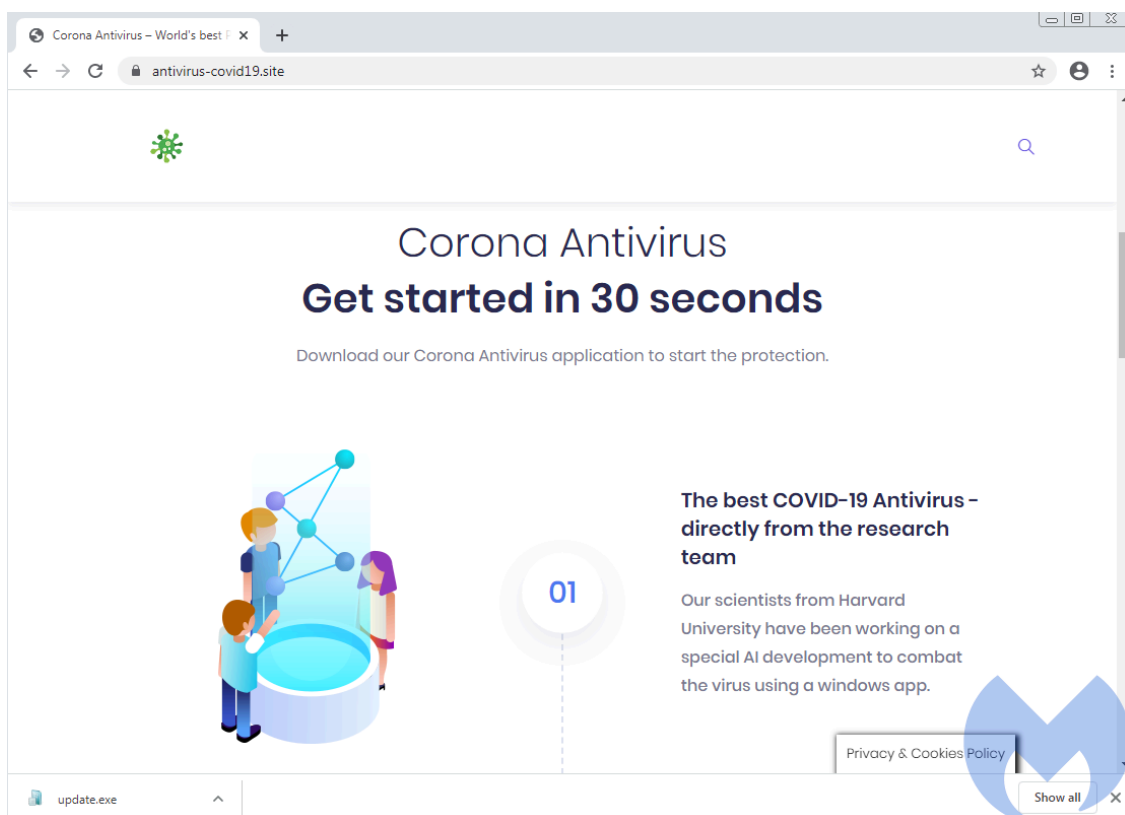
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

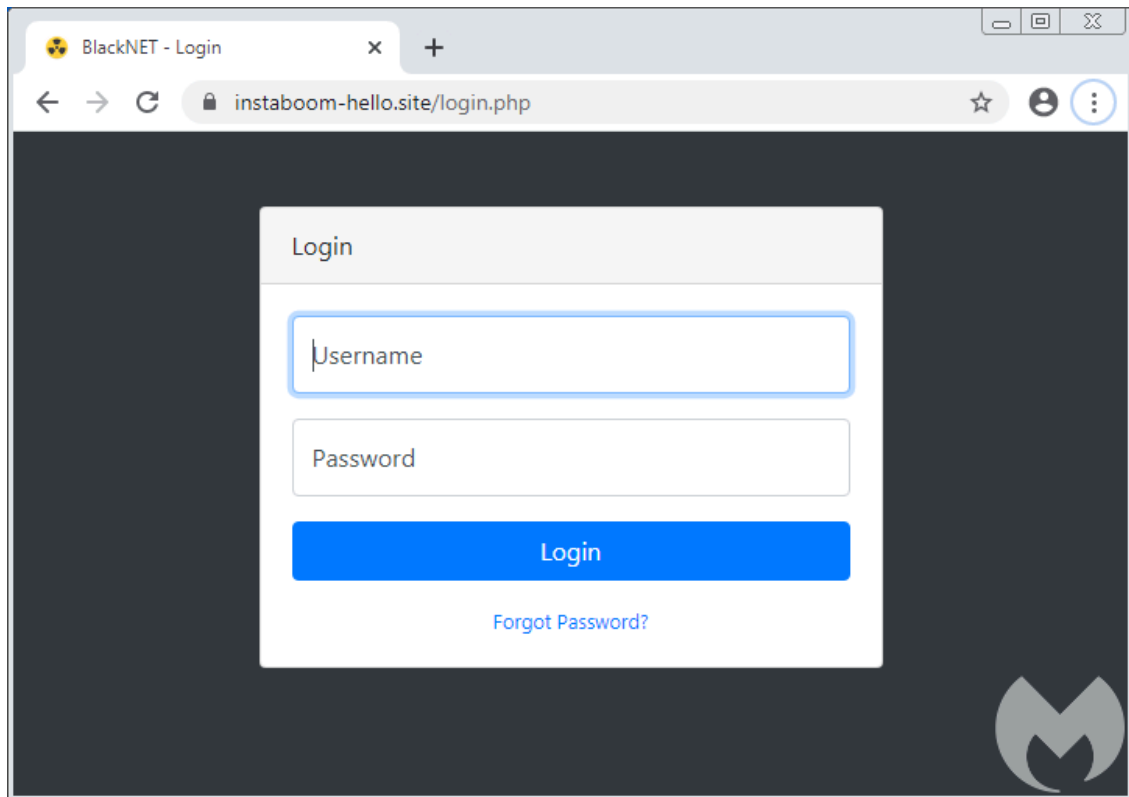


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

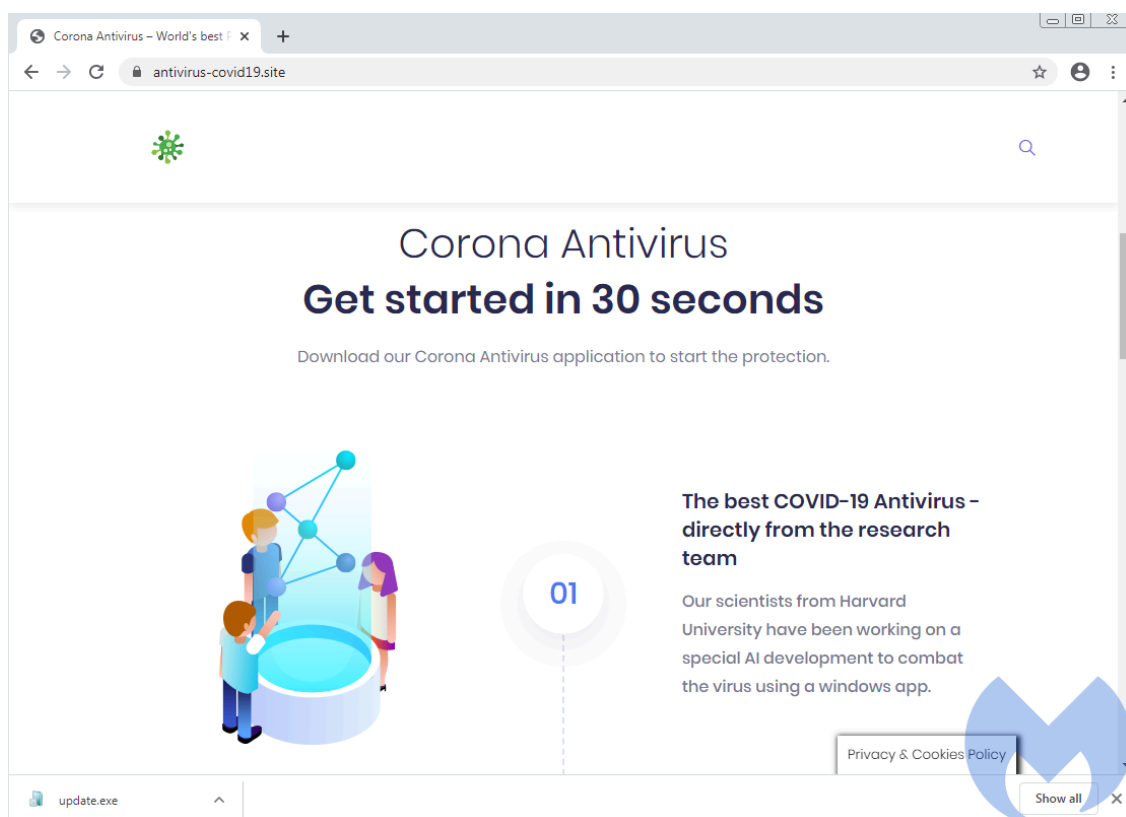
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

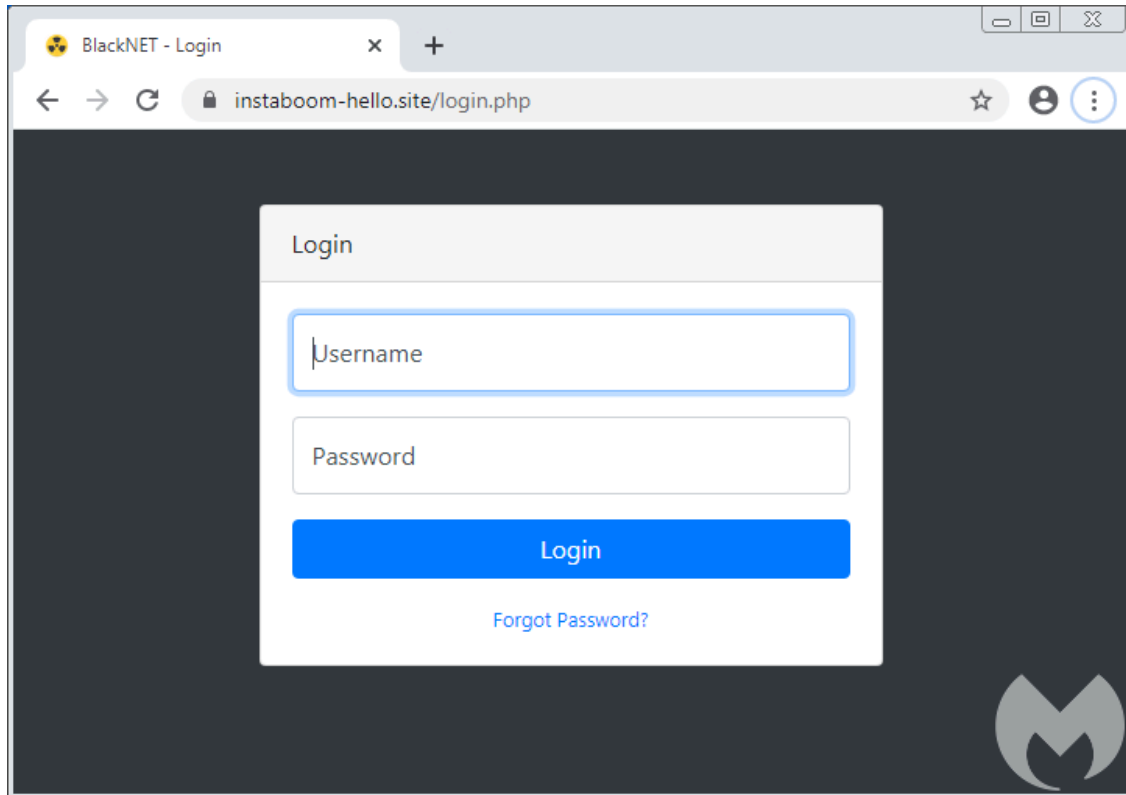


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

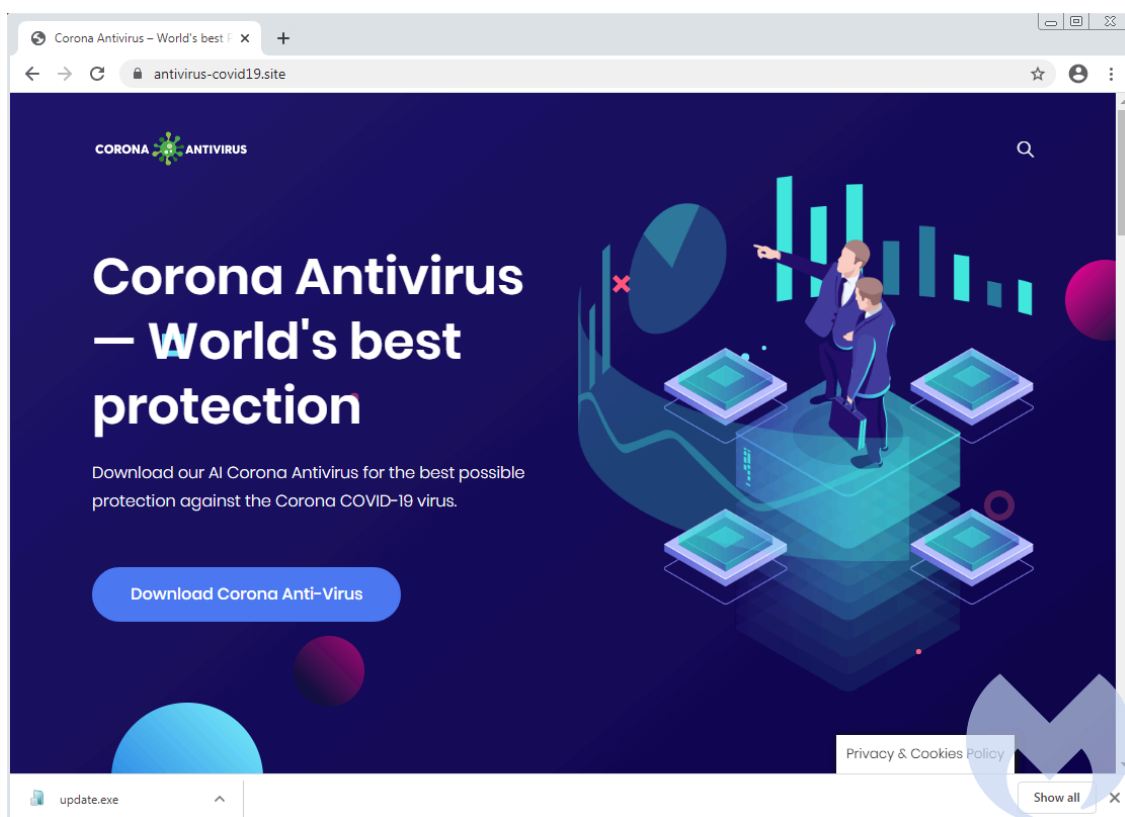
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

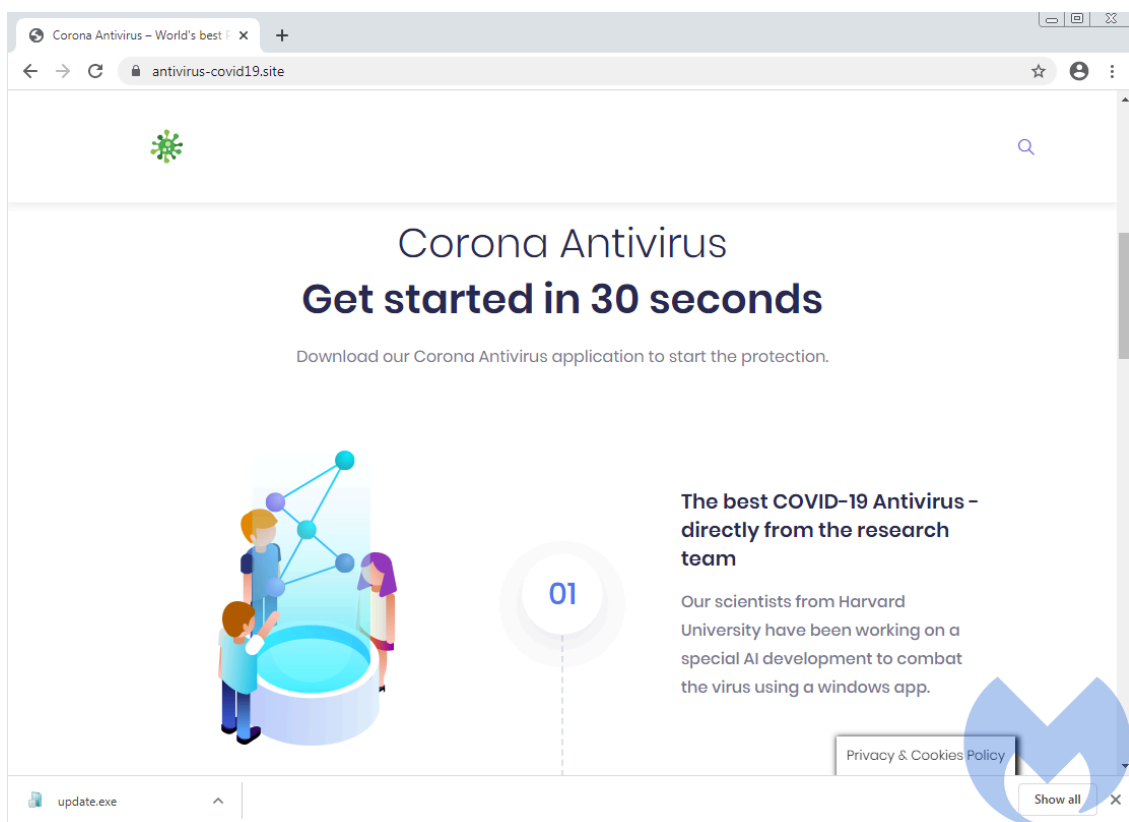
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

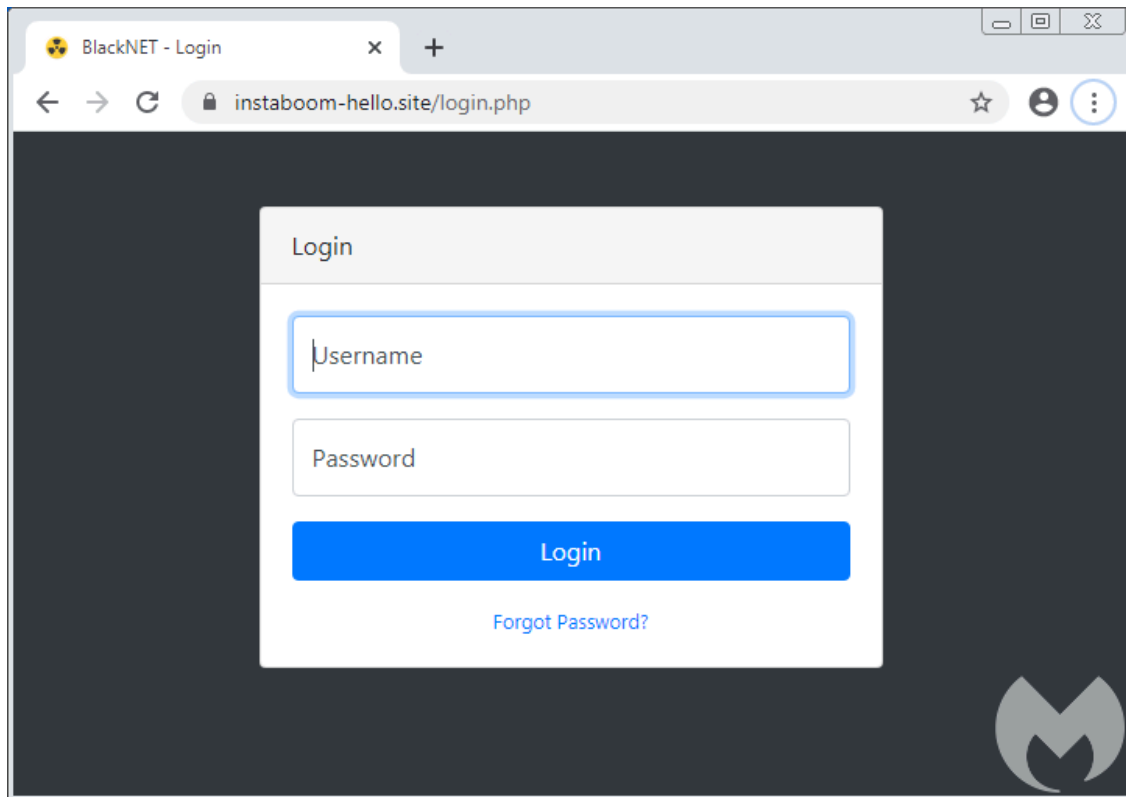


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

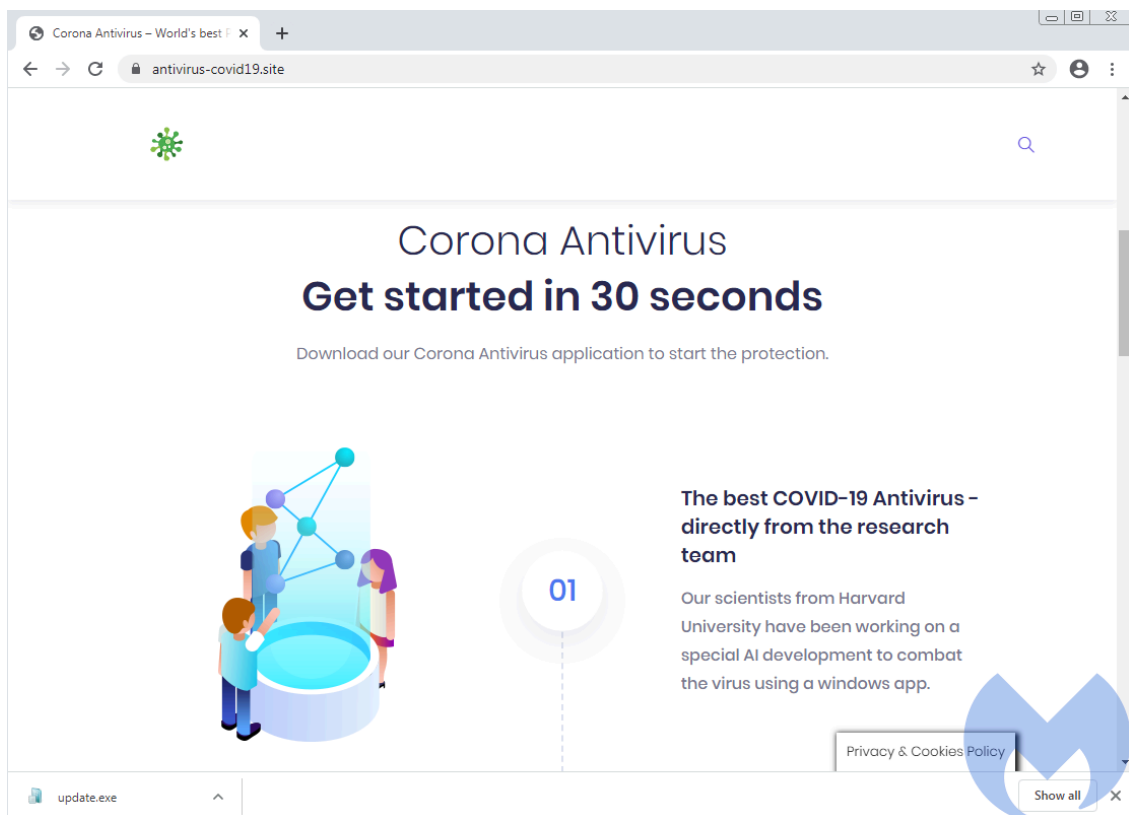
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

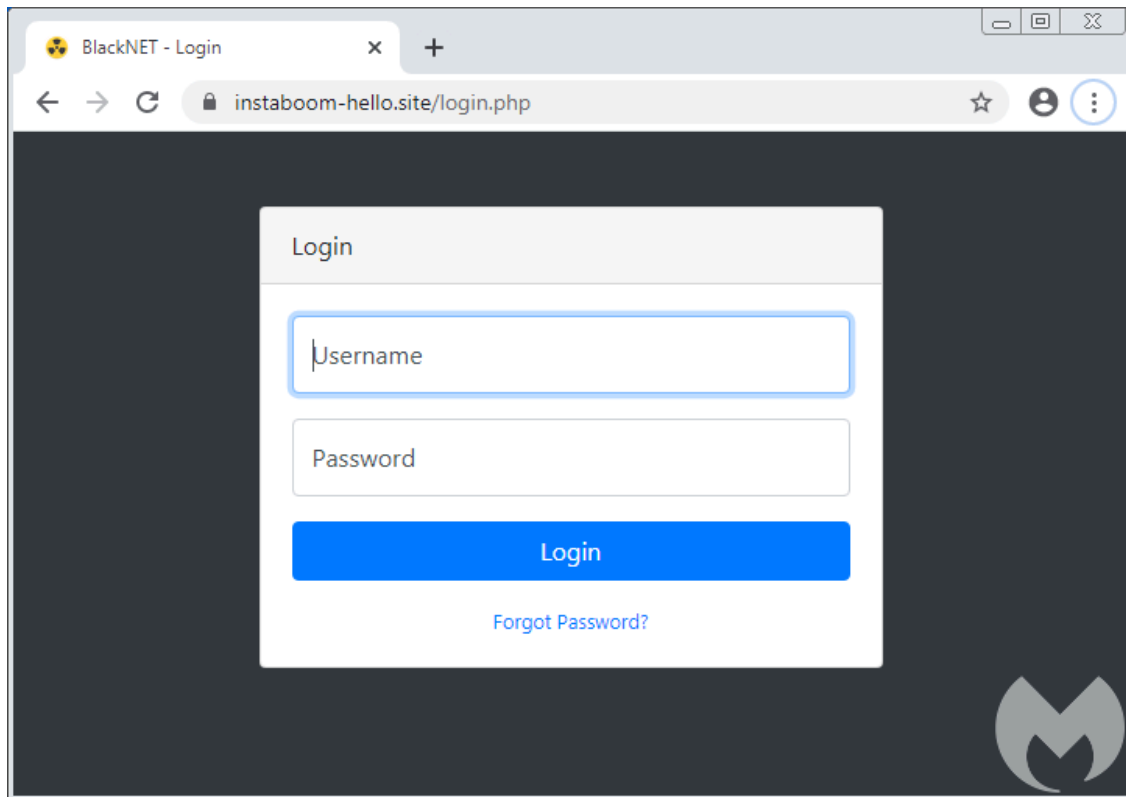


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window has a green vertical bar on the left. It features the Malwarebytes Premium logo and a close button (X). A green checkmark is next to the heading 'Malware blocked by Real-Time Protection'. Below this, it states 'It has been automatically quarantined and is no longer a threat to your computer.' The details listed are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

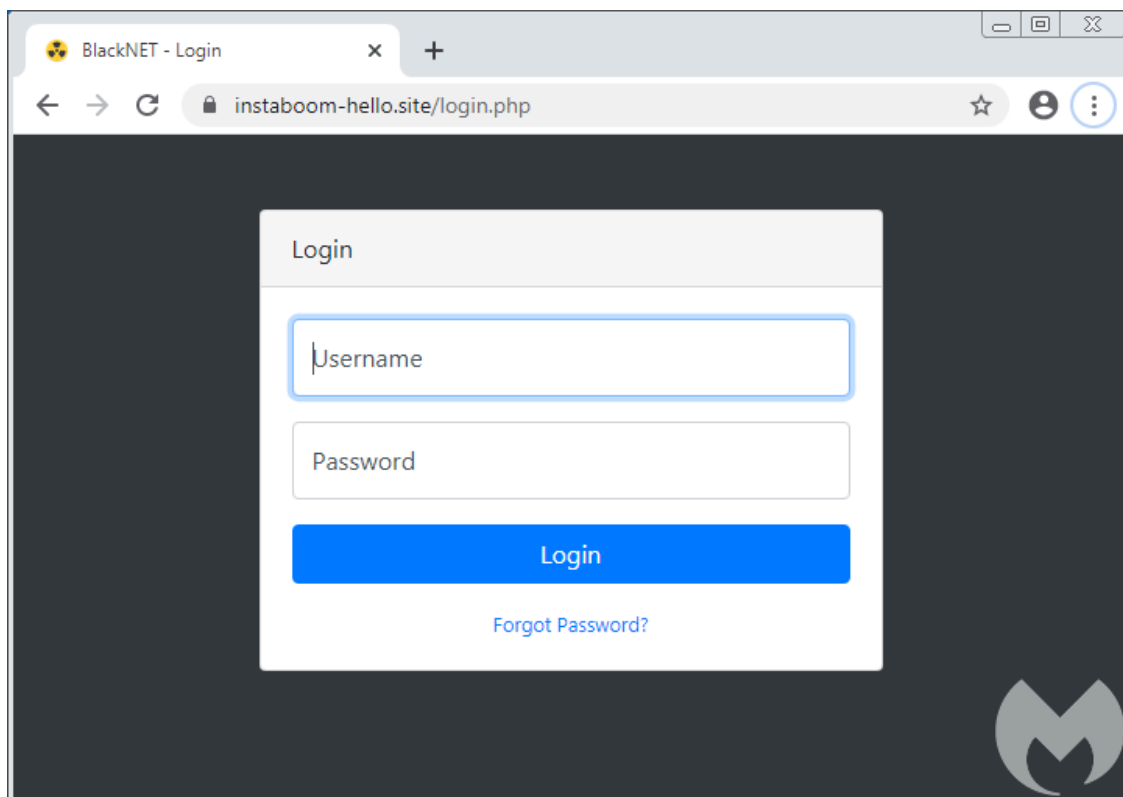
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

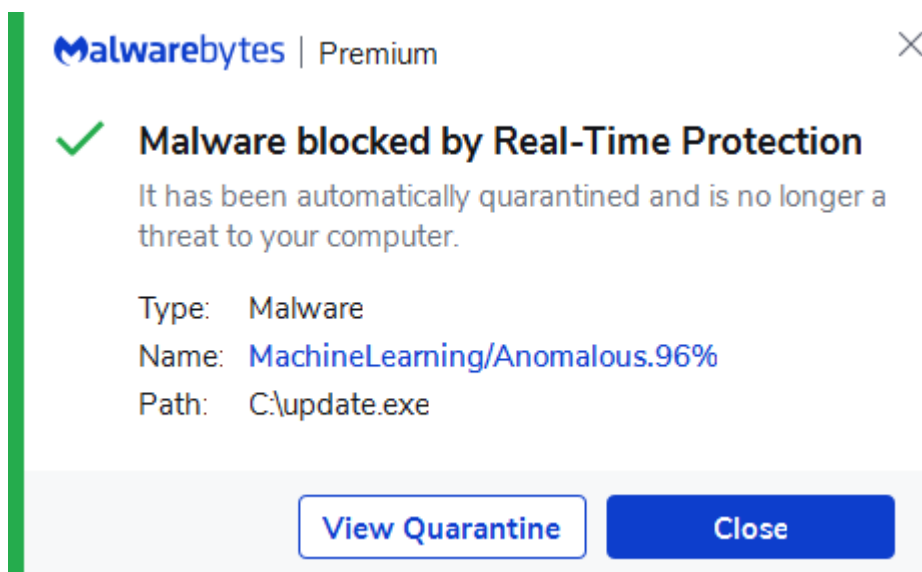
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

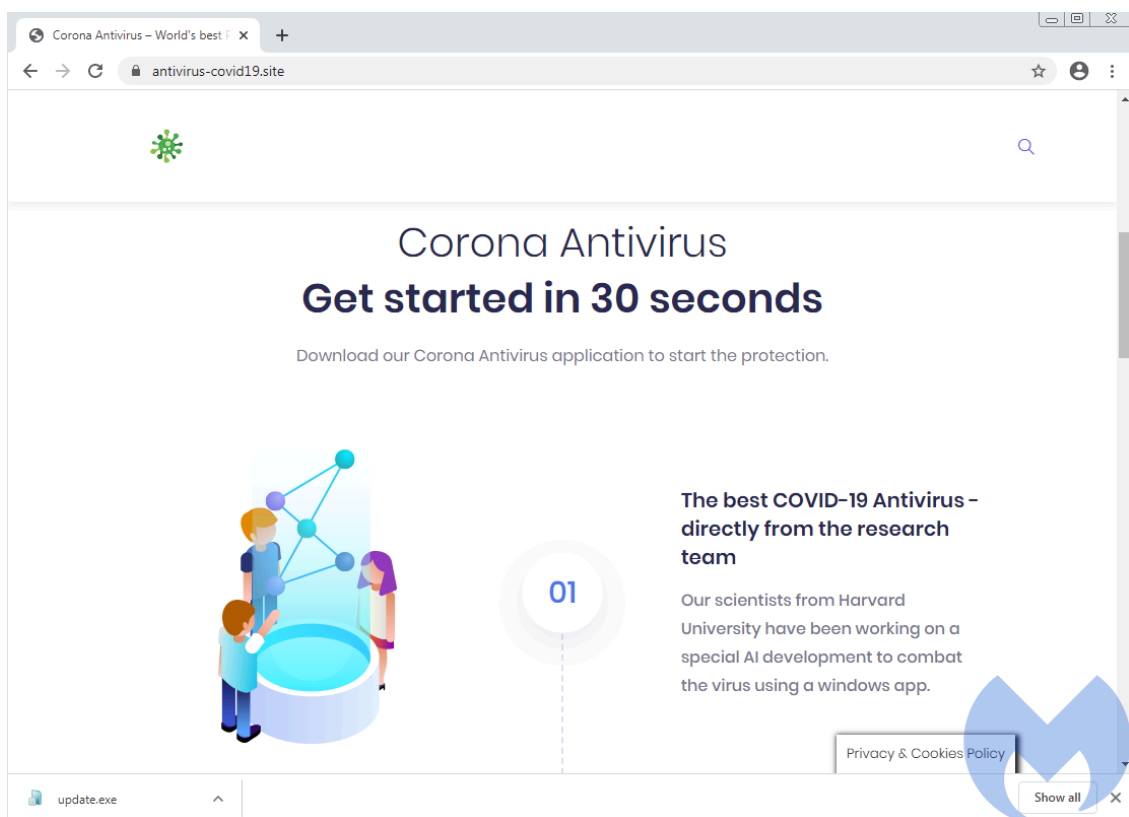
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

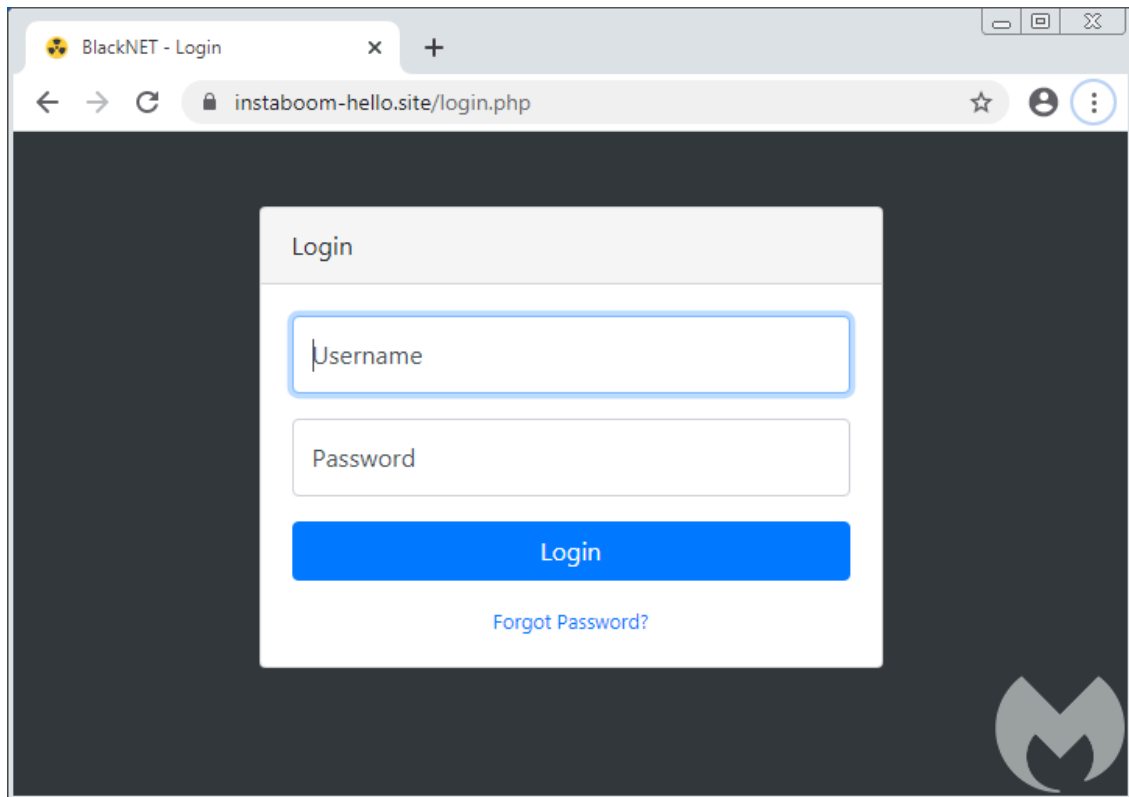


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

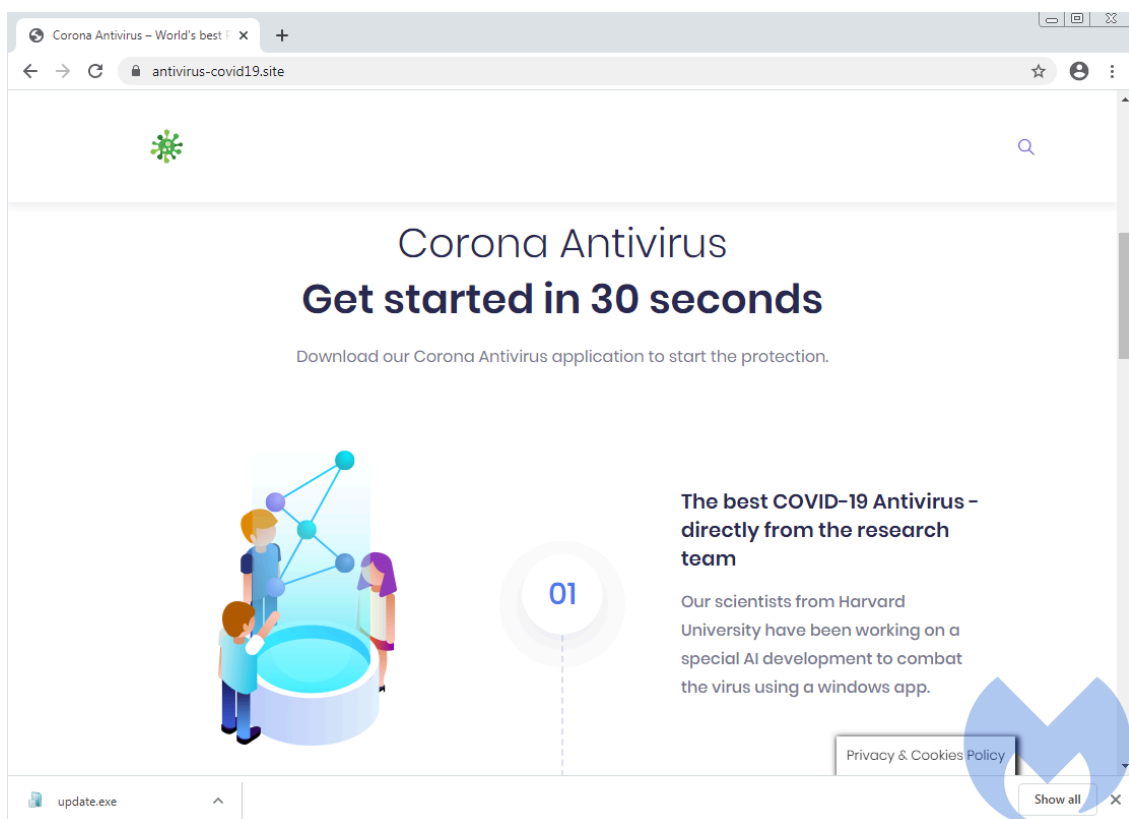
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

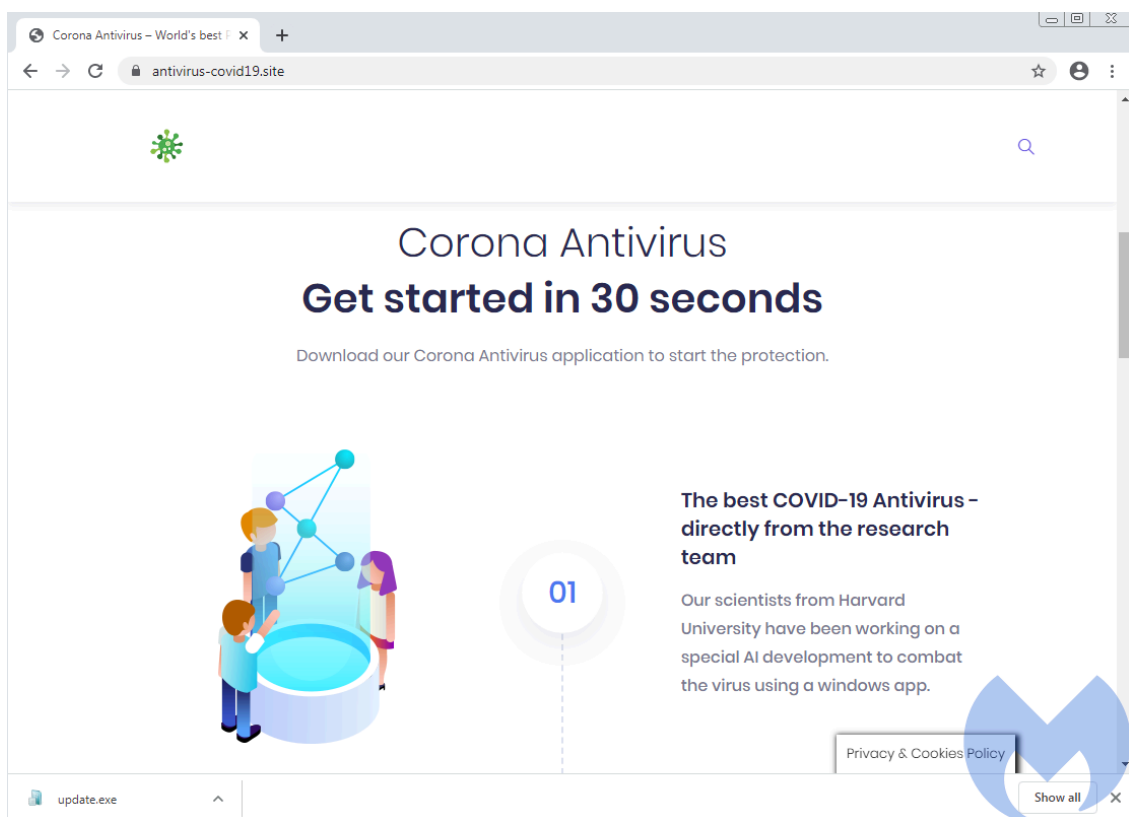
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

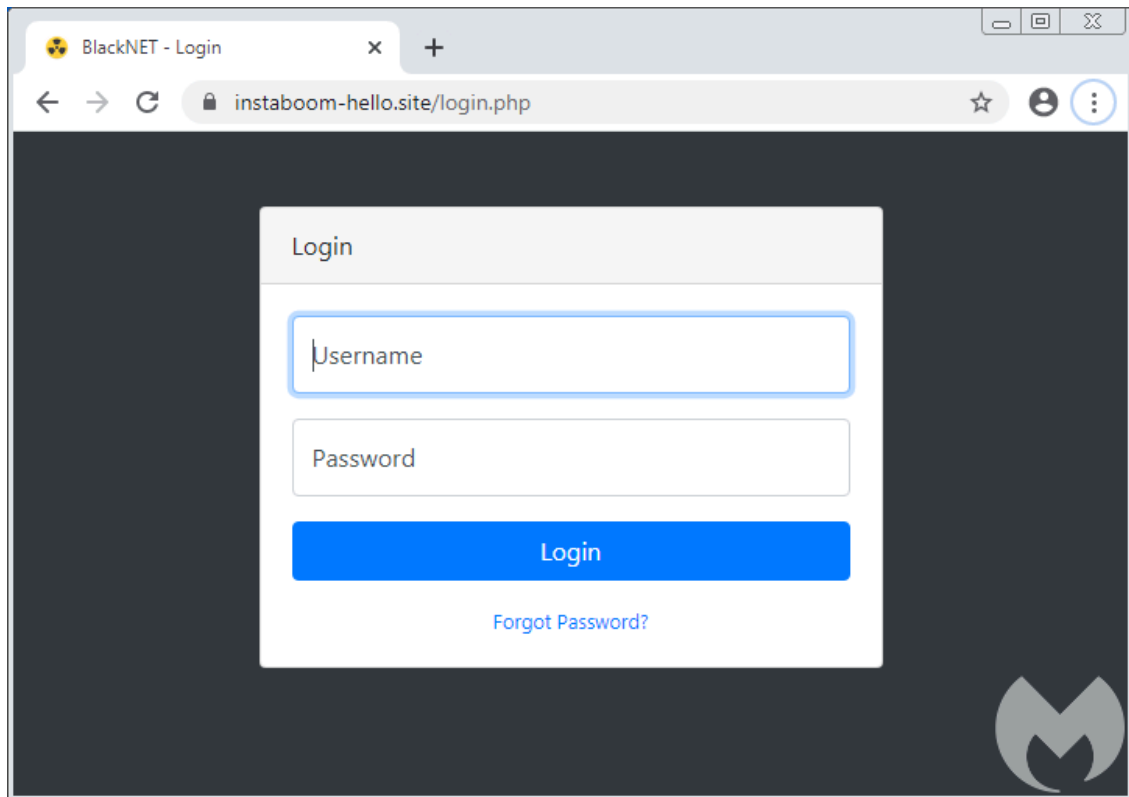


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

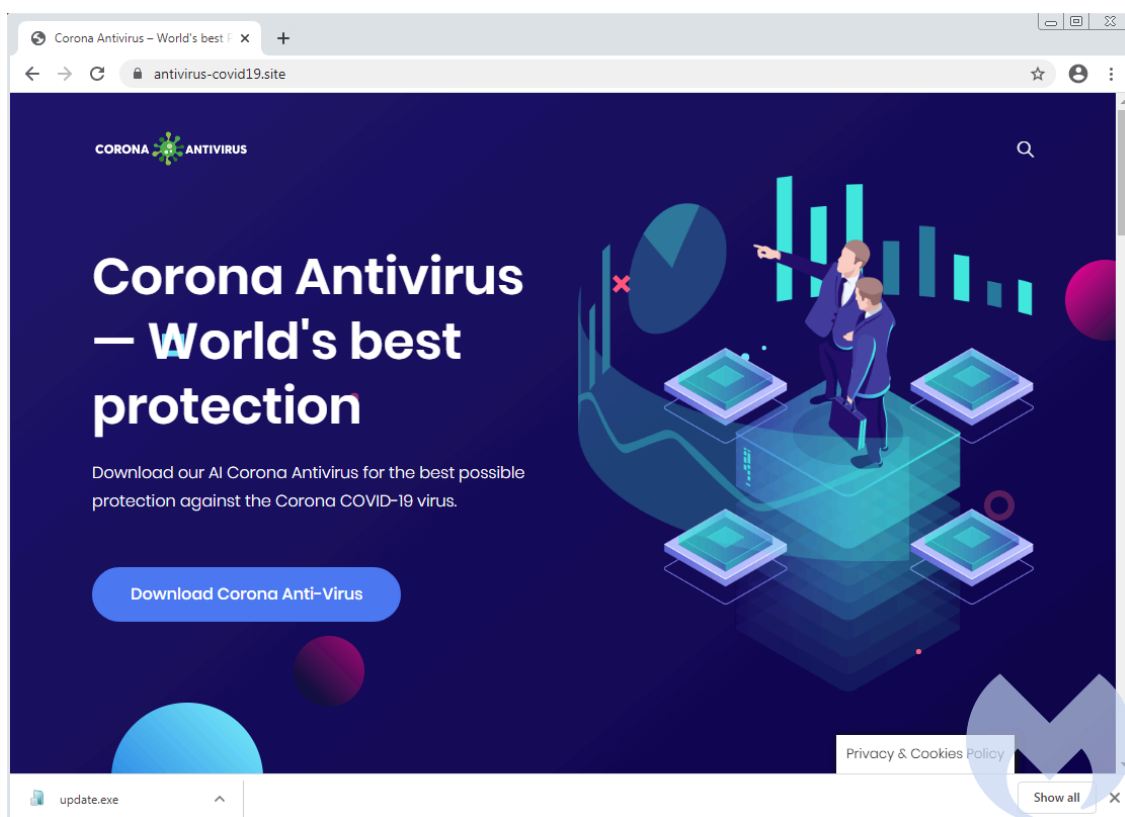
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

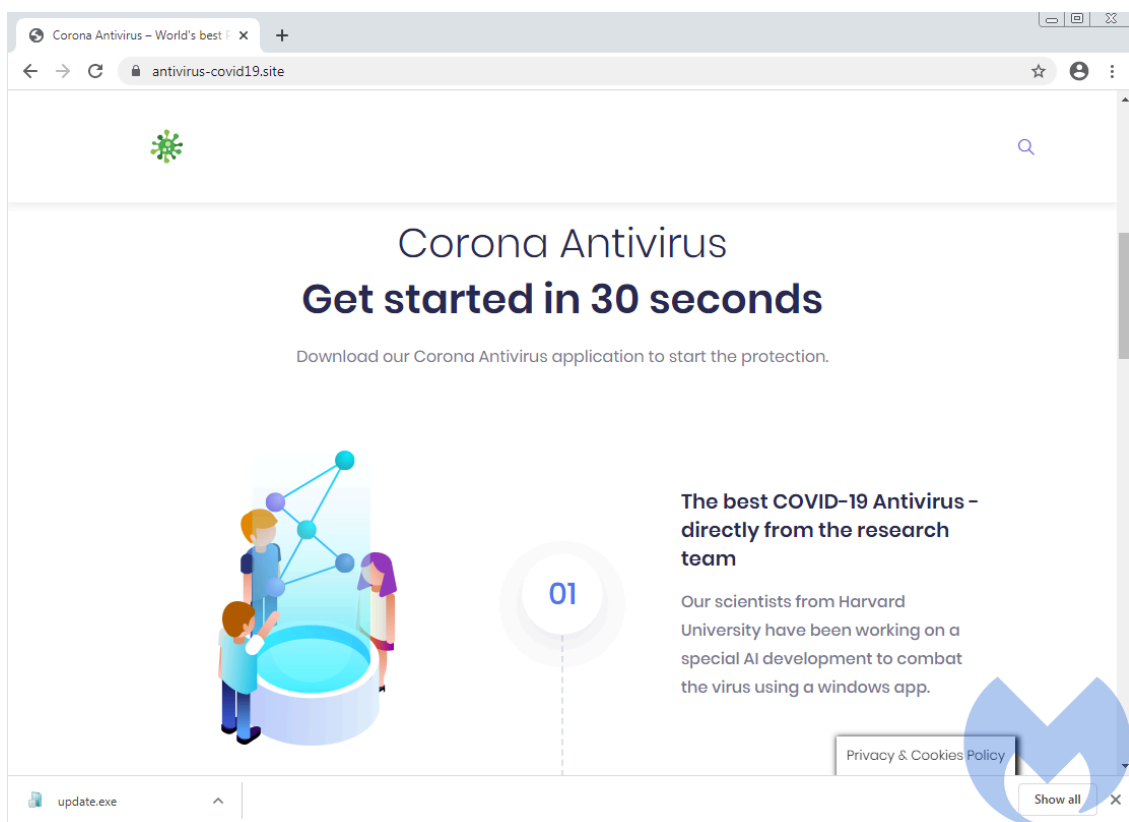
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

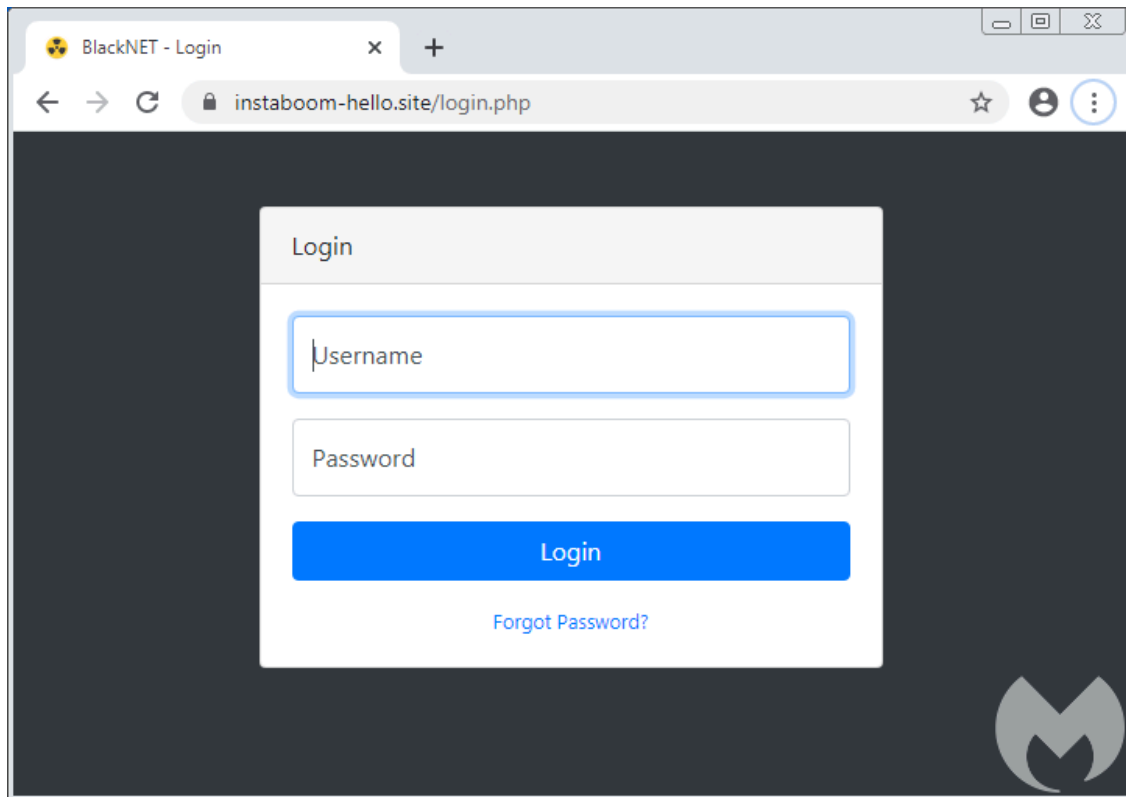


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

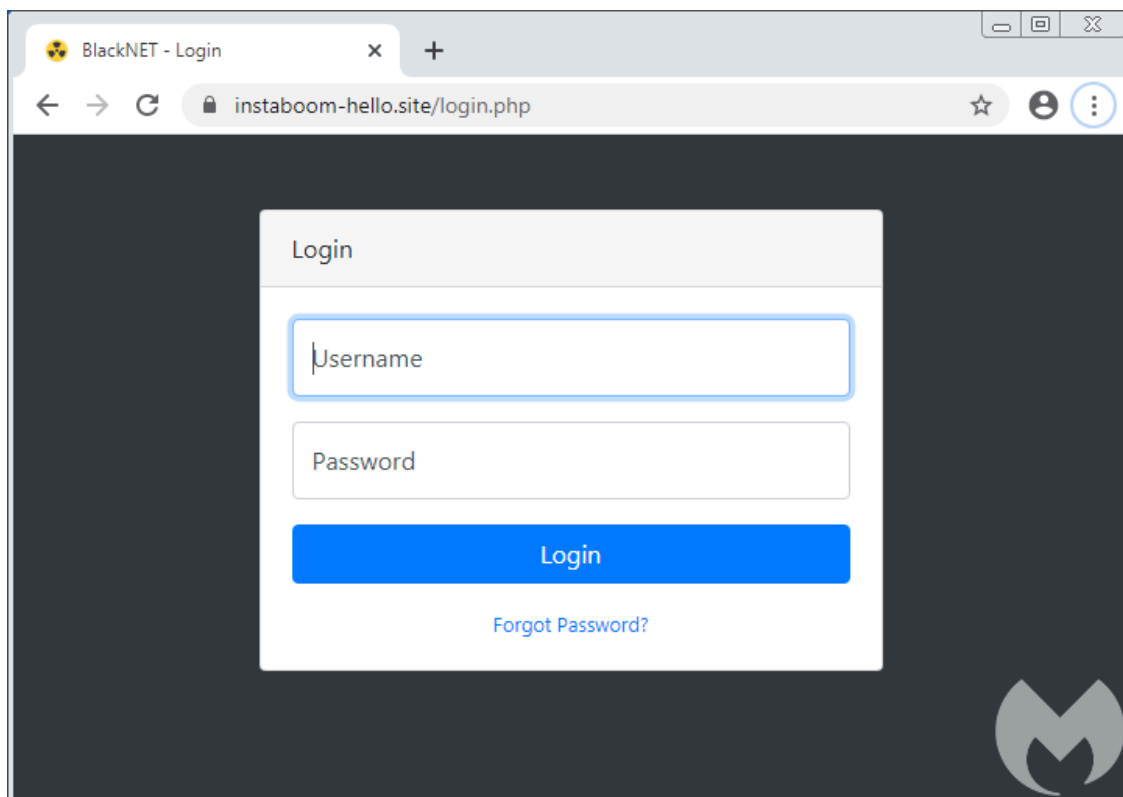
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

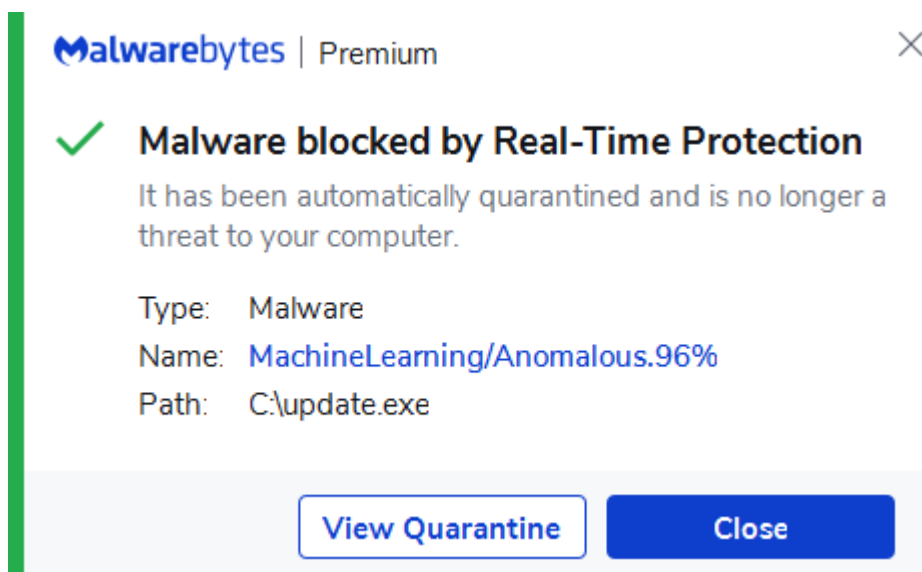
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

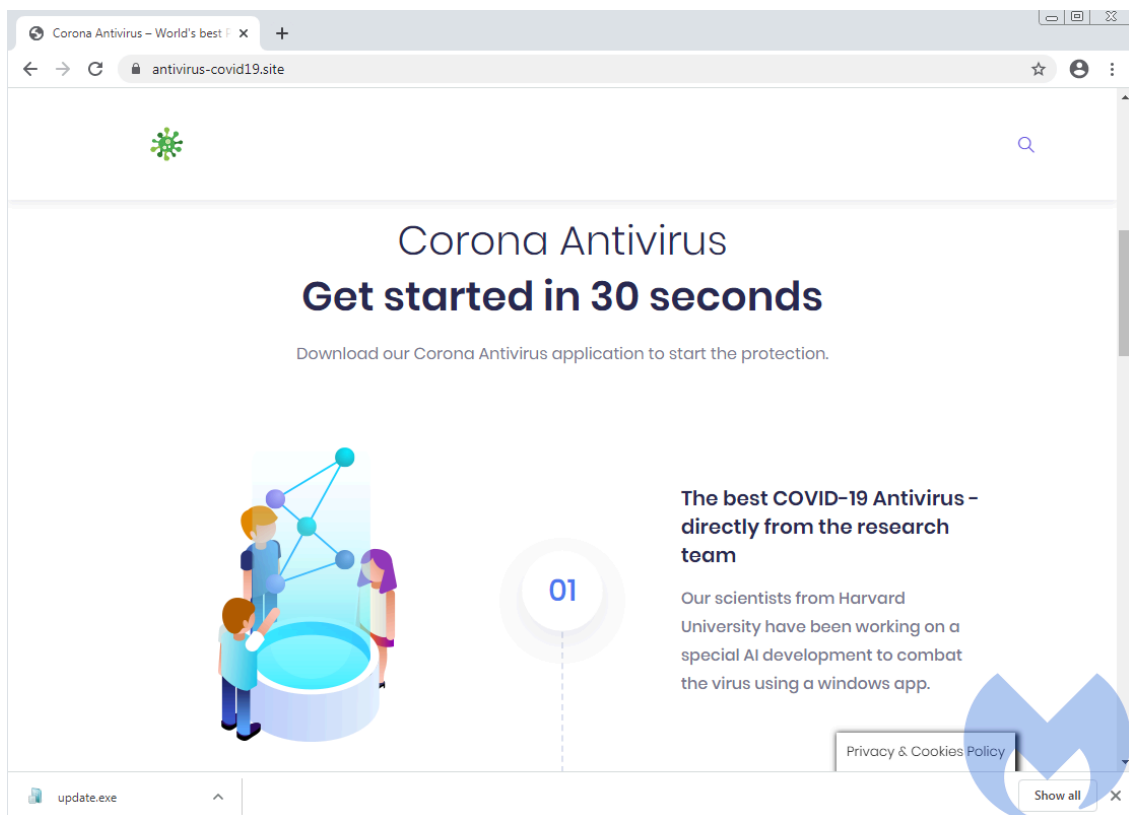
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Malwarebytes | Premium

✓ **Malware blocked by Real-Time Protection**

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: MachineLearning/Anomalous.96%

Path: C:\update.exe

View Quarantine Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

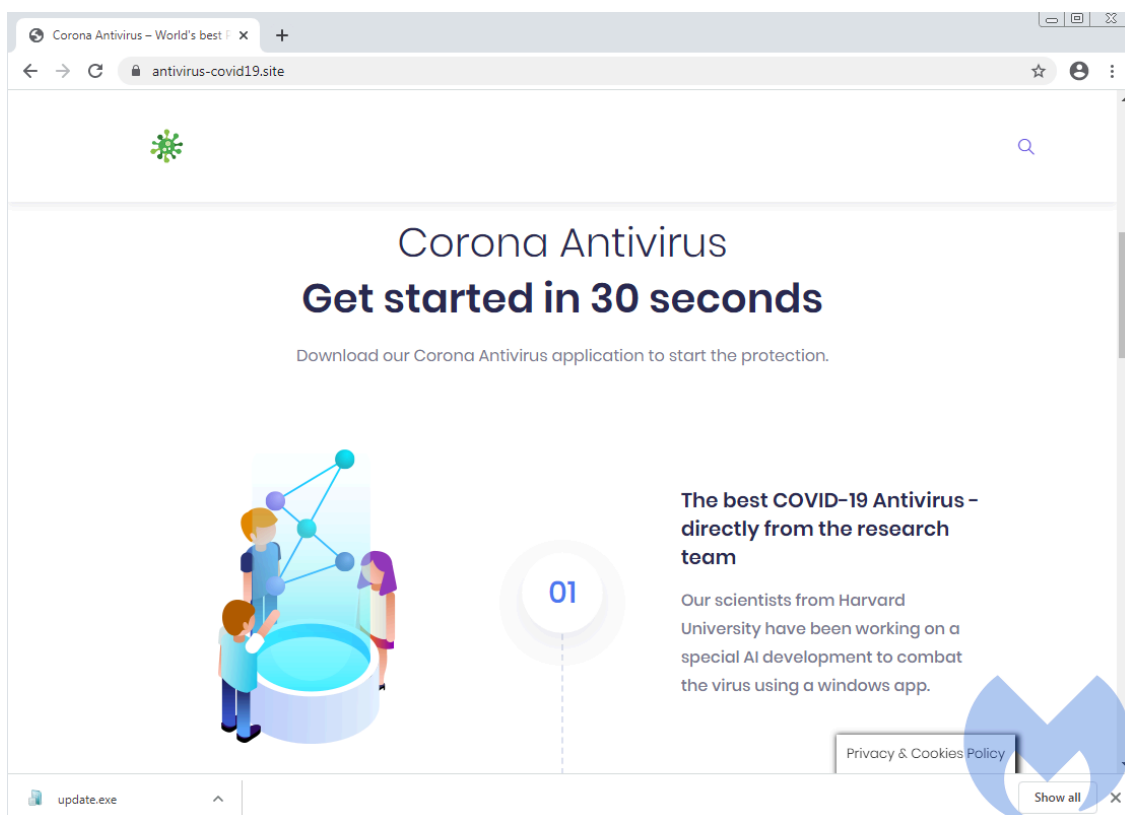
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

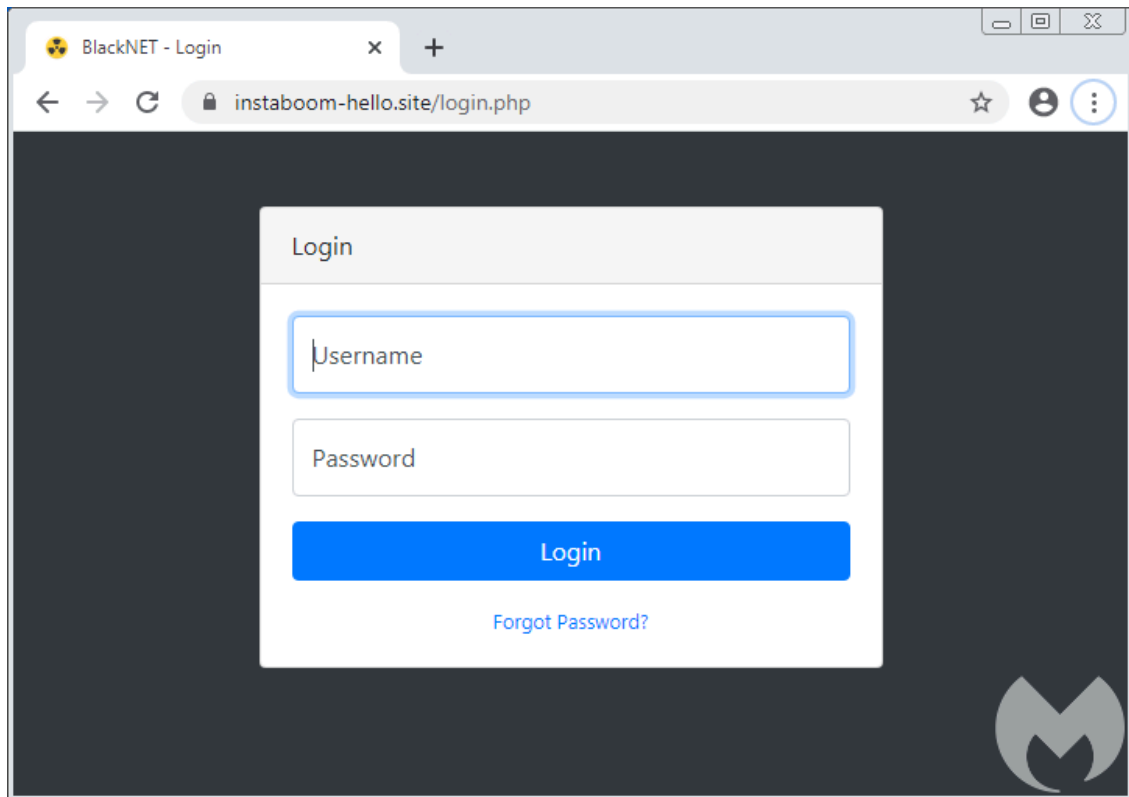


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

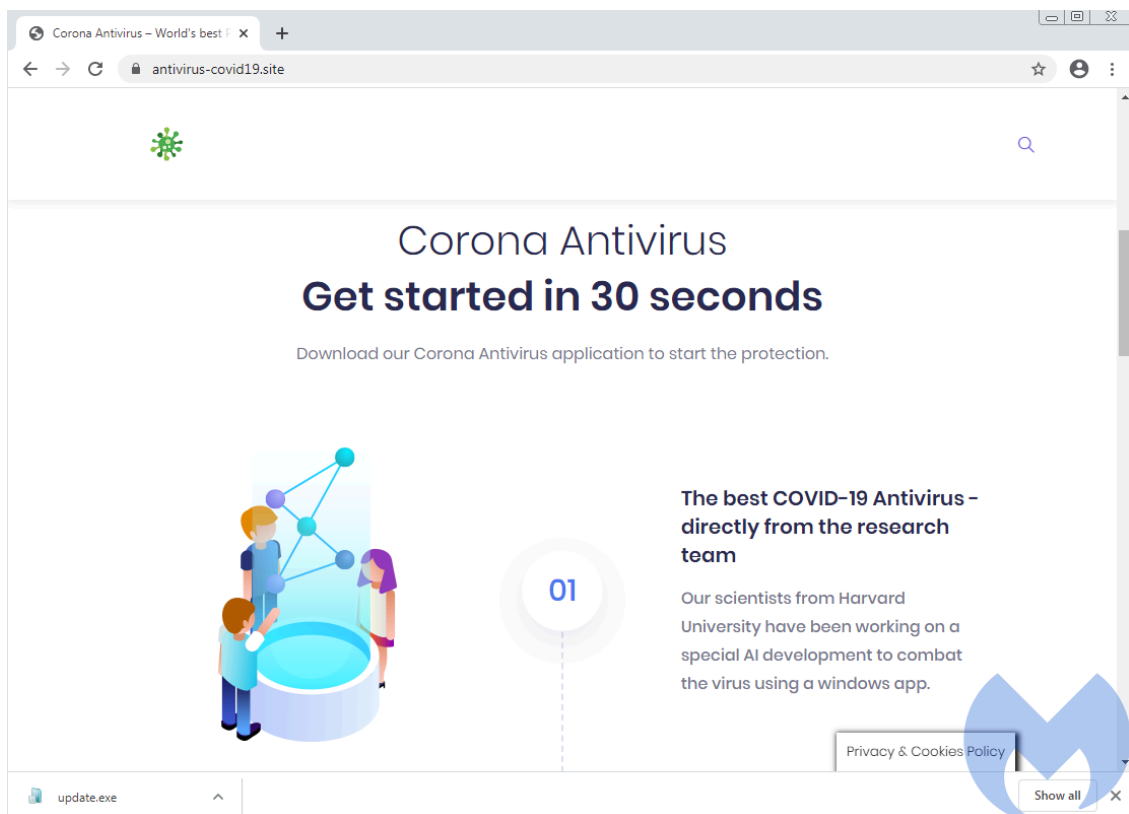
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

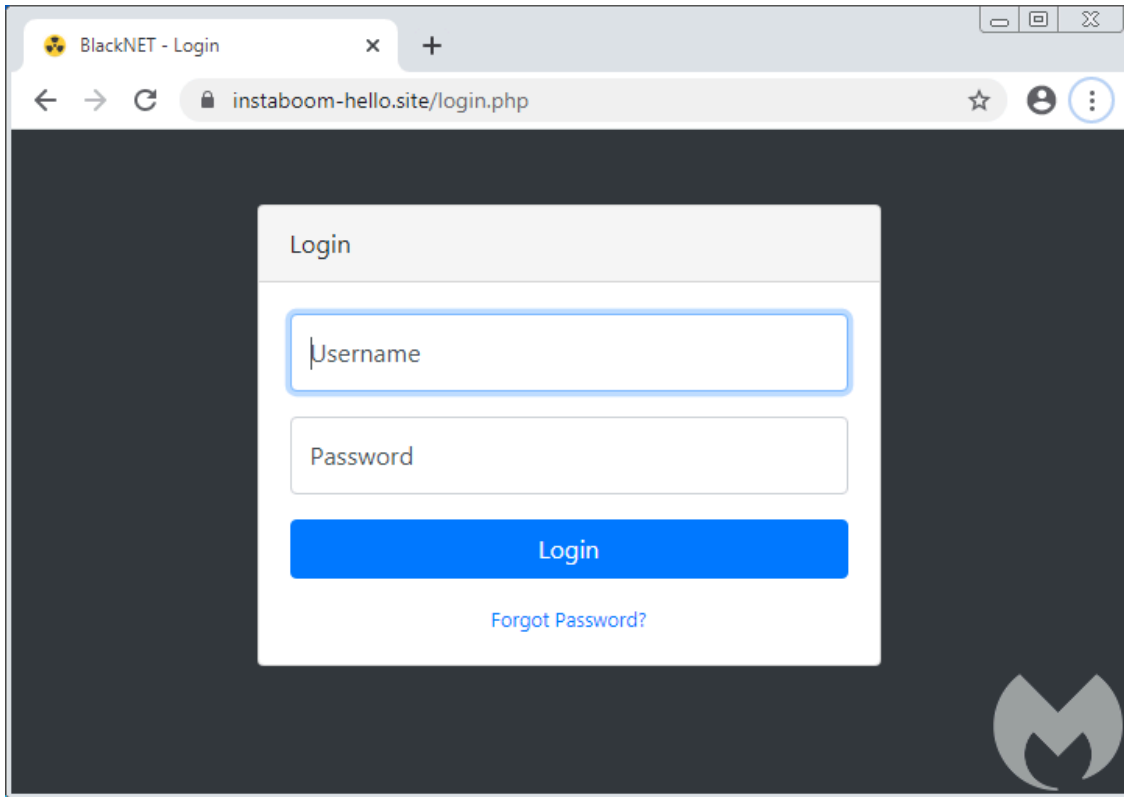


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

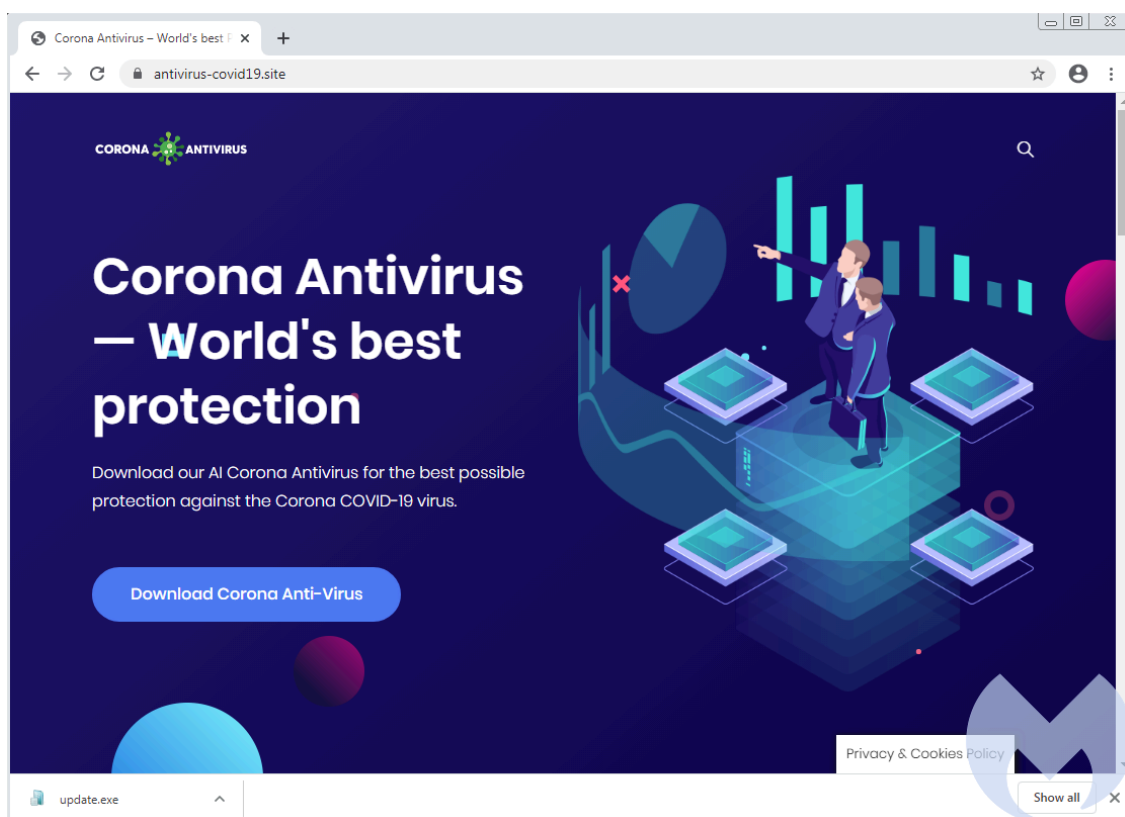
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

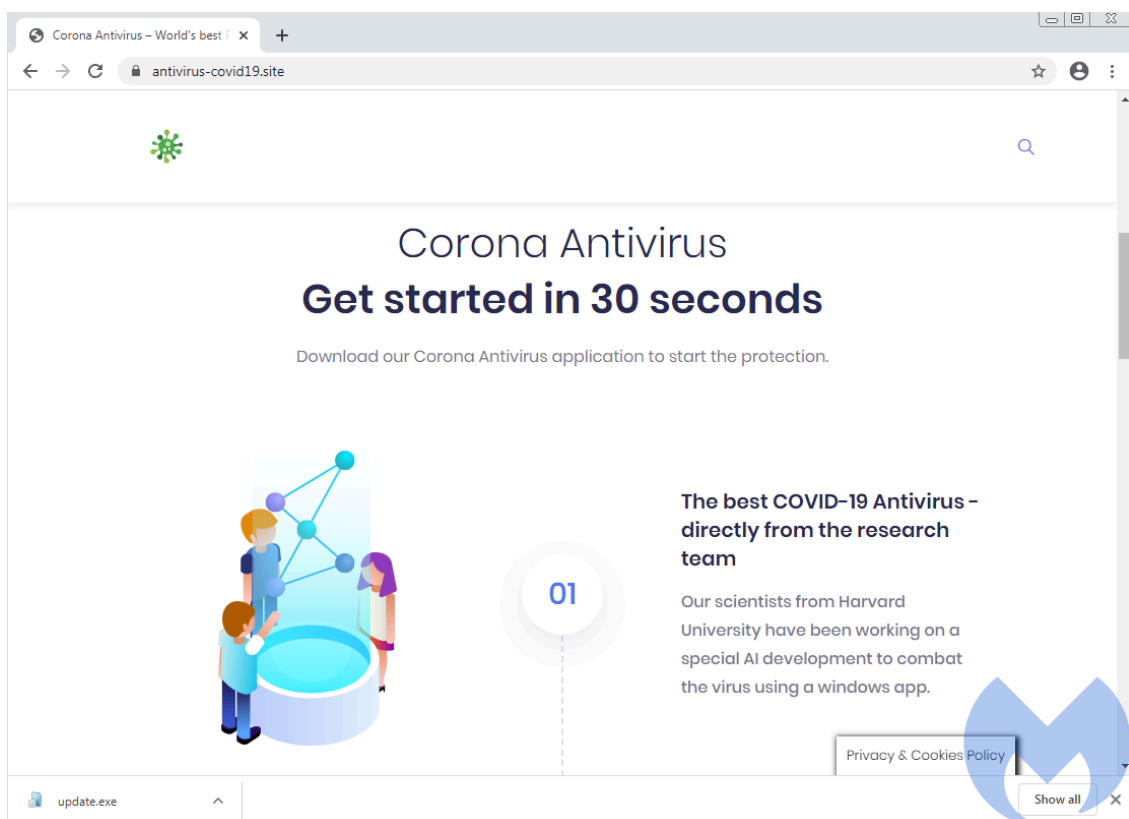
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

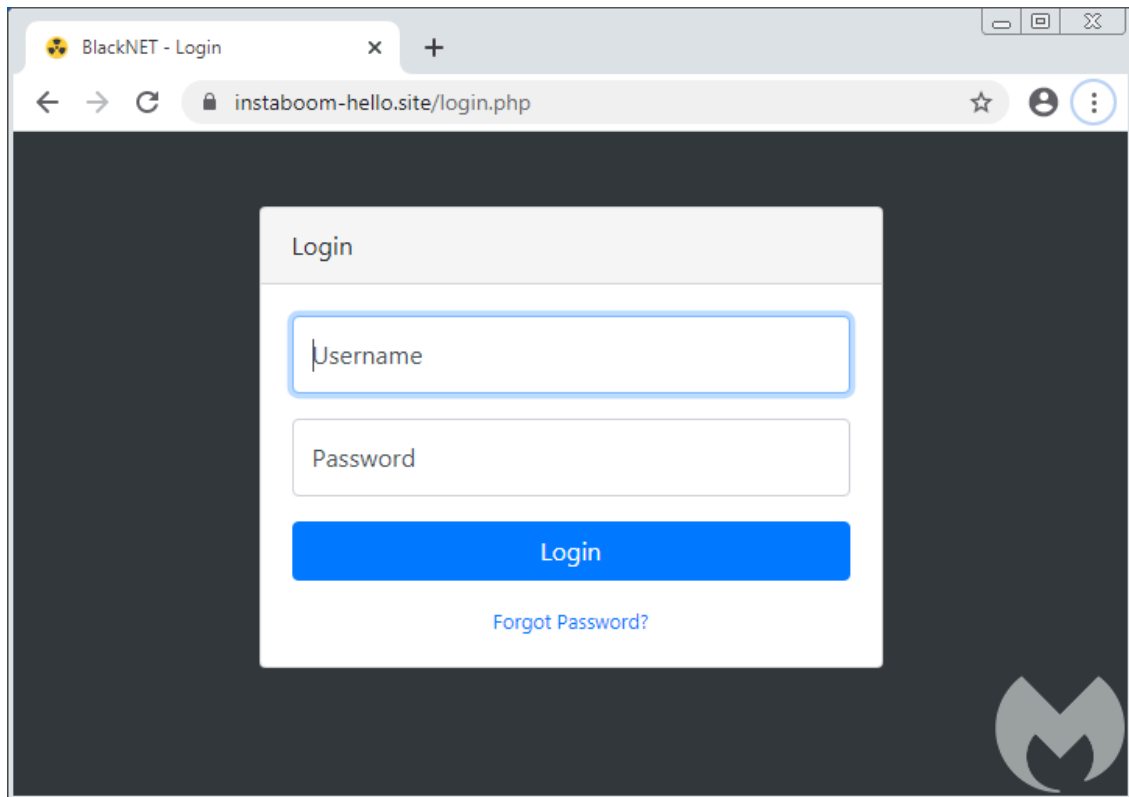


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

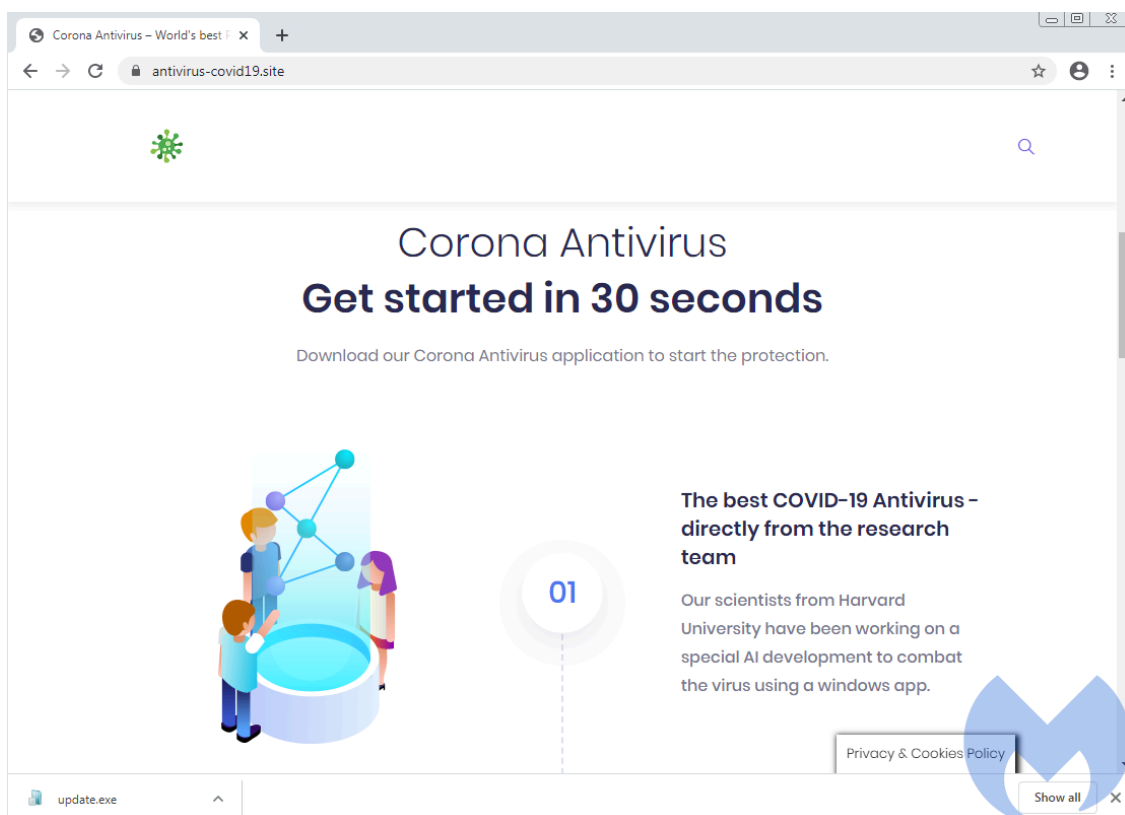
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

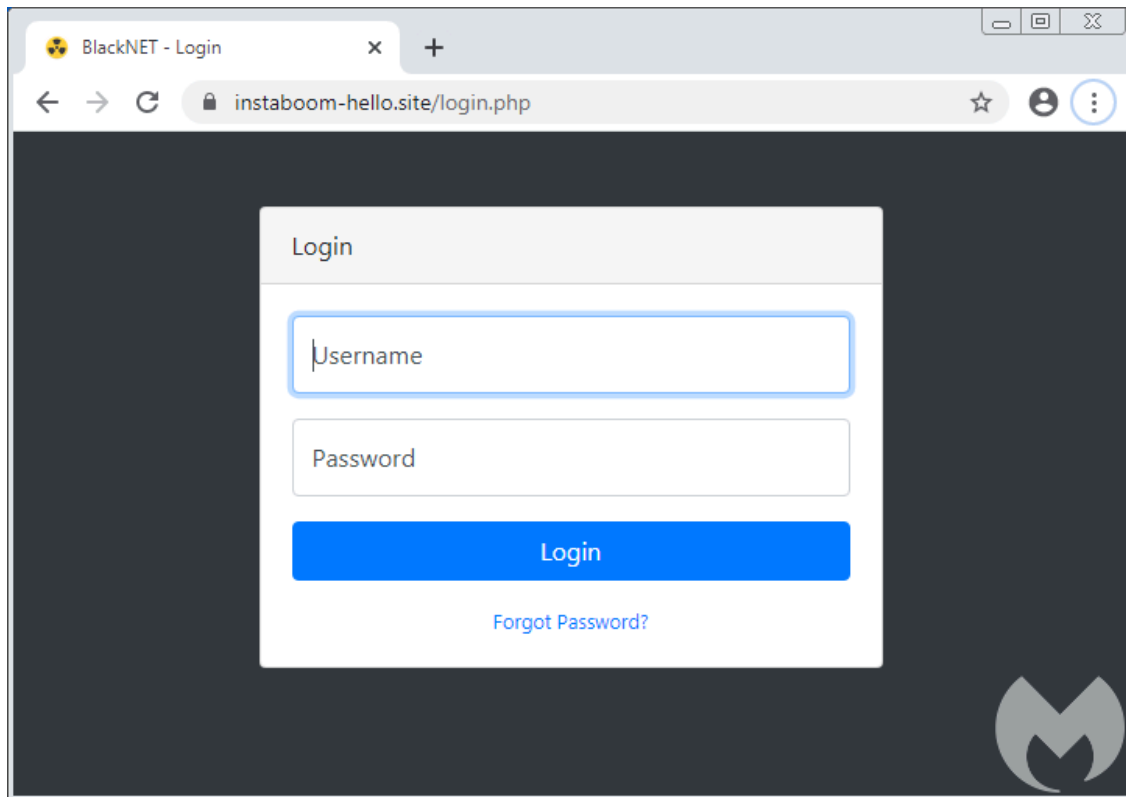


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

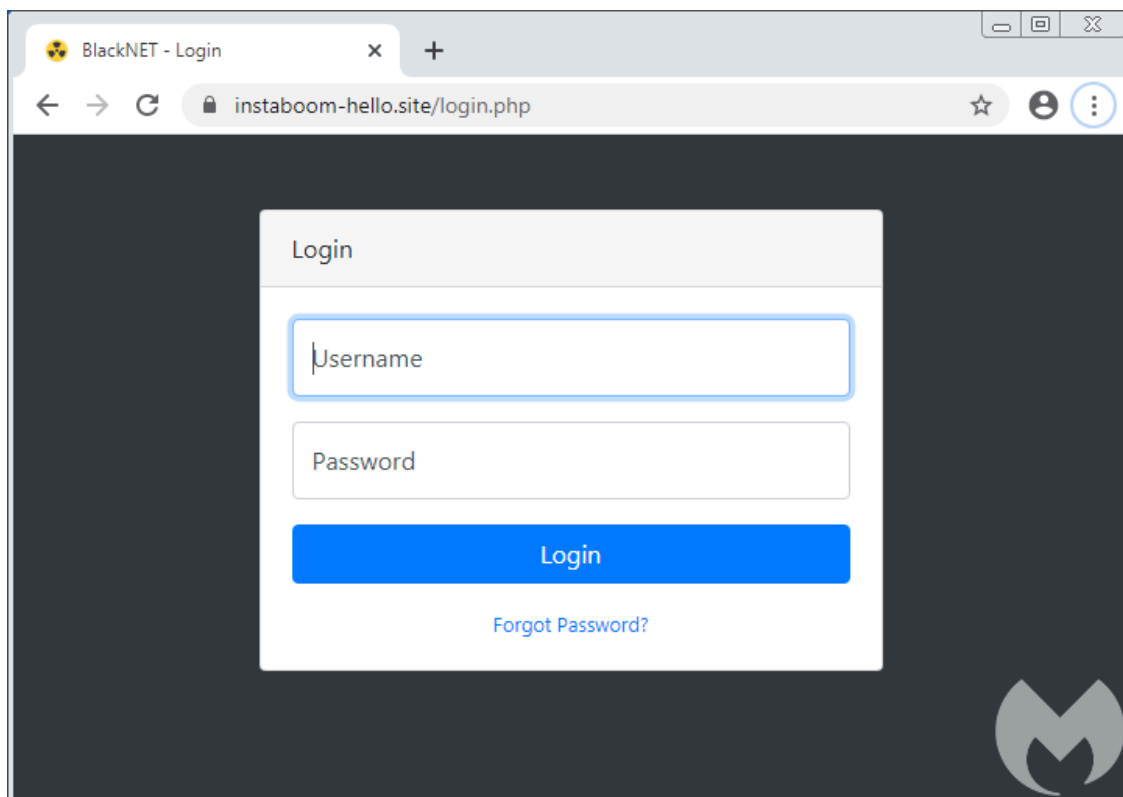
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

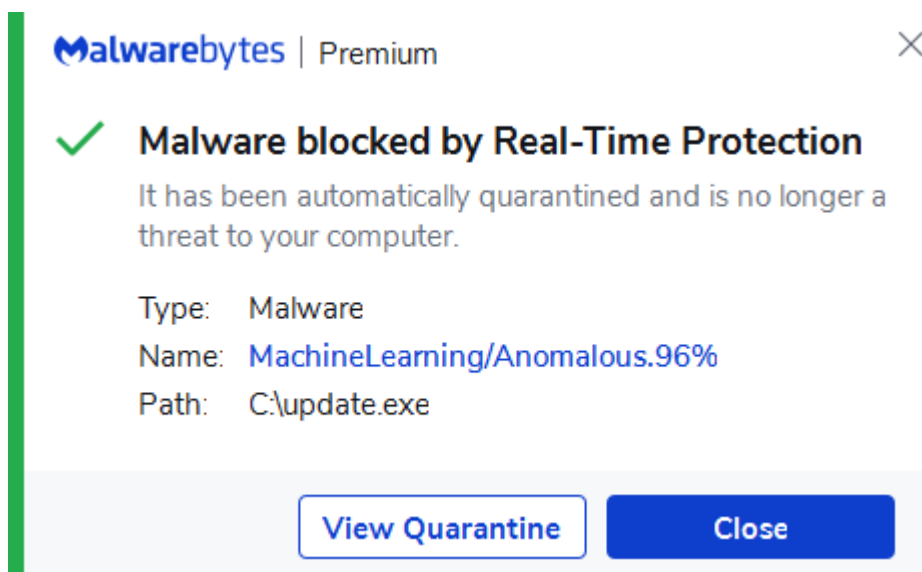
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

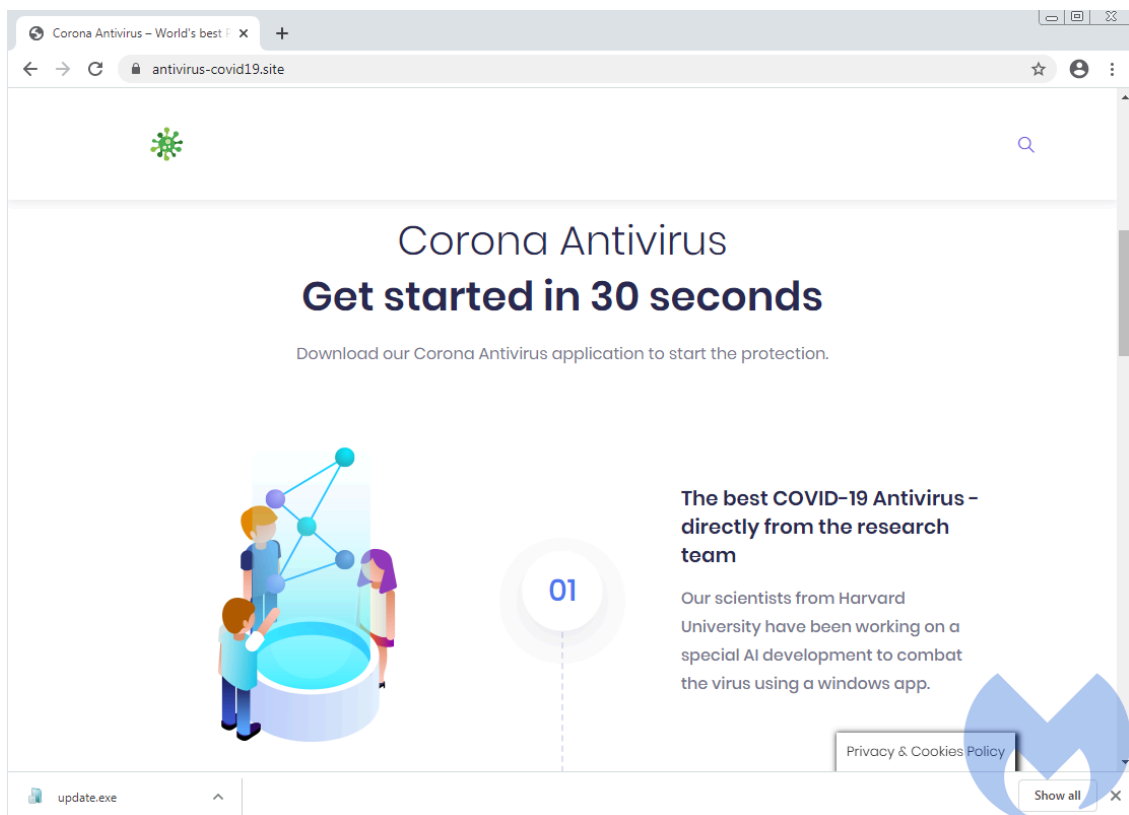
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

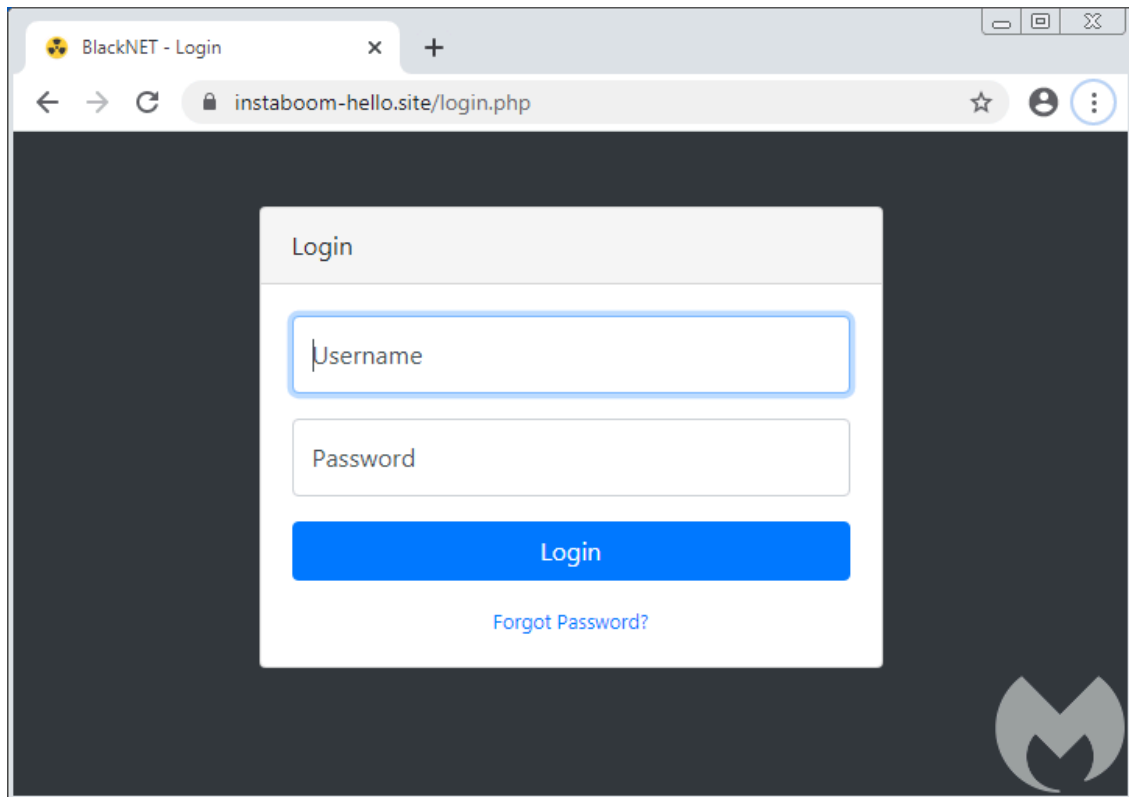


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

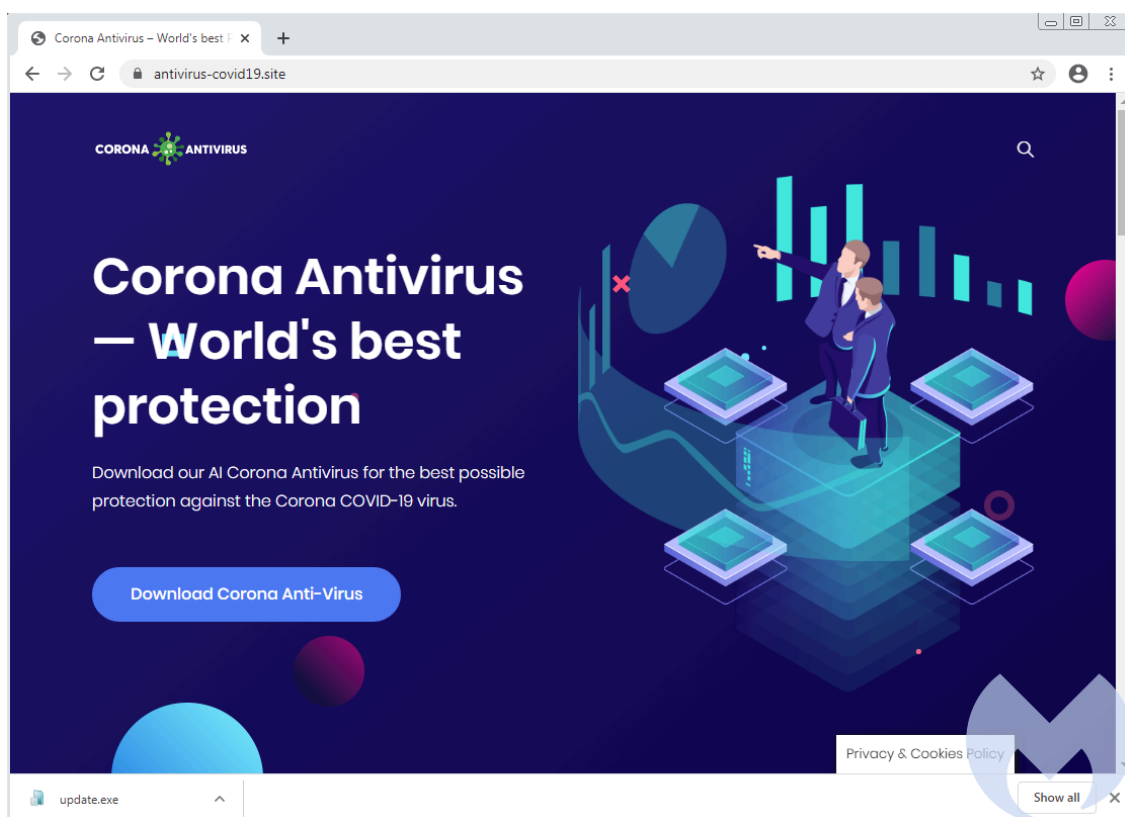
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

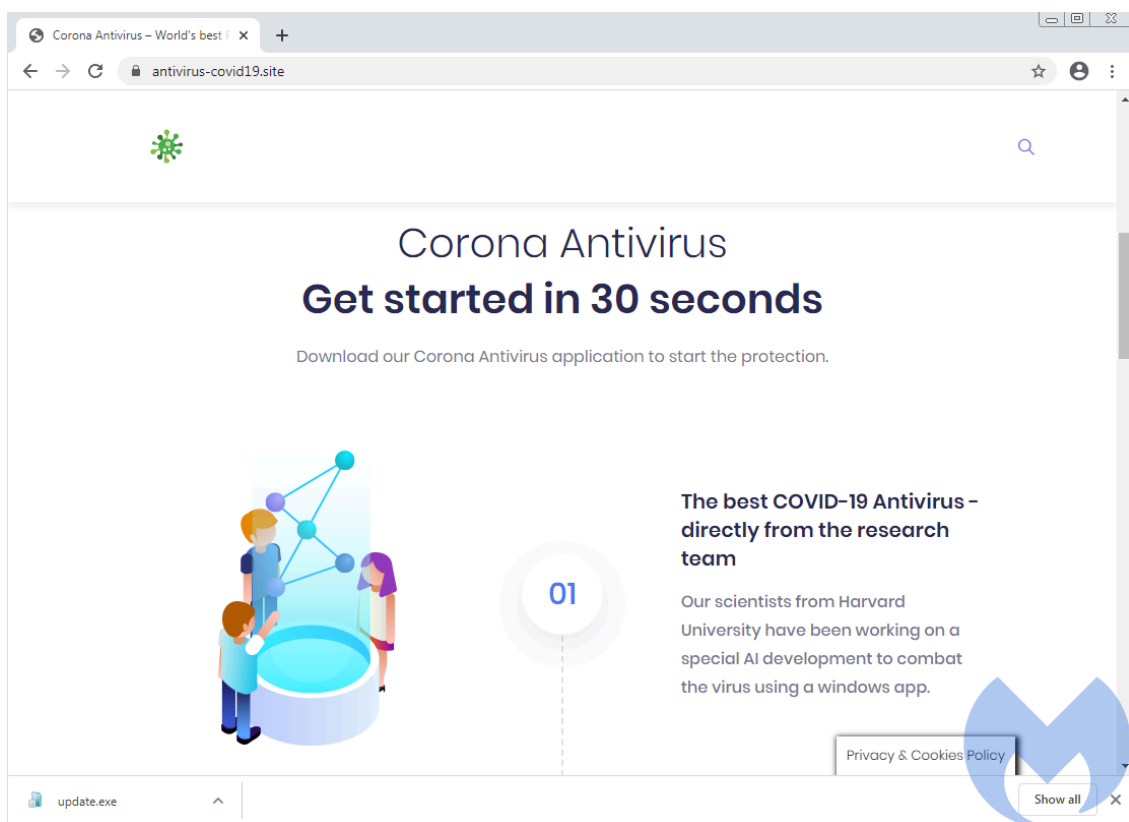
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

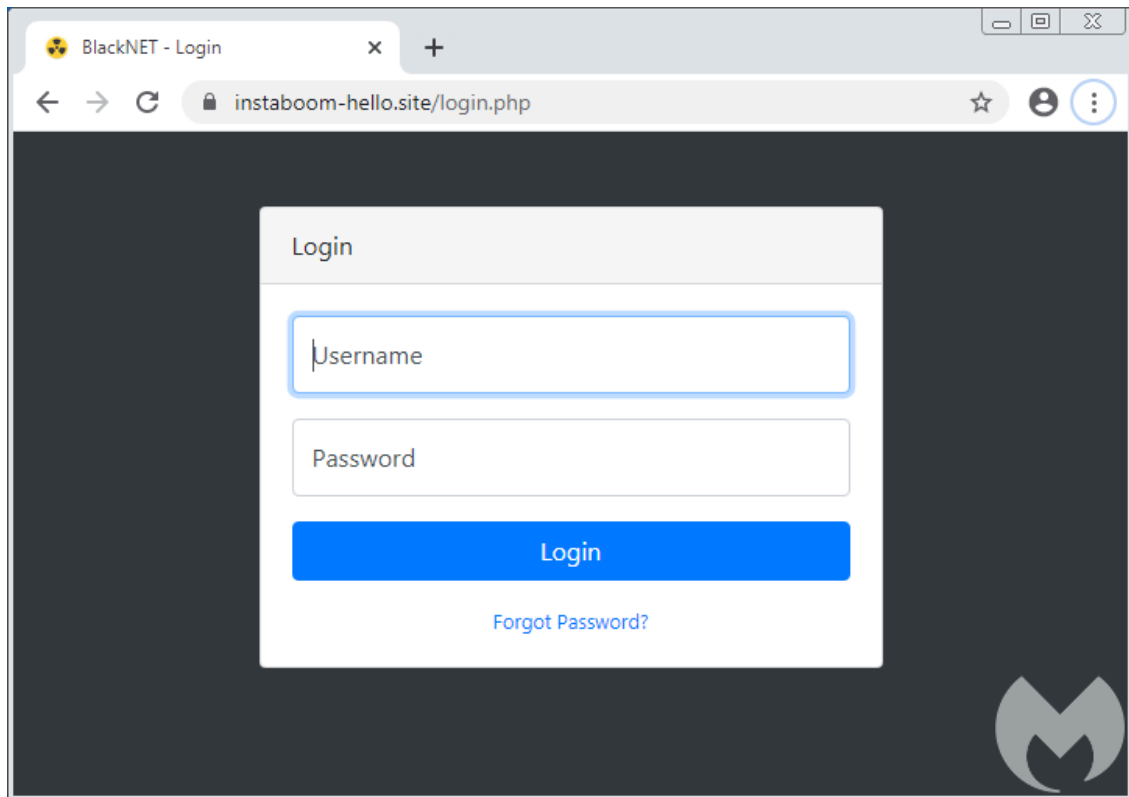


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

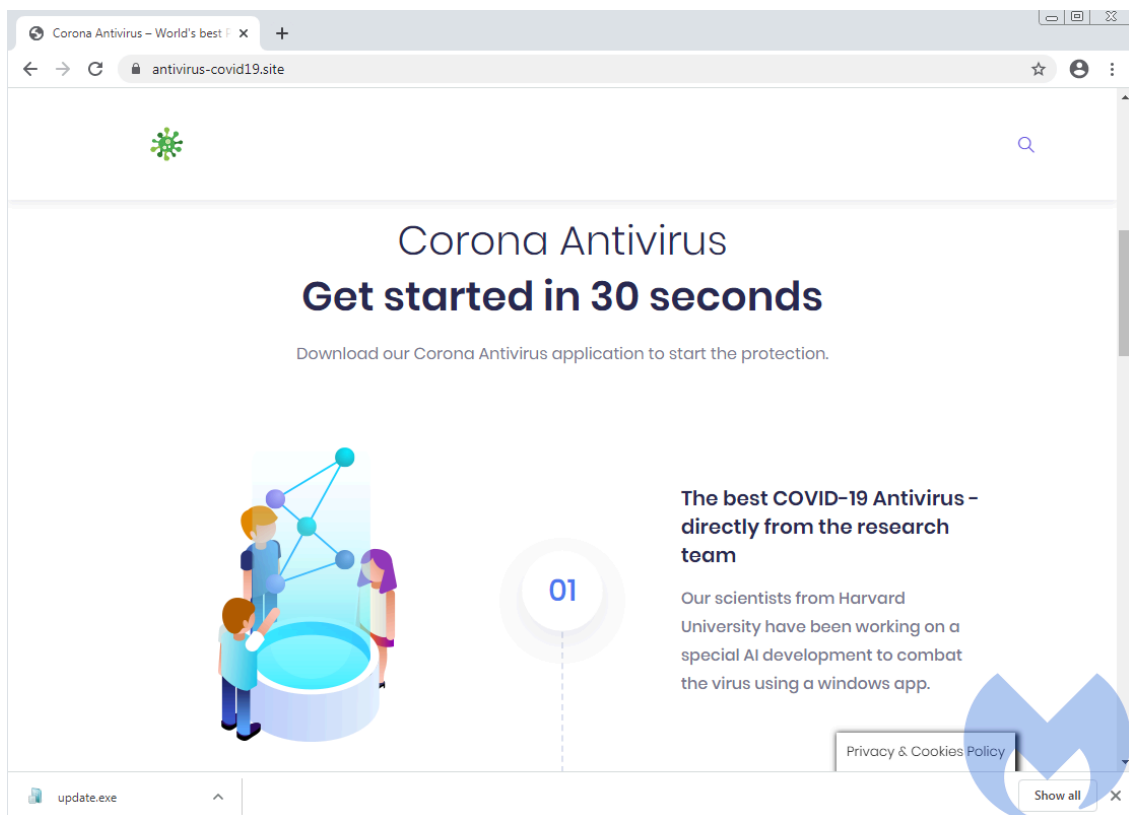
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

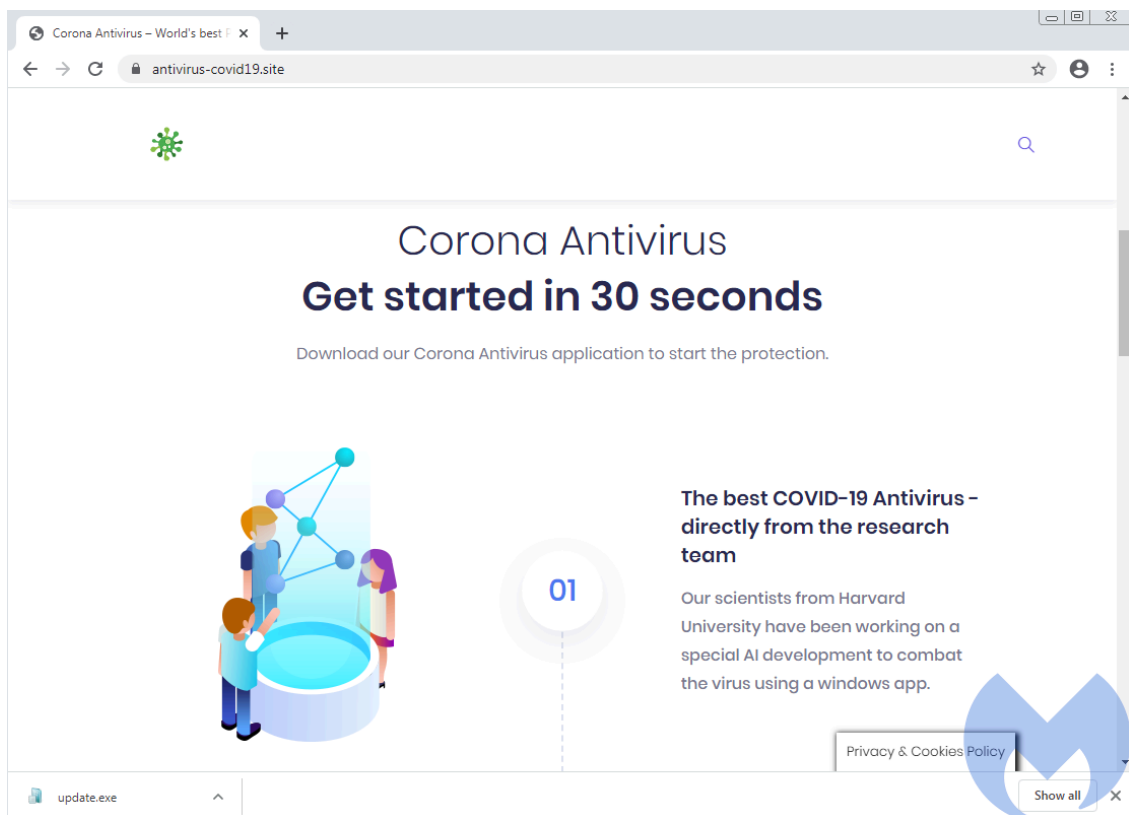
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

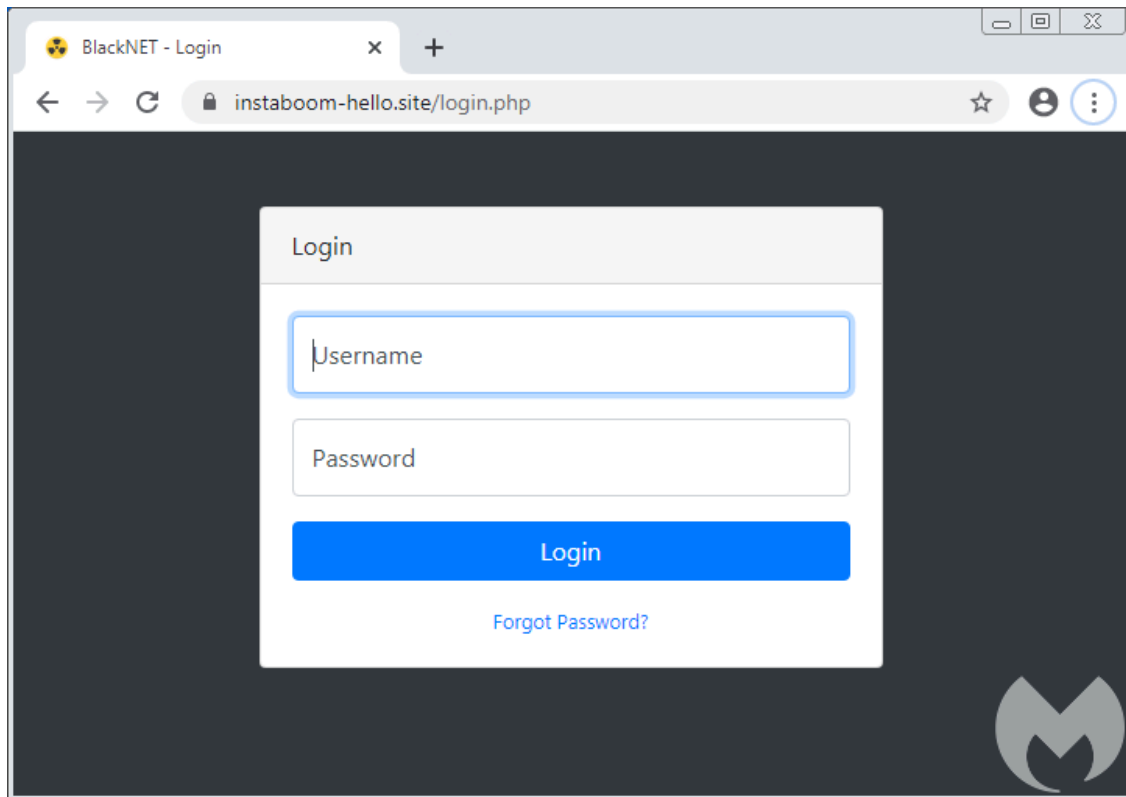


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

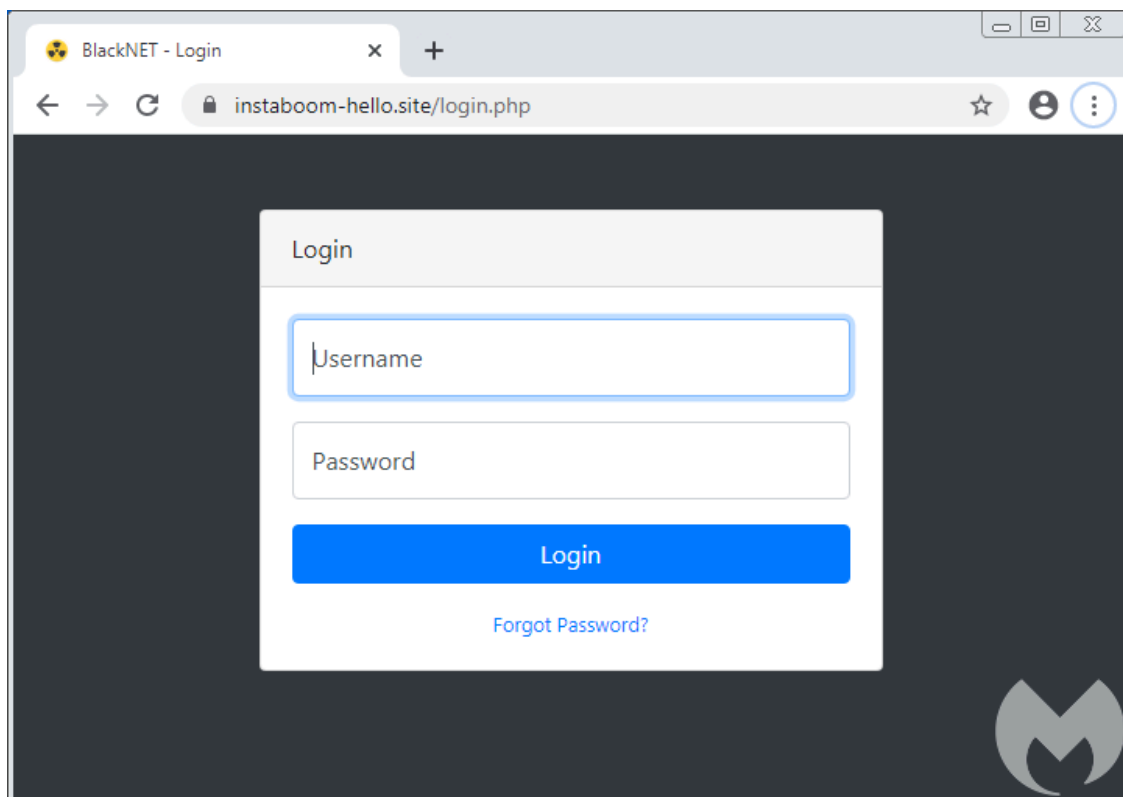
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

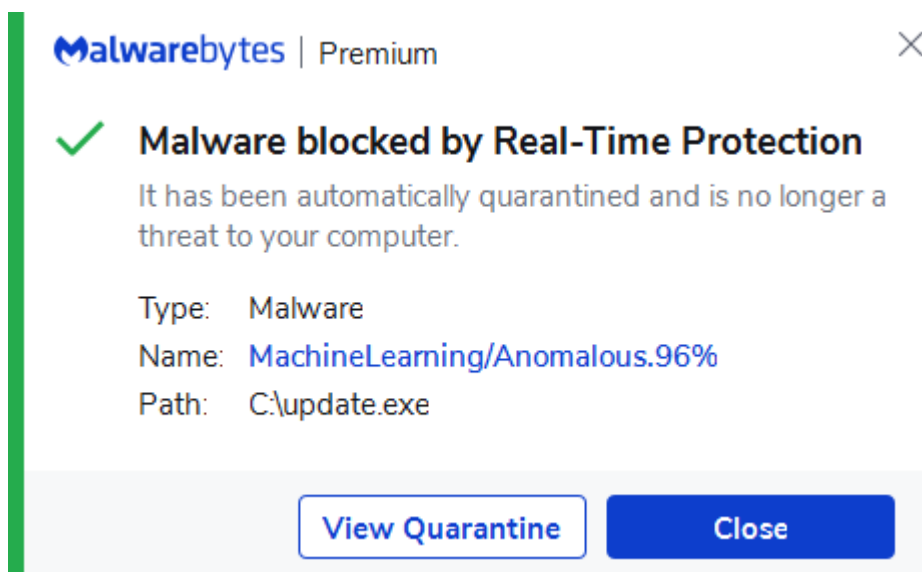
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

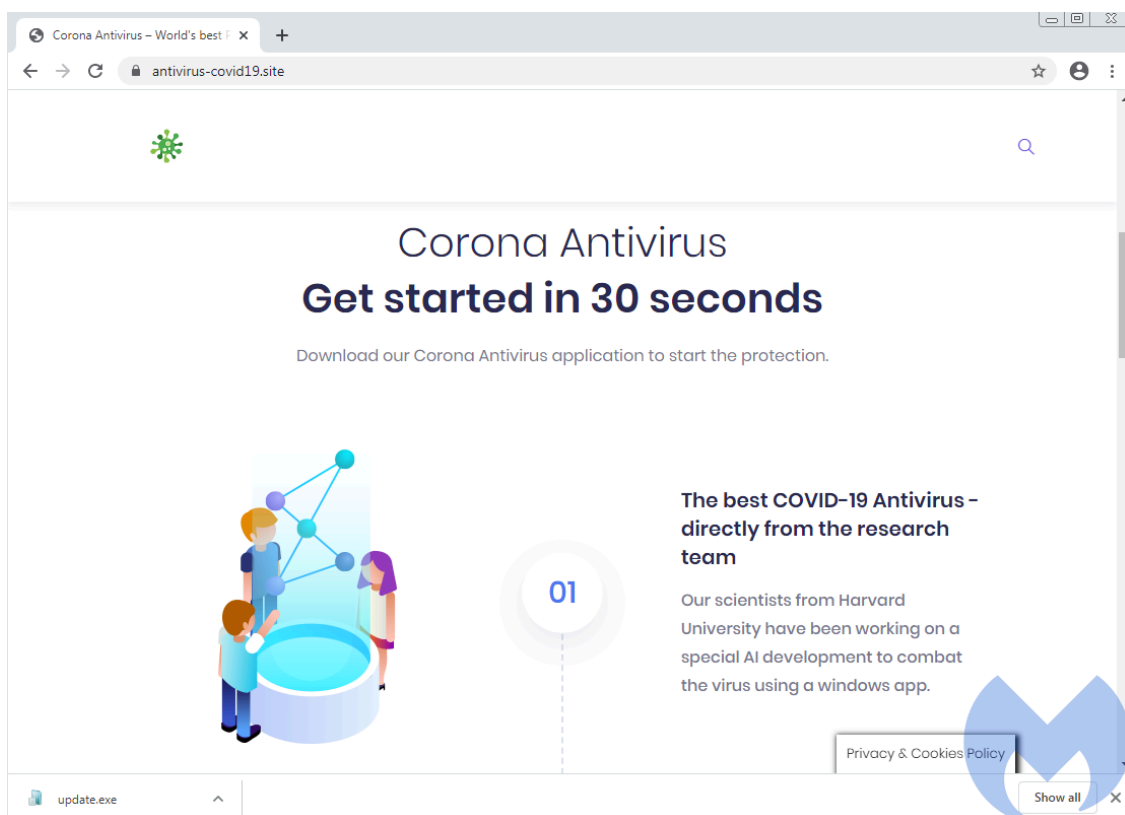
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

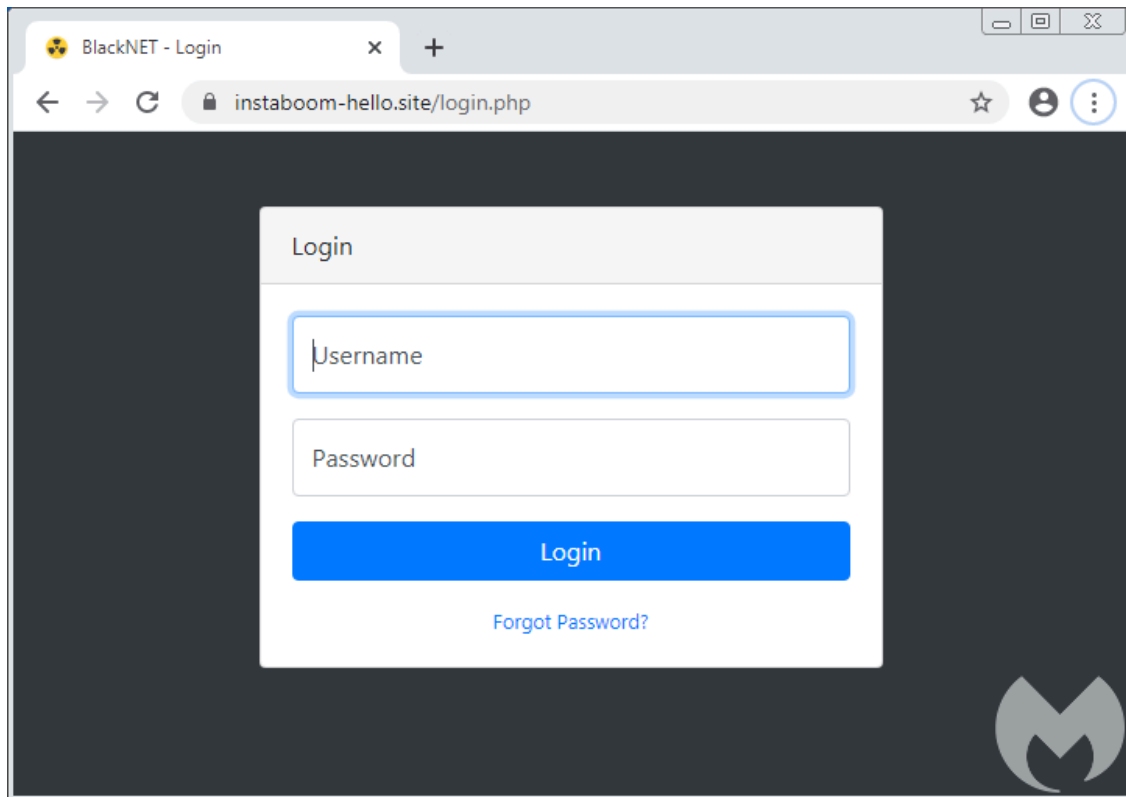


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

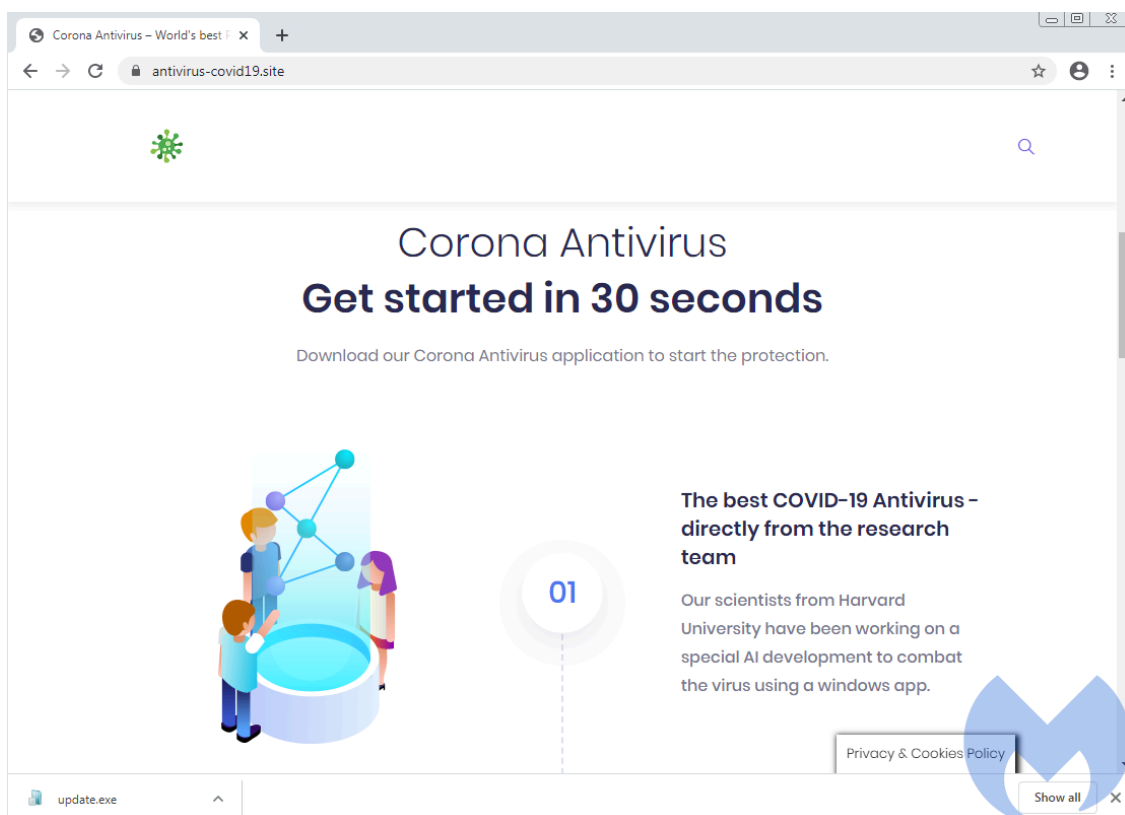
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

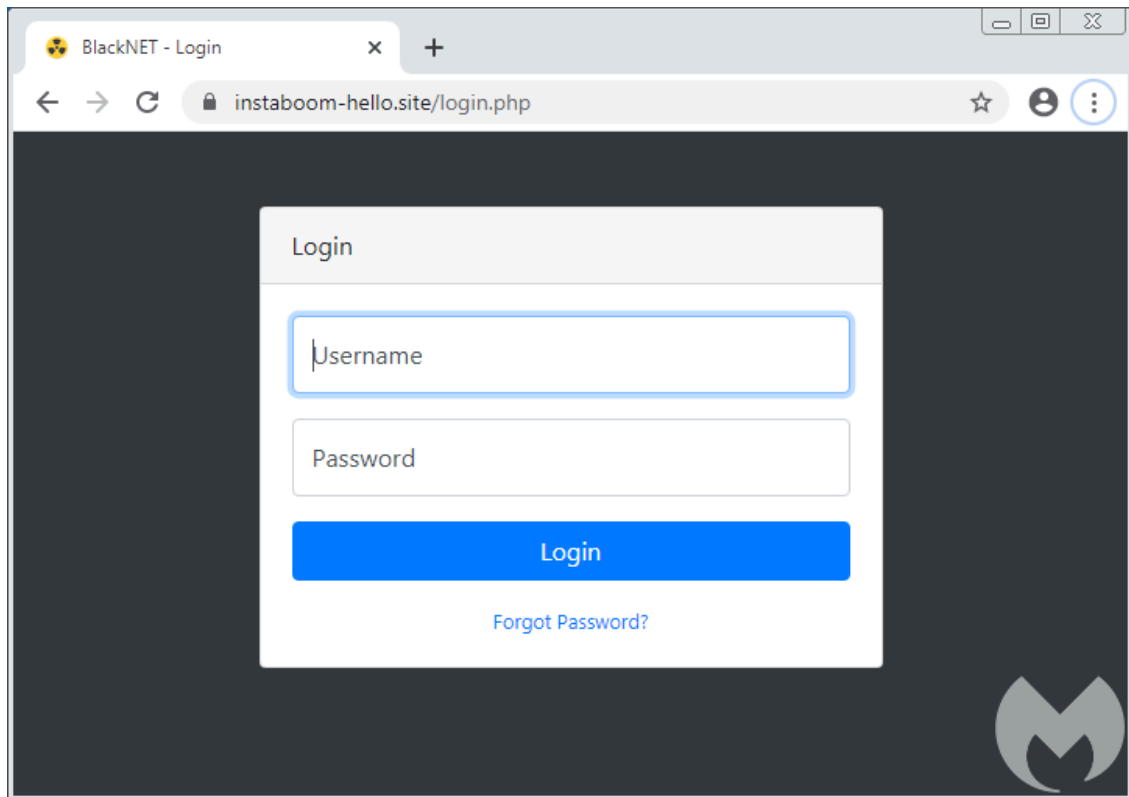


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

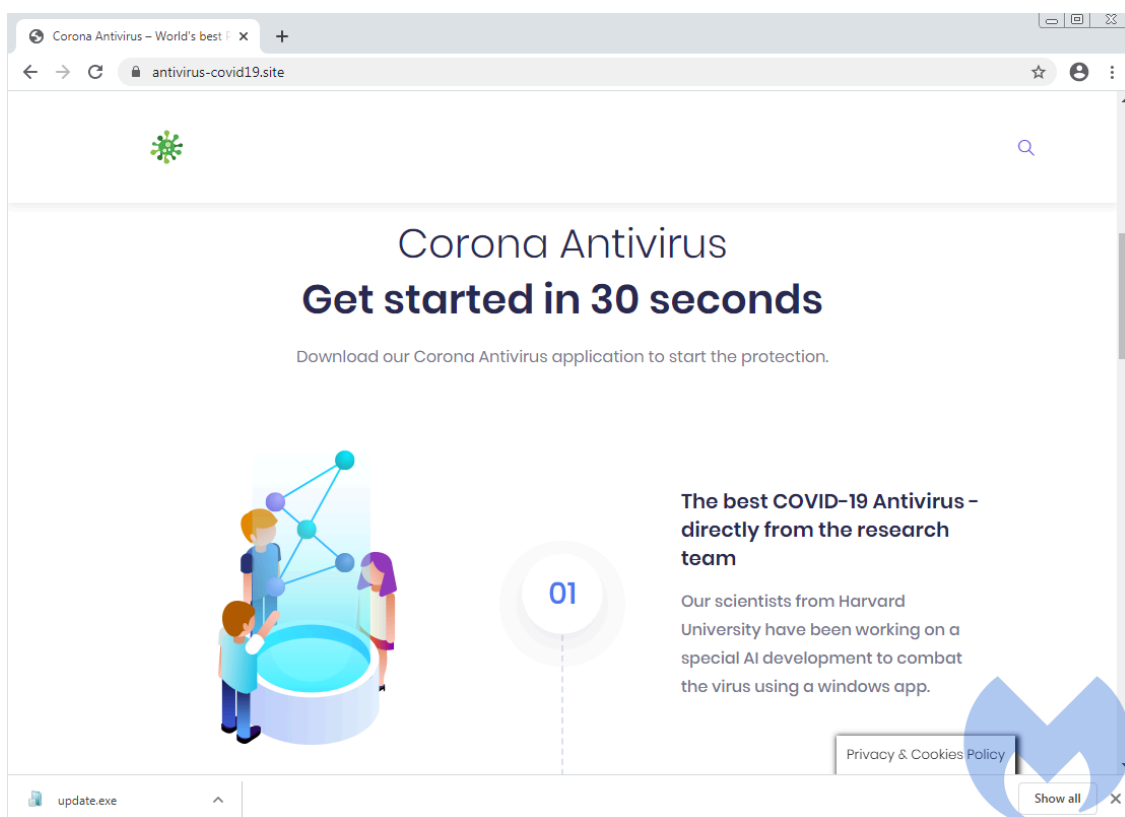
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

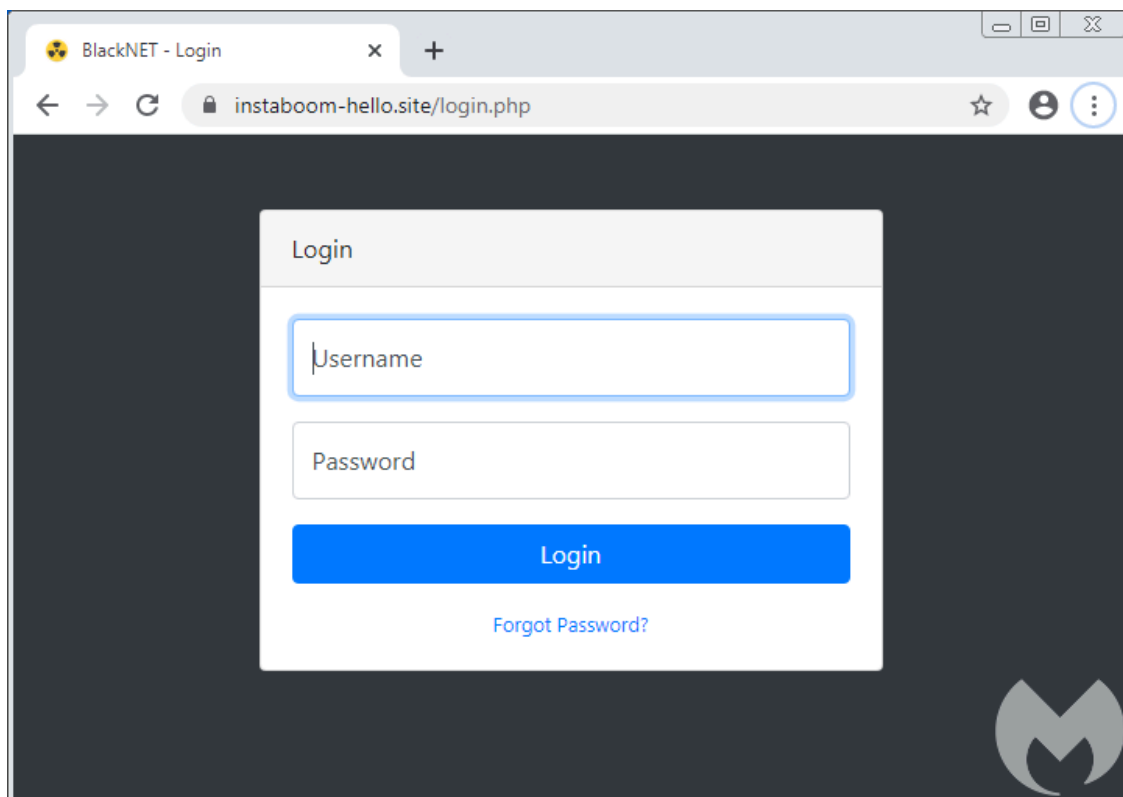


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

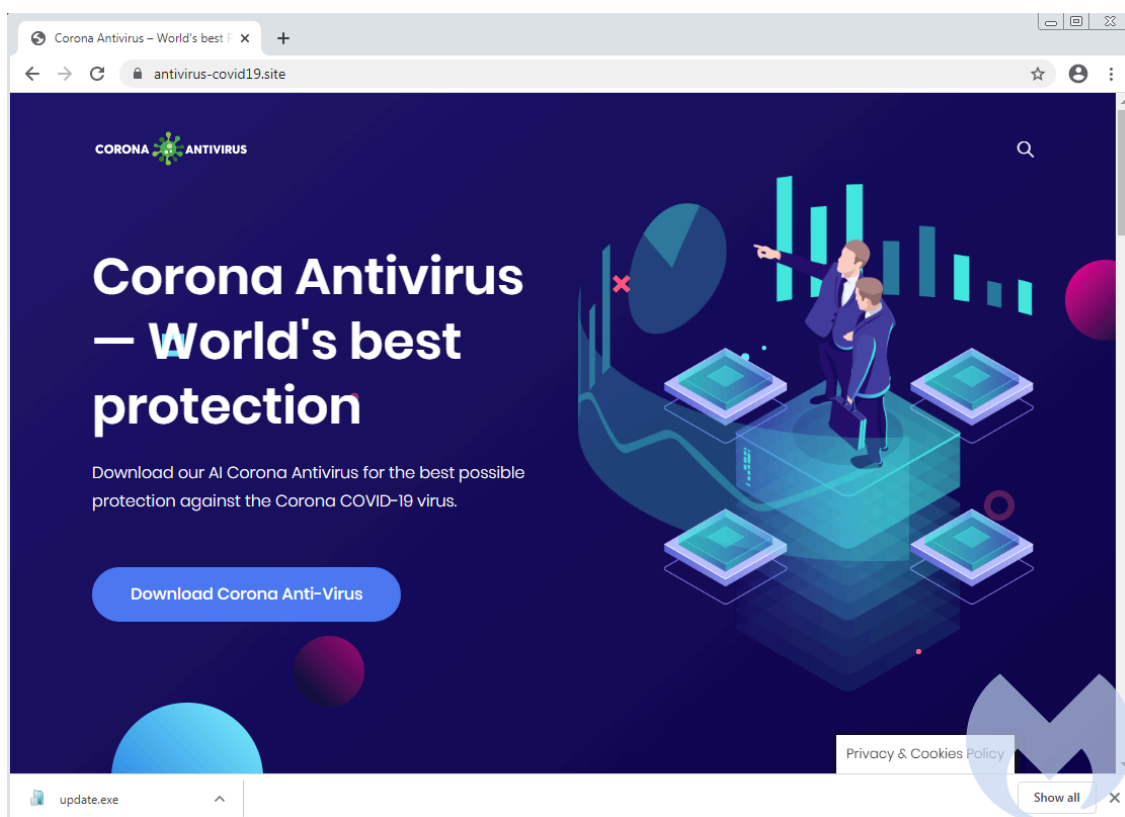
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

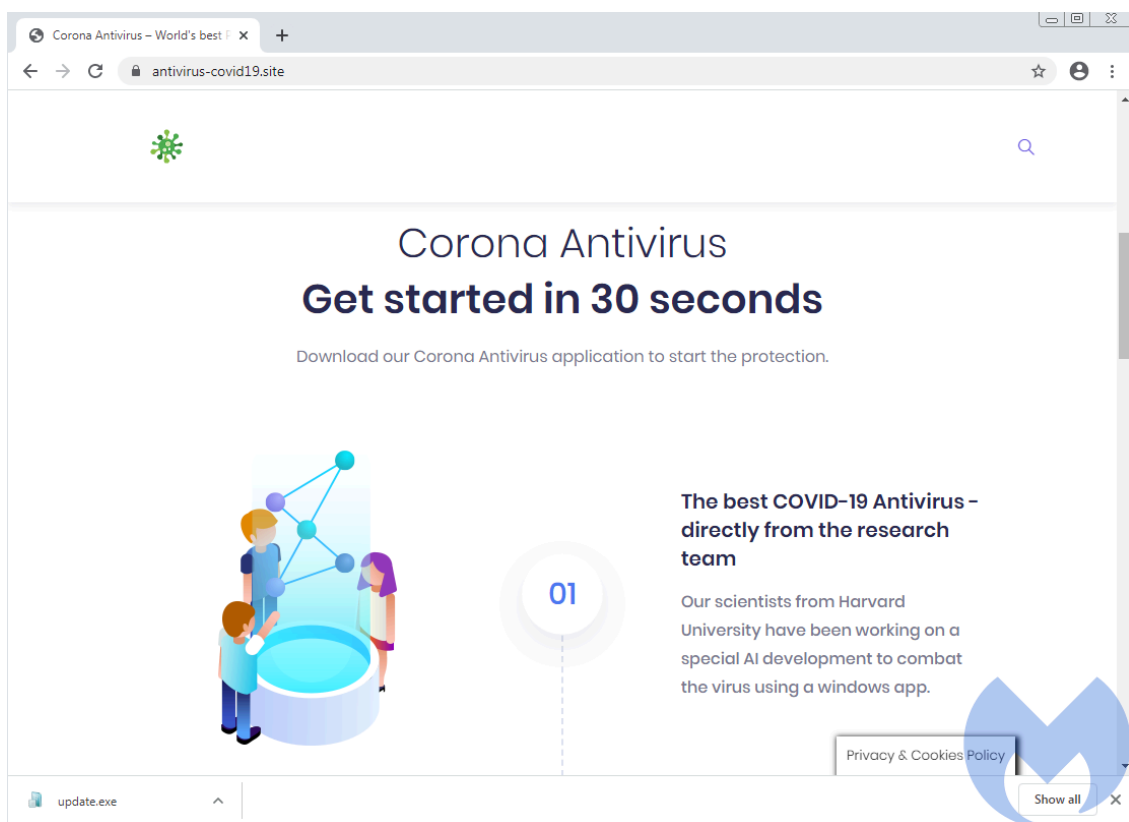
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

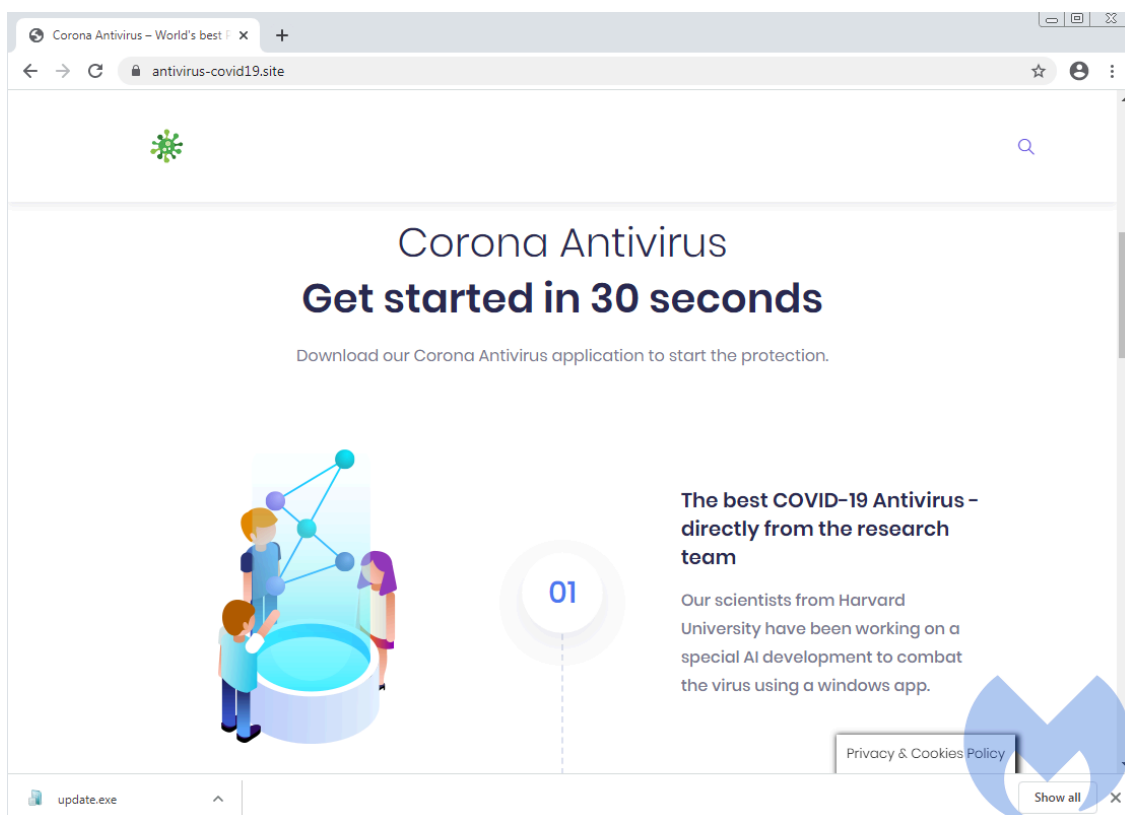
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

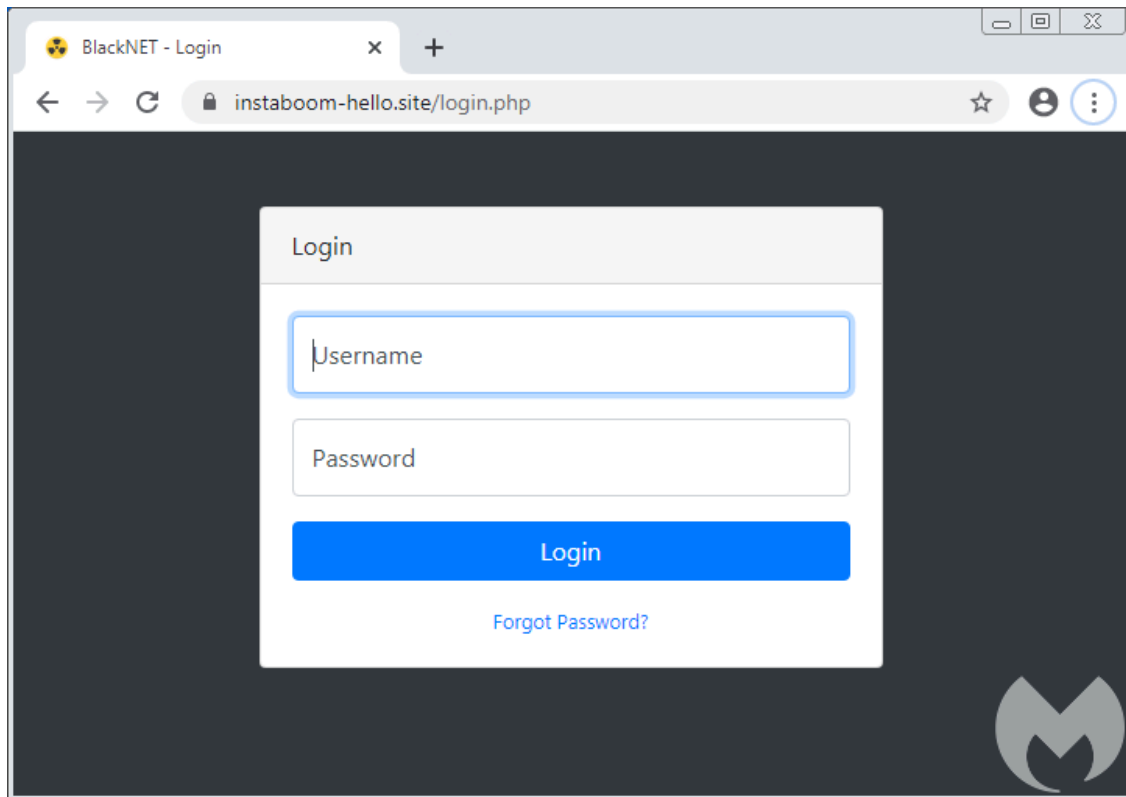


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

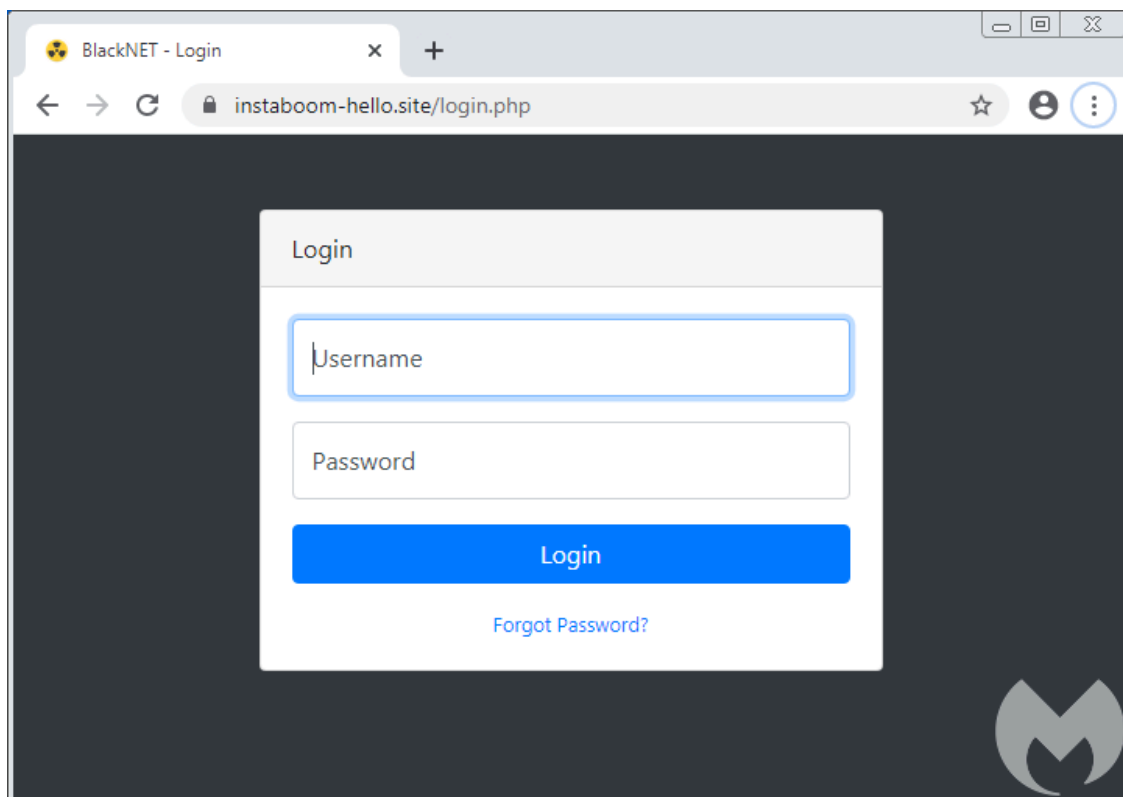
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

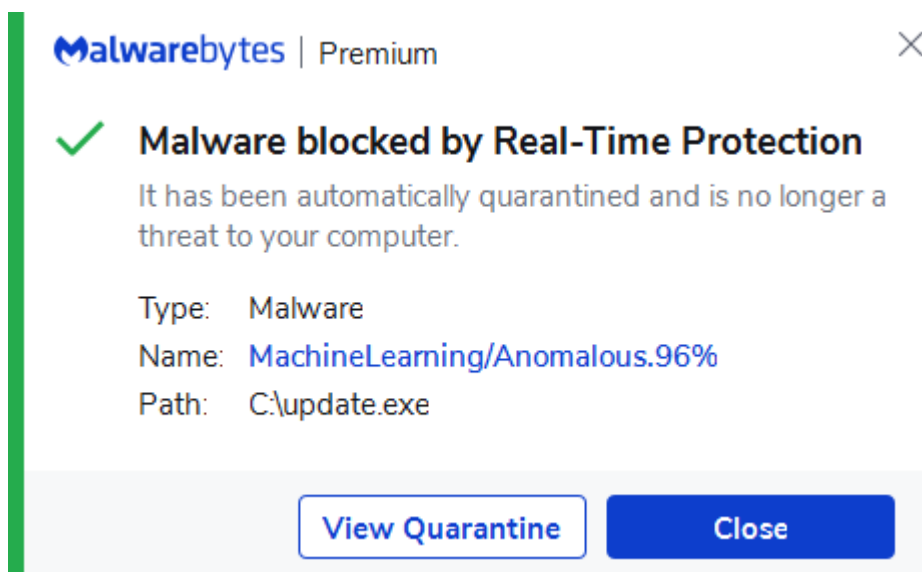
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

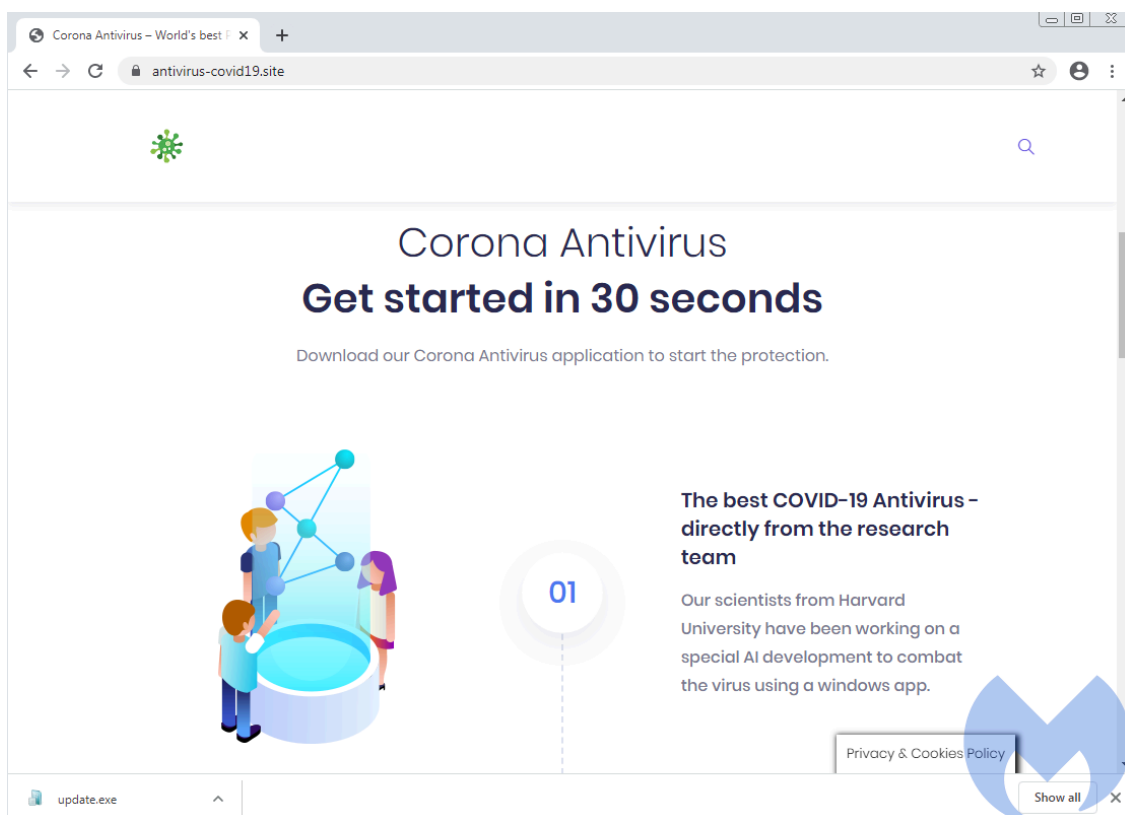
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

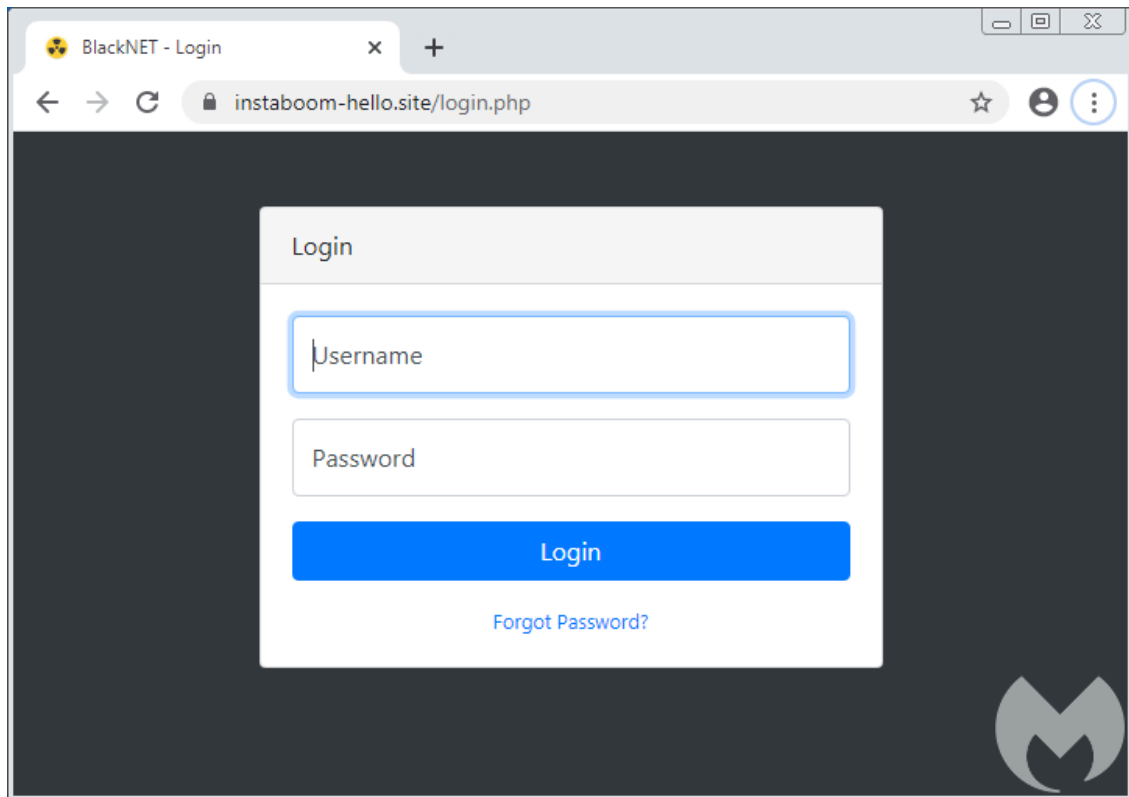


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, it lists the details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

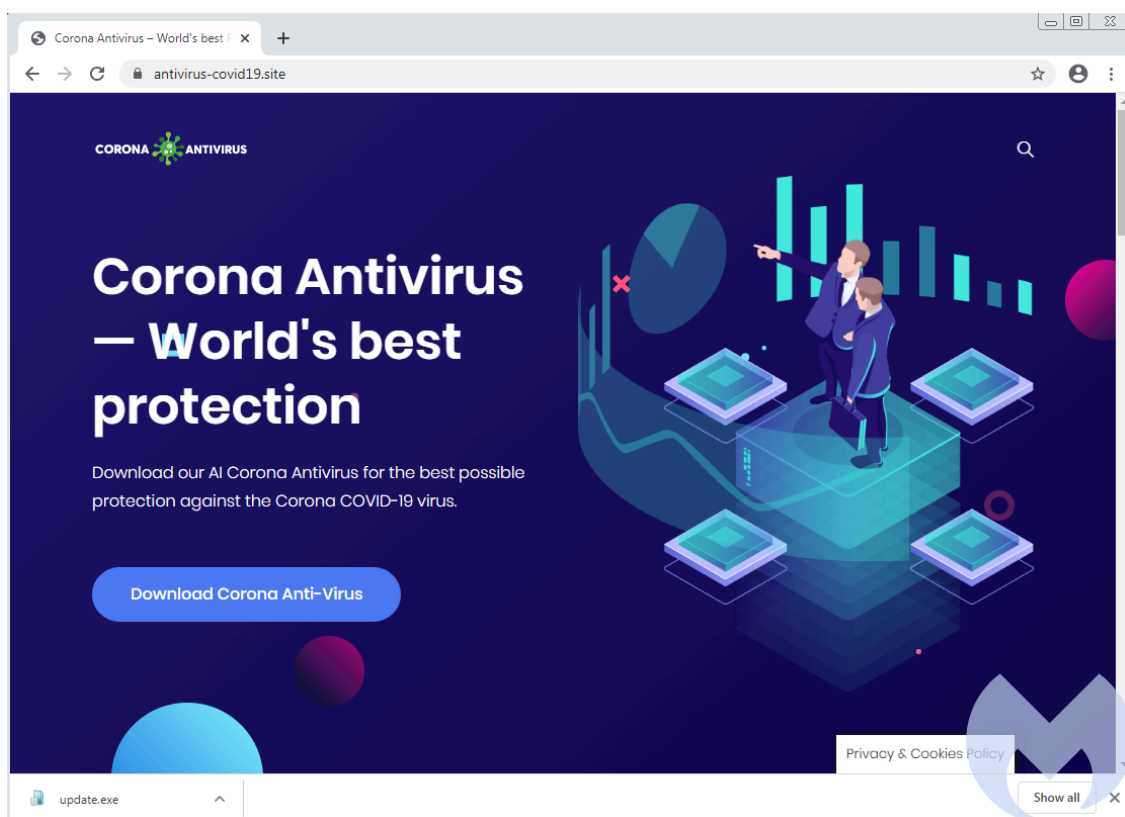
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

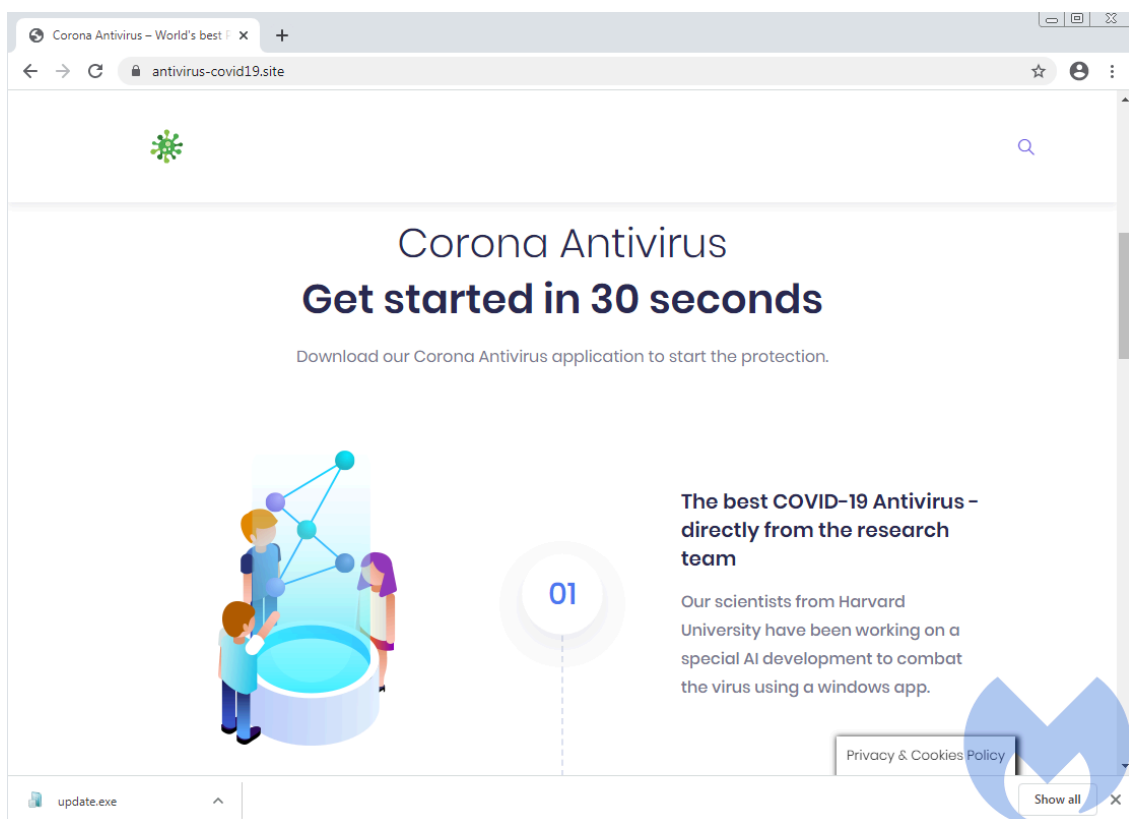
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

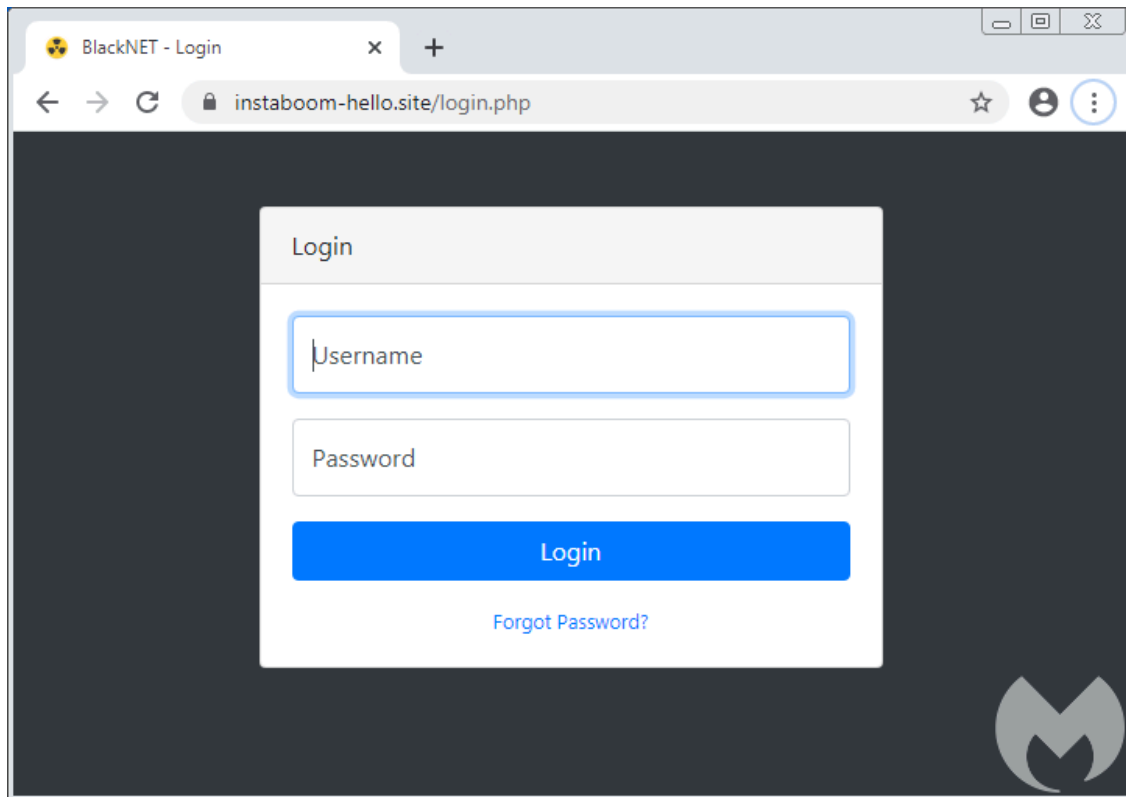


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

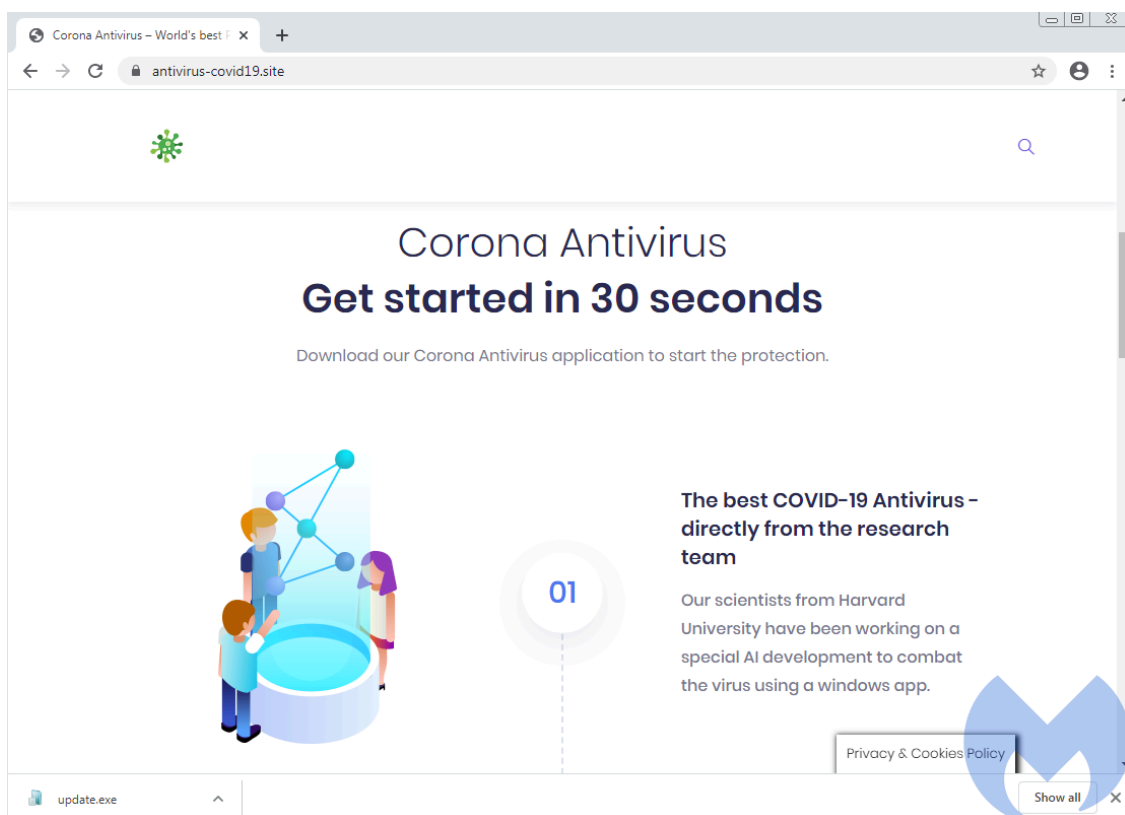
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

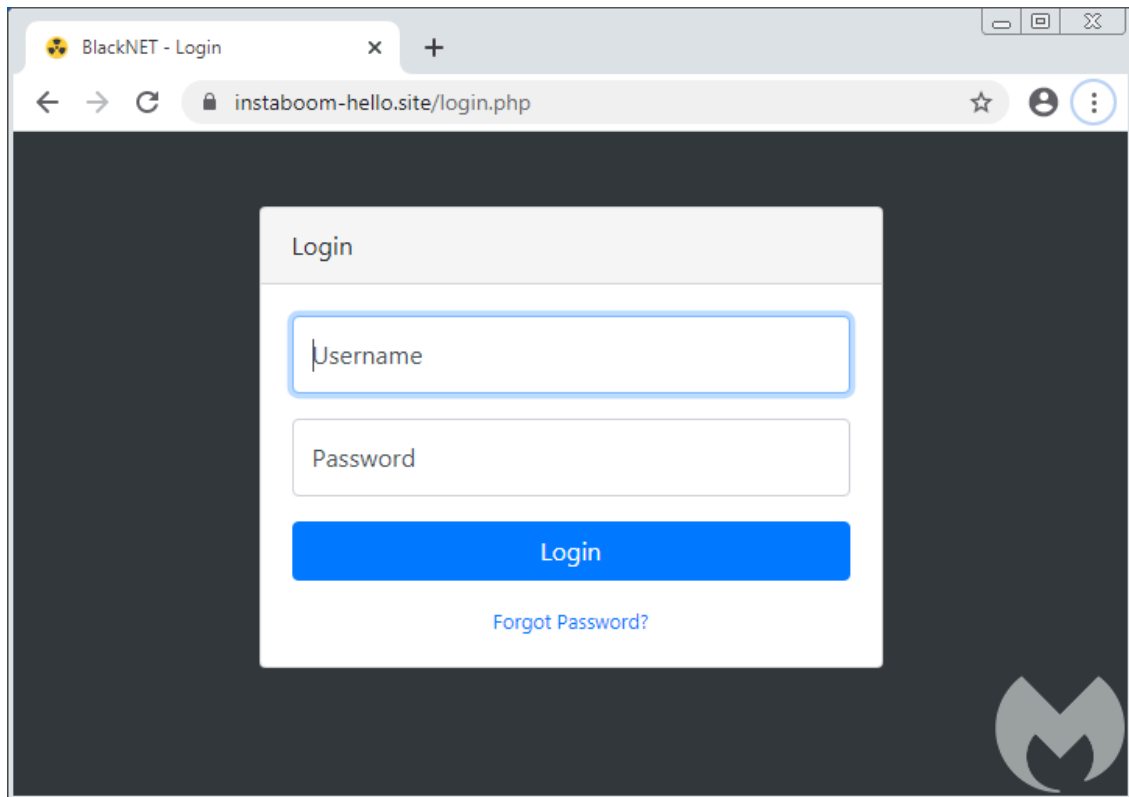


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

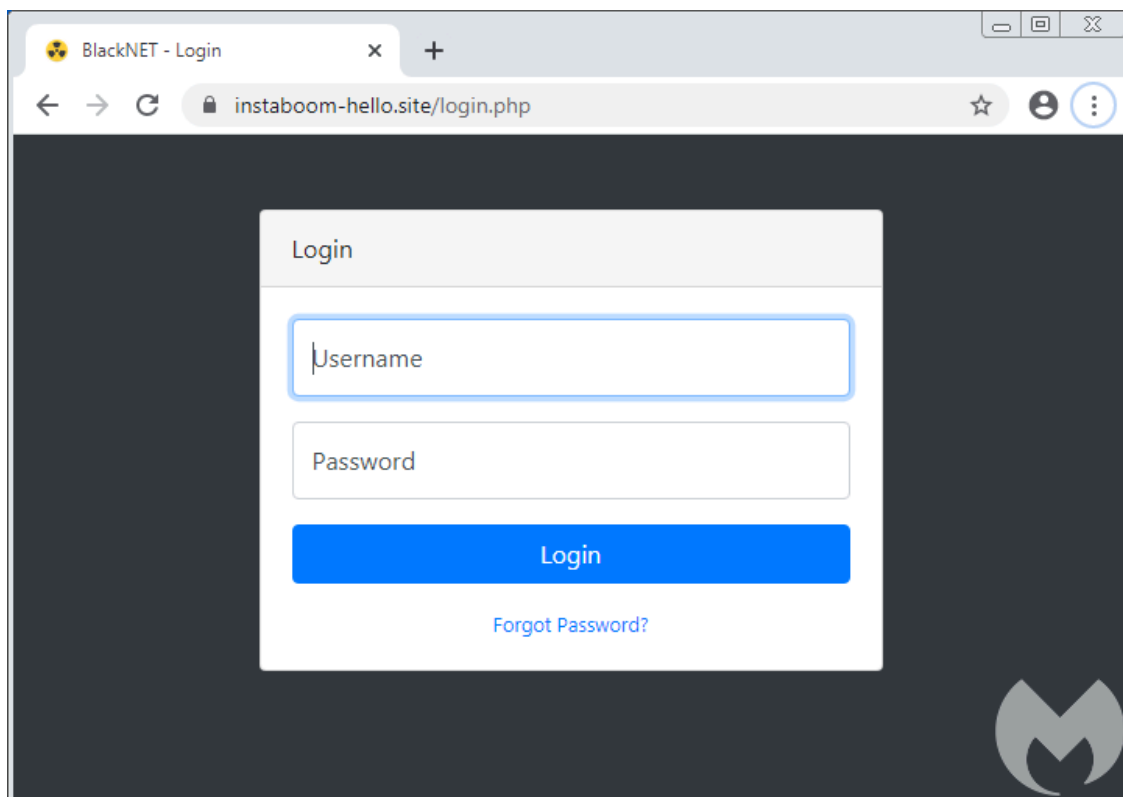
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

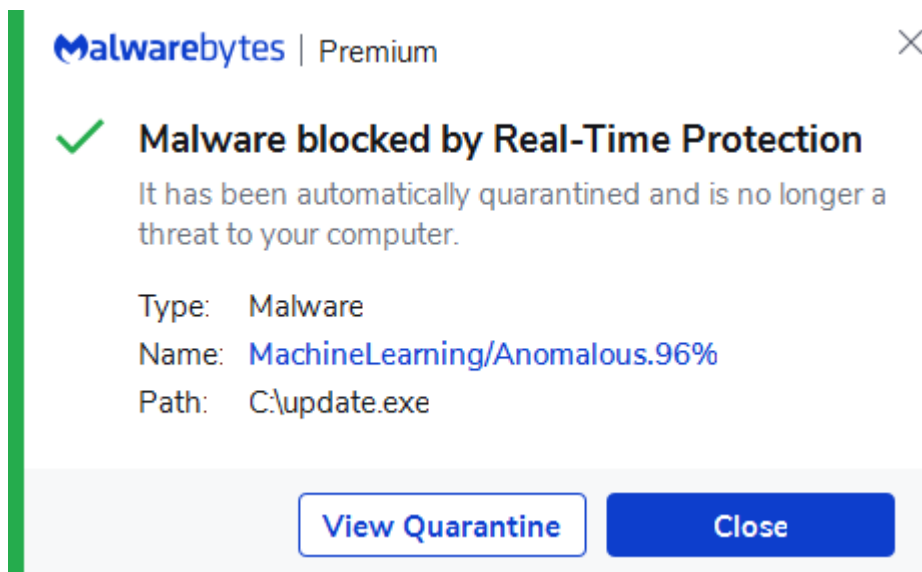
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

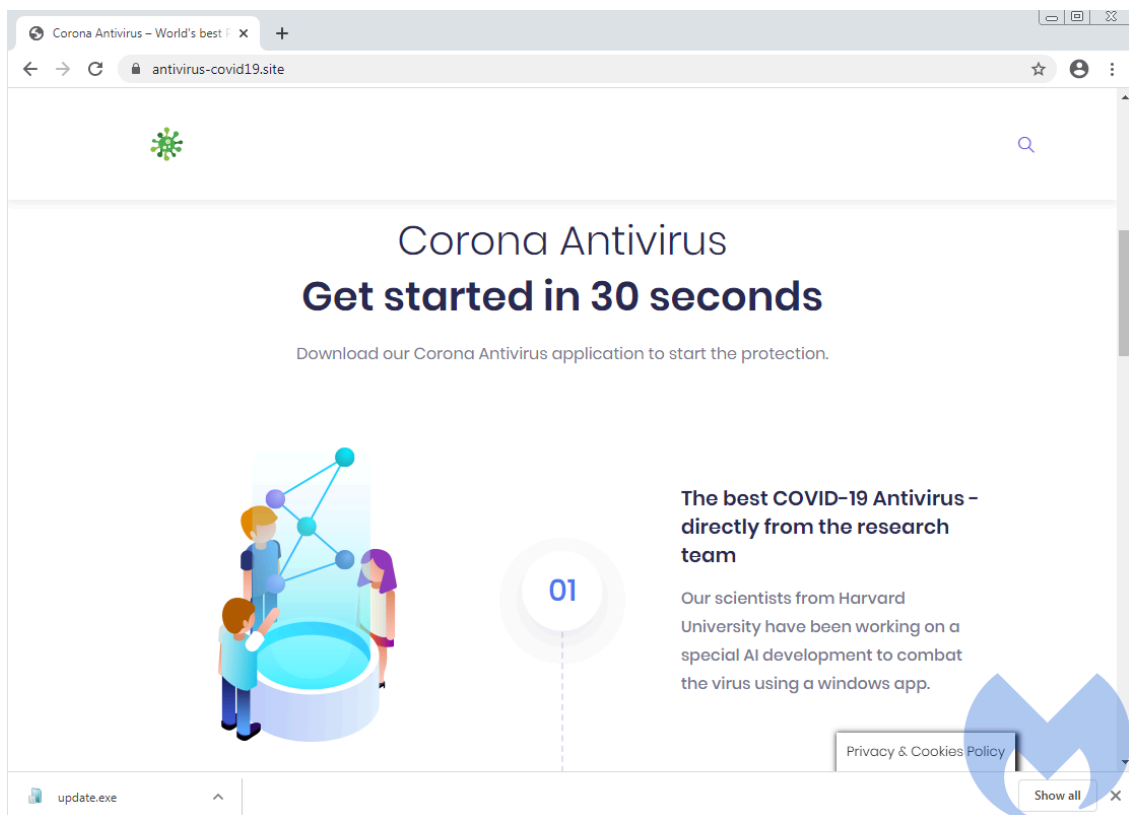
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

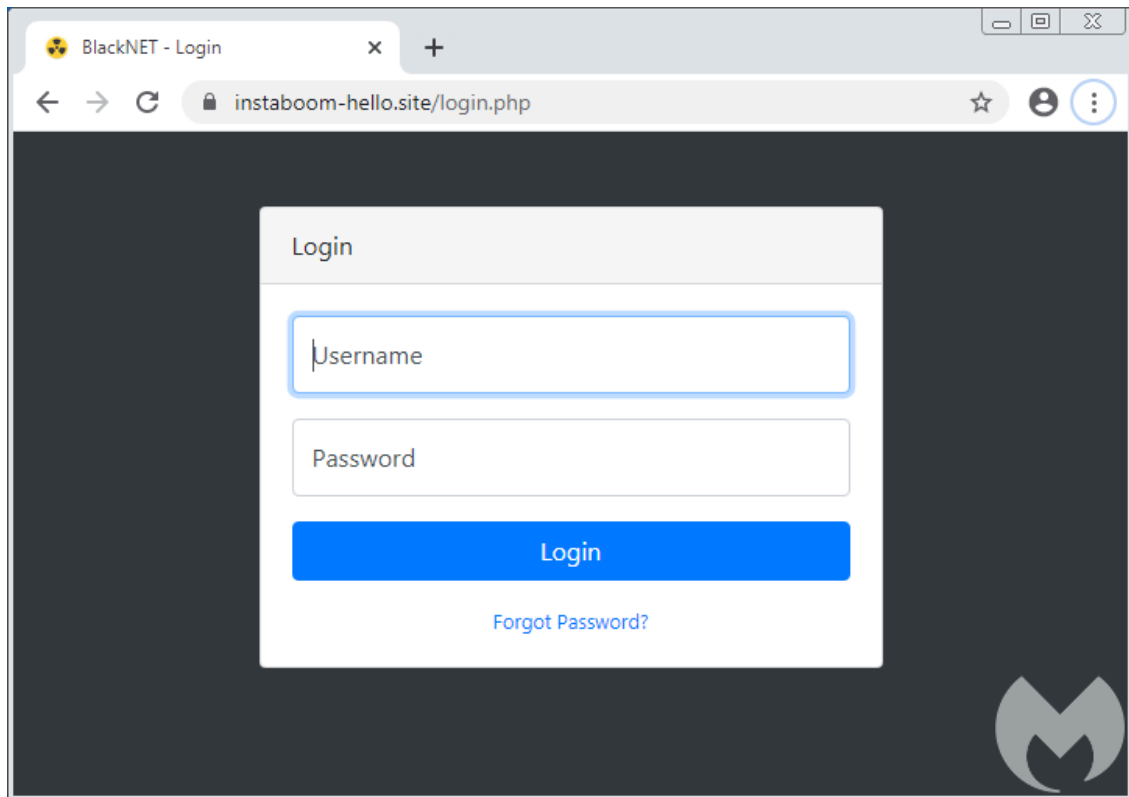


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

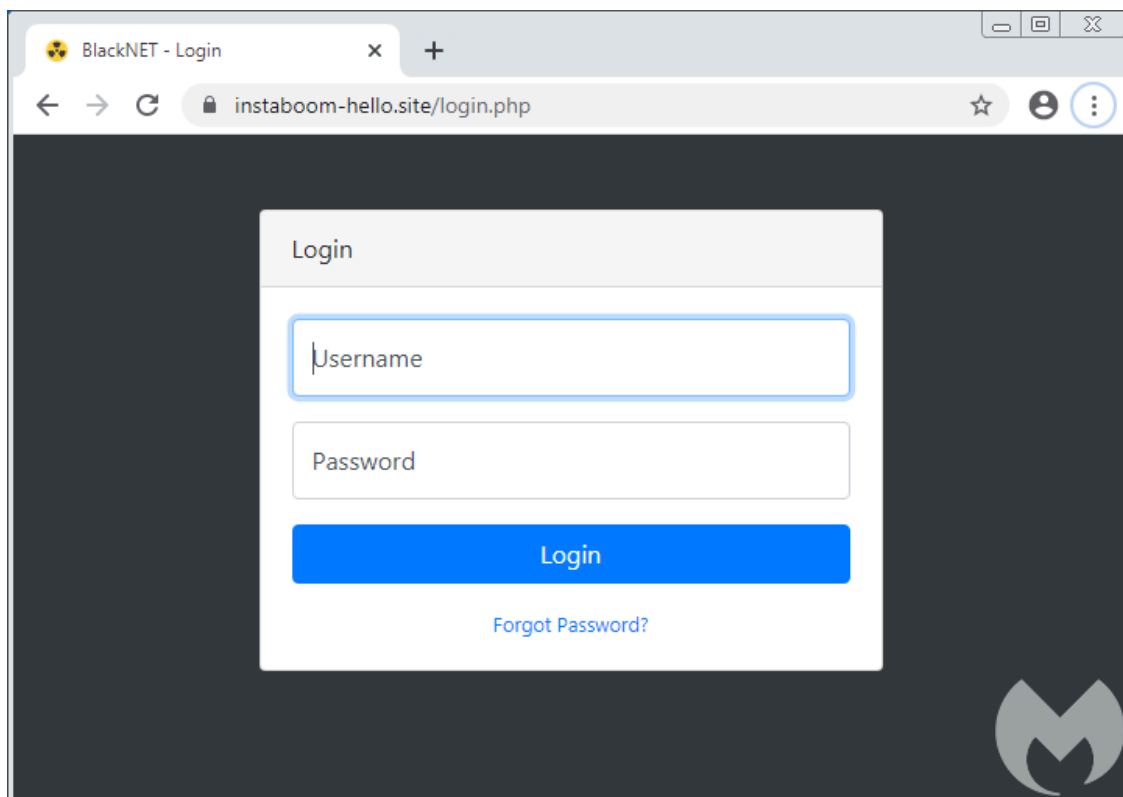
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

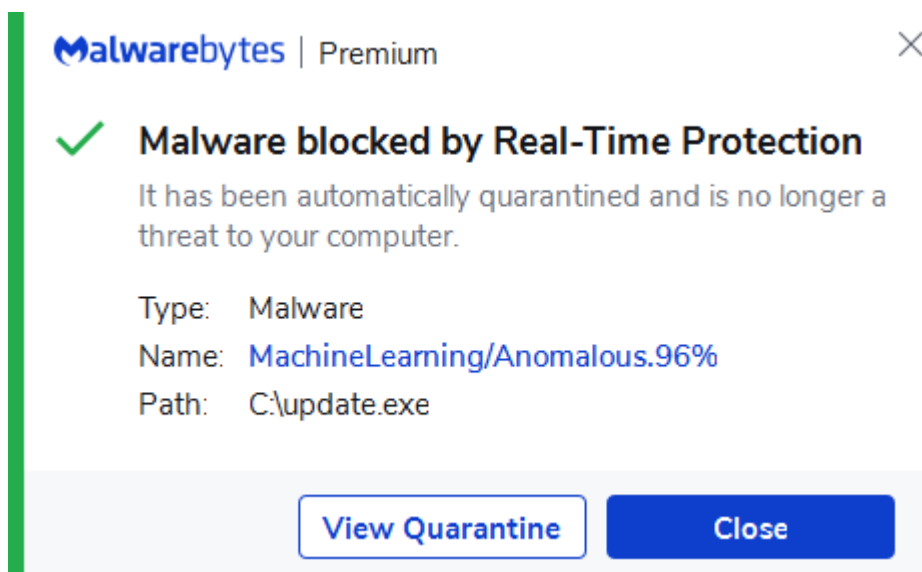
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a 'Select Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

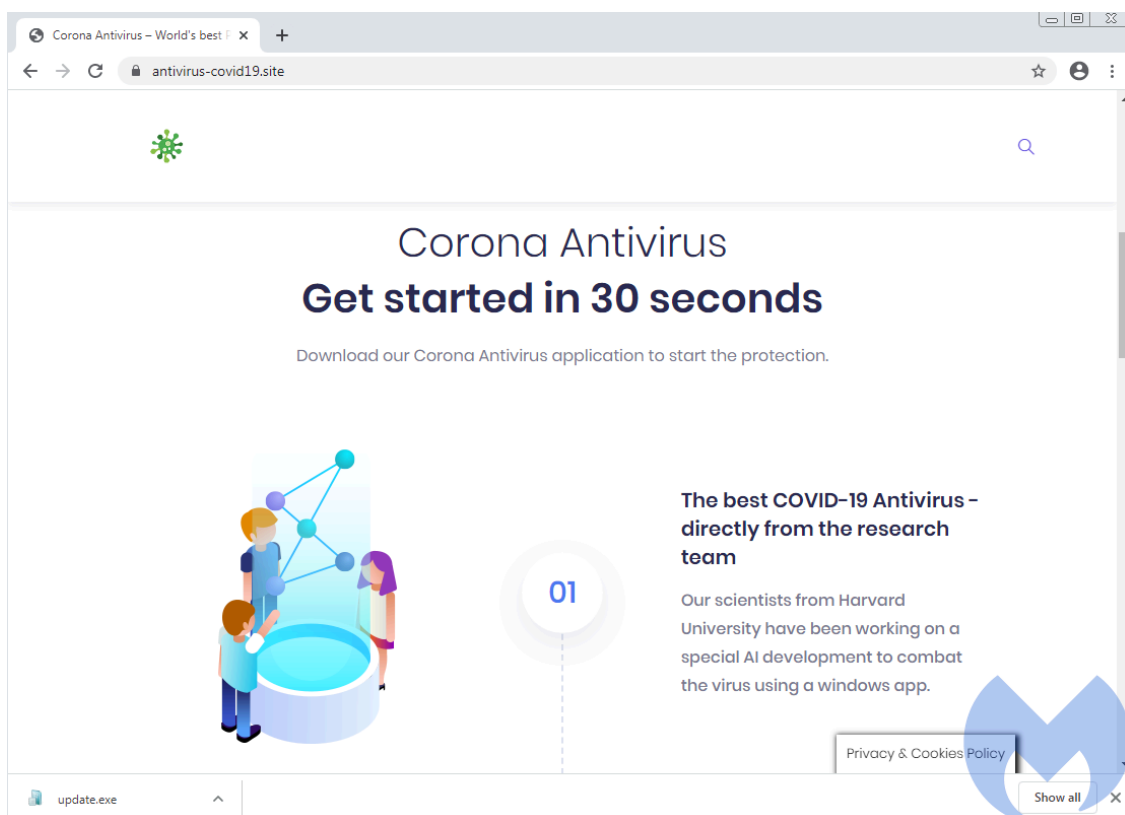
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

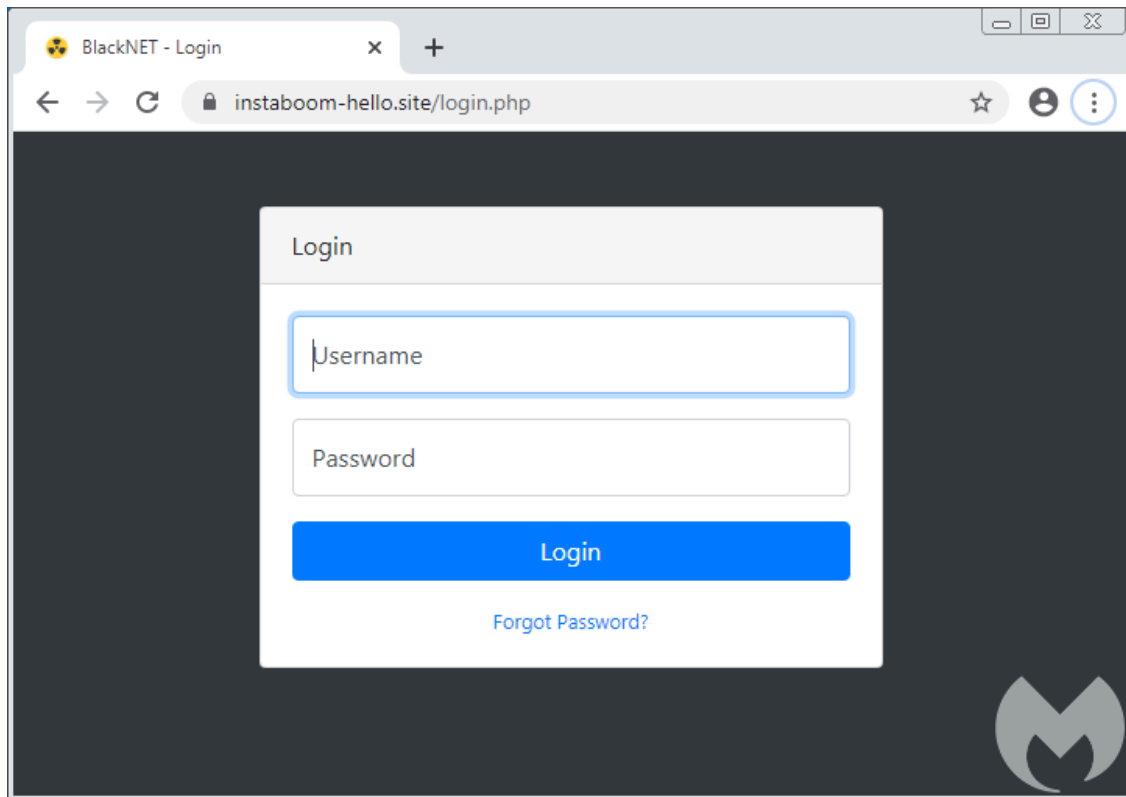


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

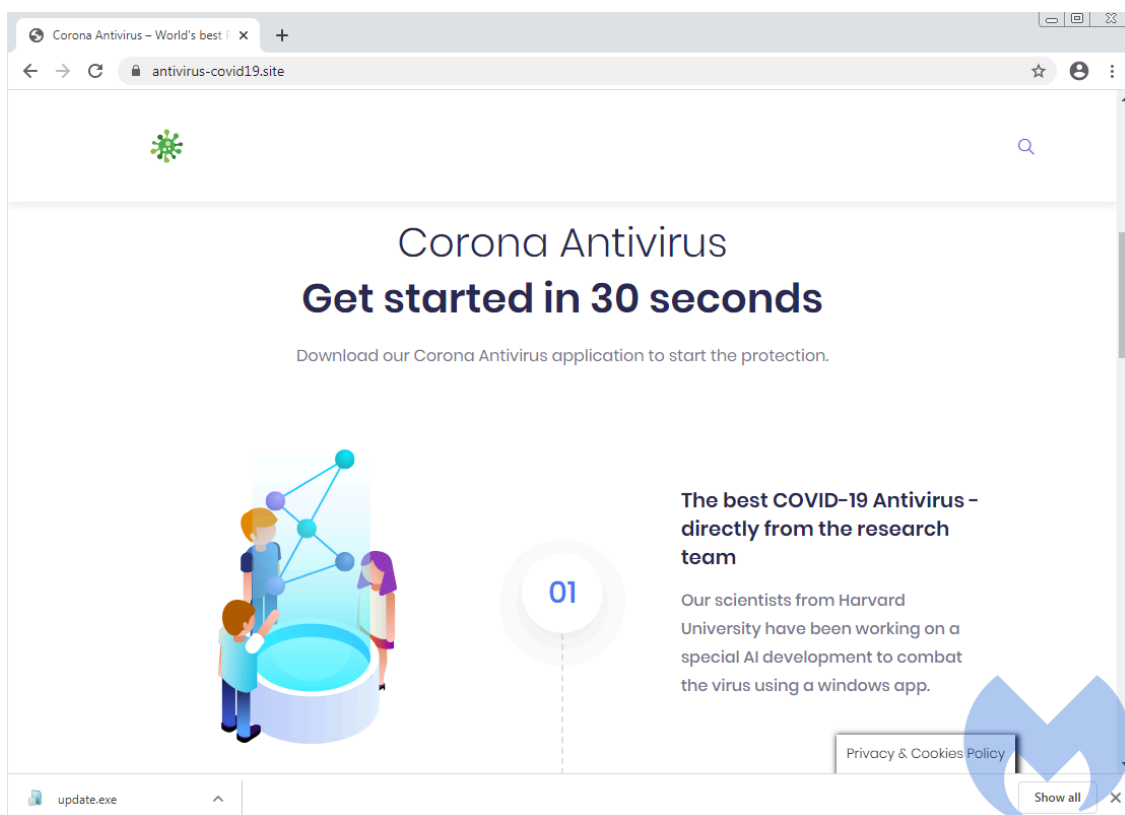
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

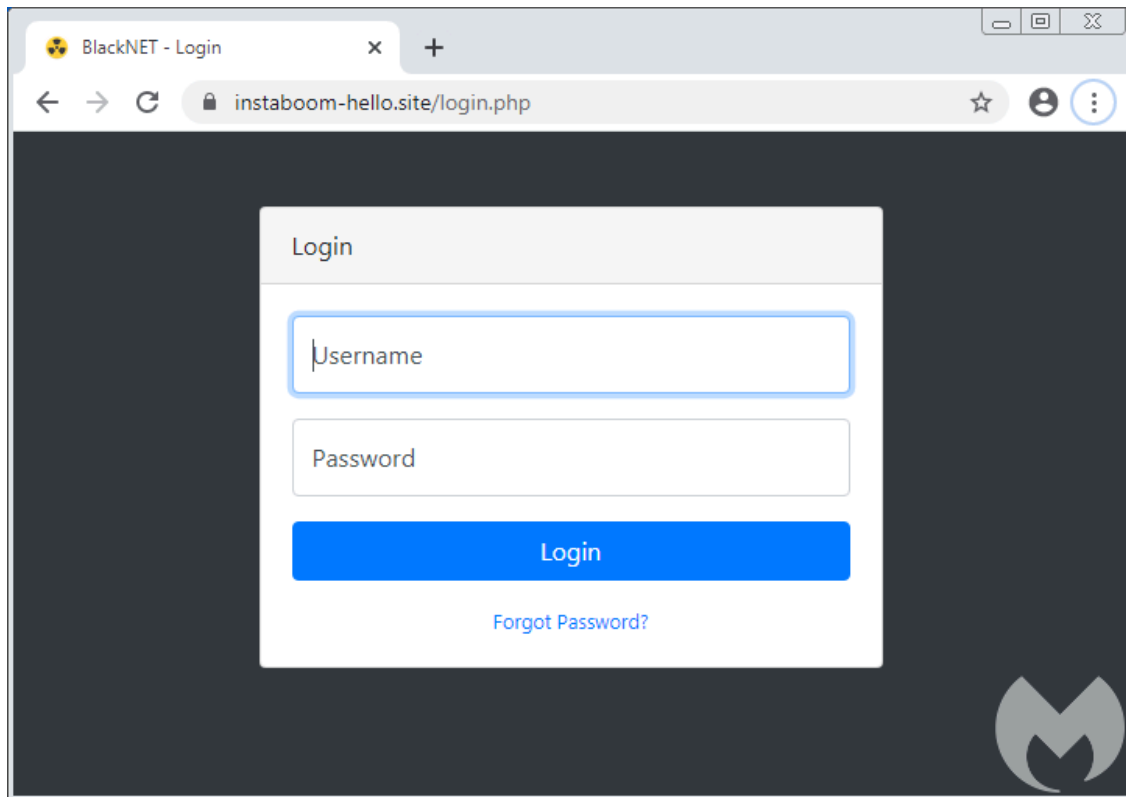


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

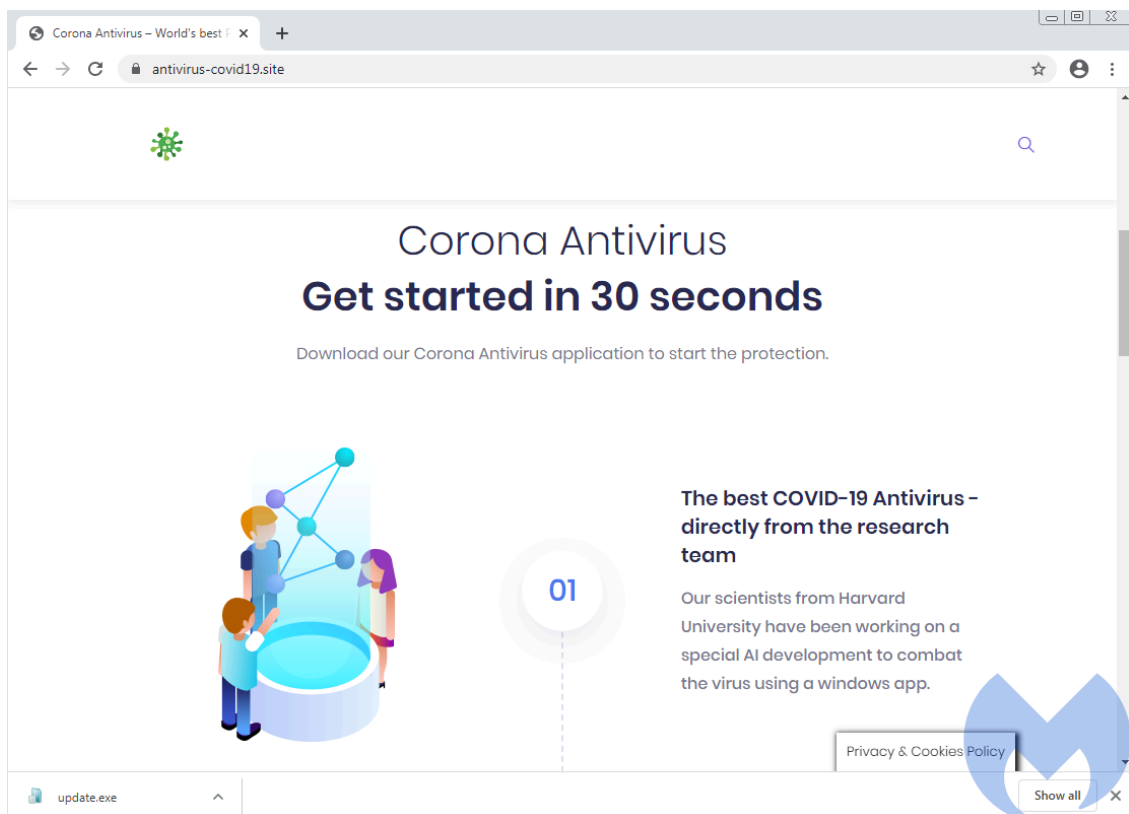
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

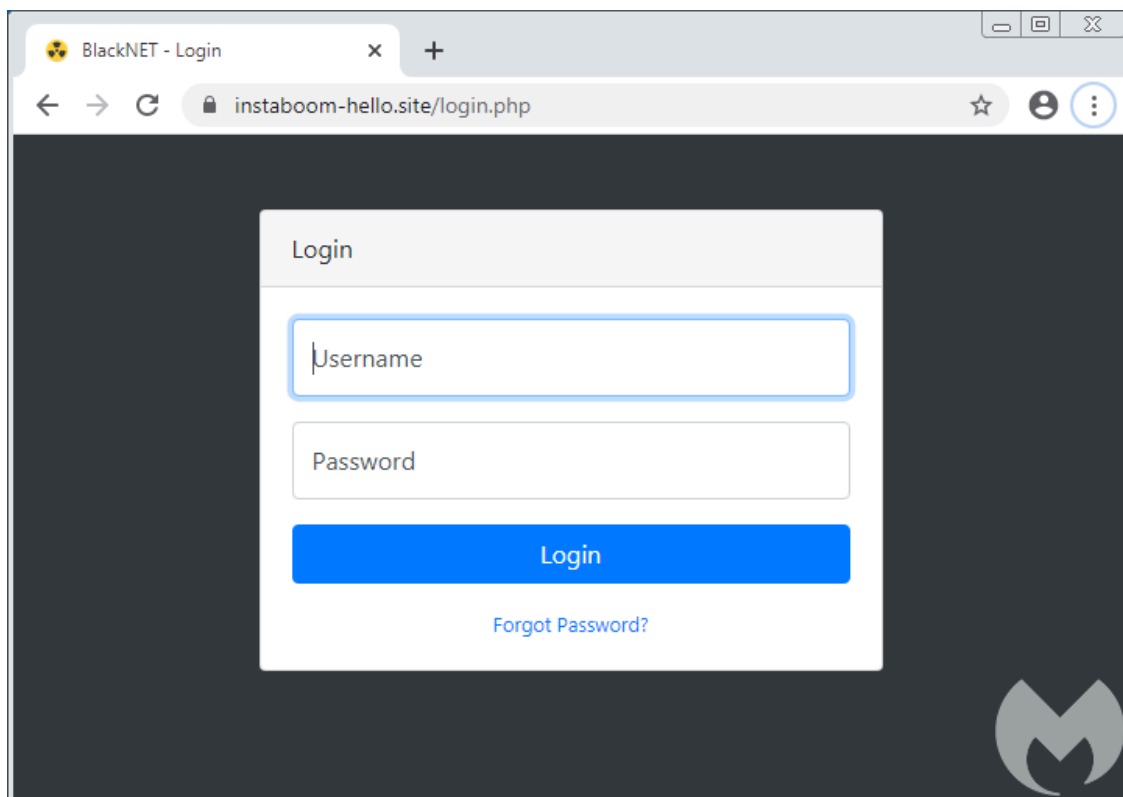


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

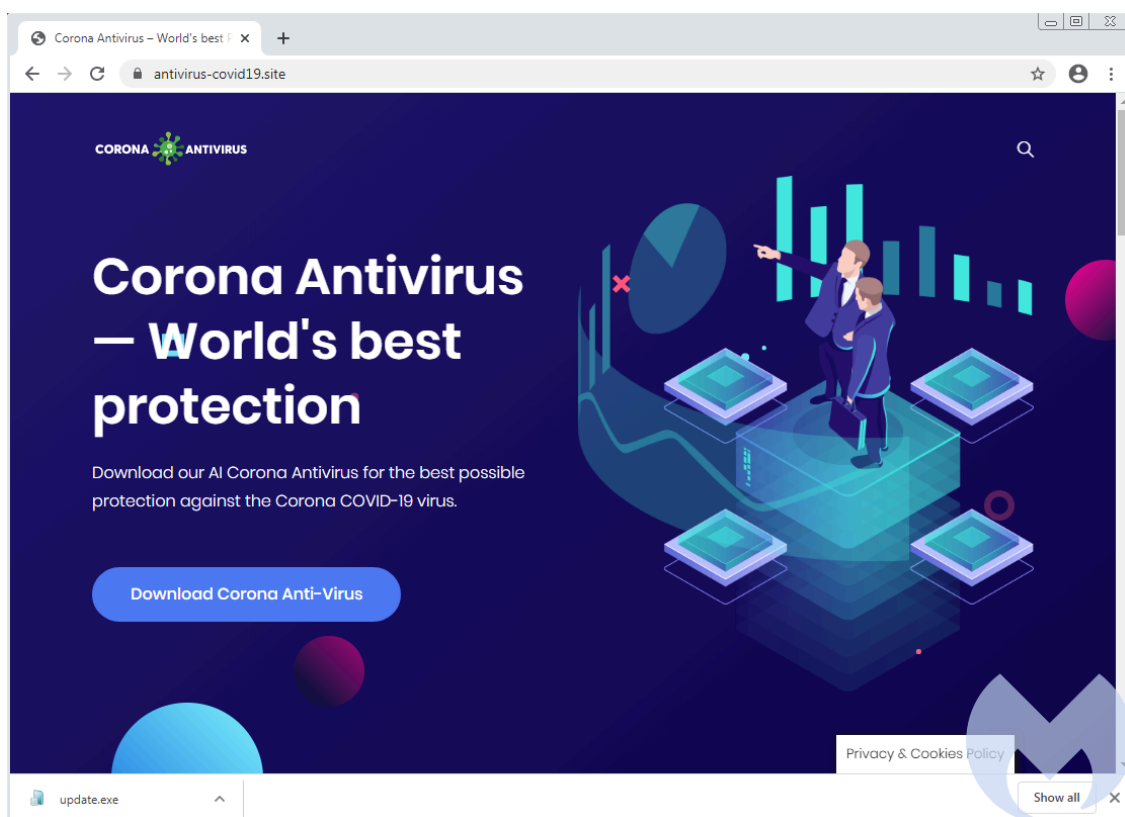
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

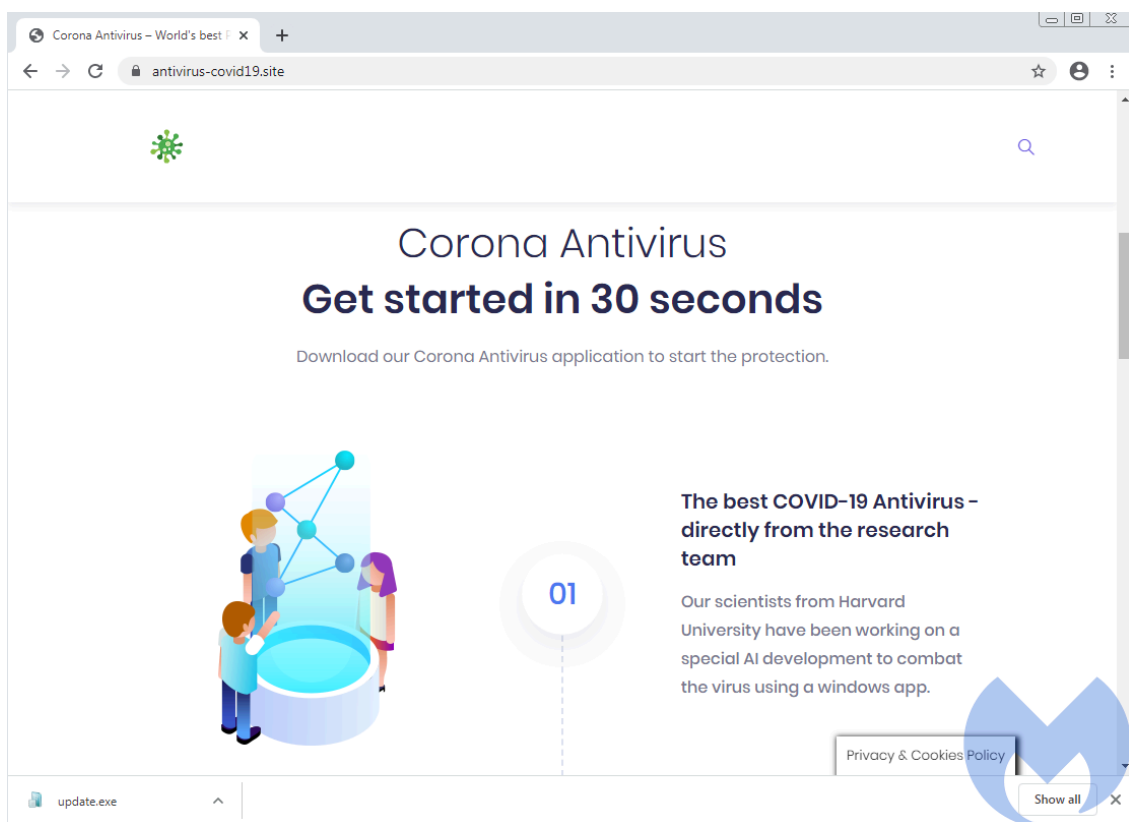
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

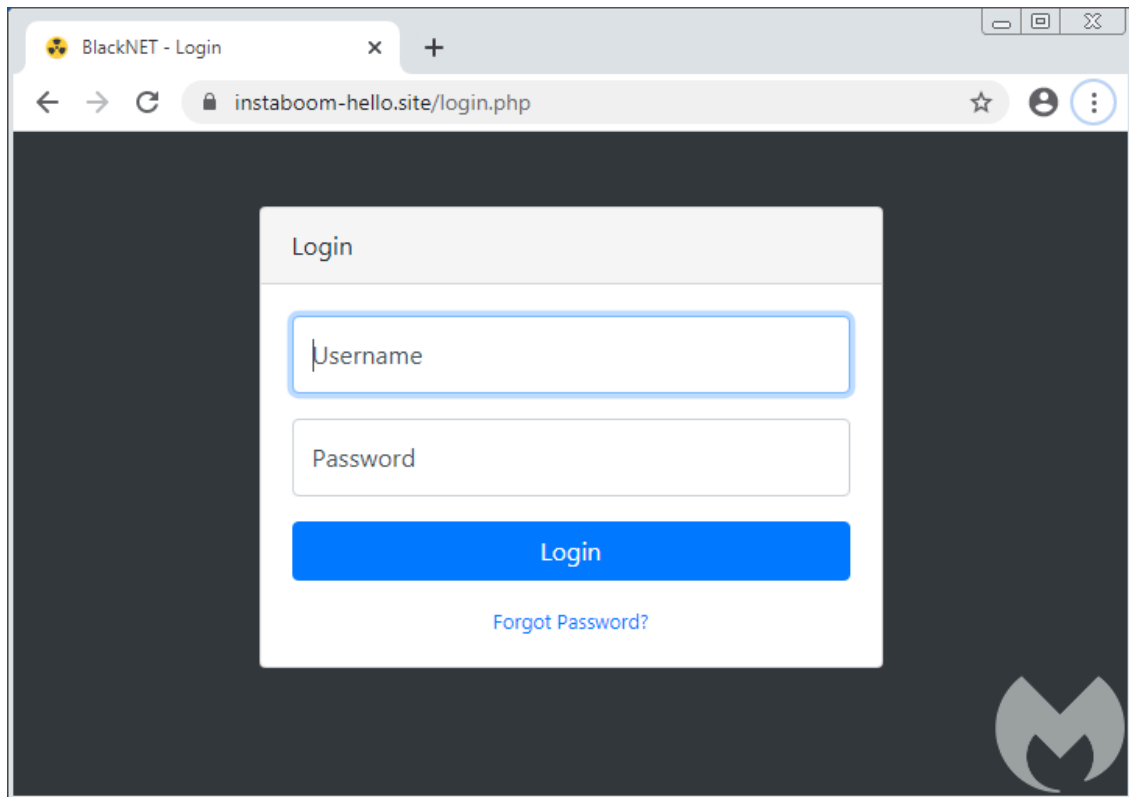


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

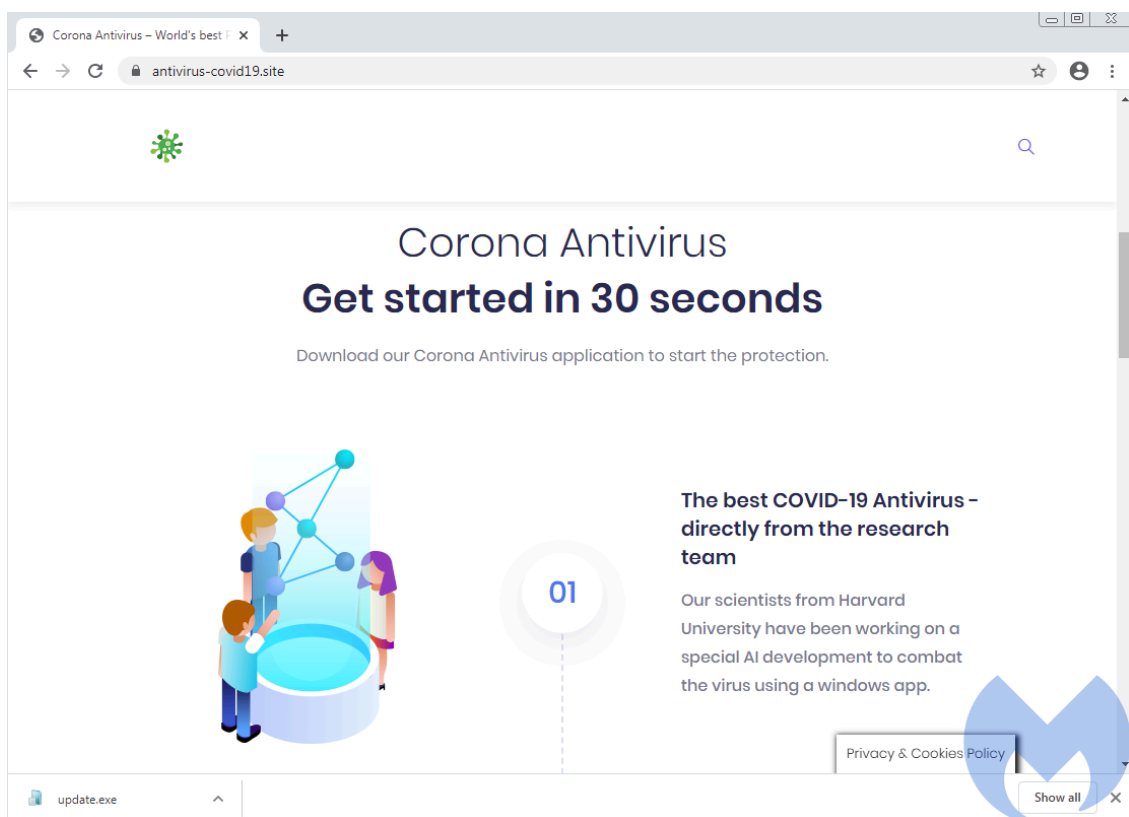
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

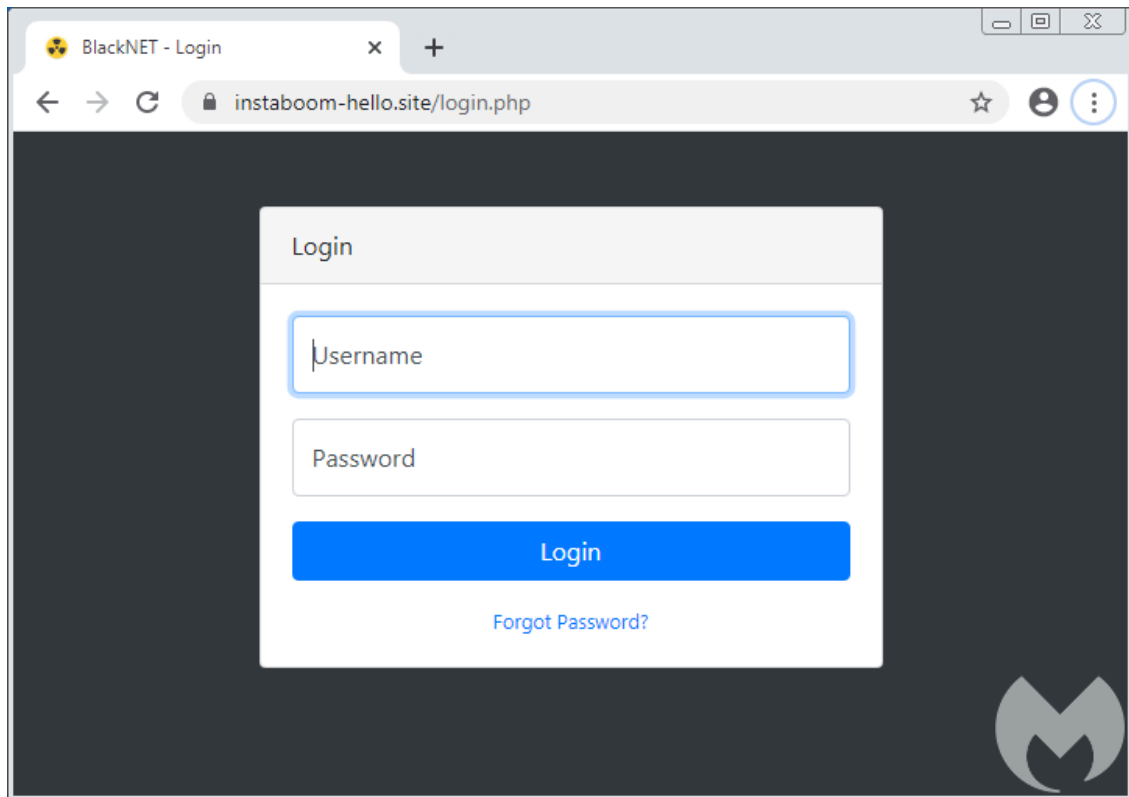


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

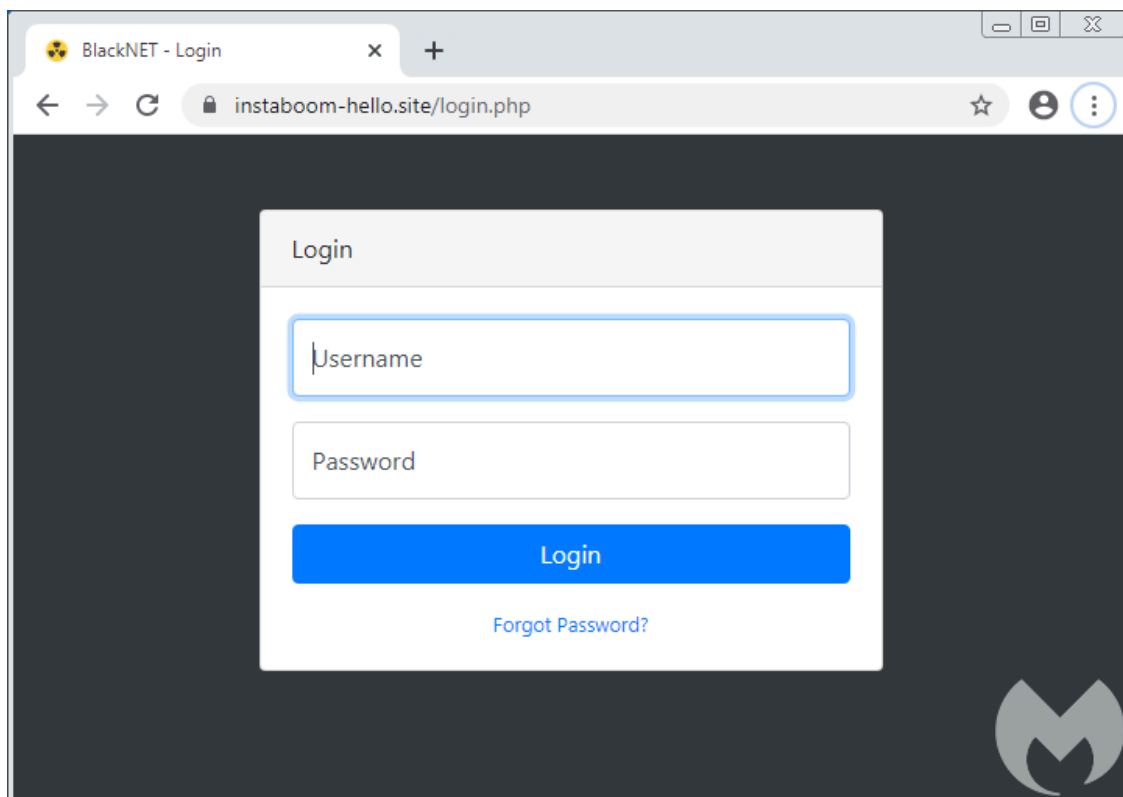
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

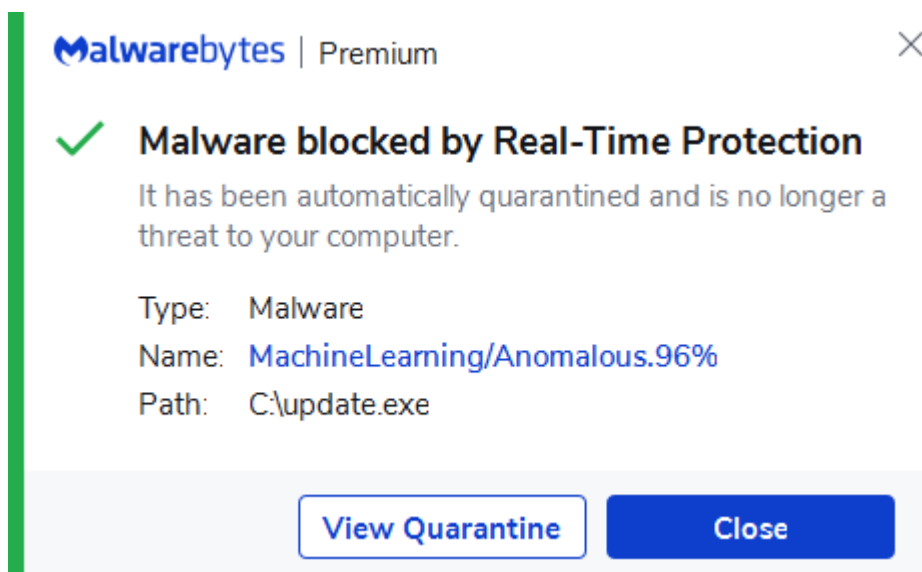
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

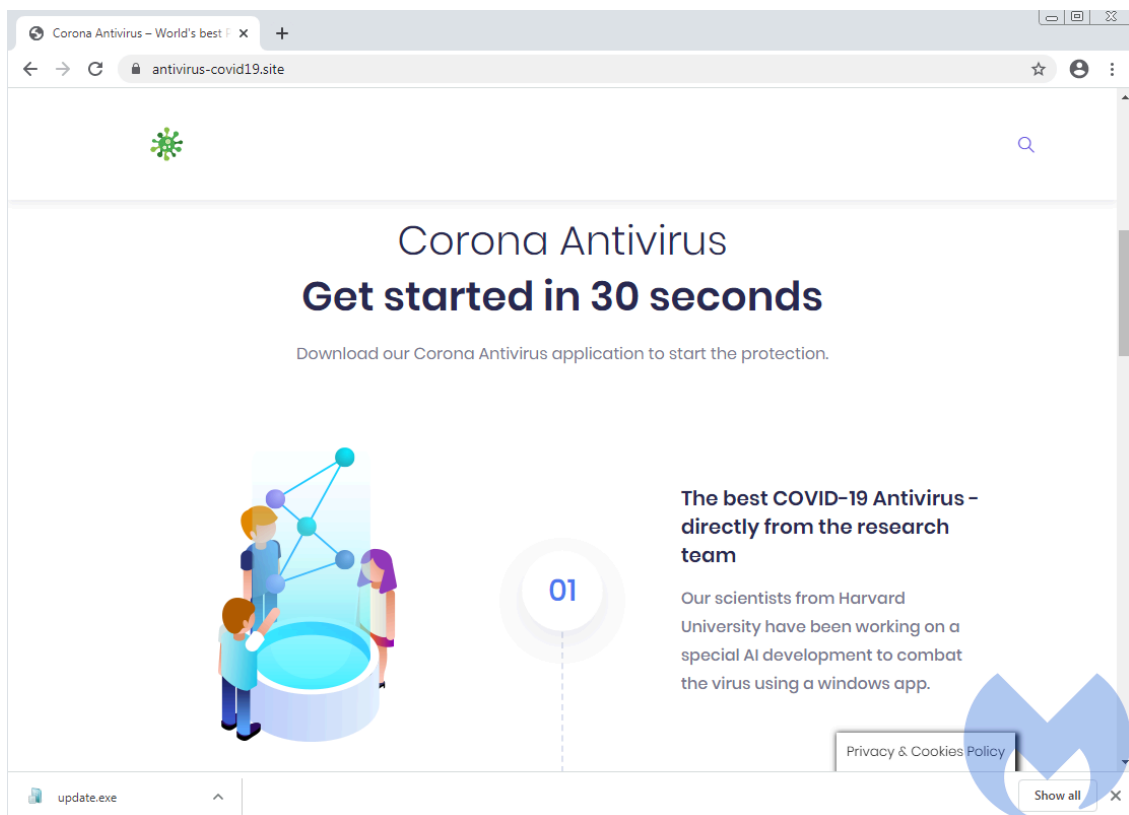
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

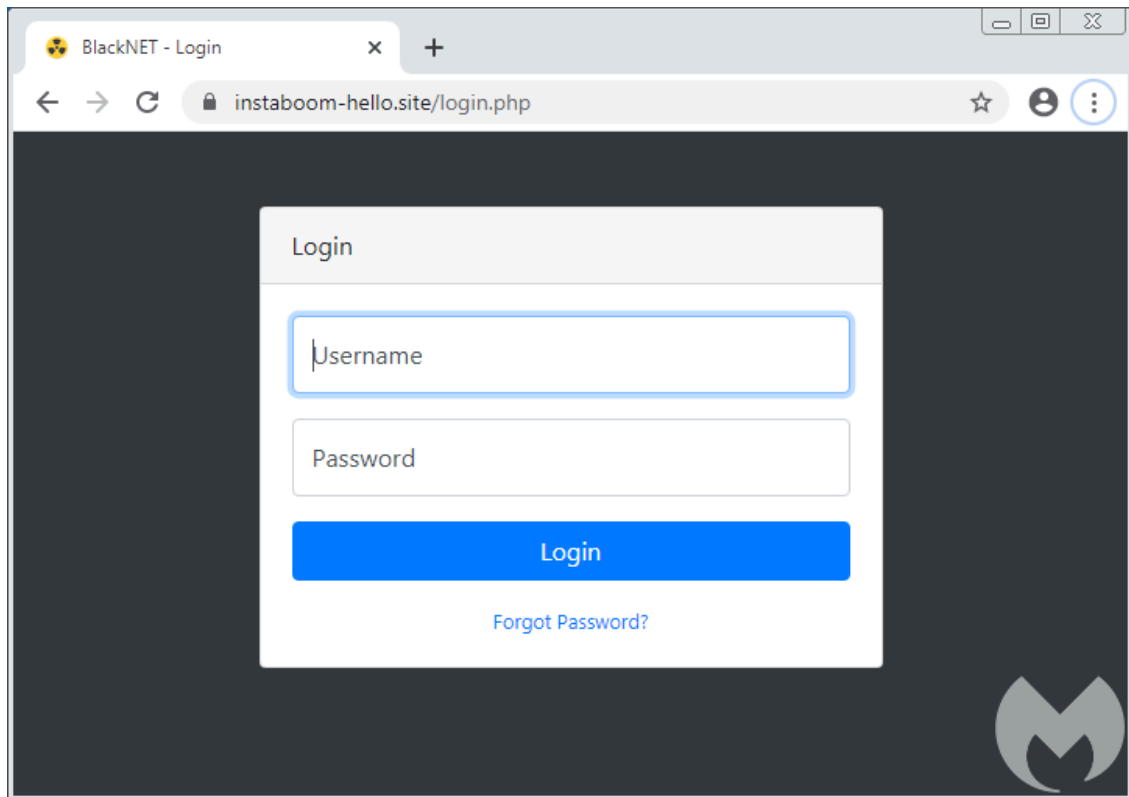


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

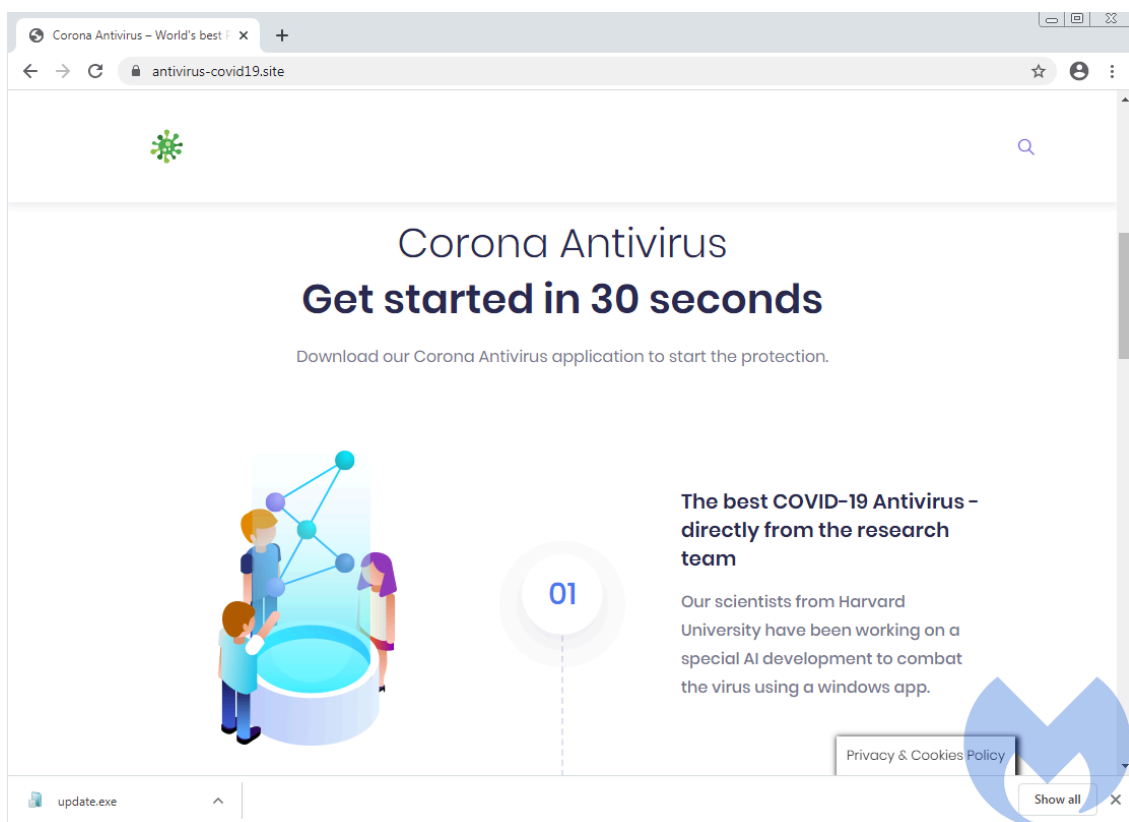
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

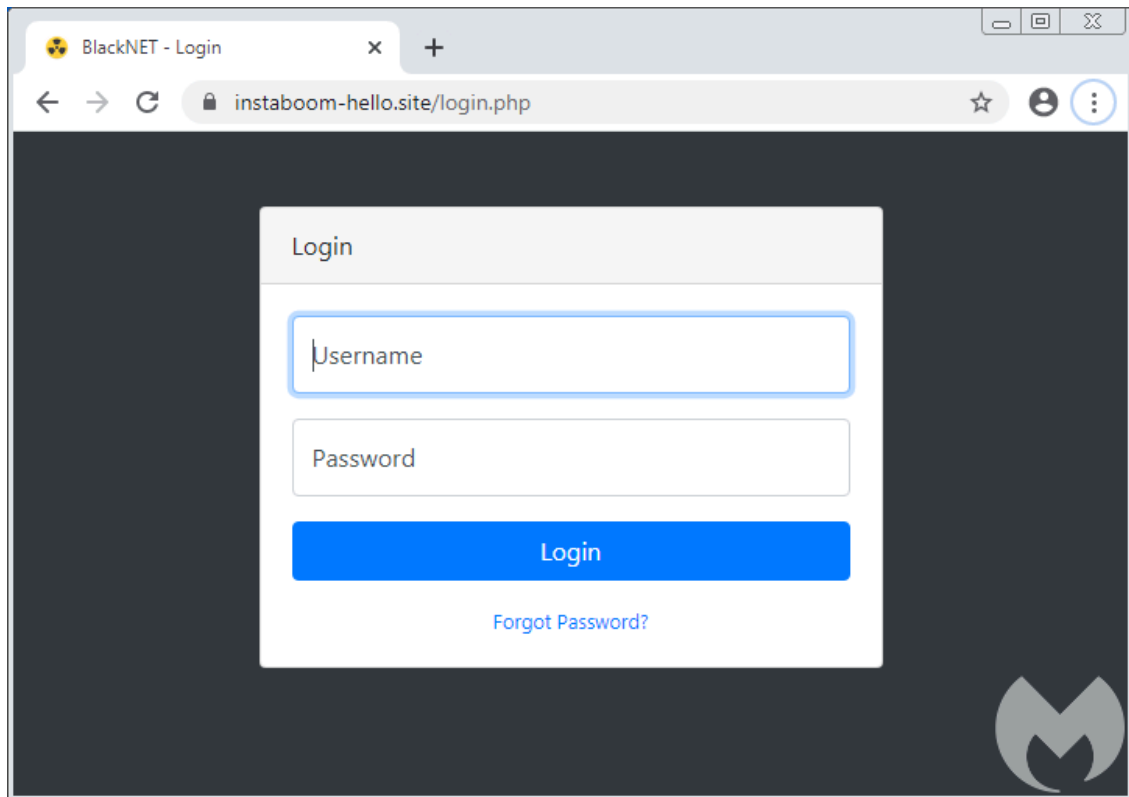


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

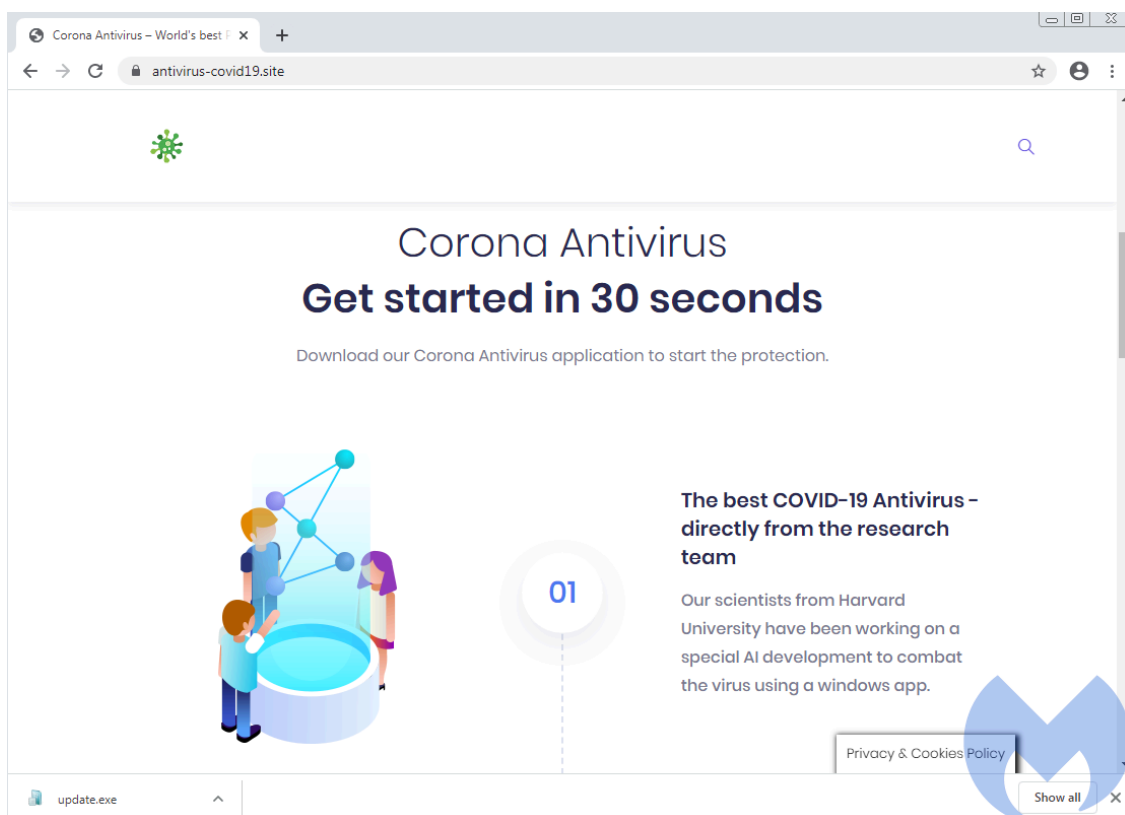
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

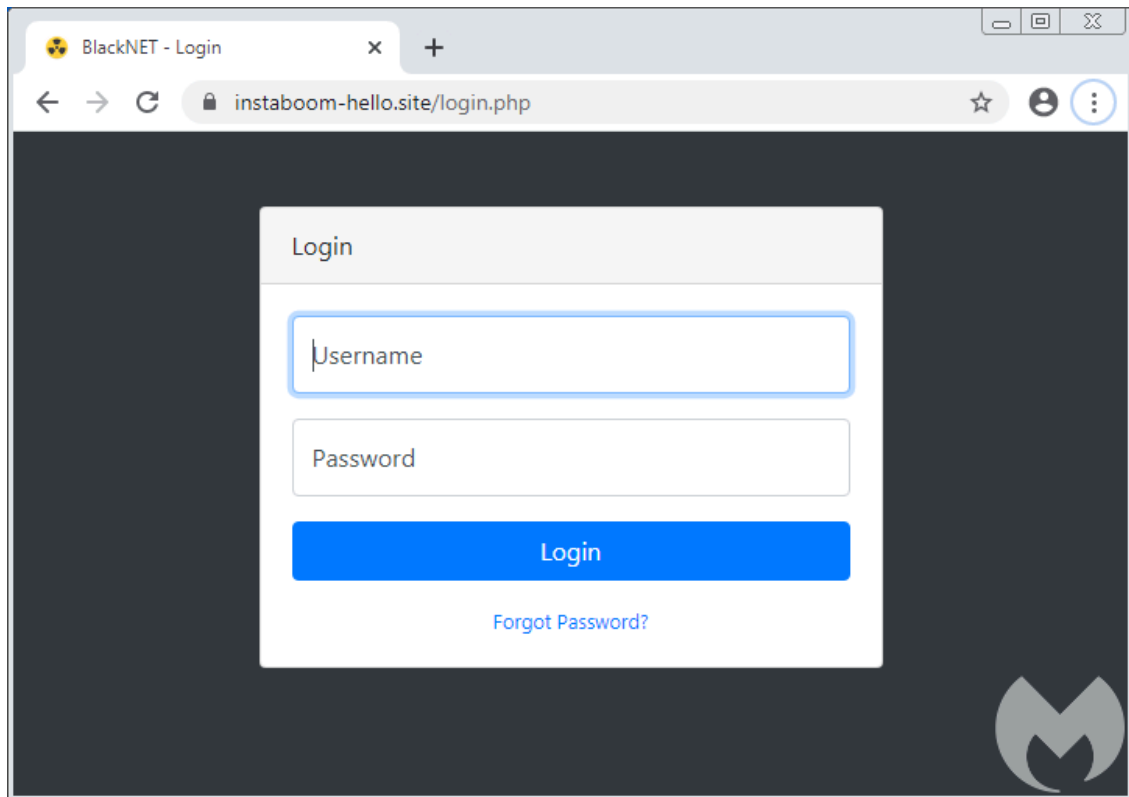


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

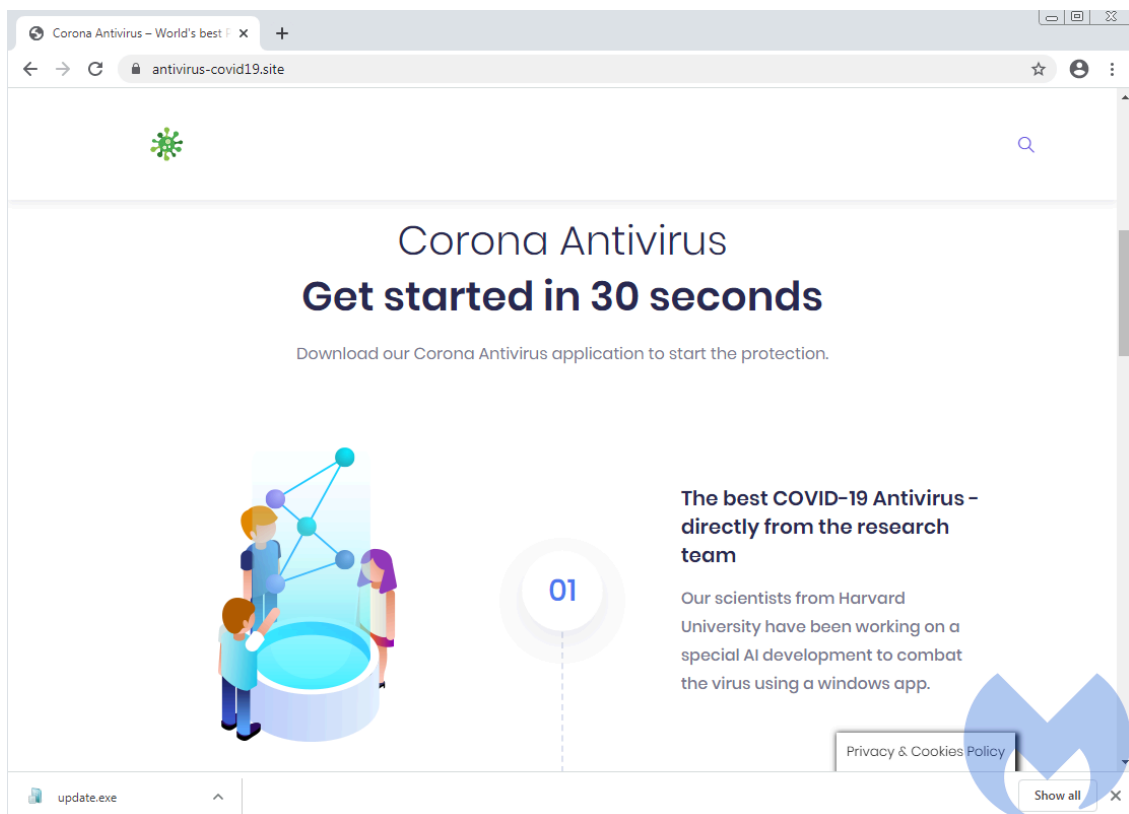
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

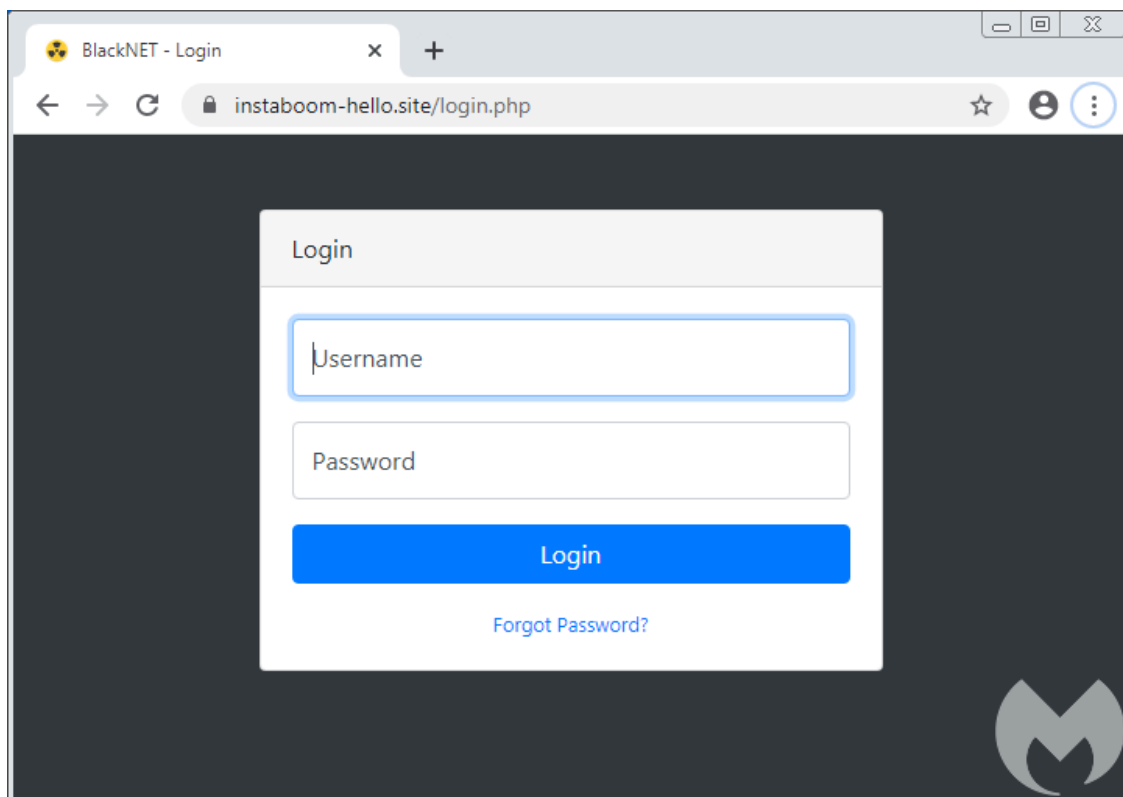


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

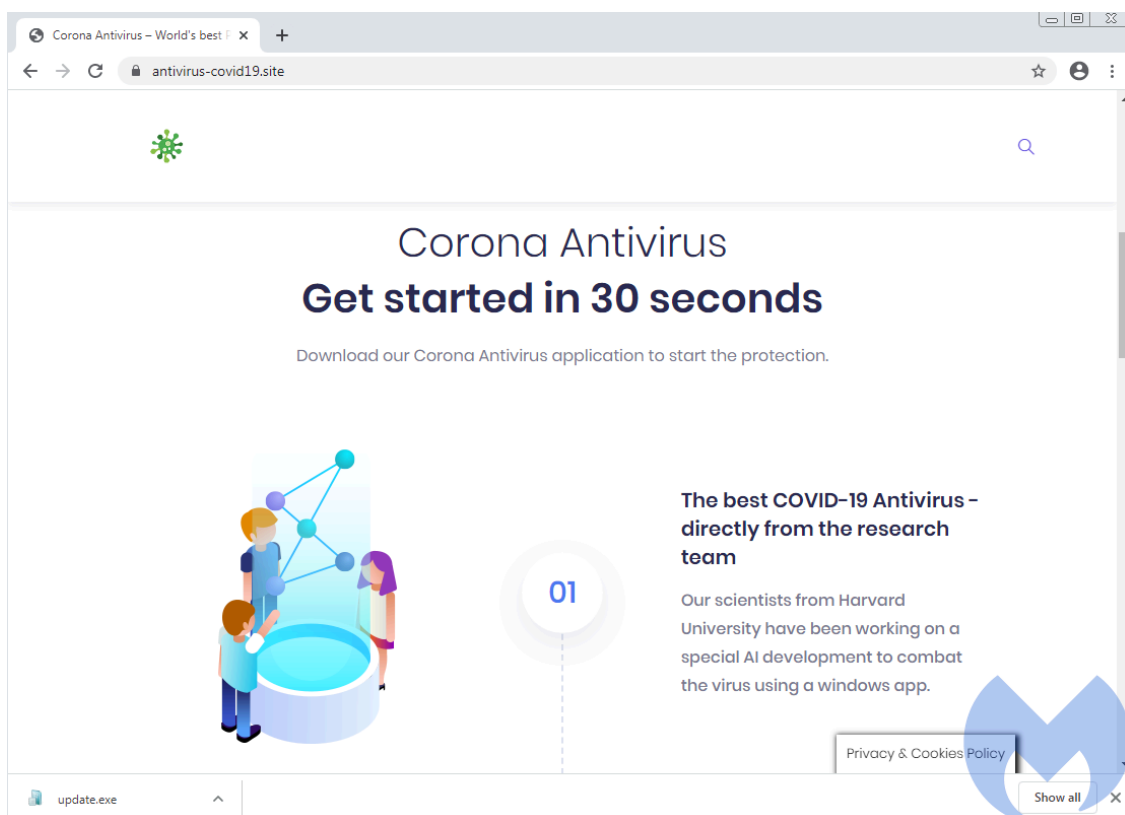
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

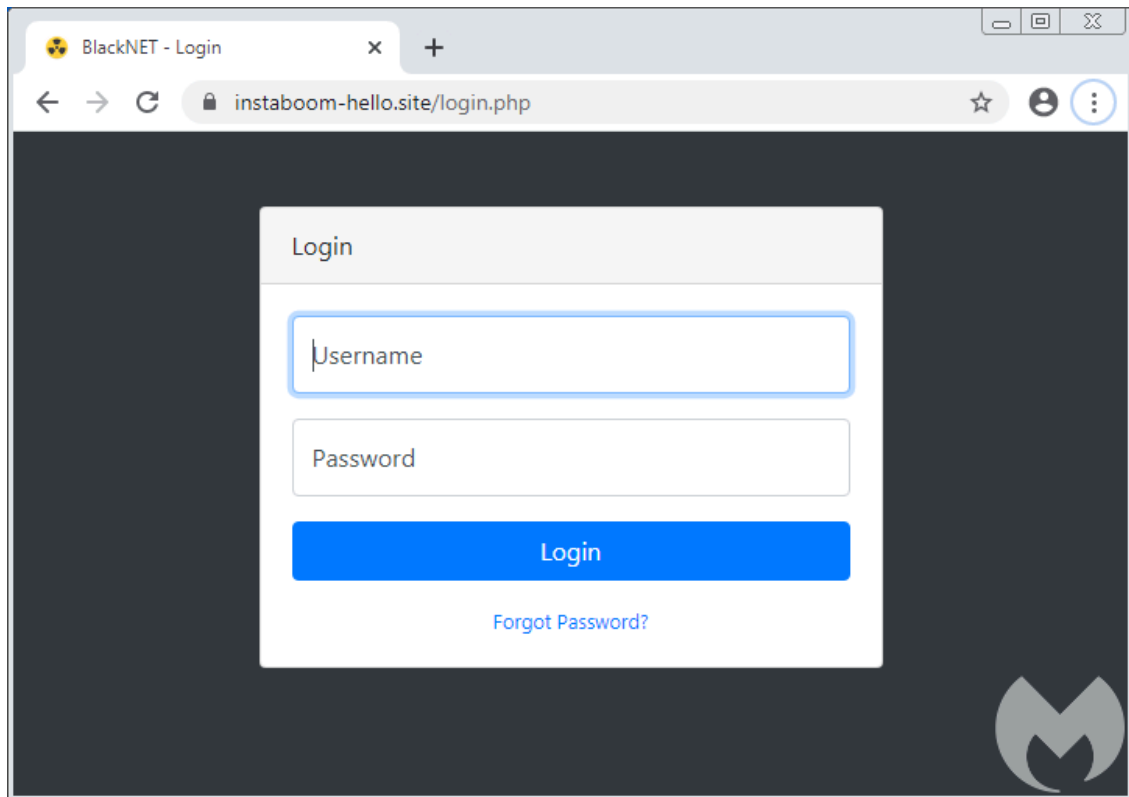


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

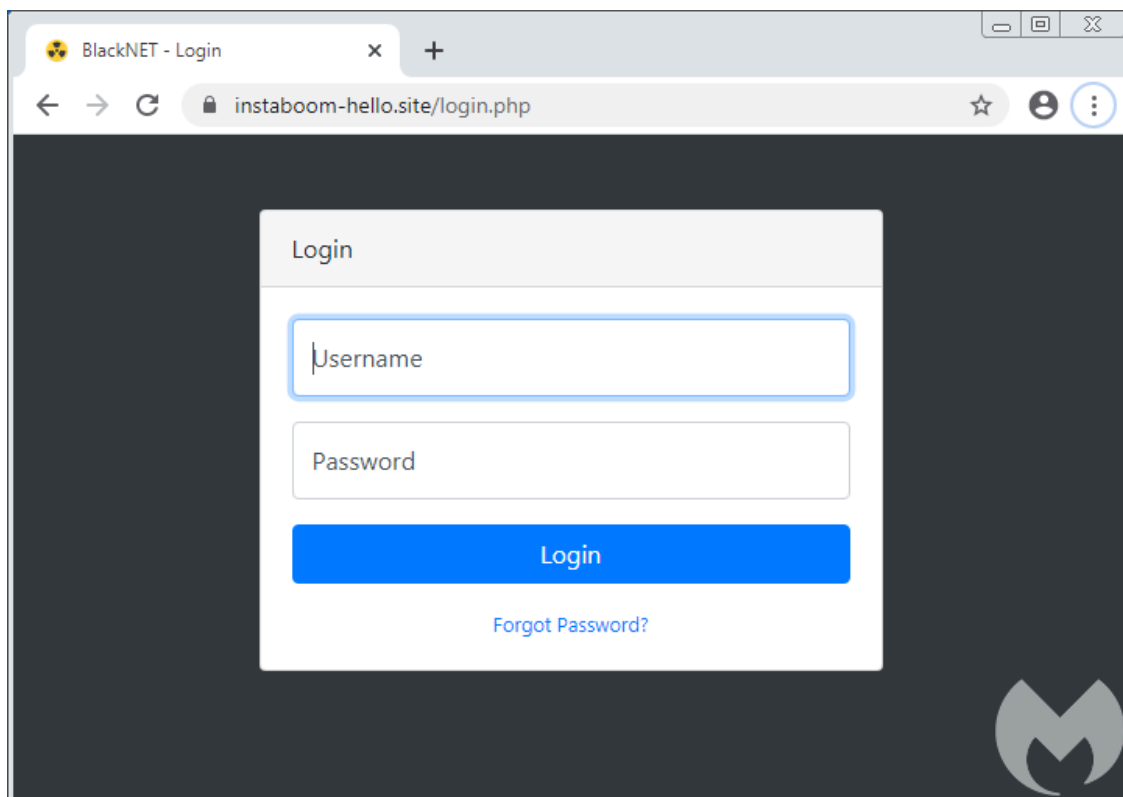
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

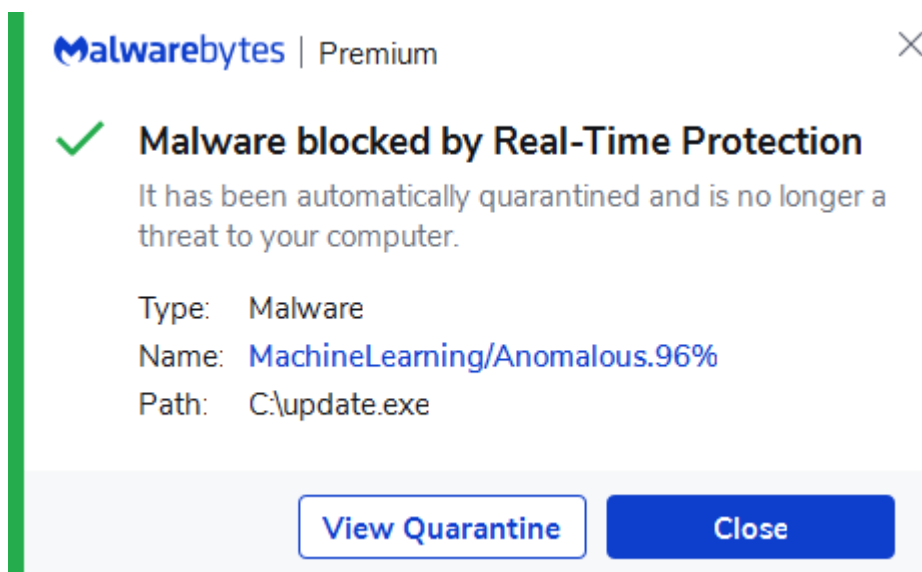
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

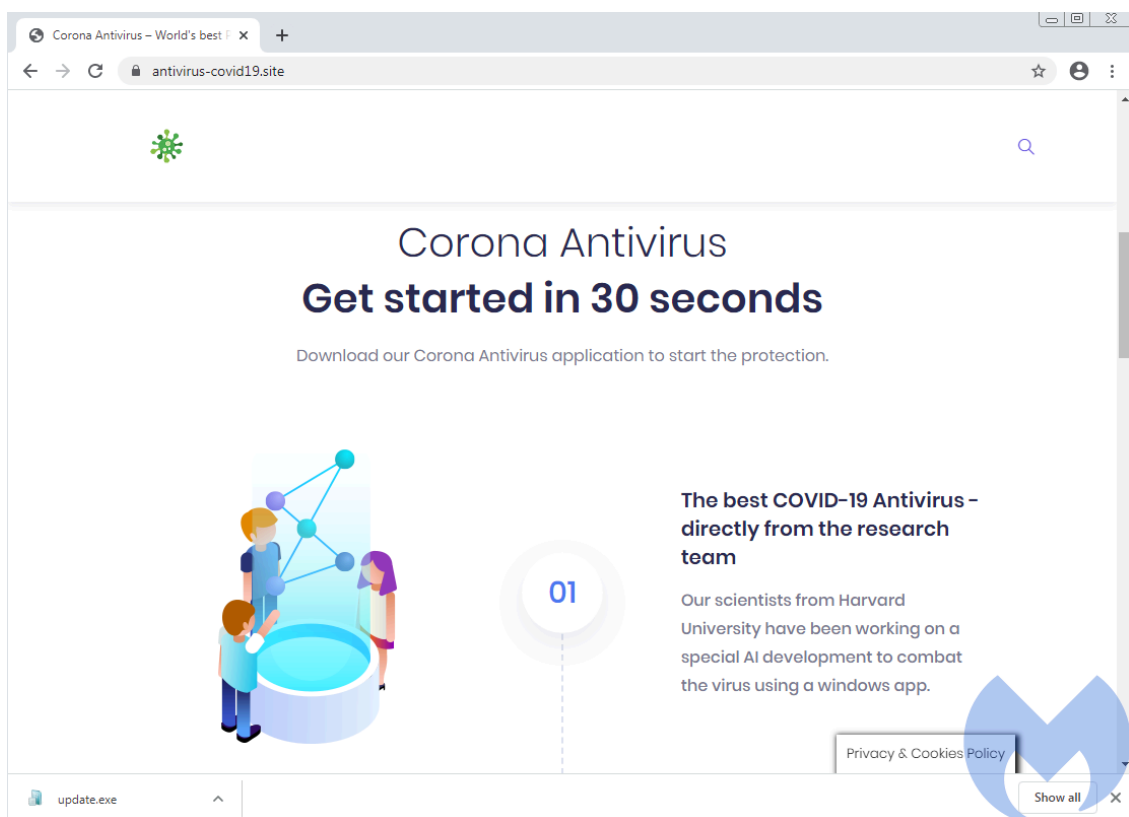
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

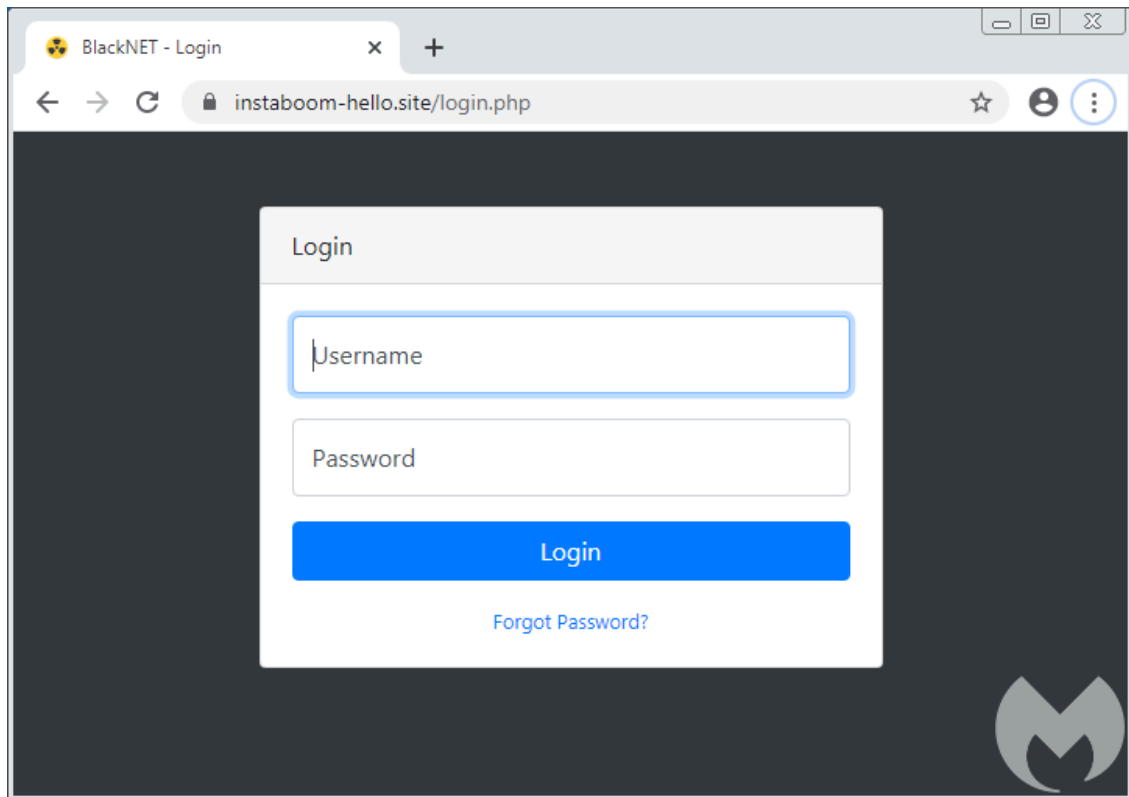


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

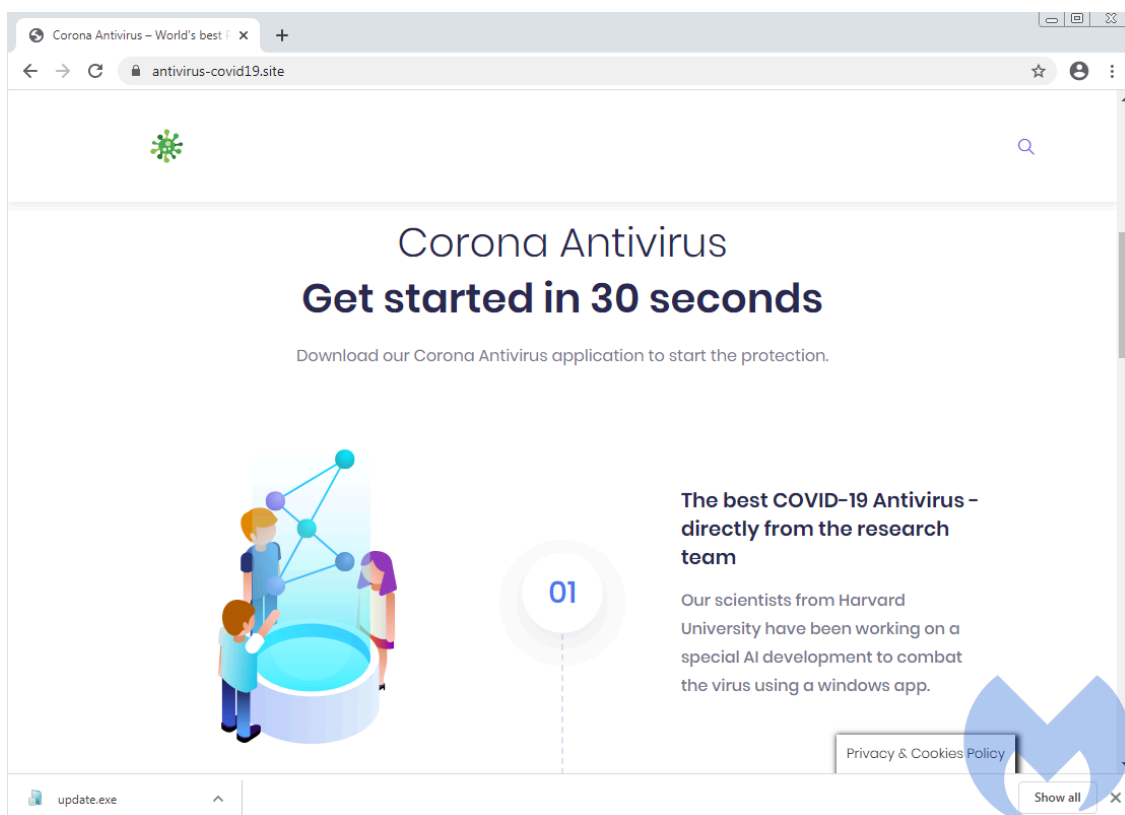
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

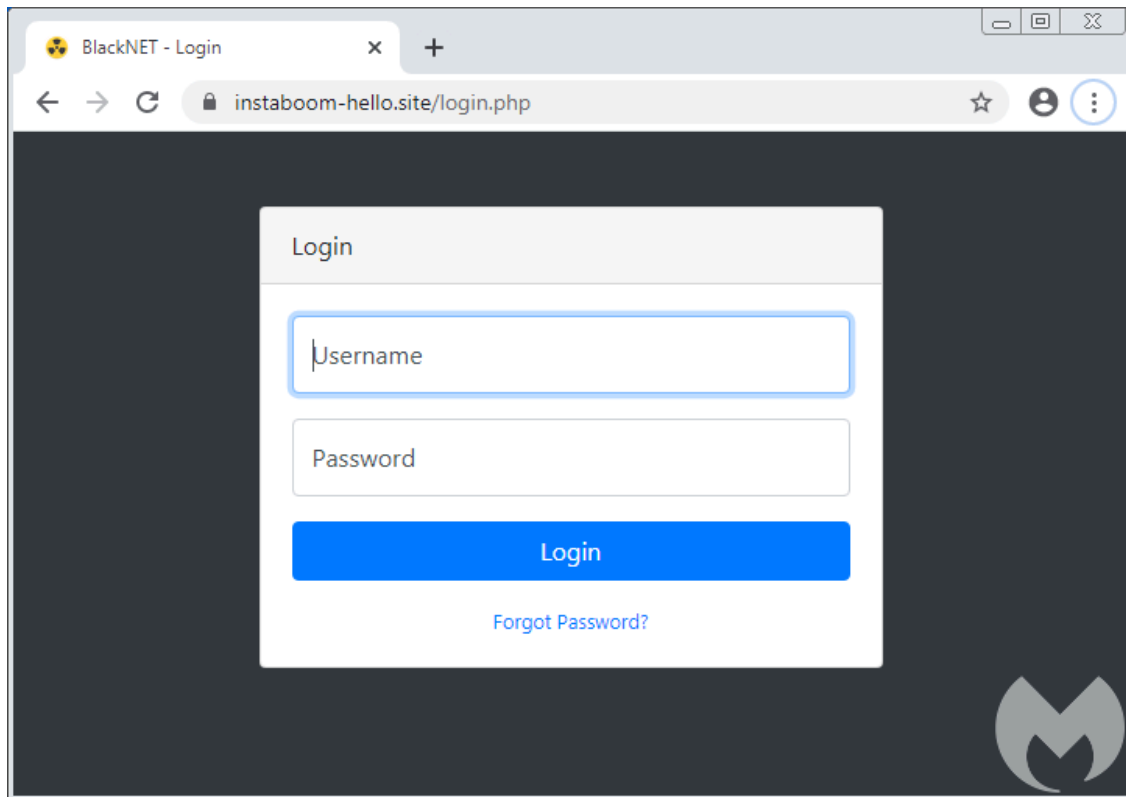


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a table header including Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. Further right is a 'Map Visualization' section showing a world map with a few blue dots indicating client locations. At the bottom, a copyright notice reads 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

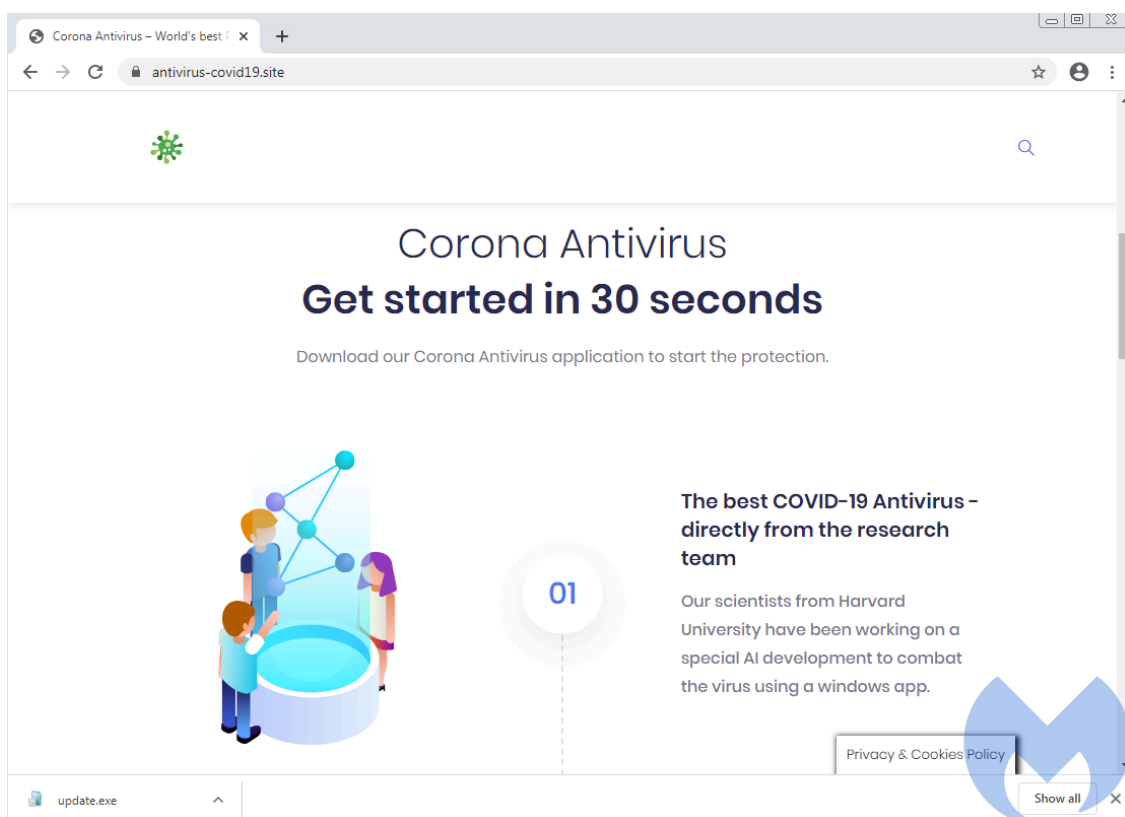
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

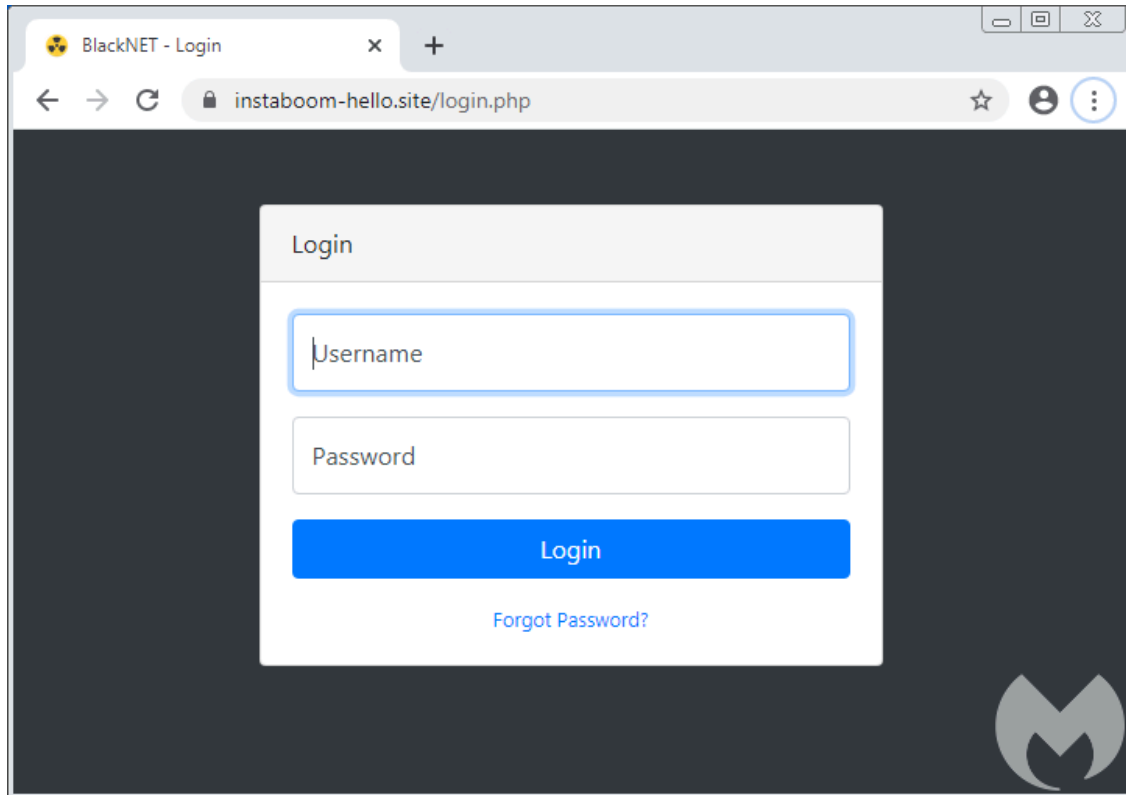


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

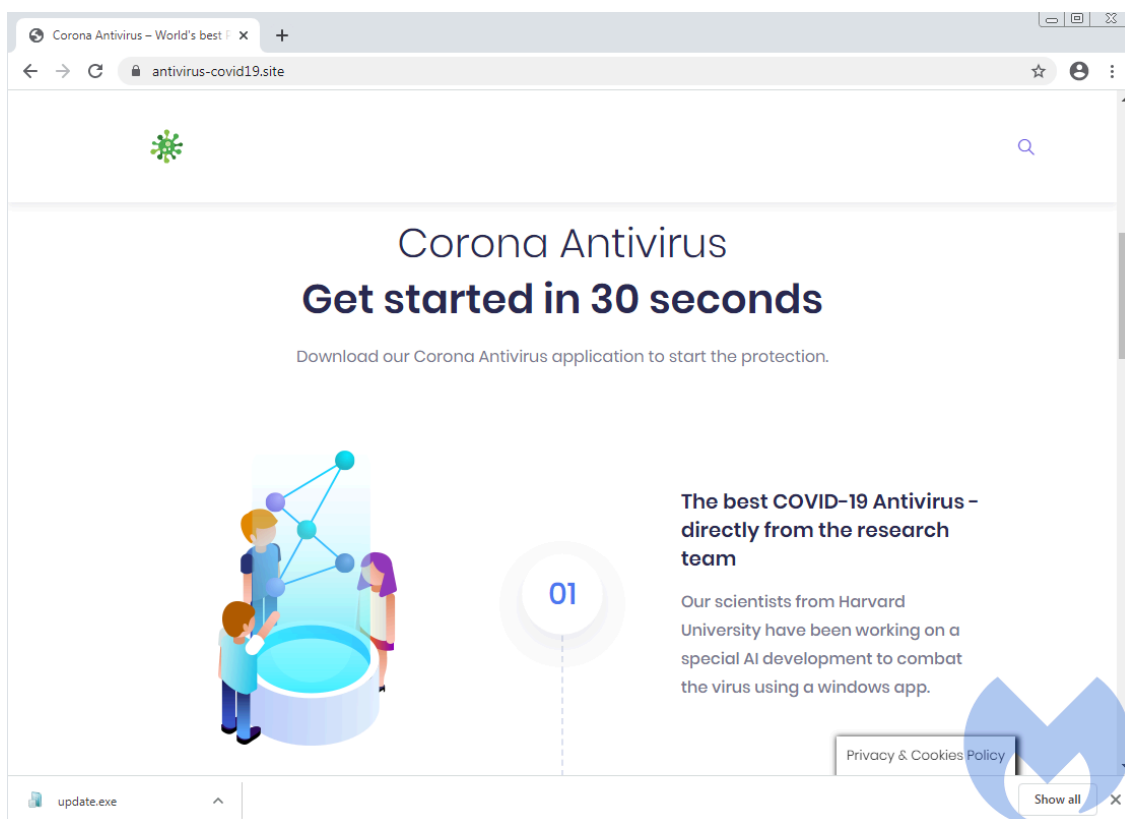
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

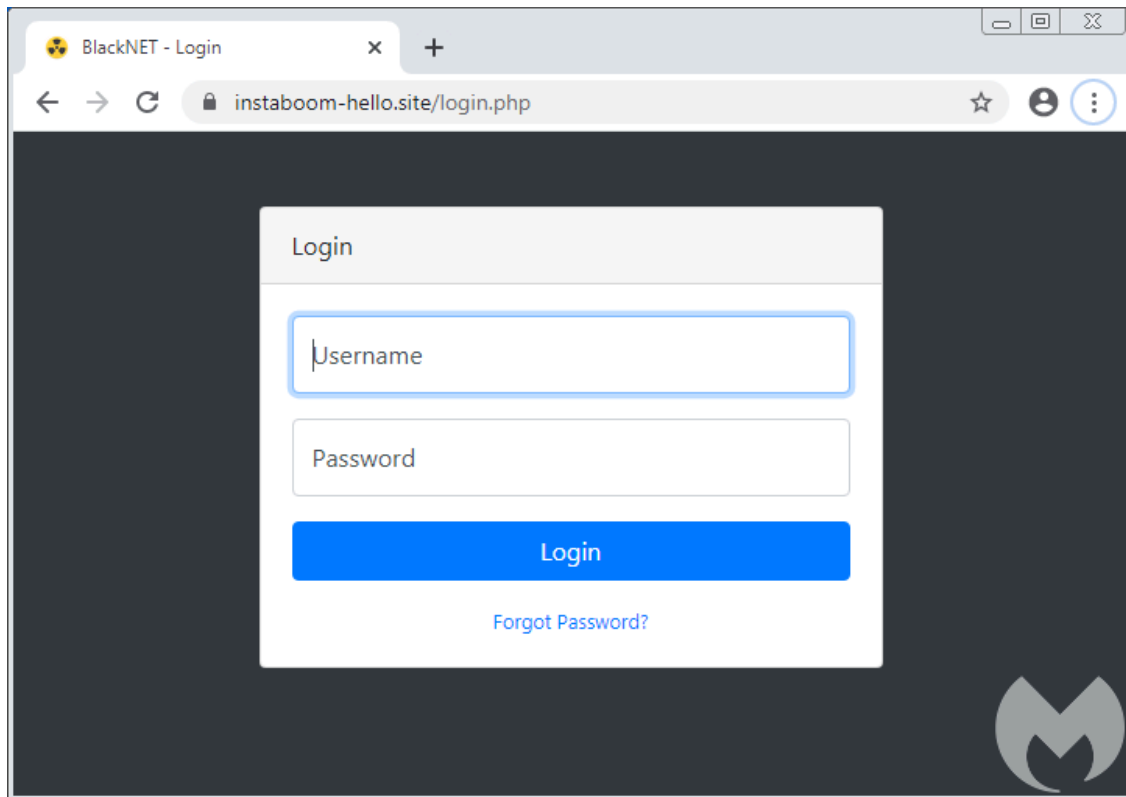


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

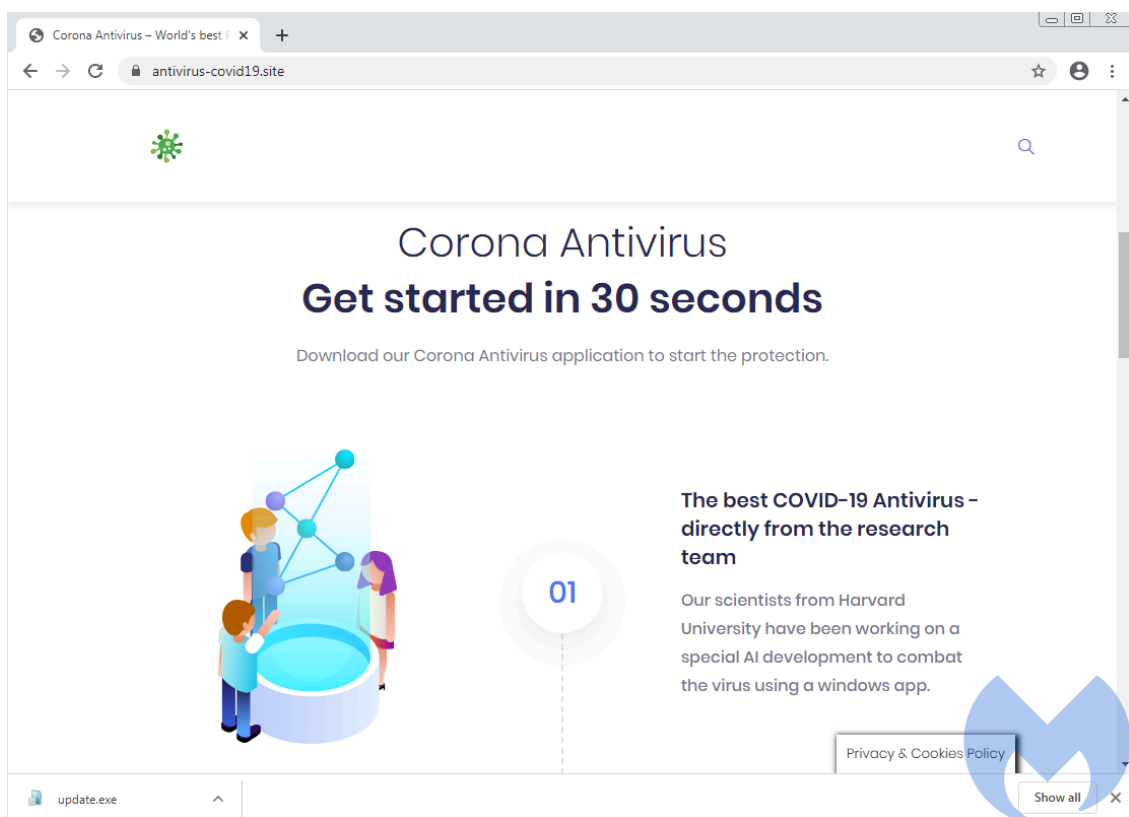
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

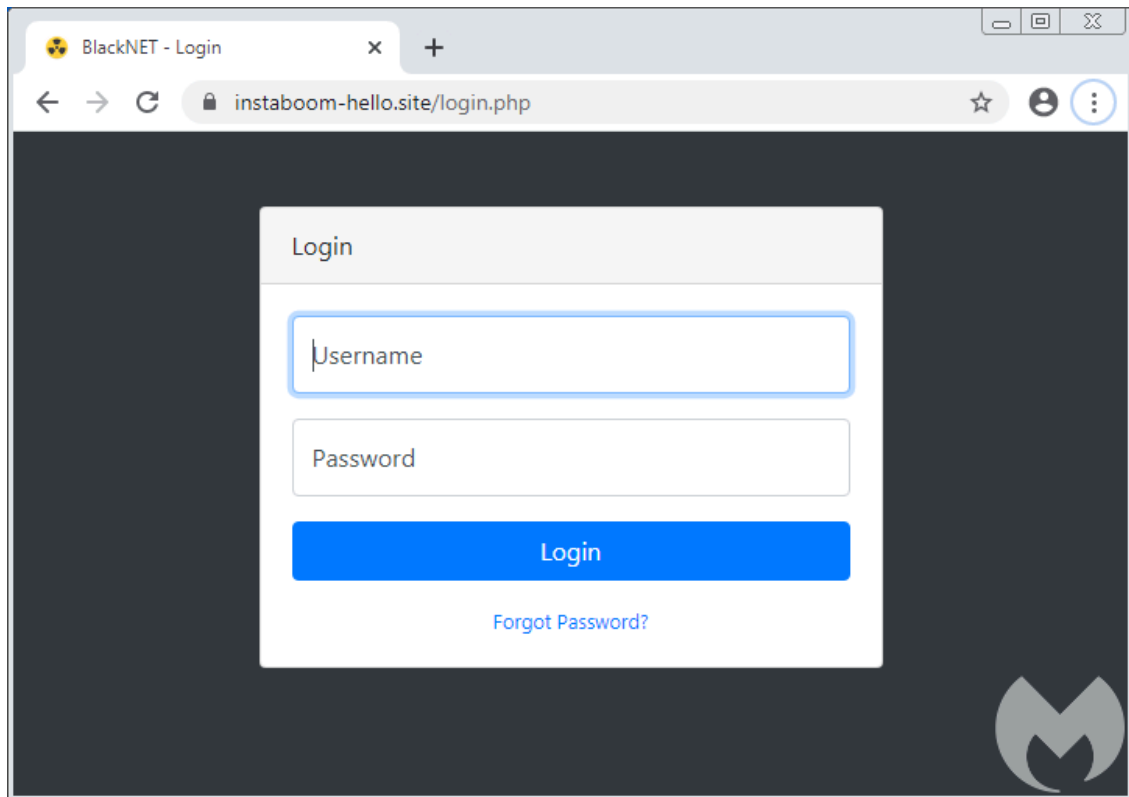


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

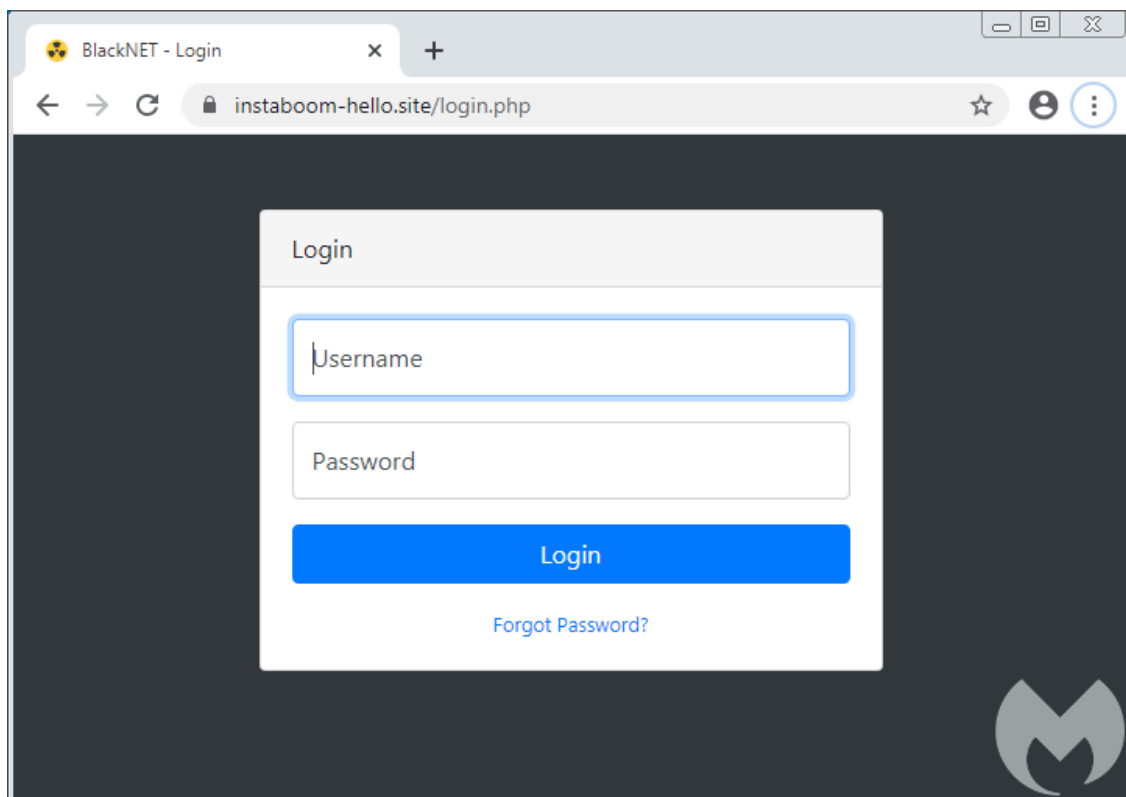
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

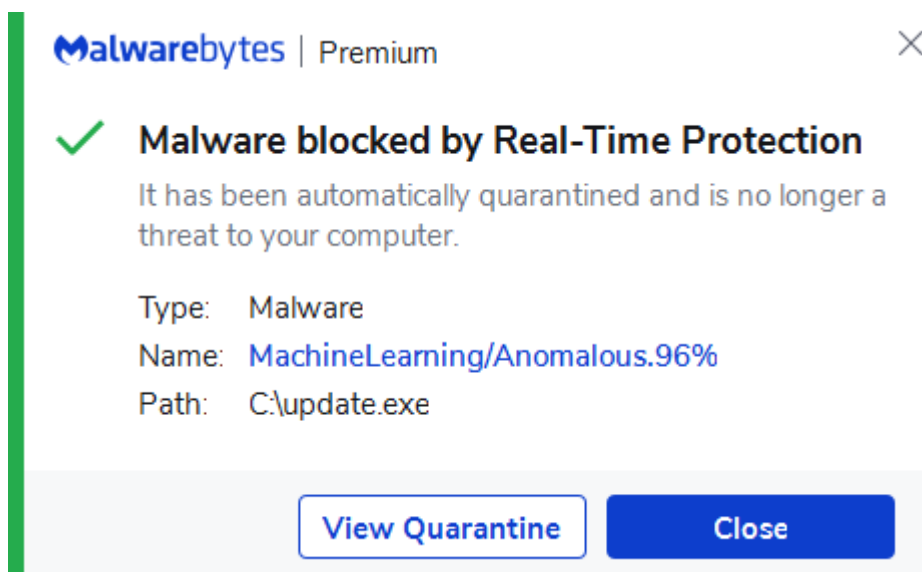
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

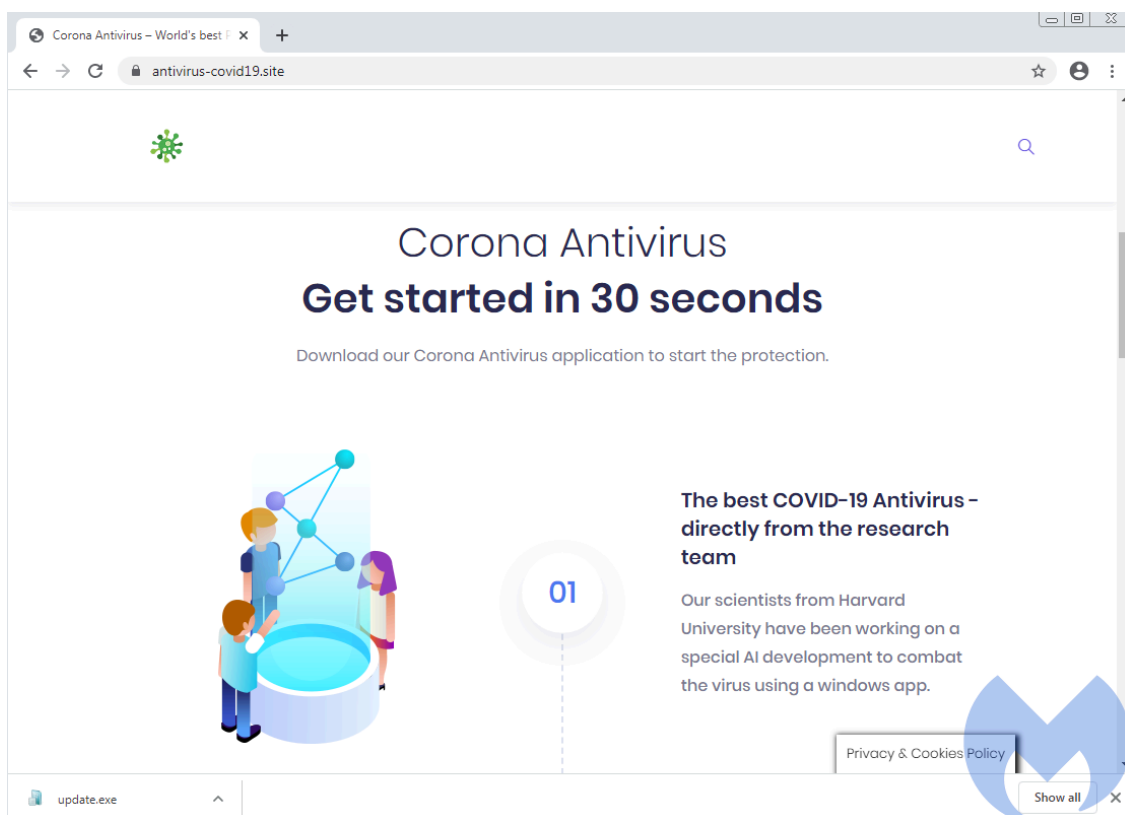
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

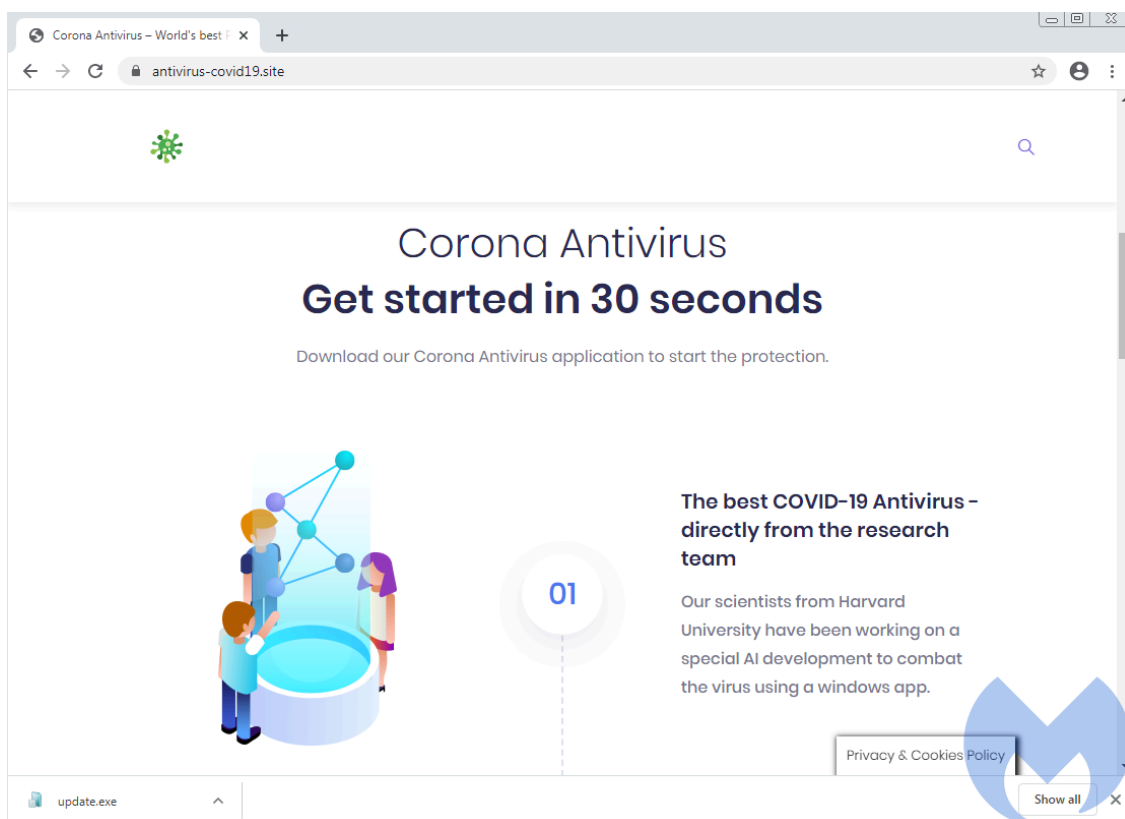
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

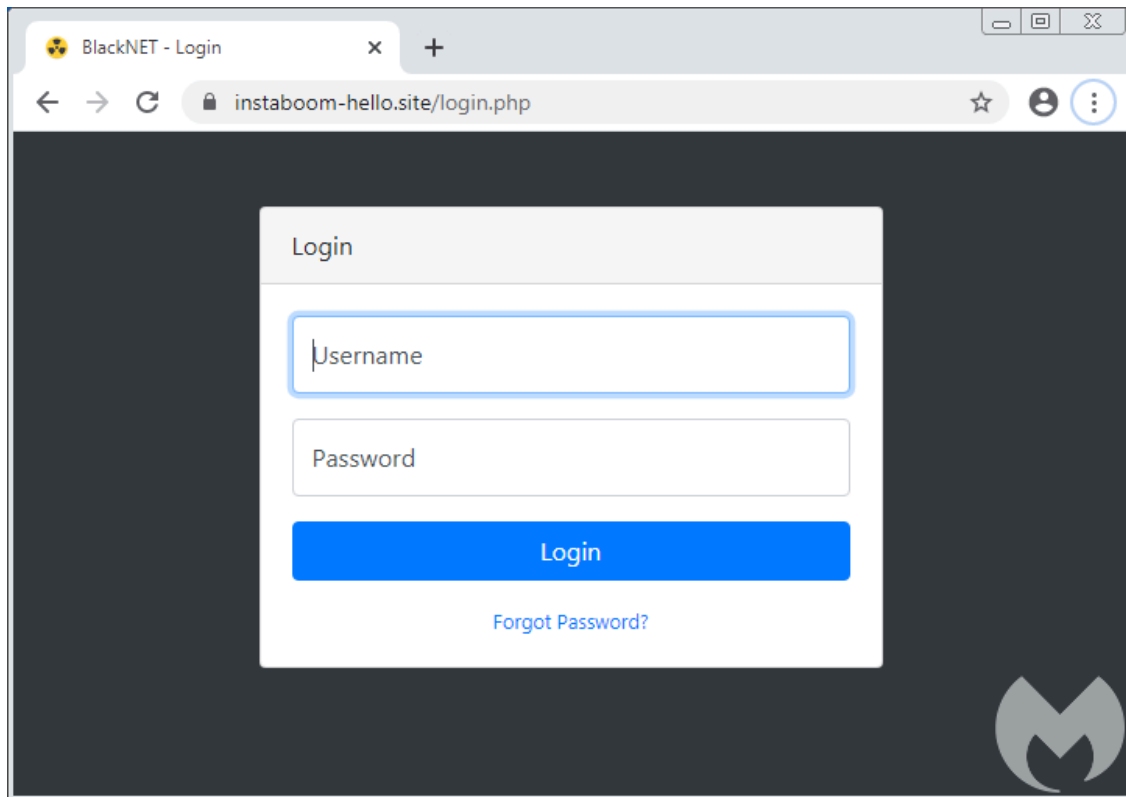


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue dot indicating a client location. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. The window has a green vertical bar on the left and a close button (X) in the top right corner. The main content area features a green checkmark icon and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

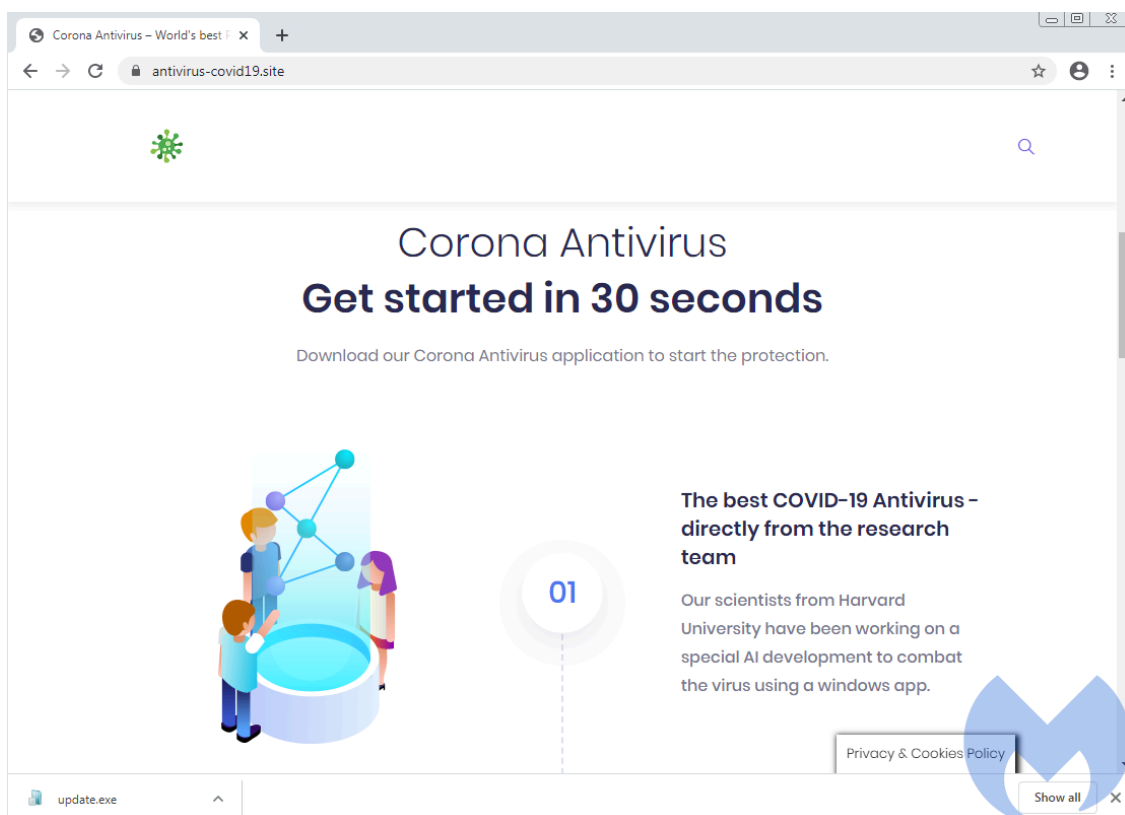
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

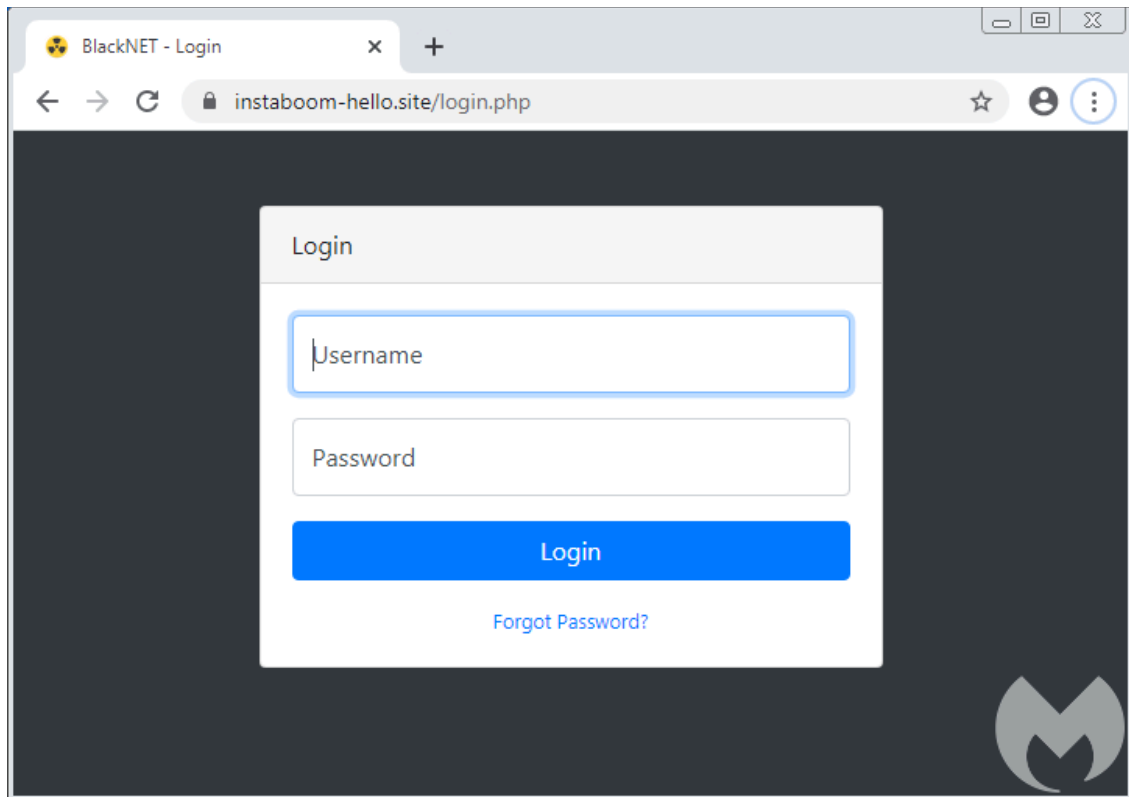


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

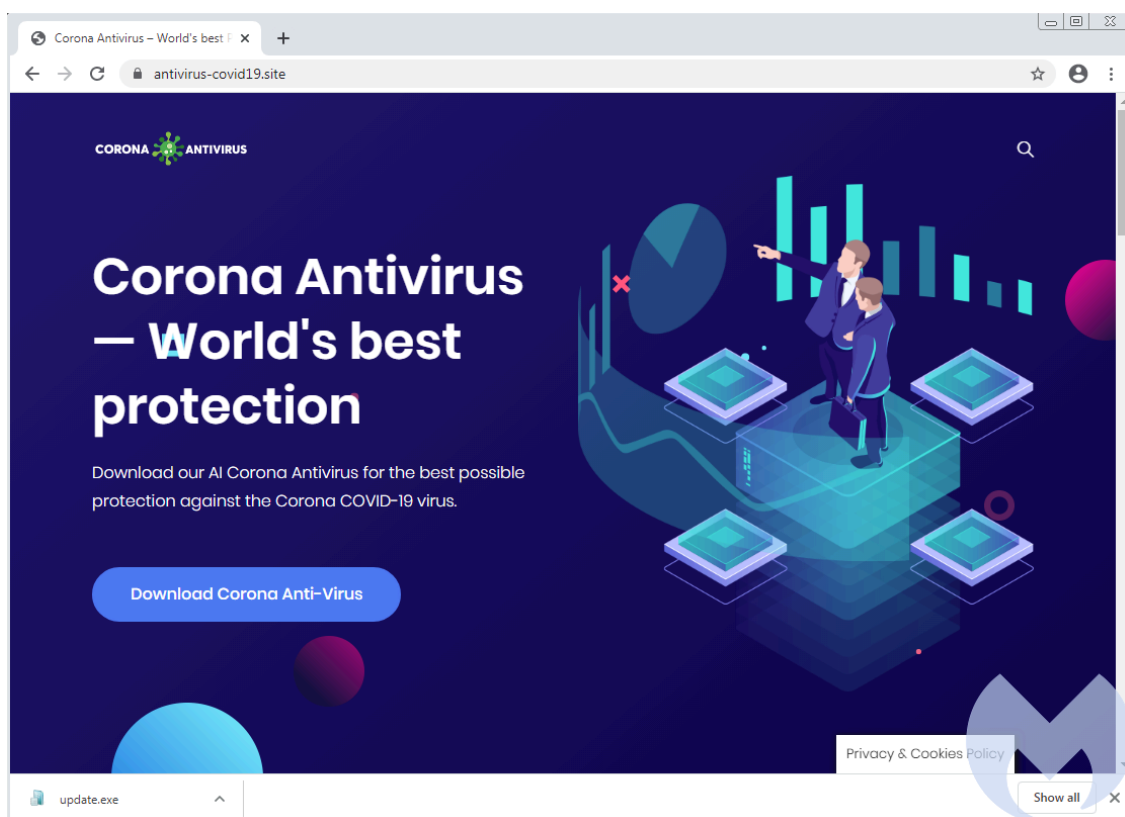
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

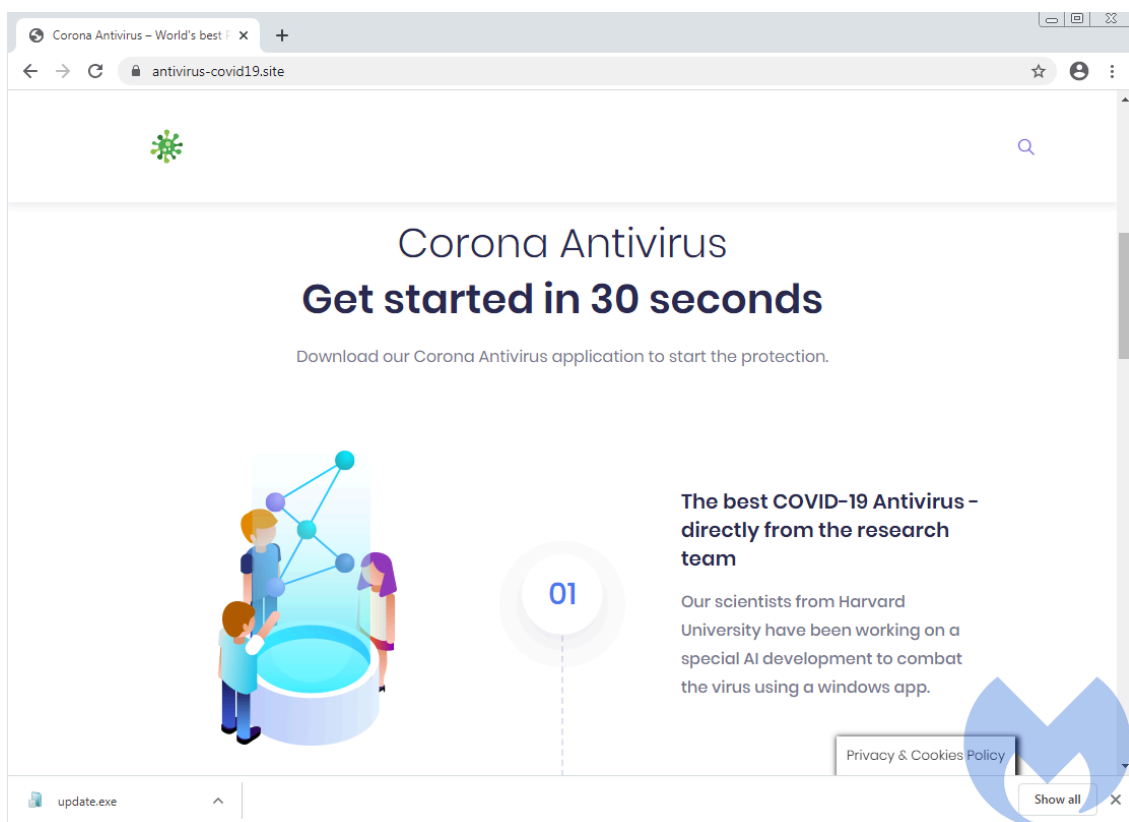
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

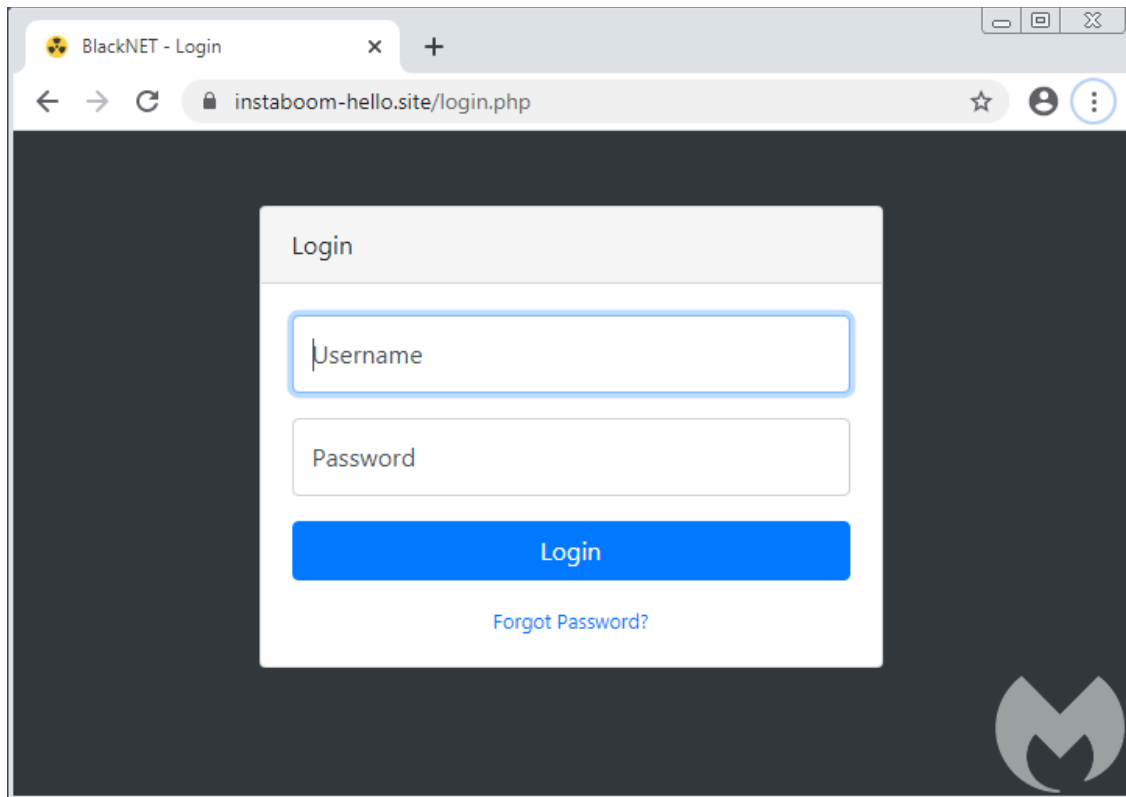


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

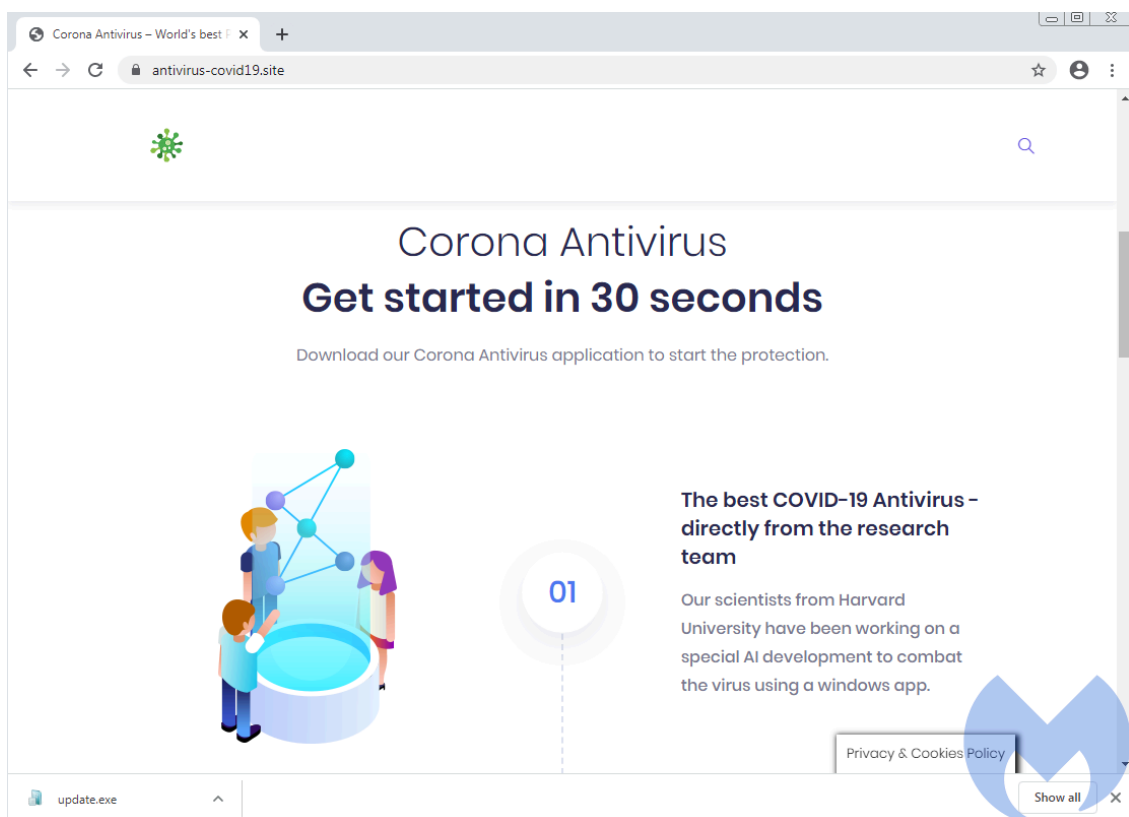
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

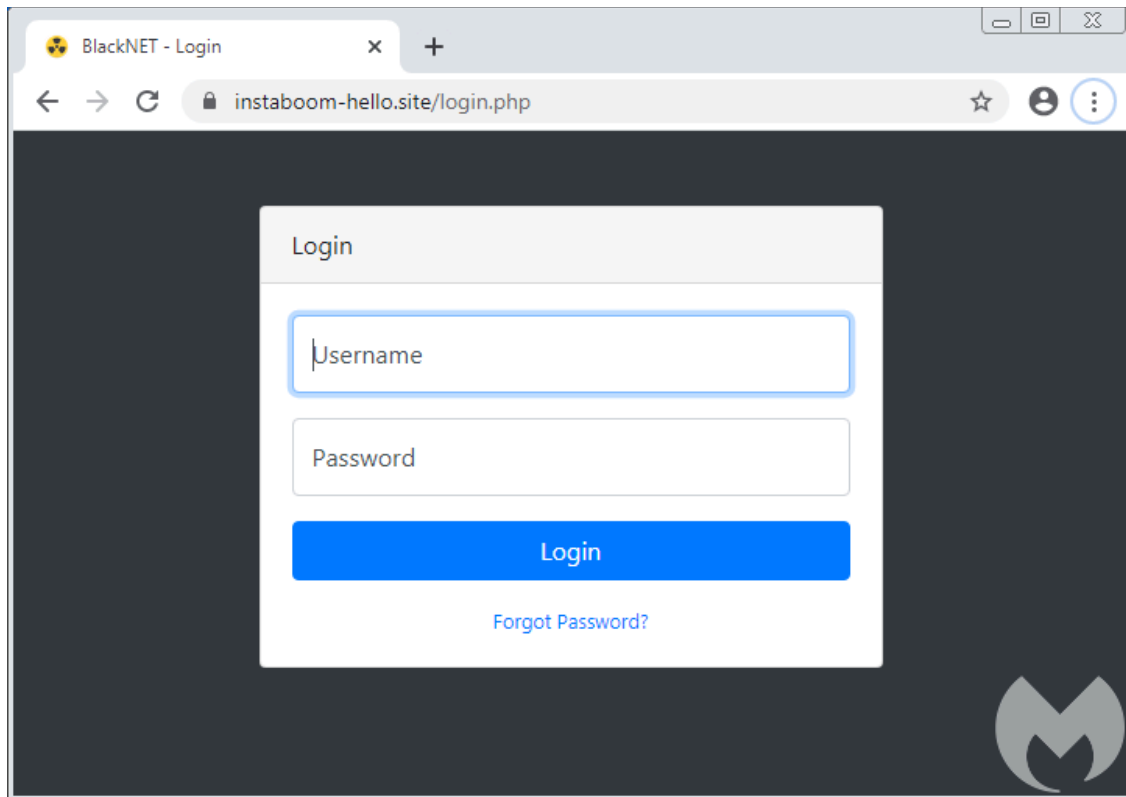


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, a copyright notice reads 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

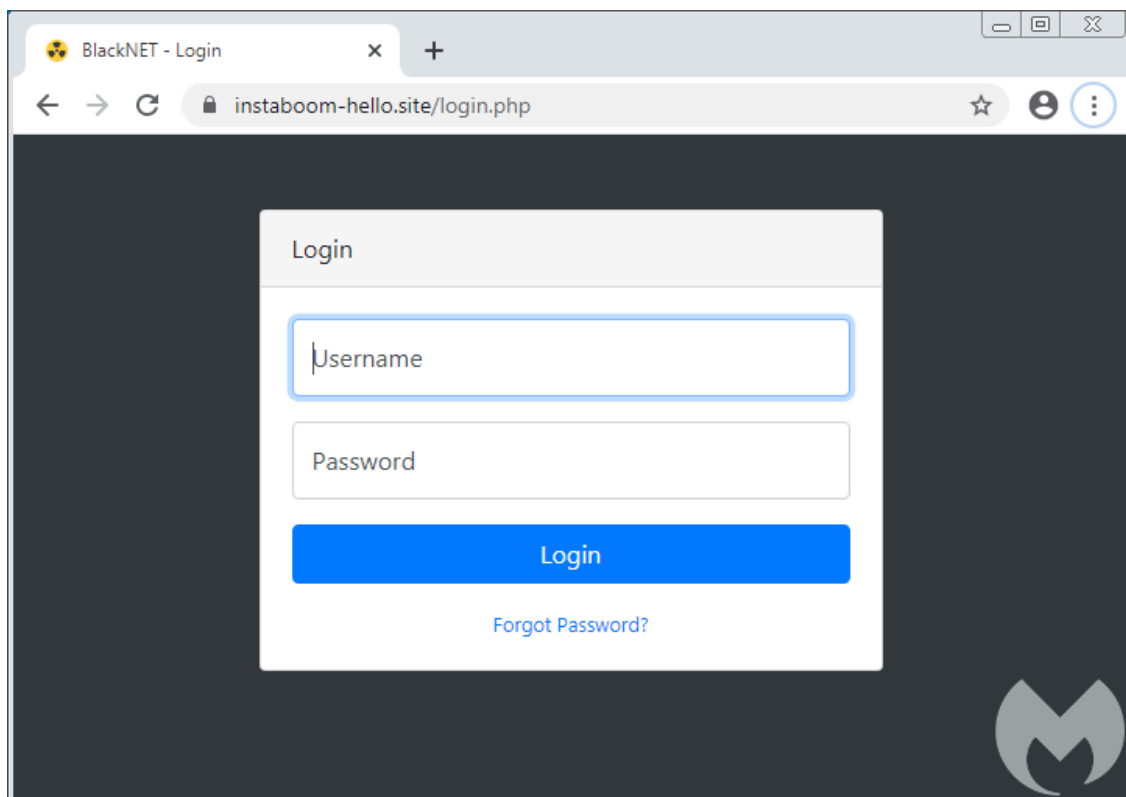
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

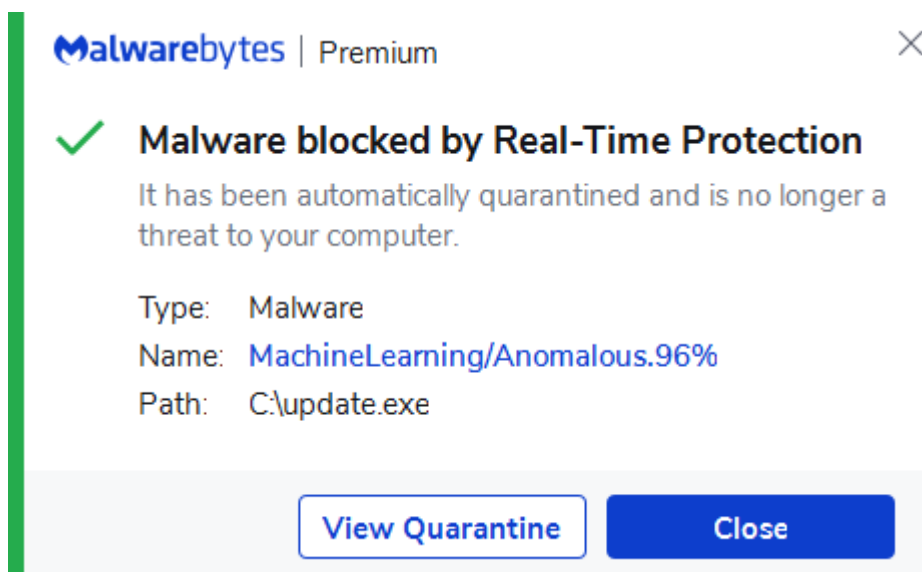
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a 'Select Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

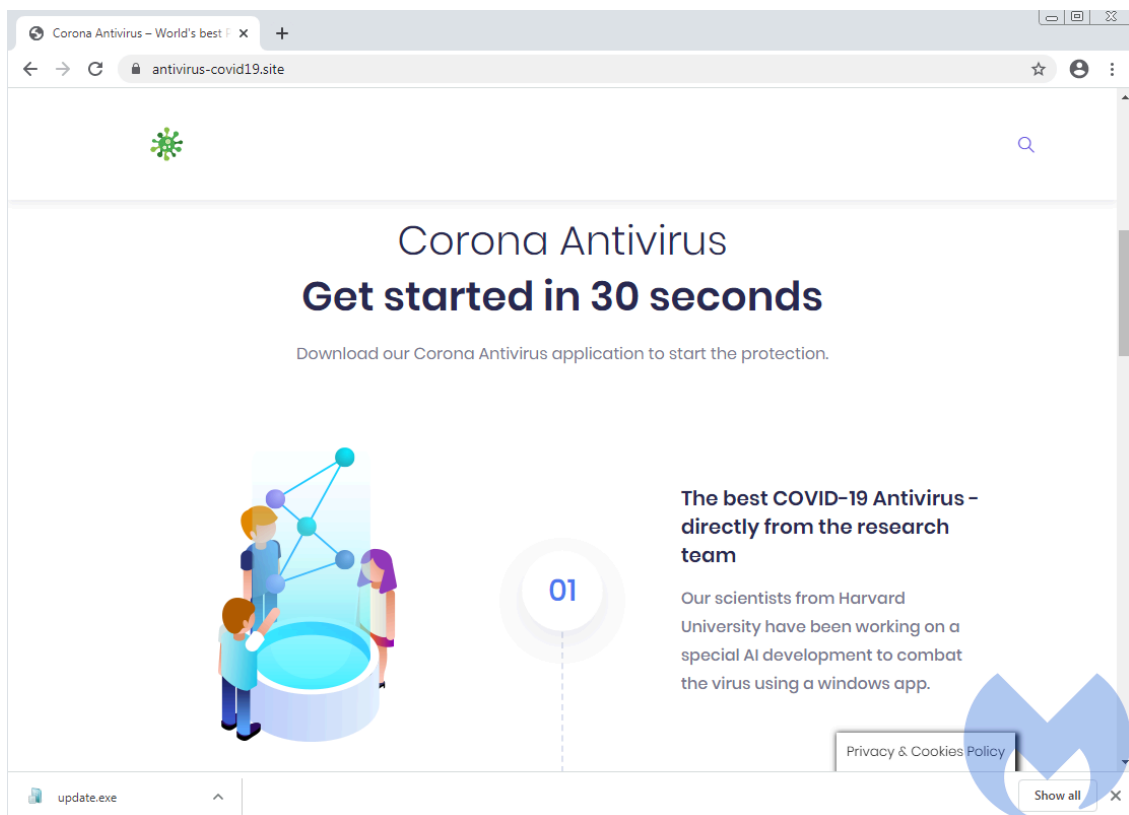
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

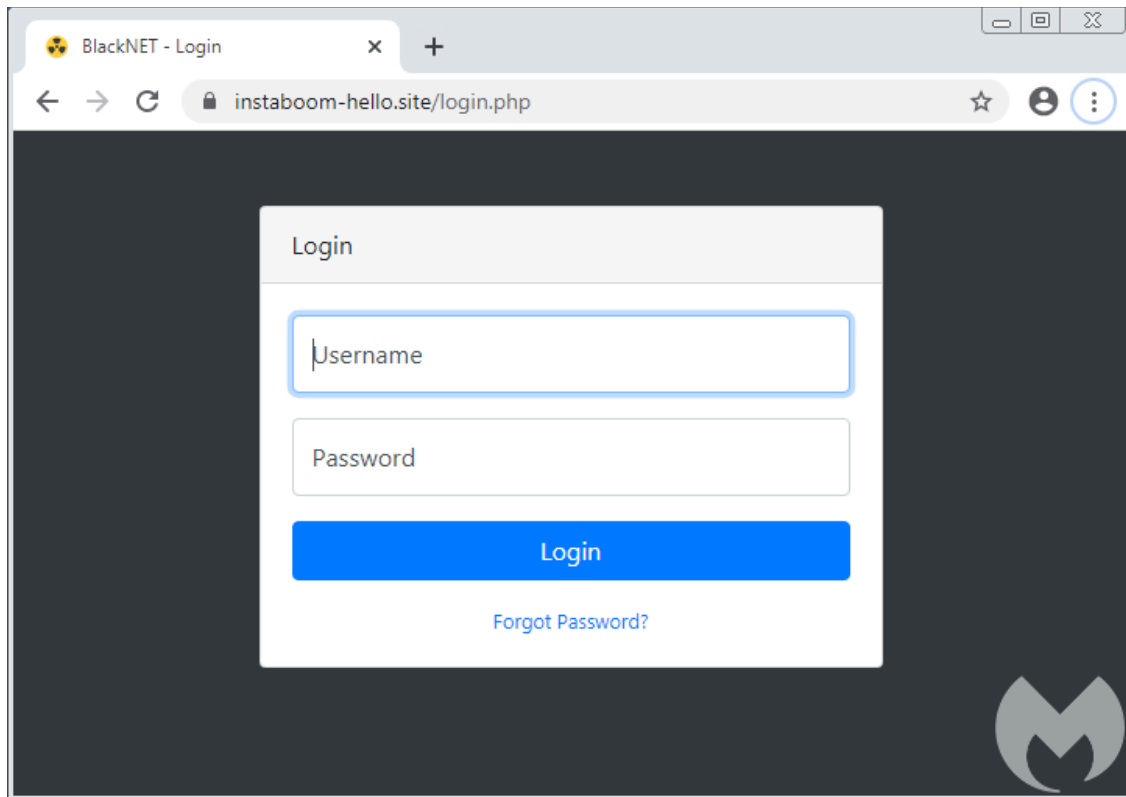


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes representing client statistics: 0 Total Clients (blue), 0 USB Clients (yellow), 0 Online Clients (green), and 0 Offline Clients (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots indicating client locations. The footer contains the copyright notice: Copyright © BLACKNET by Black.Hacker - 2020.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it provides details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

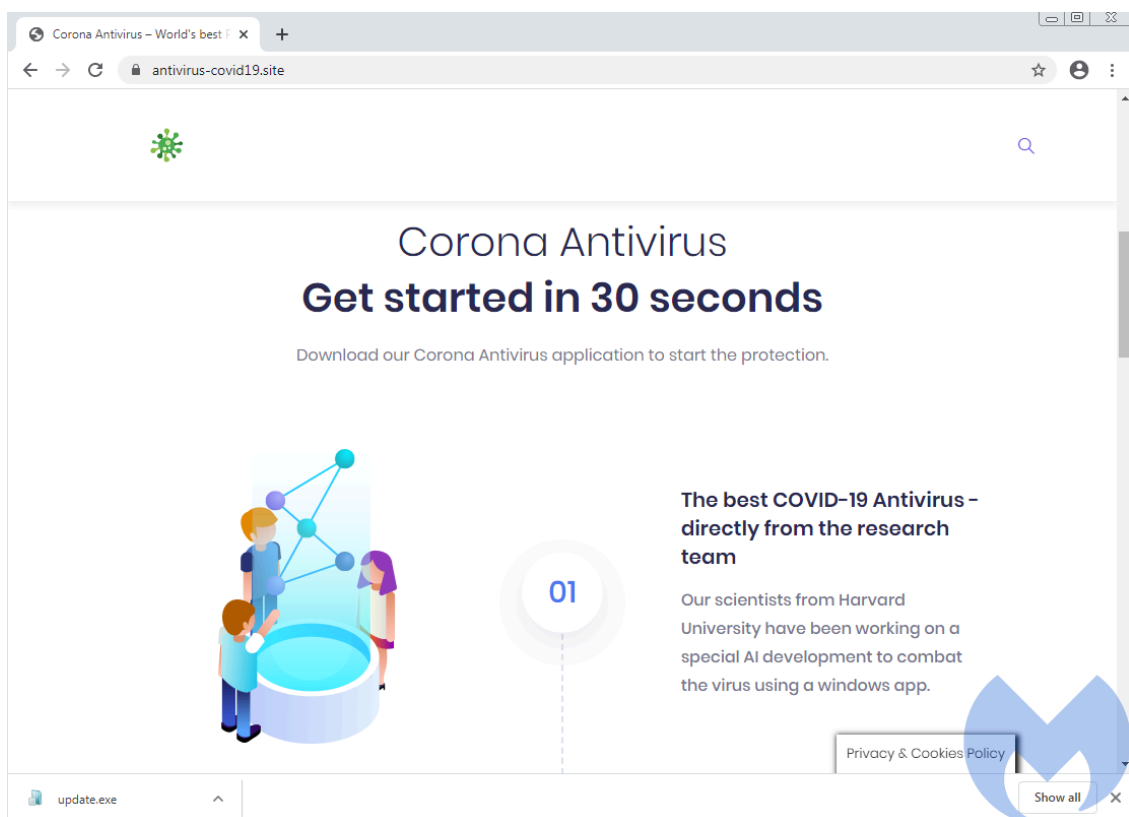
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

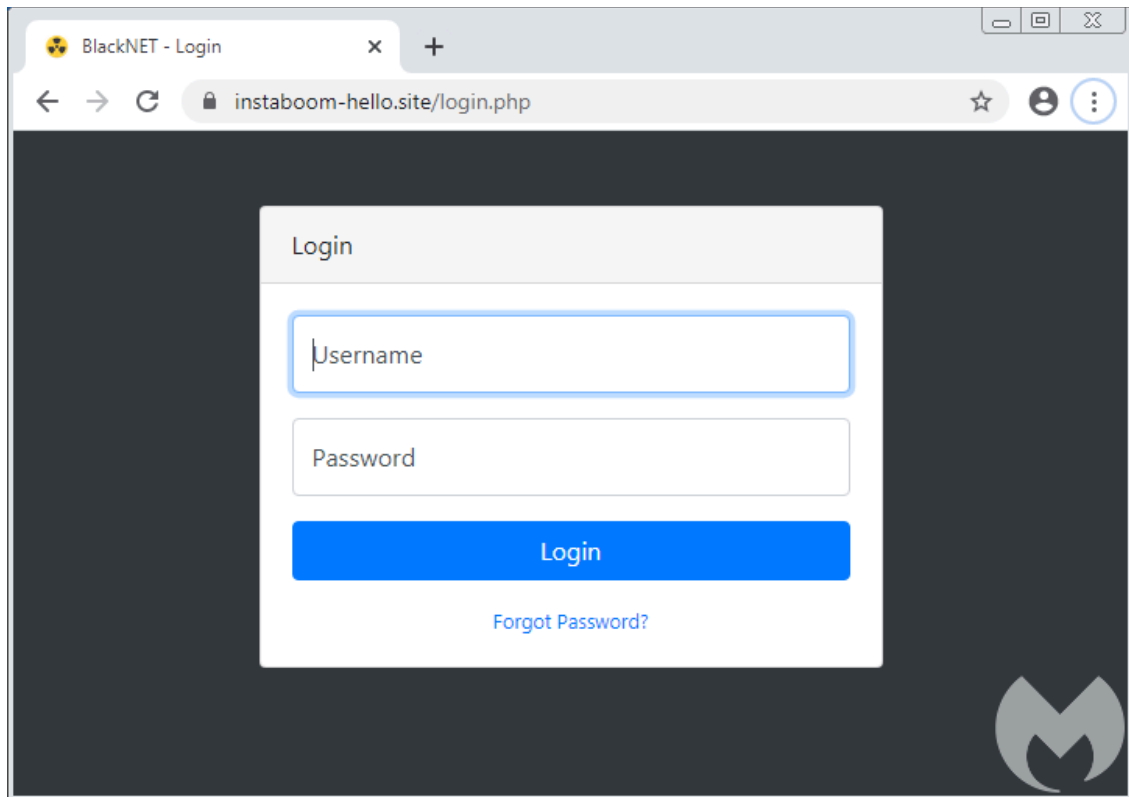


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

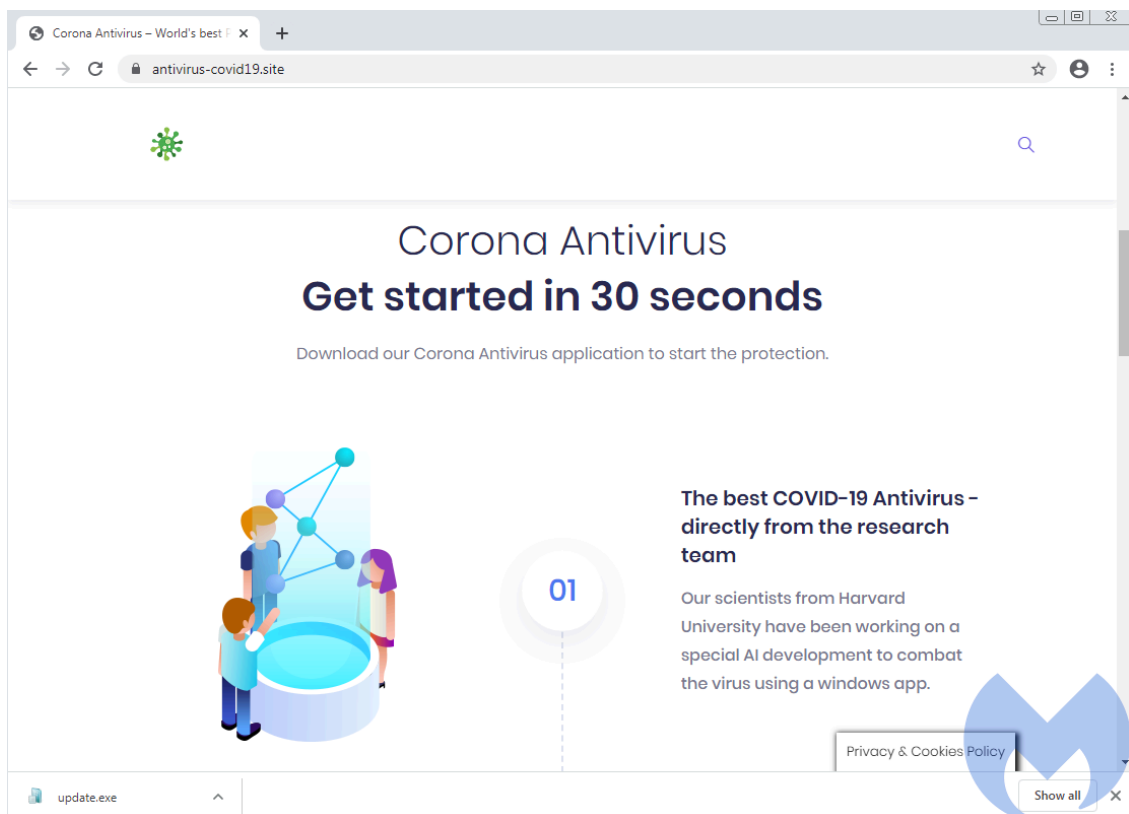
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

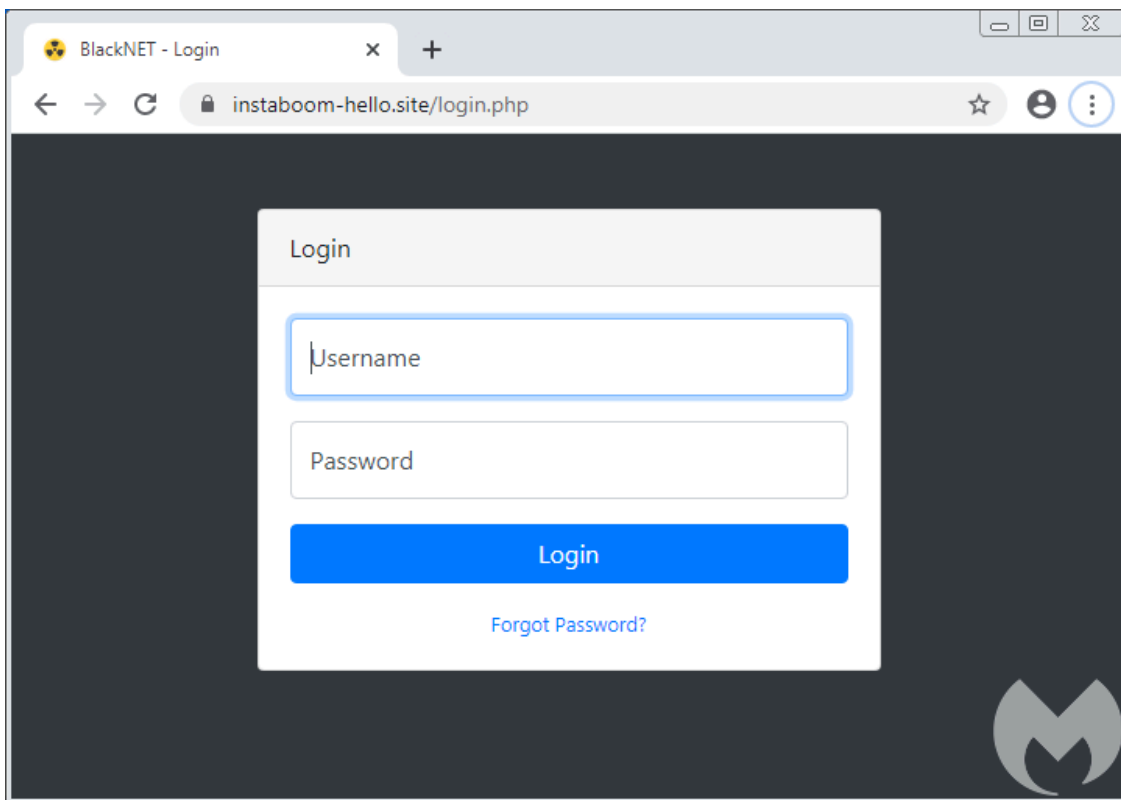


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

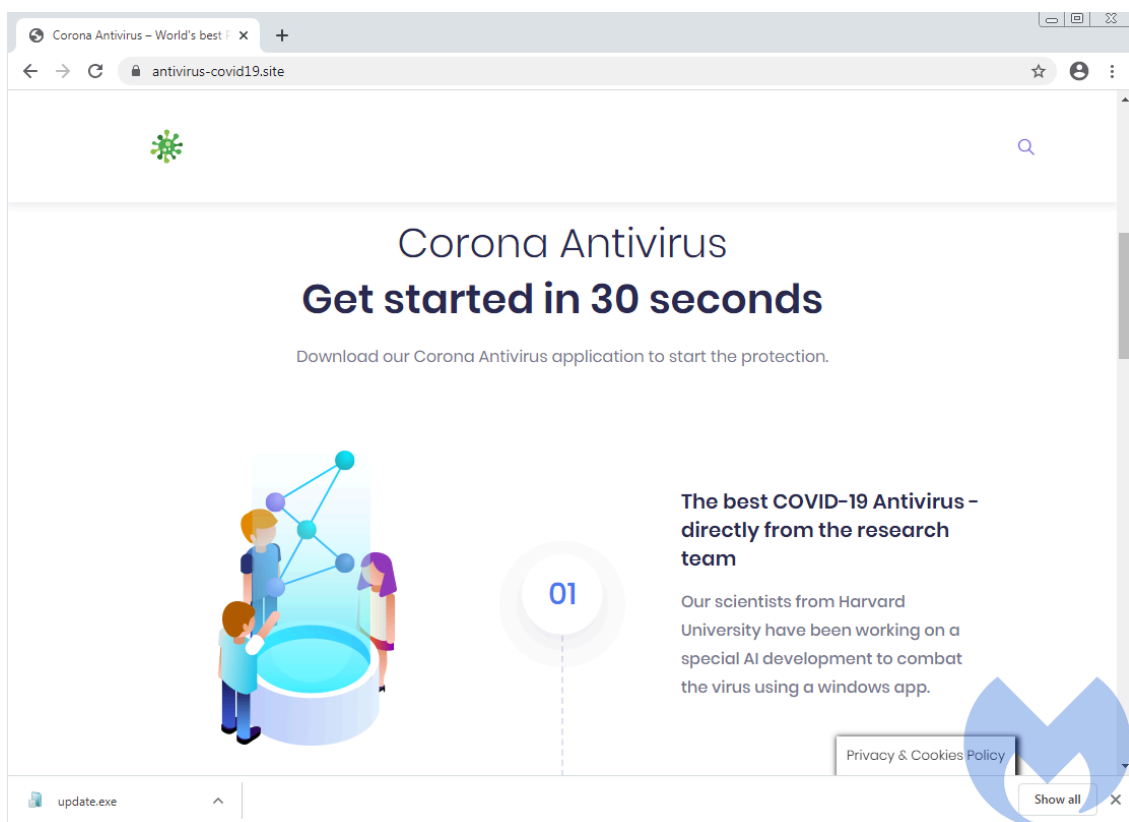
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

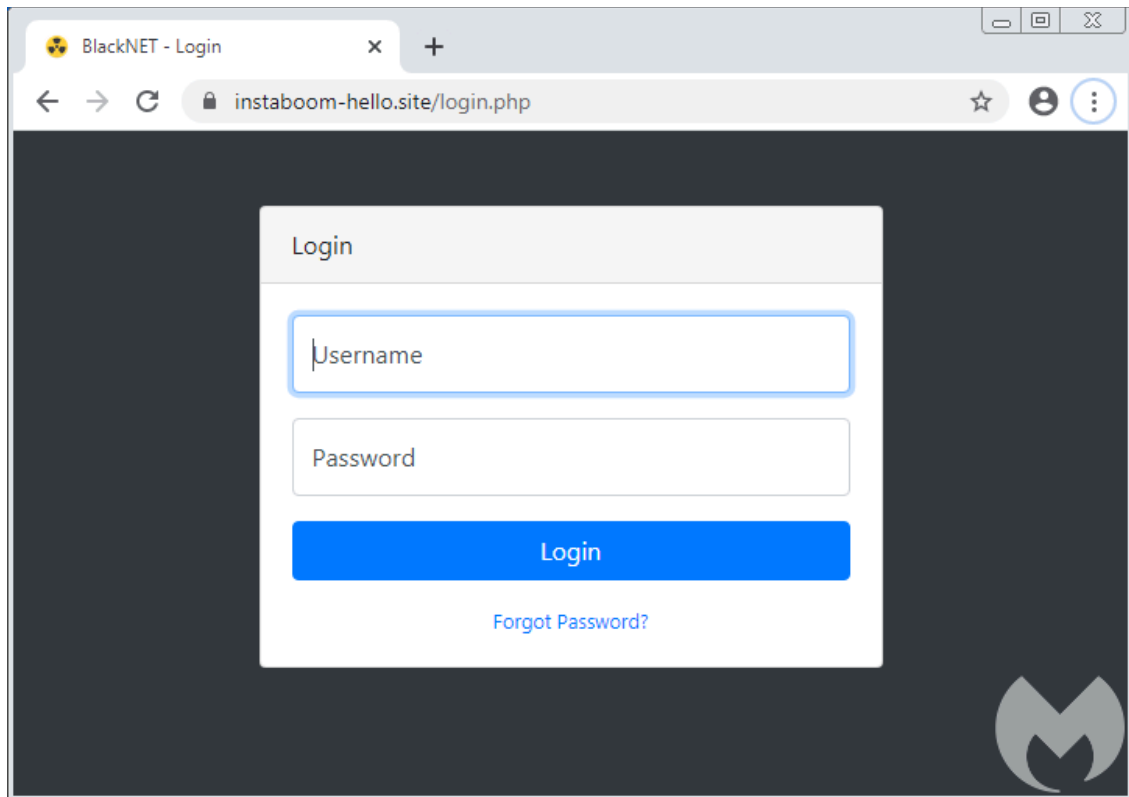


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

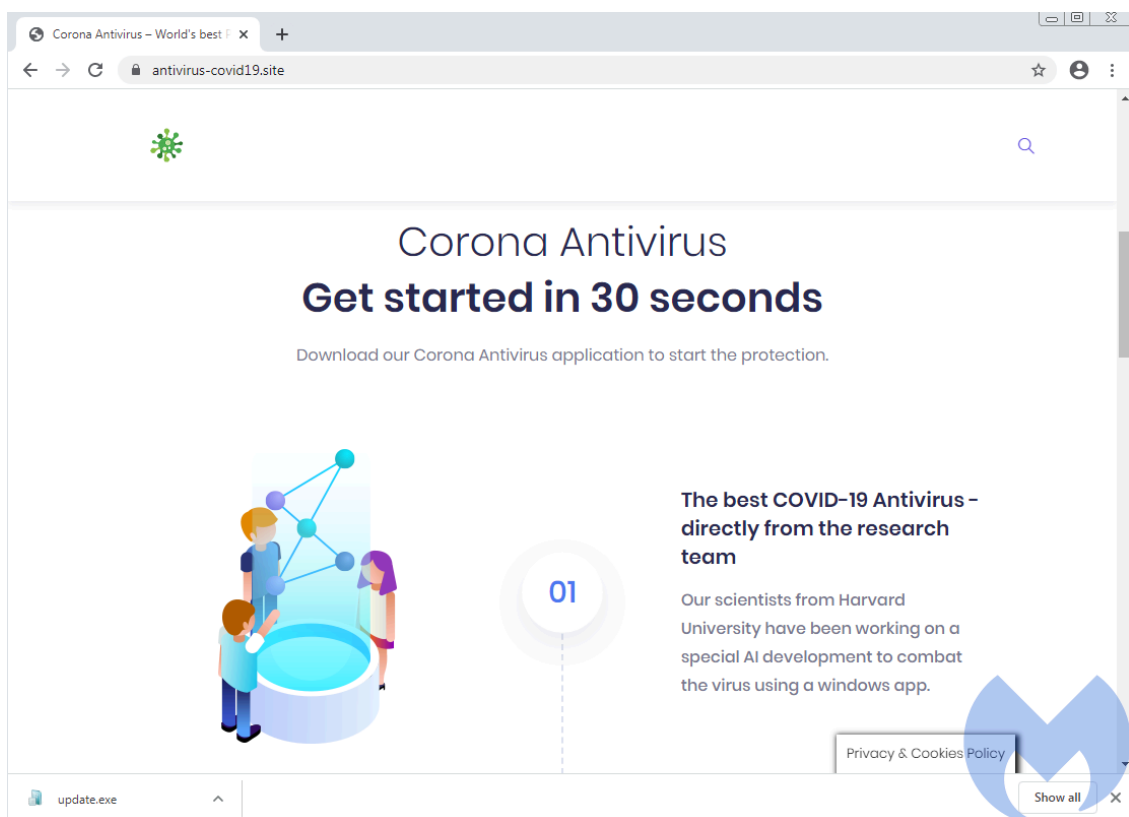
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

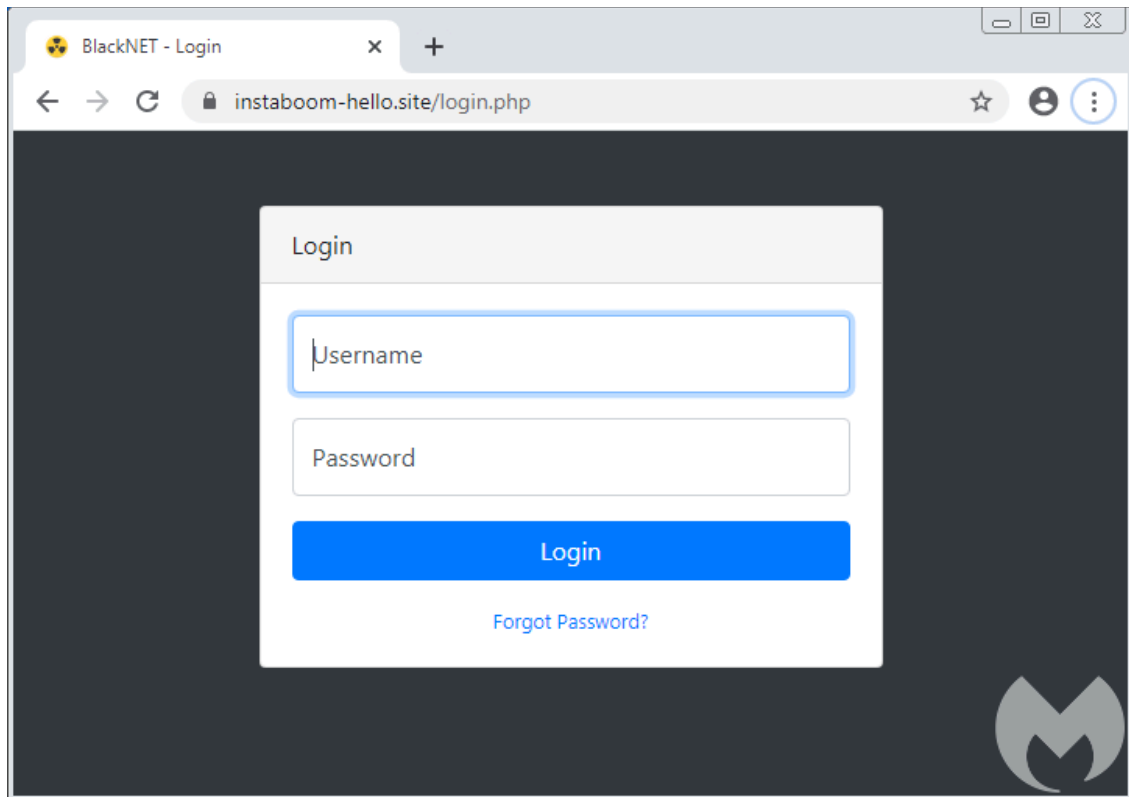


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

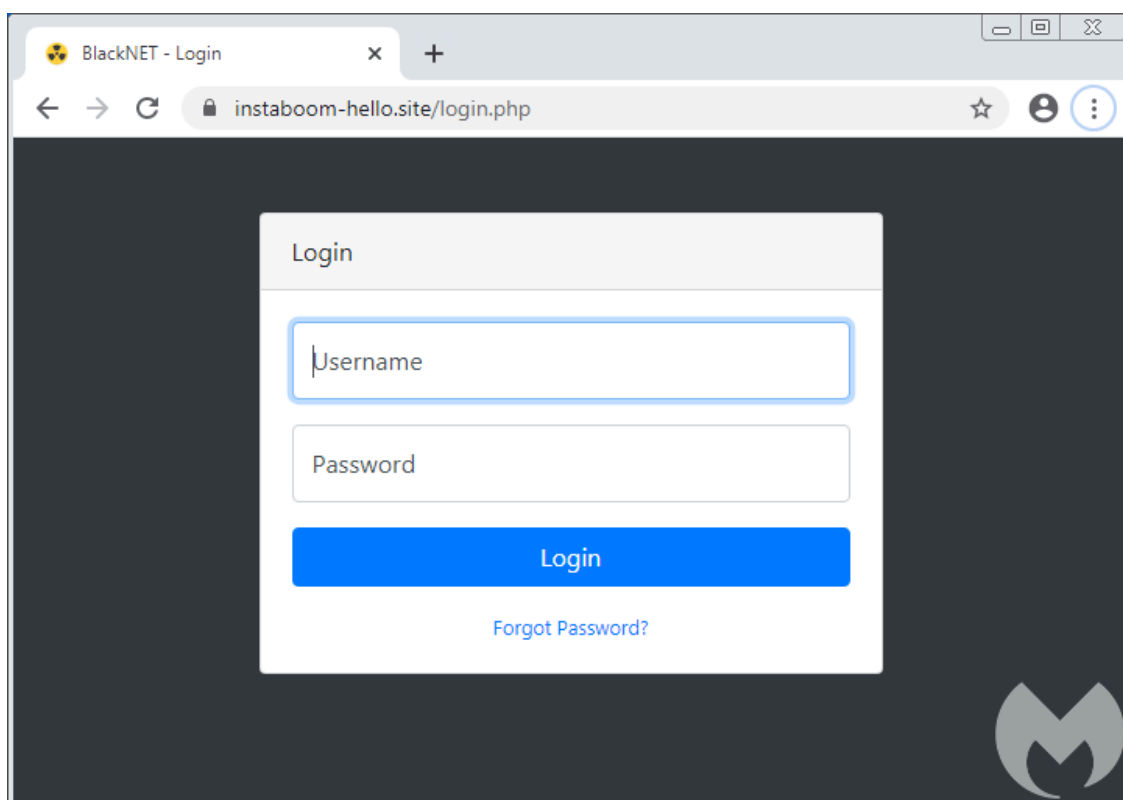
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

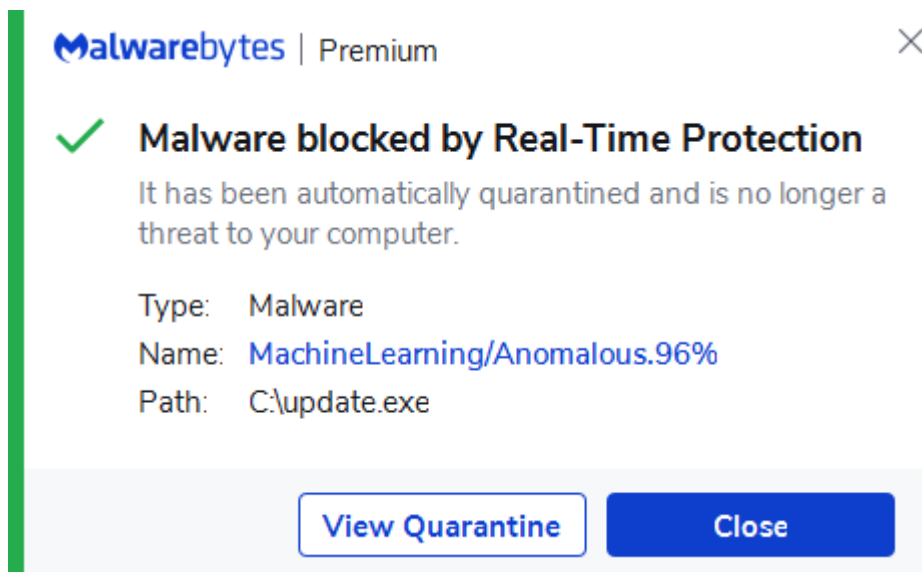
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

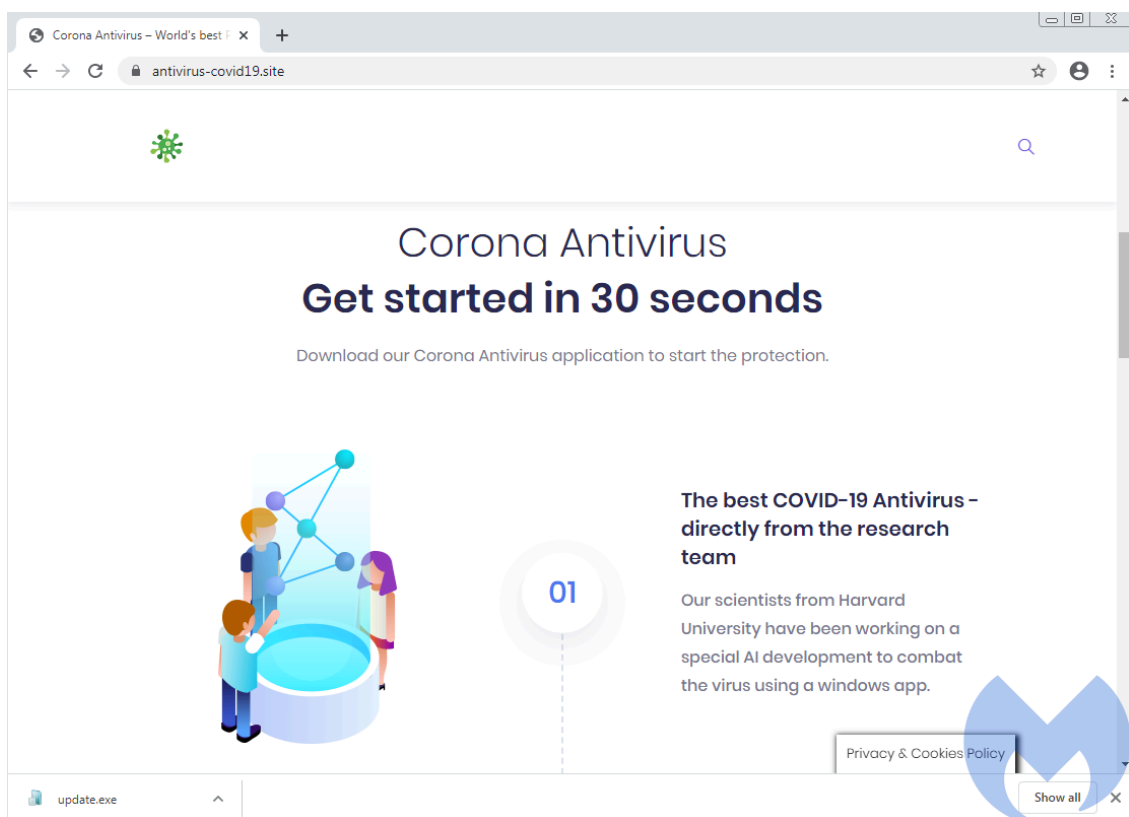
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored tiles: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

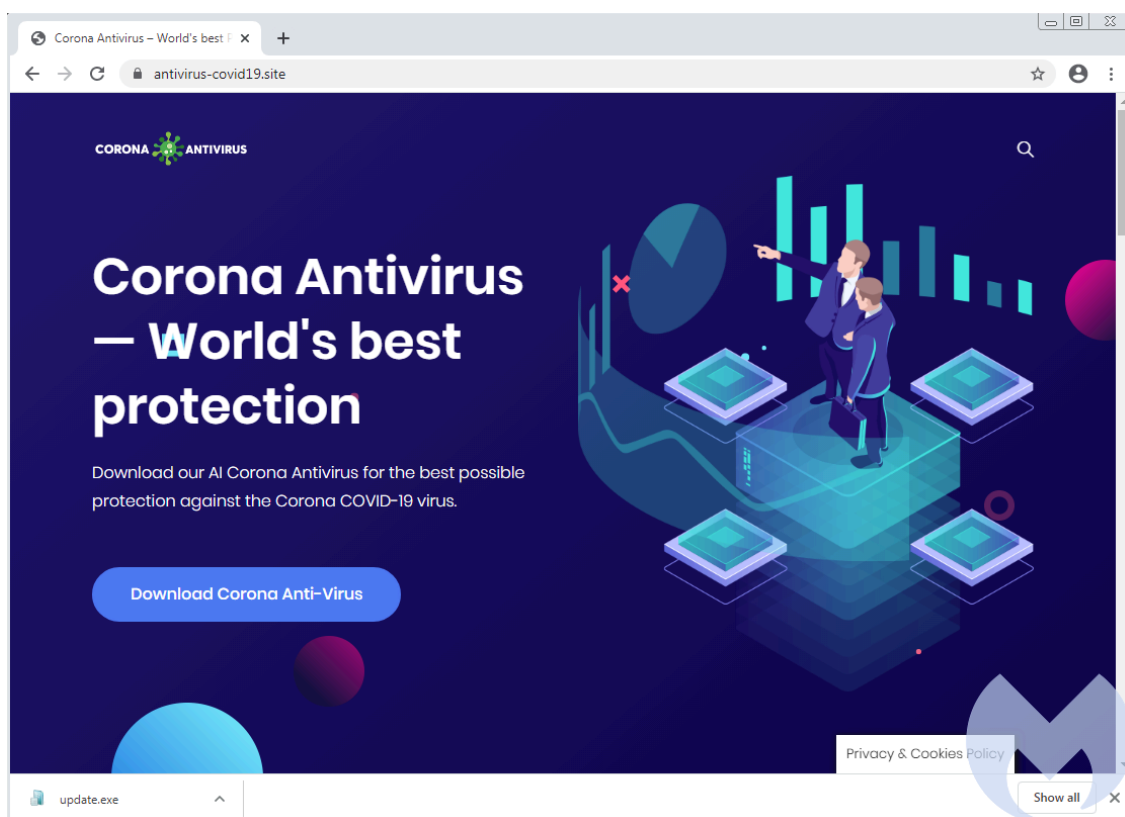
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

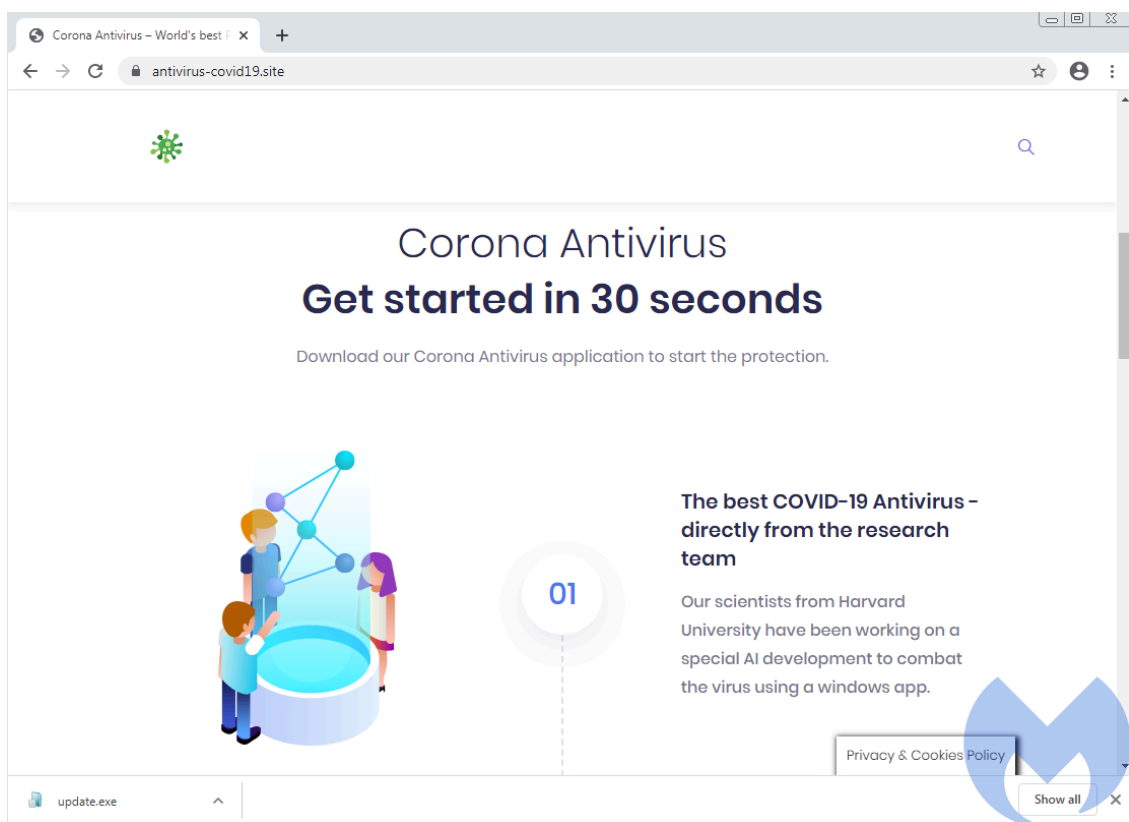
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

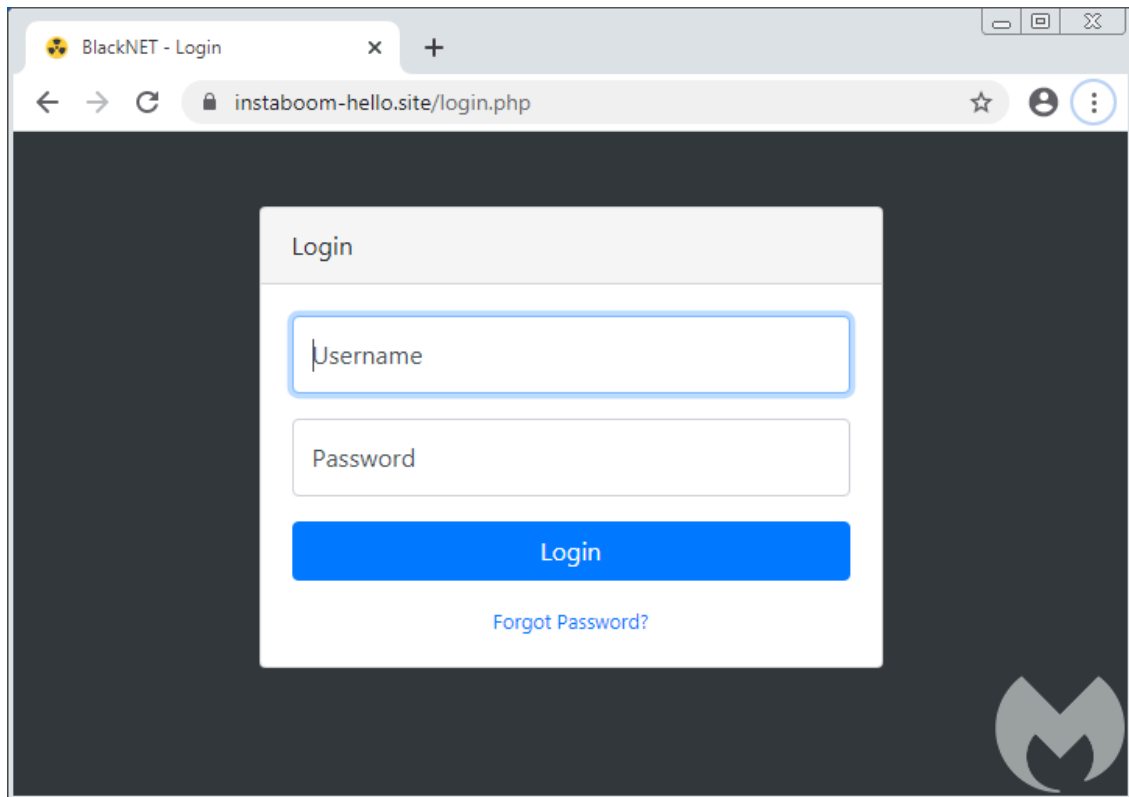


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots indicating client locations. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it provides details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

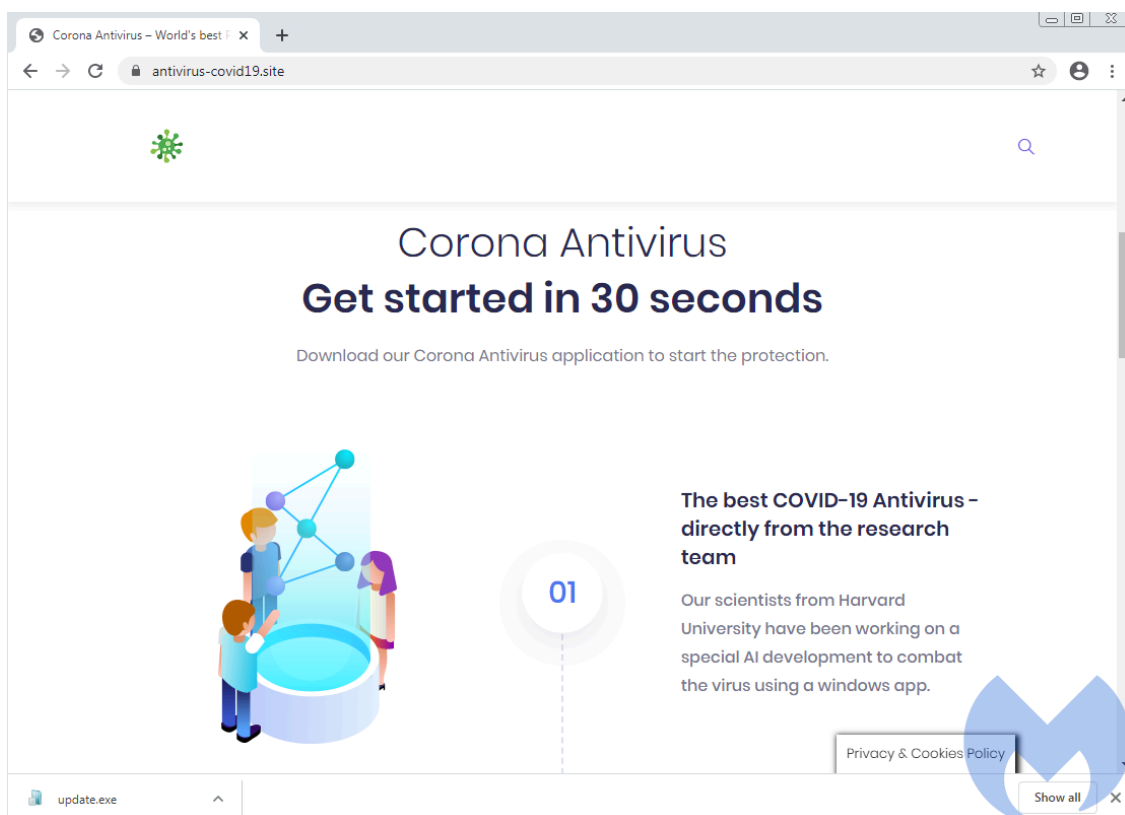
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

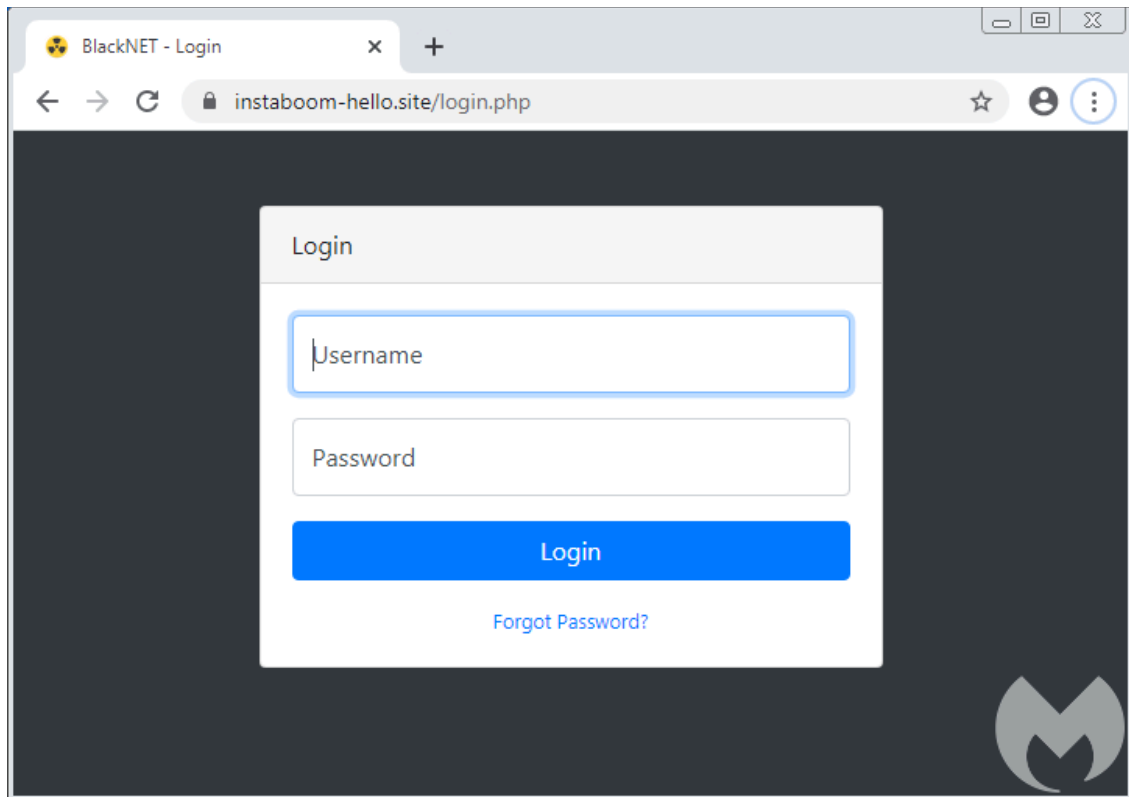


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

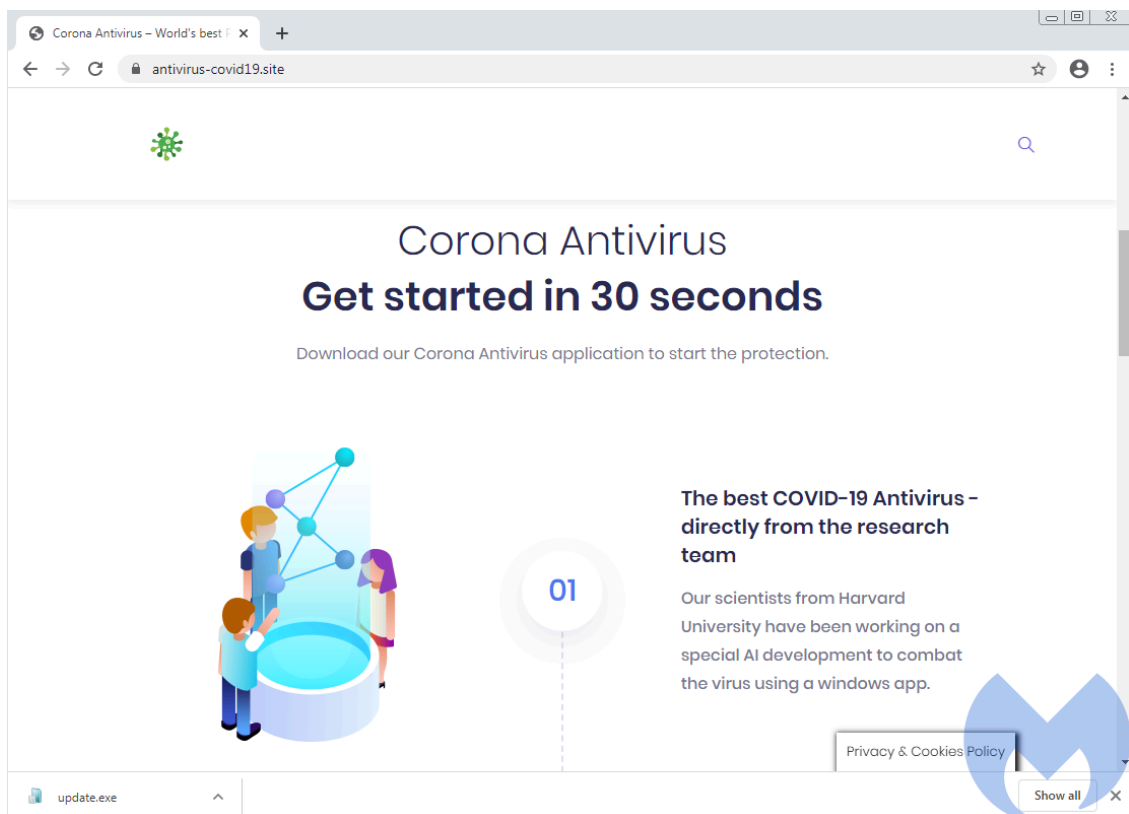
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

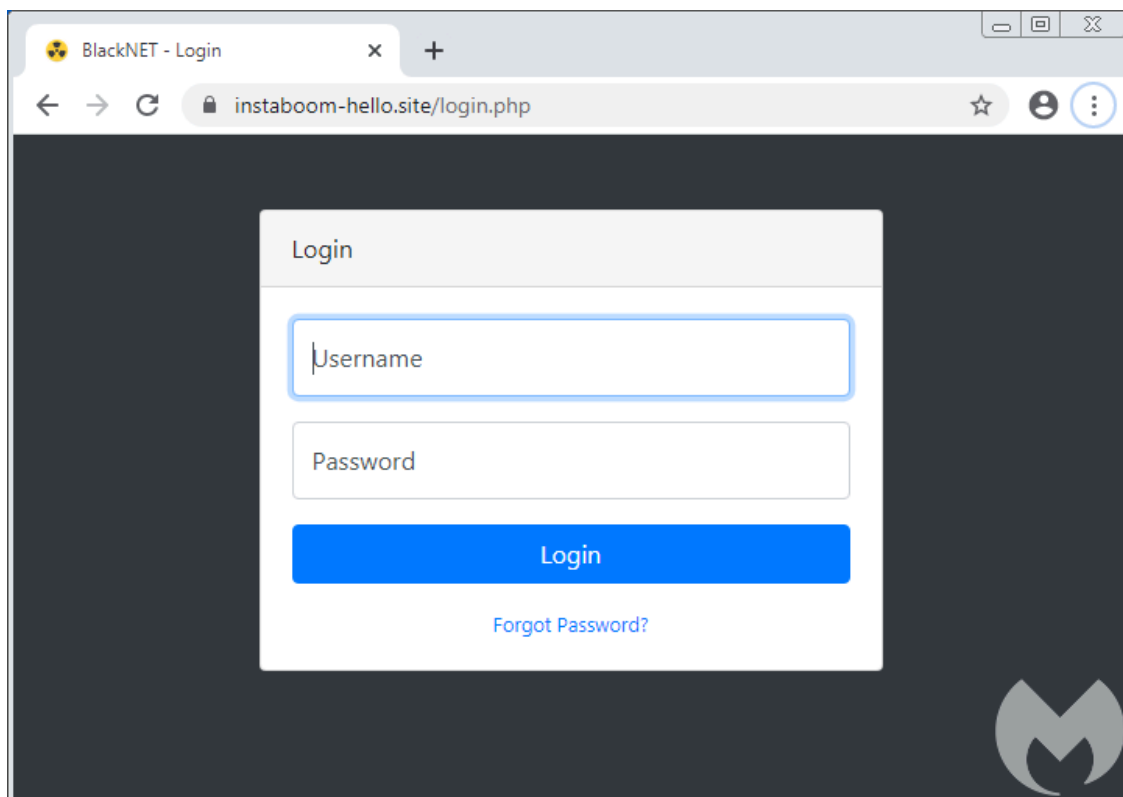


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

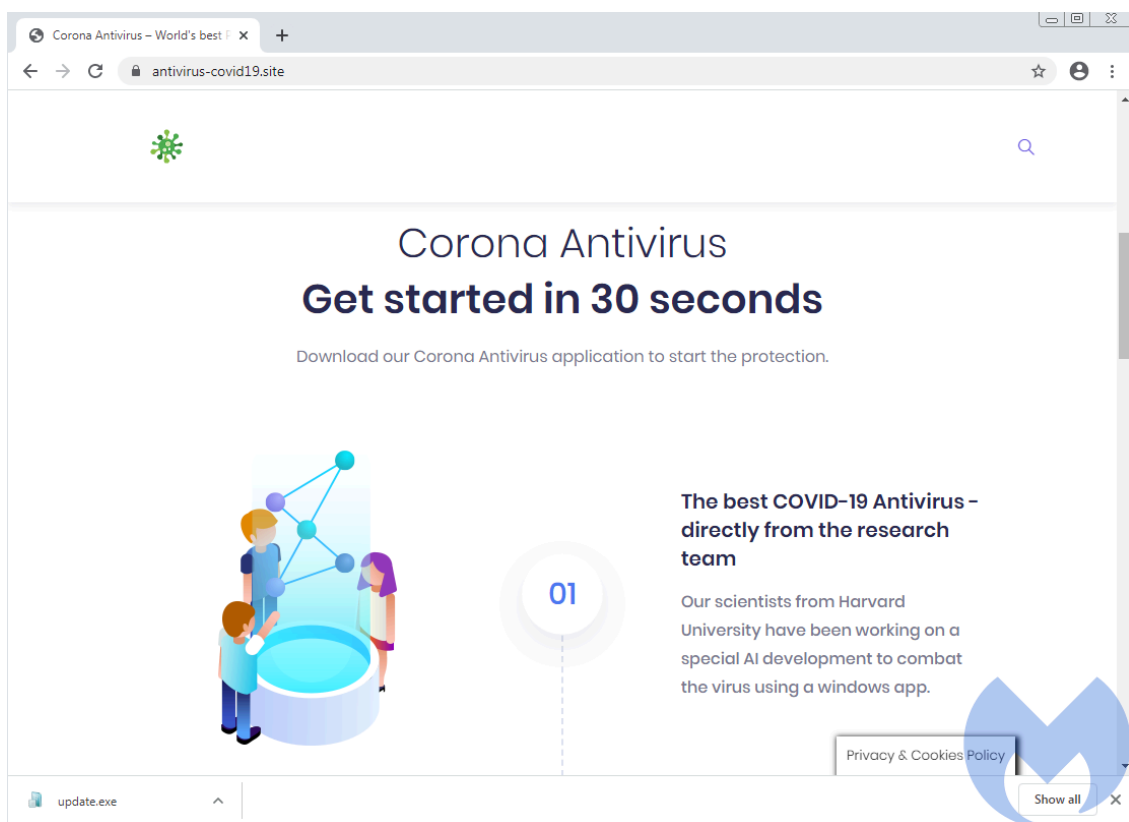
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table are 'Previous' and 'Next' buttons. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right of the commands center is a 'Map Visualization' section showing a world map with a blue overlay. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

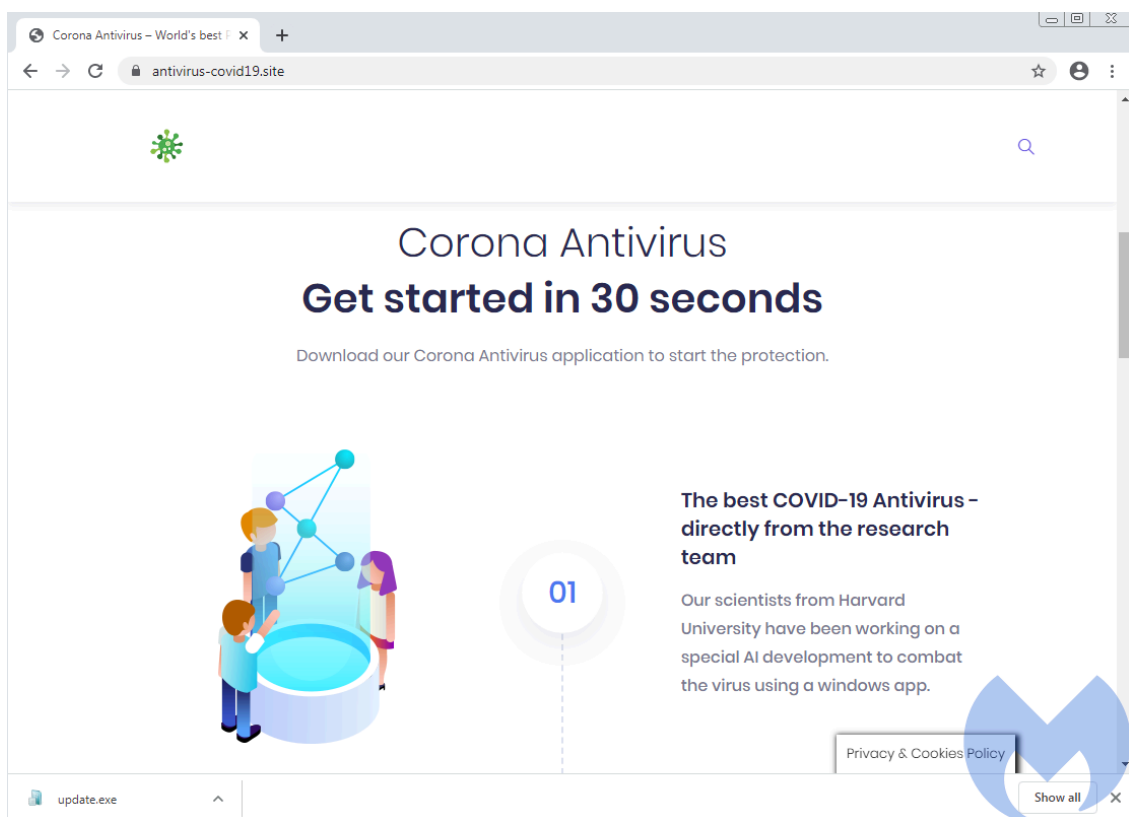
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

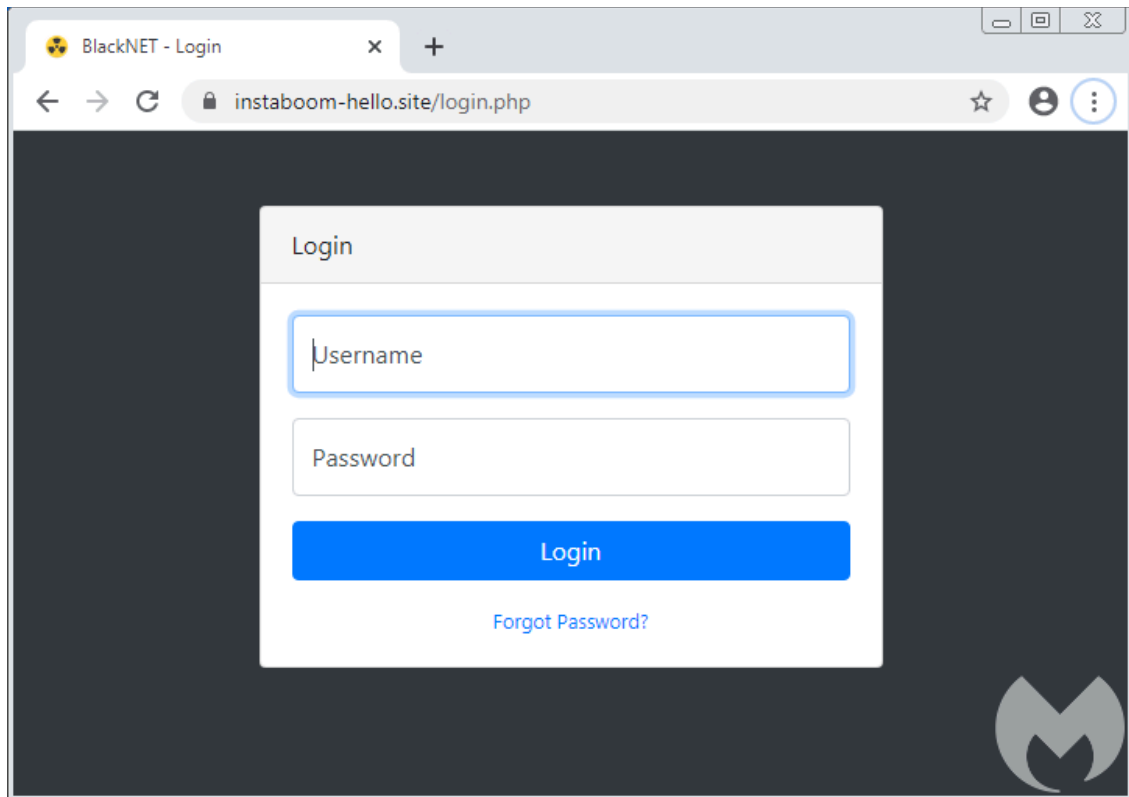


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

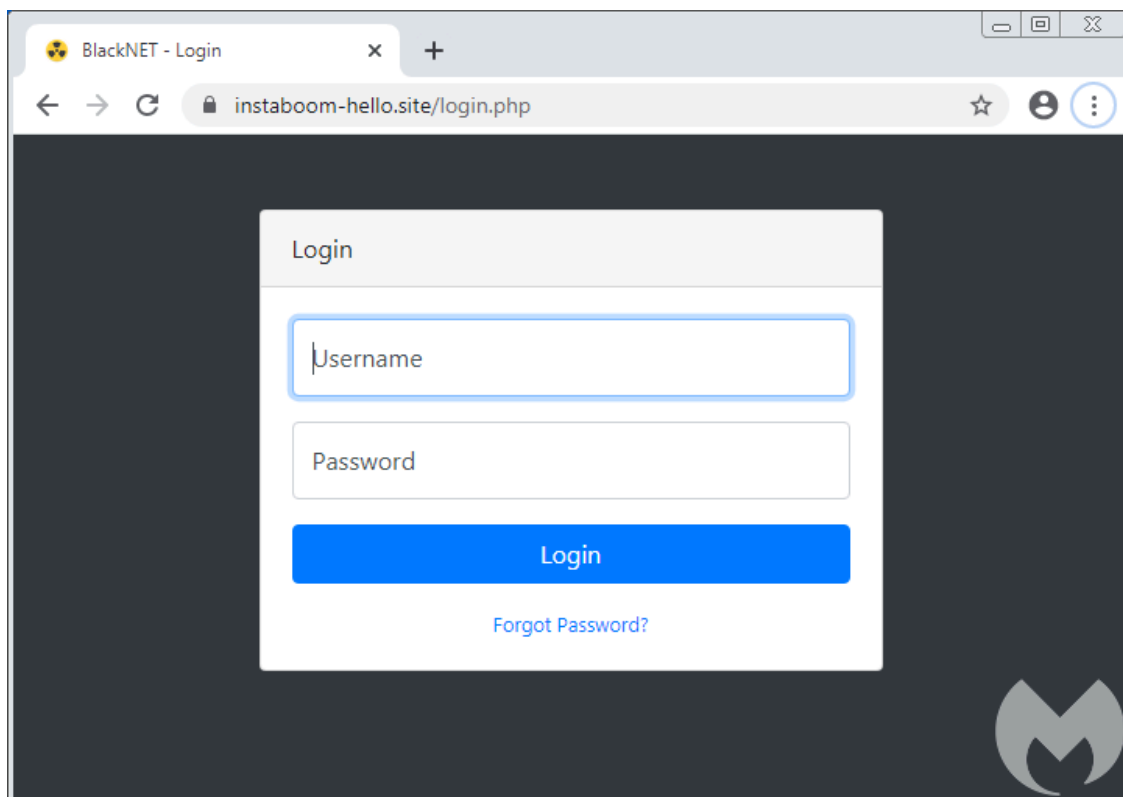
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET

Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from **here**.

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

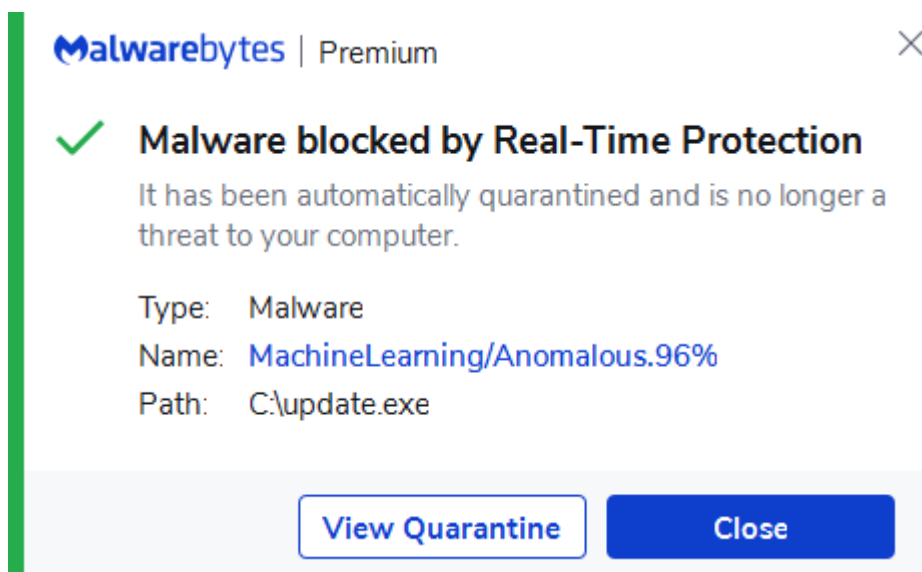
Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

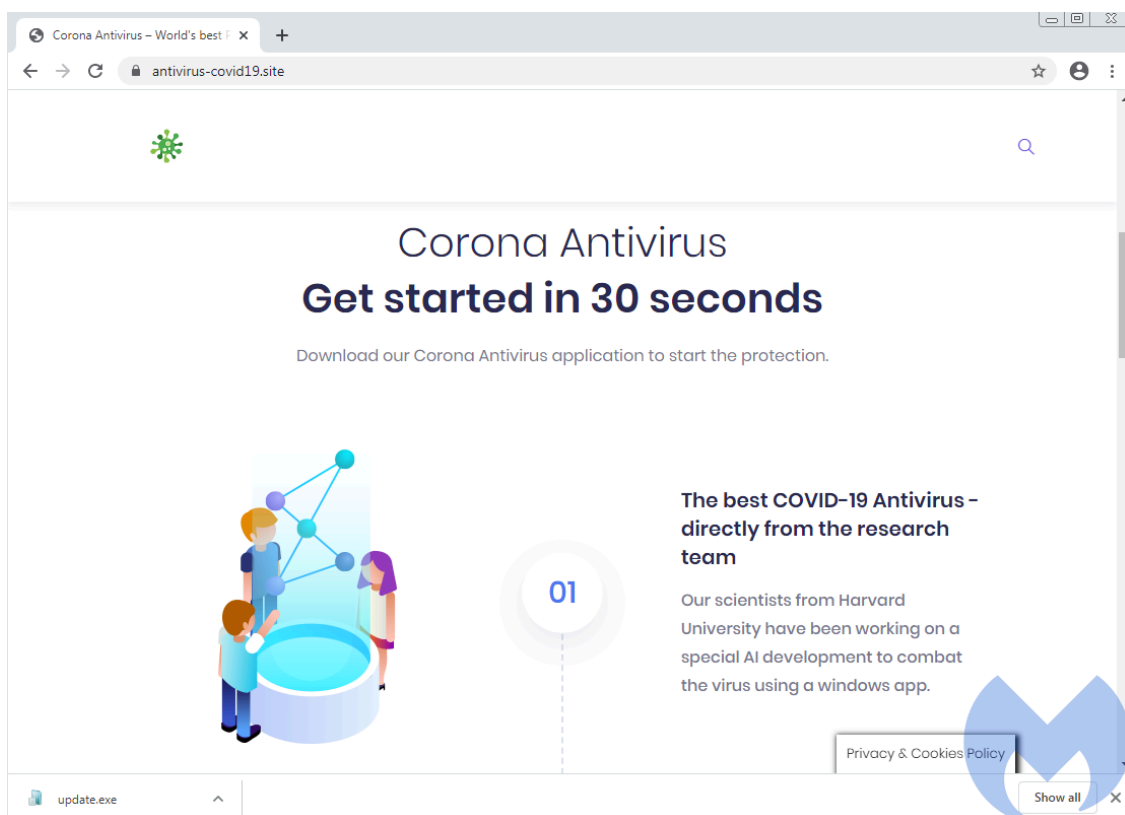
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

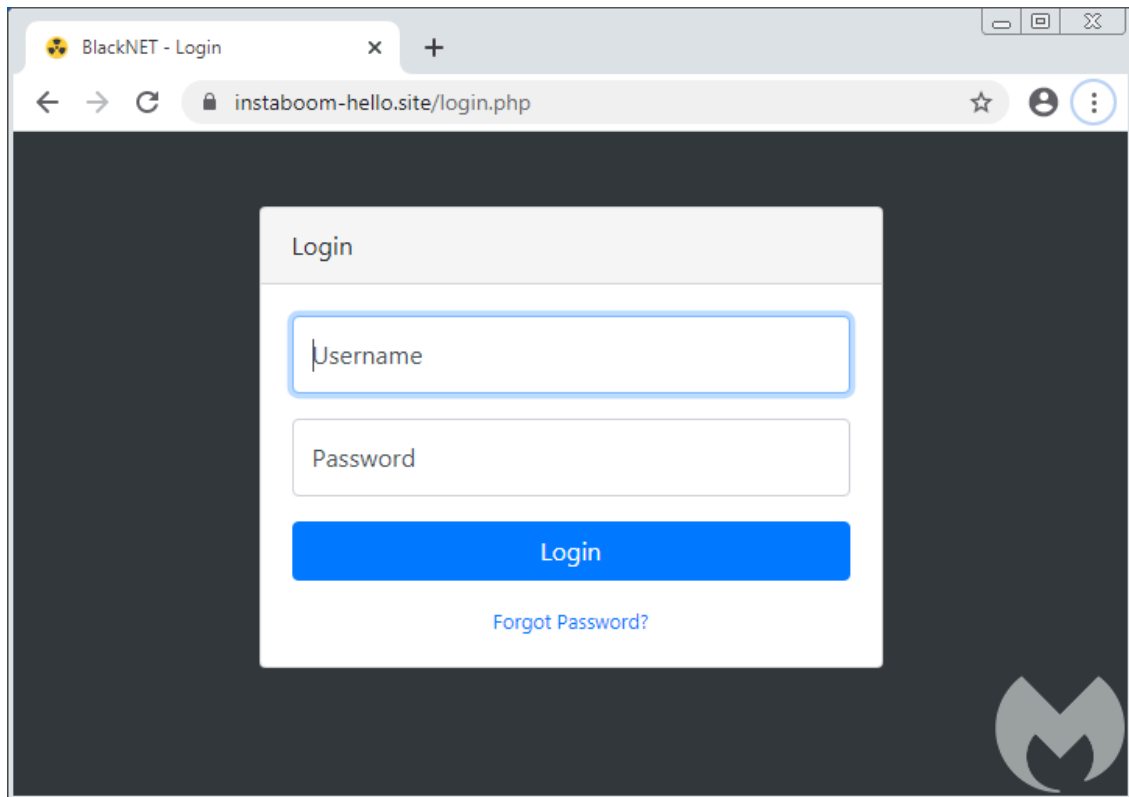


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with a few blue dots representing clients. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

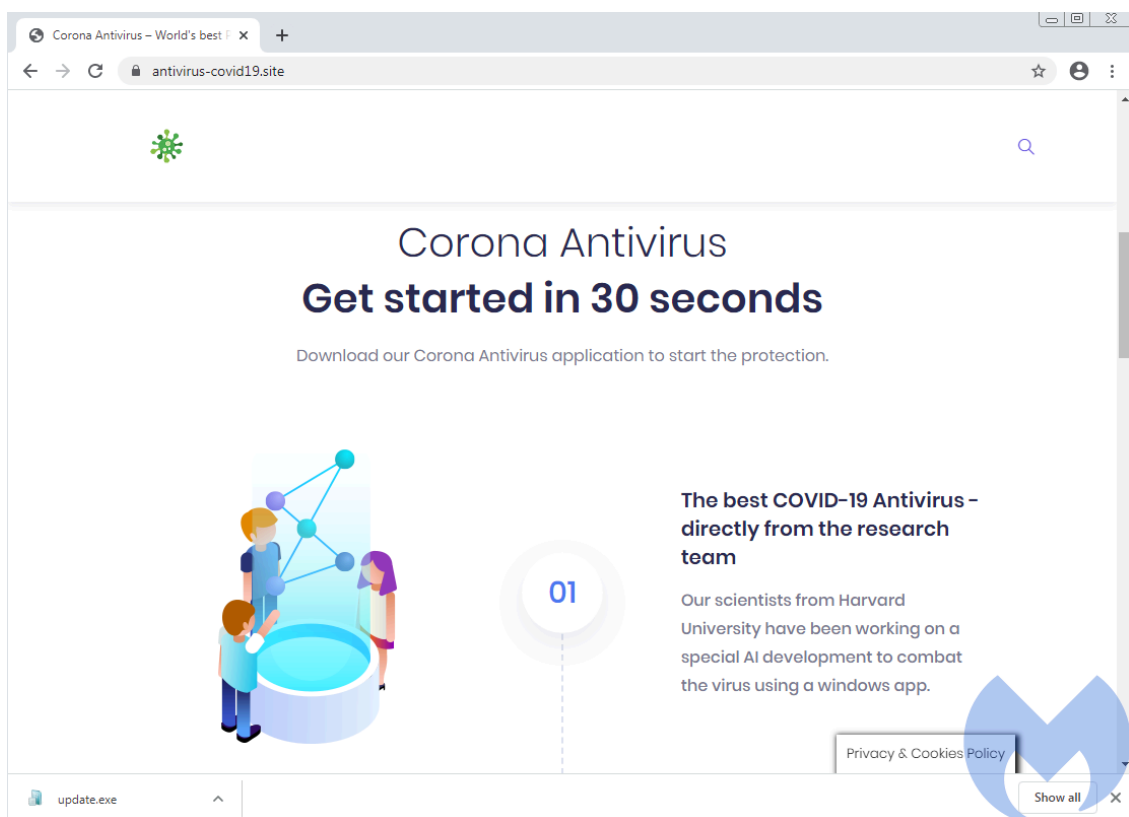
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

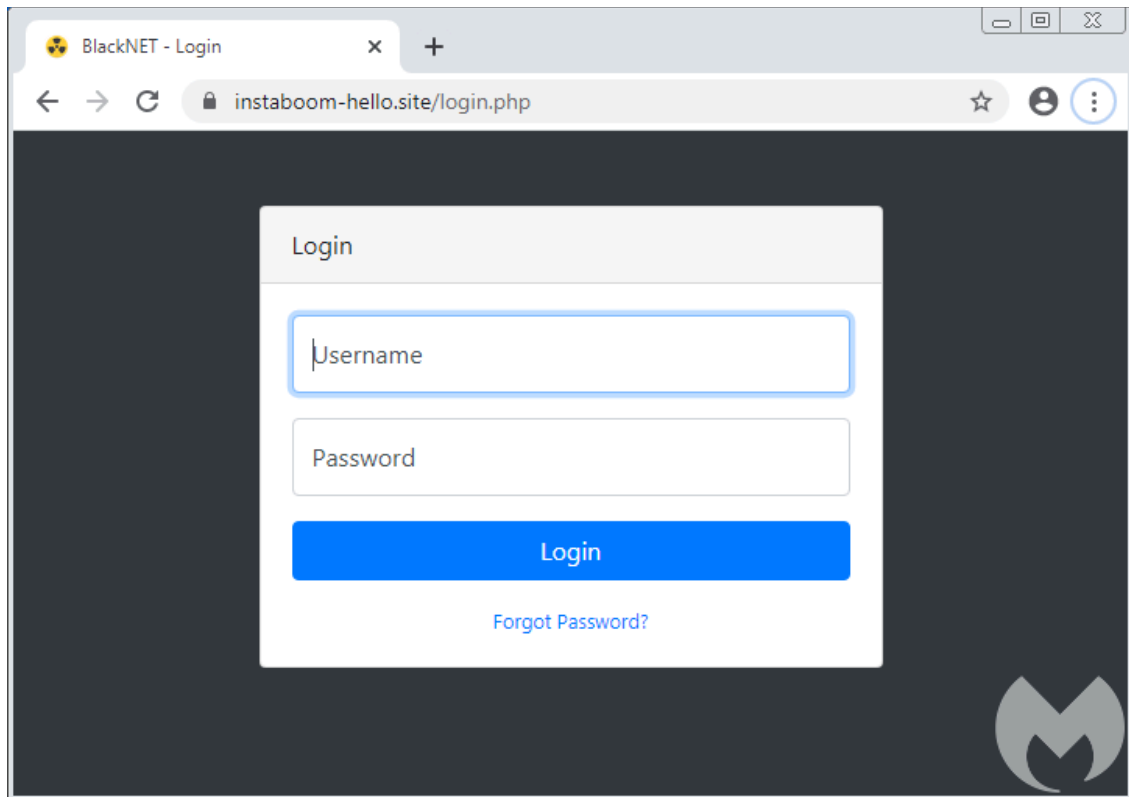


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, it lists the details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

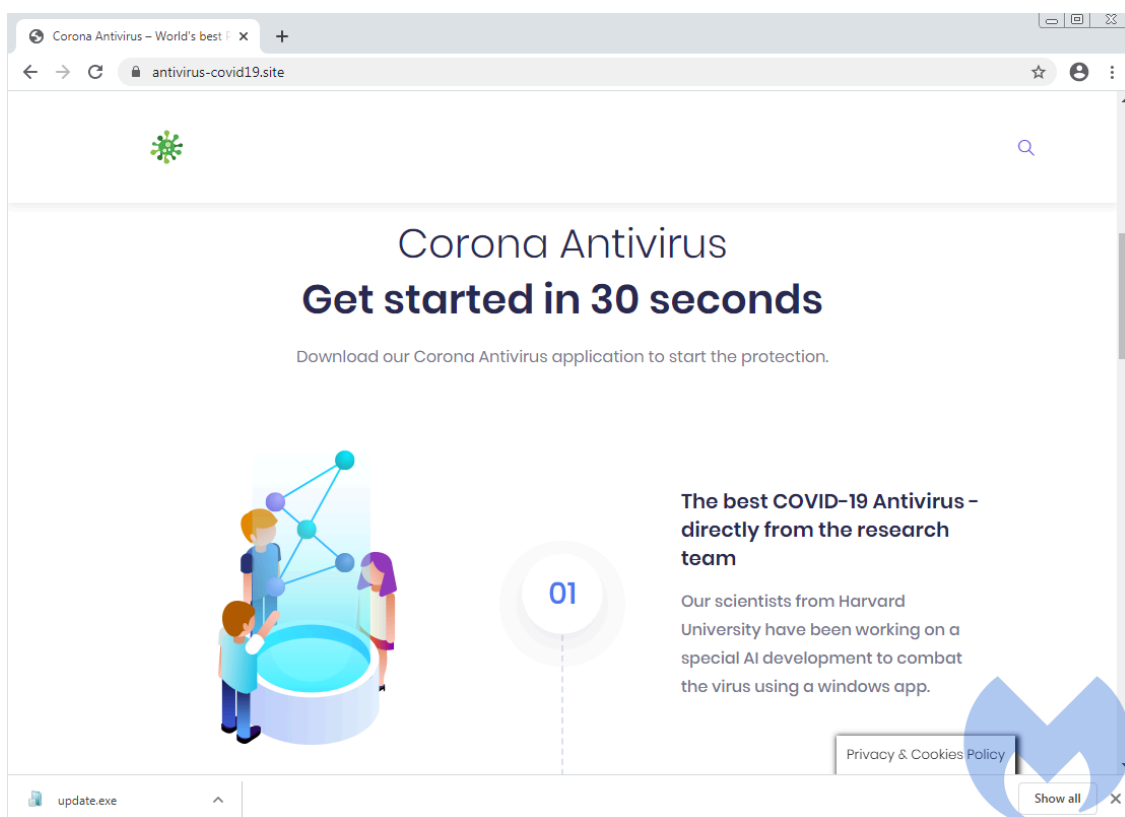
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

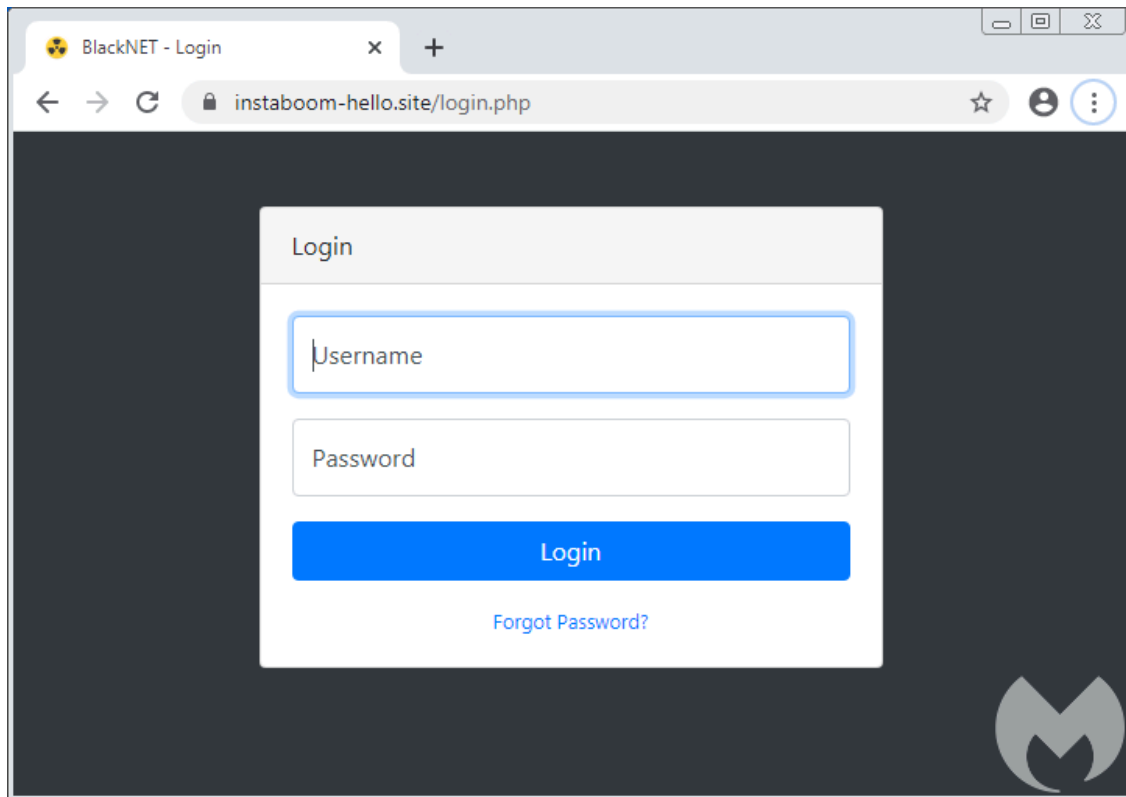


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored tiles: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

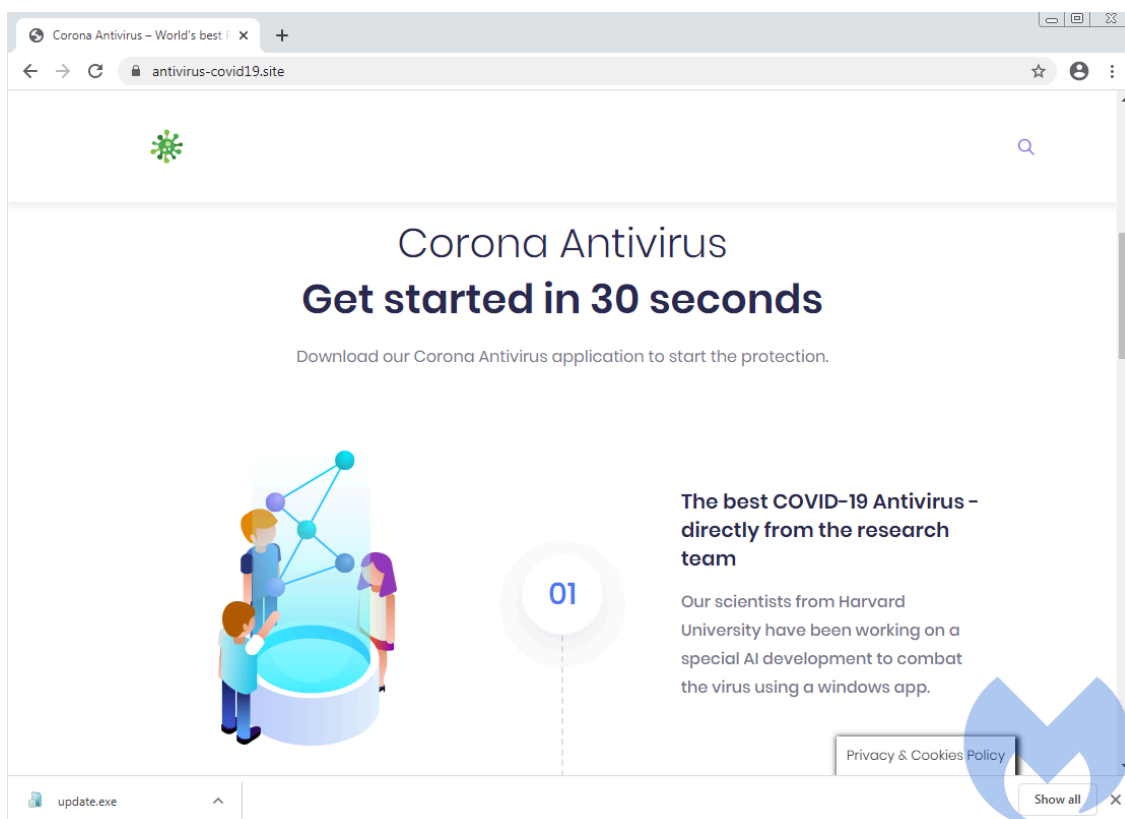
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

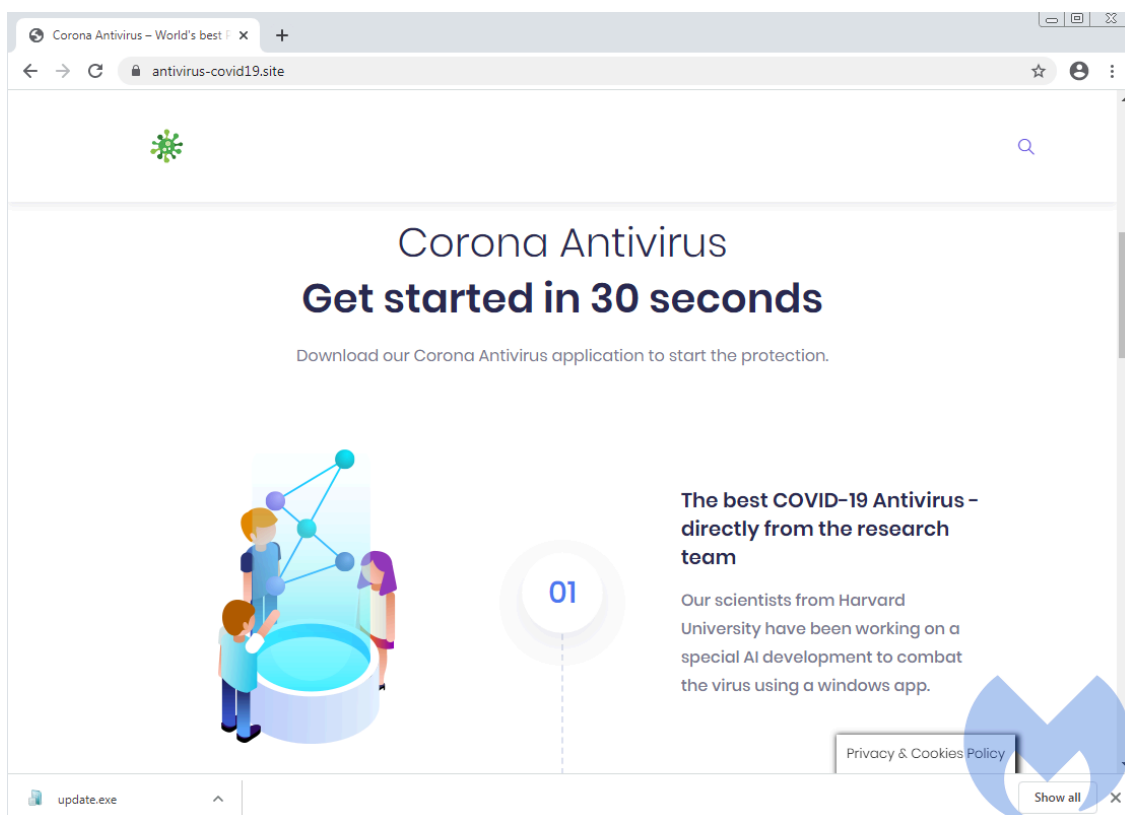
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

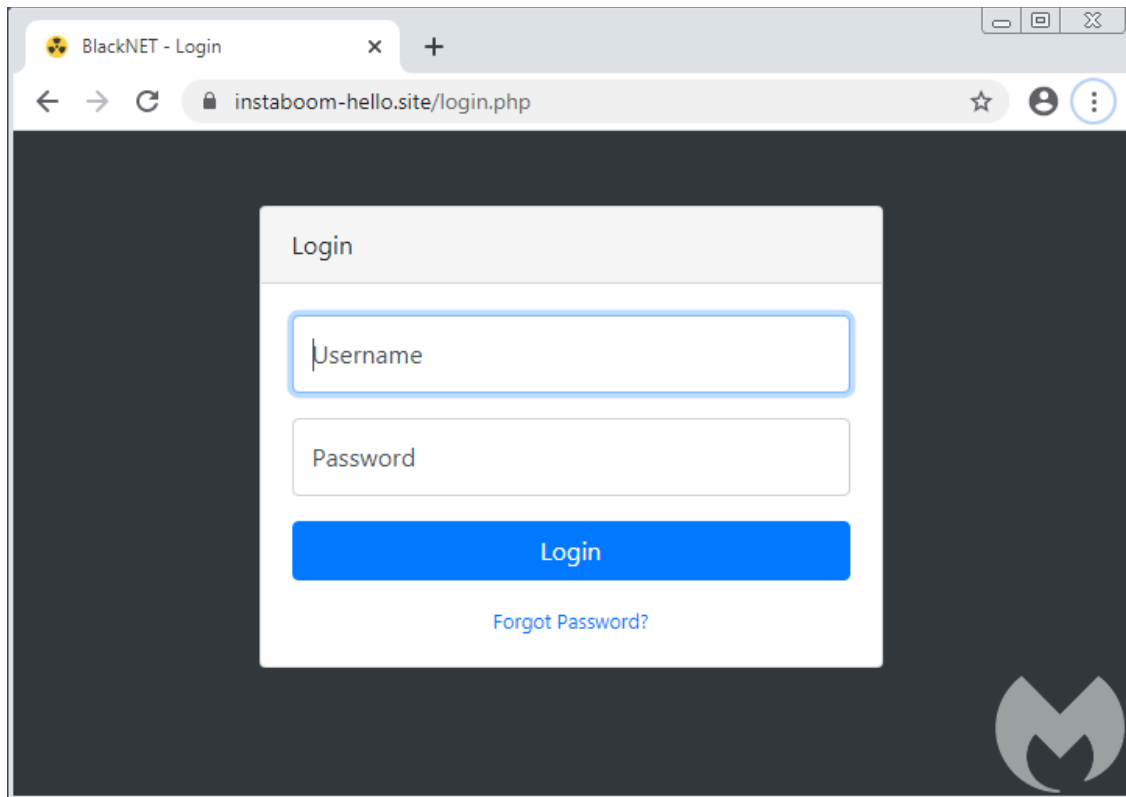


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

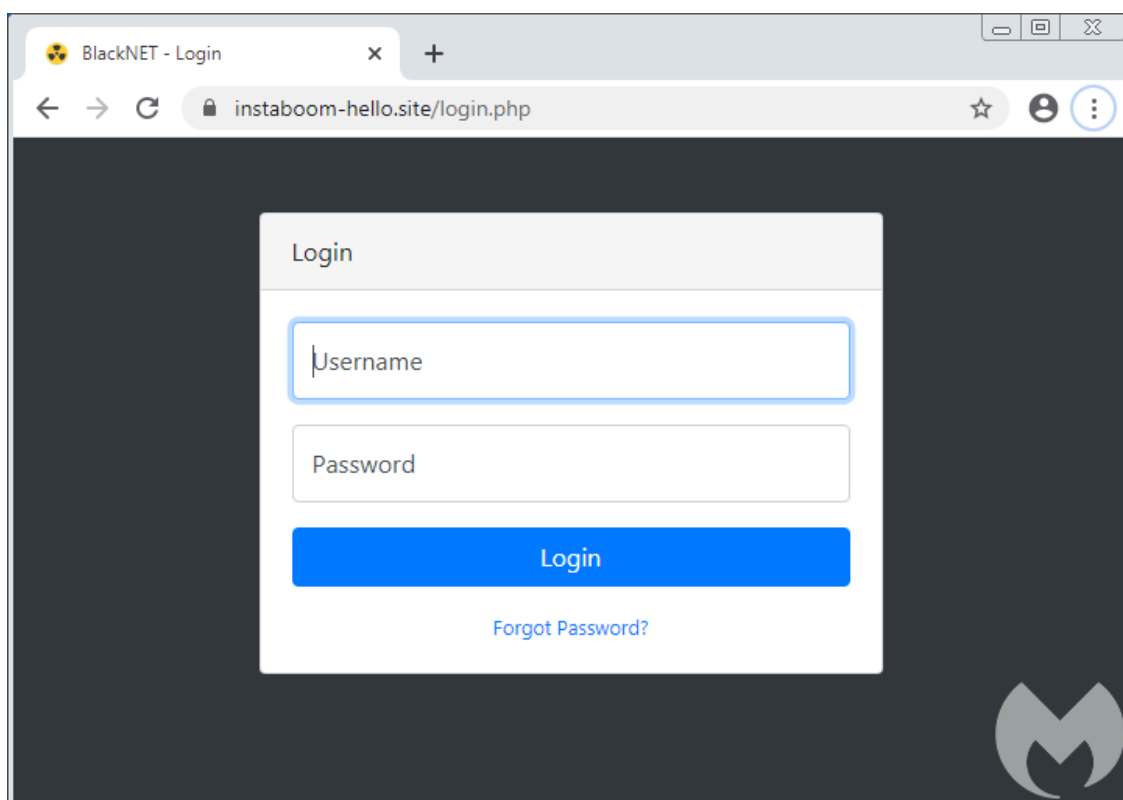
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

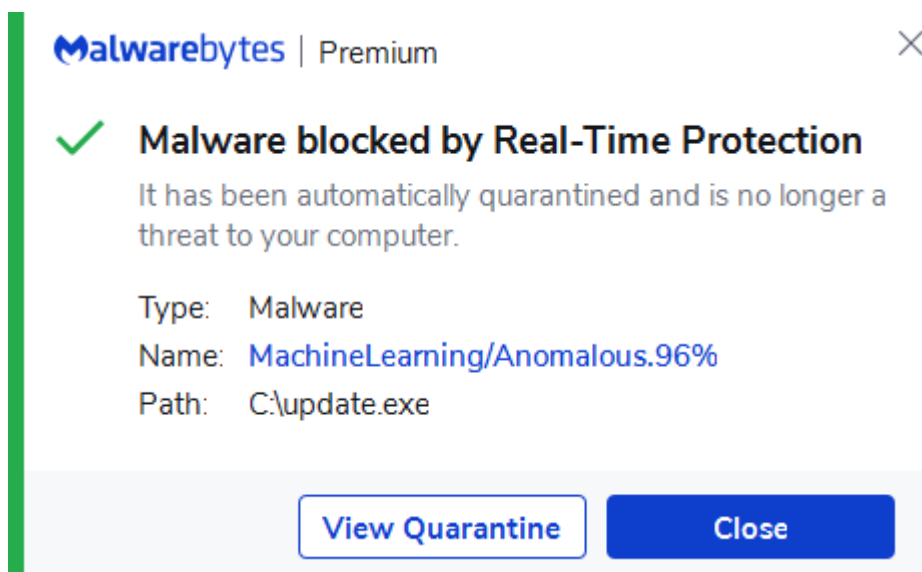
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

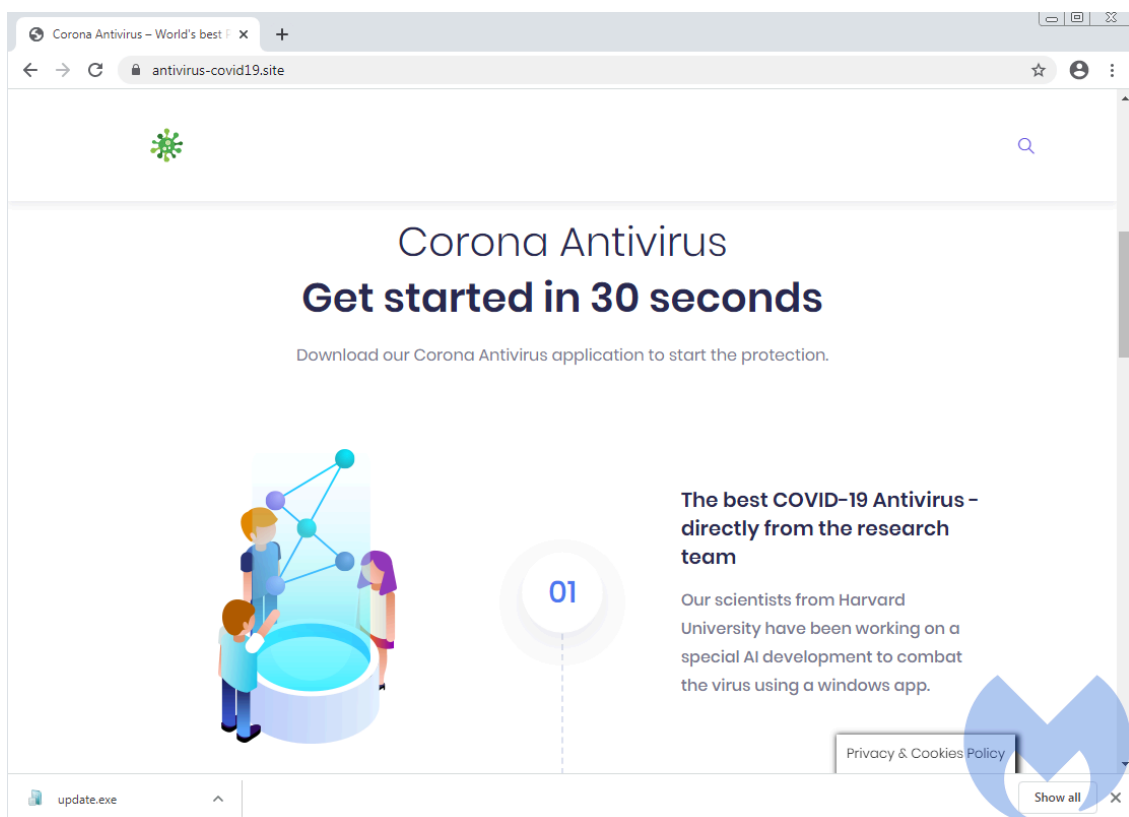
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

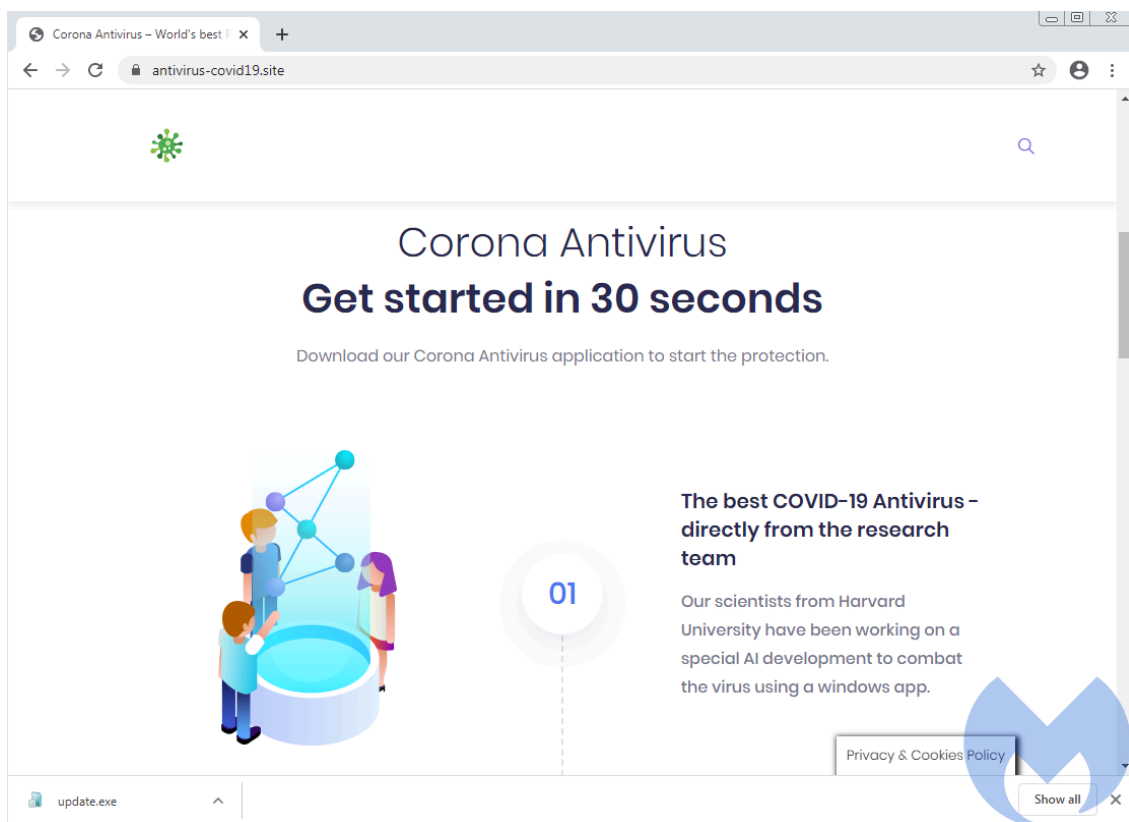
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

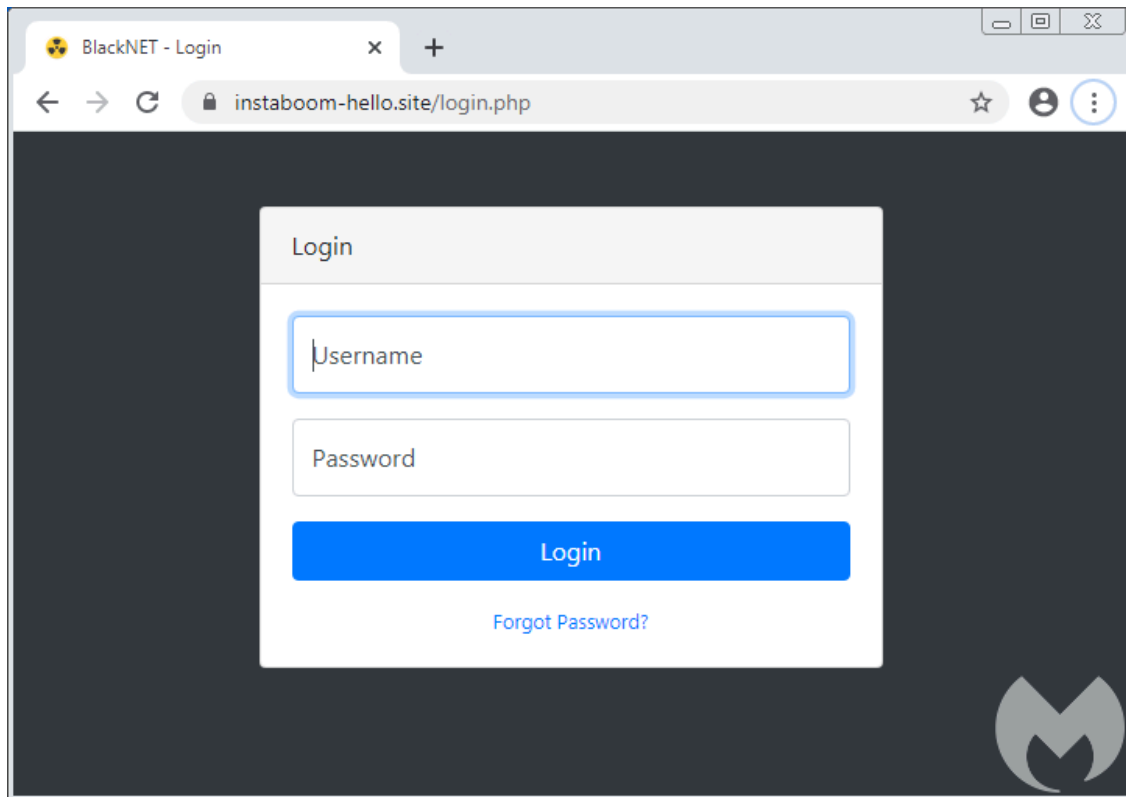


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. Further right is a 'Map Visualization' section showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

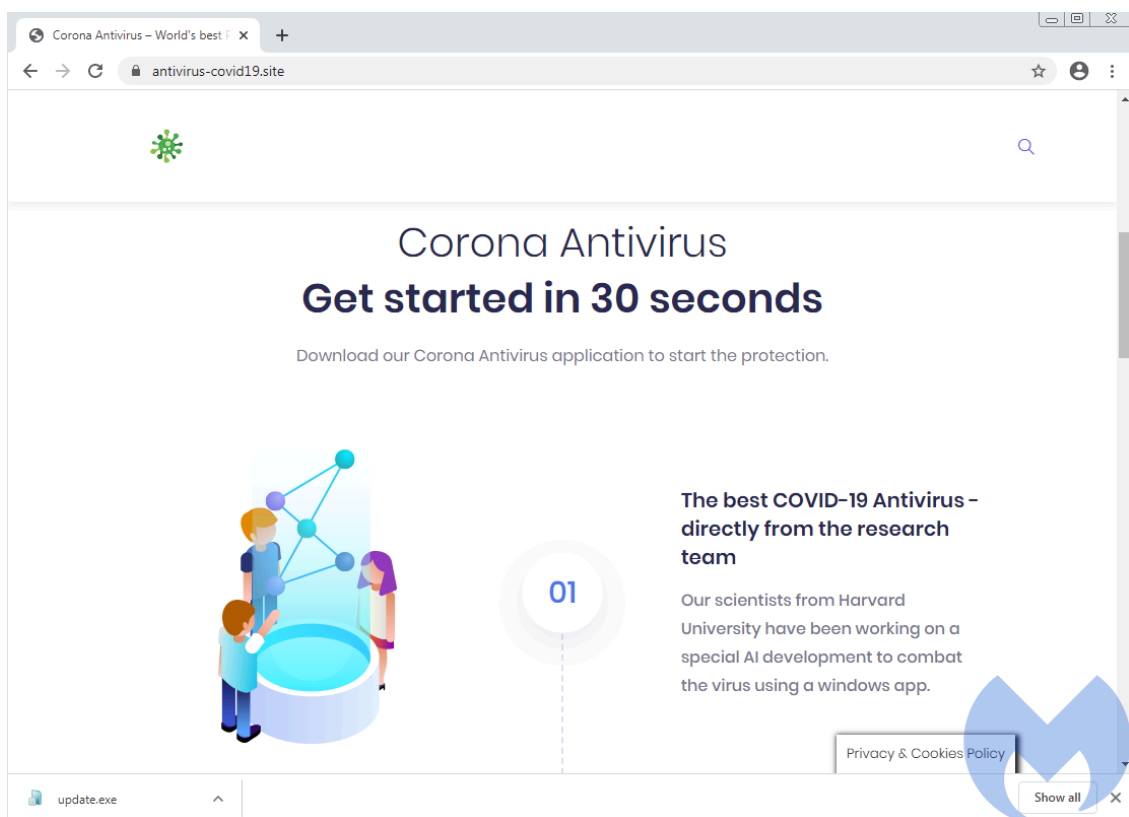
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

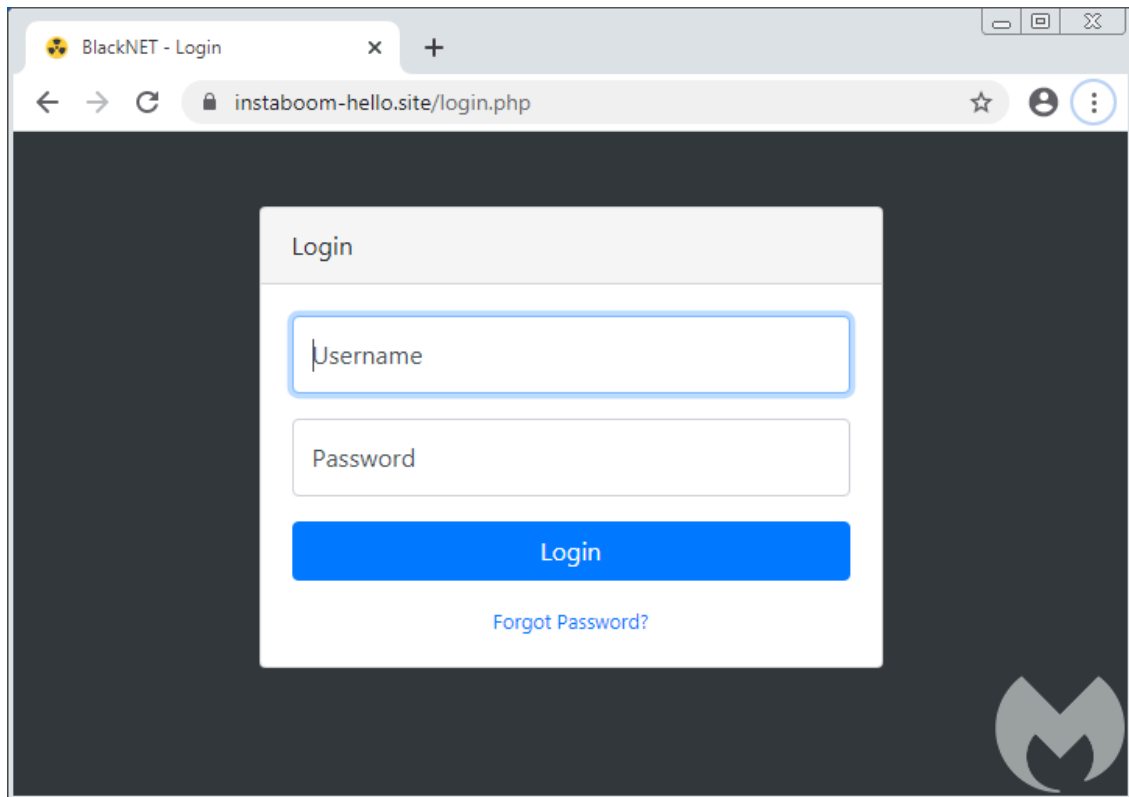


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

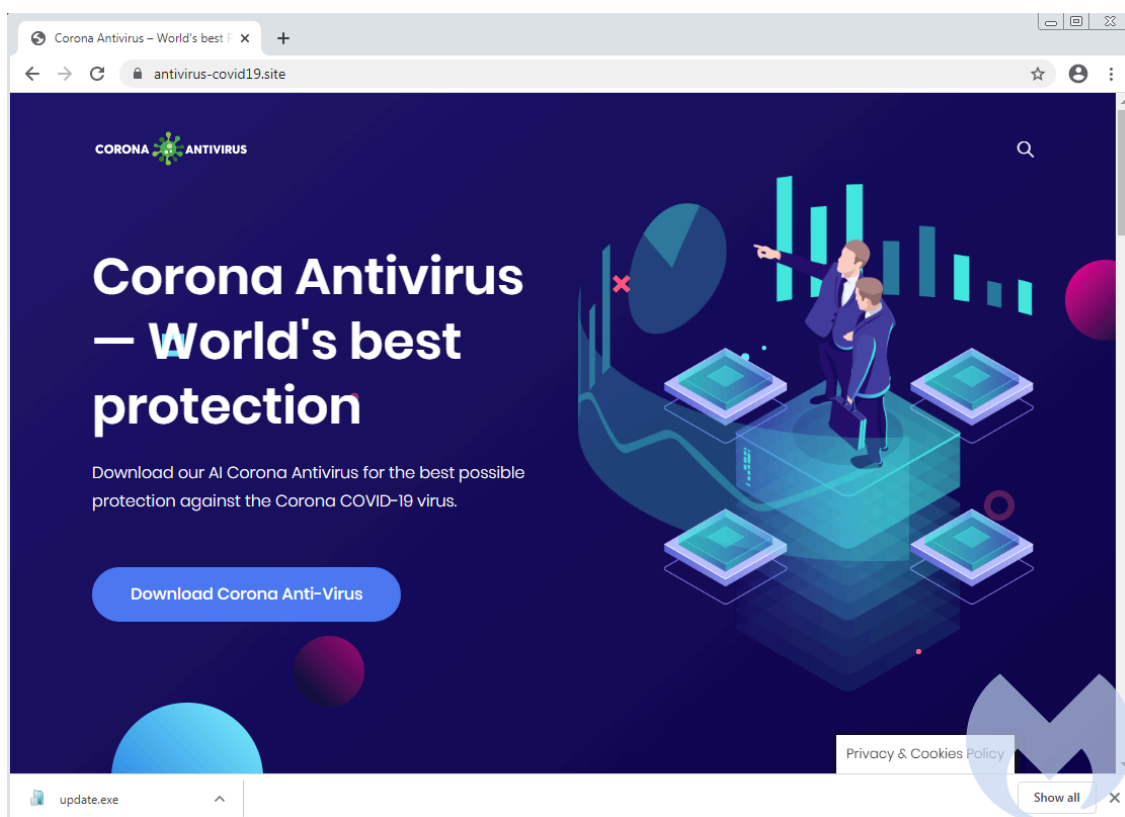
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

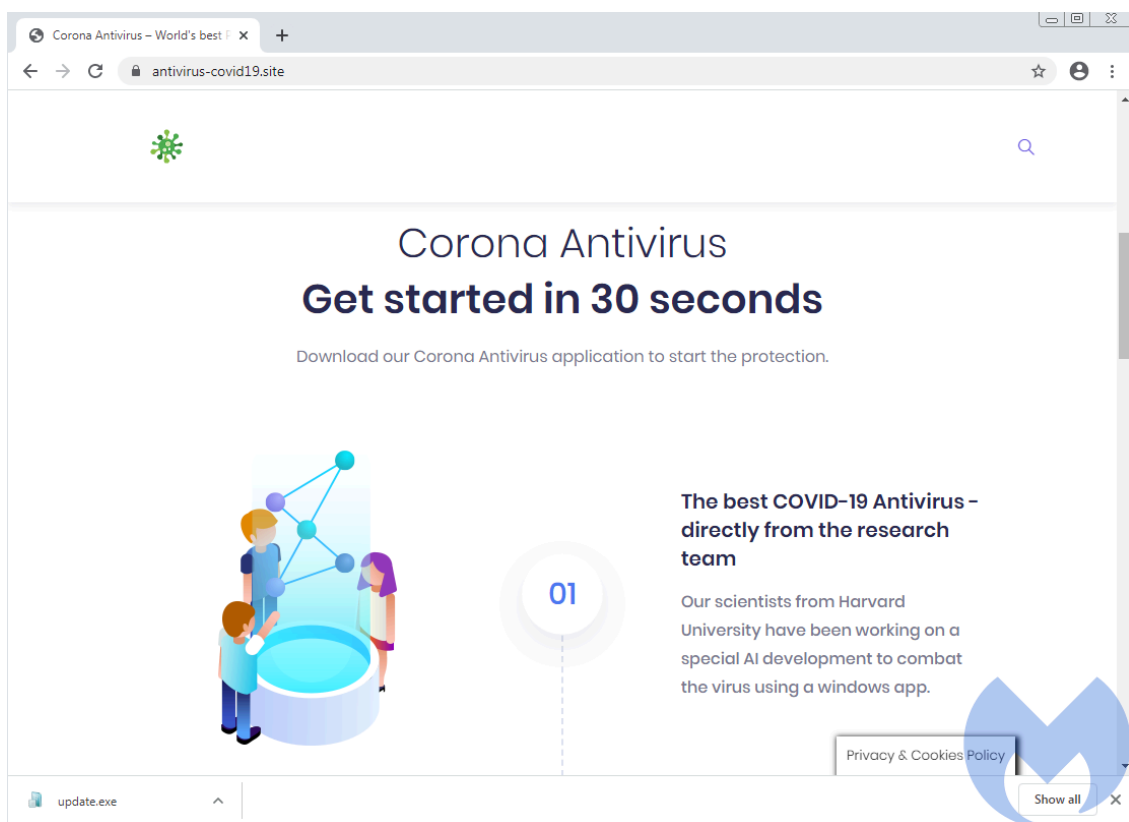
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table are 'Previous' and 'Next' buttons. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right of the commands center is a 'Map Visualization' section showing a world map with a blue overlay. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

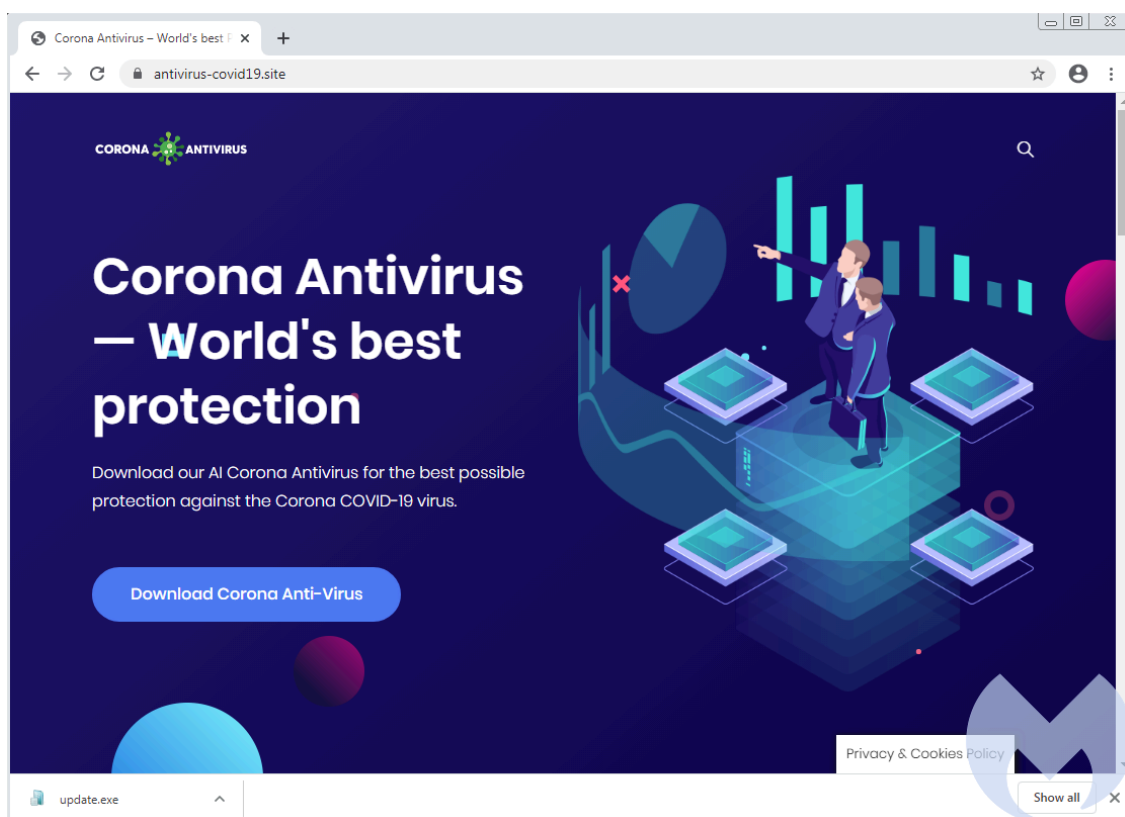
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

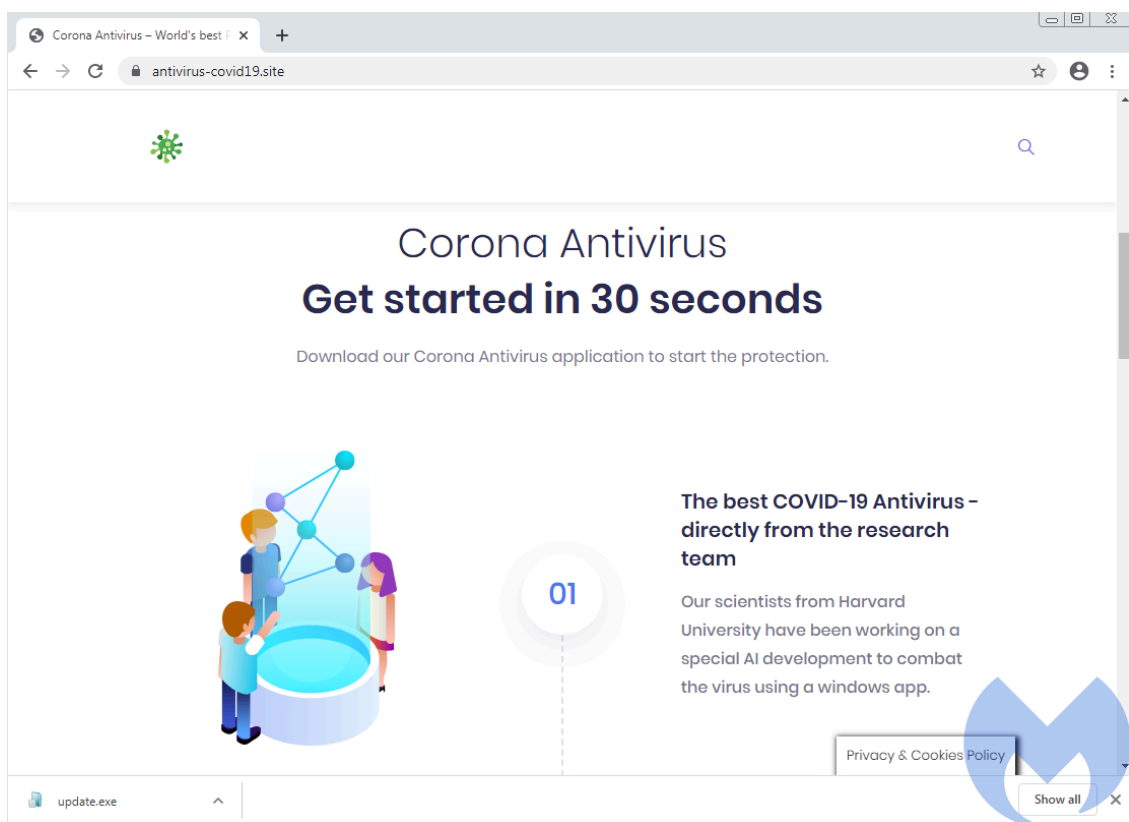
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

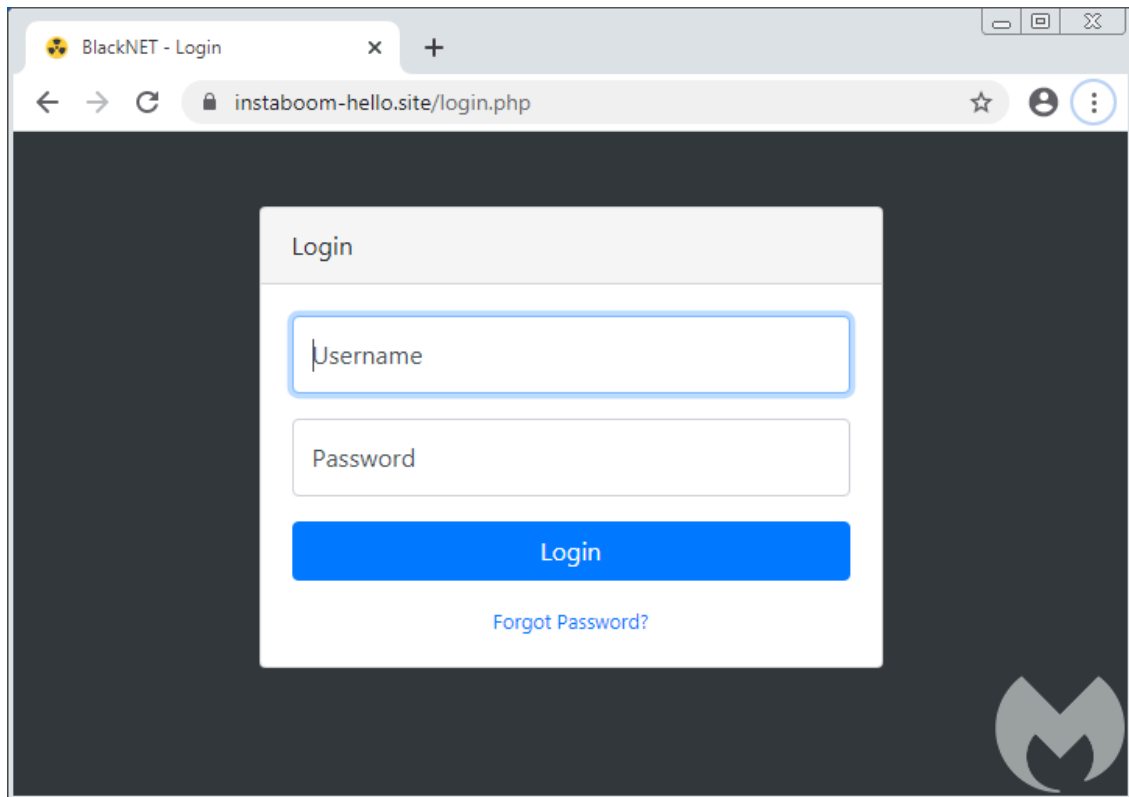


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features the Malwarebytes logo and the word 'Premium' in the top left corner. A green checkmark icon is next to the heading 'Malware blocked by Real-Time Protection'. Below this, a message states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

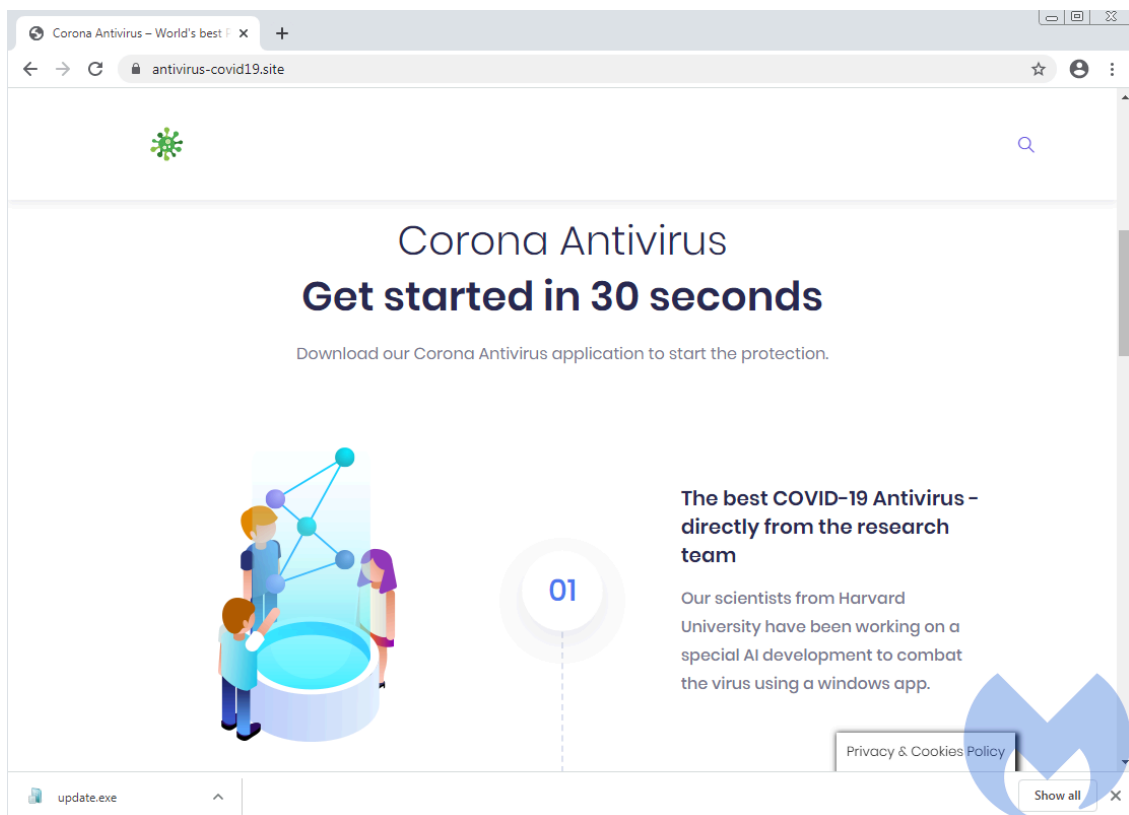
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

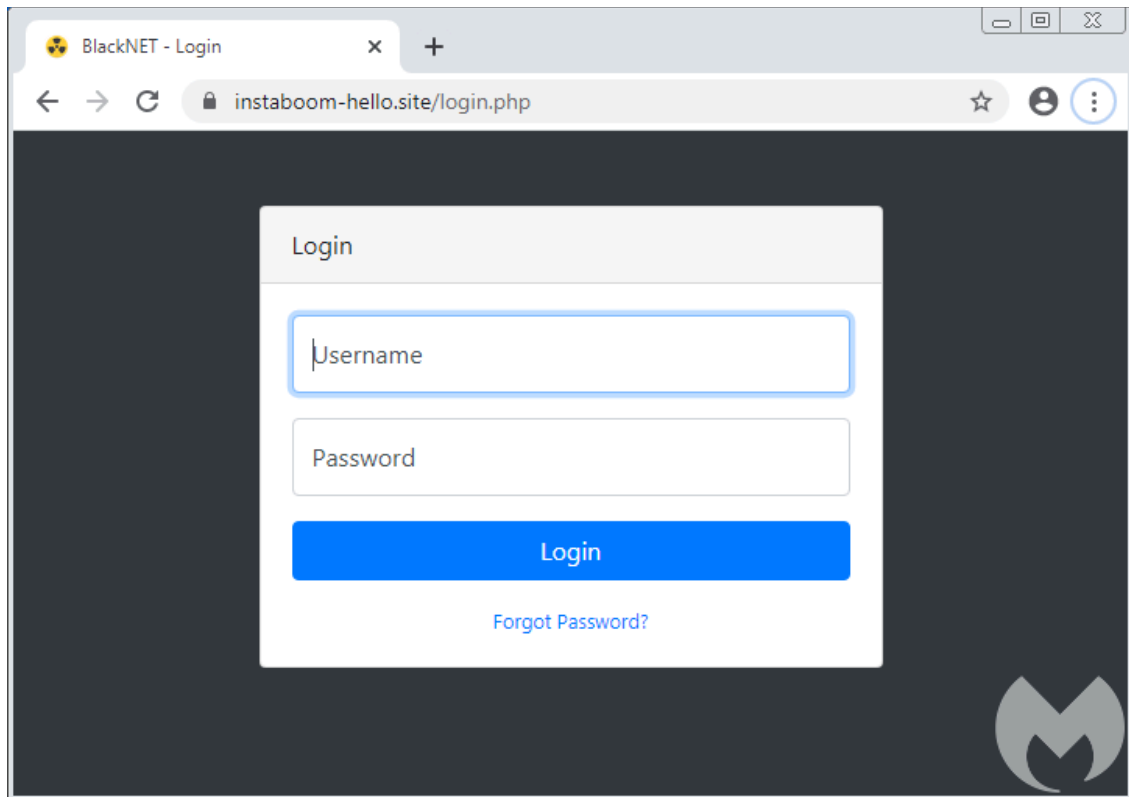


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

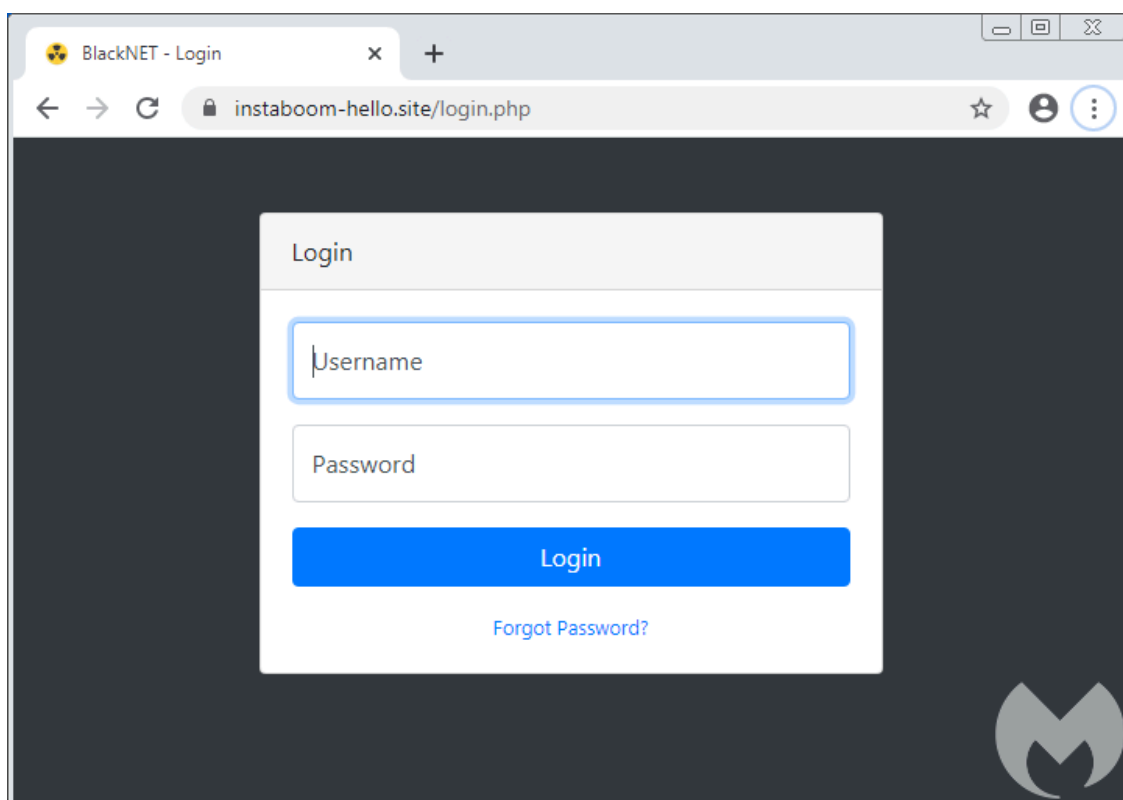
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

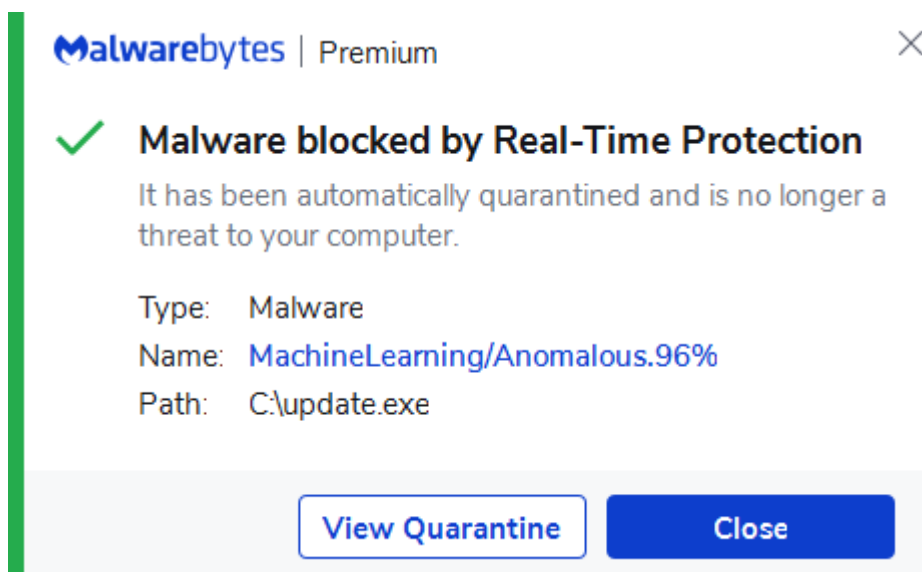
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' navigation buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

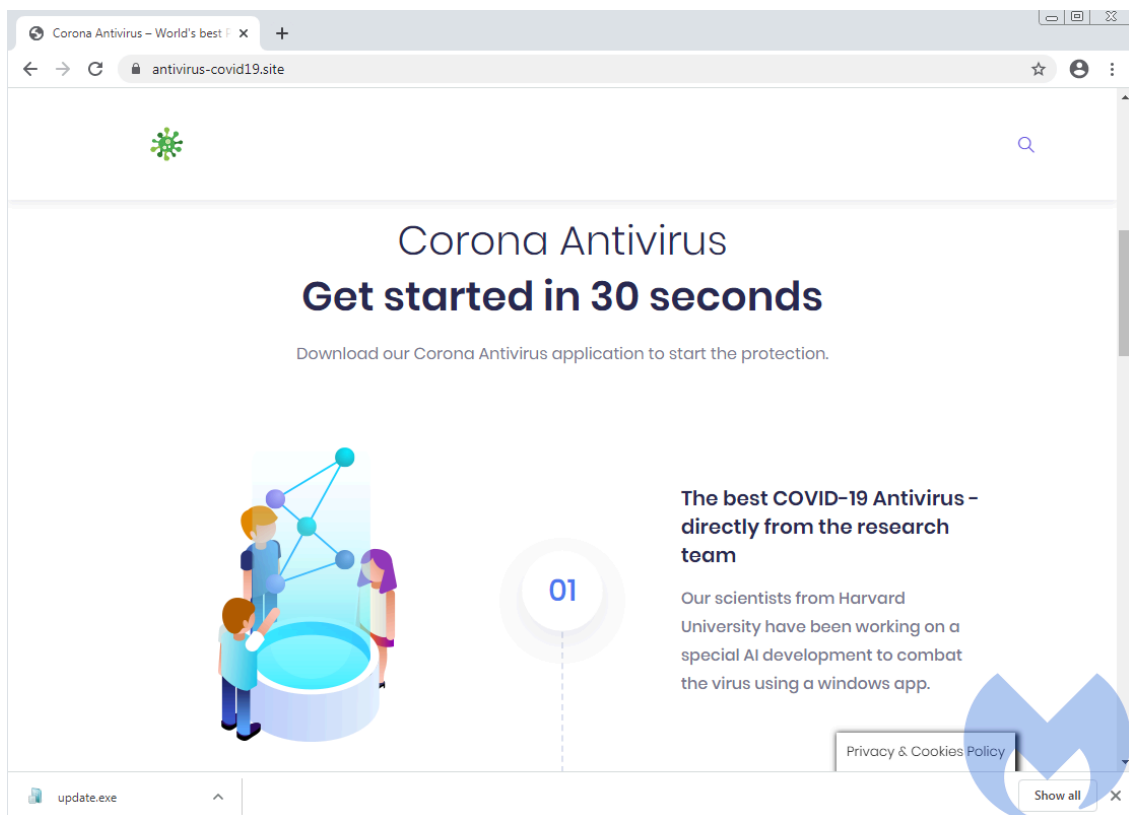
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

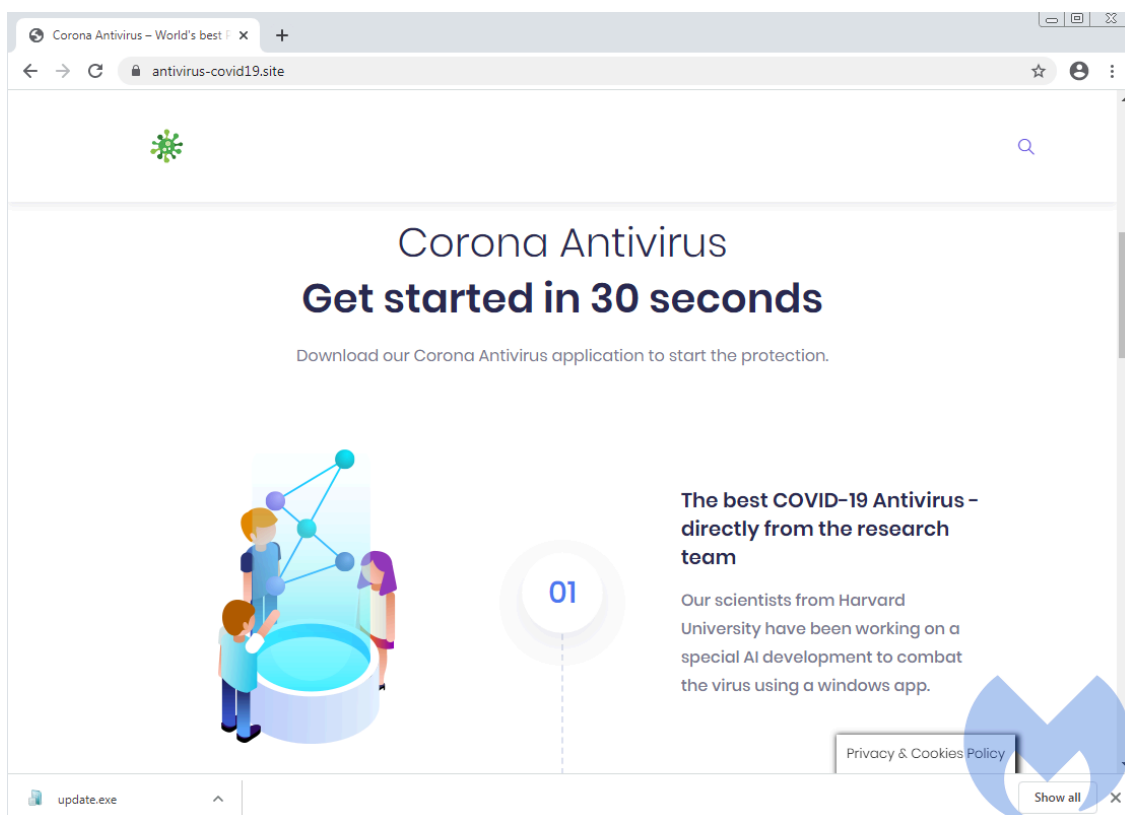
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

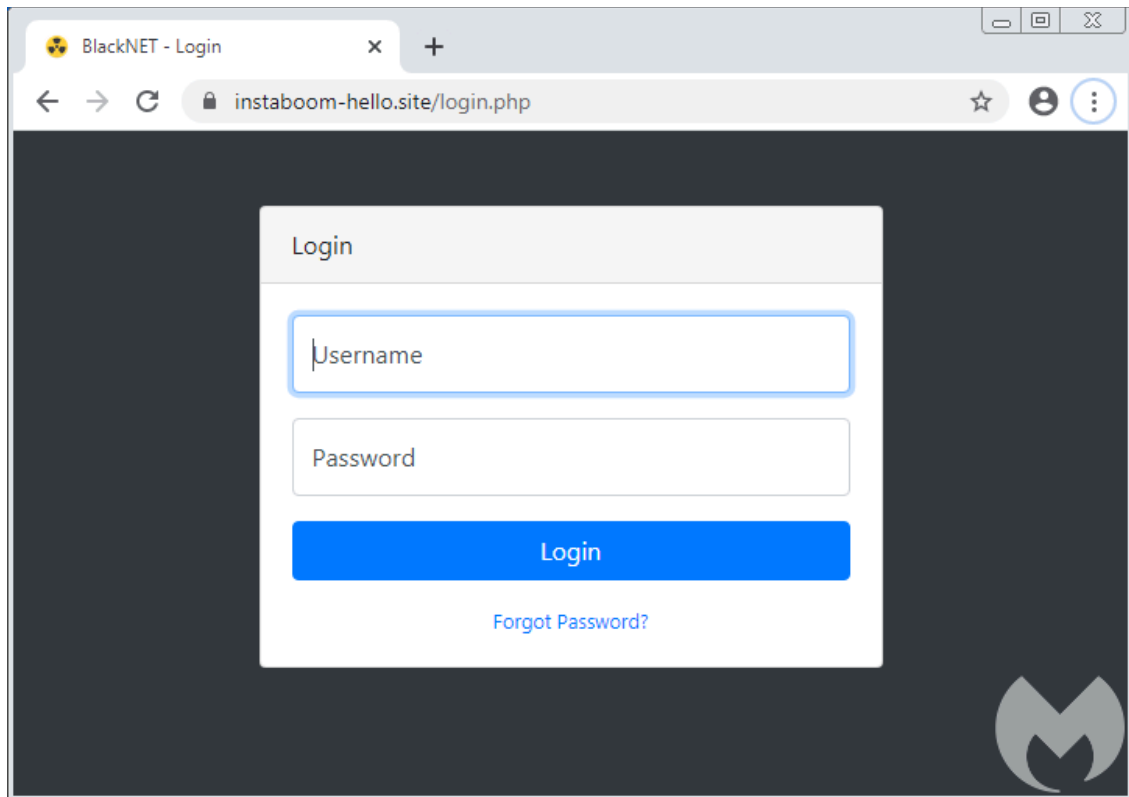


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with a few blue dots indicating client locations. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features the Malwarebytes logo and 'Premium' text. A green checkmark icon is next to the heading 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

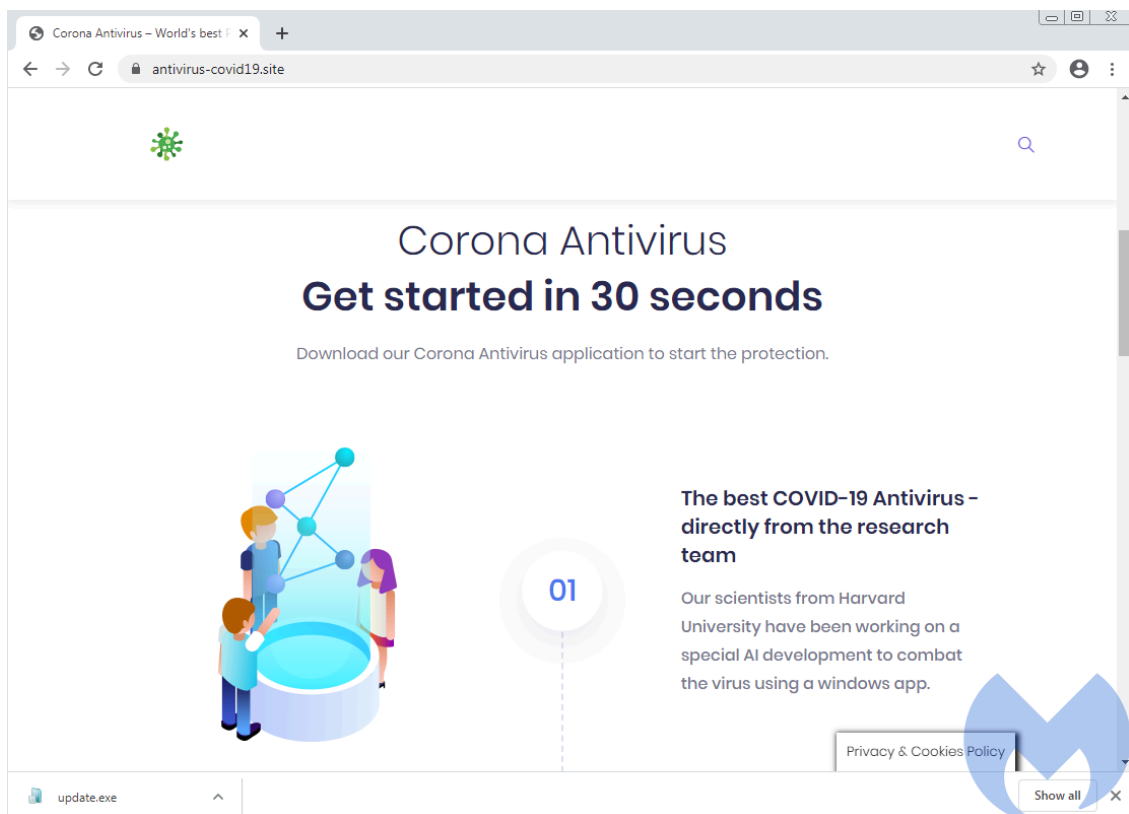
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

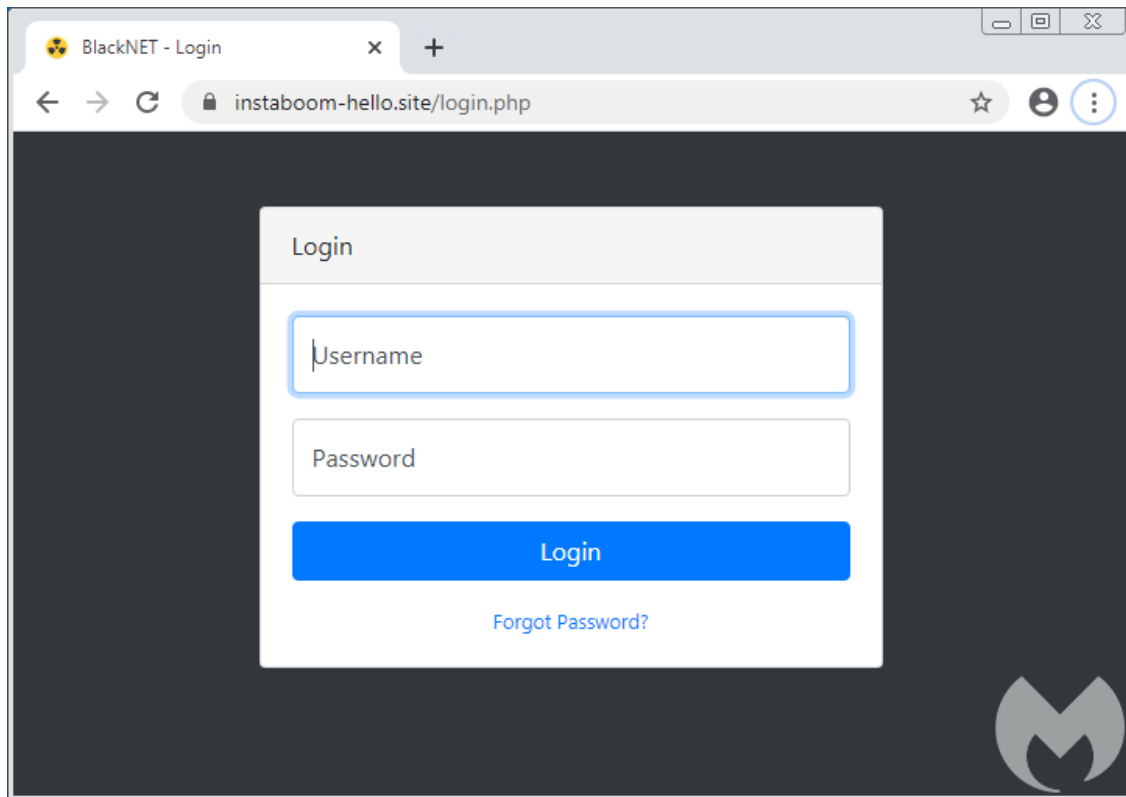


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

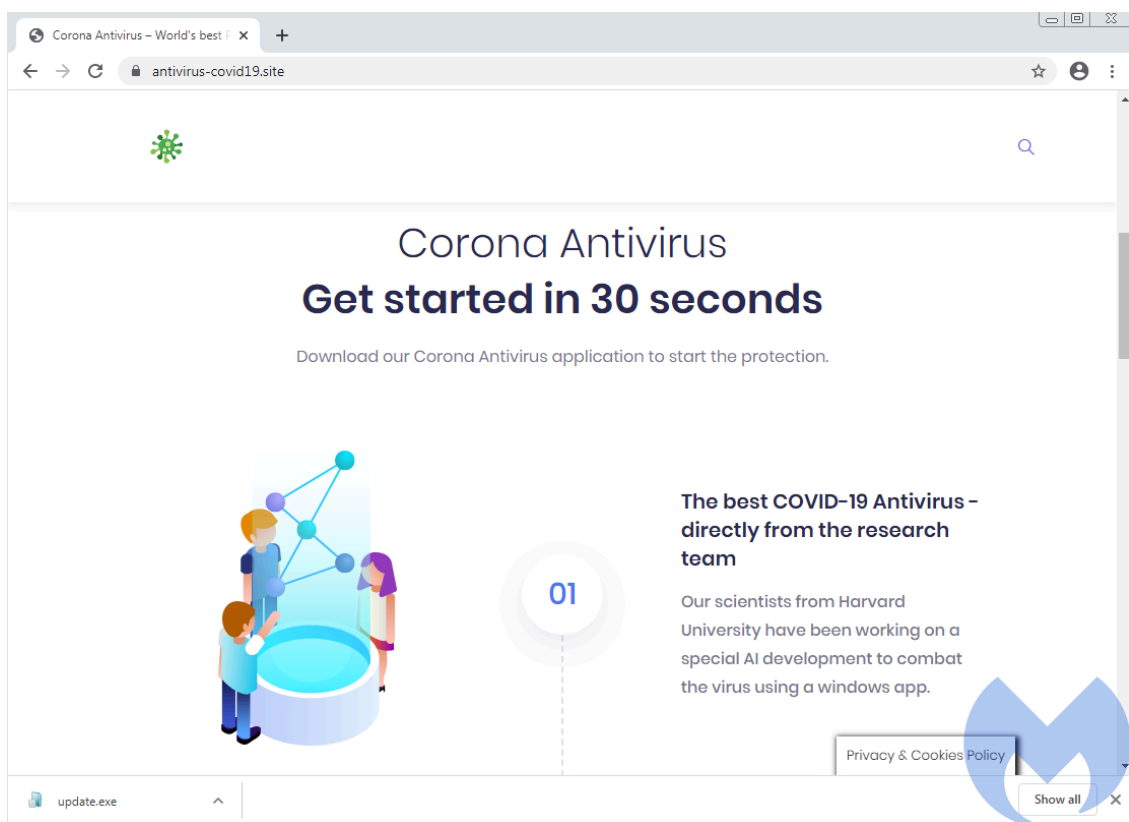
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

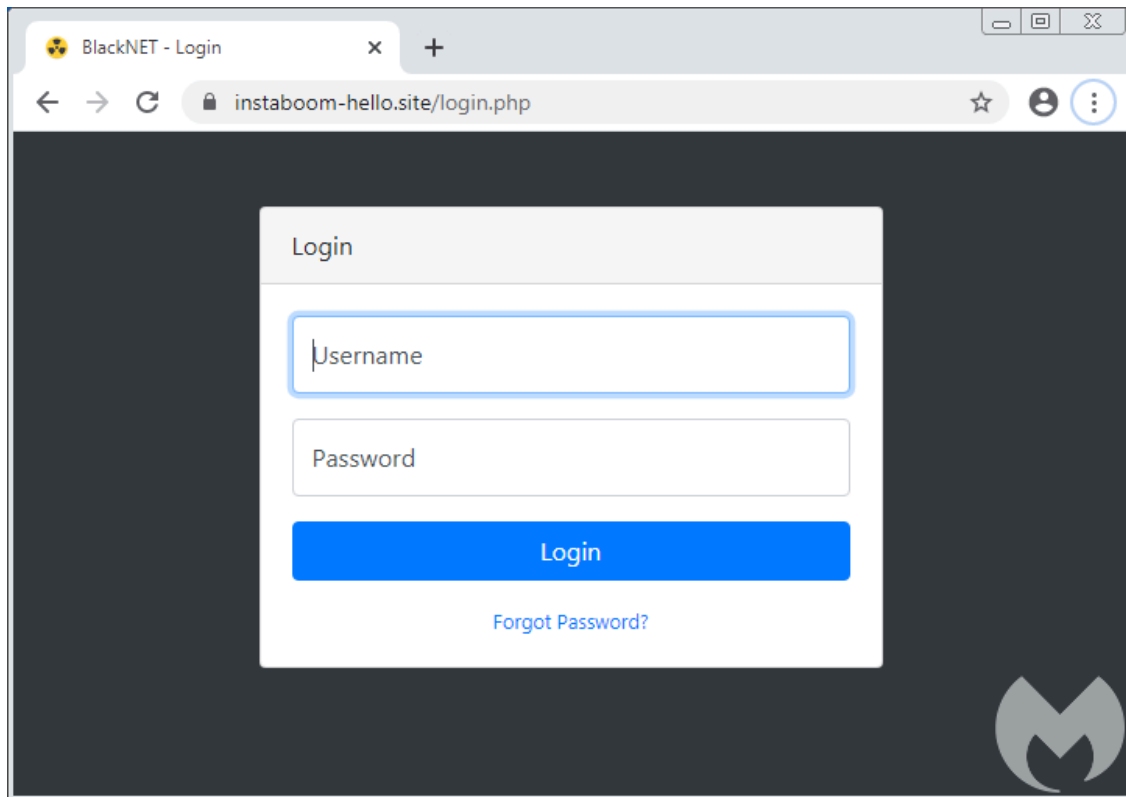


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

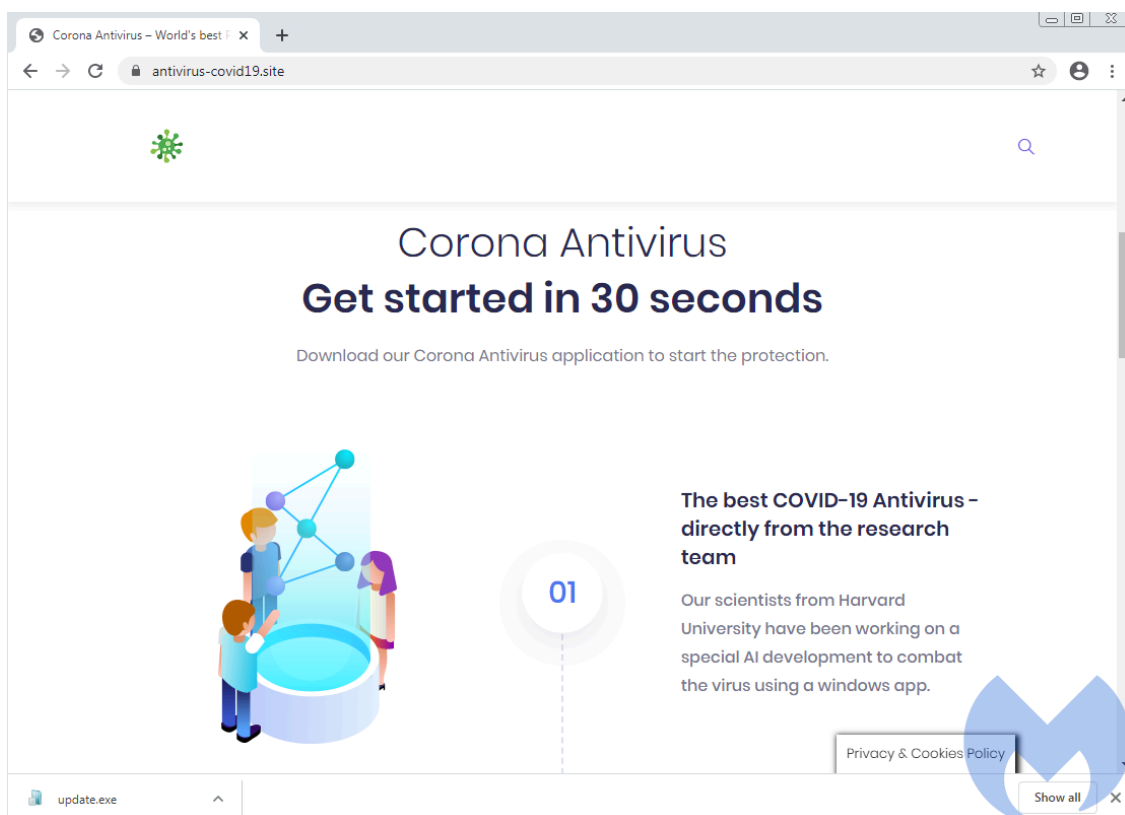
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

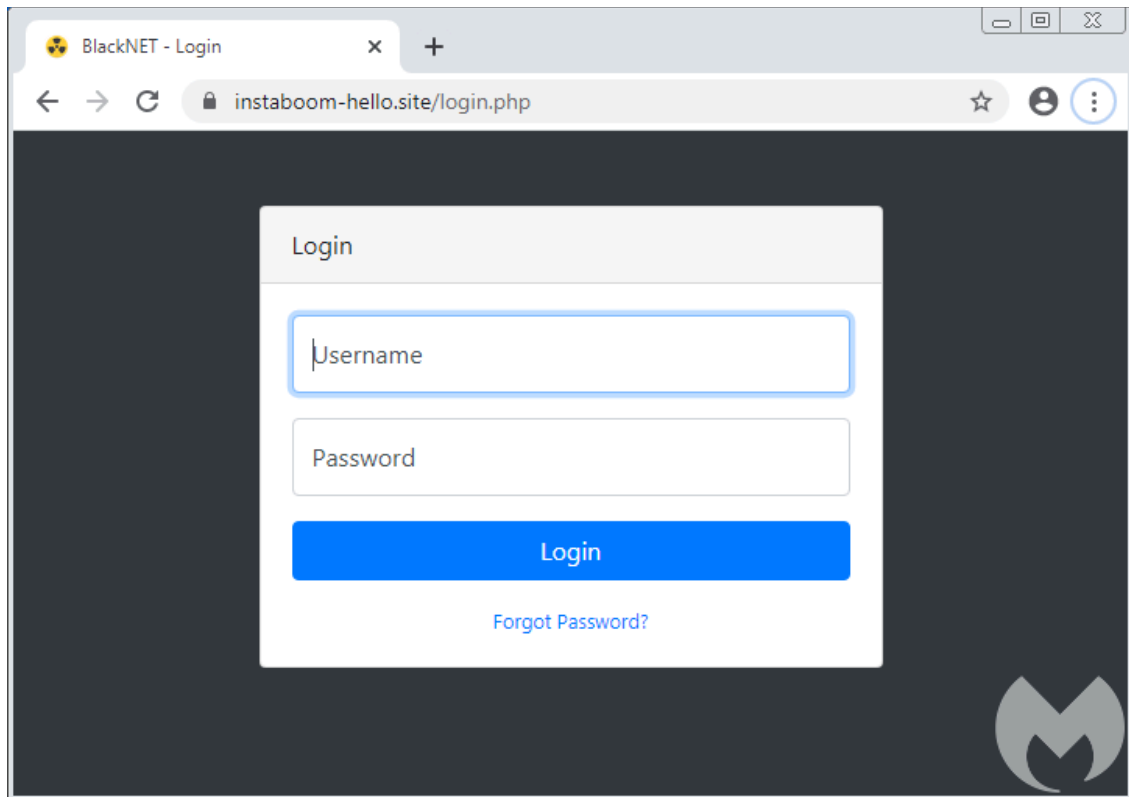


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

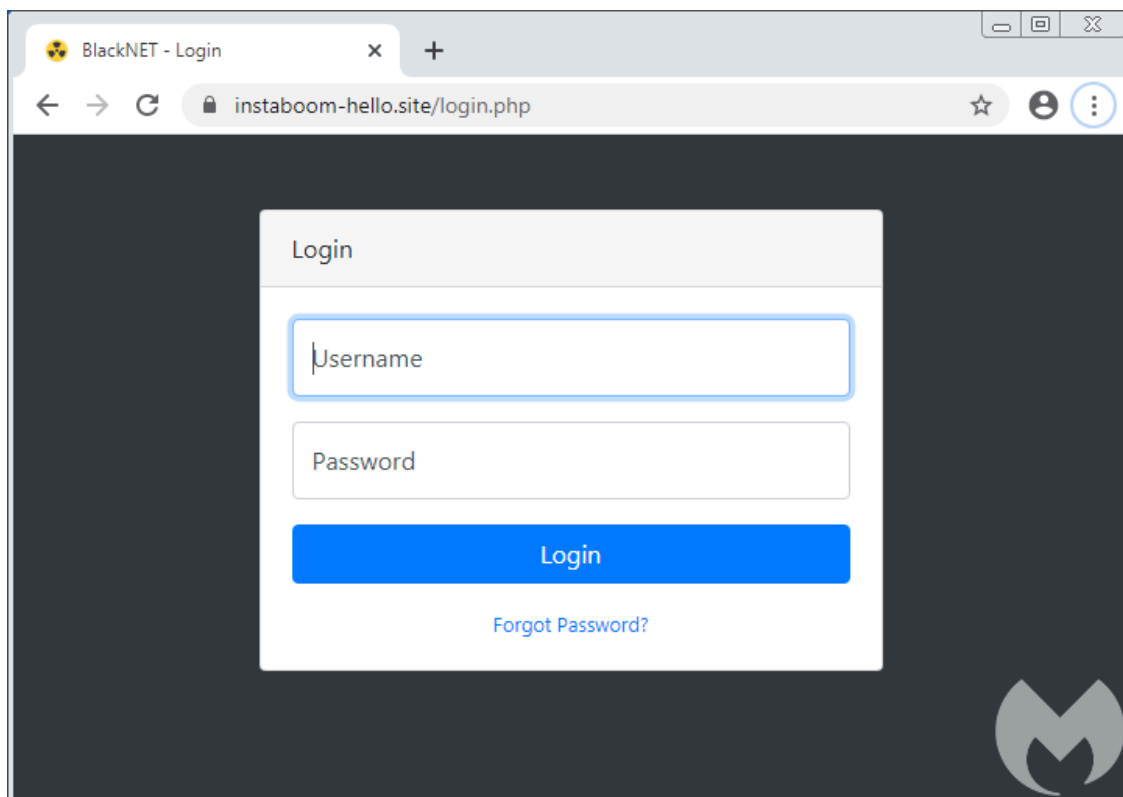
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

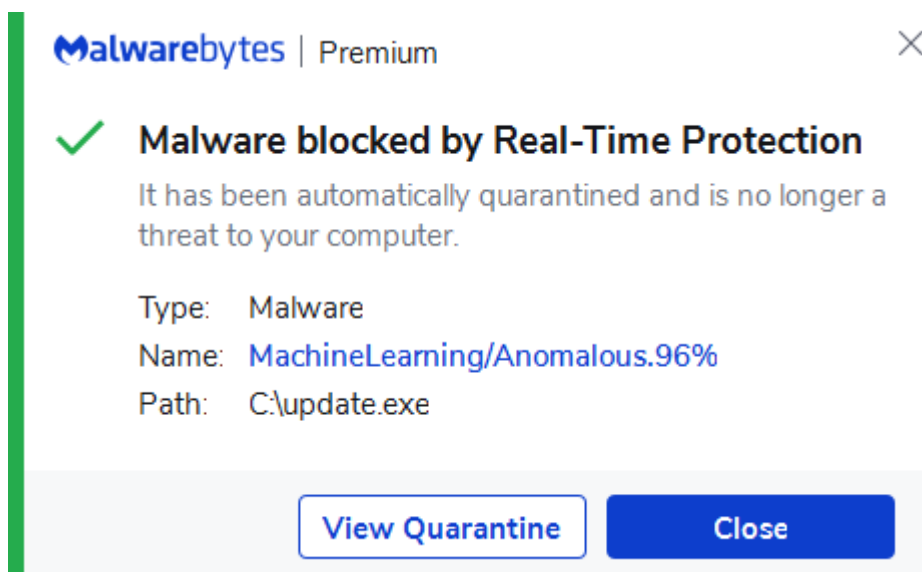
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' navigation buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

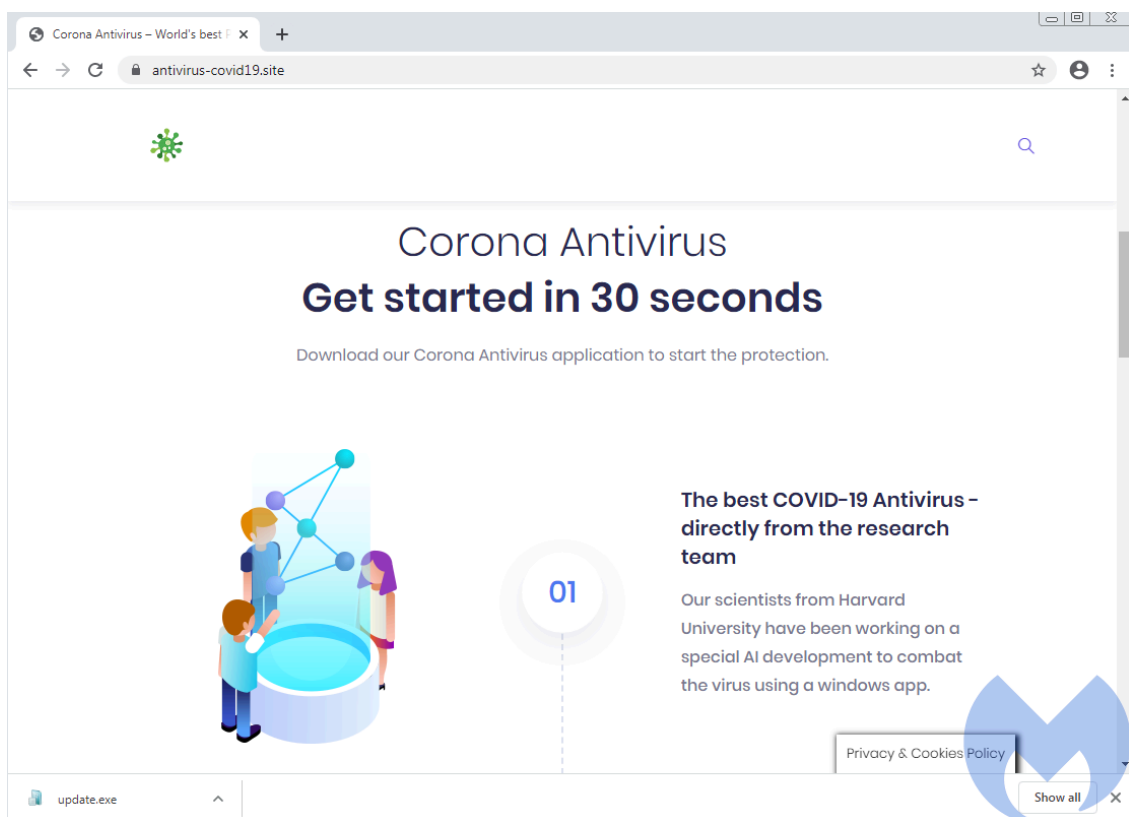
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

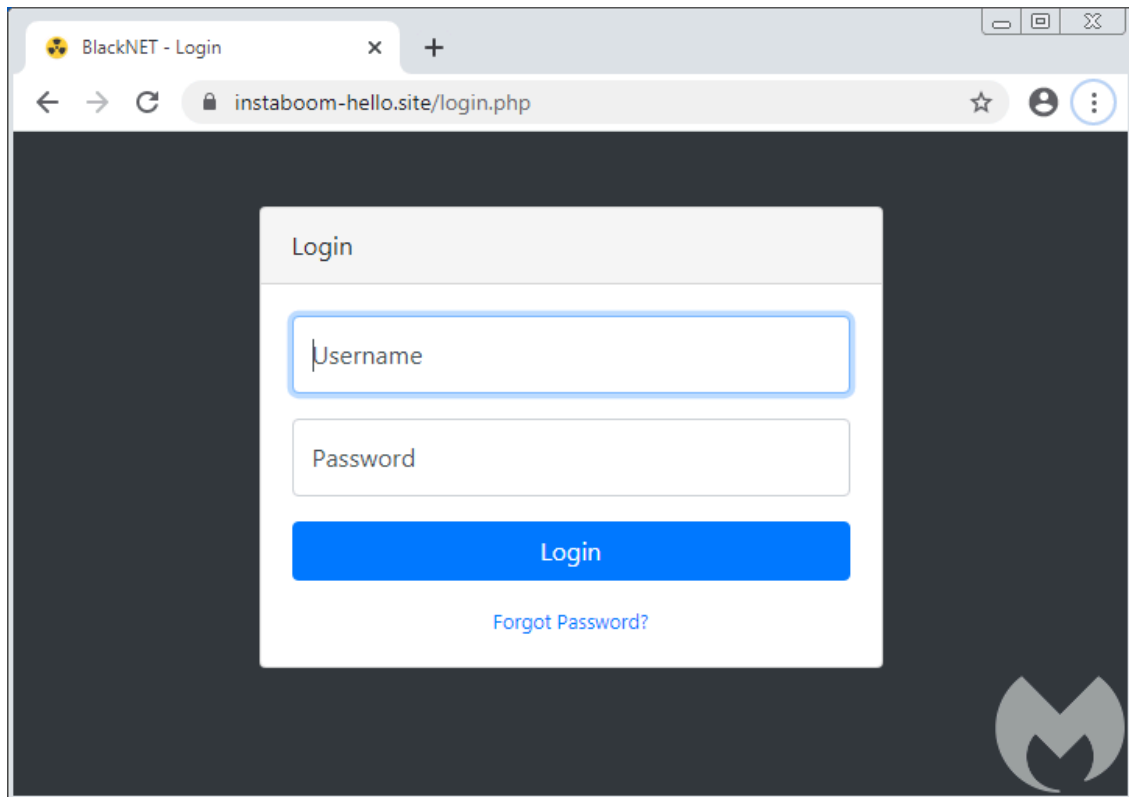


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

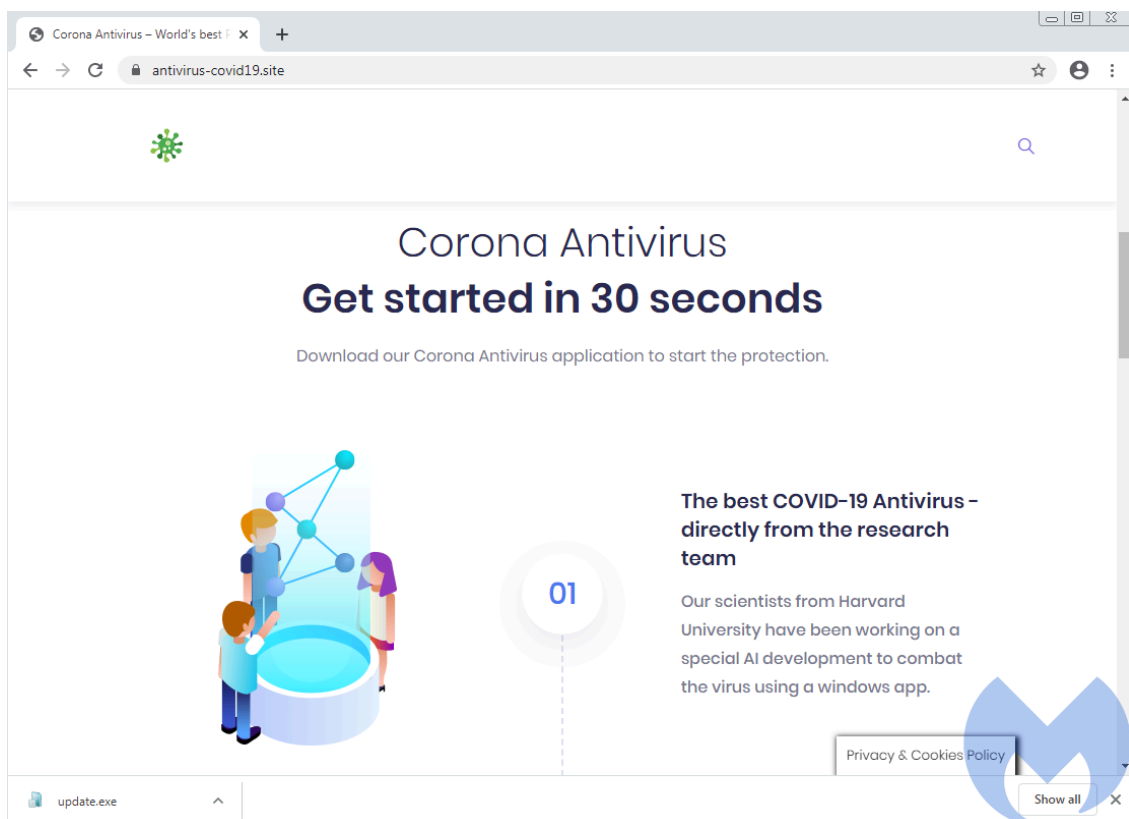
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

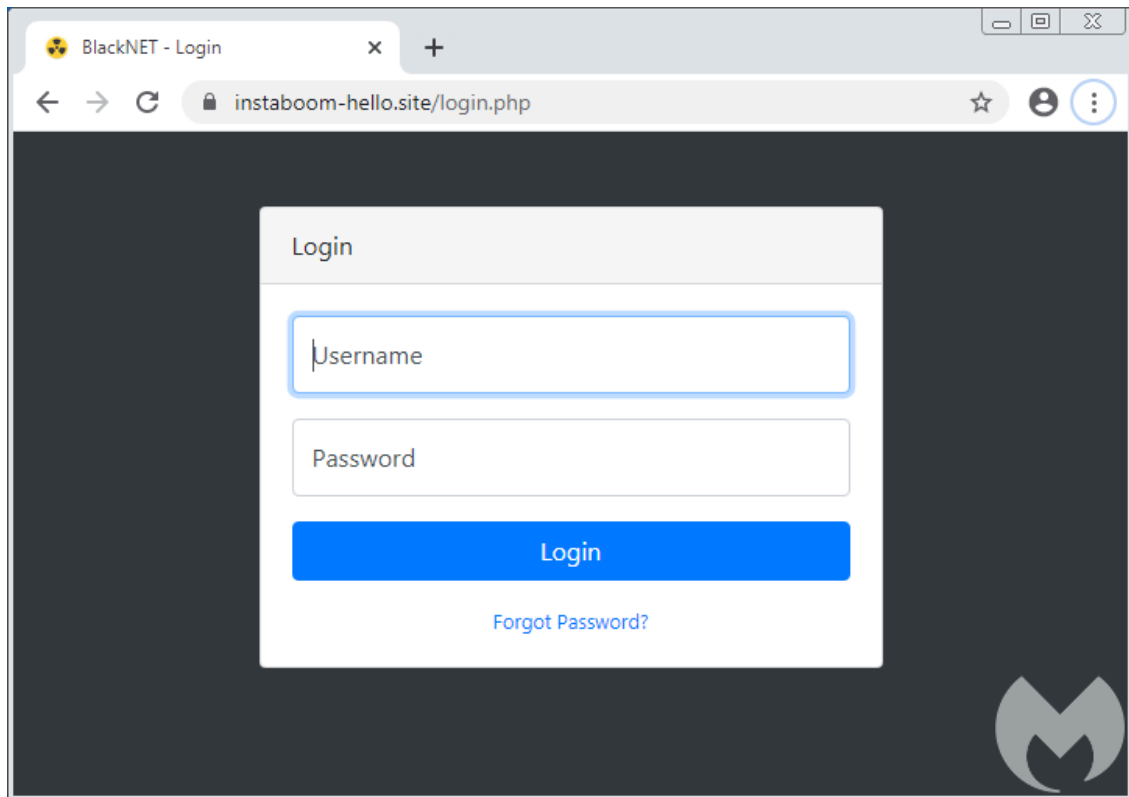


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

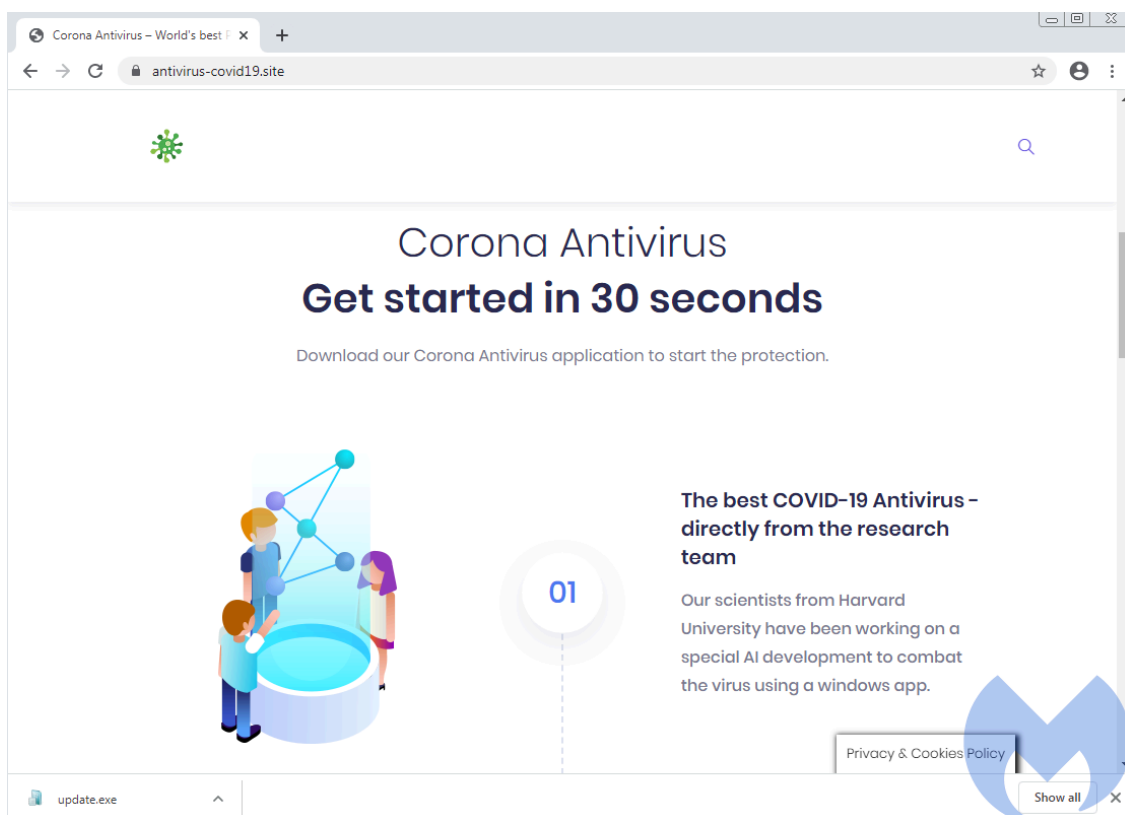
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, the details are listed: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

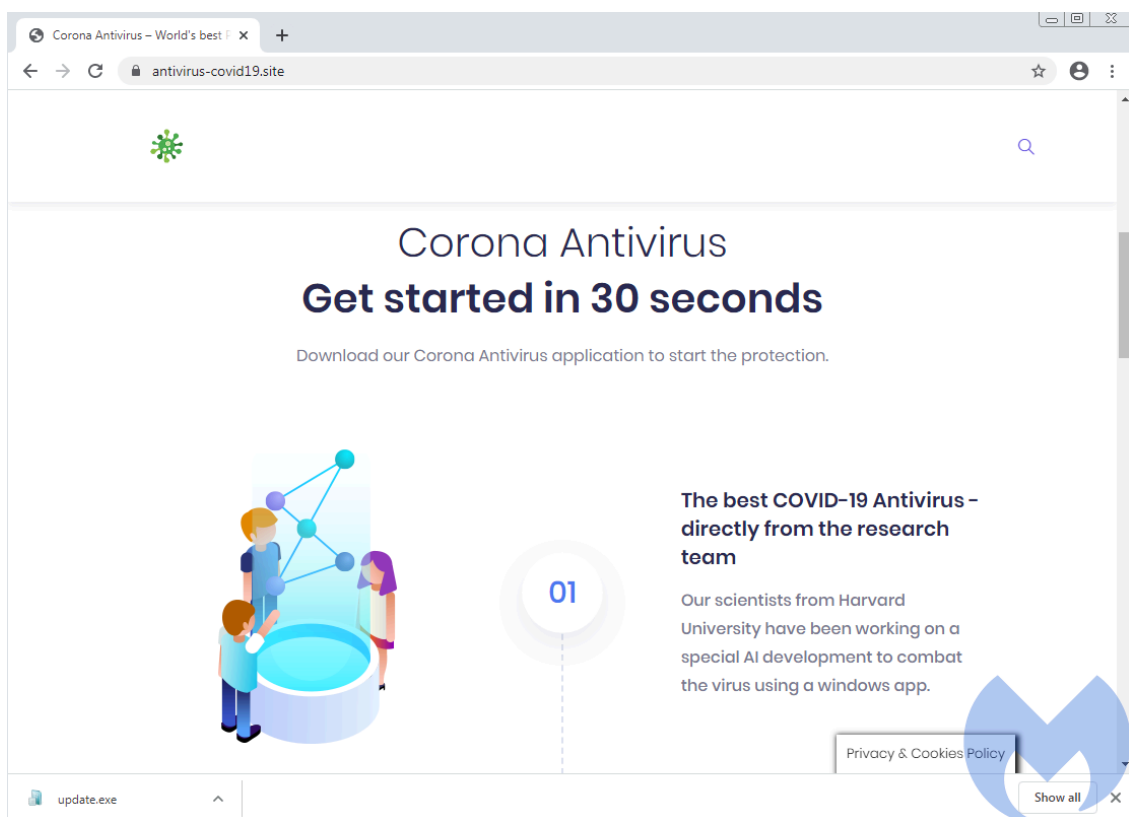
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

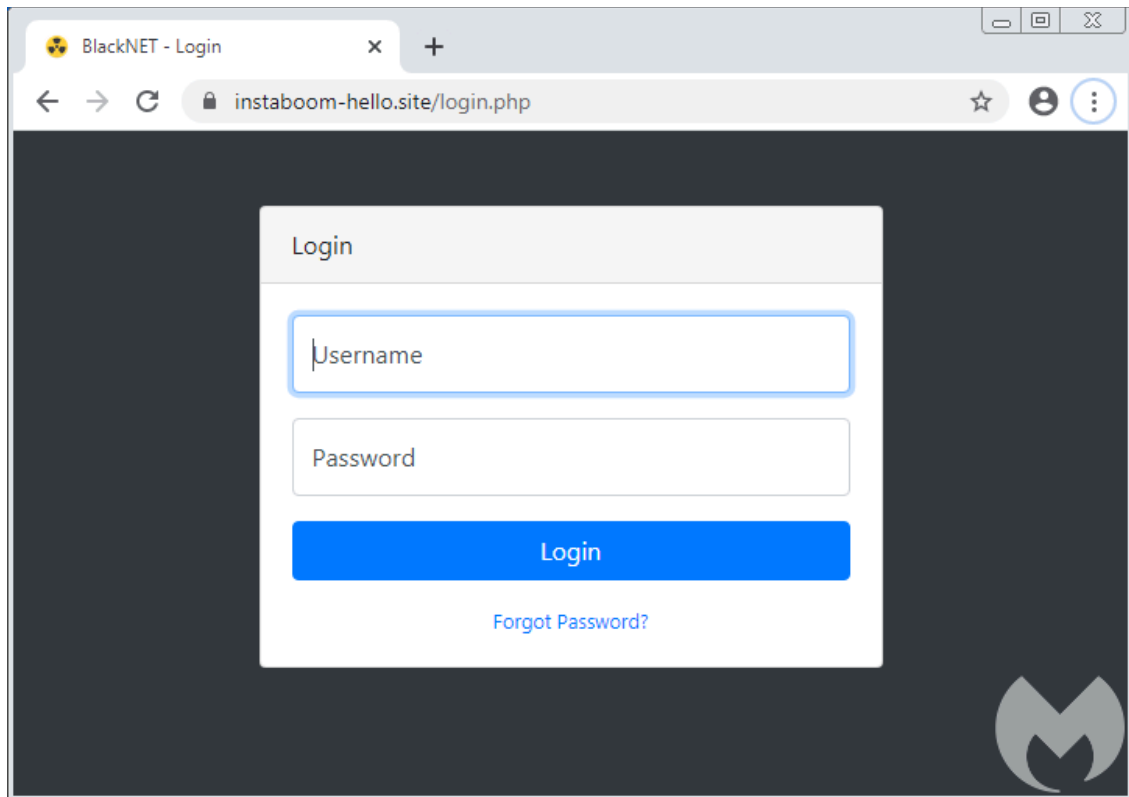


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

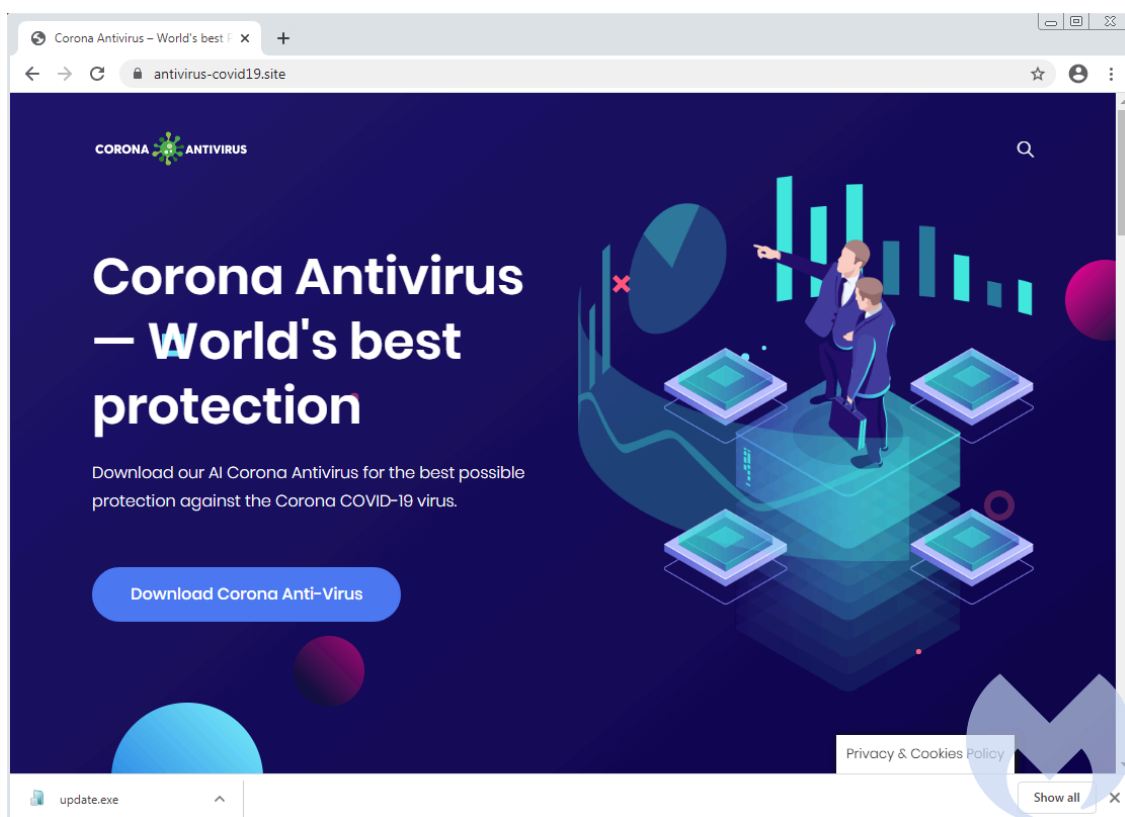
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

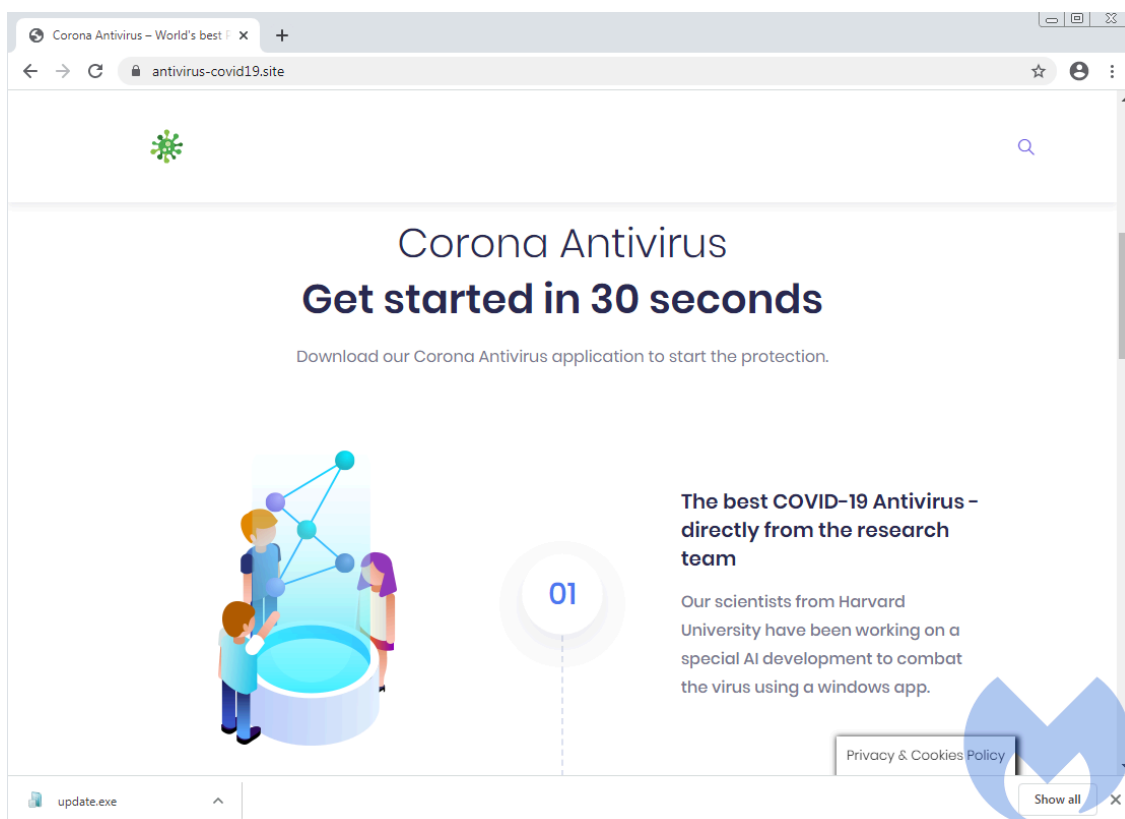
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

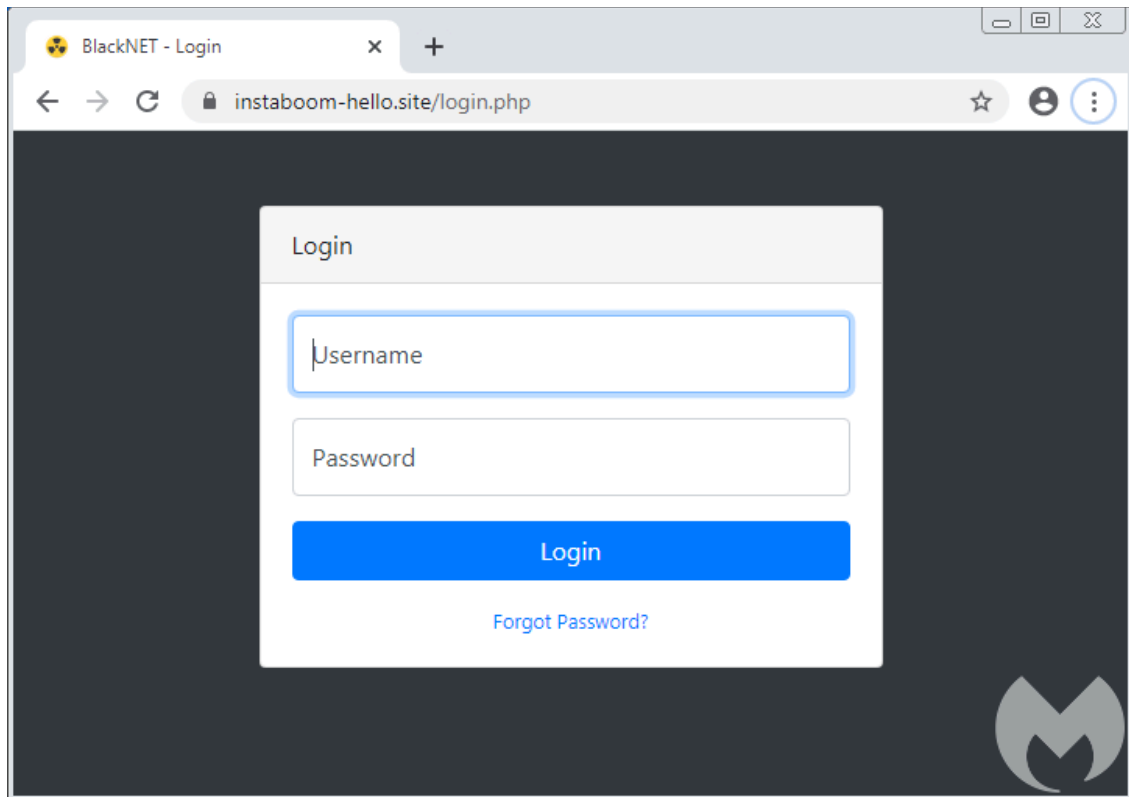


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

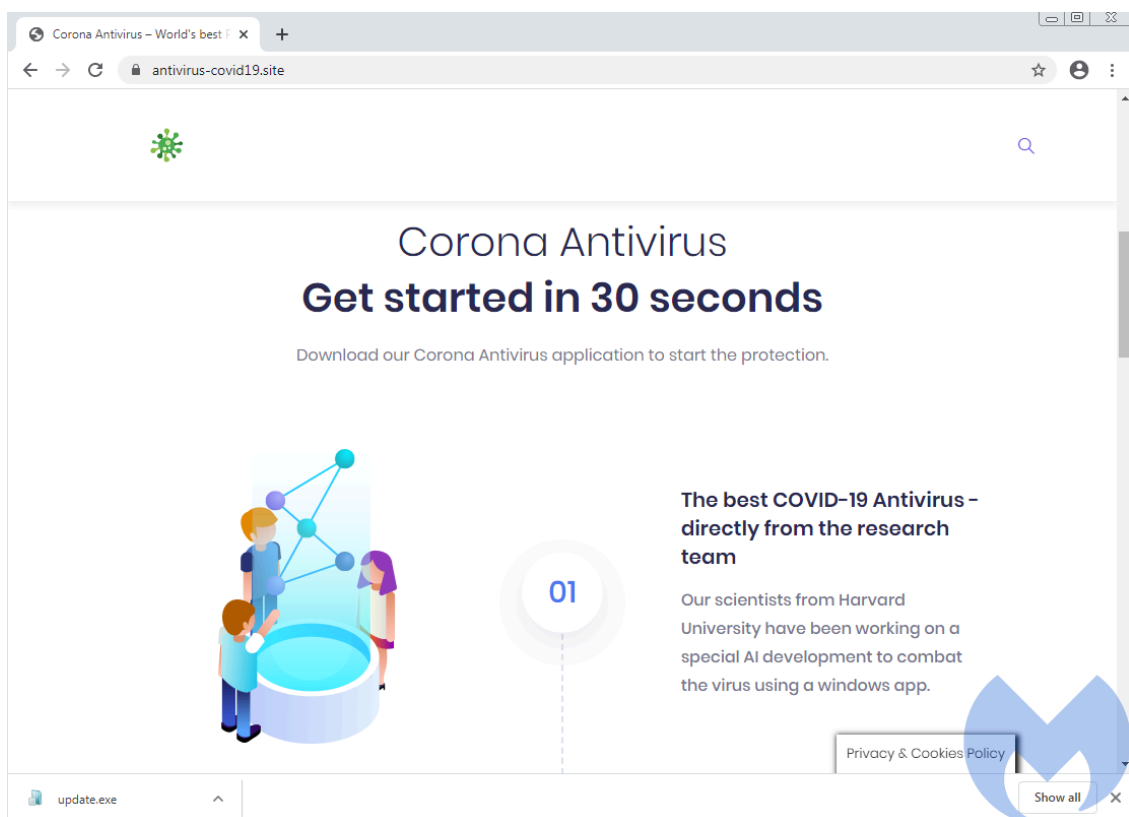
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

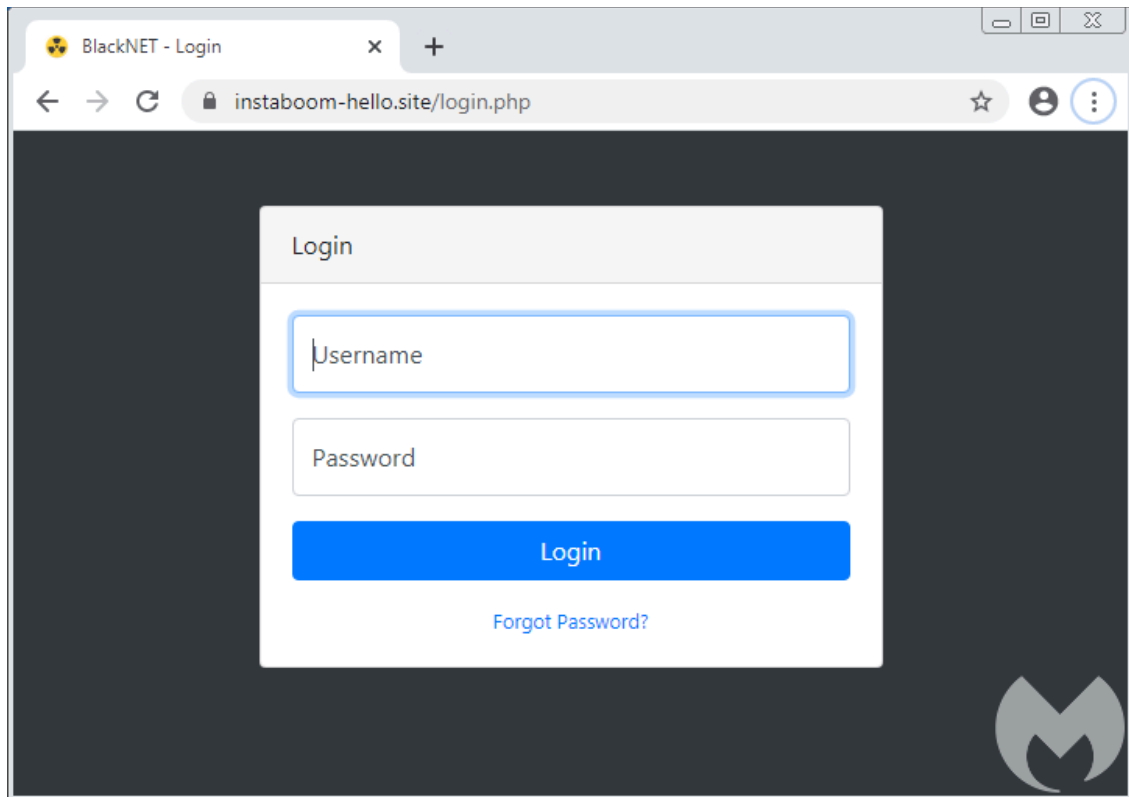


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

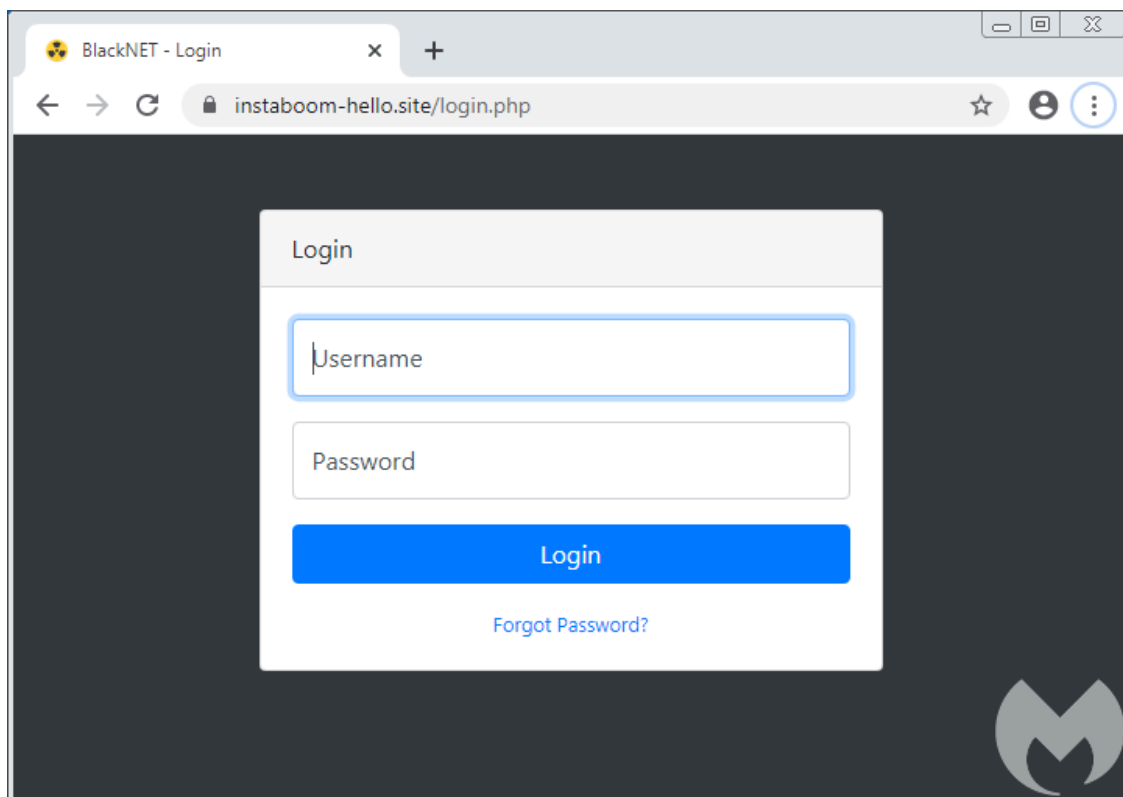
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

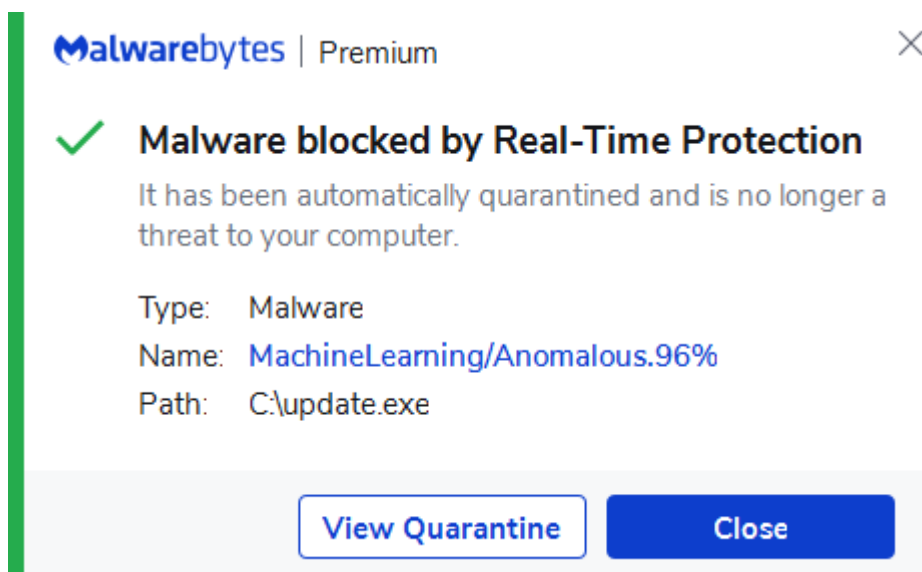
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, displaying 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

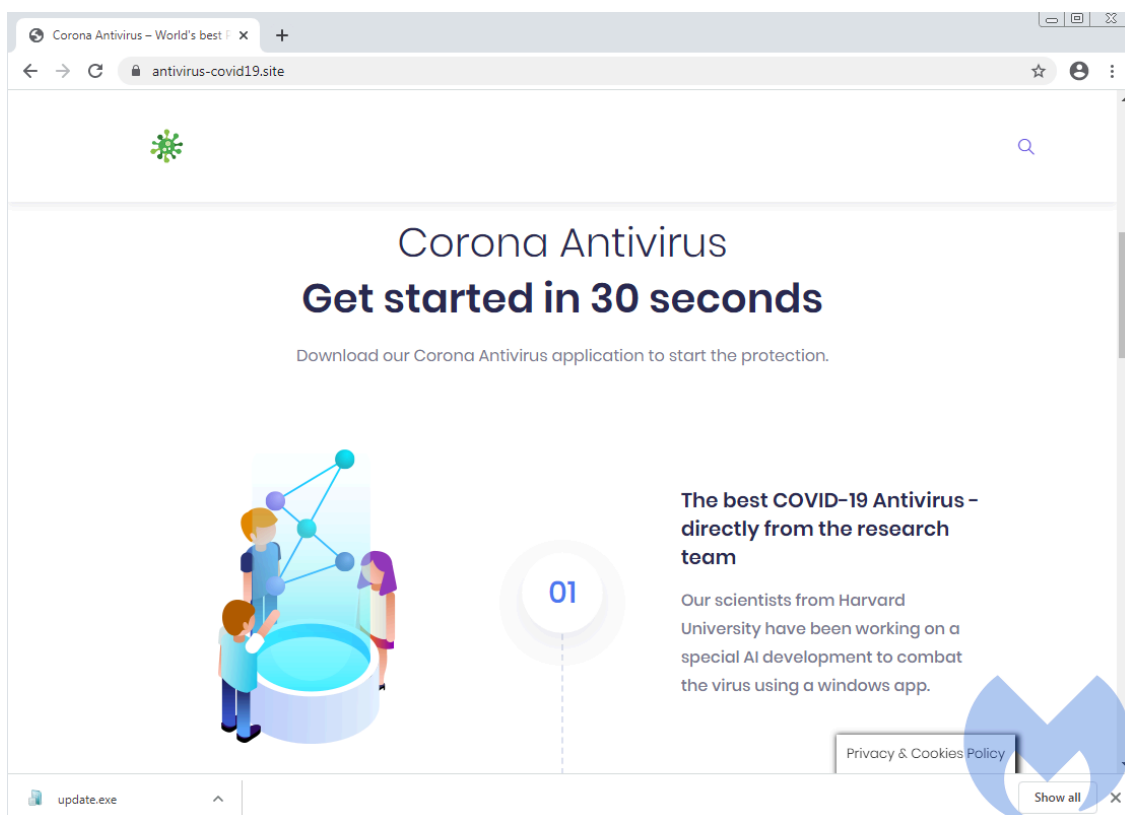
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

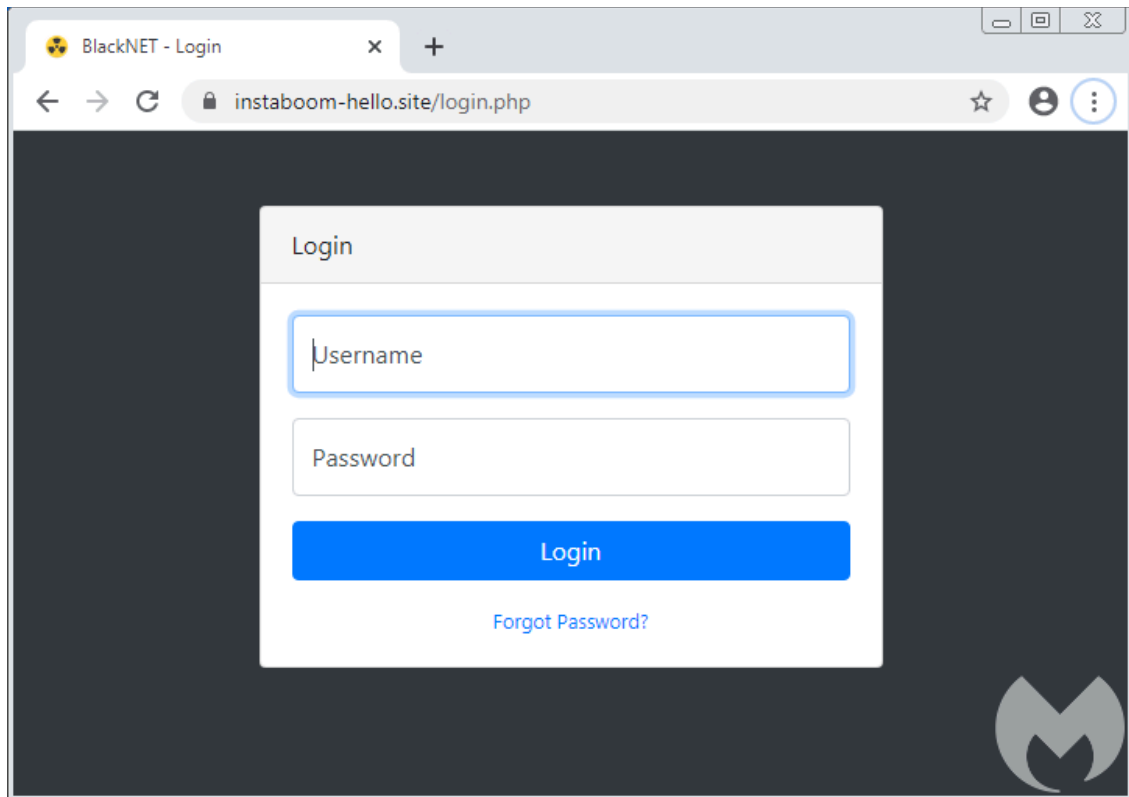


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features a green checkmark icon and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

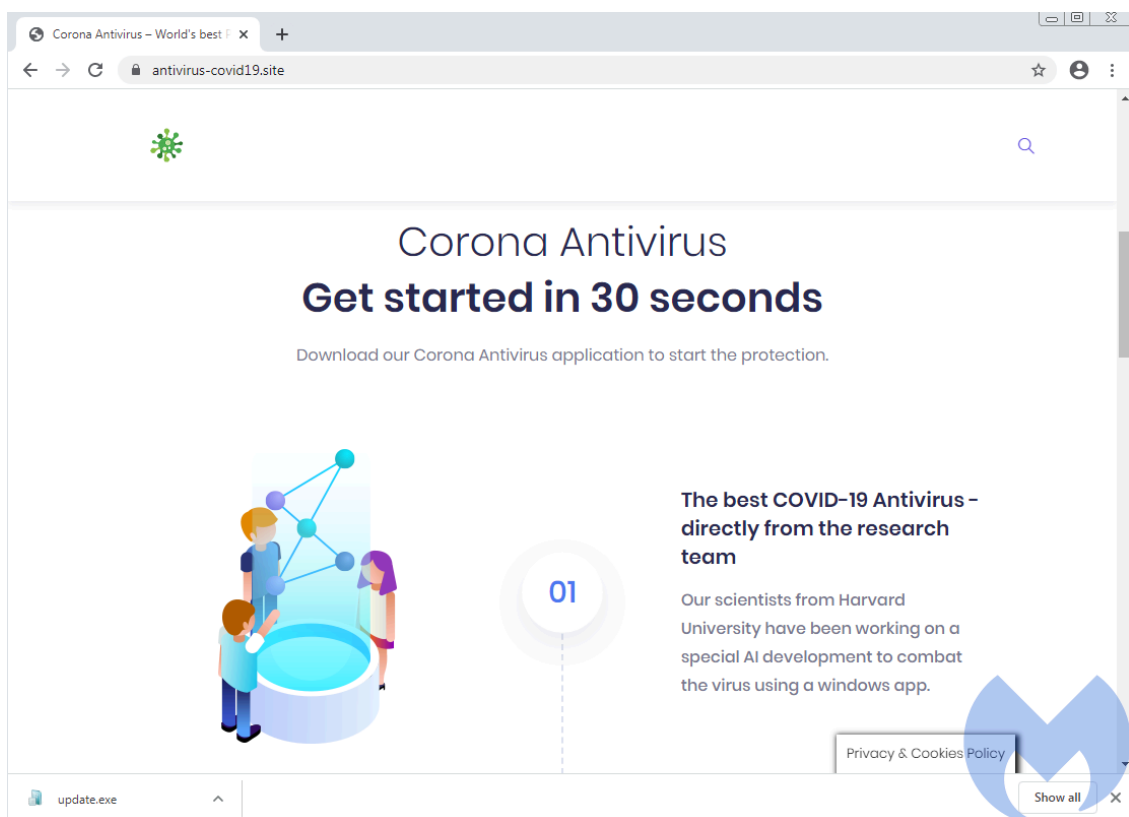
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

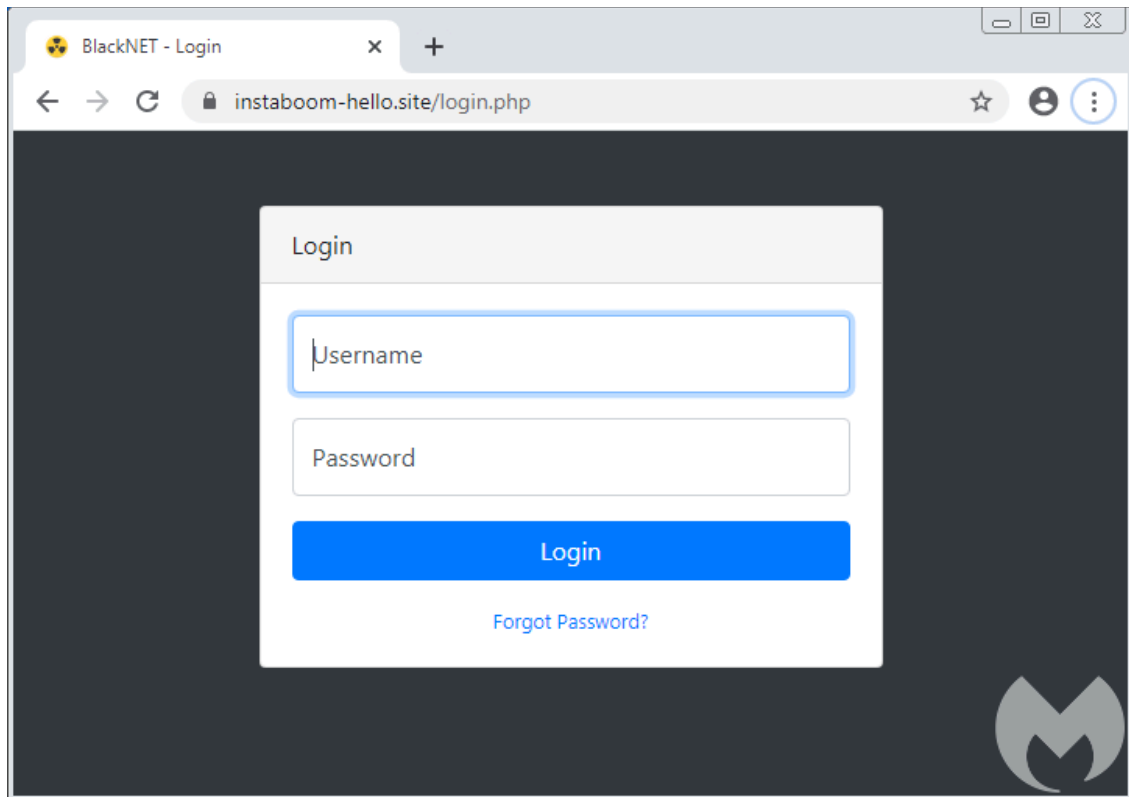


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

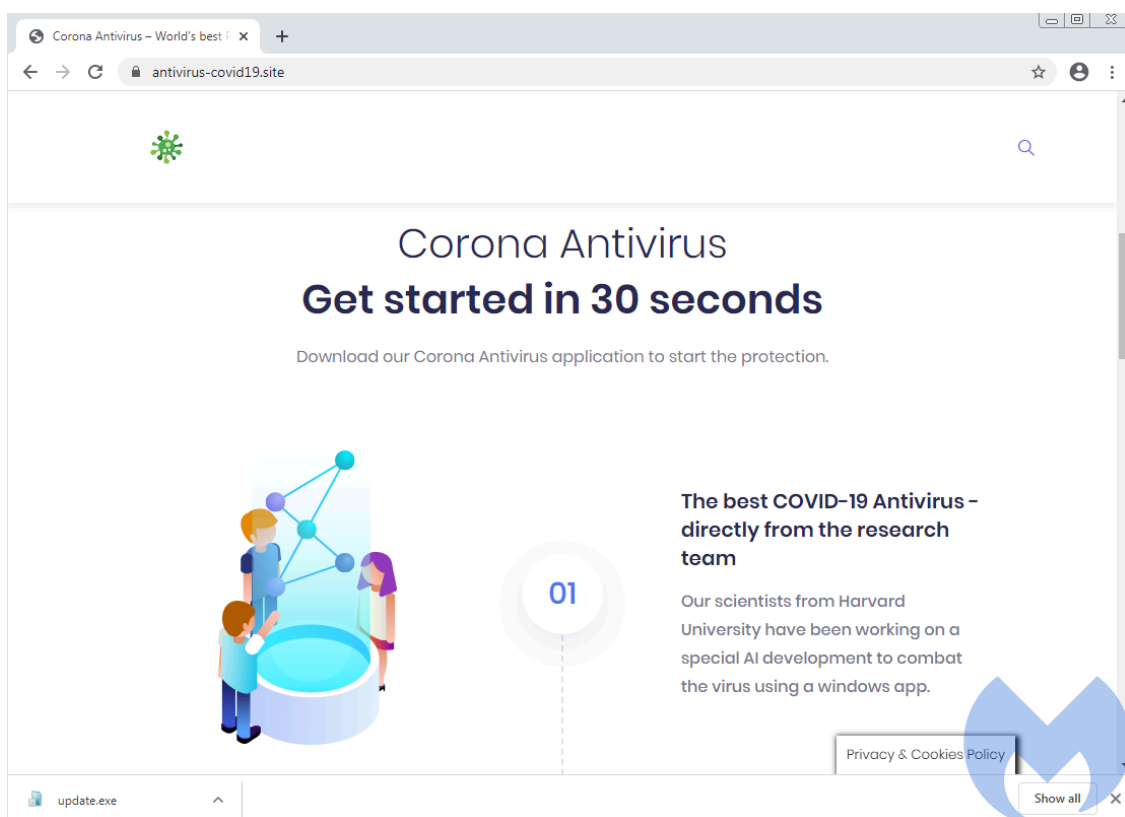
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

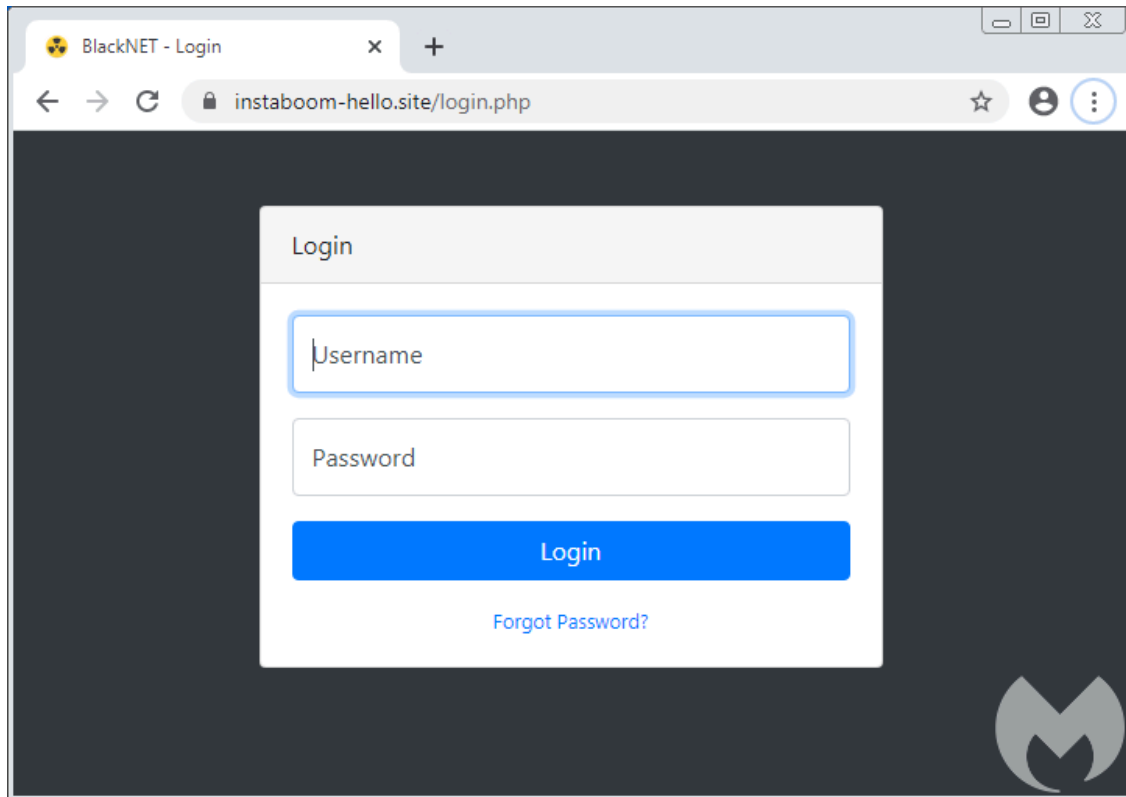


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored tiles: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

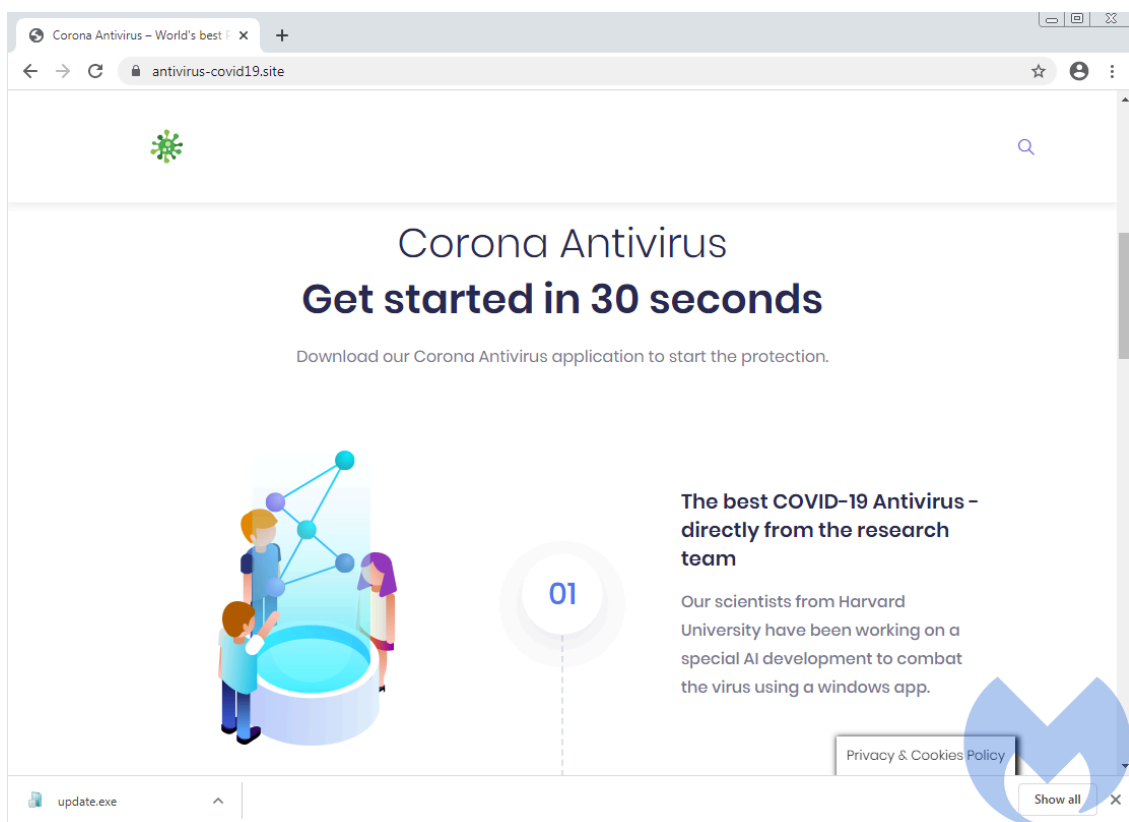
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

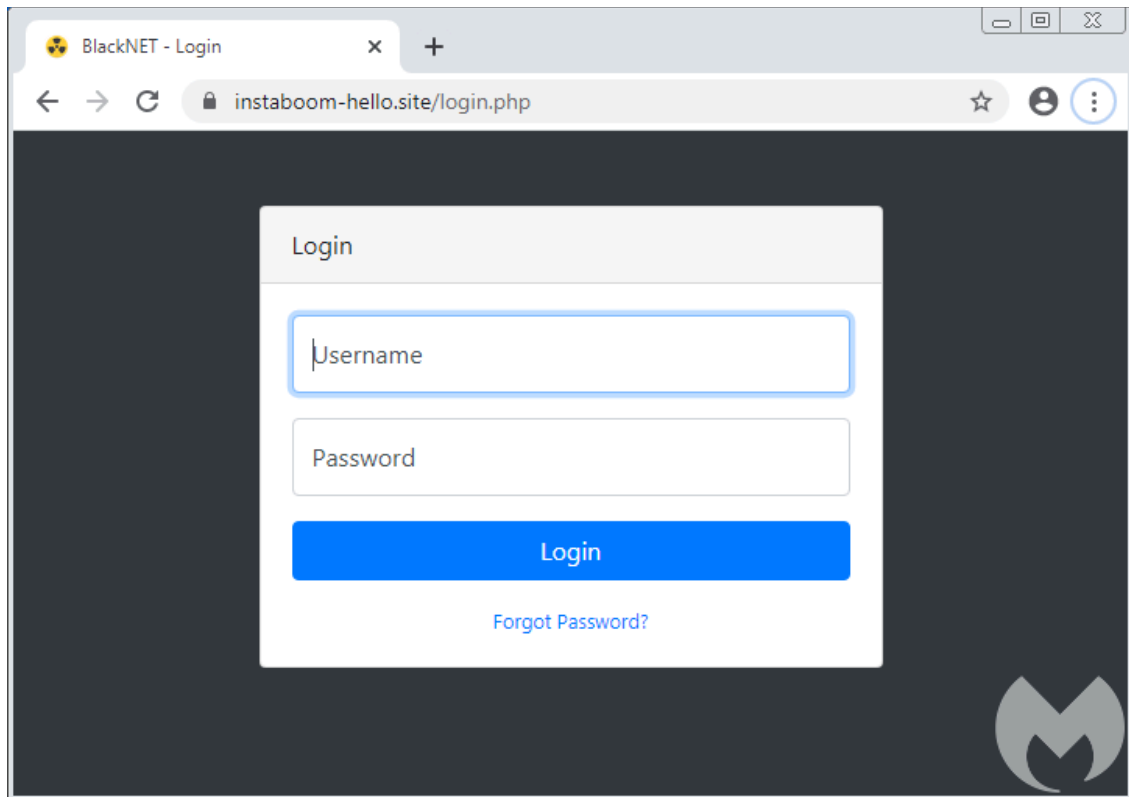


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

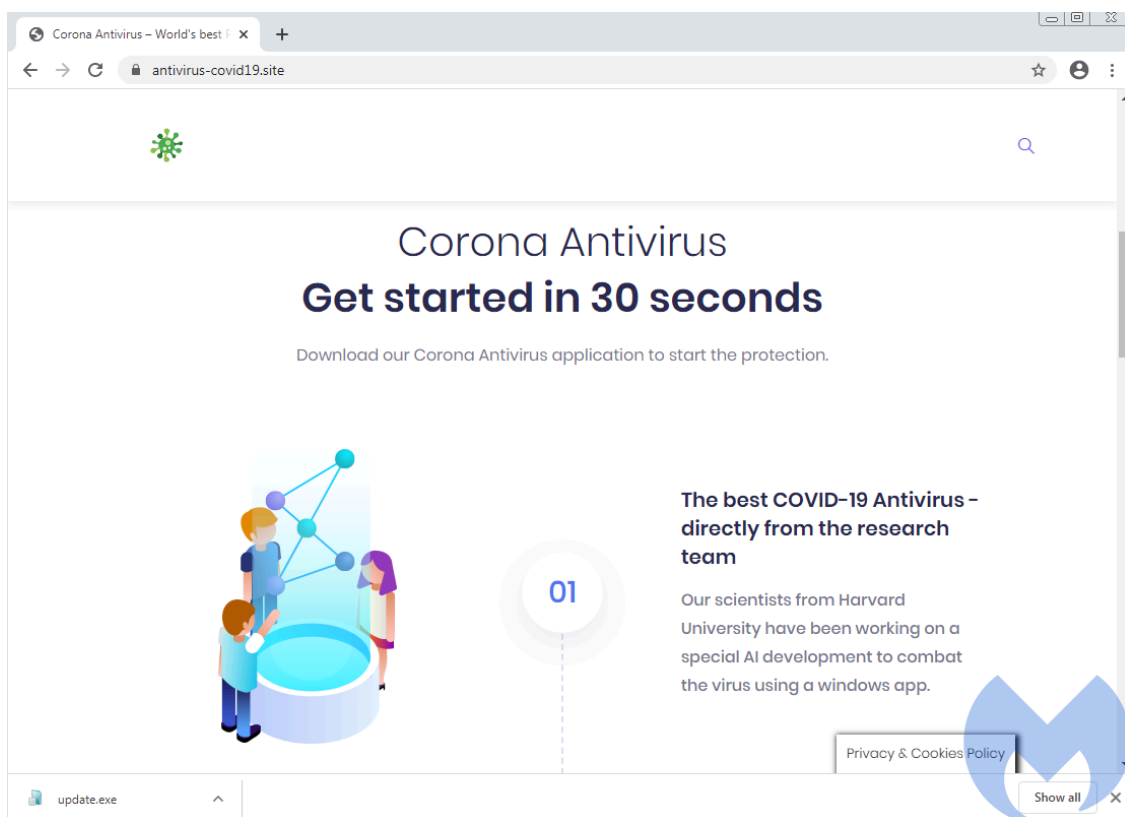
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

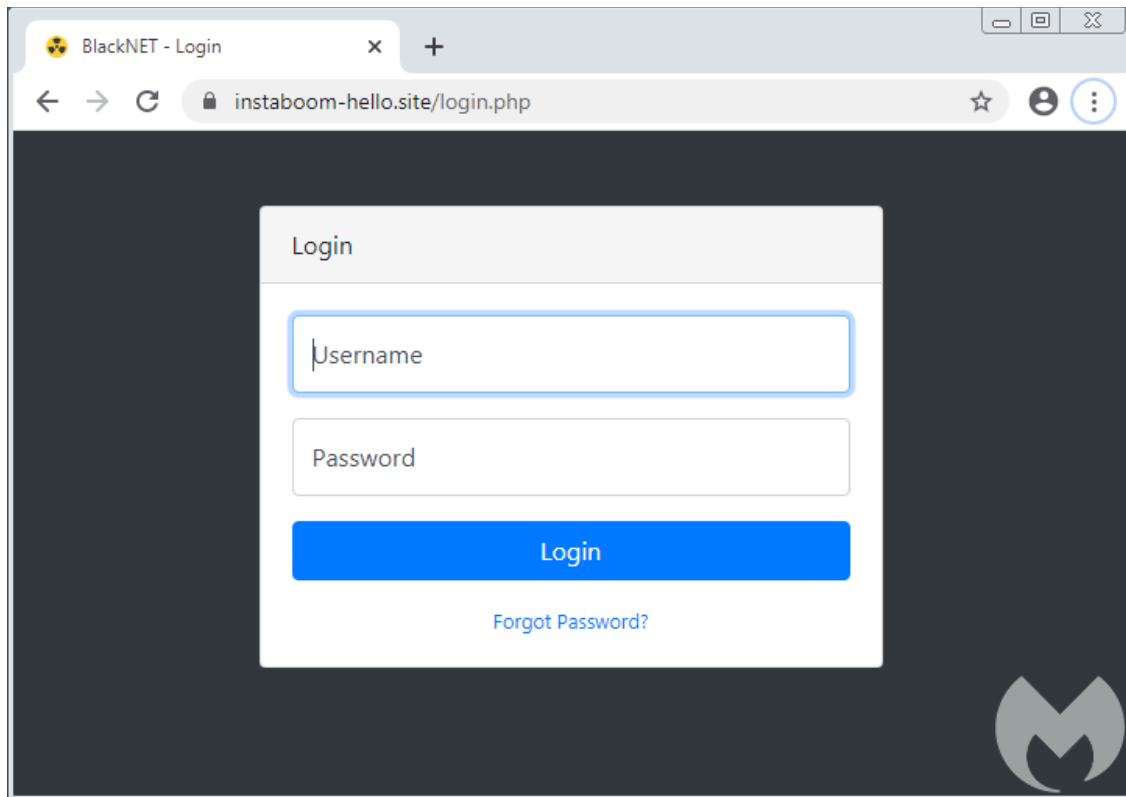


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

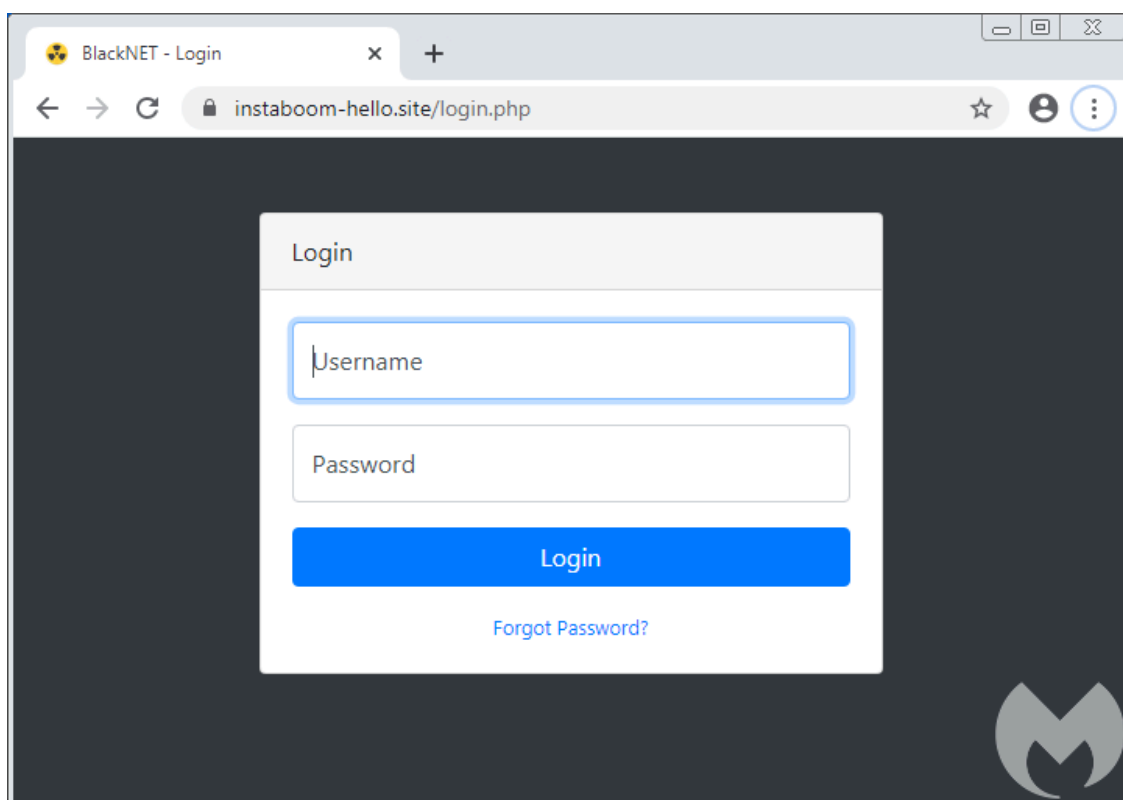
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

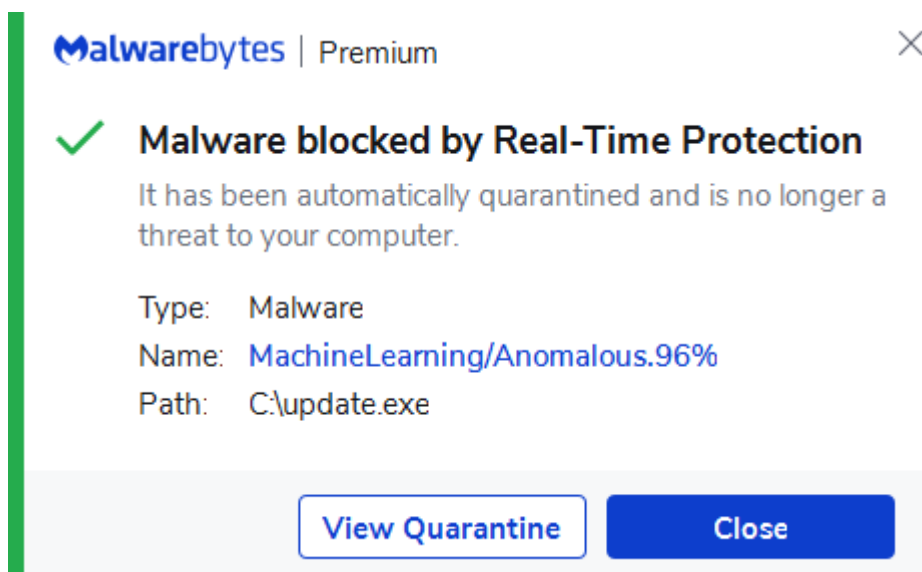
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

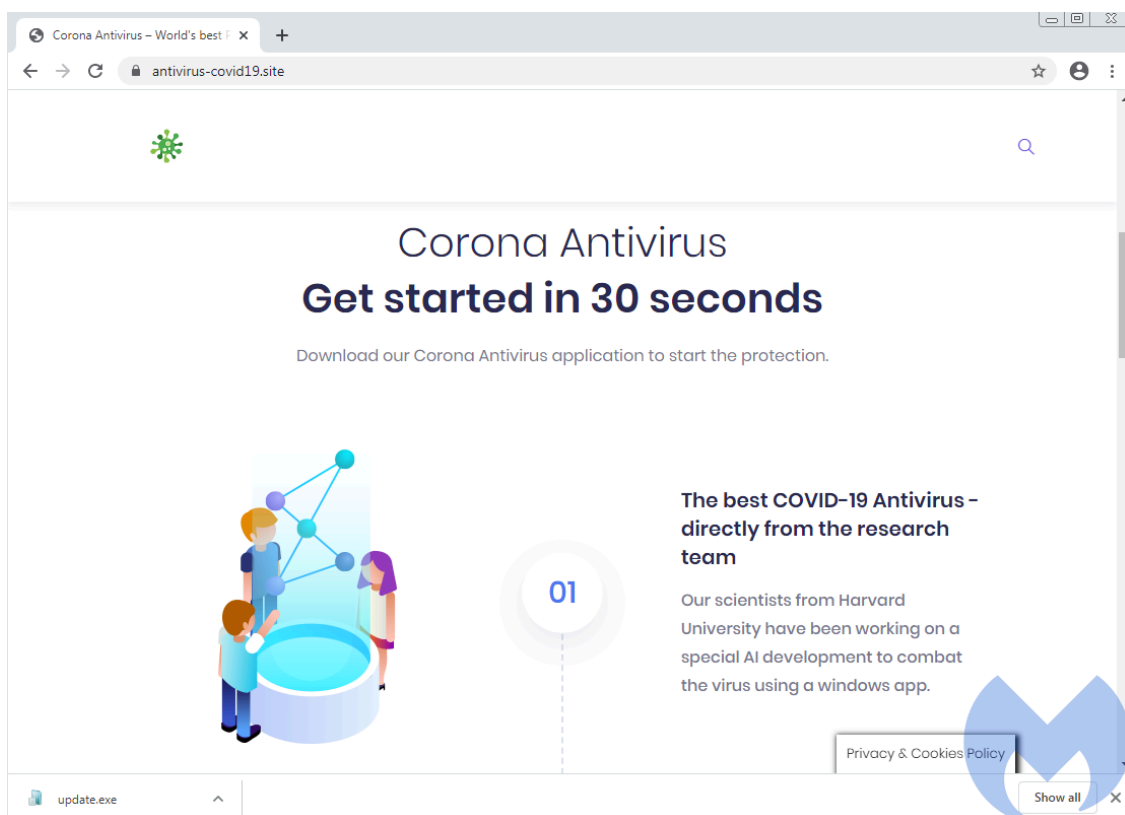
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

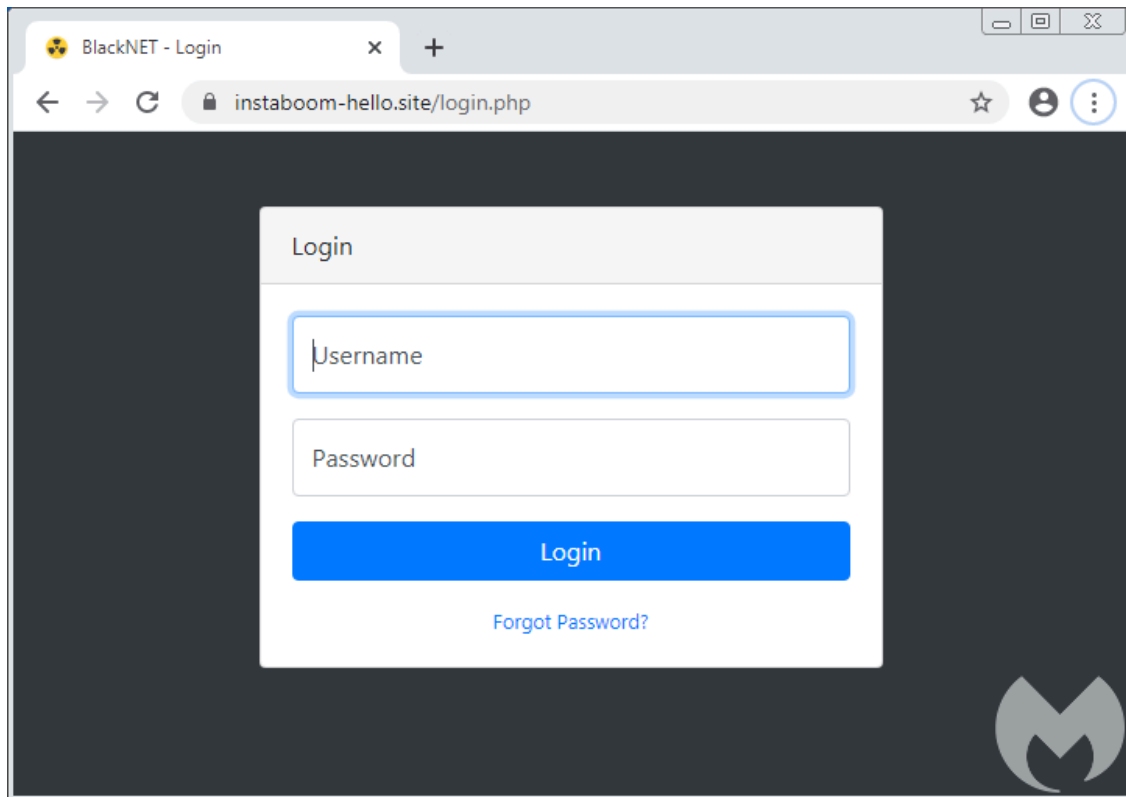


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

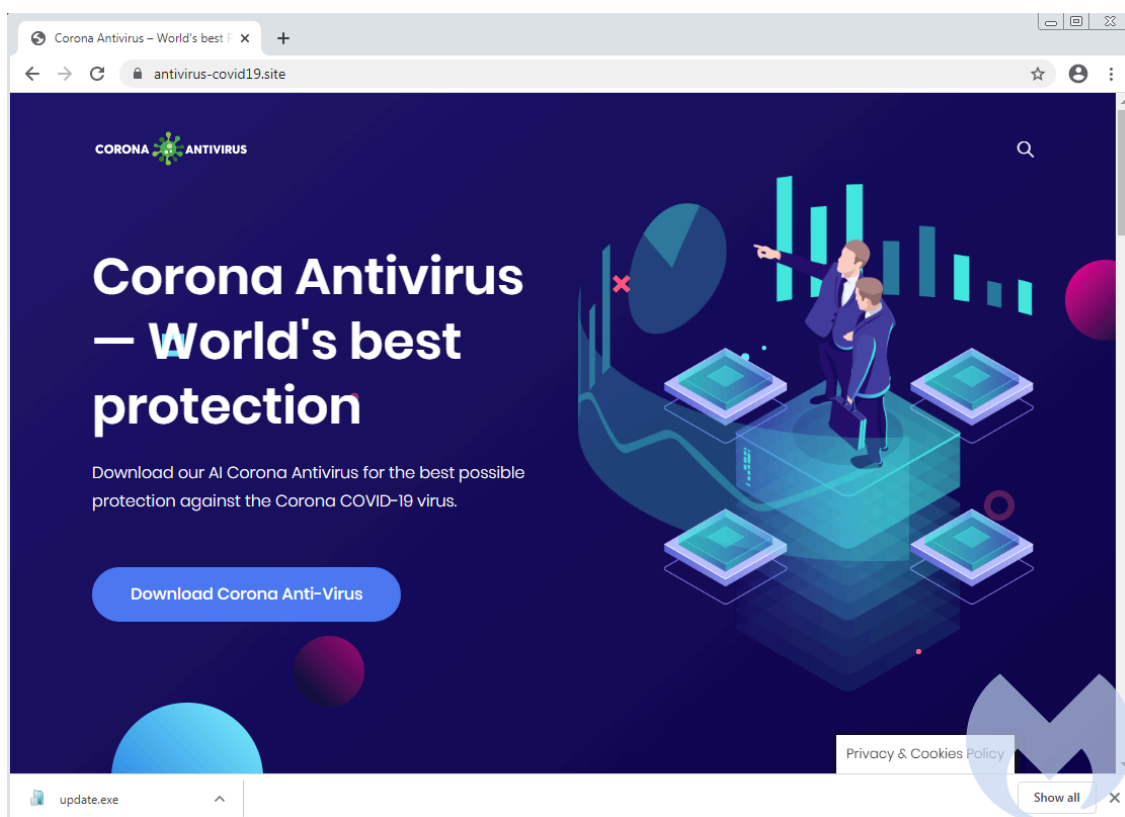
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

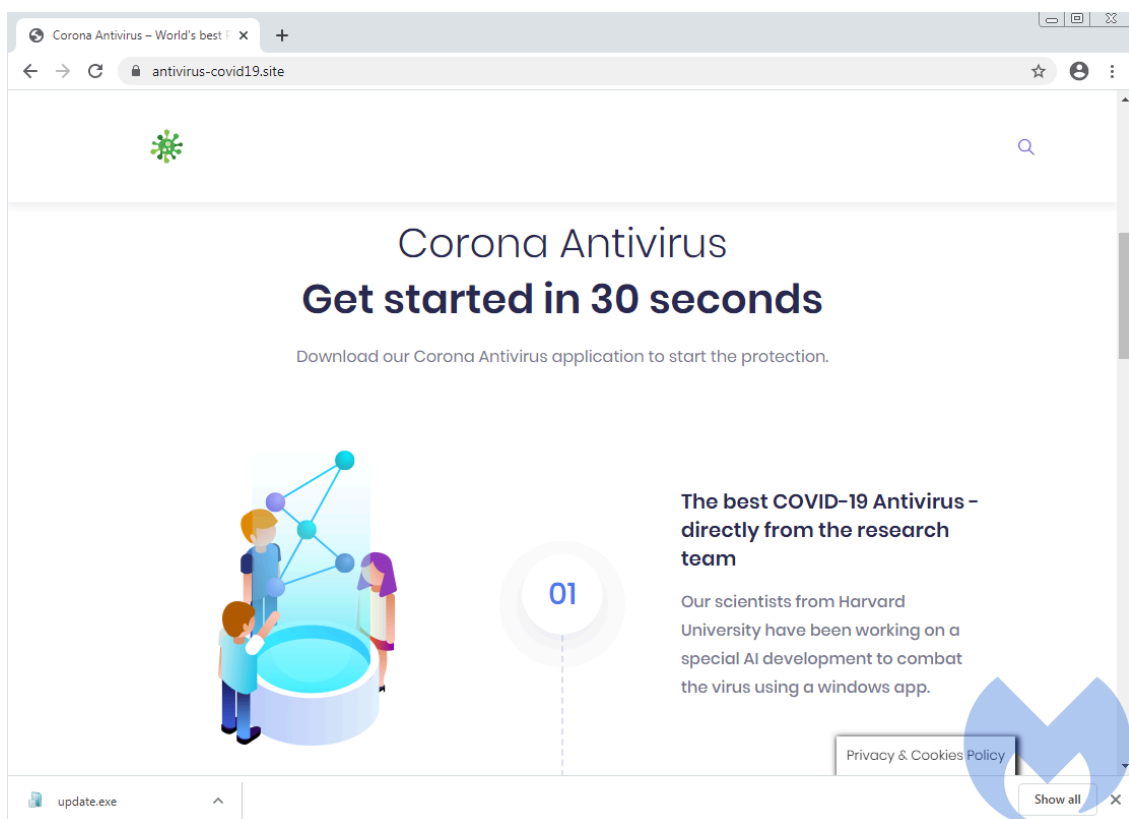
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

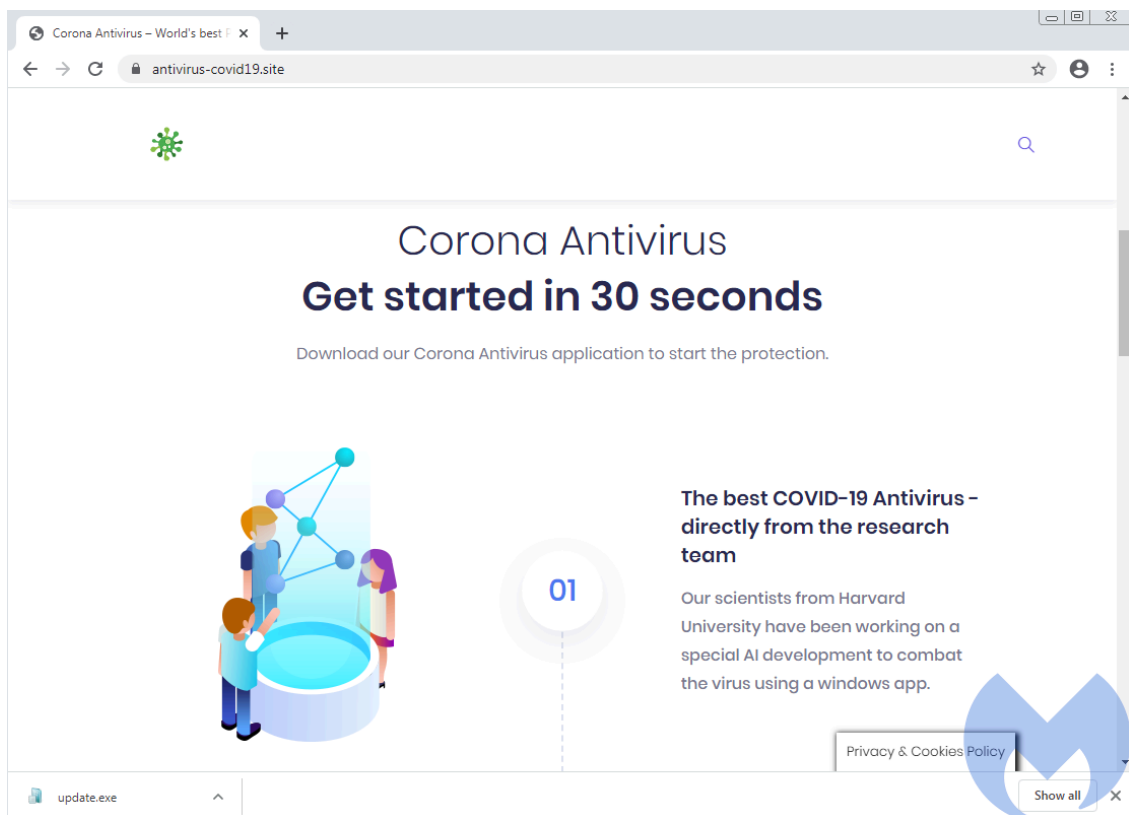
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

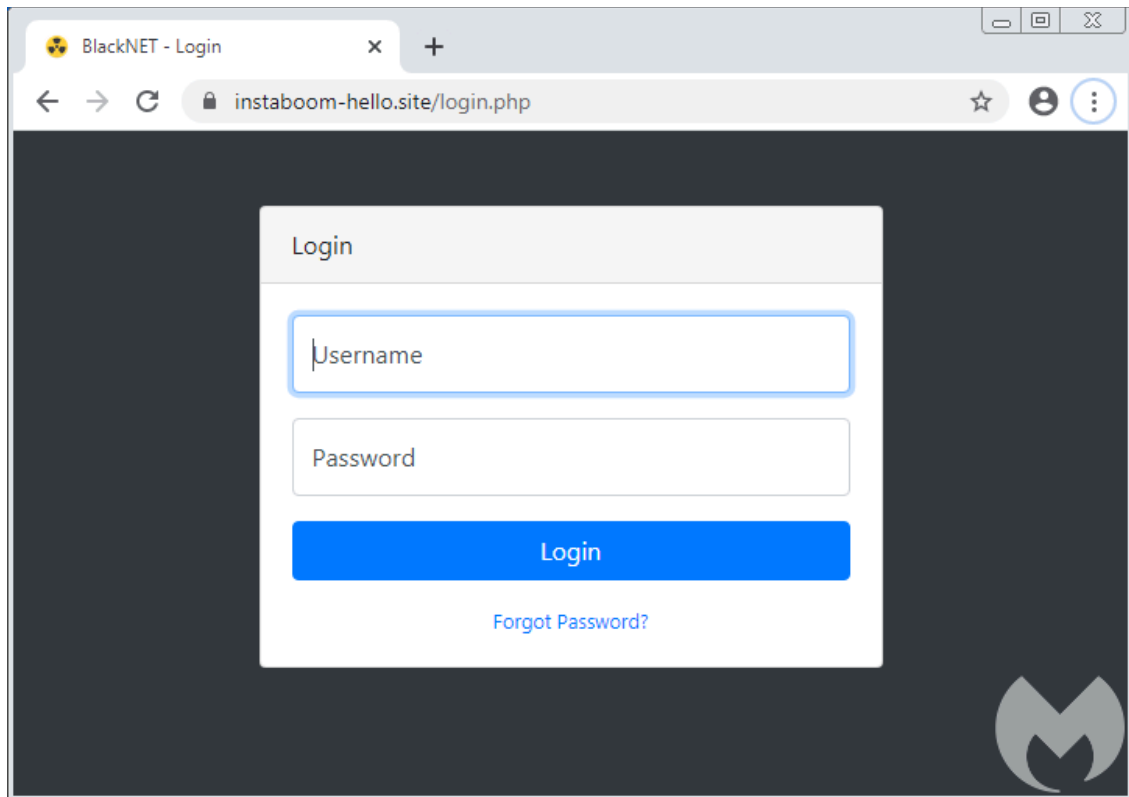


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

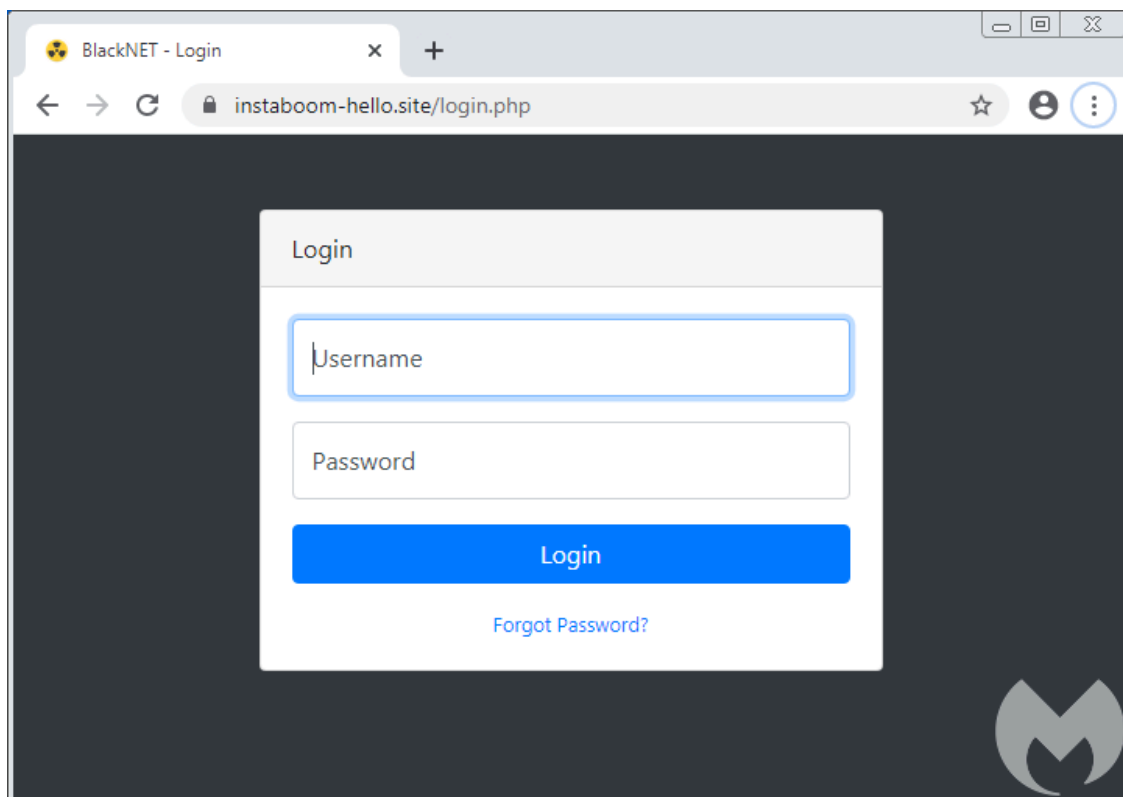
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

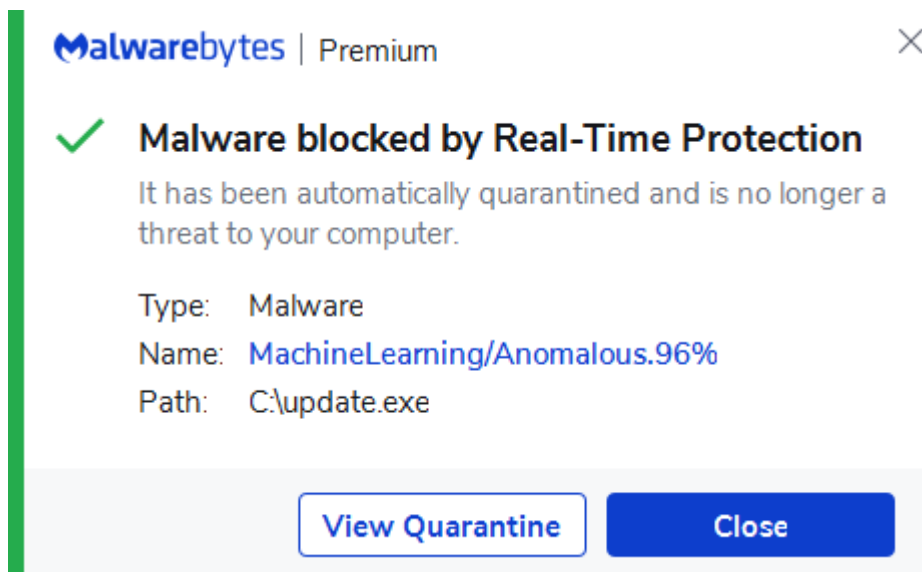
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

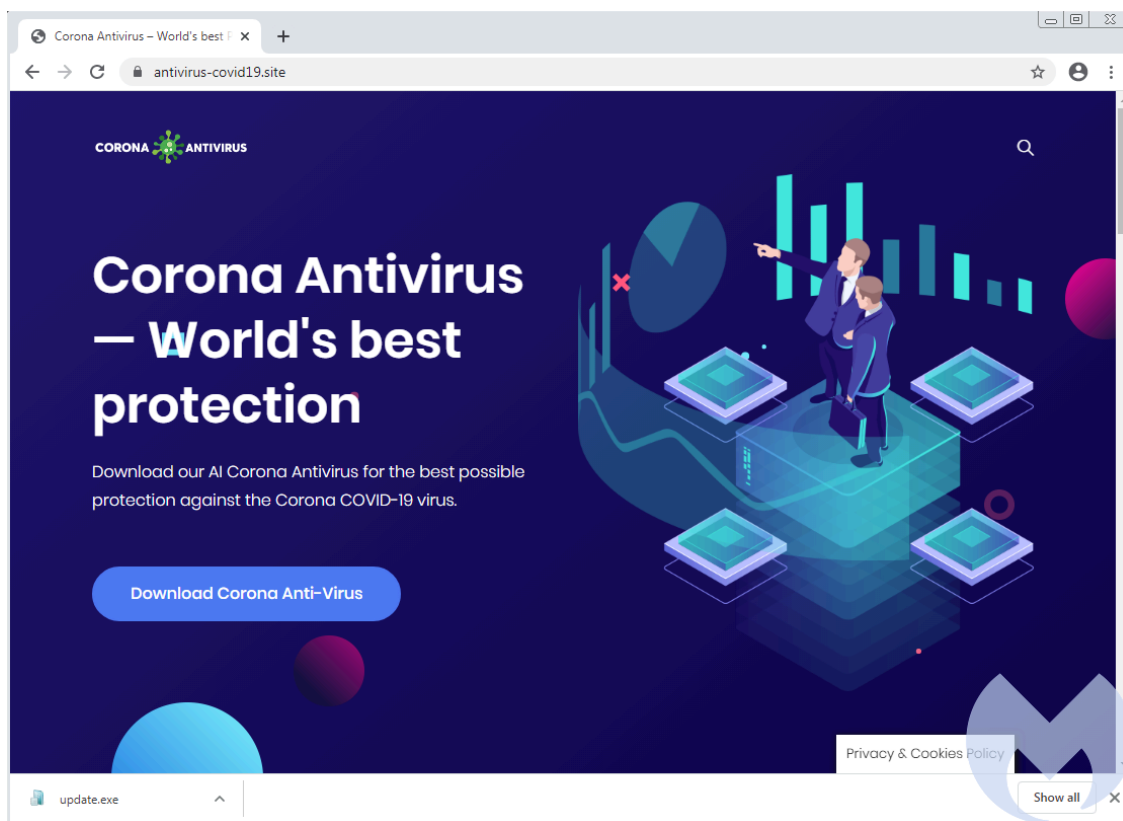
```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

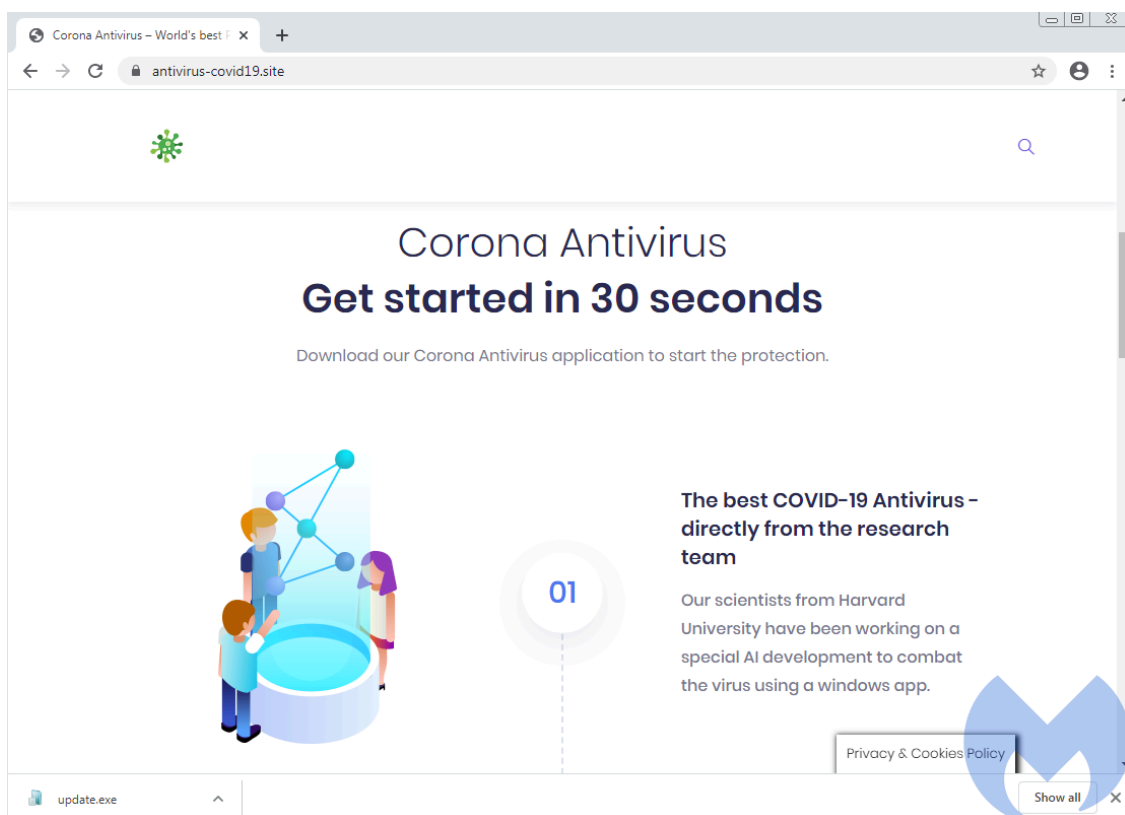
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

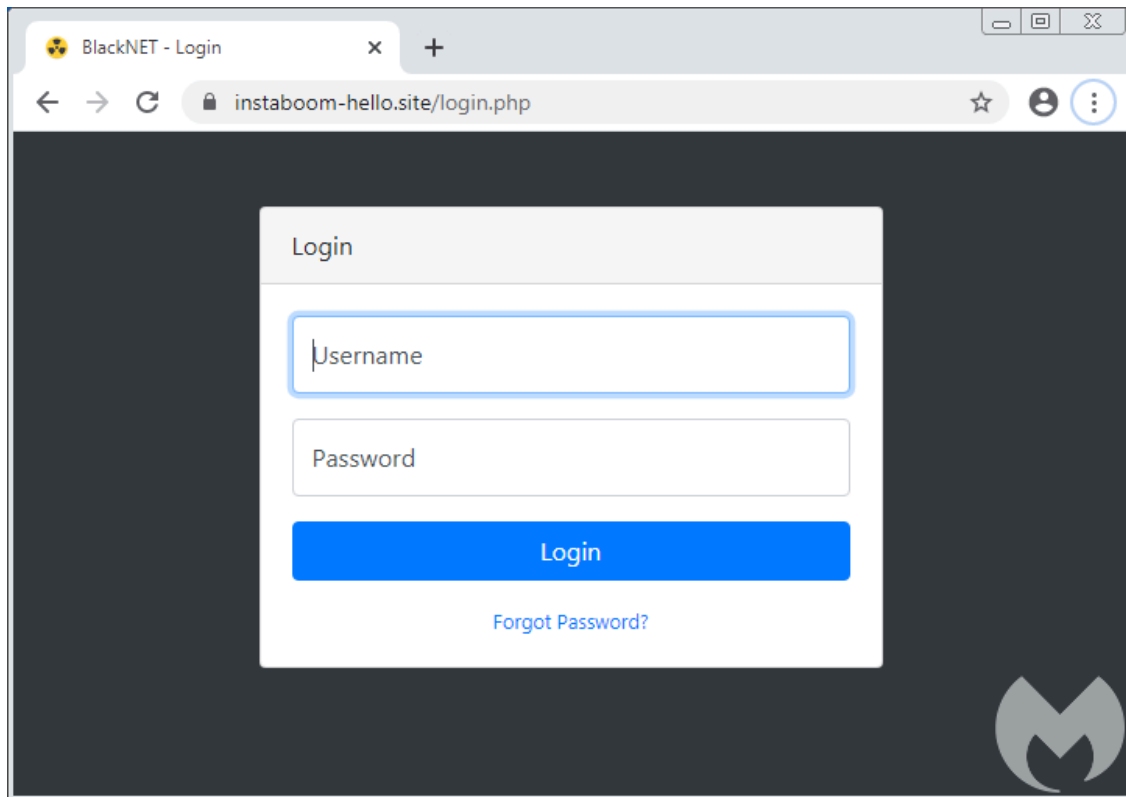


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with a few blue dots representing clients. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

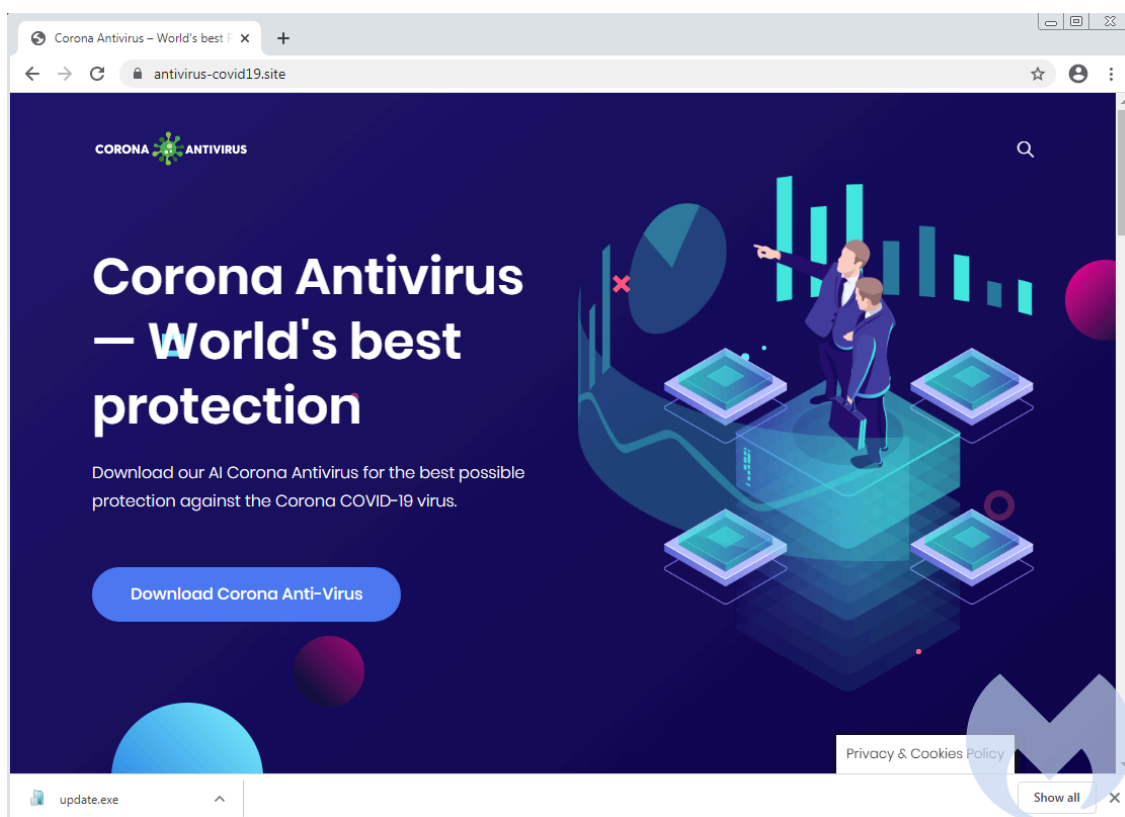
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

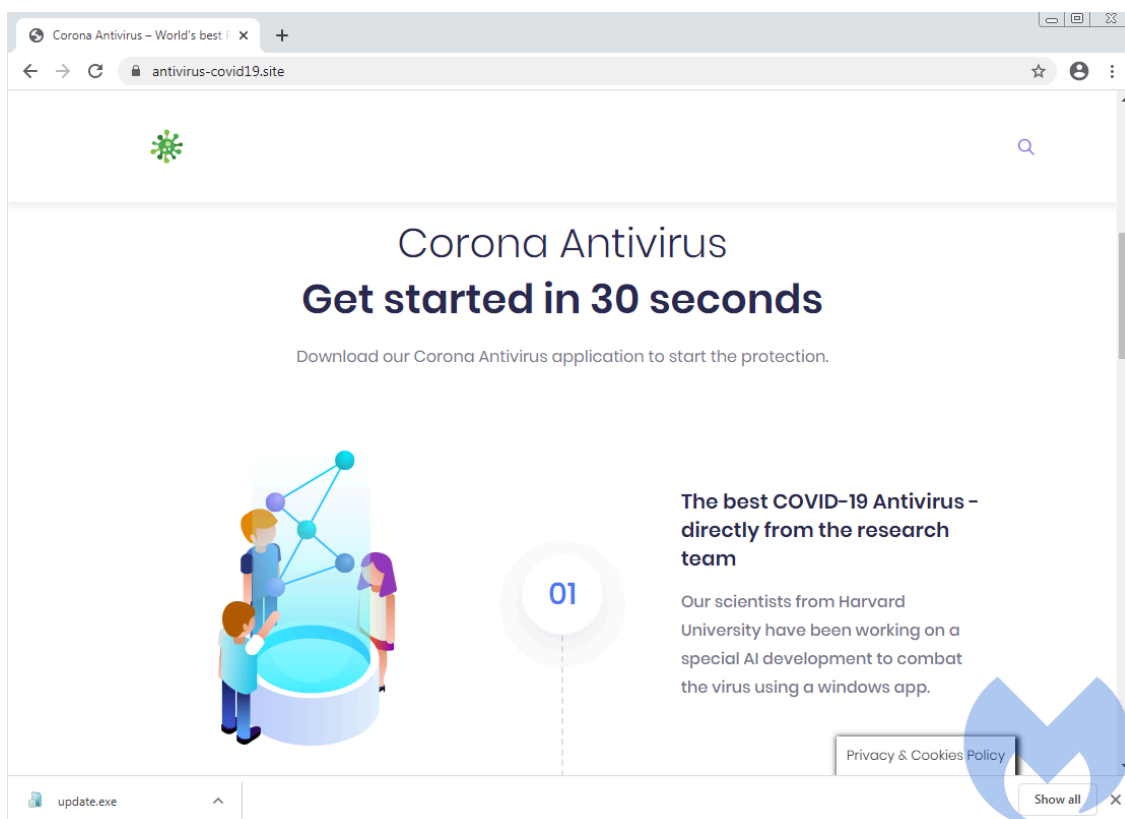
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

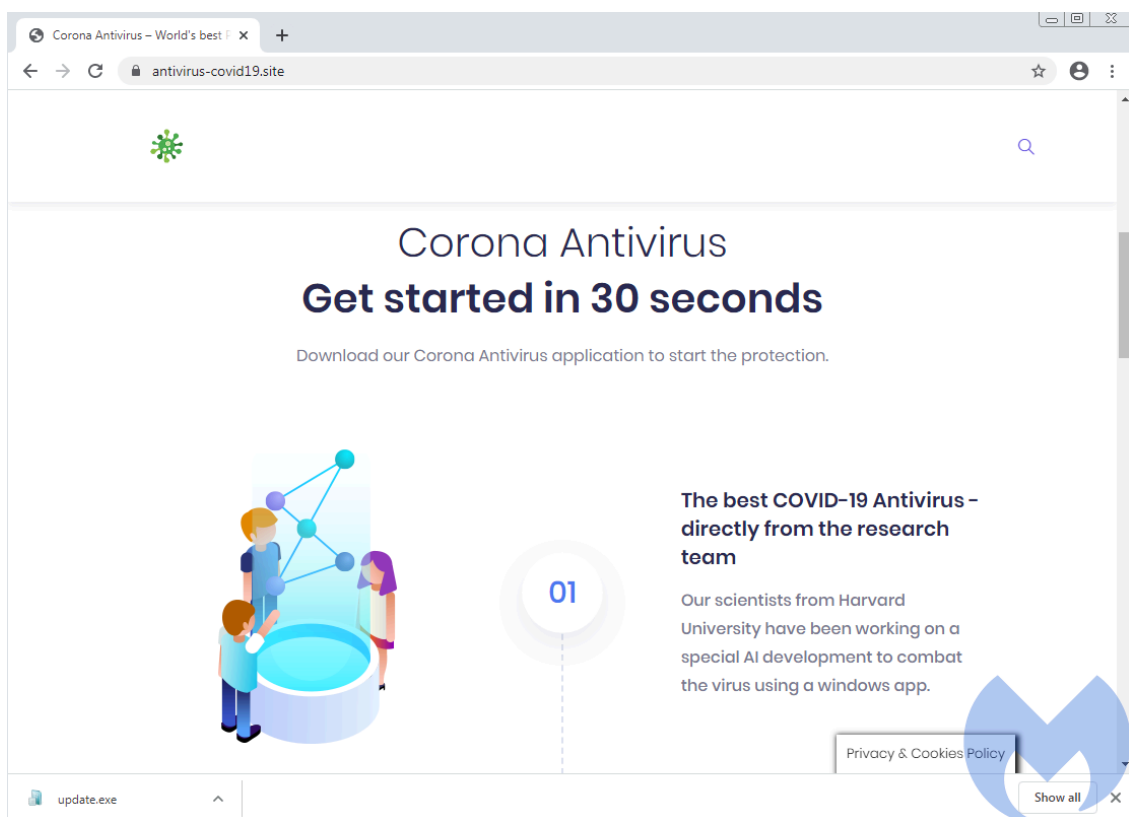
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

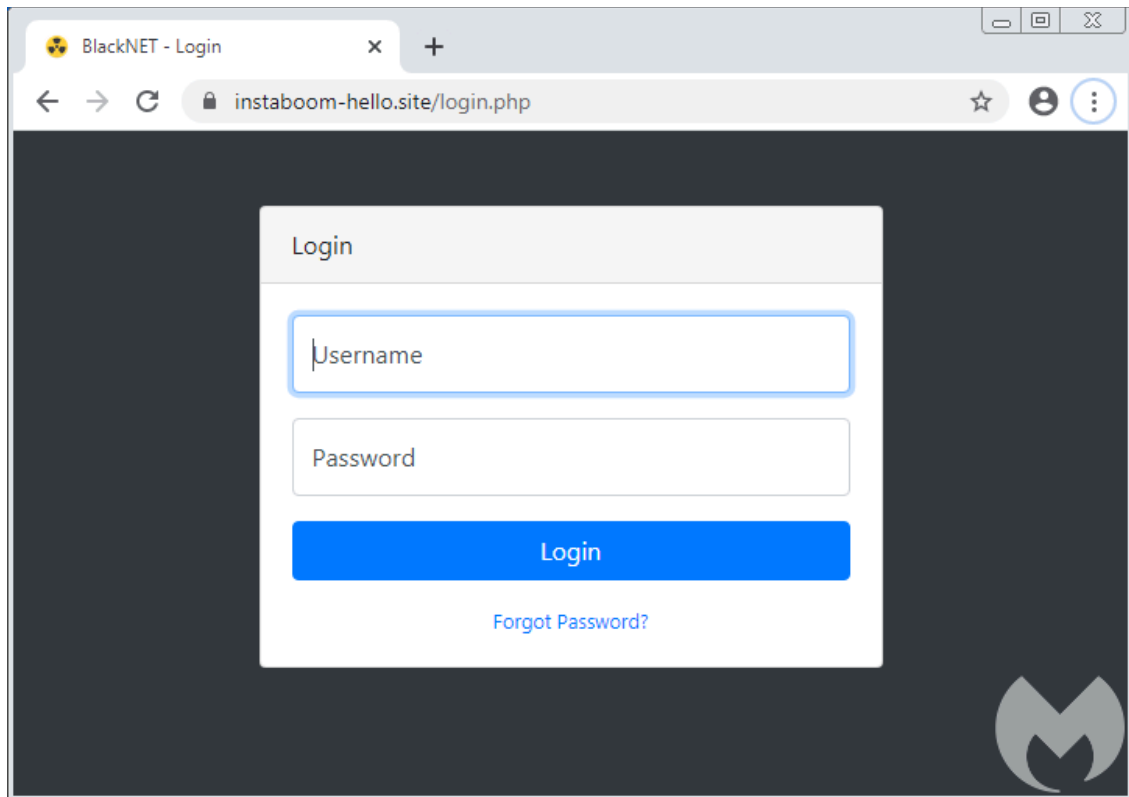


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

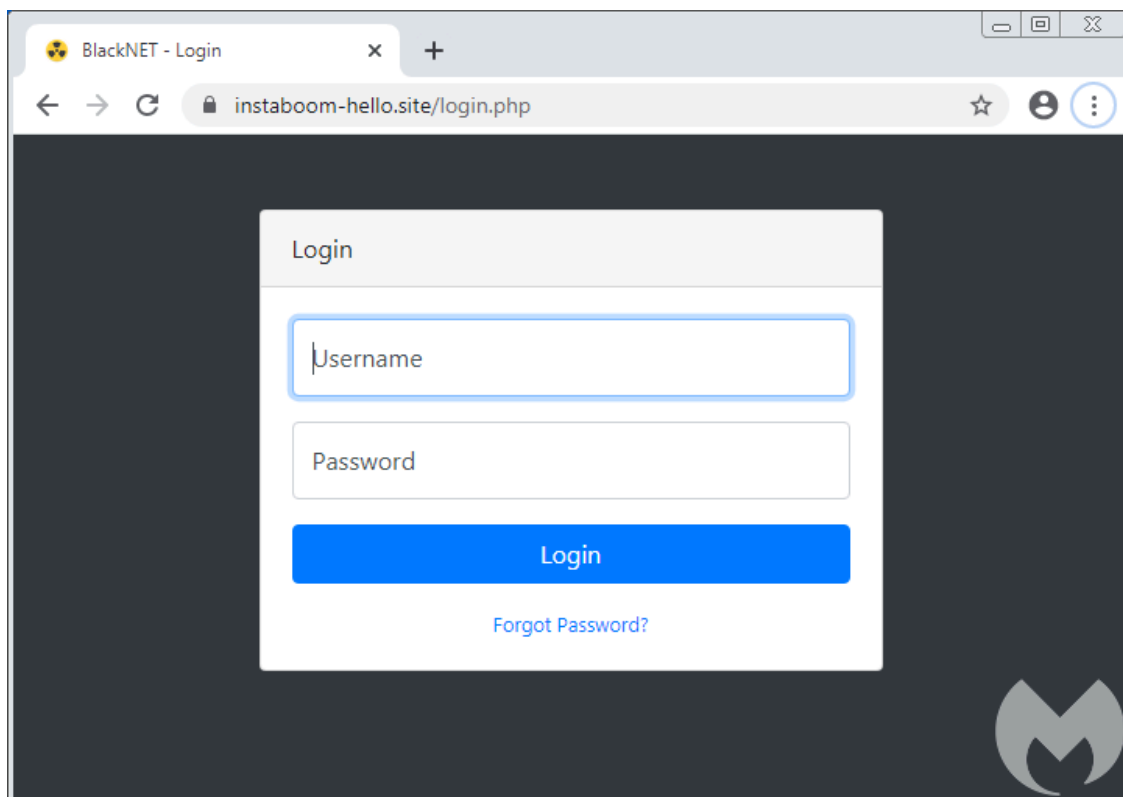
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

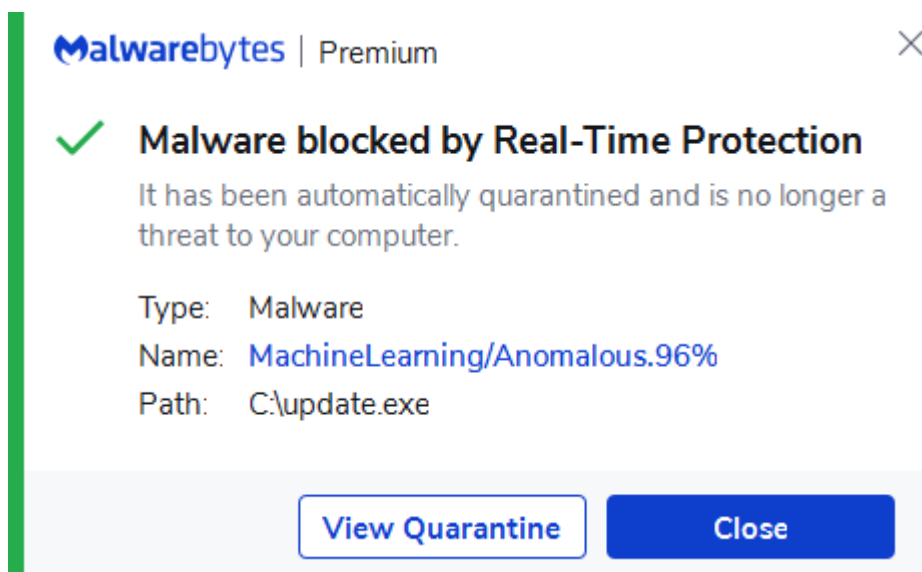
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

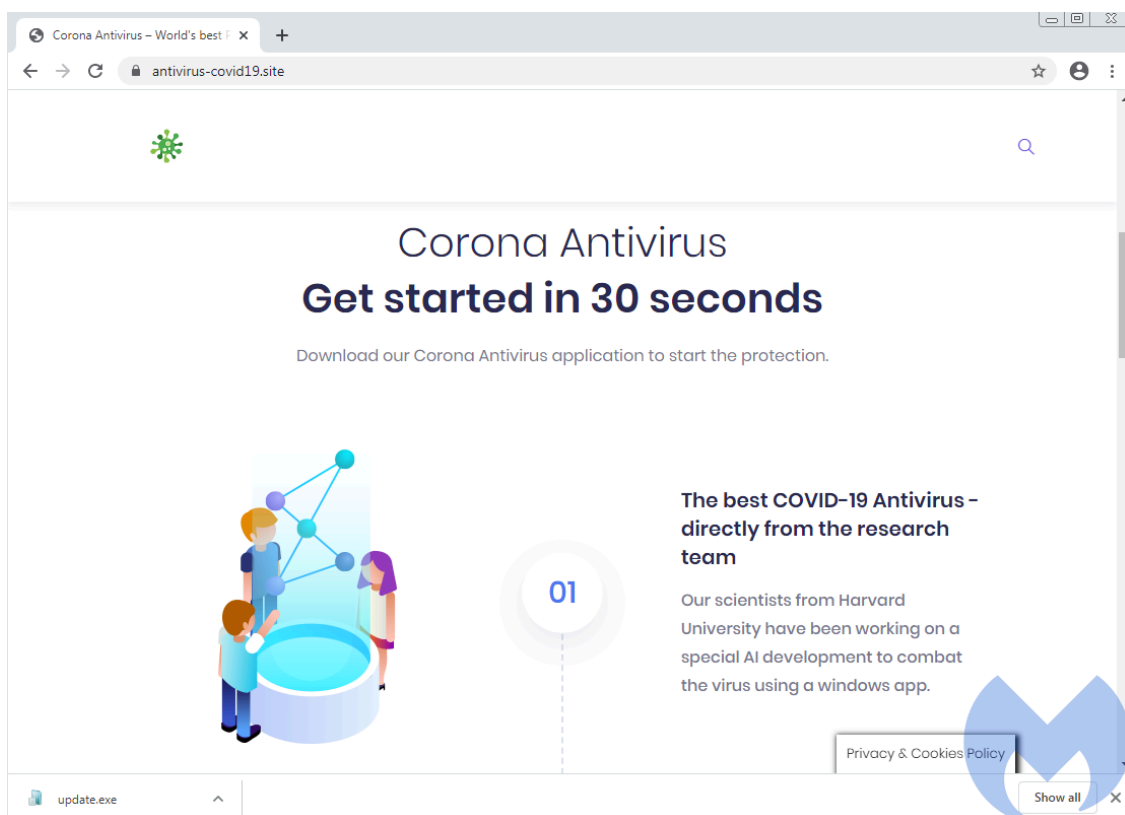
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

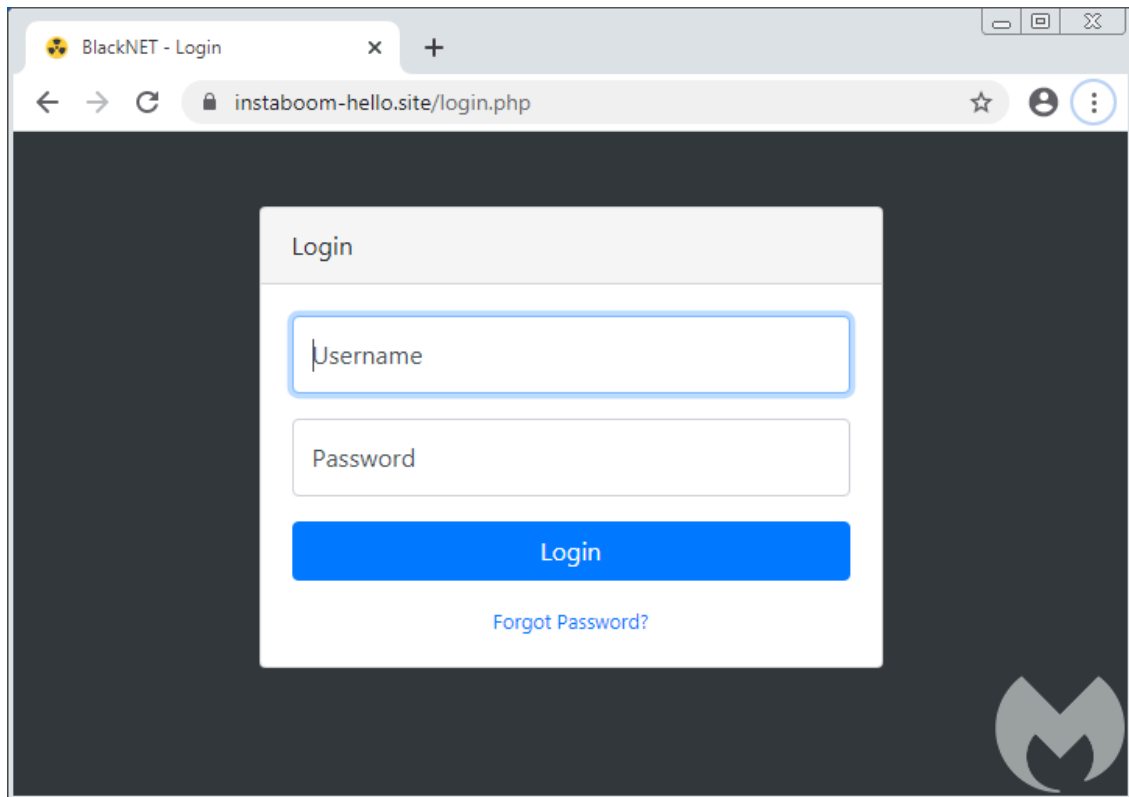


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

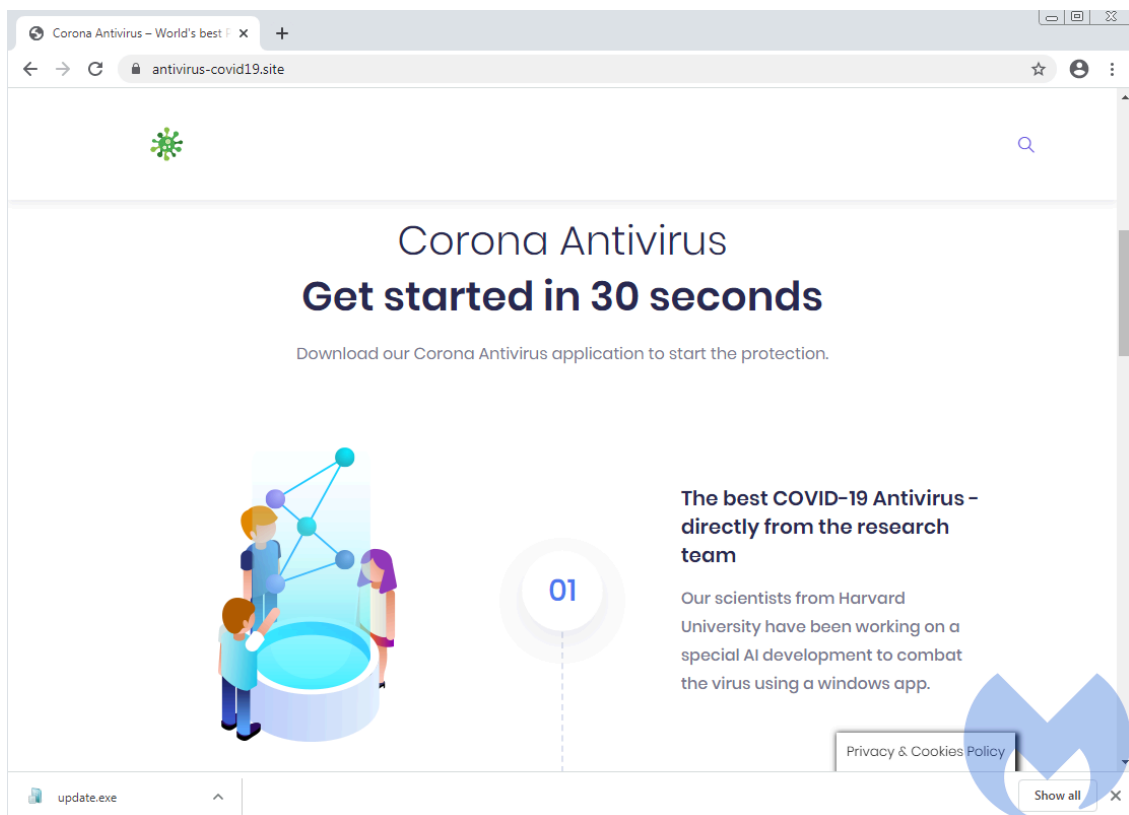
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

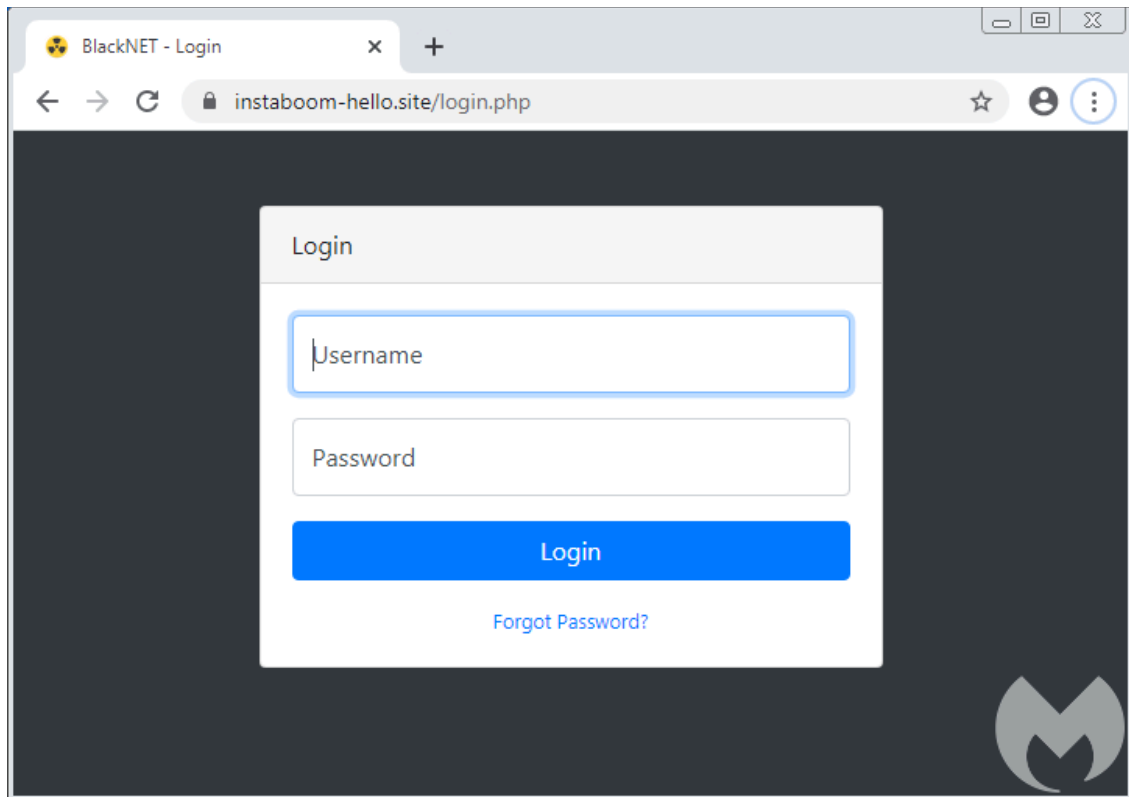


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

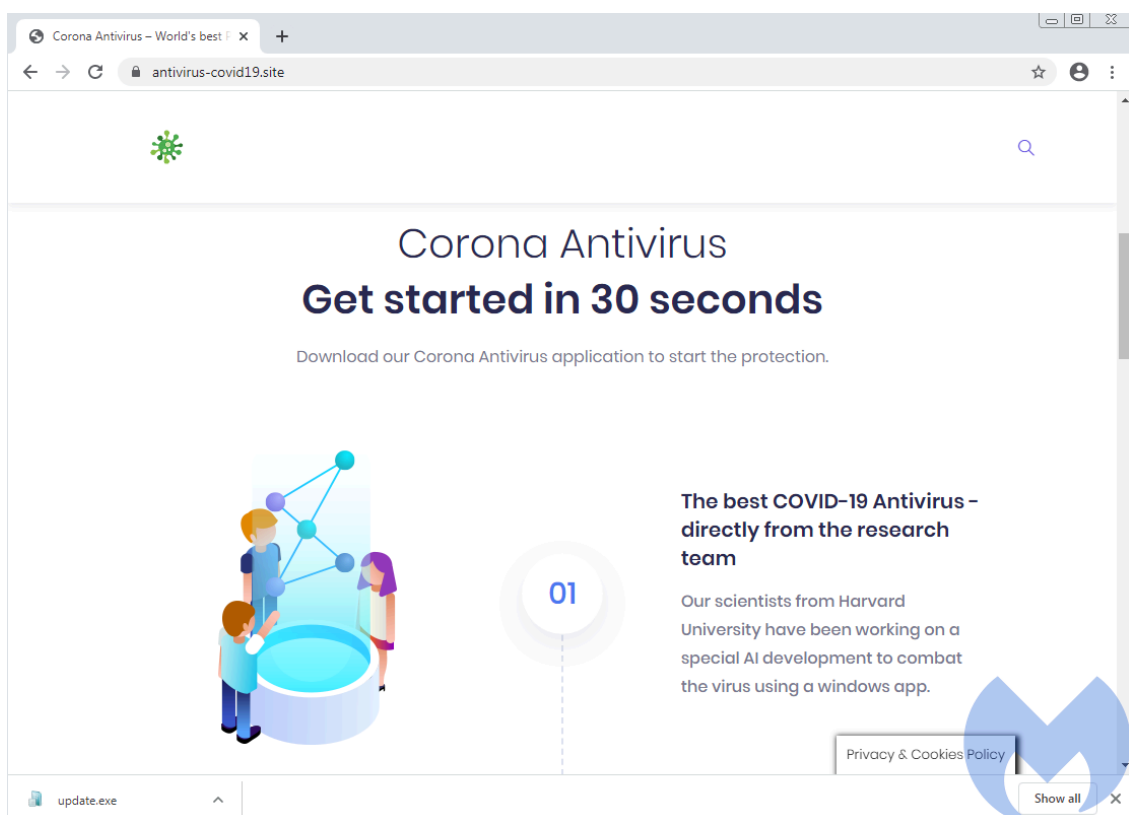
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

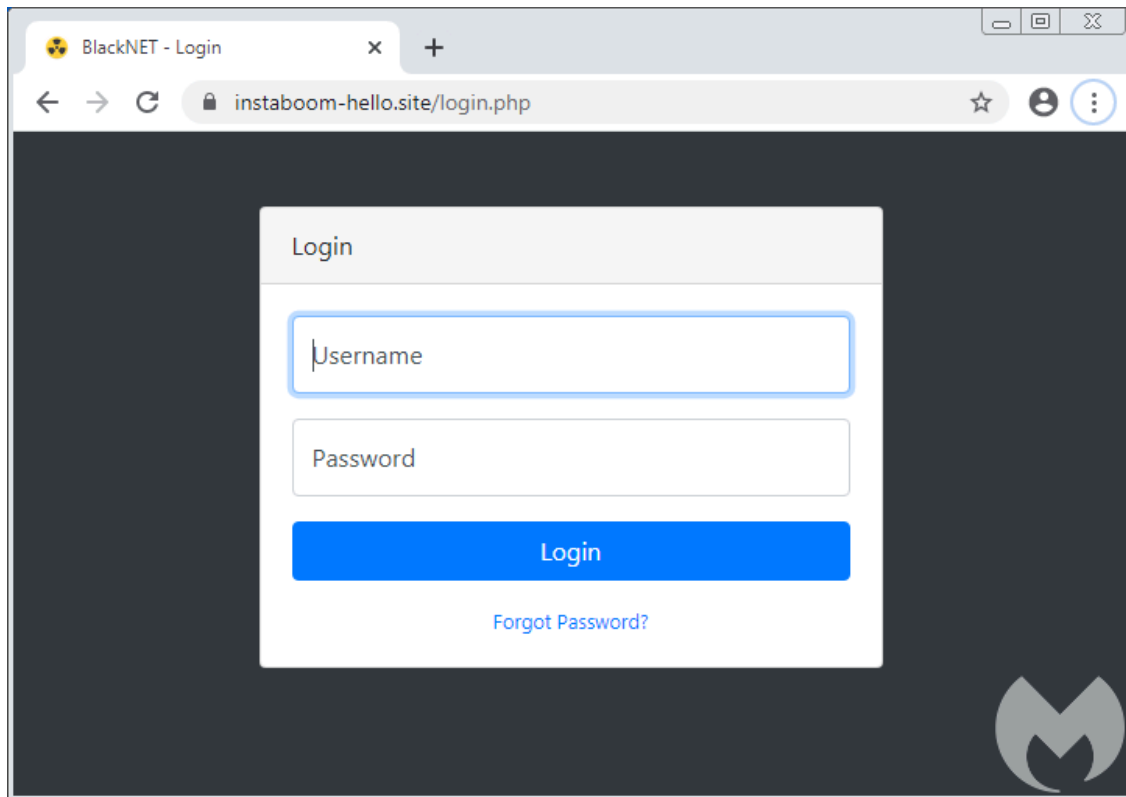


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

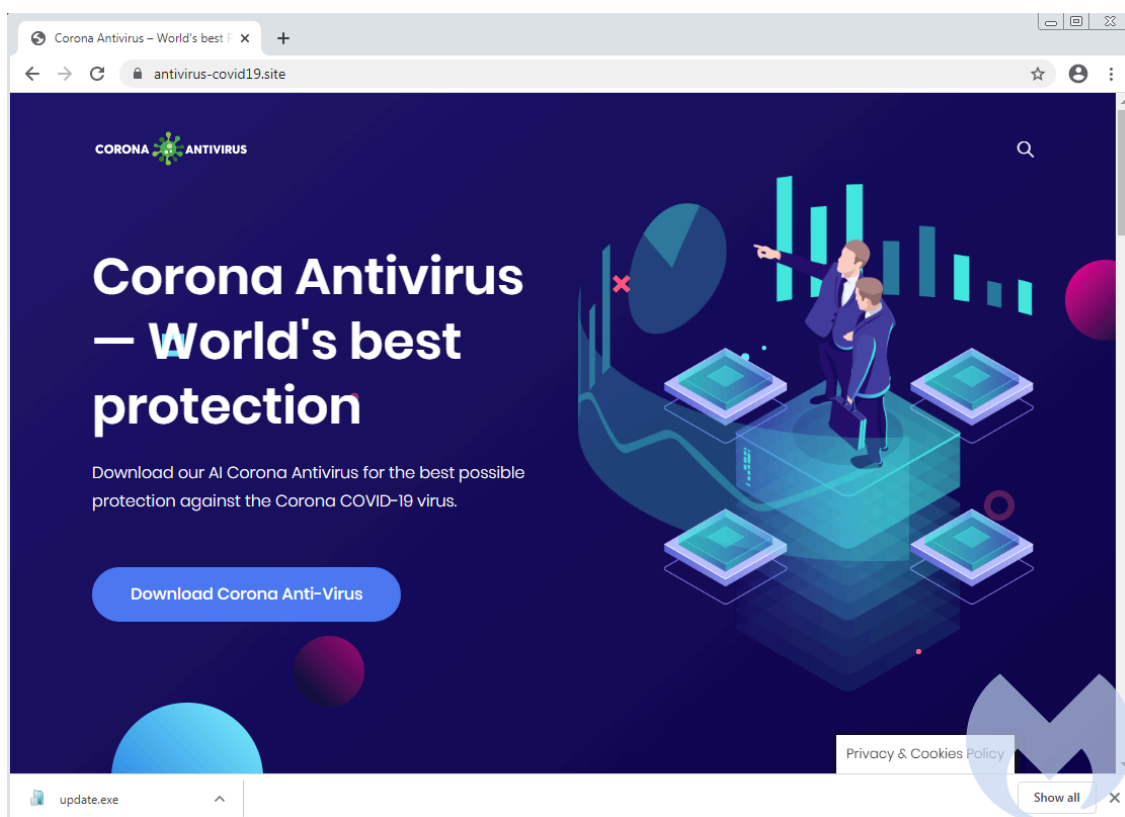
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

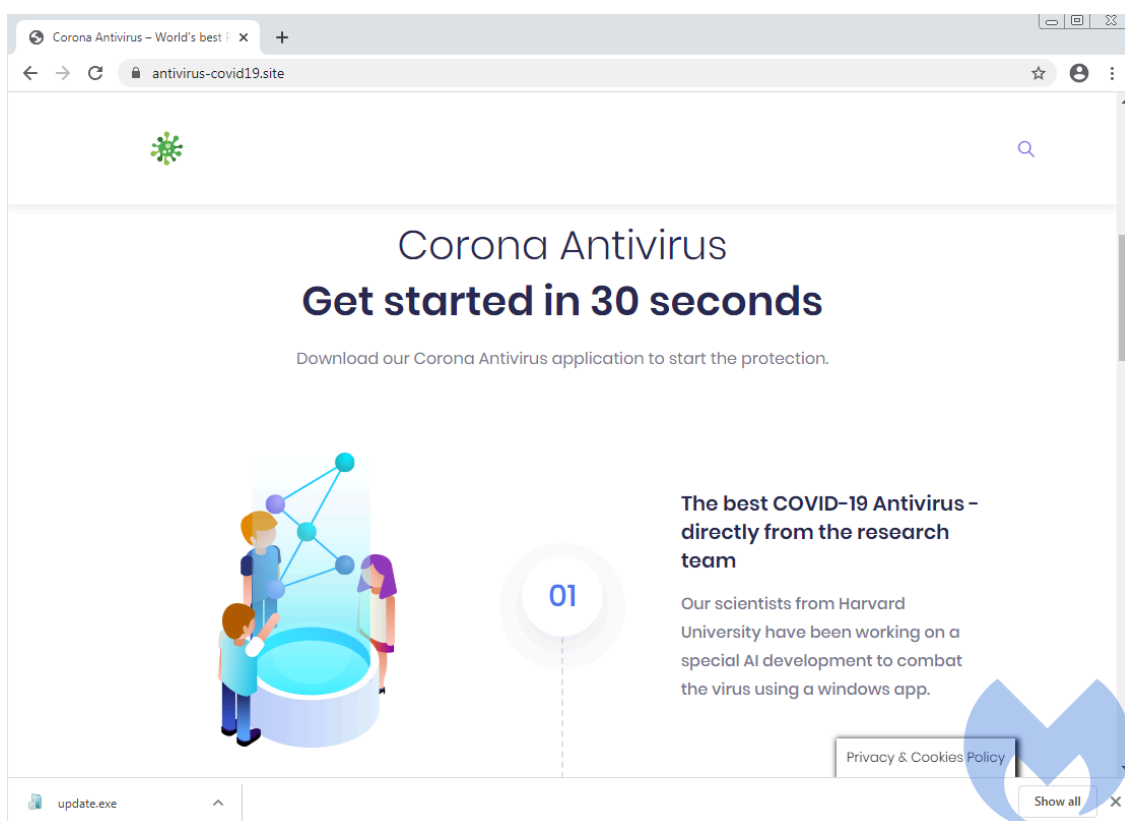
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

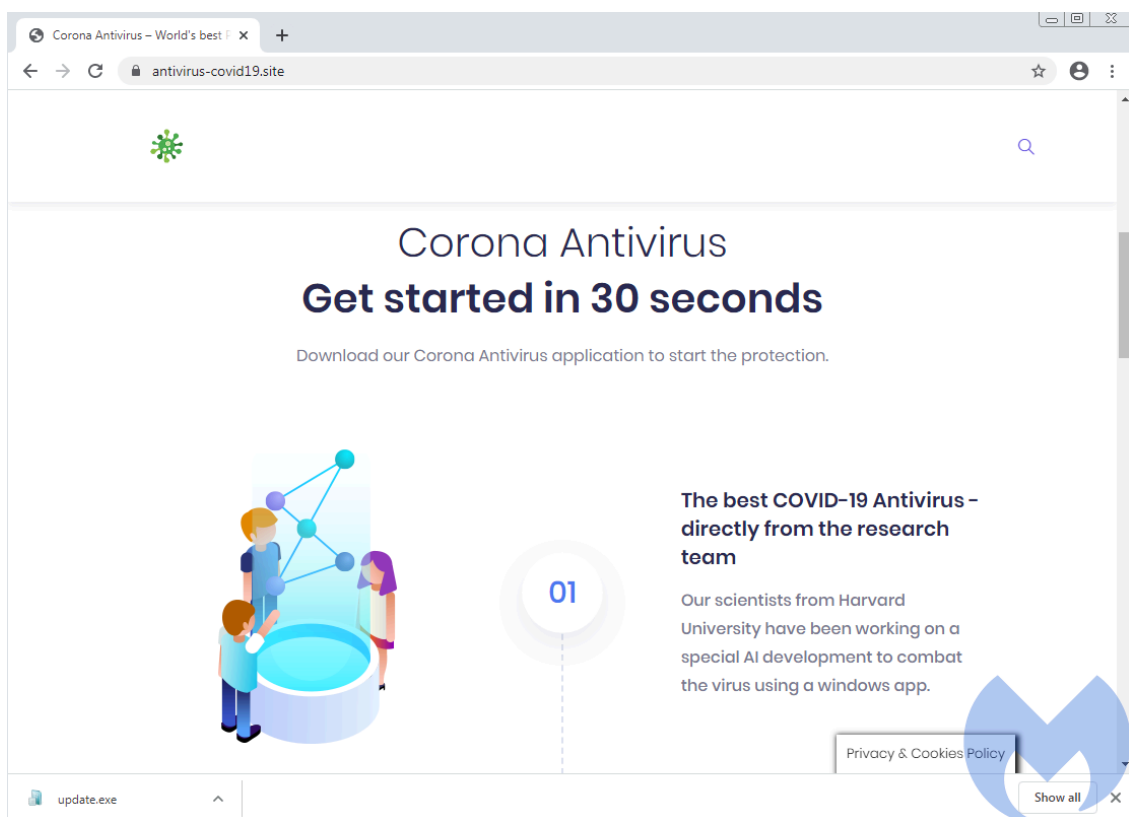
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

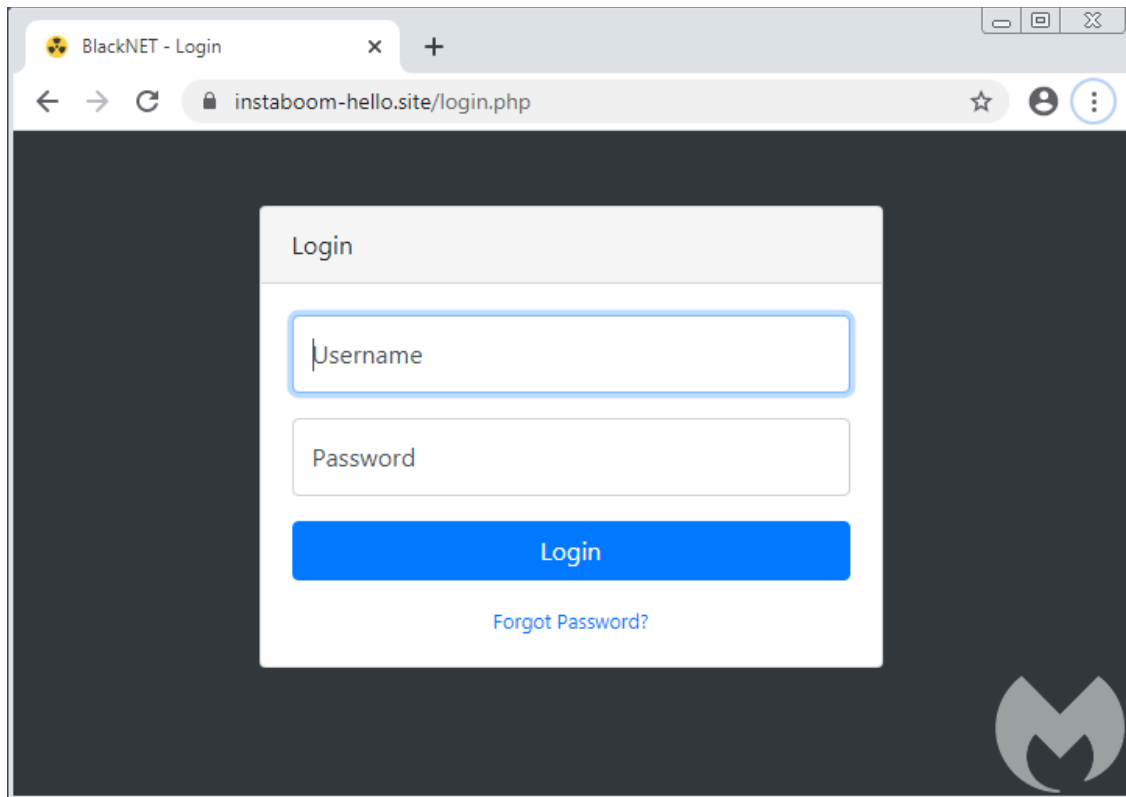


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored tiles: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

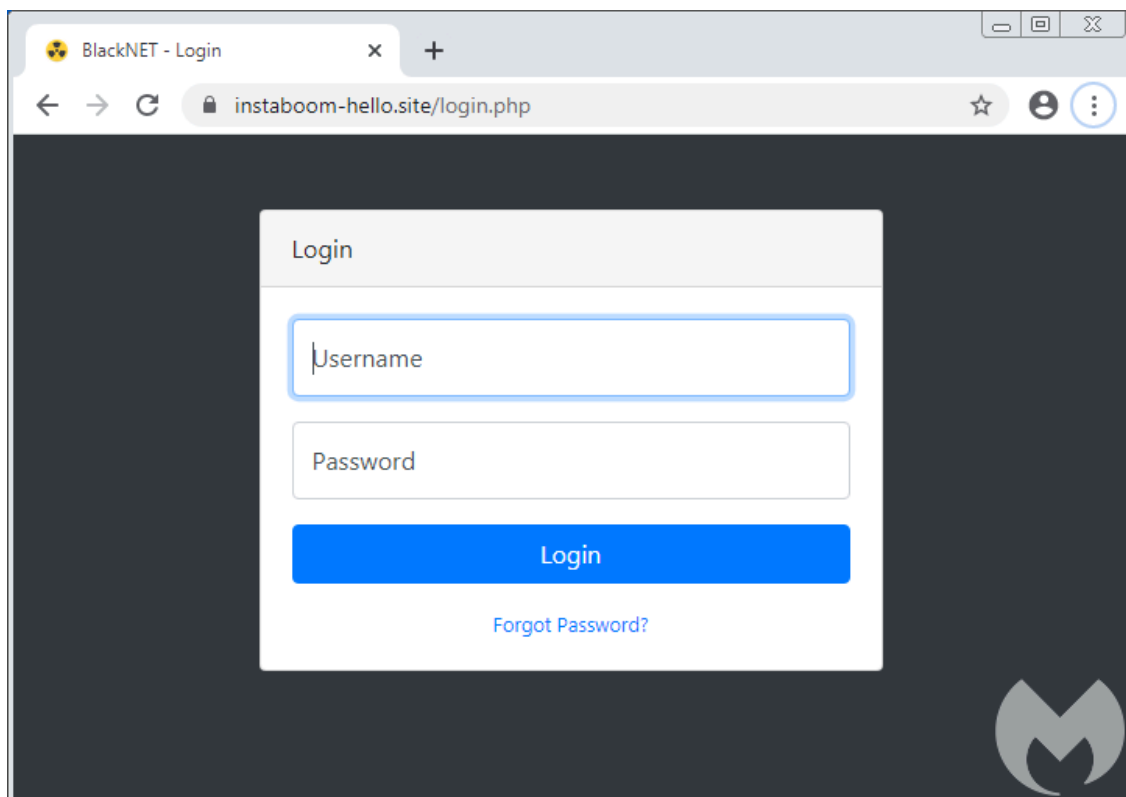
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

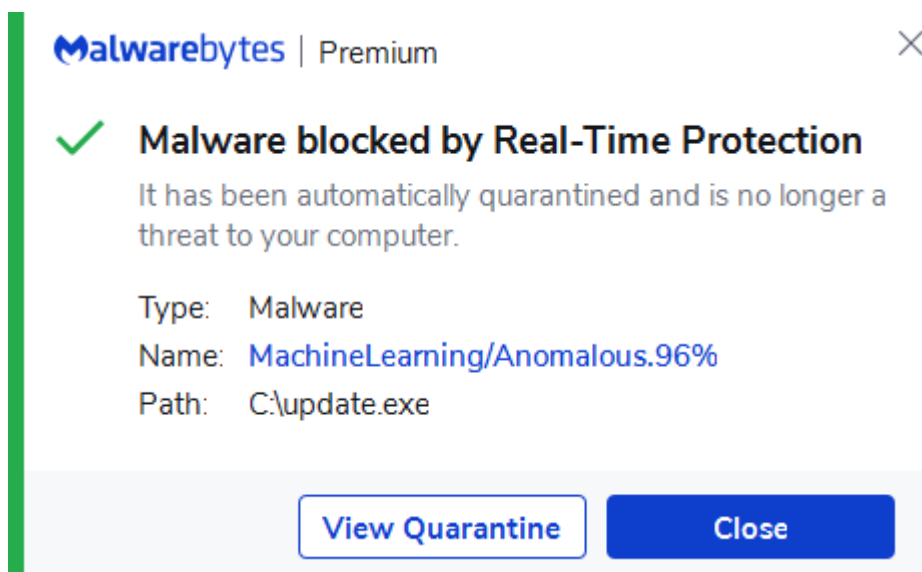
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

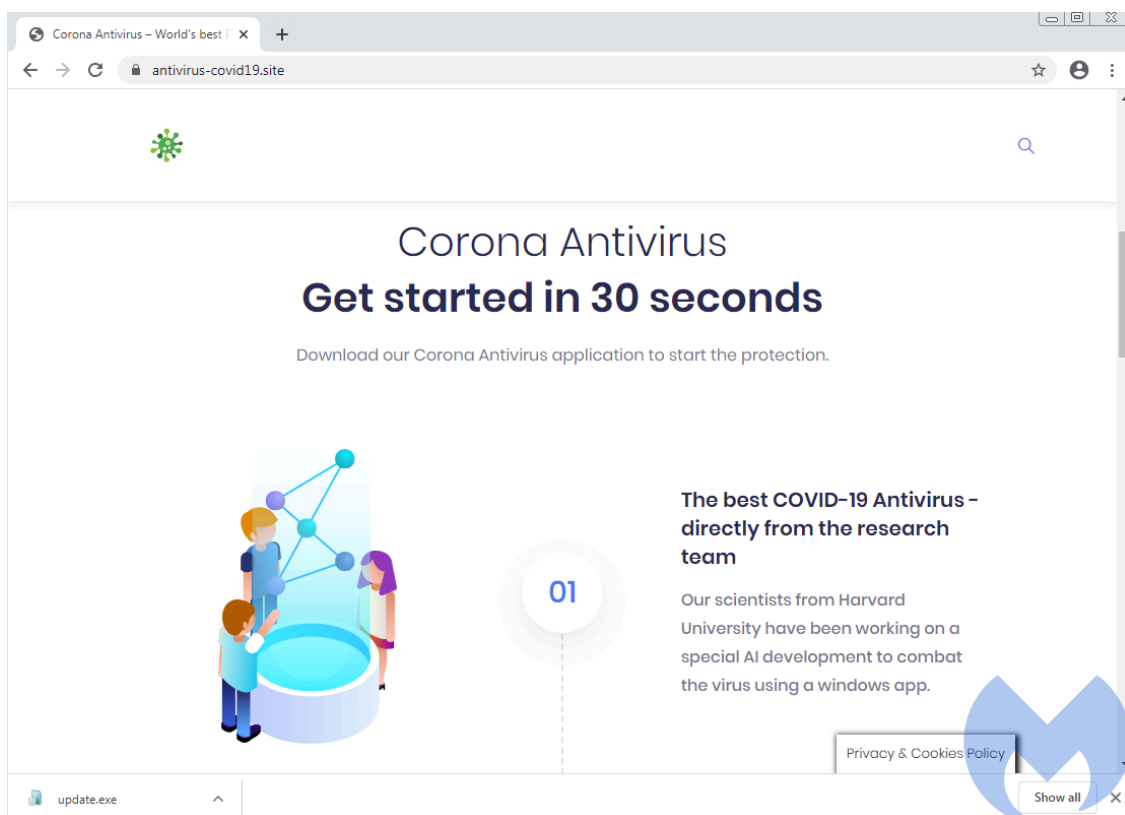
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

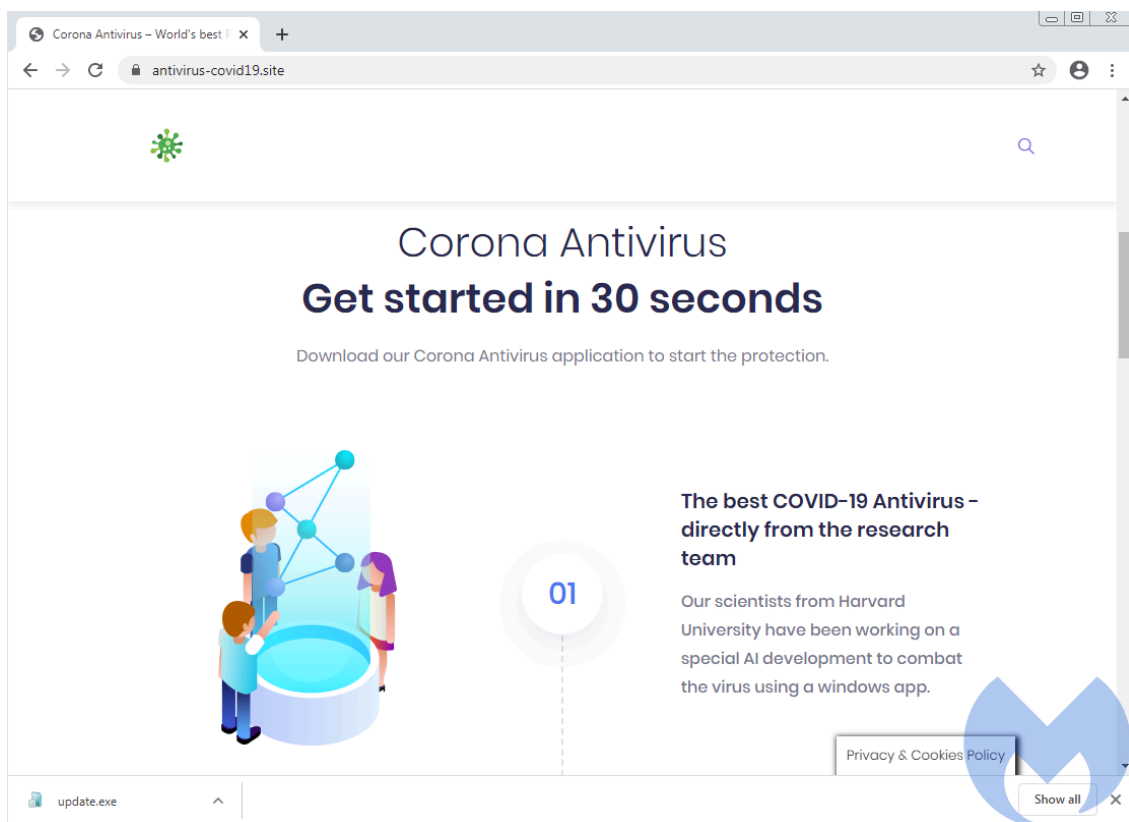
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

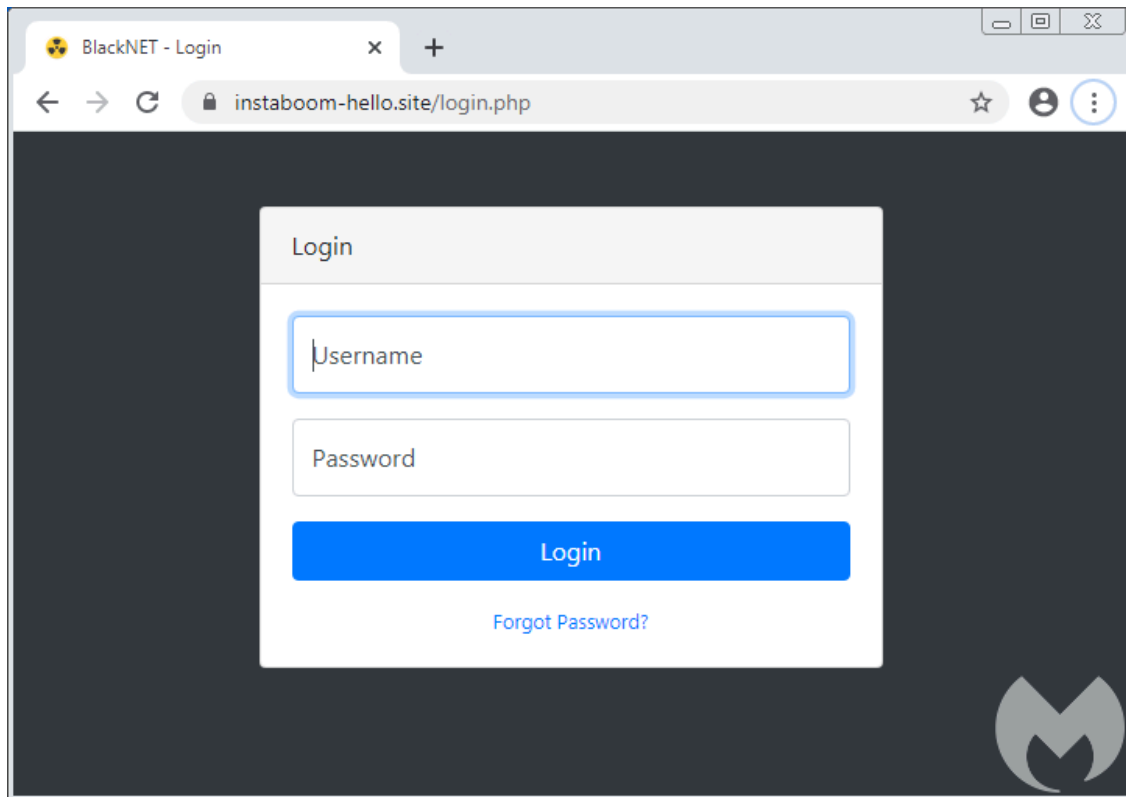


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

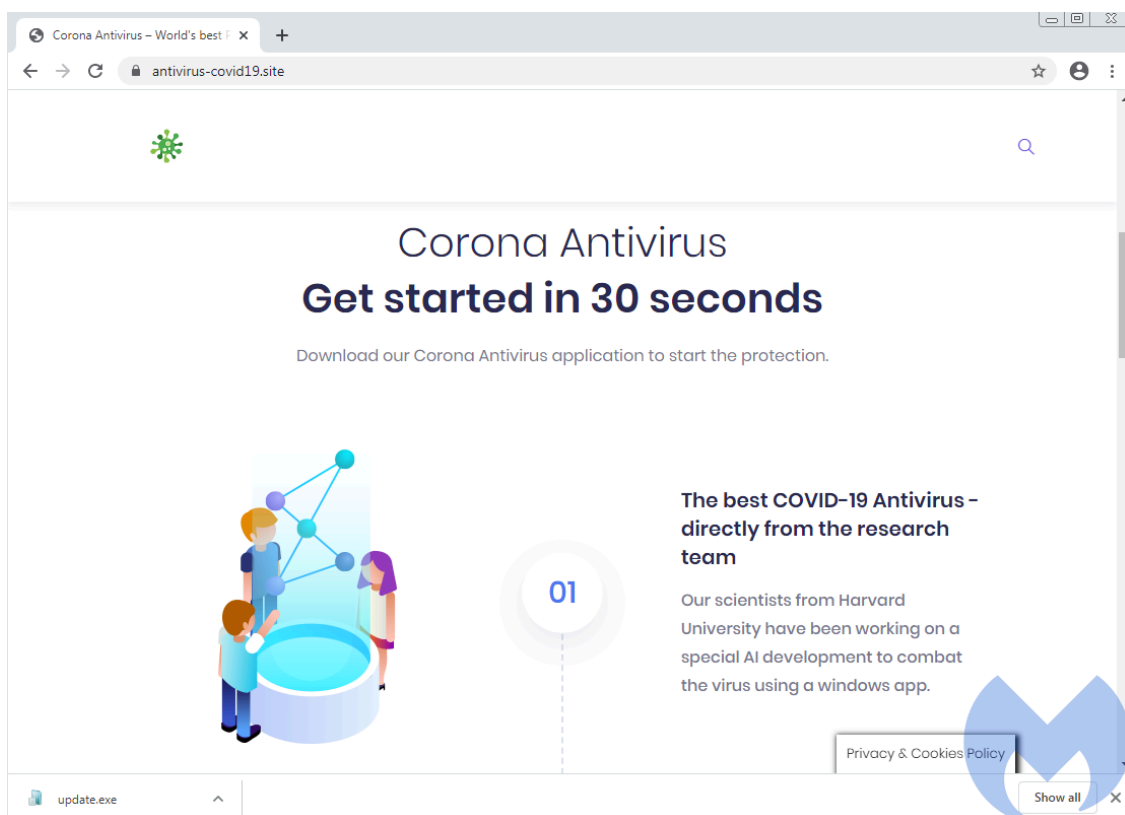
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

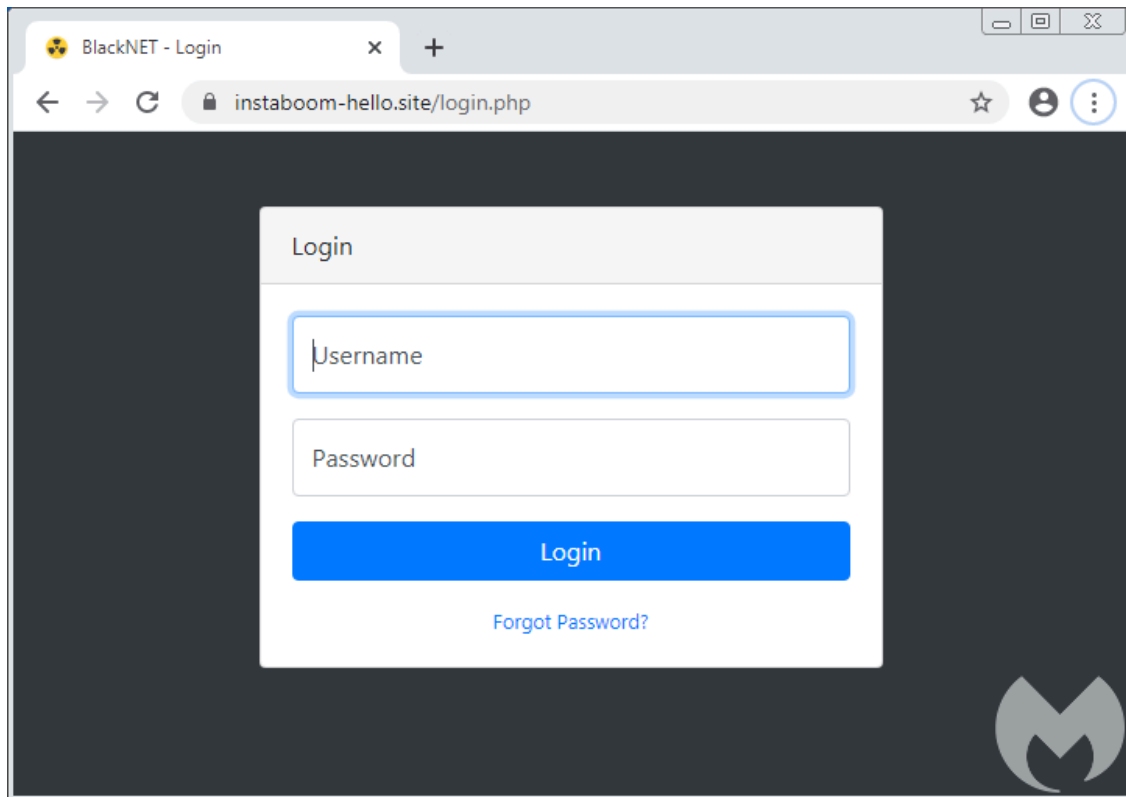


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

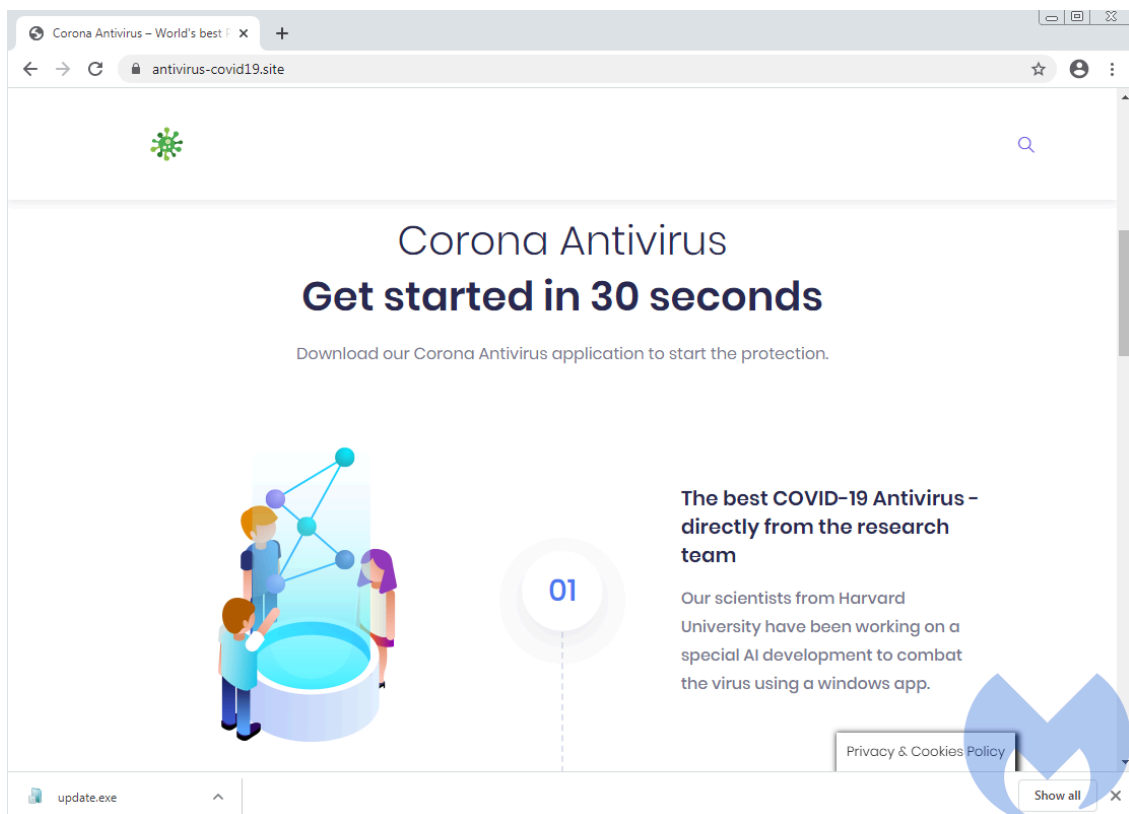
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

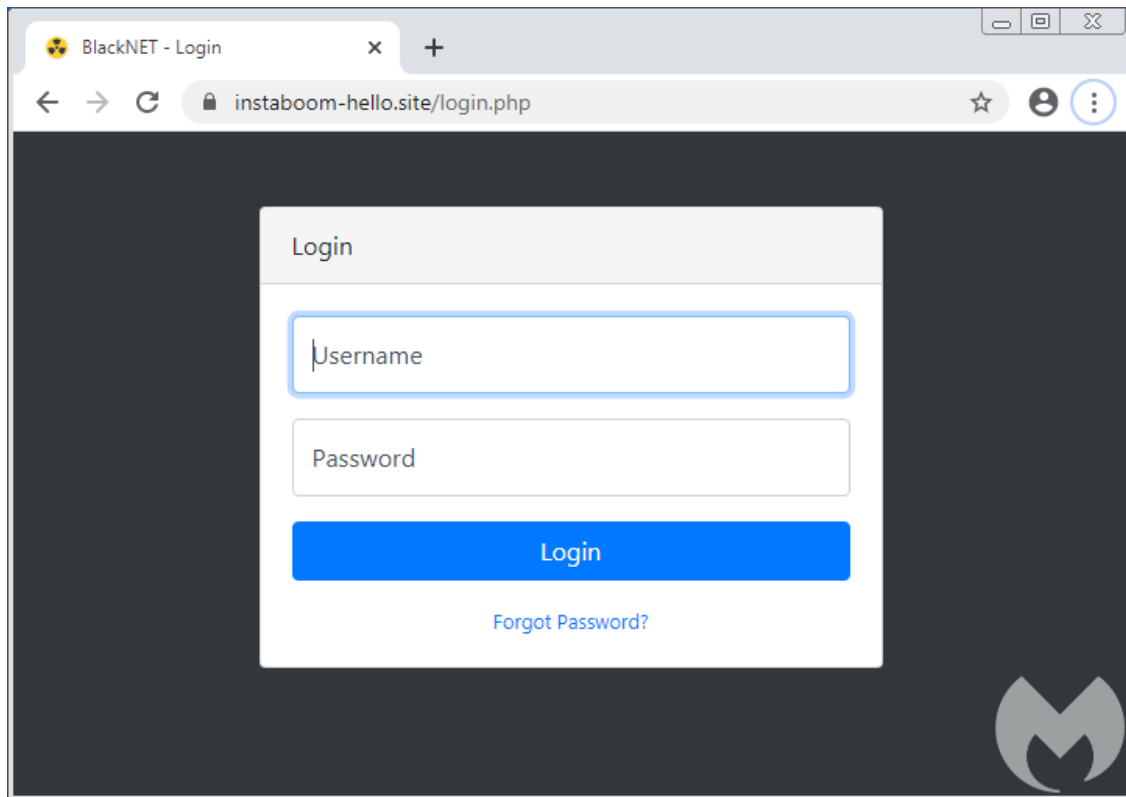


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

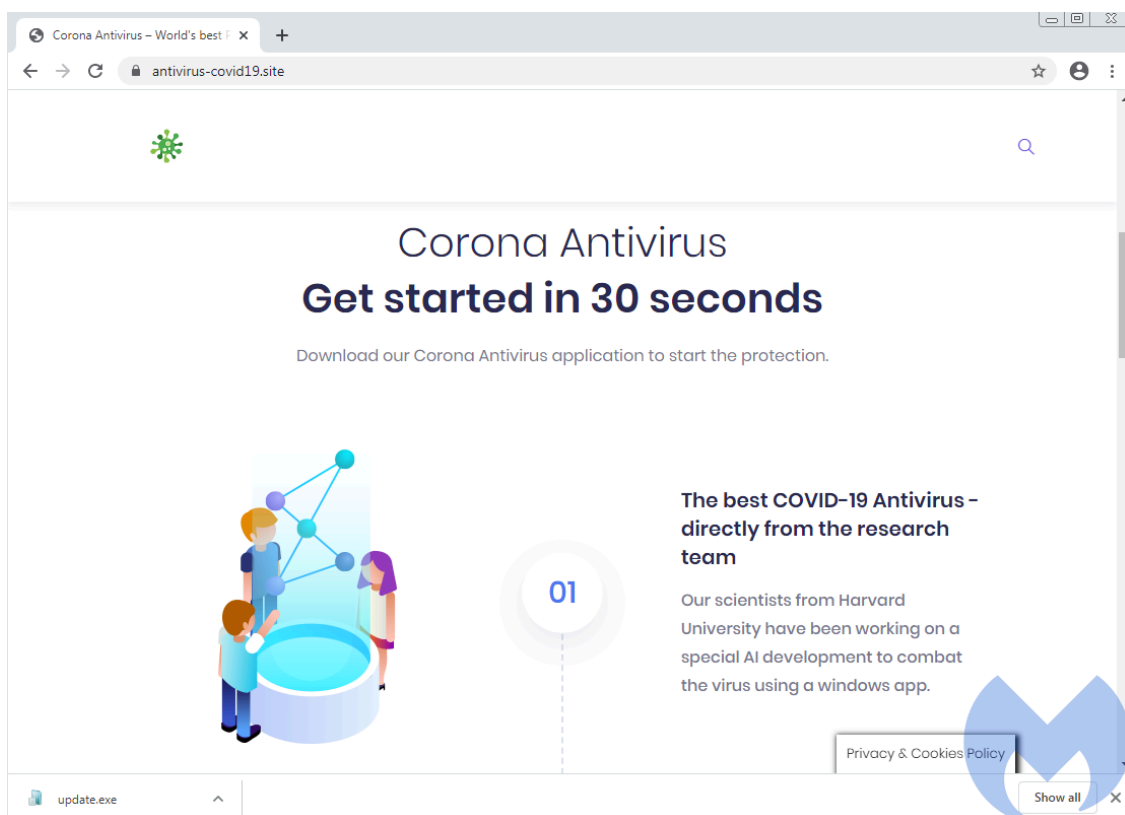
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

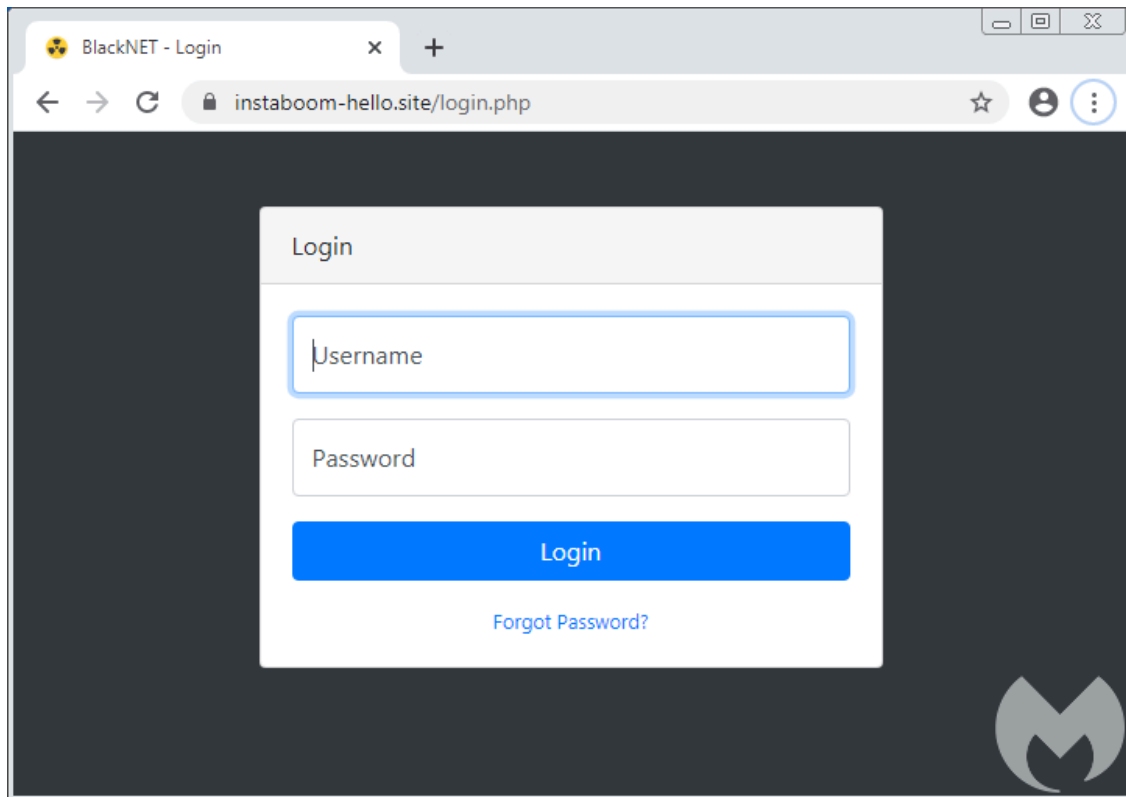


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

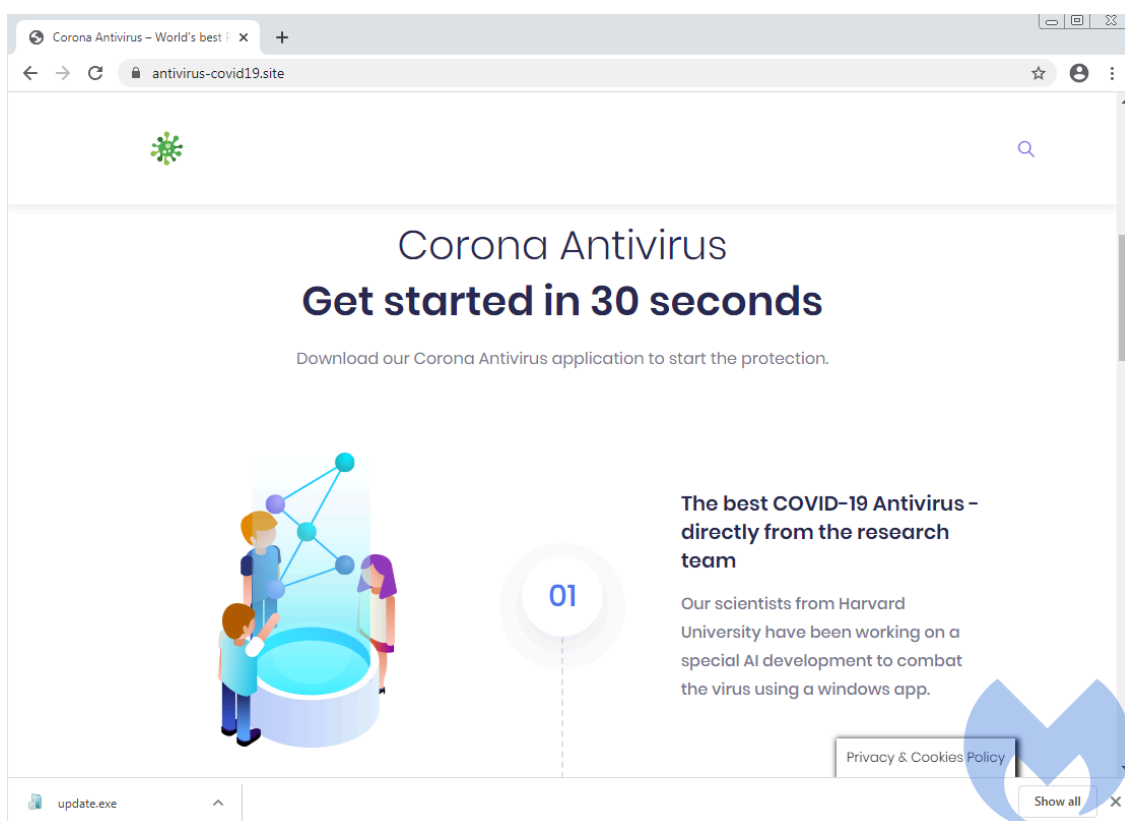
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

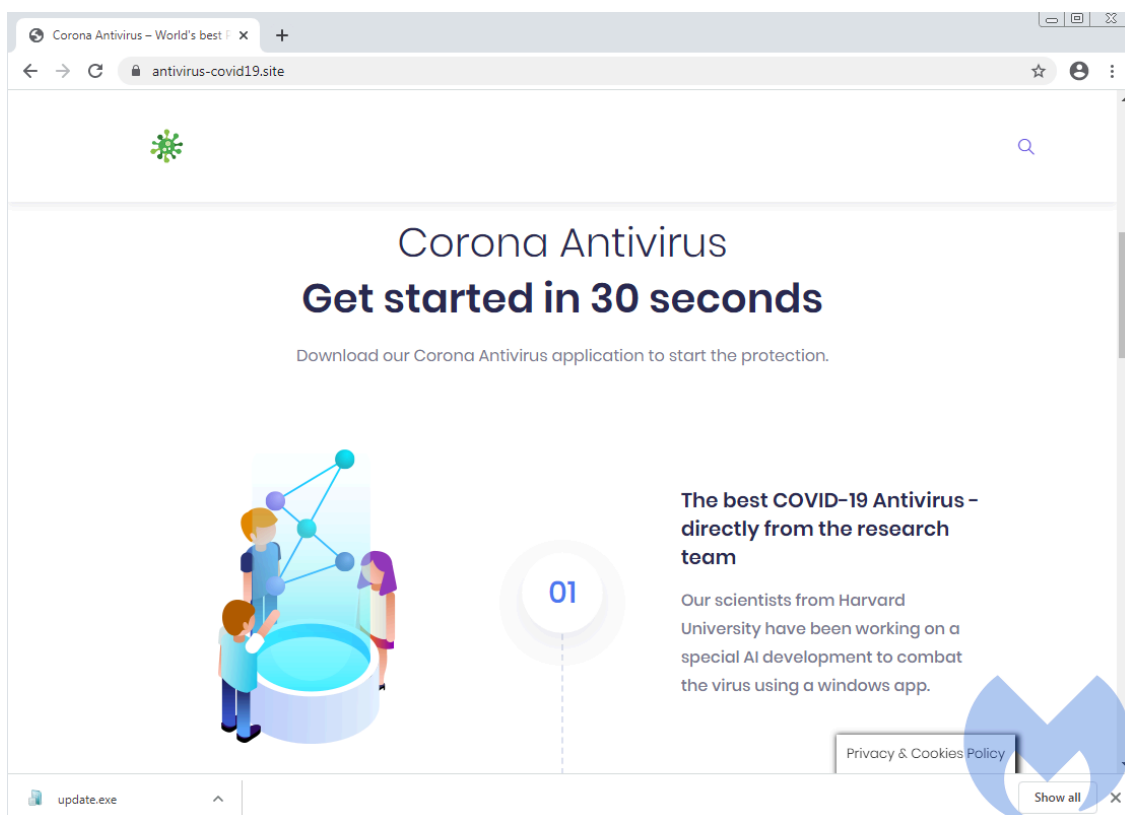
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

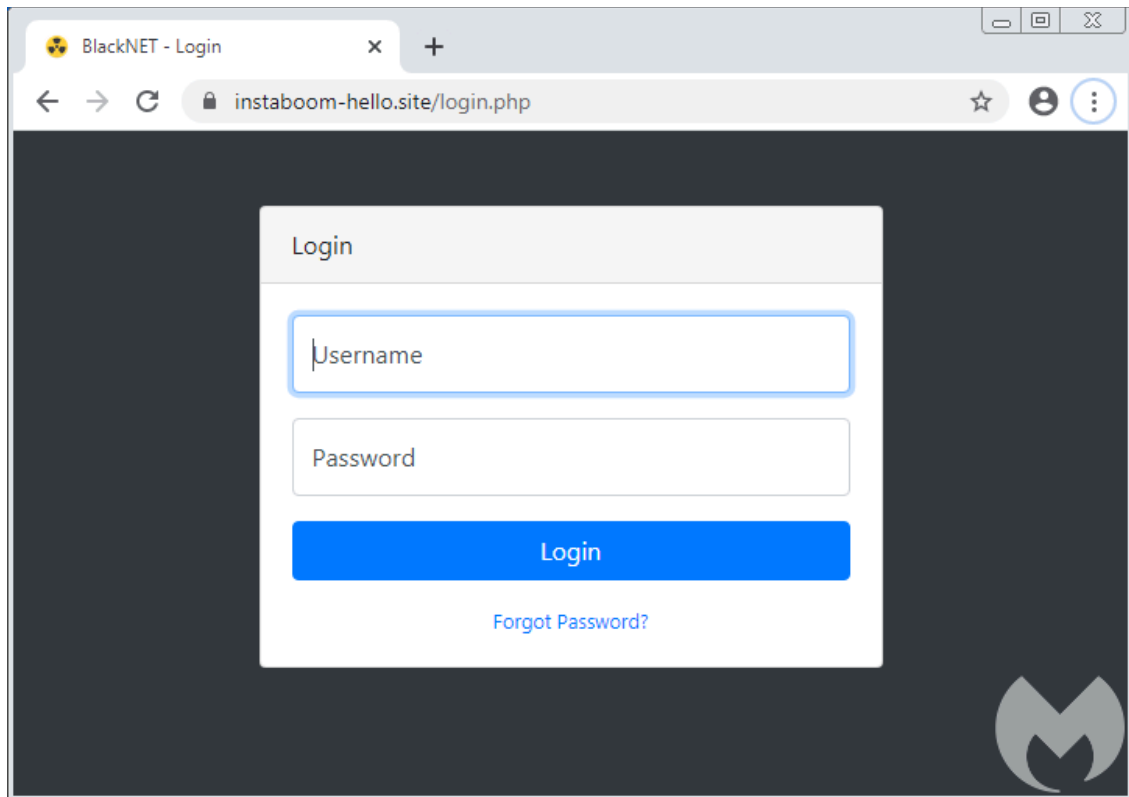


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

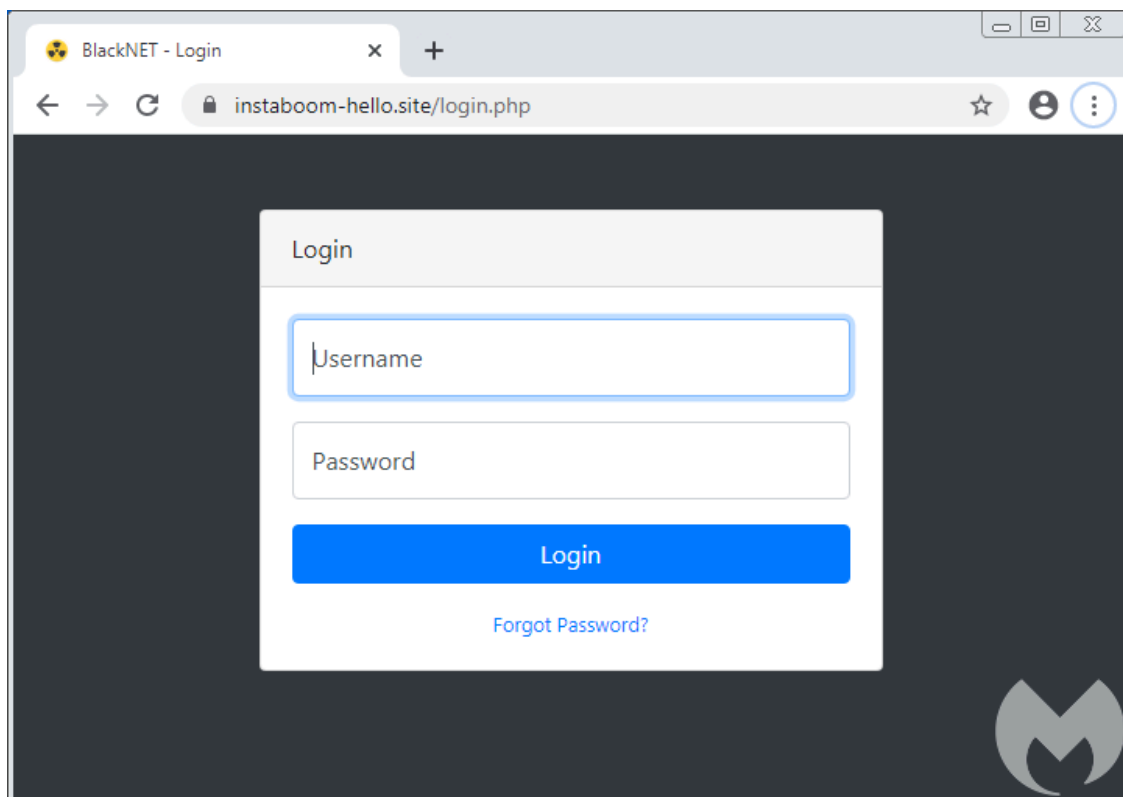
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

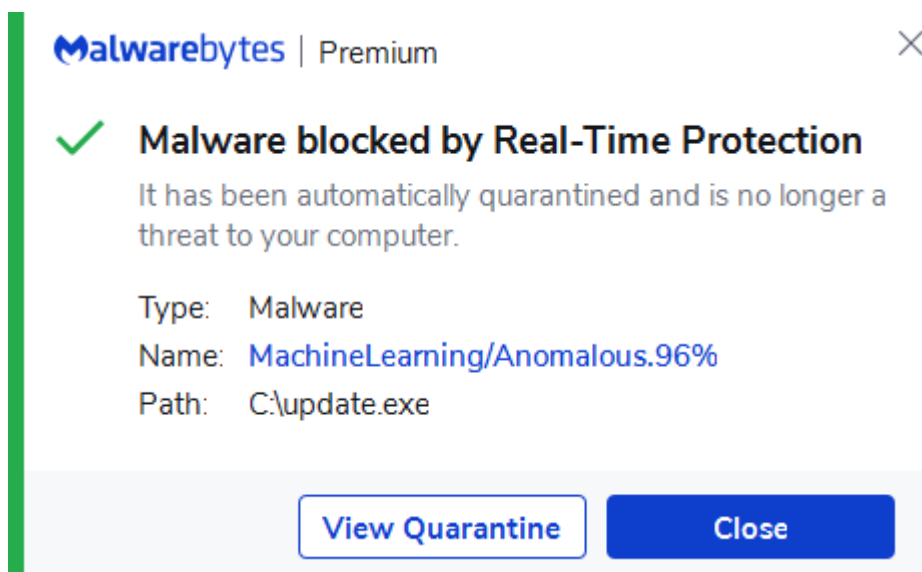
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' navigation buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

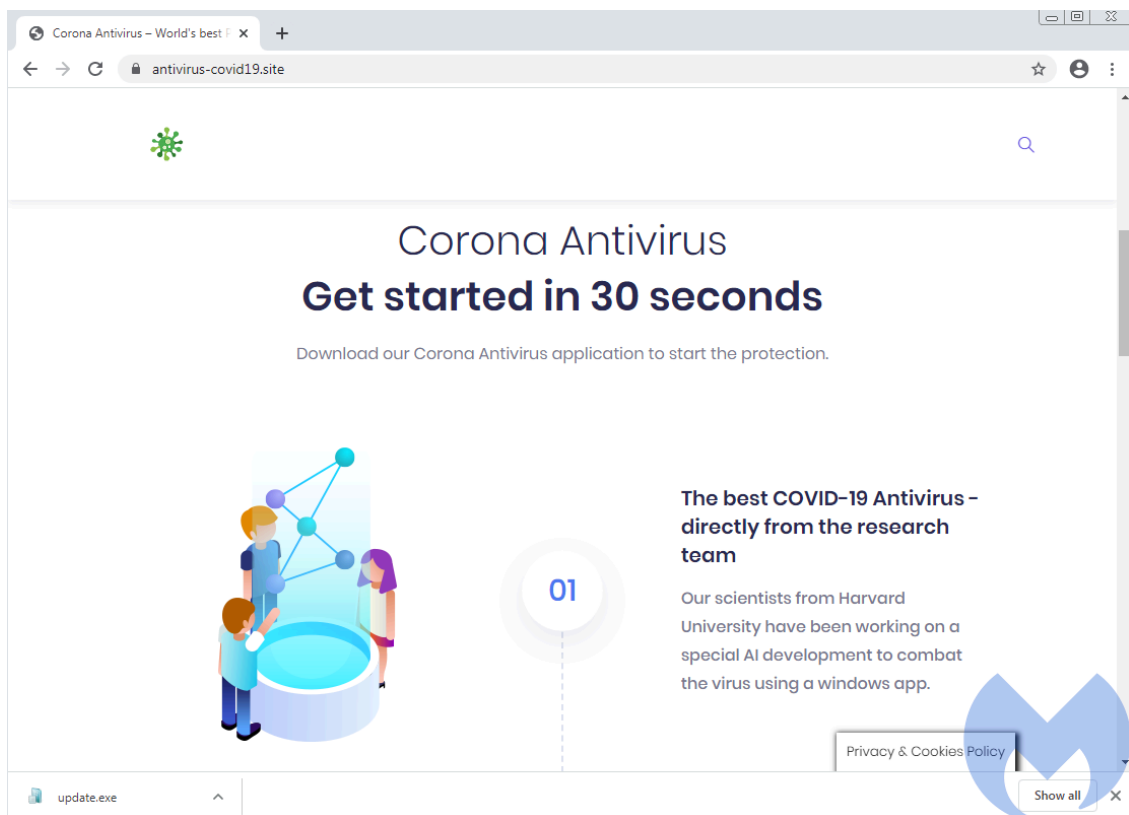
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

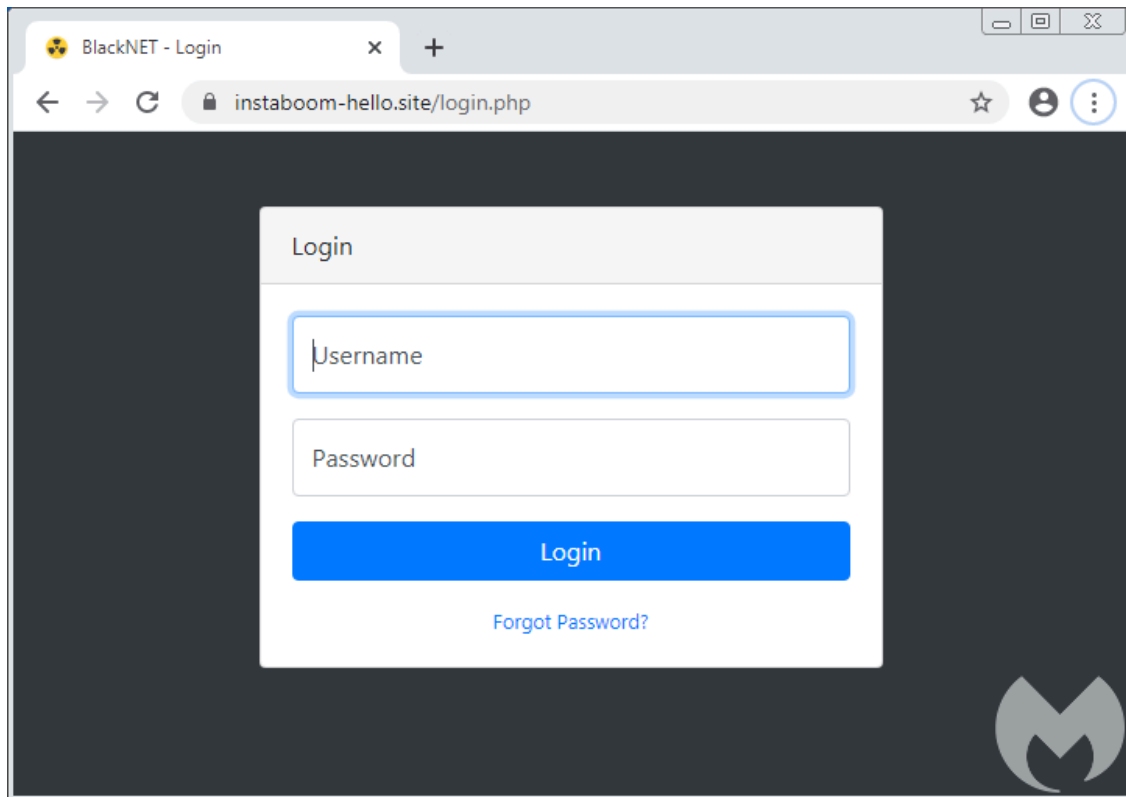


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

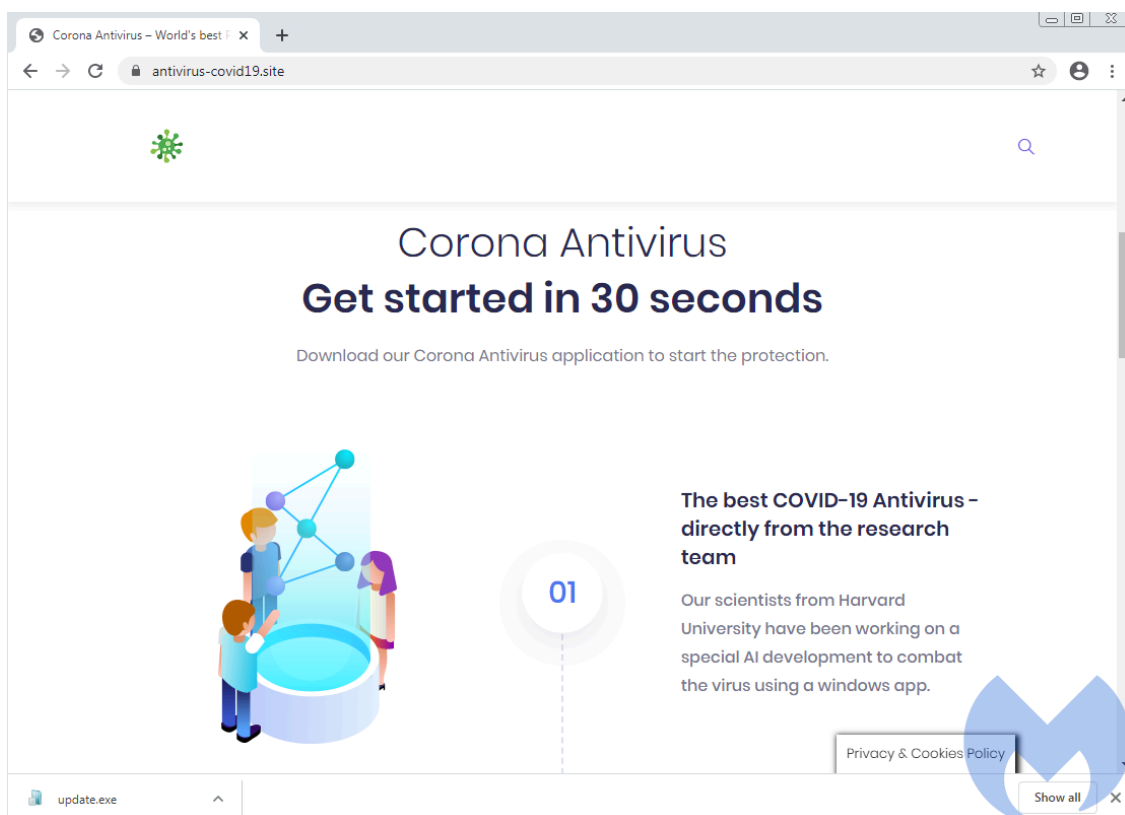
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

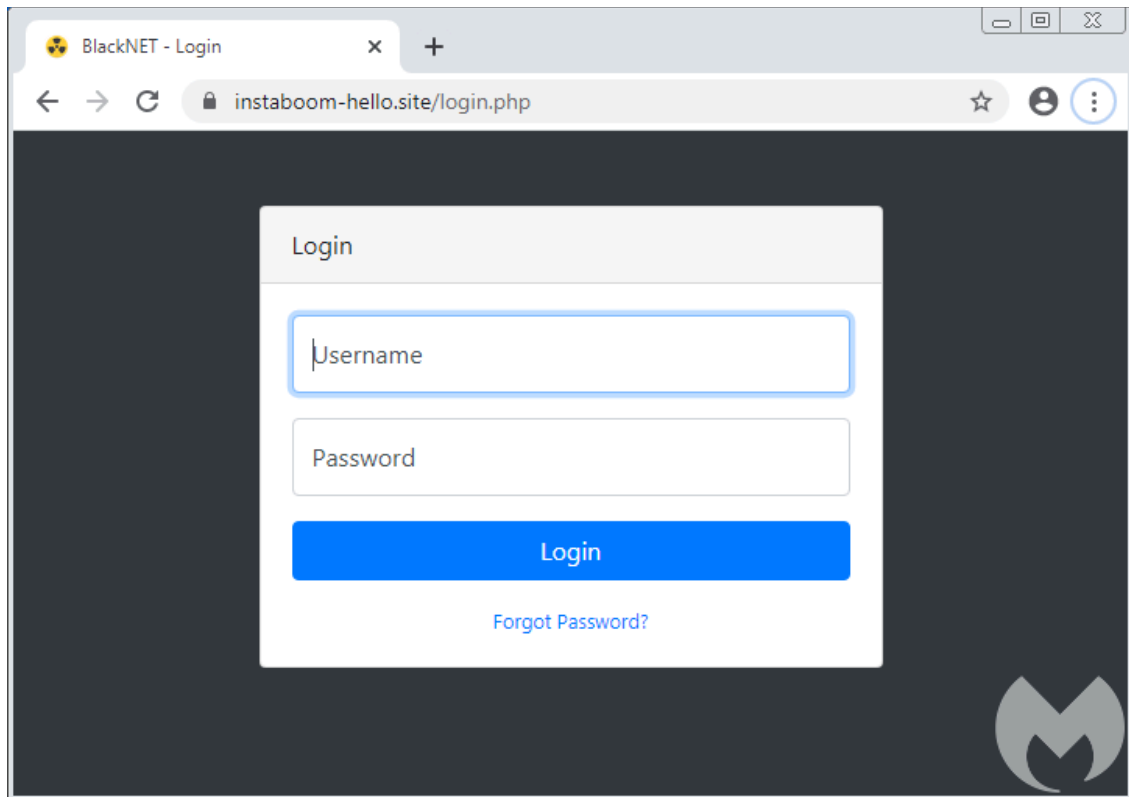


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

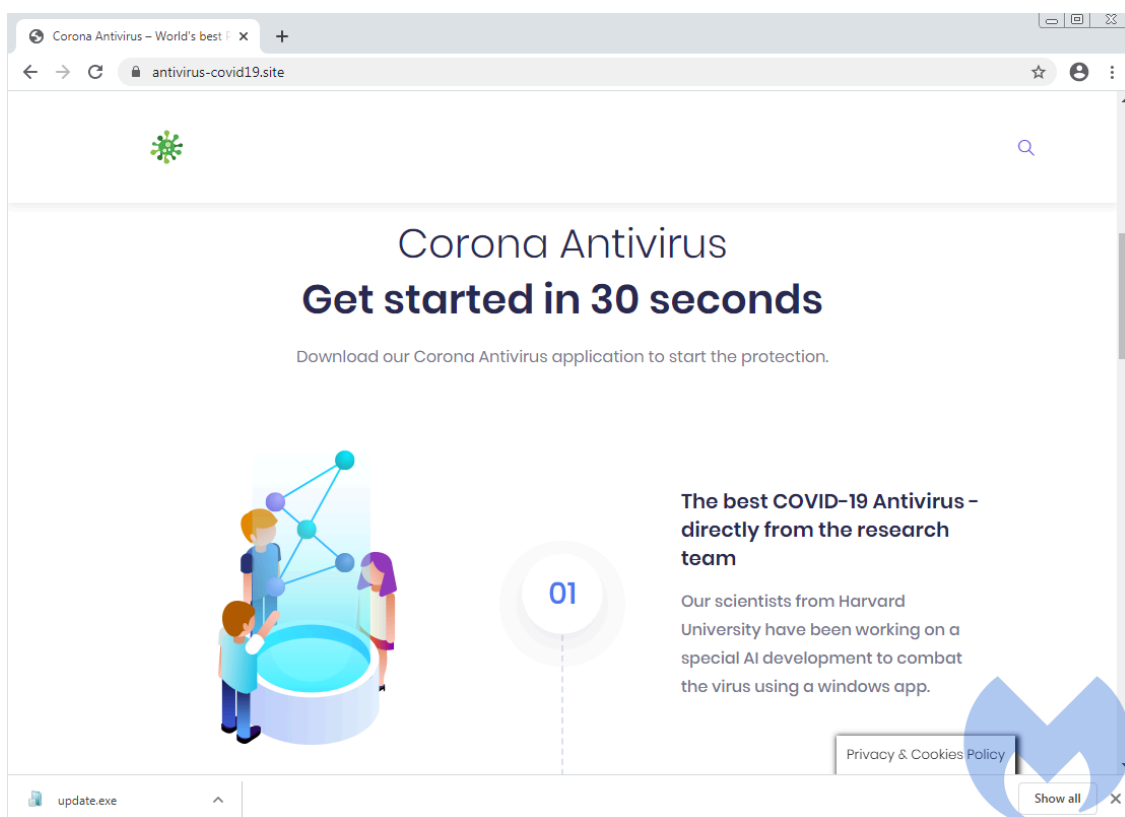
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

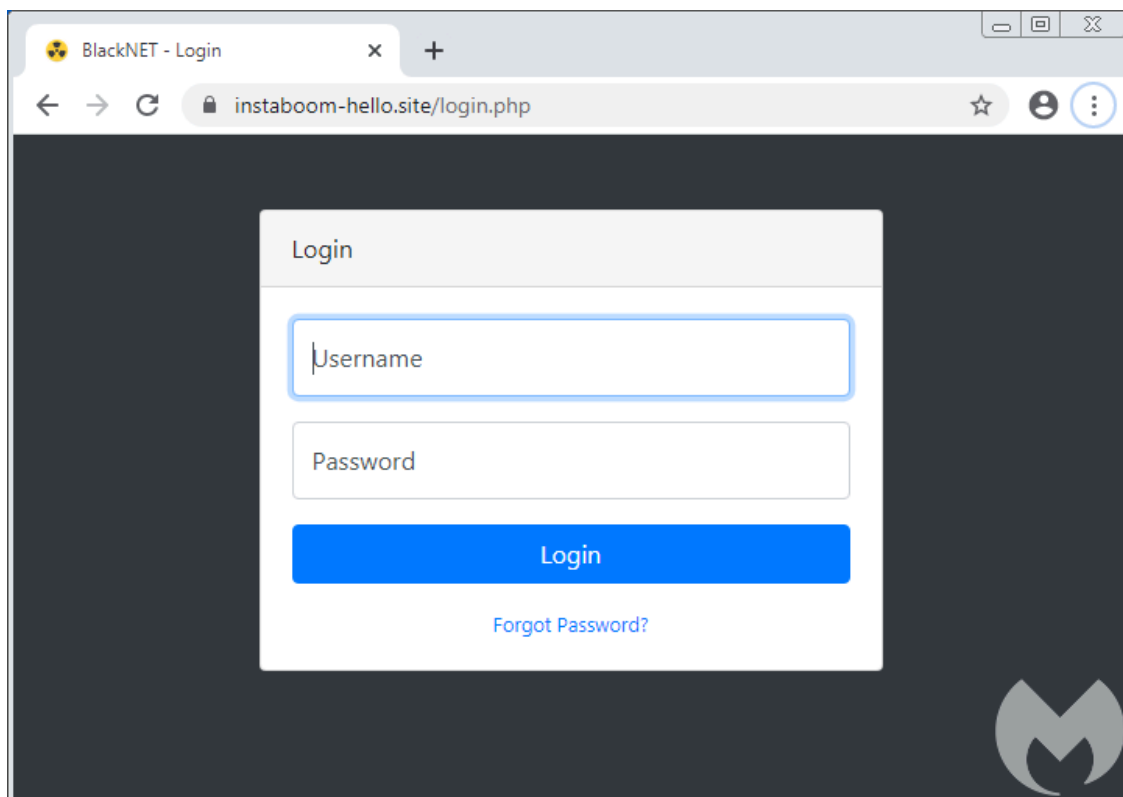


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

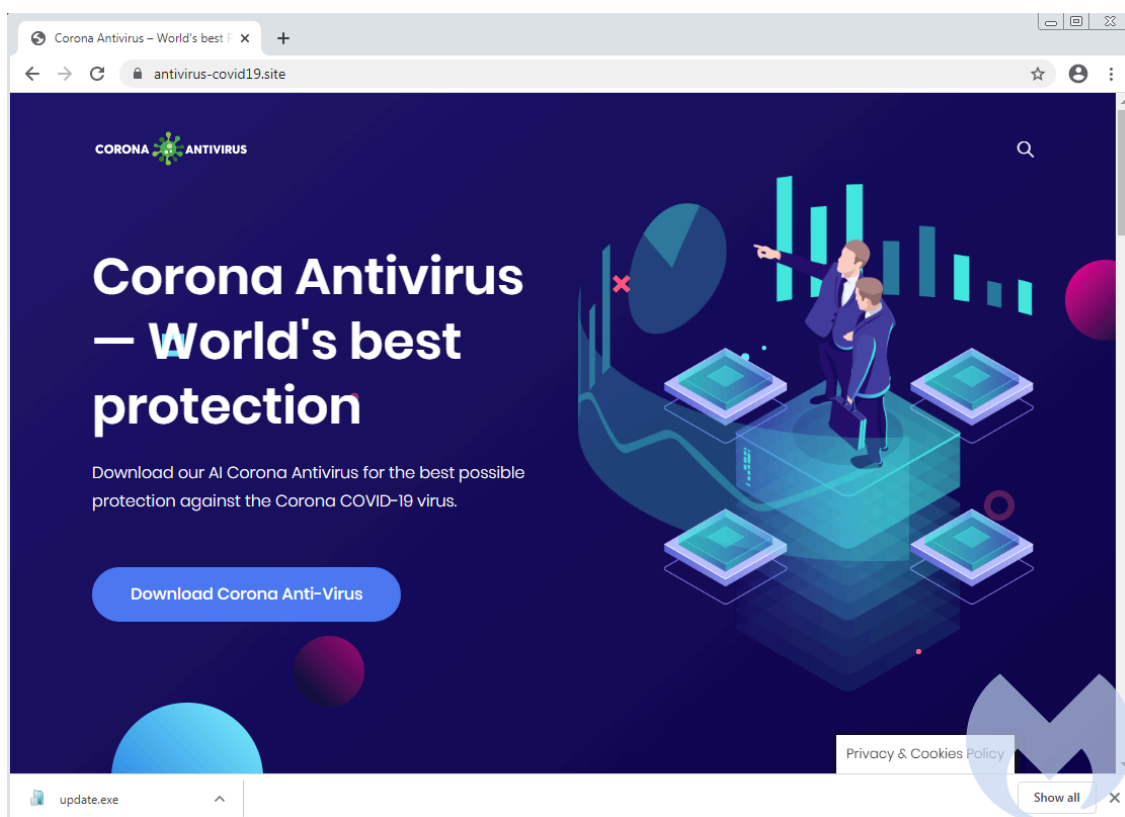
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

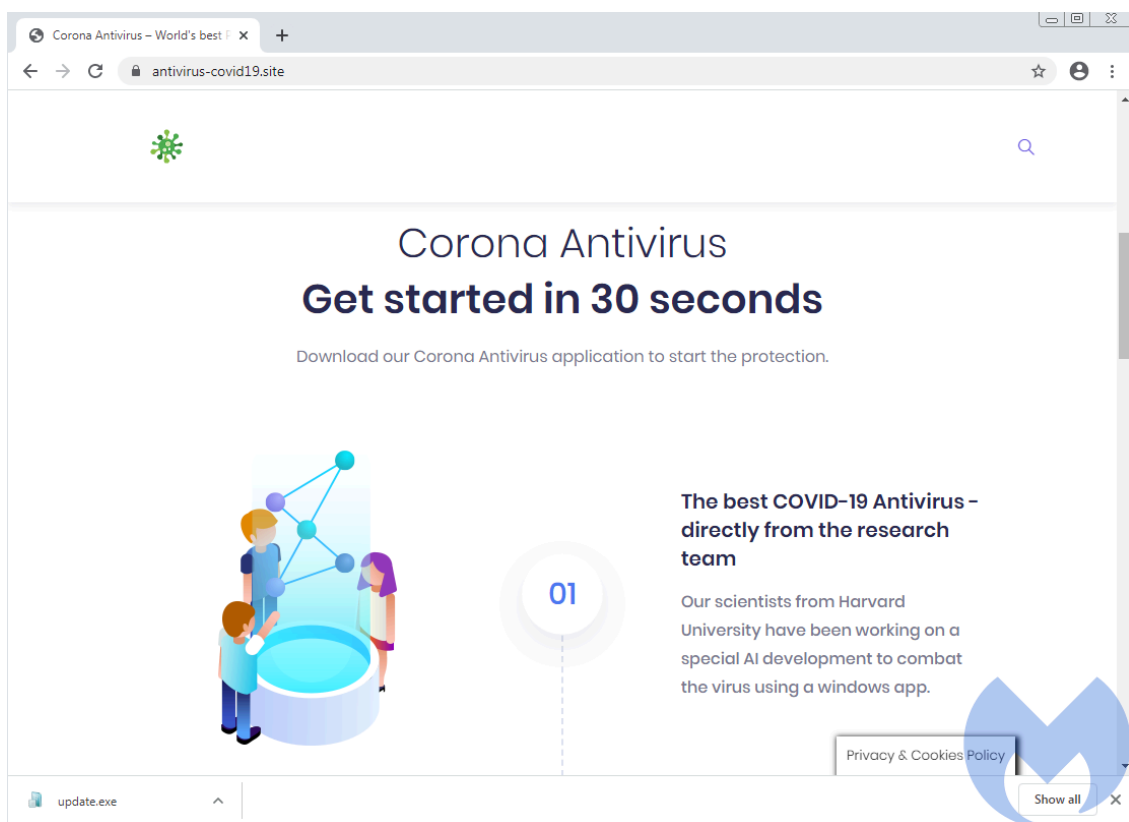
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

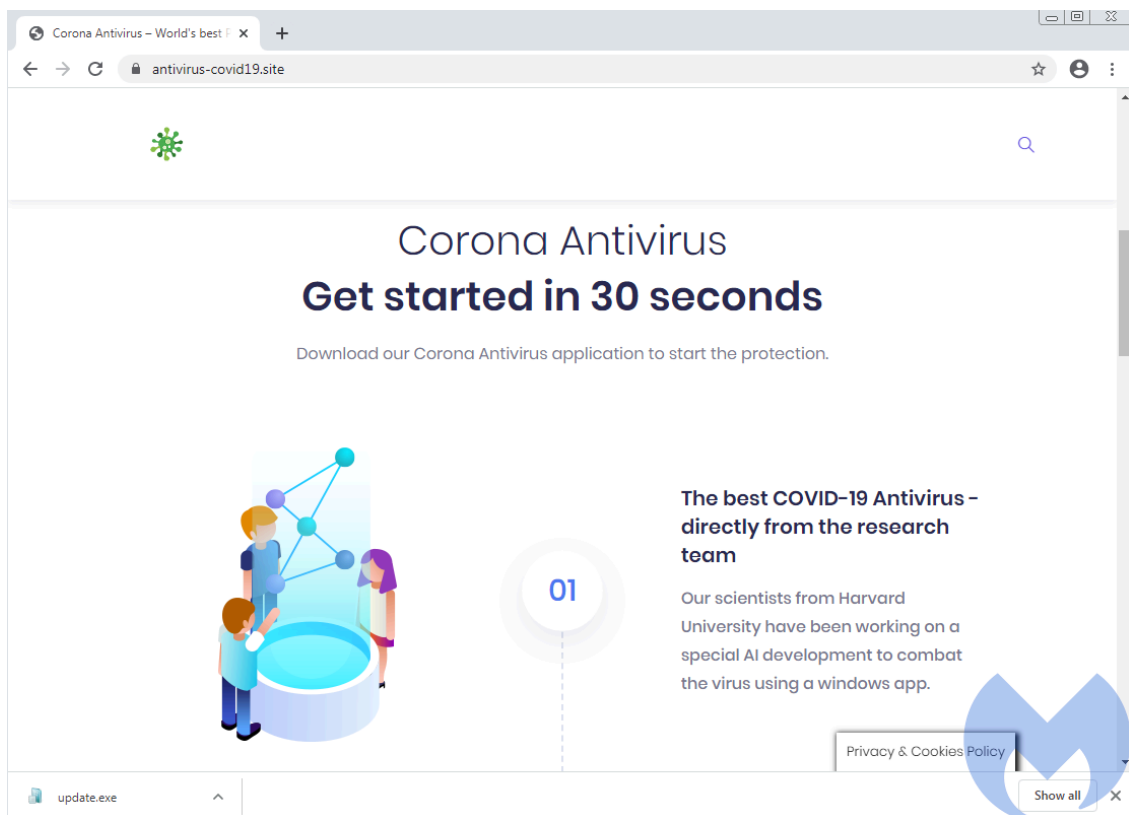
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

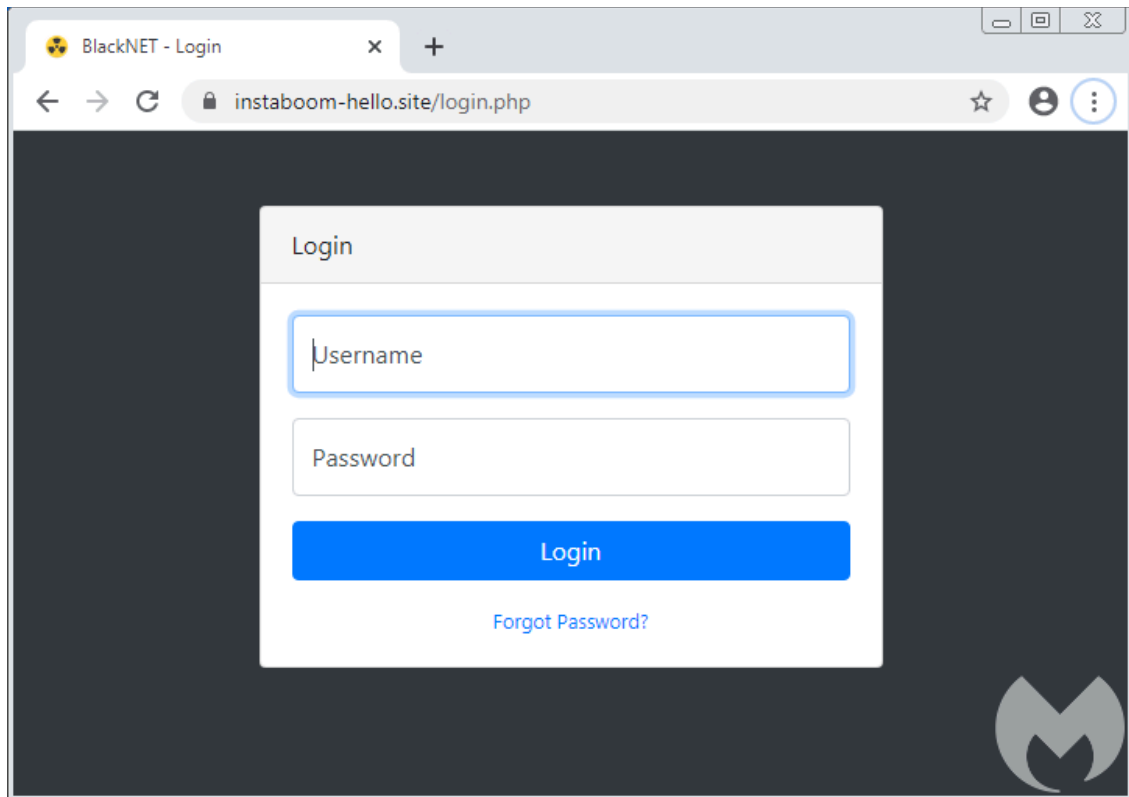


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

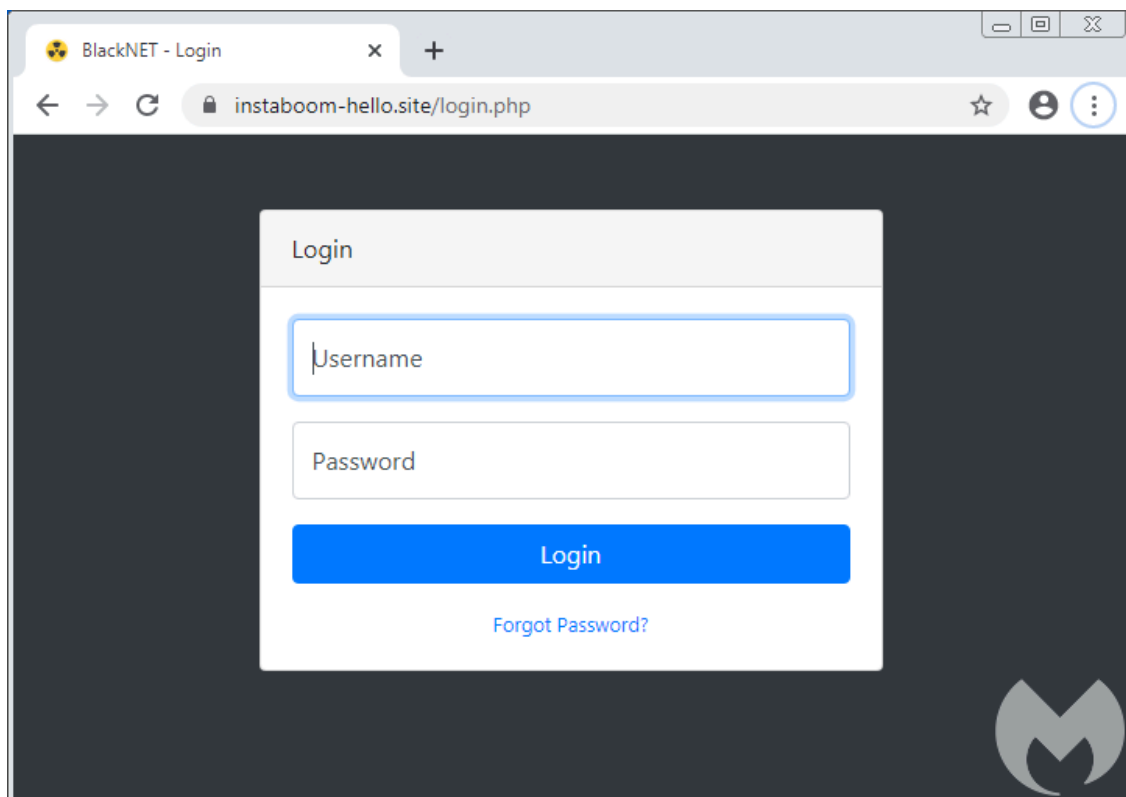
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

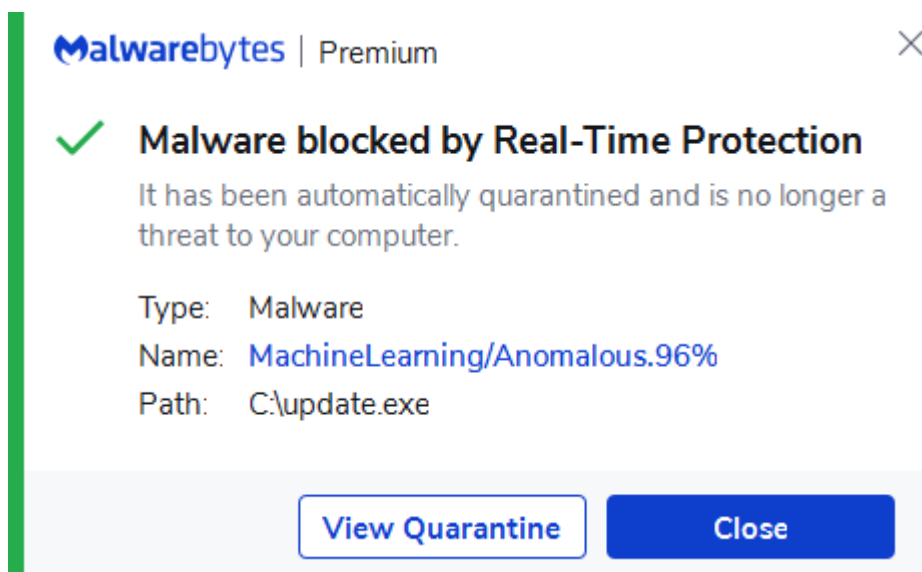
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

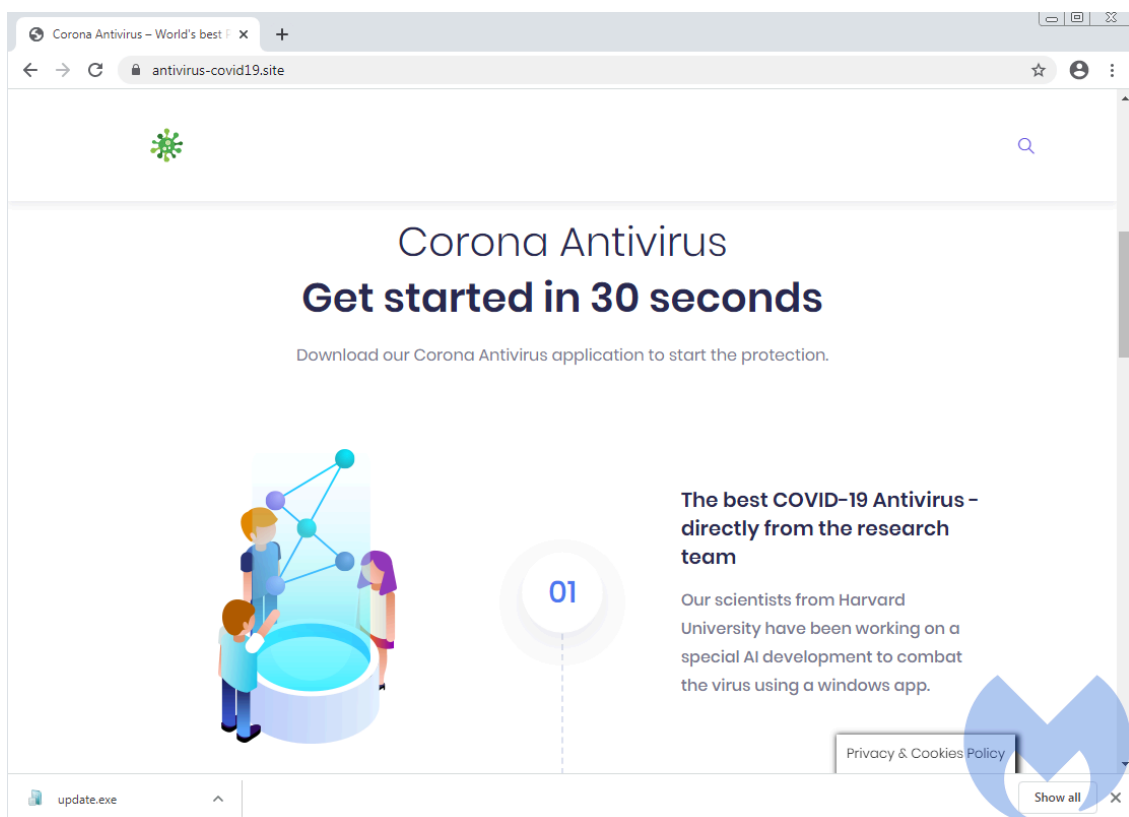
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

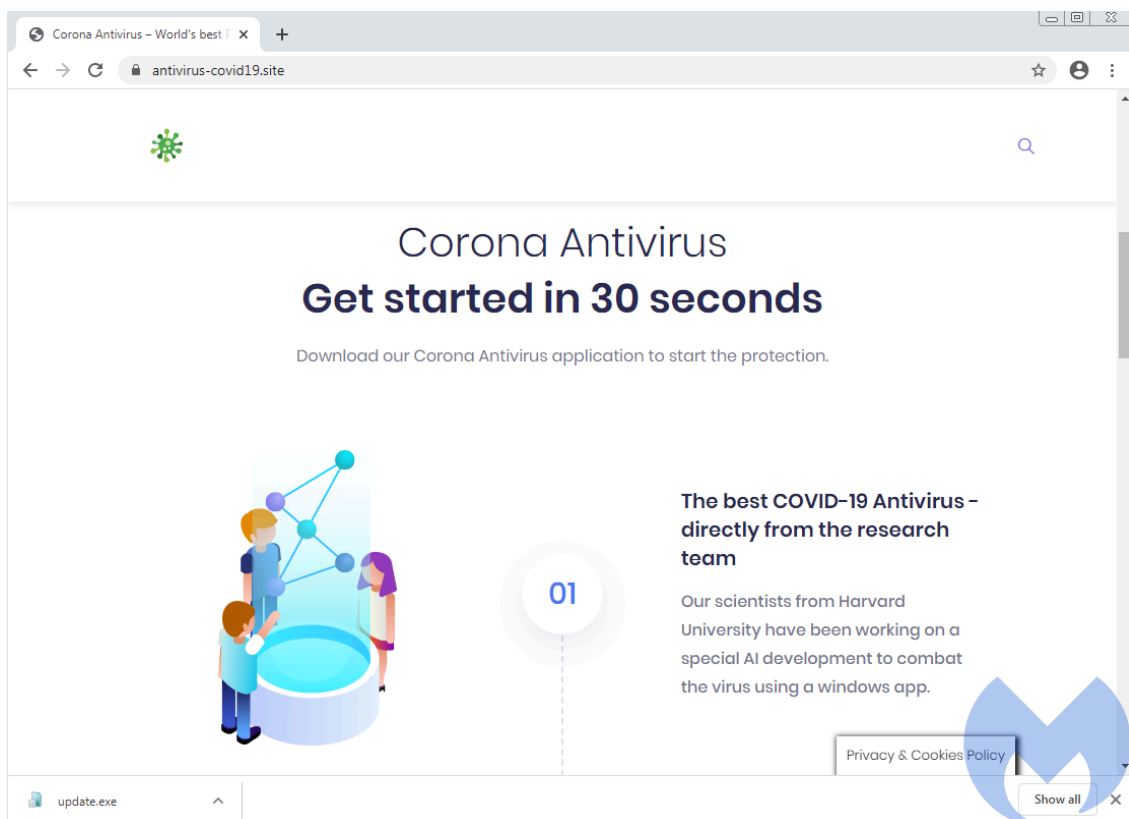
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

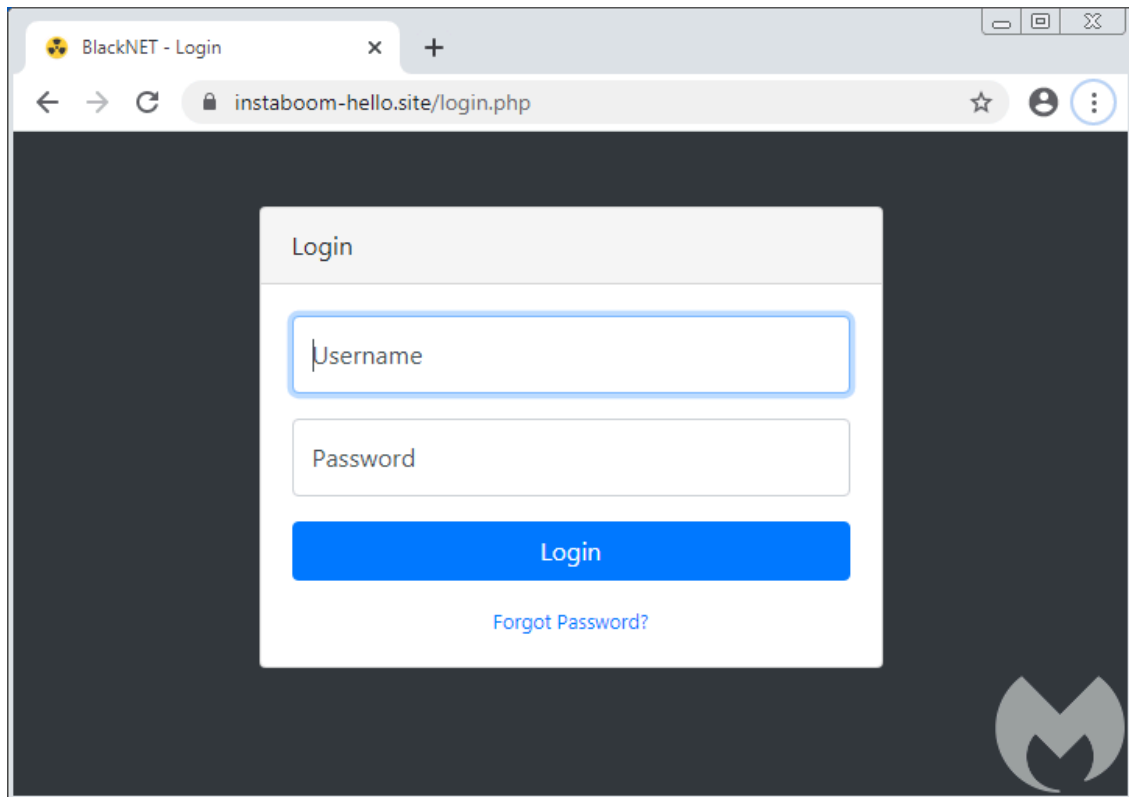


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

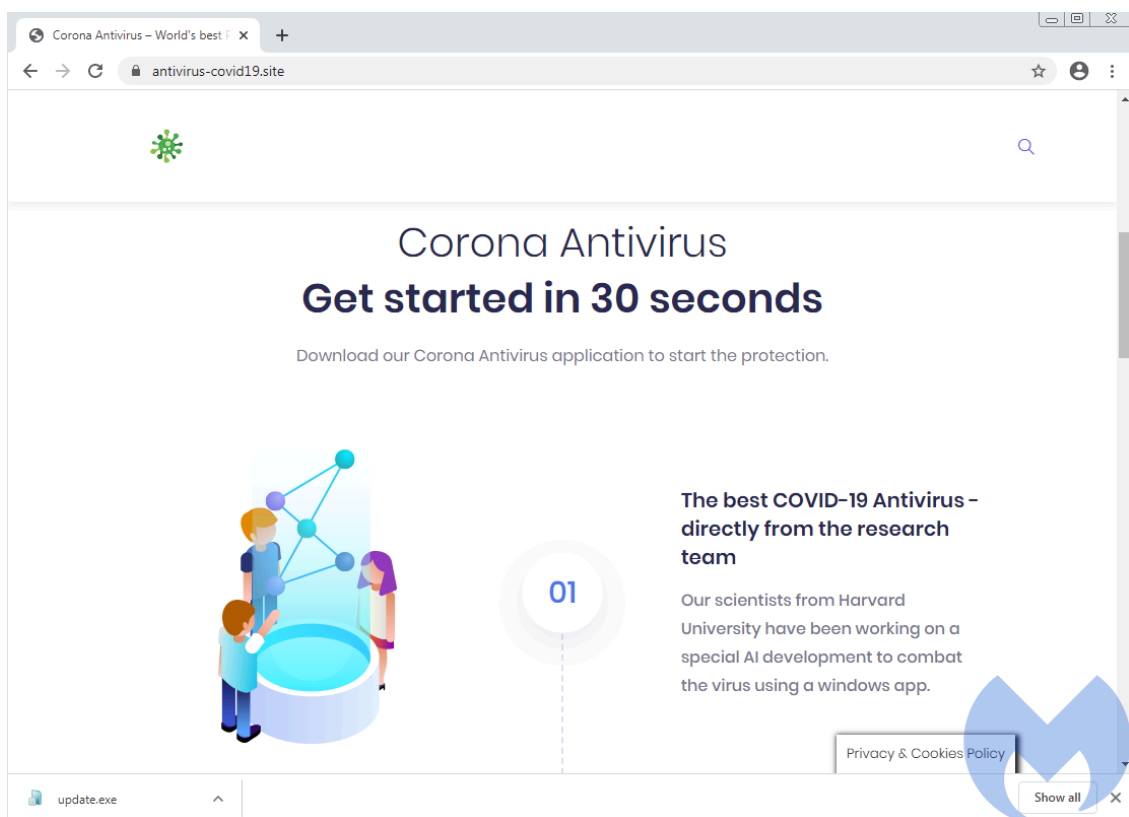
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

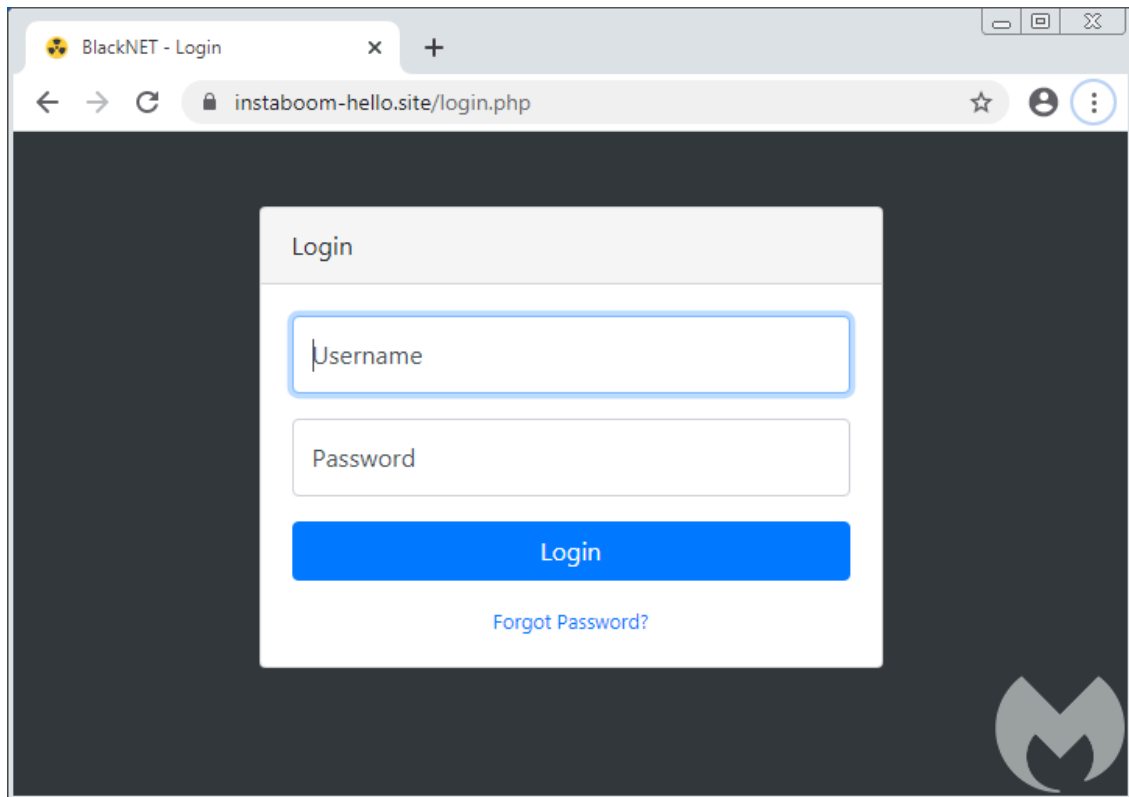


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this are two warning banners: one about logging in as 'admin' and another about two-factor authentication. The main content area is titled 'Slaves Menu' and contains four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the right of the table are 'Previous' and 'Next' buttons. Below the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right of the commands center is a 'Map Visualization' section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

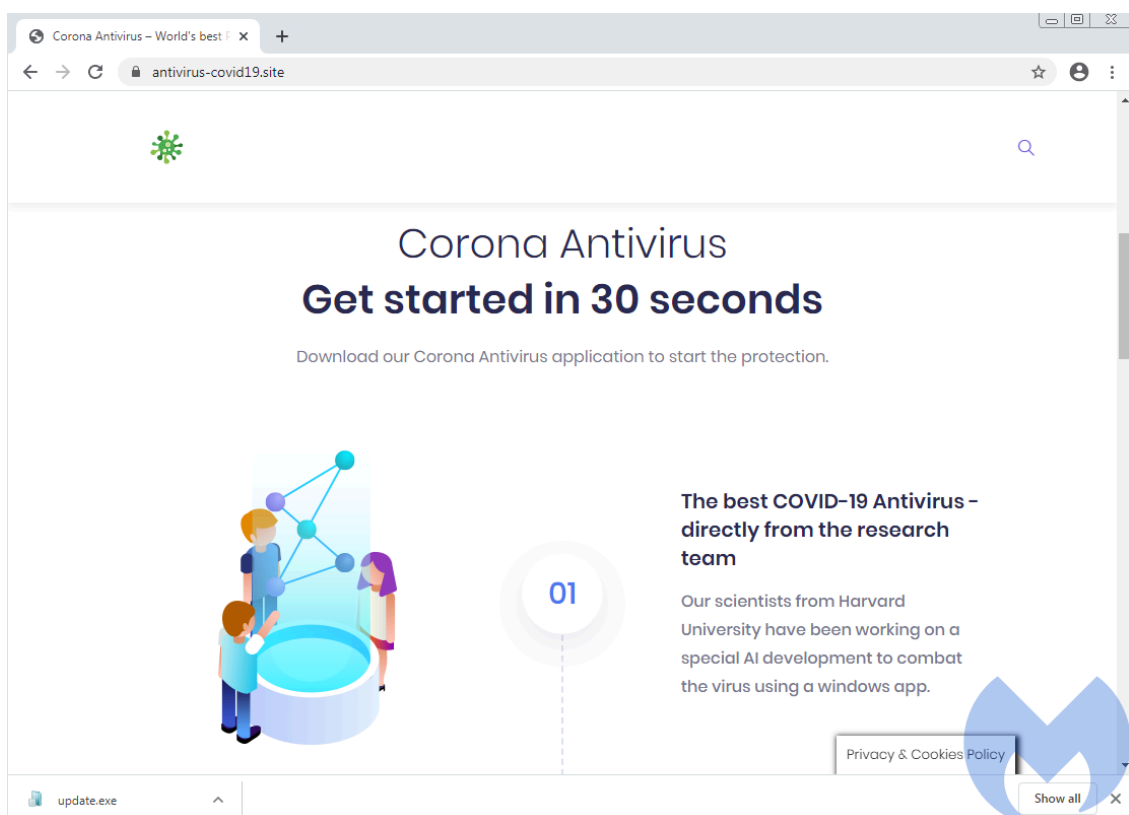
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

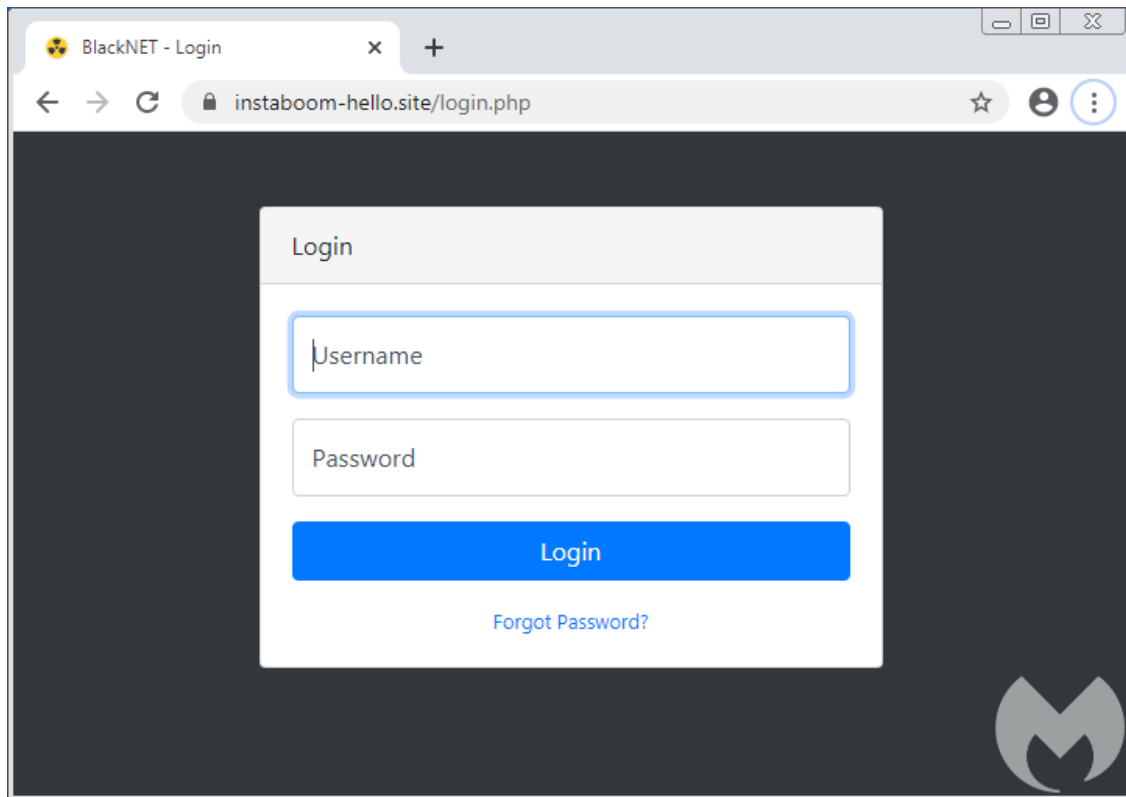


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

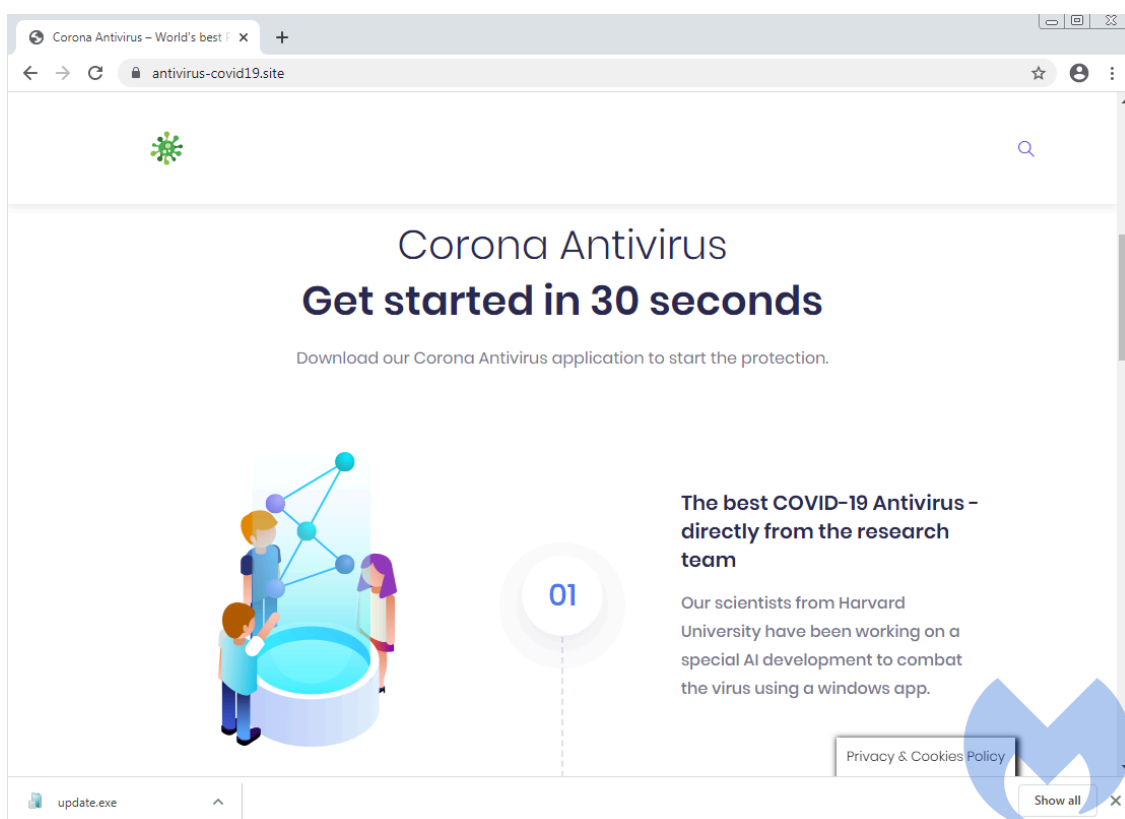
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

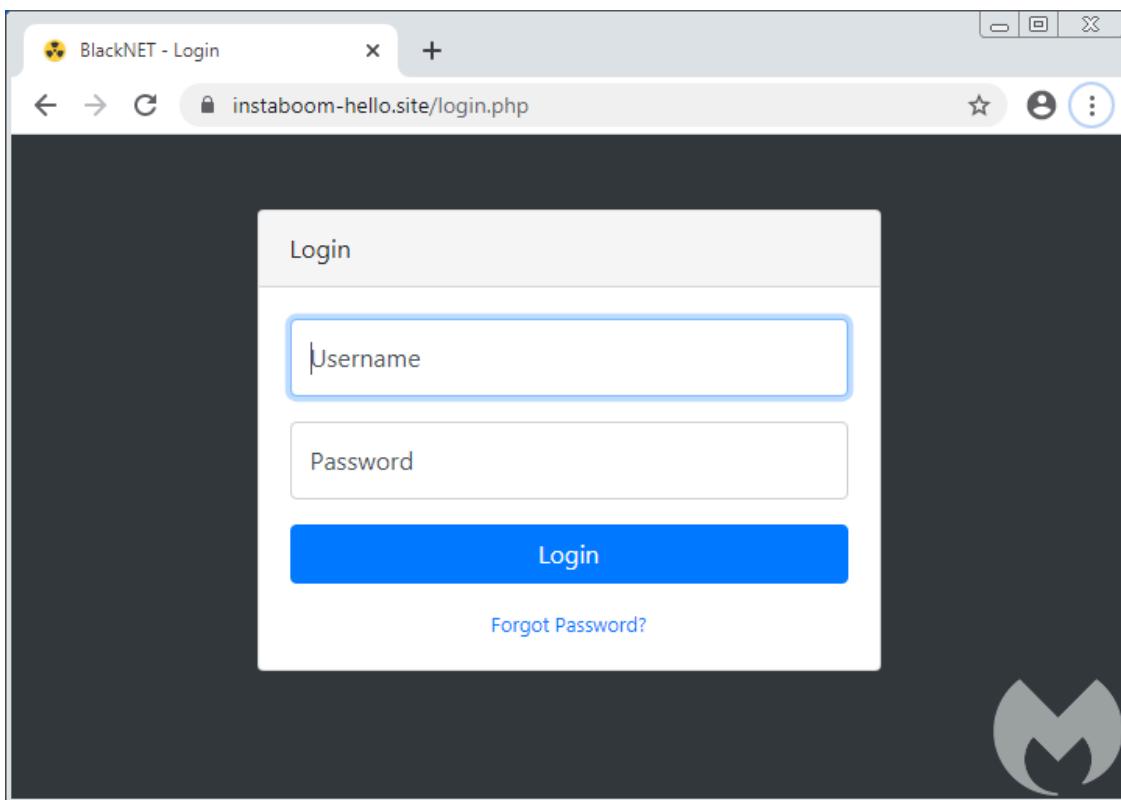


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

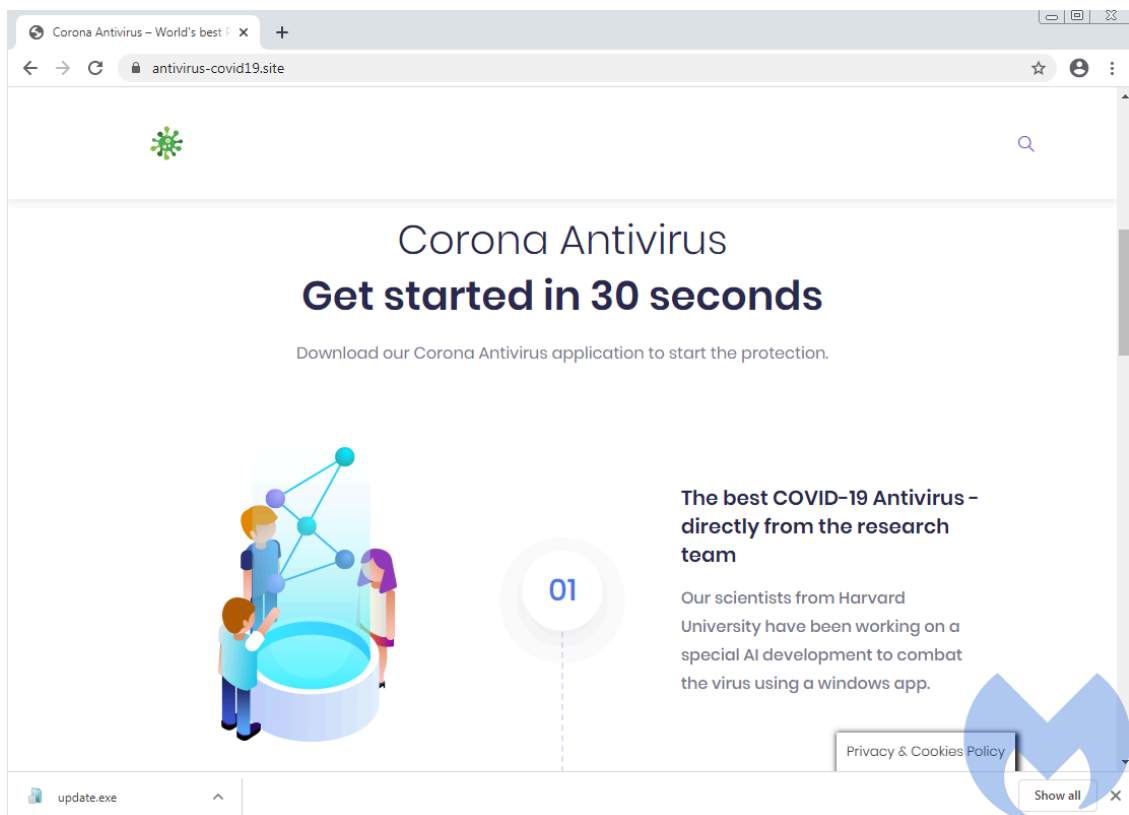
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

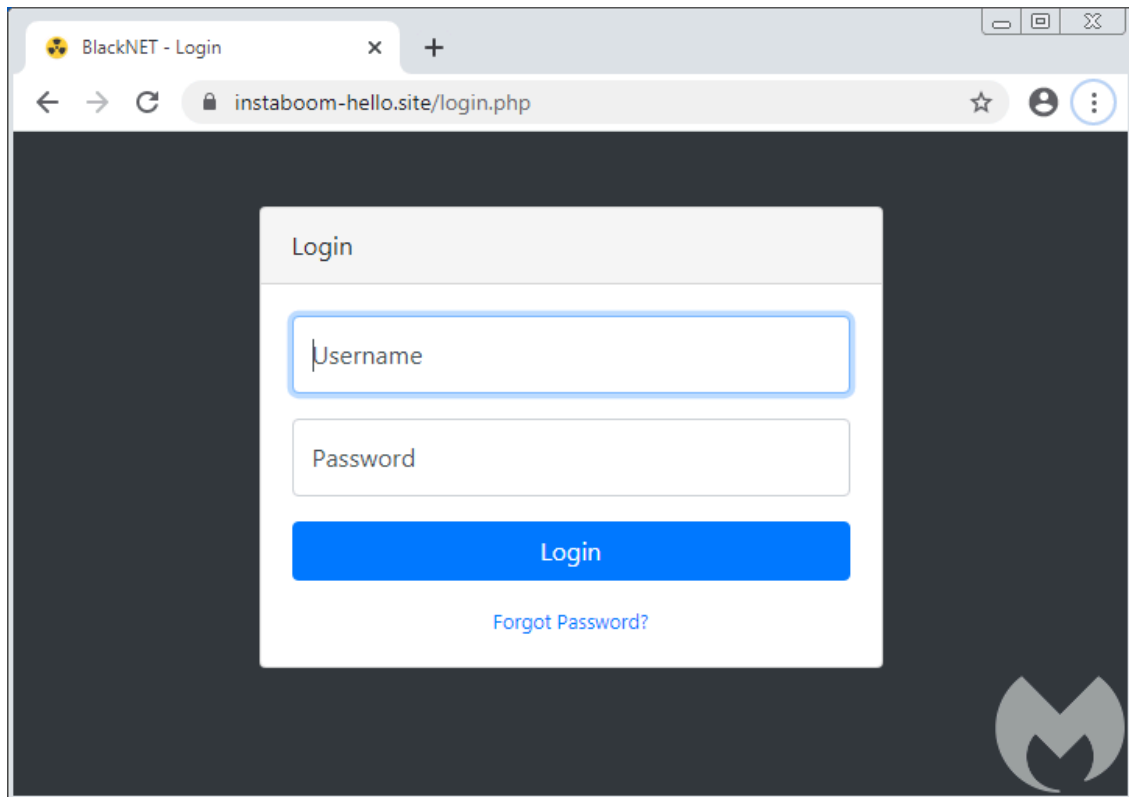


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

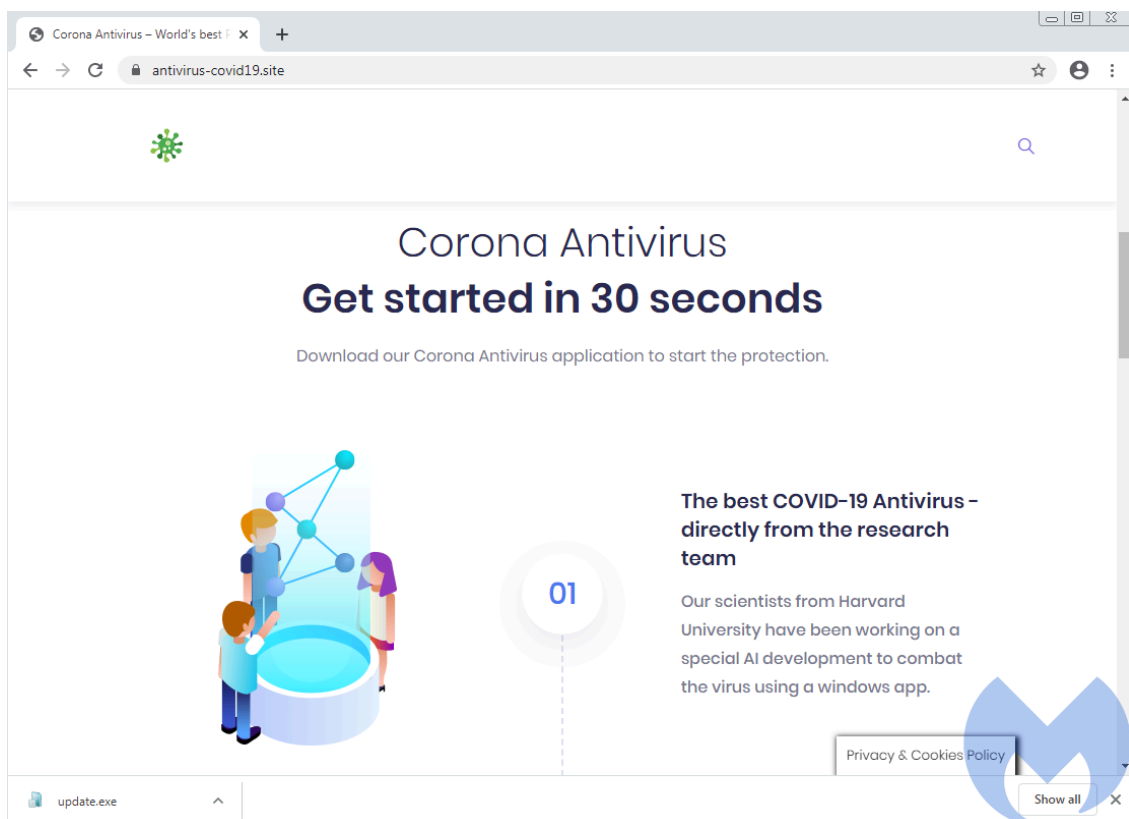
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[:]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[:]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

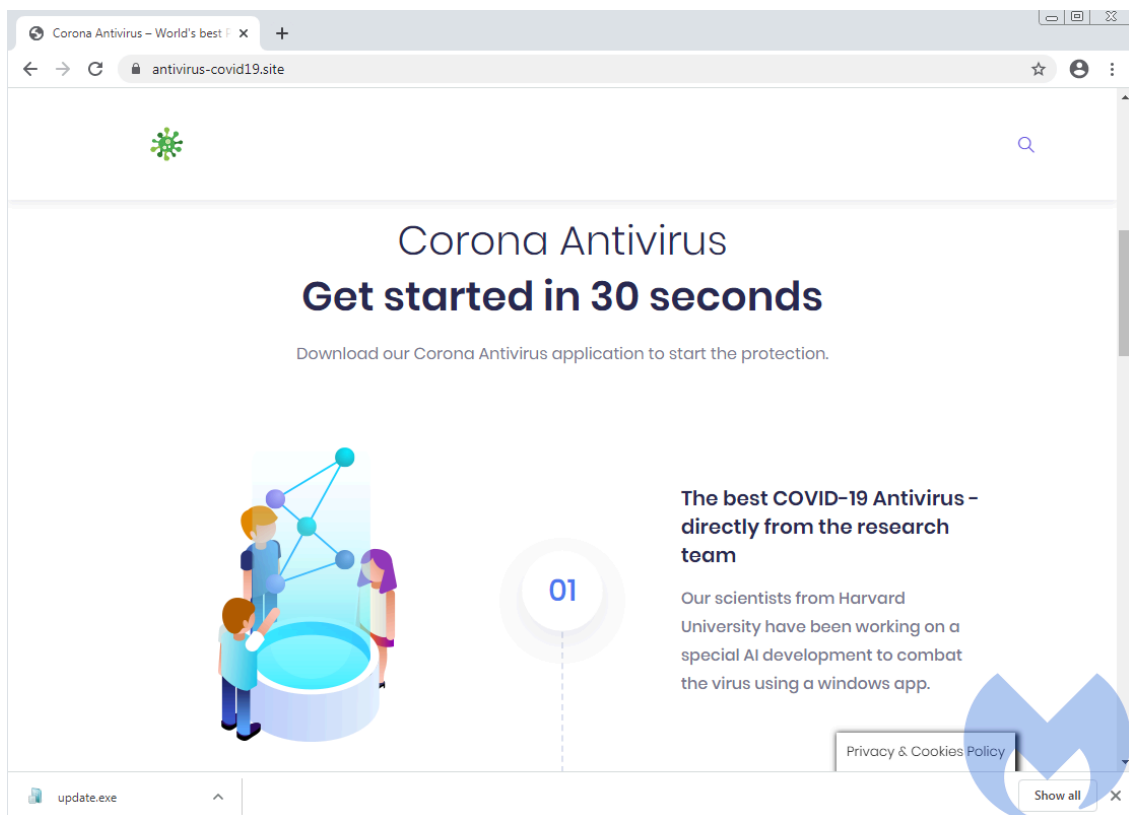
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

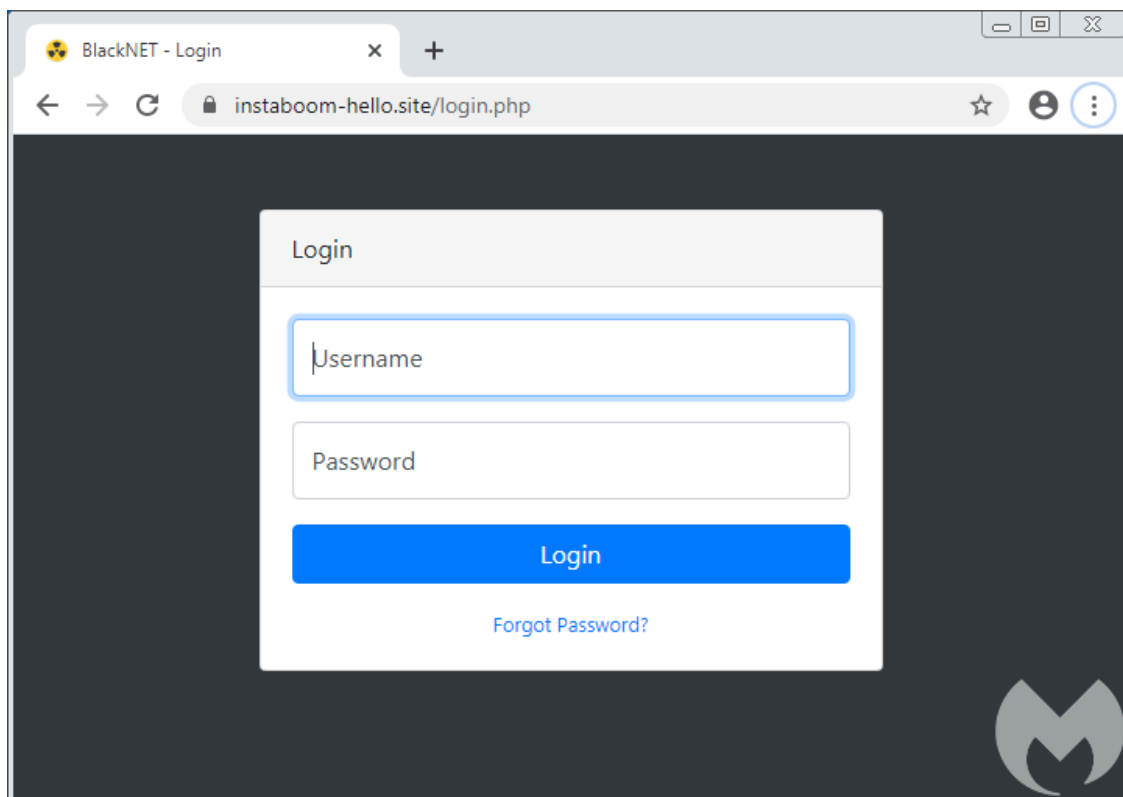
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

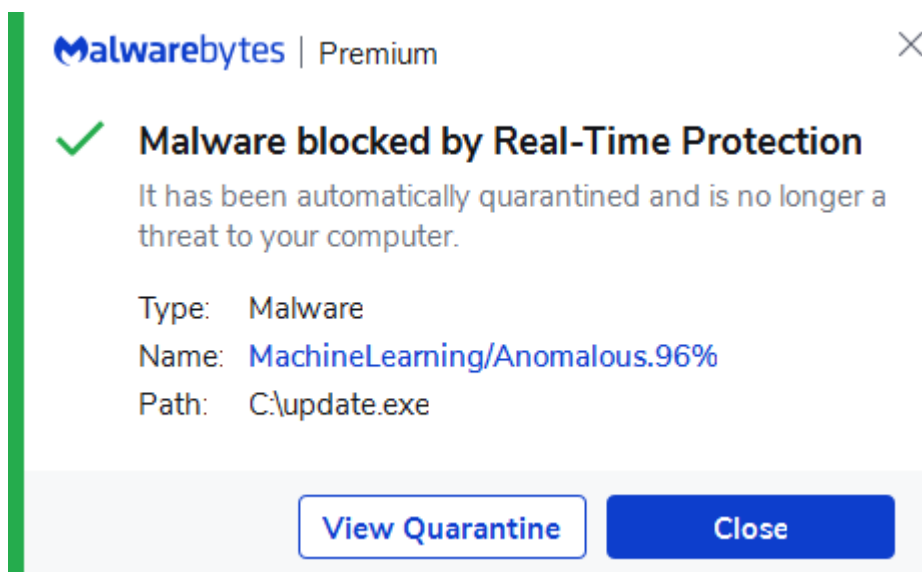
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

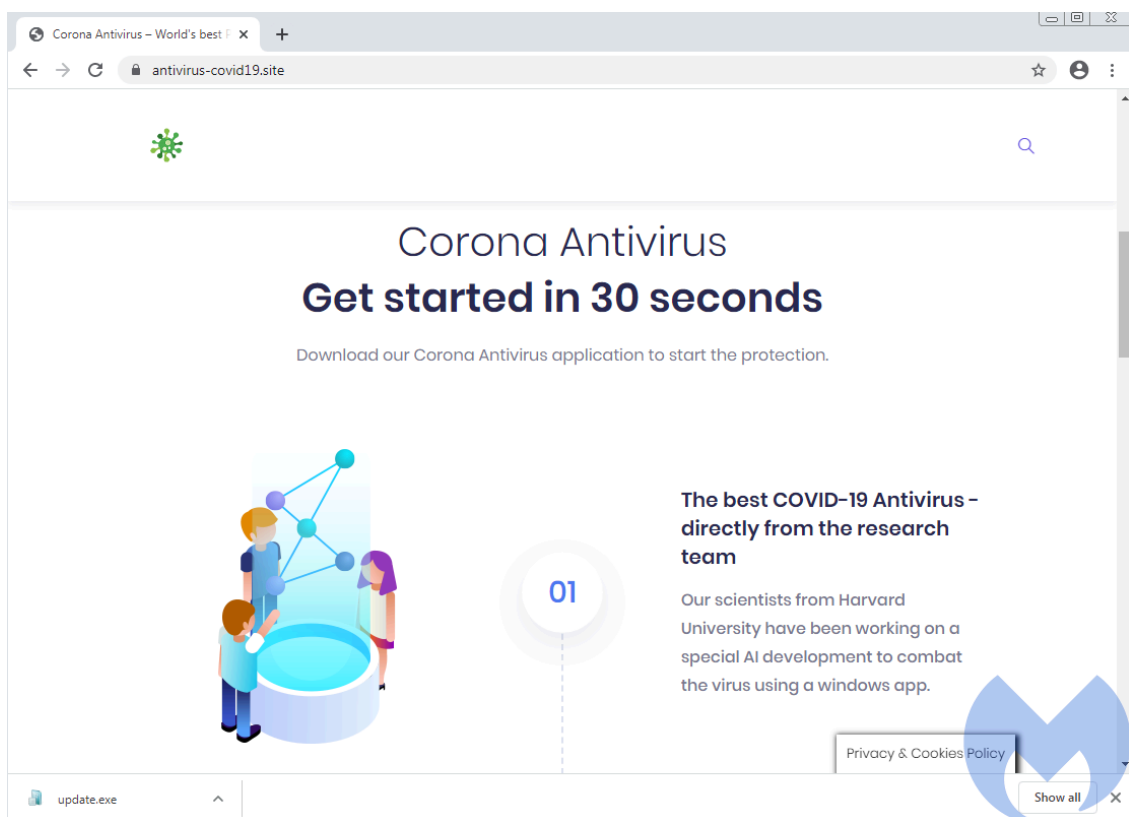
C2 panel

```
instaboom-hello[.]site
```




To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

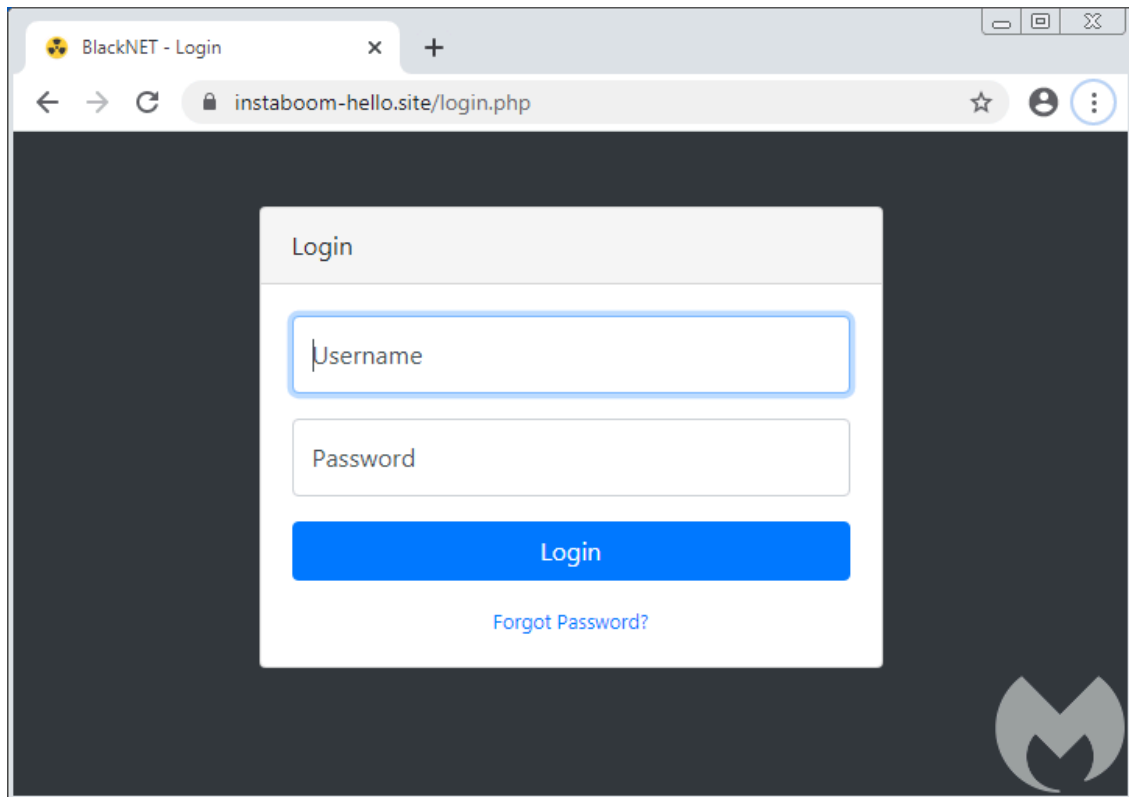


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

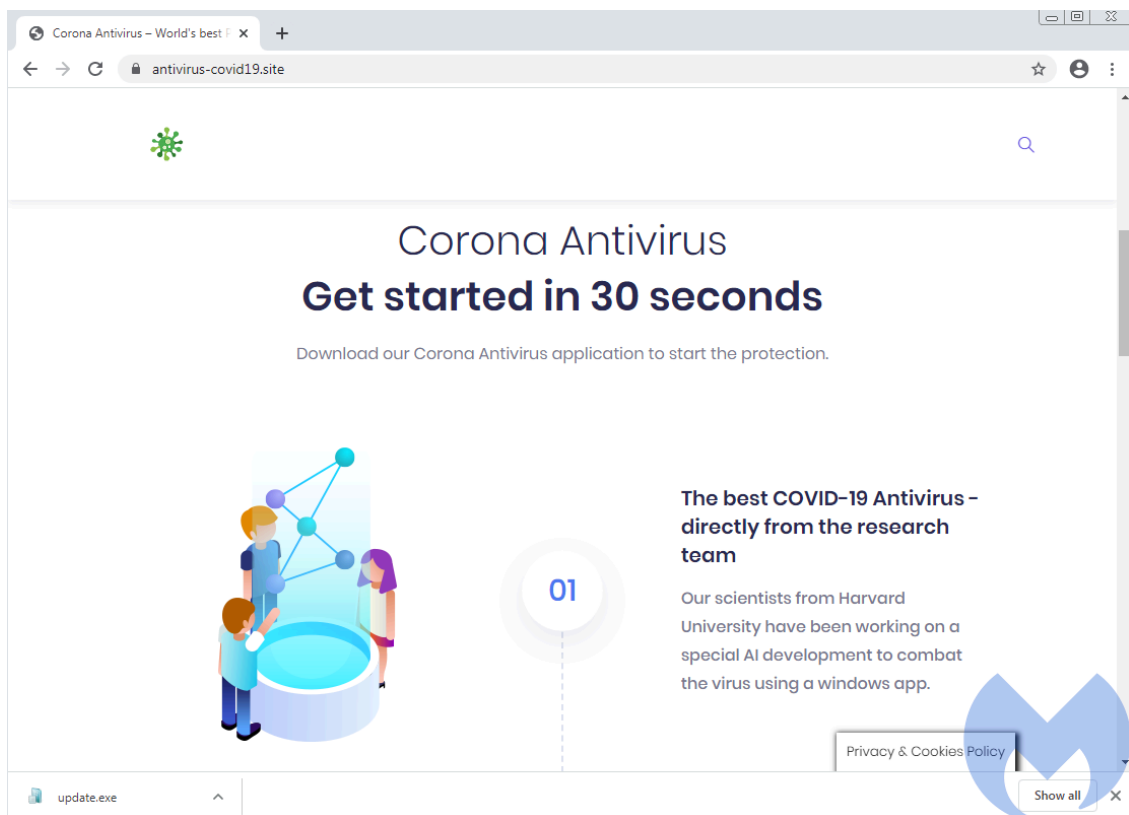
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

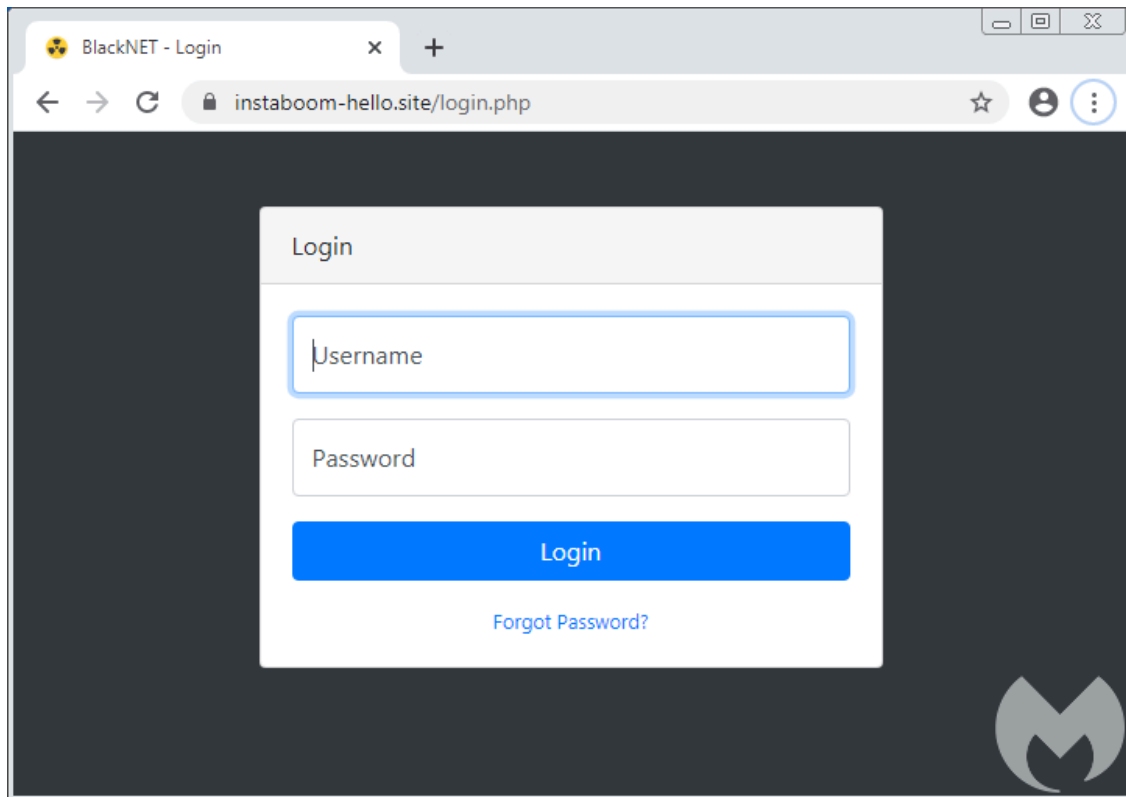


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

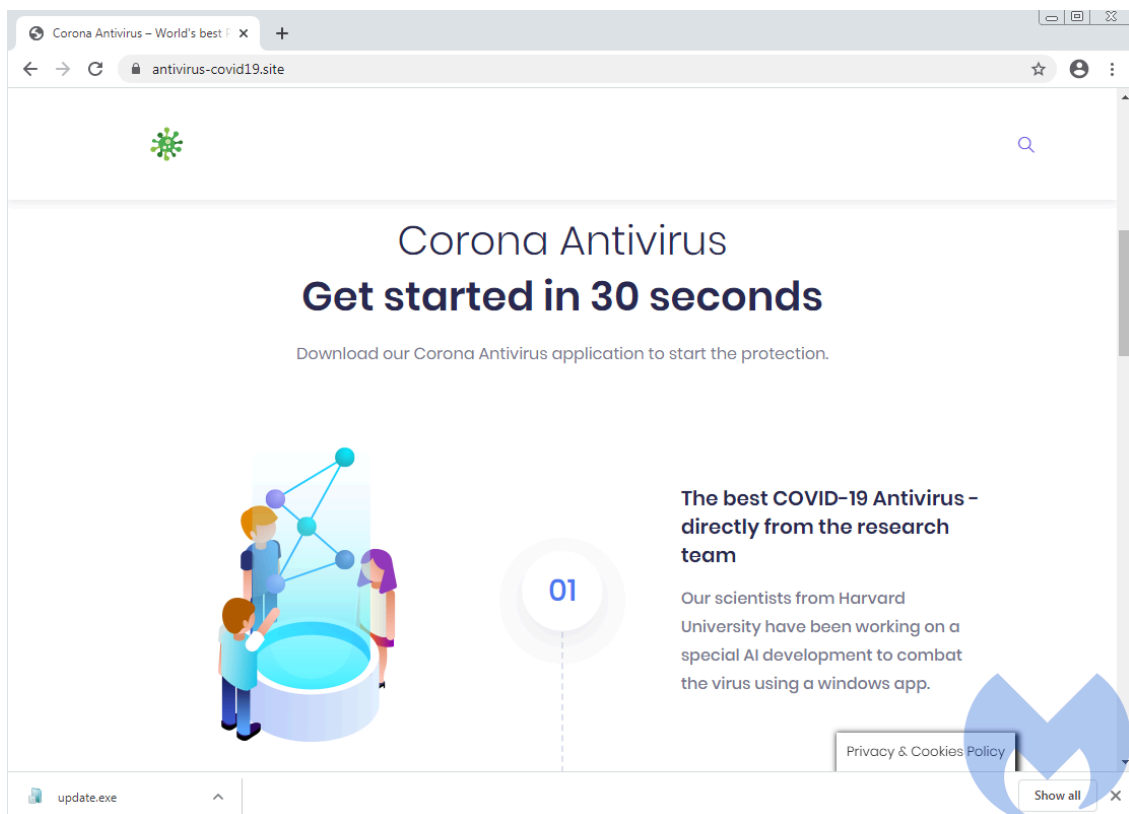
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

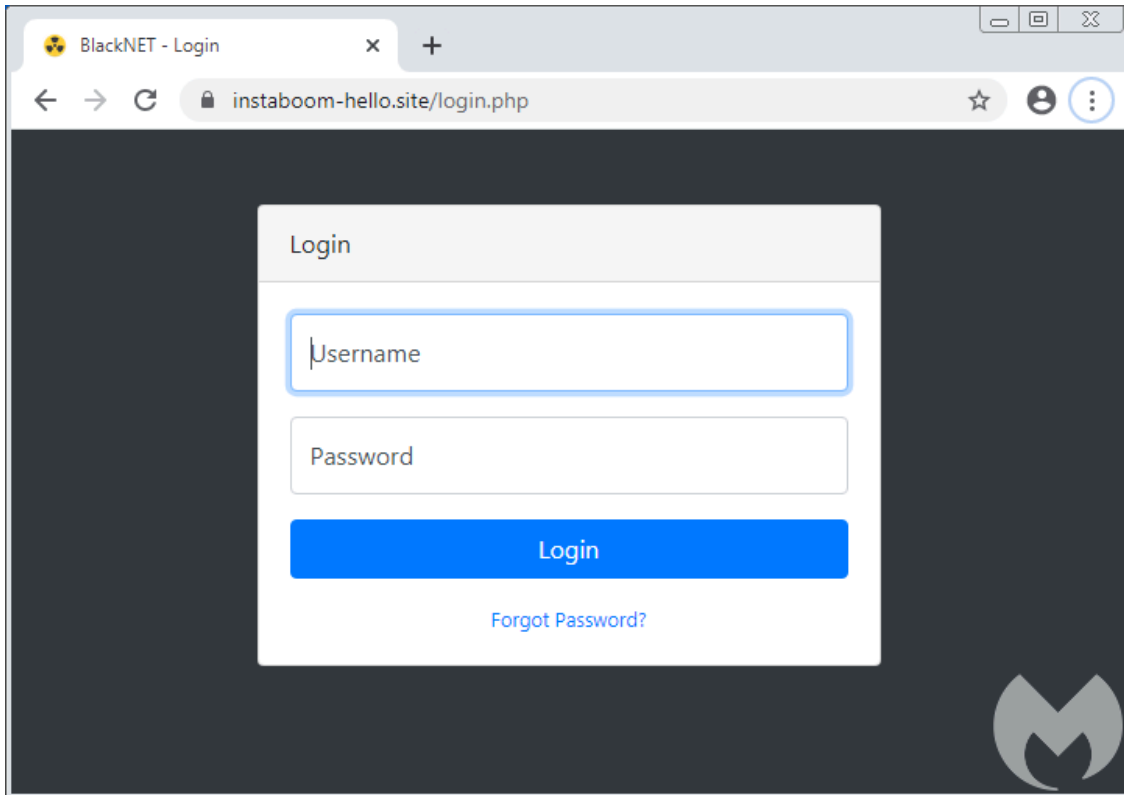


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

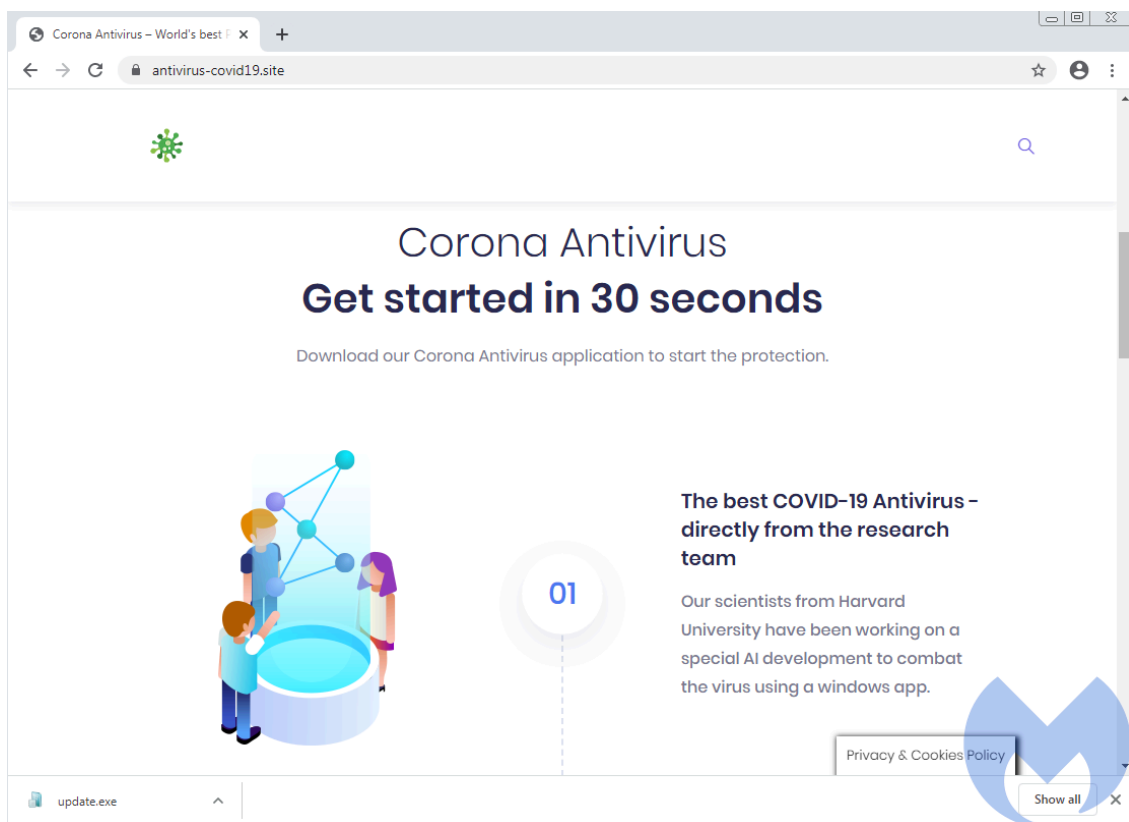
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

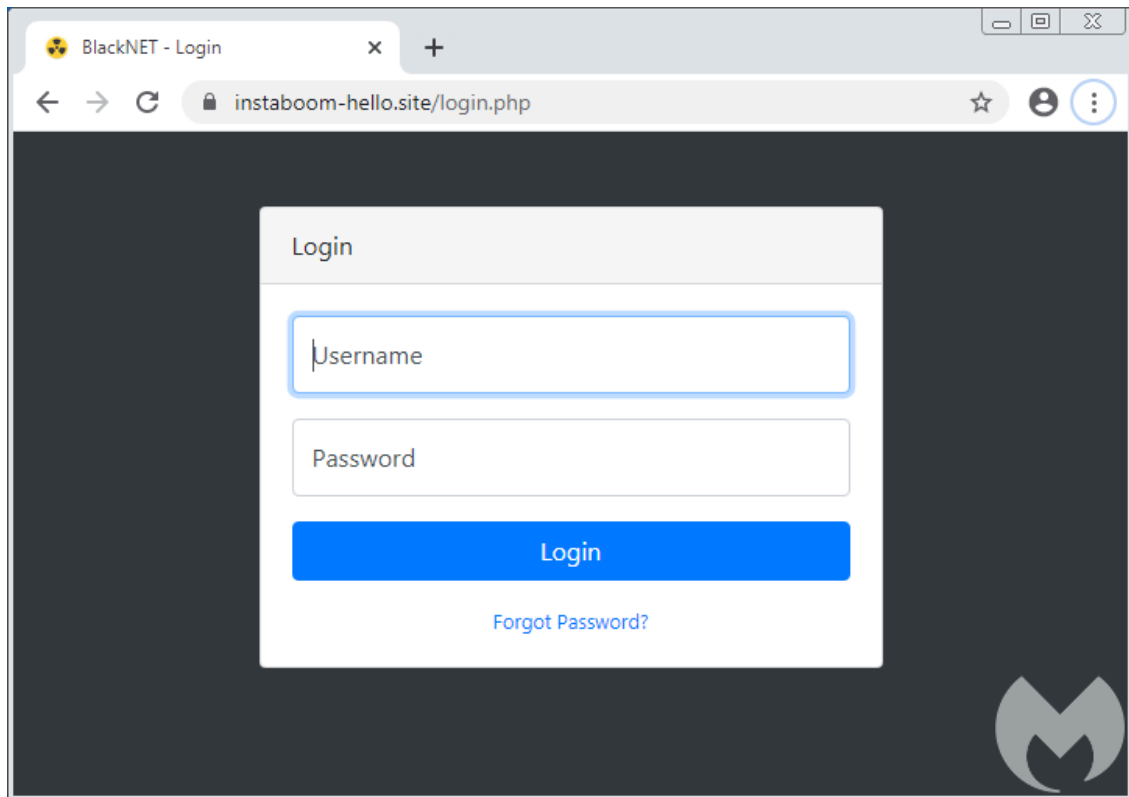


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

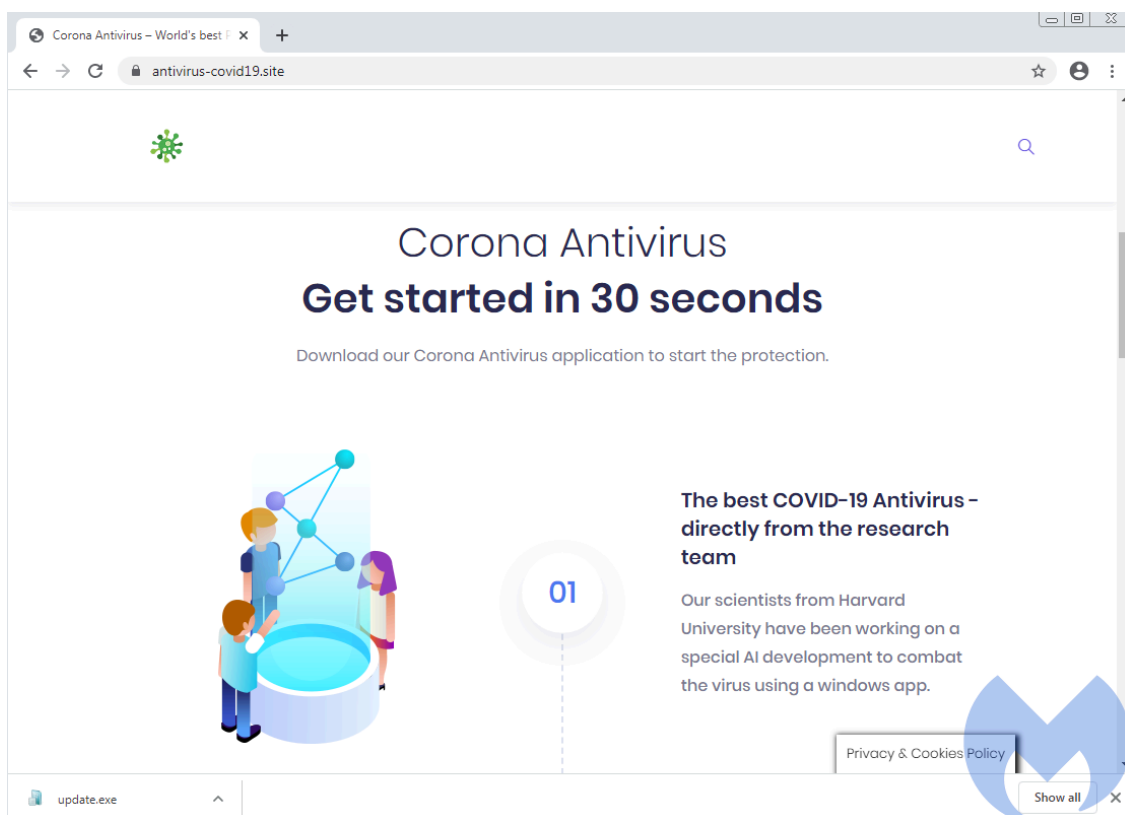
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

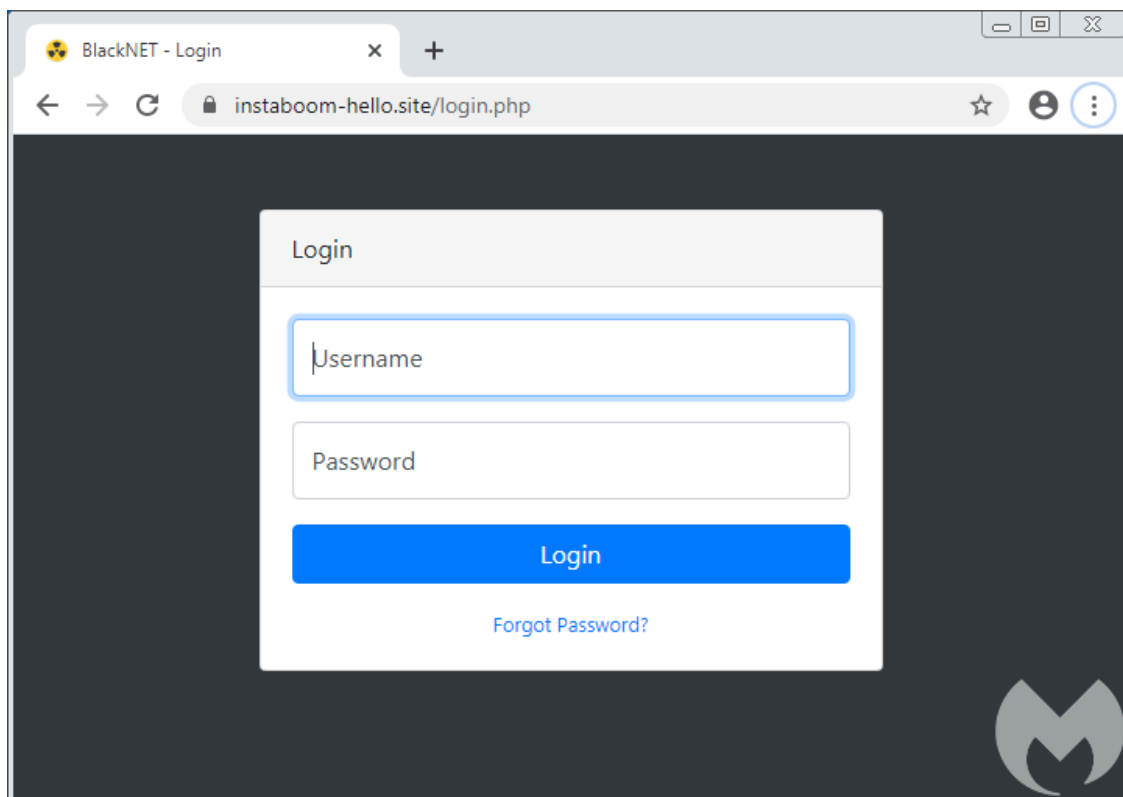
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

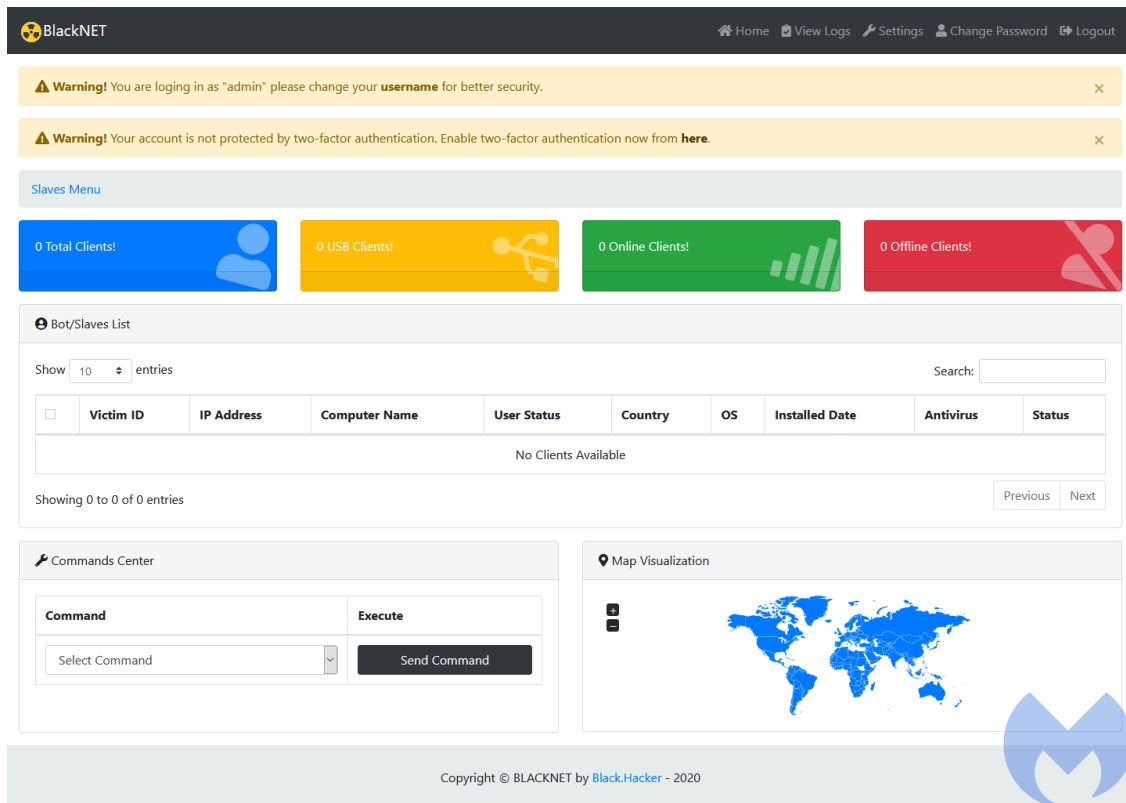
```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

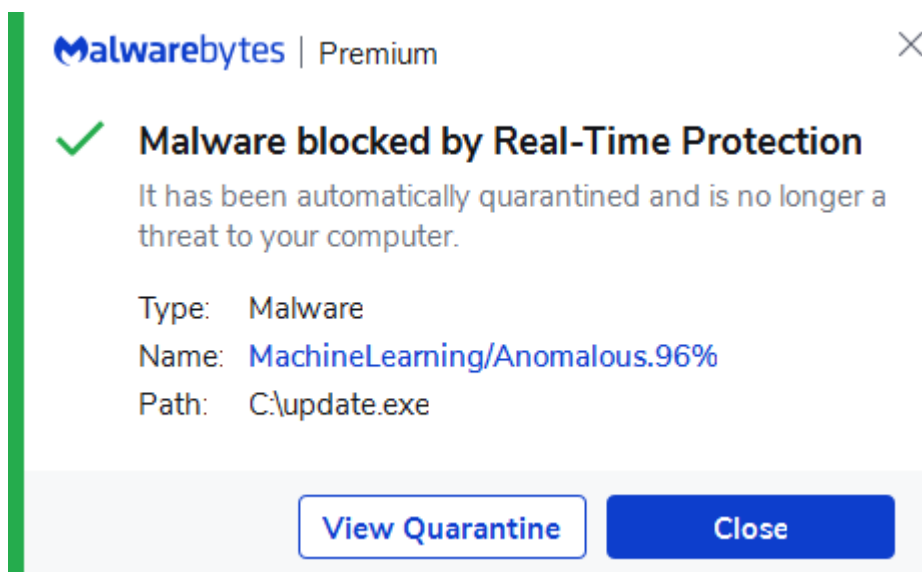


Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

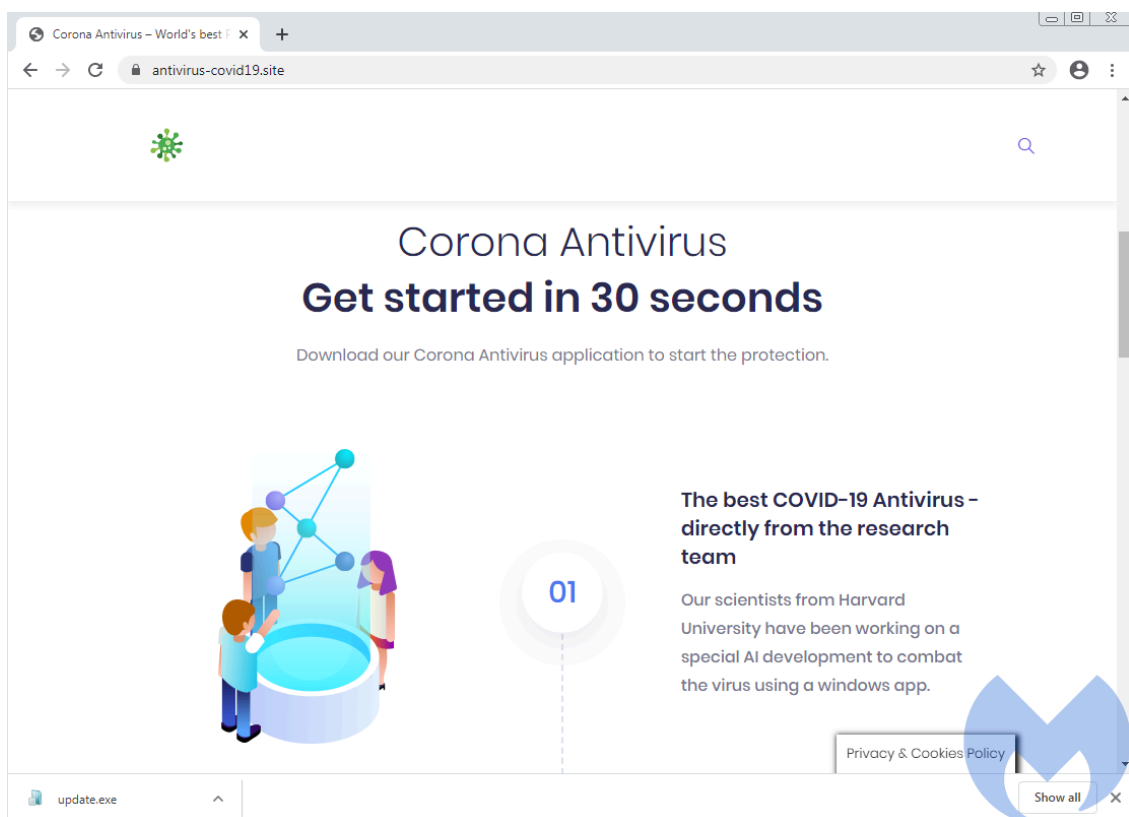
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

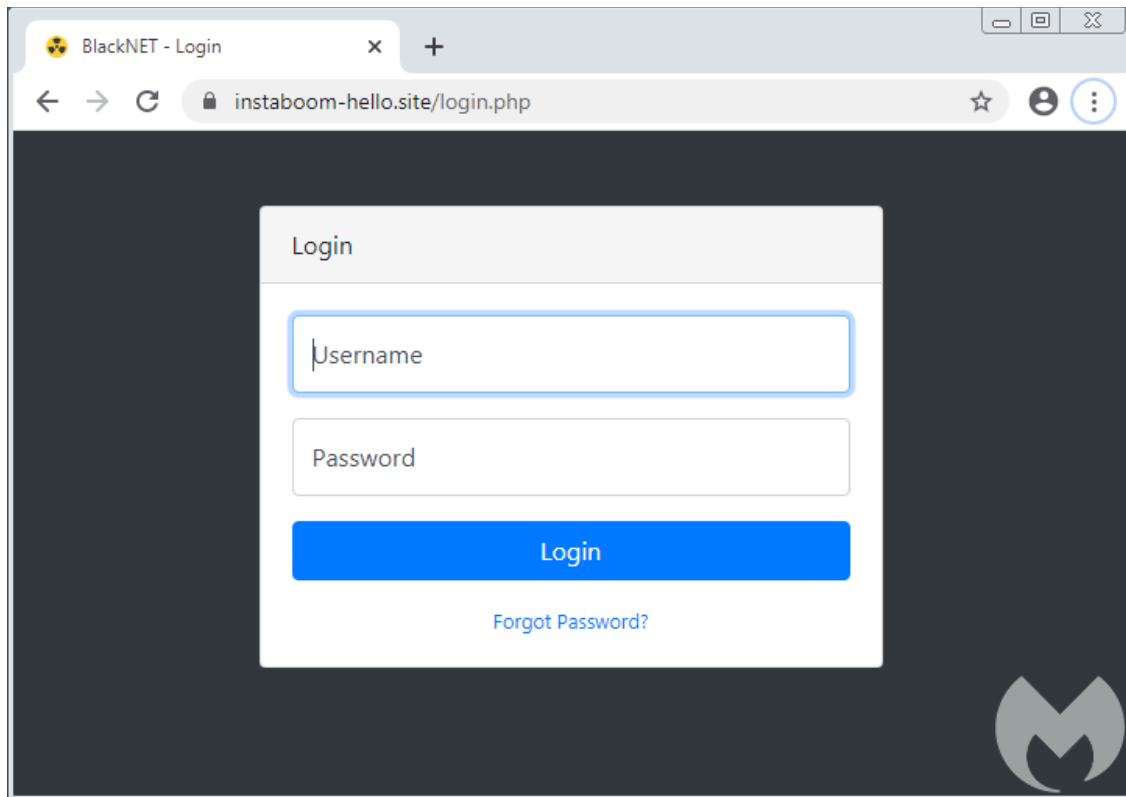



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a blue overlay. The footer contains the copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, the details are listed: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

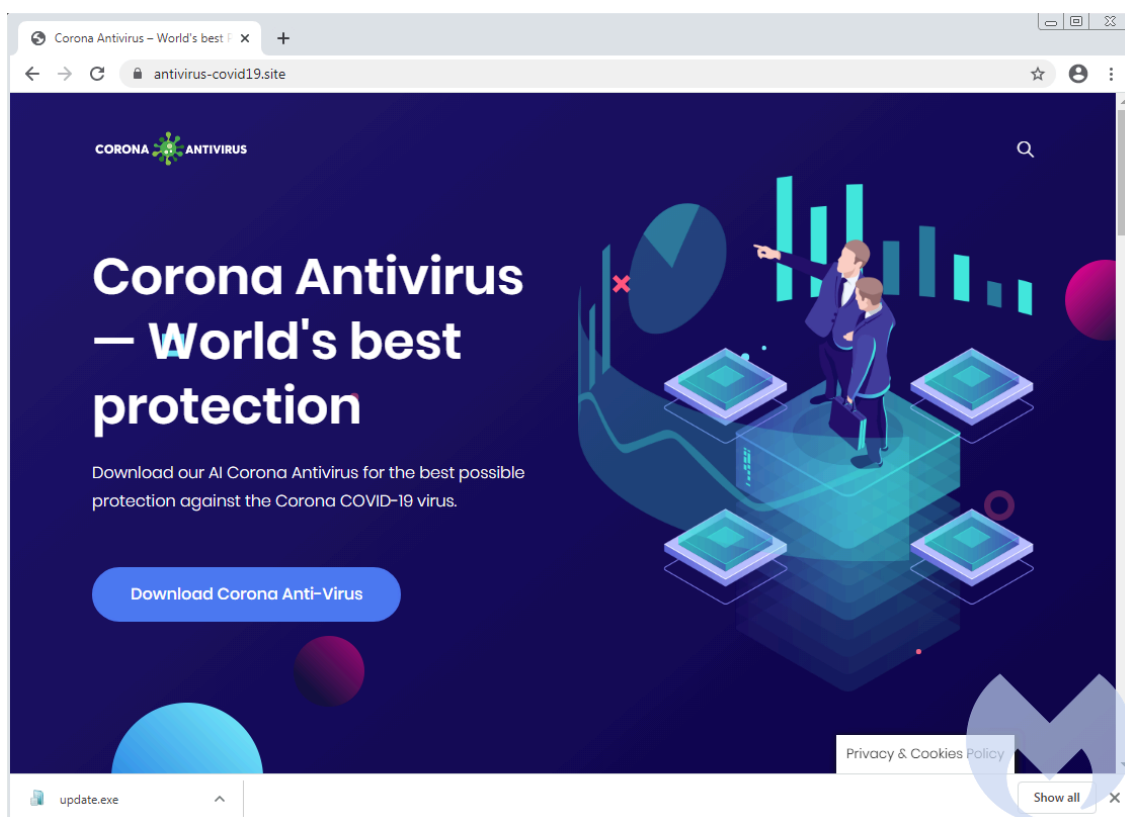
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

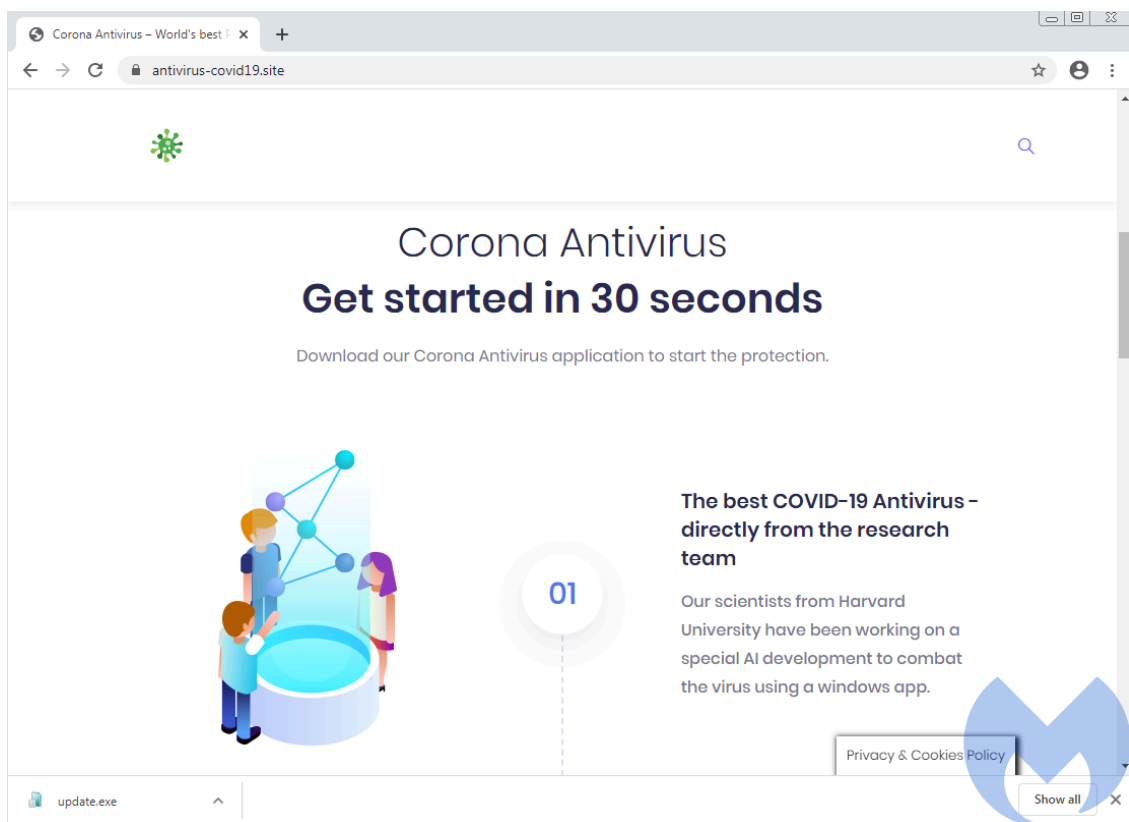
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

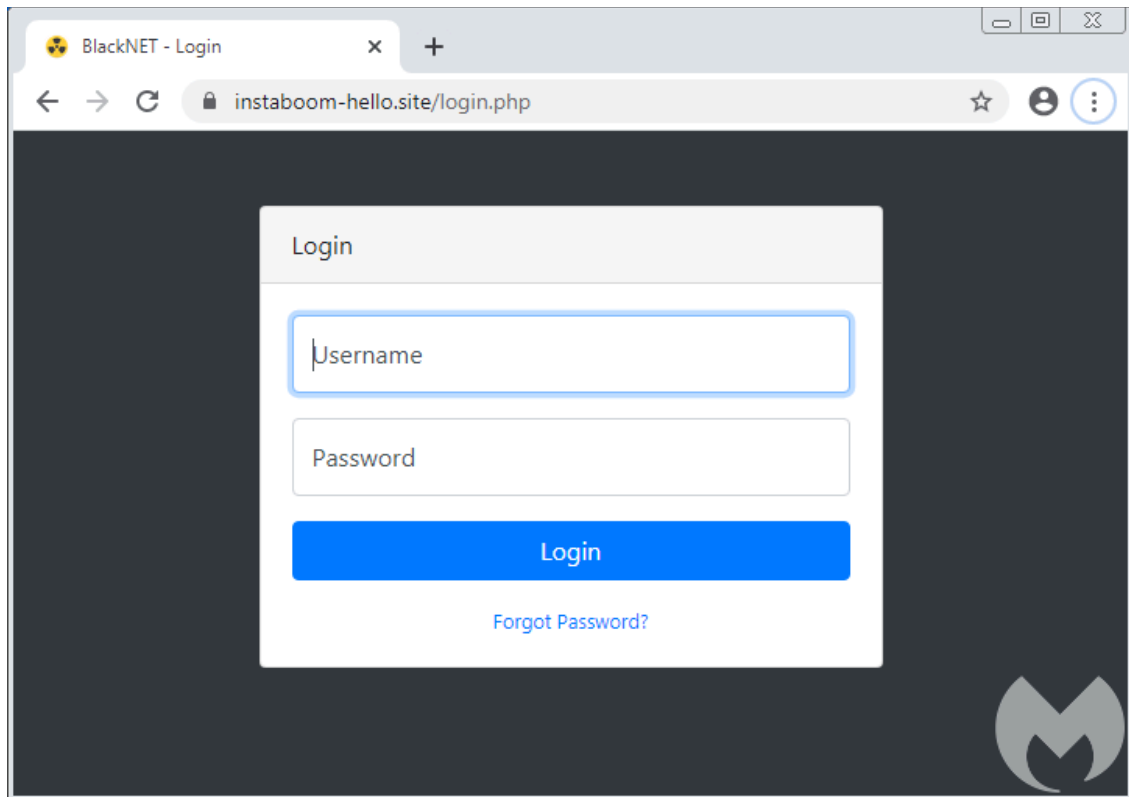


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a few blue dots indicating client locations. At the bottom, a copyright notice reads "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, it lists the details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

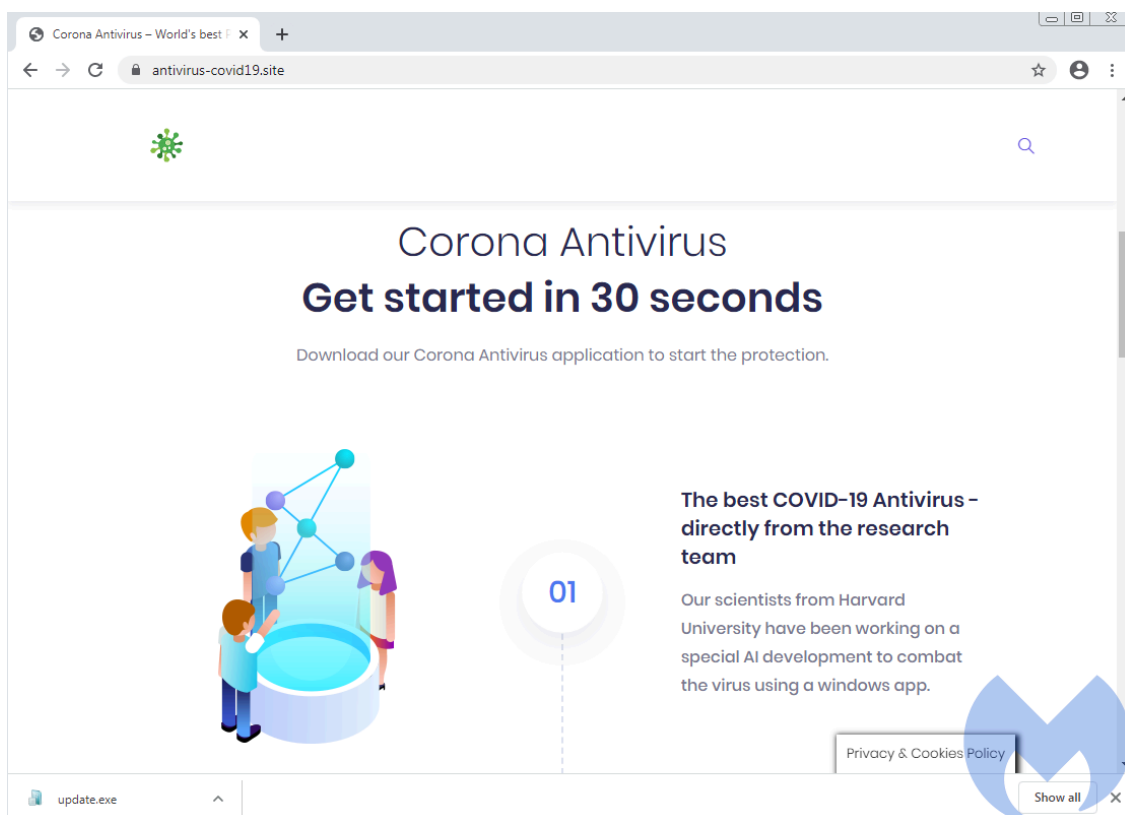
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

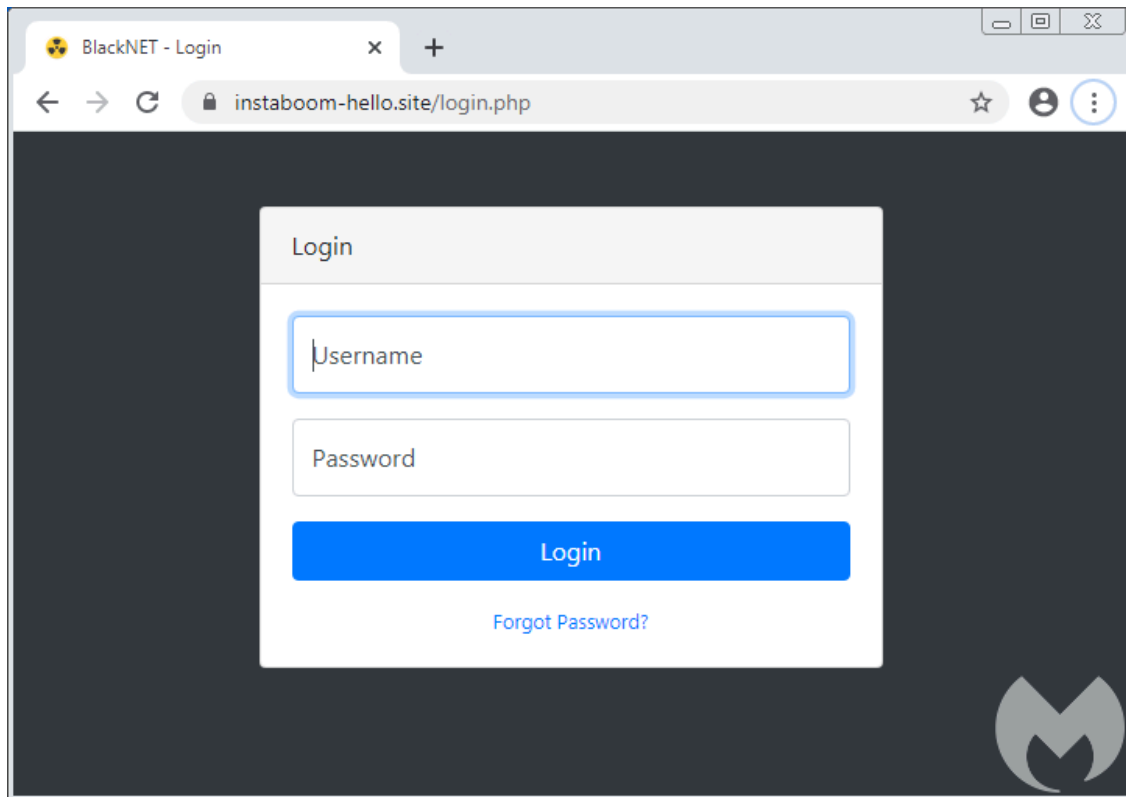


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

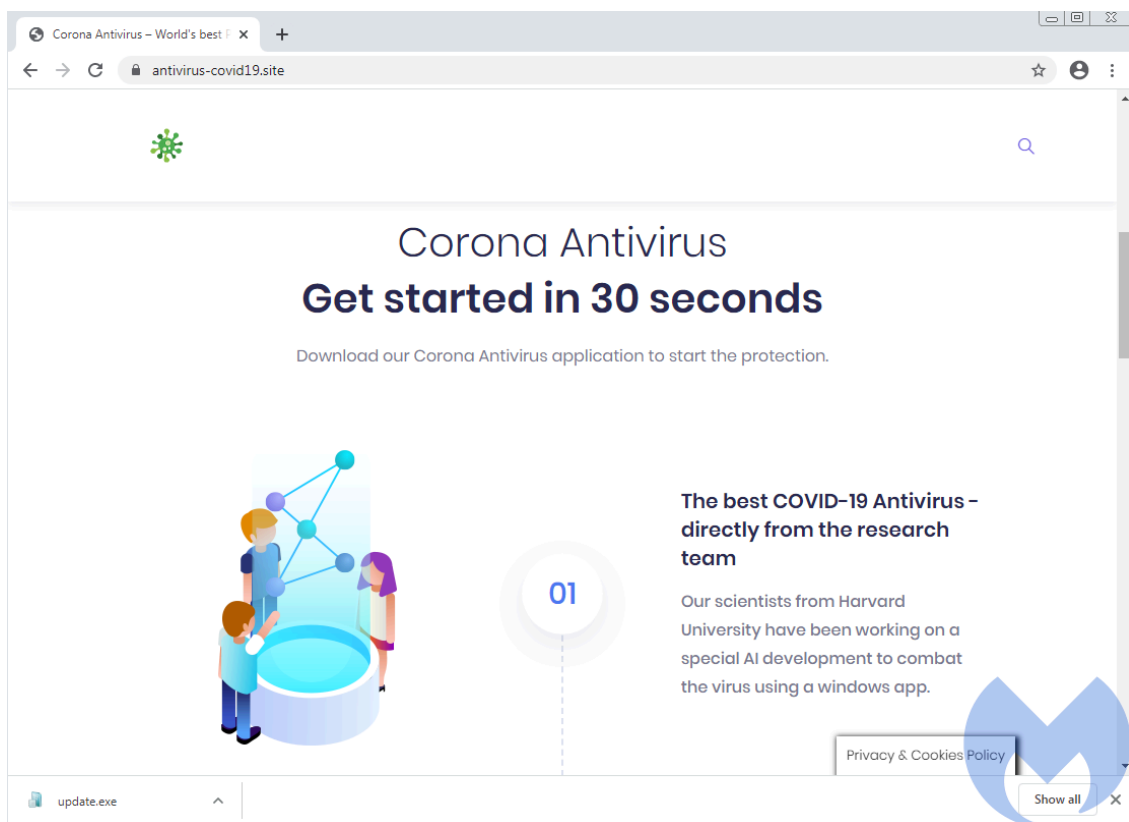
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

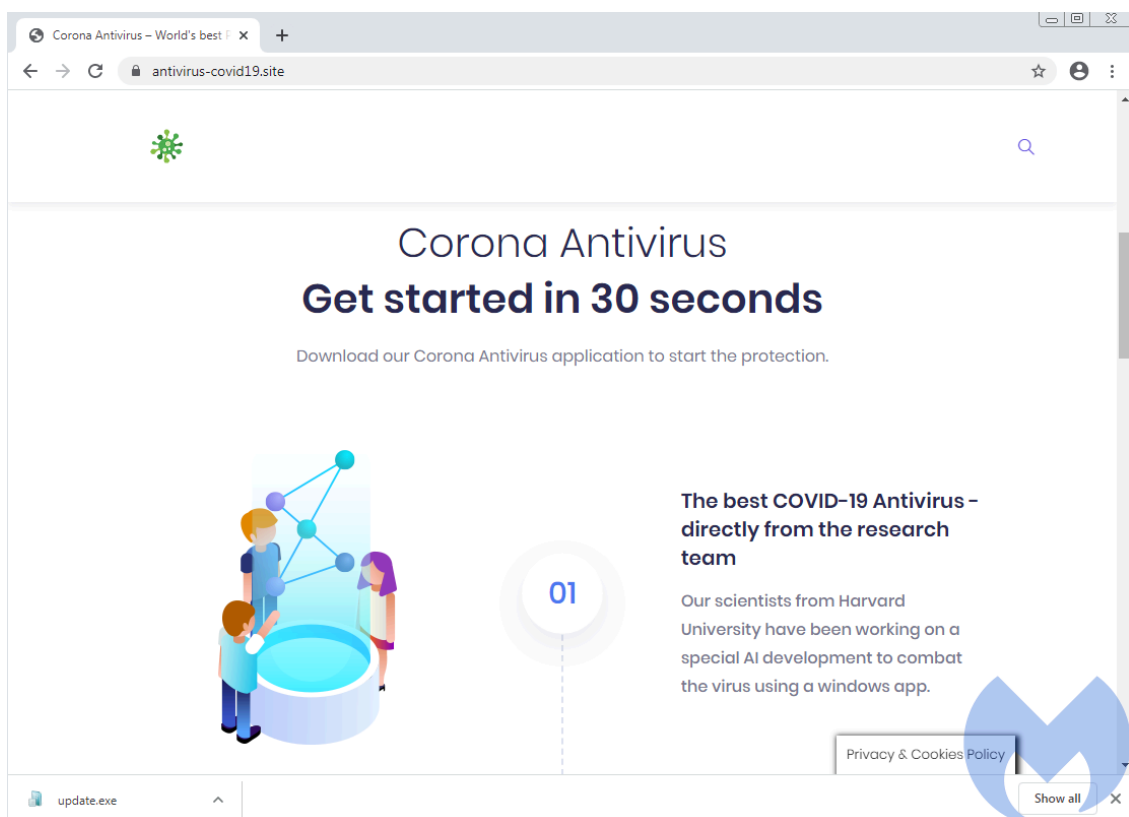
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

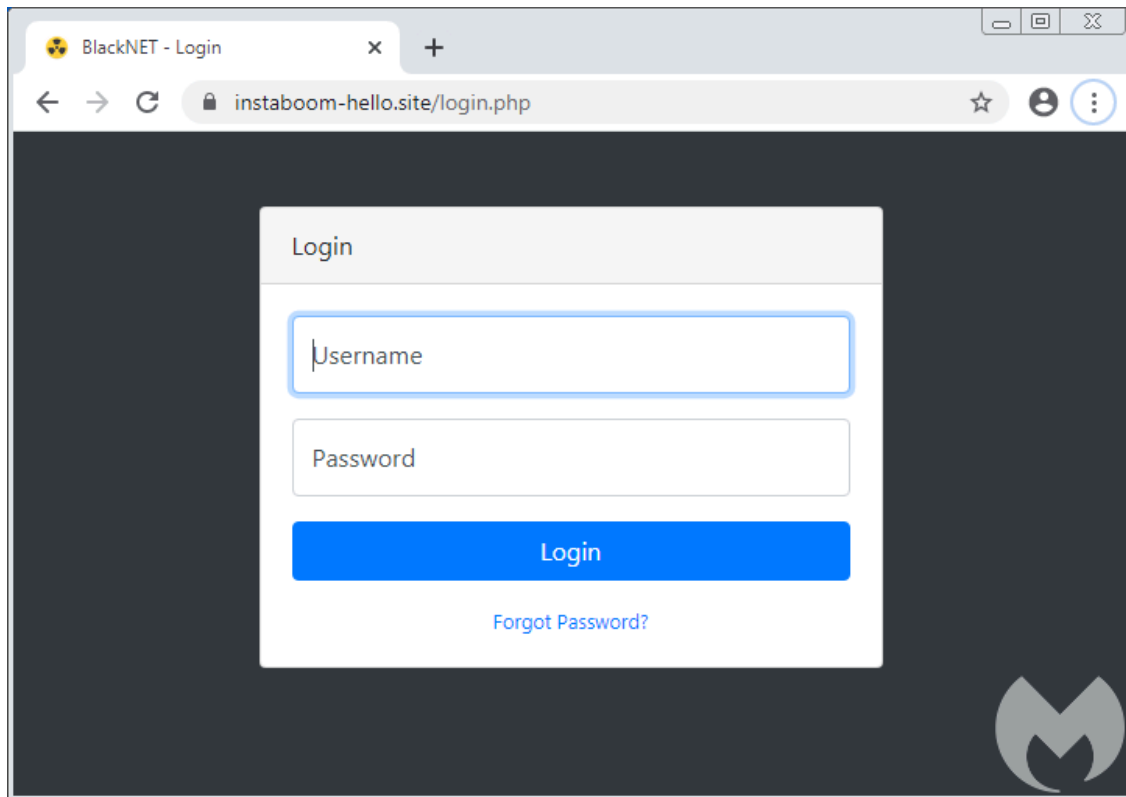


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

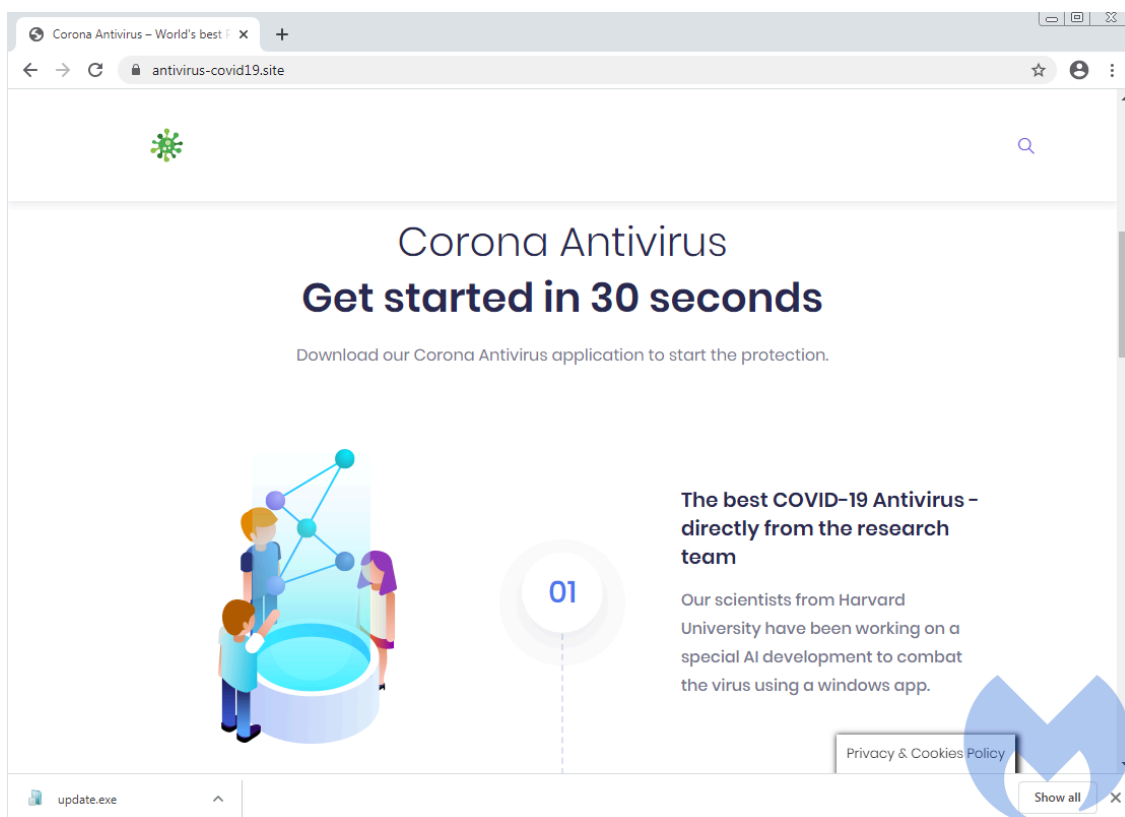
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

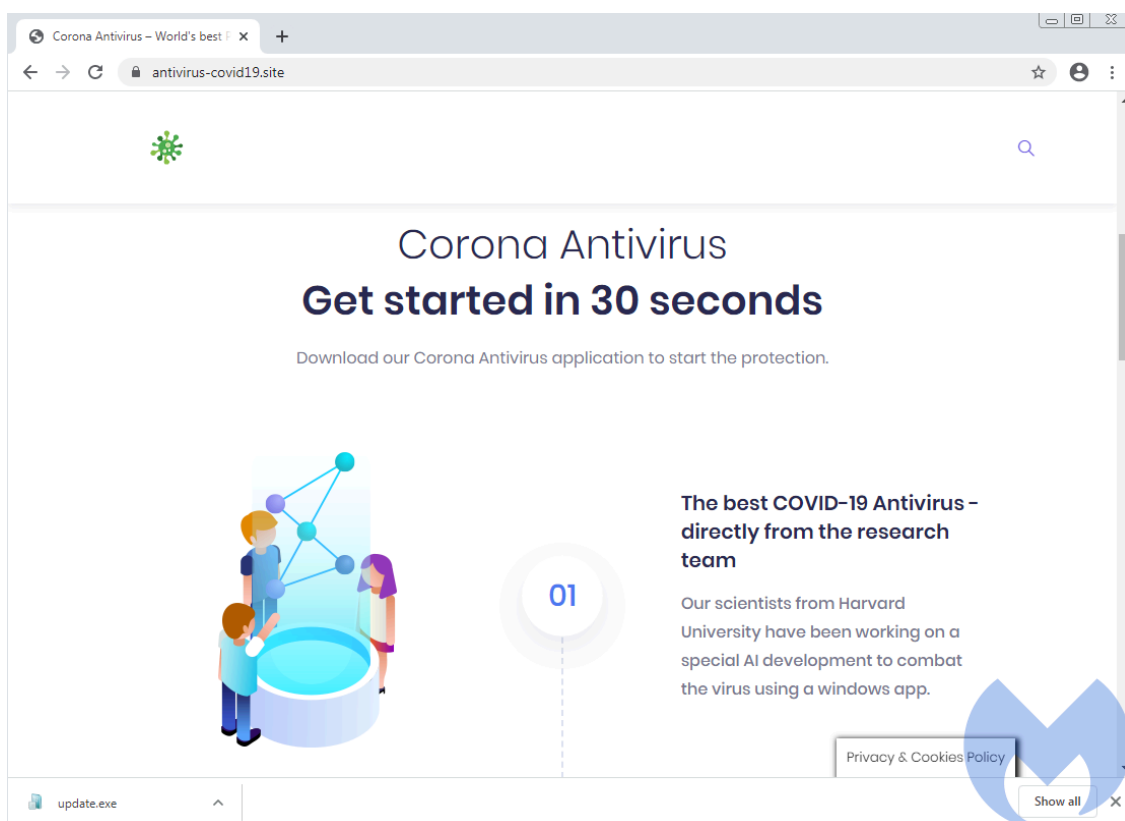
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

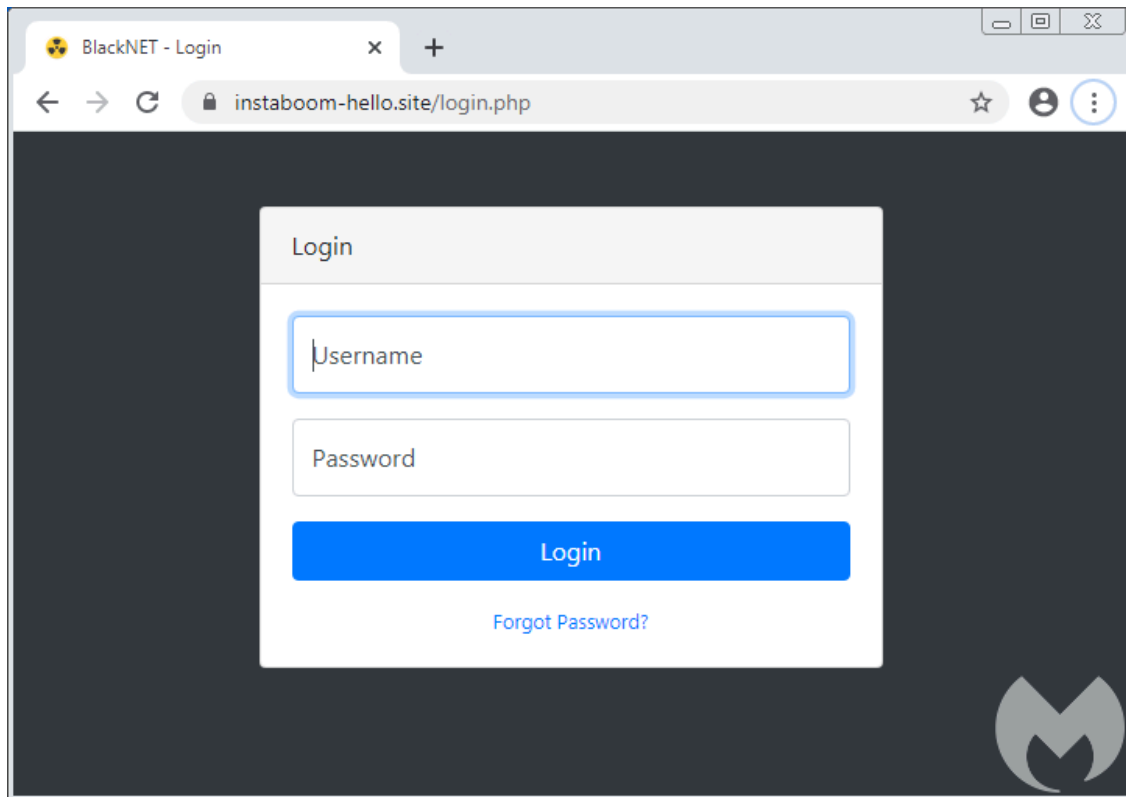


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

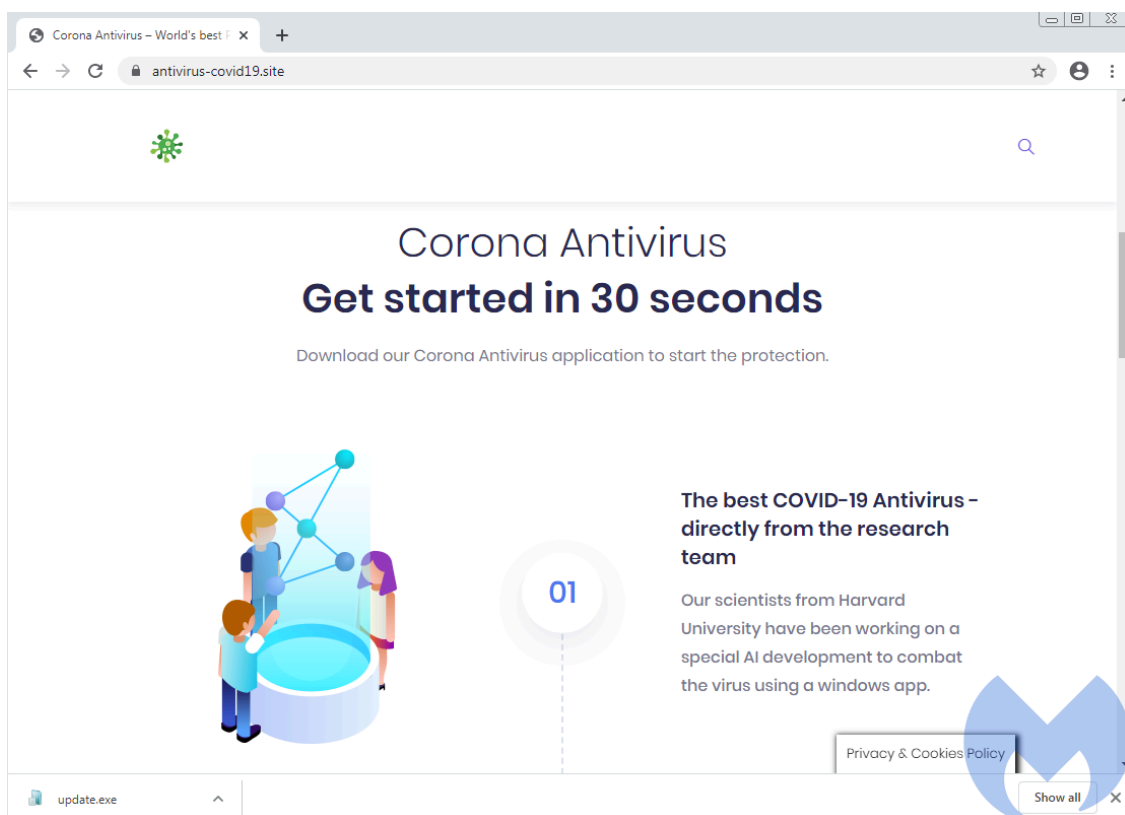
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

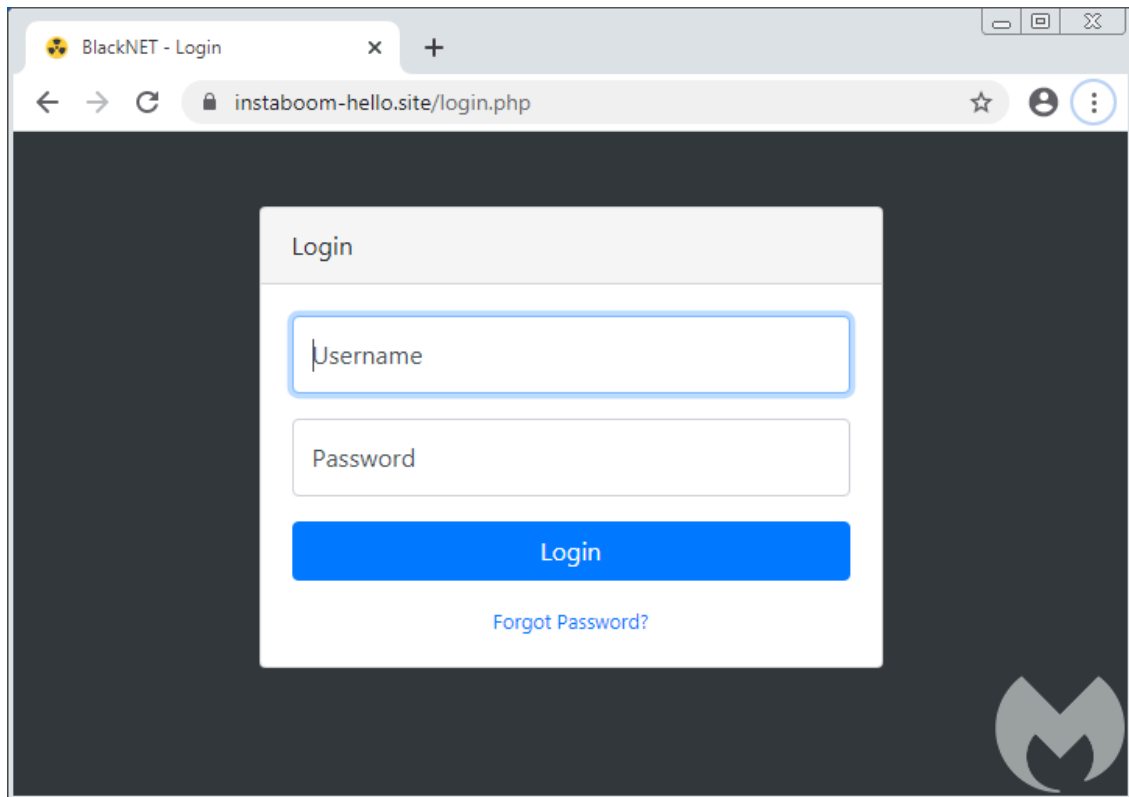


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

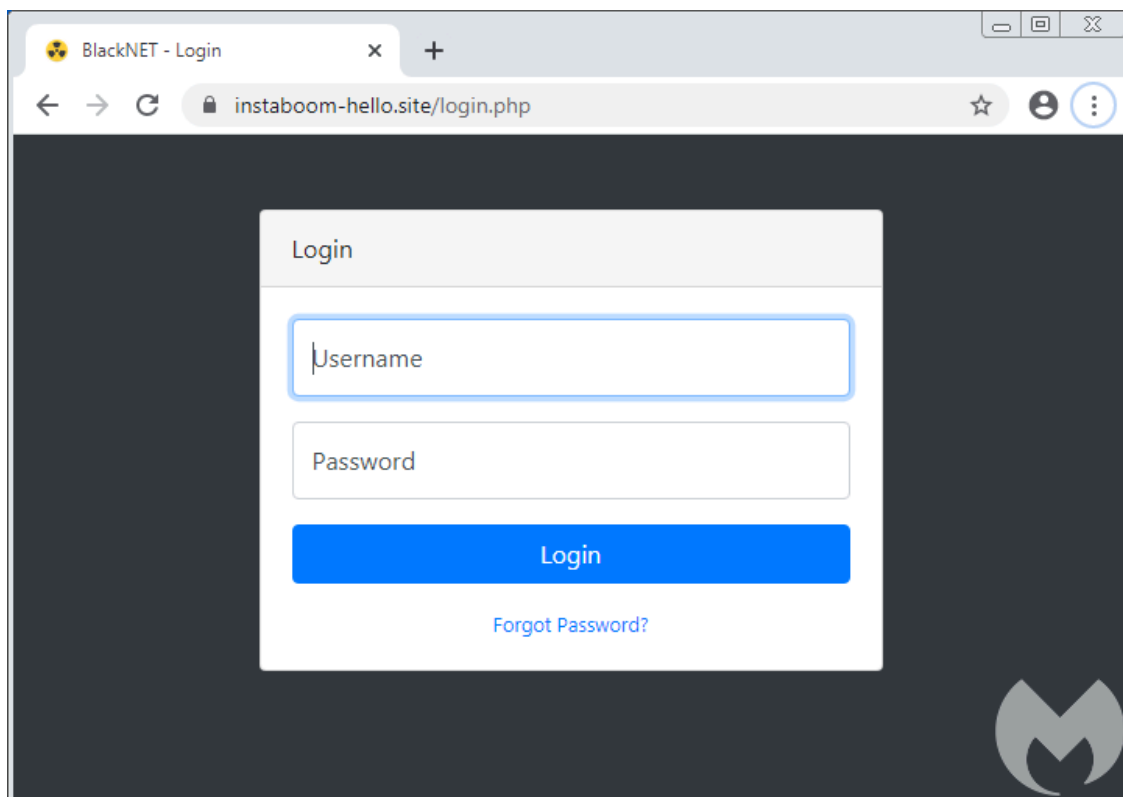
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

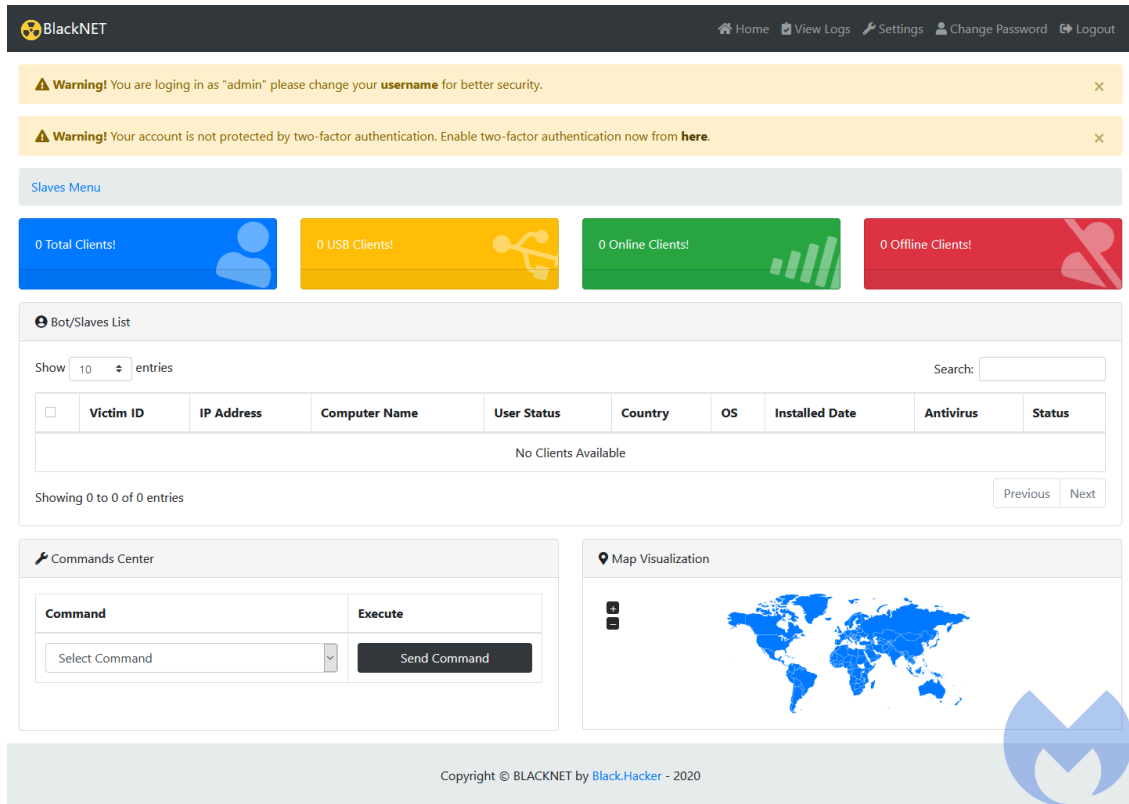
```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

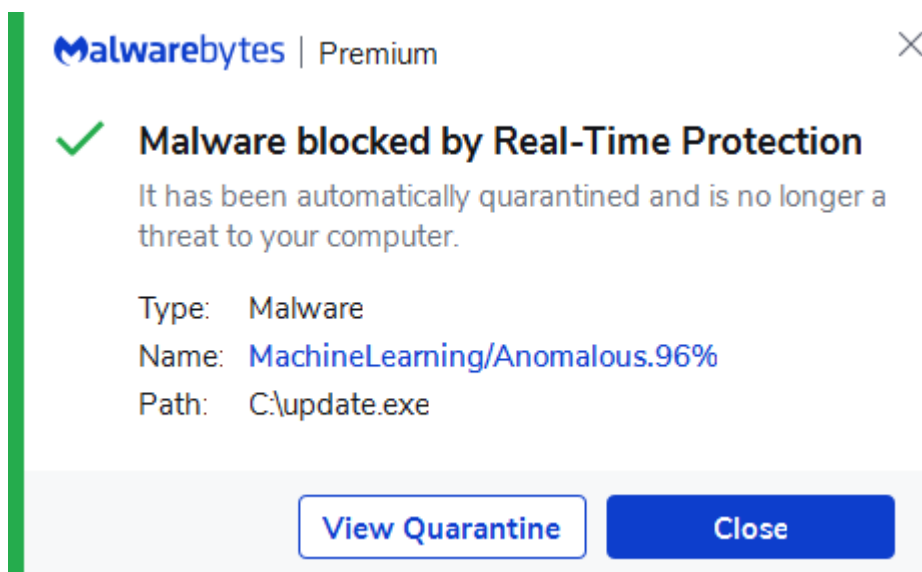


Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

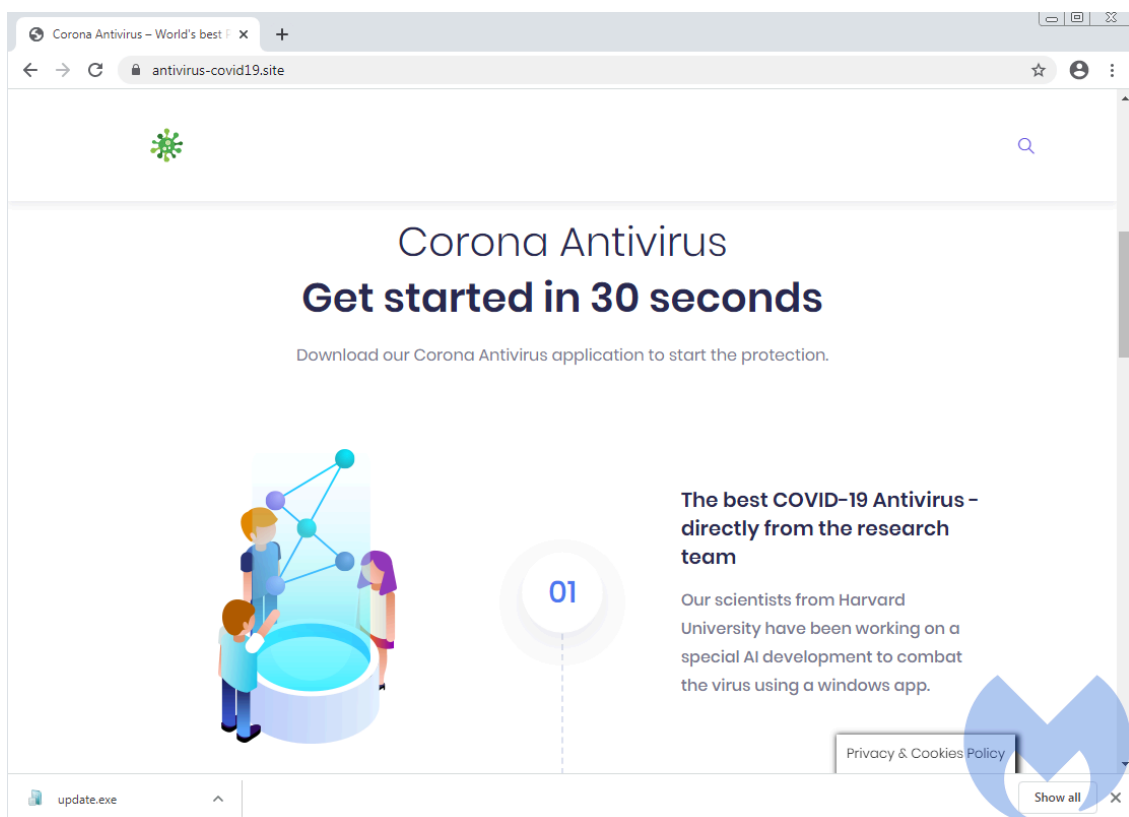
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

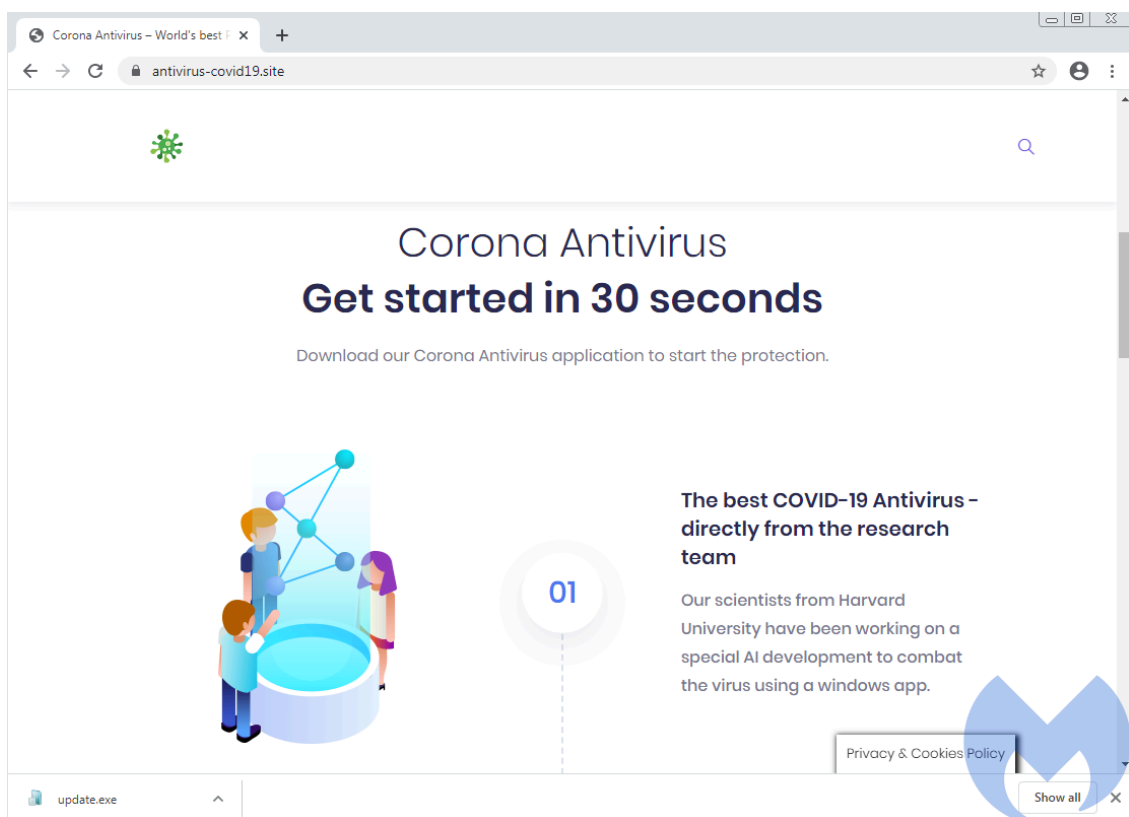
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

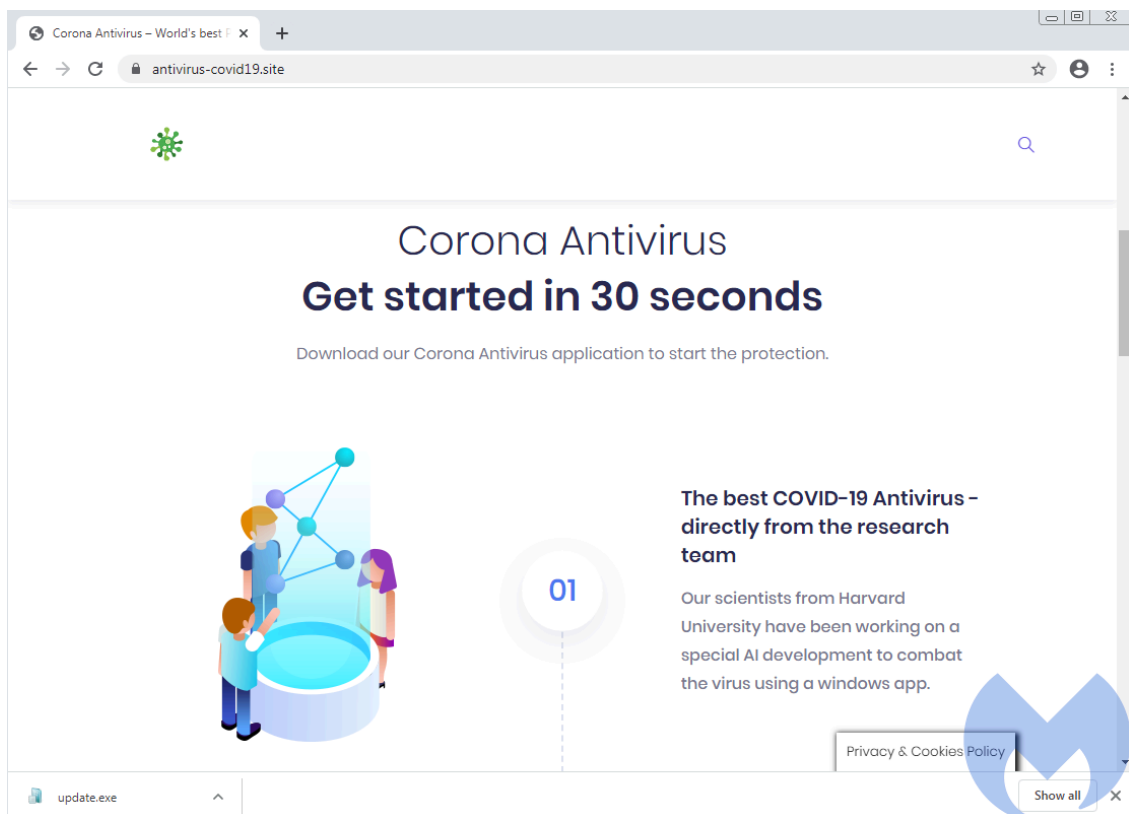
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

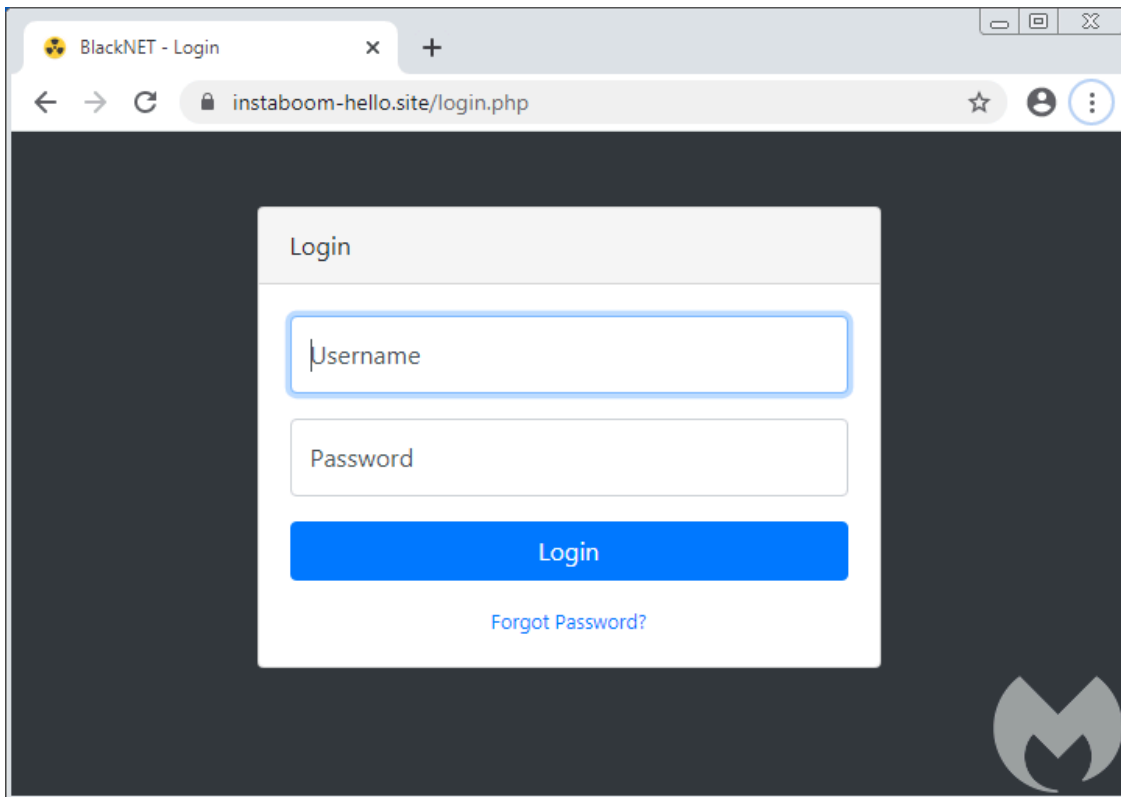


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

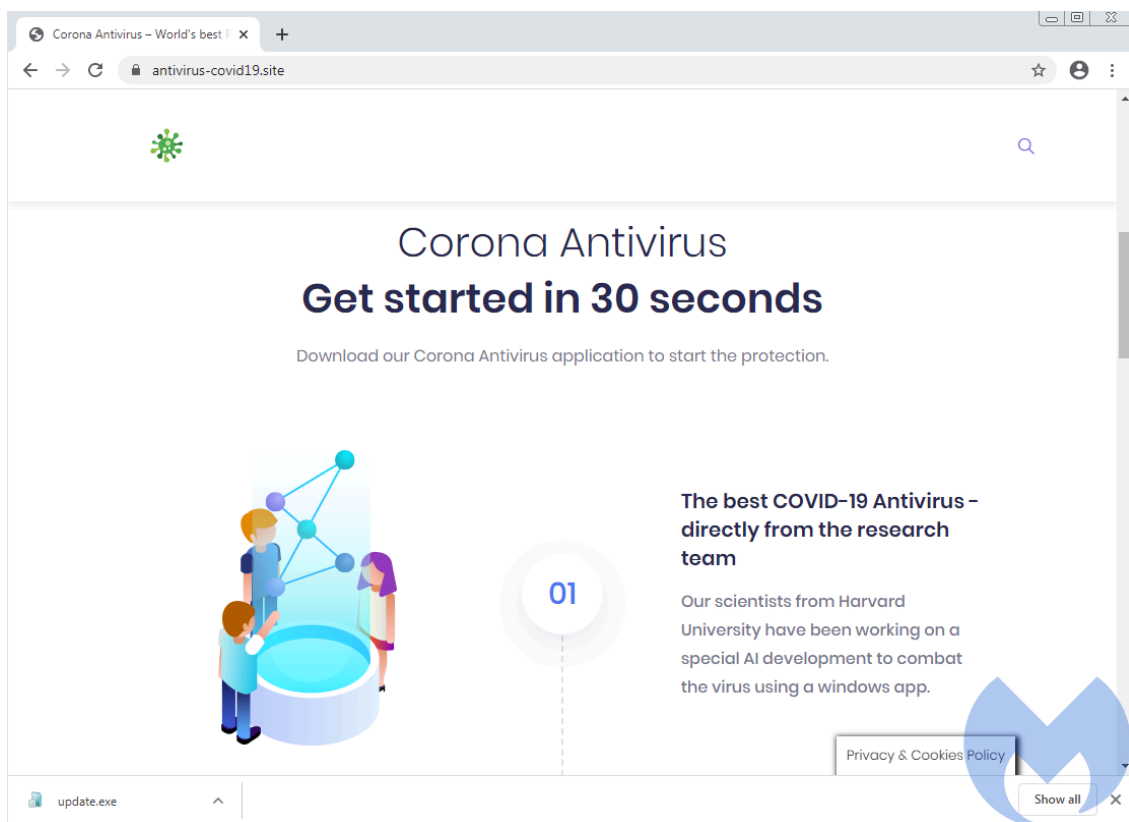
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

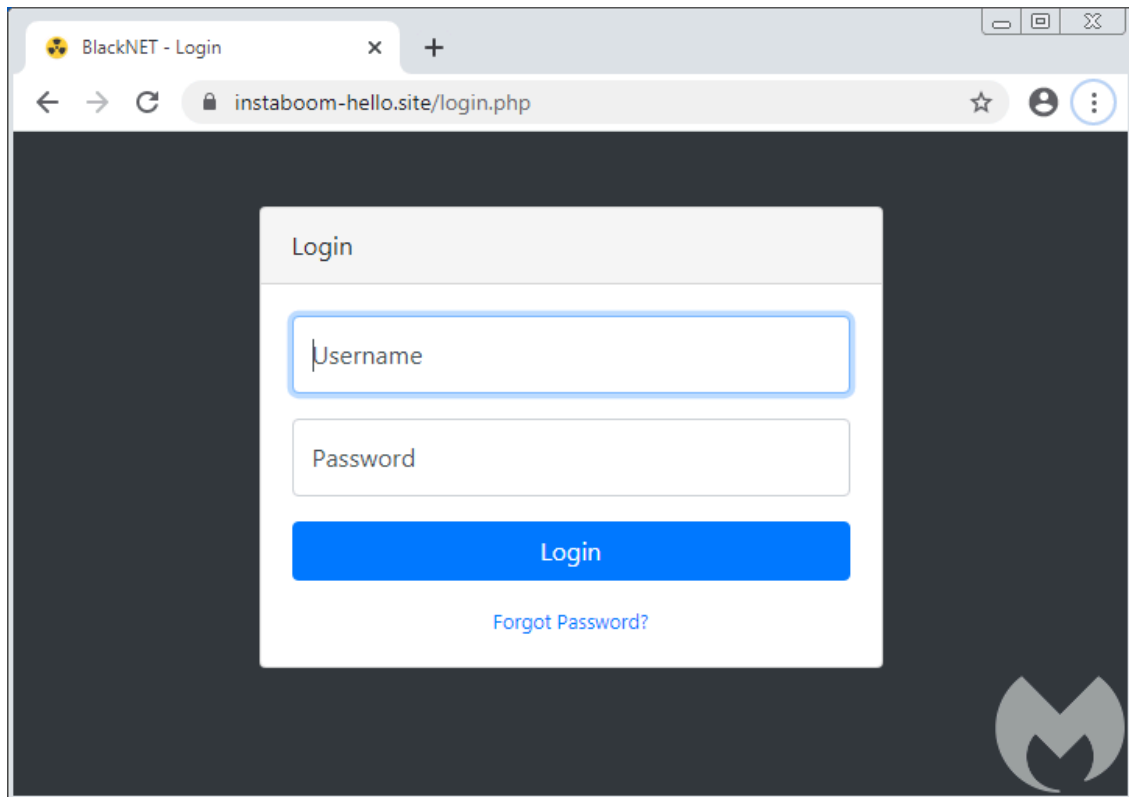


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

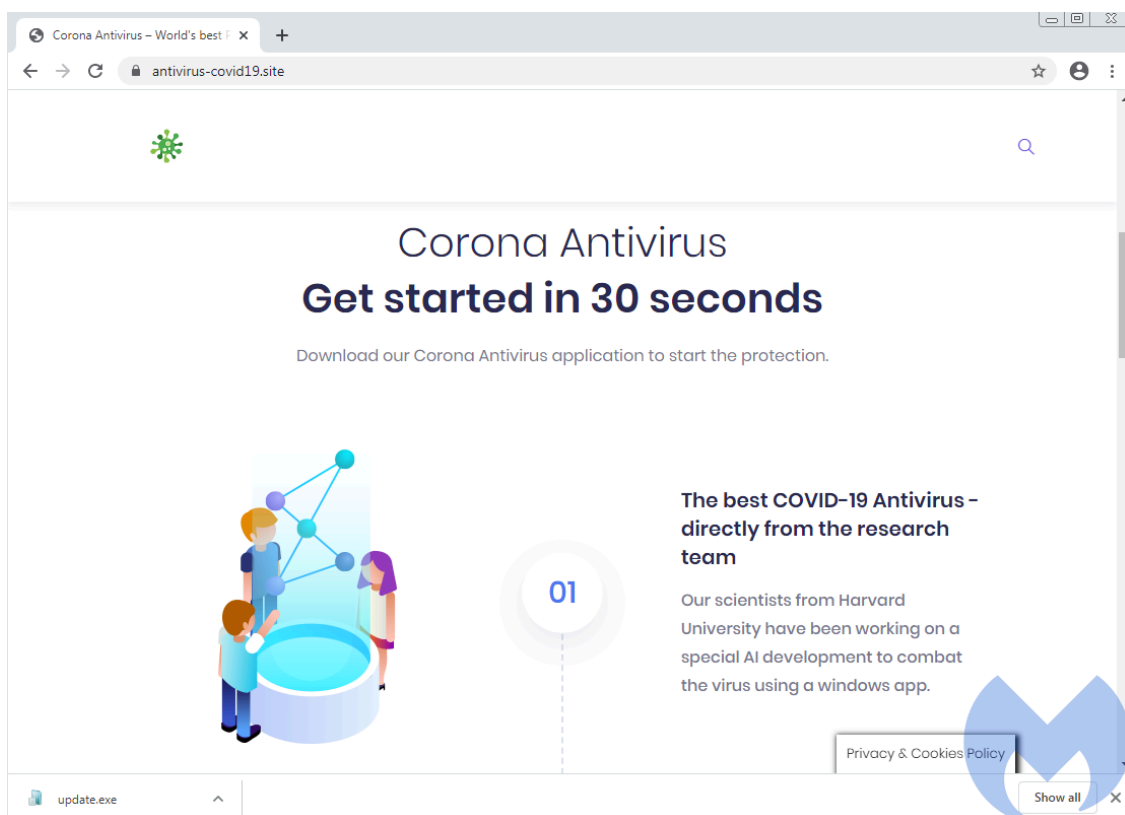
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

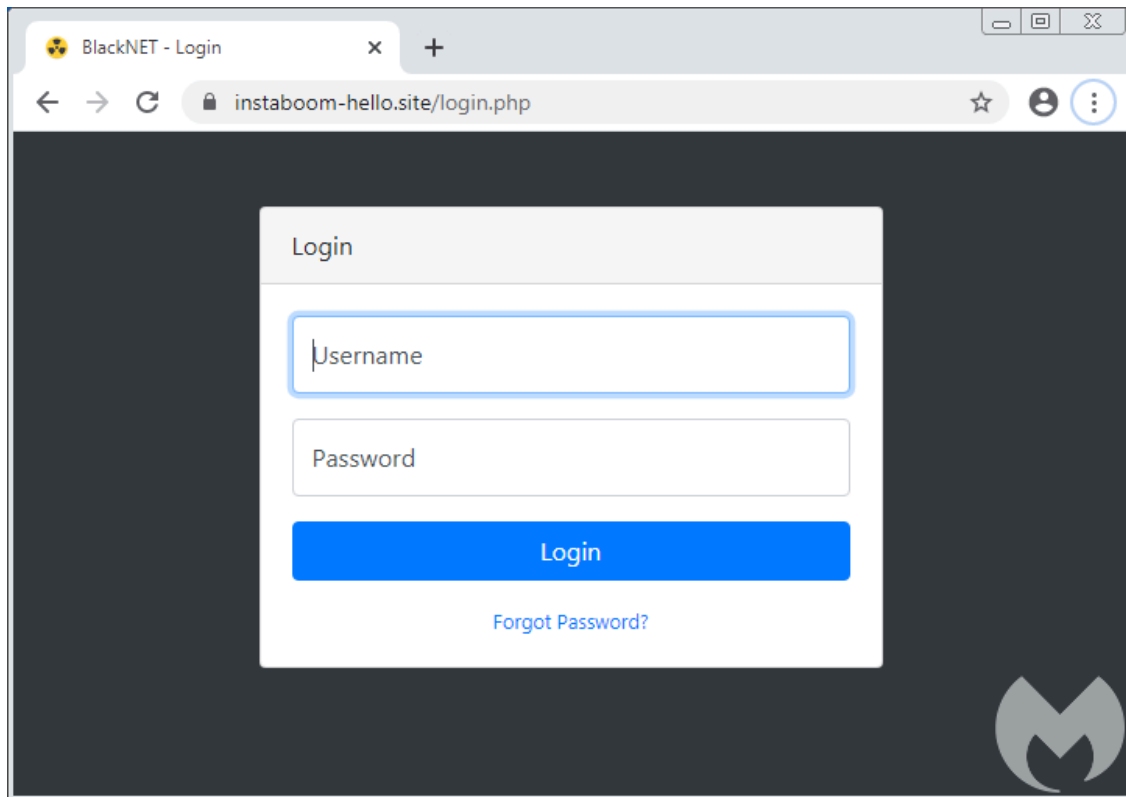


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

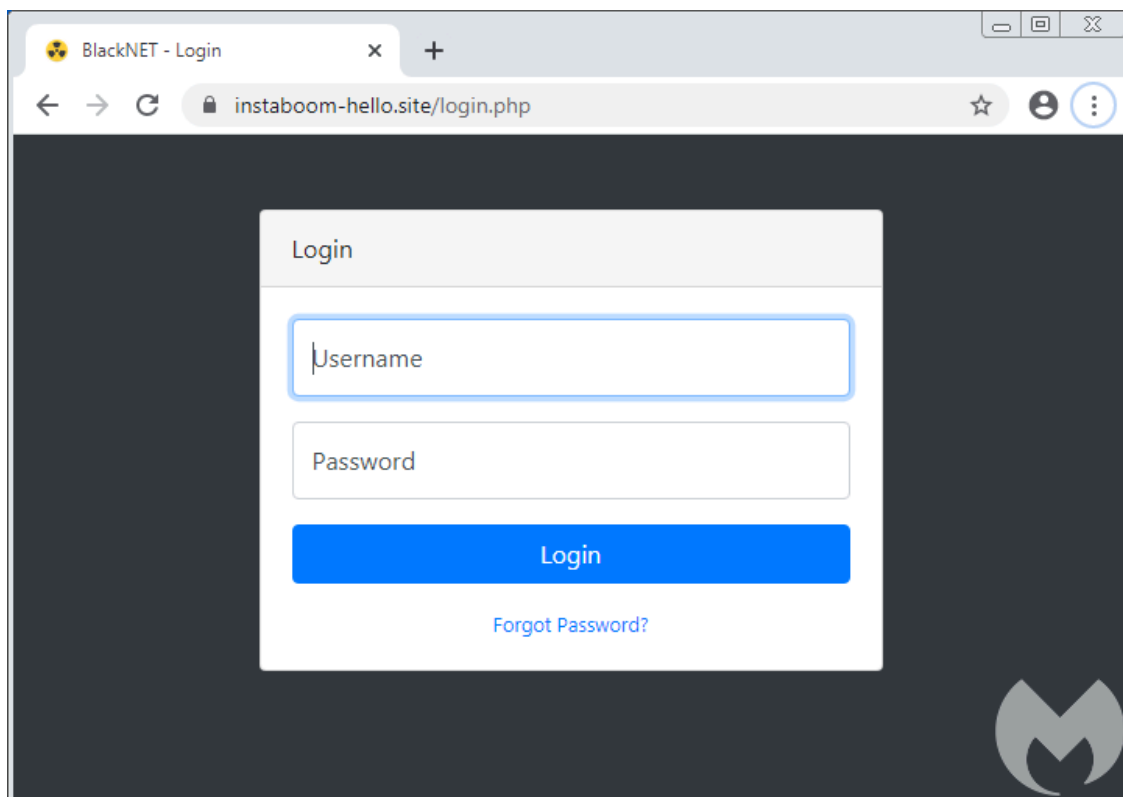
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

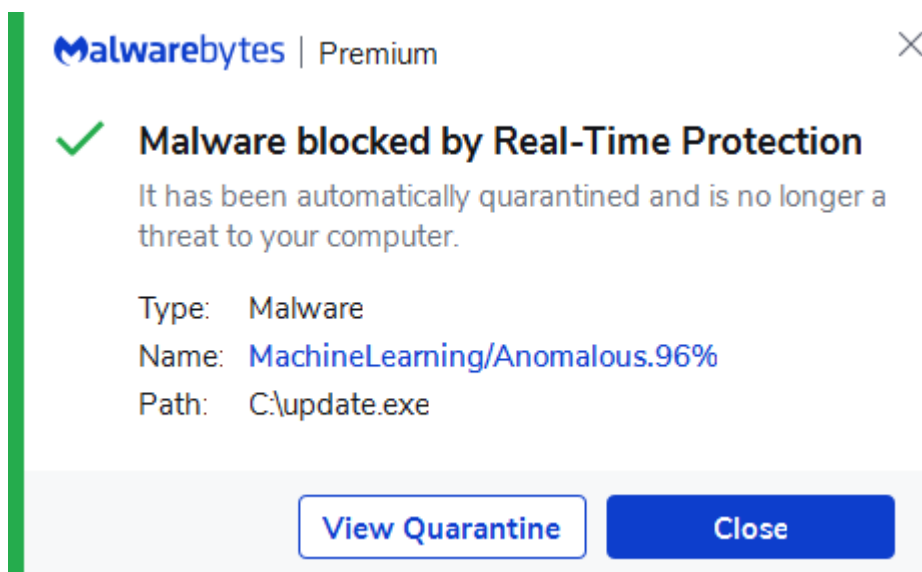
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

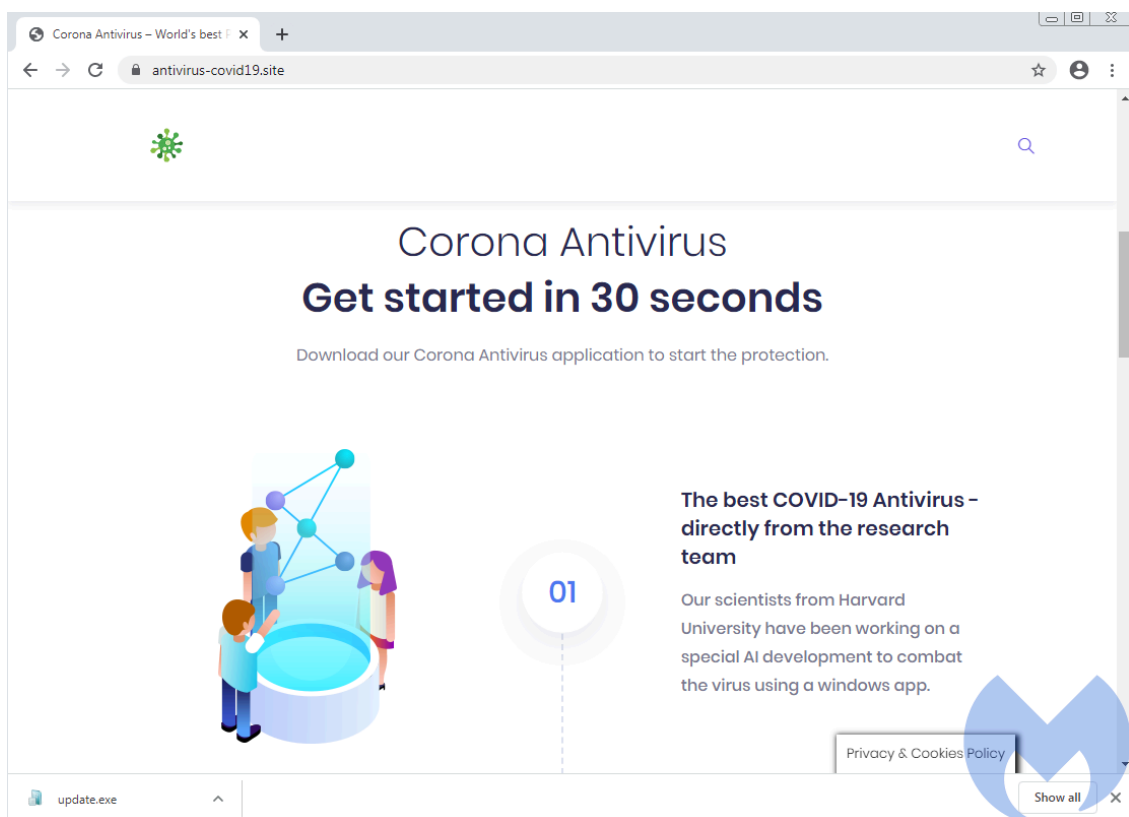
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

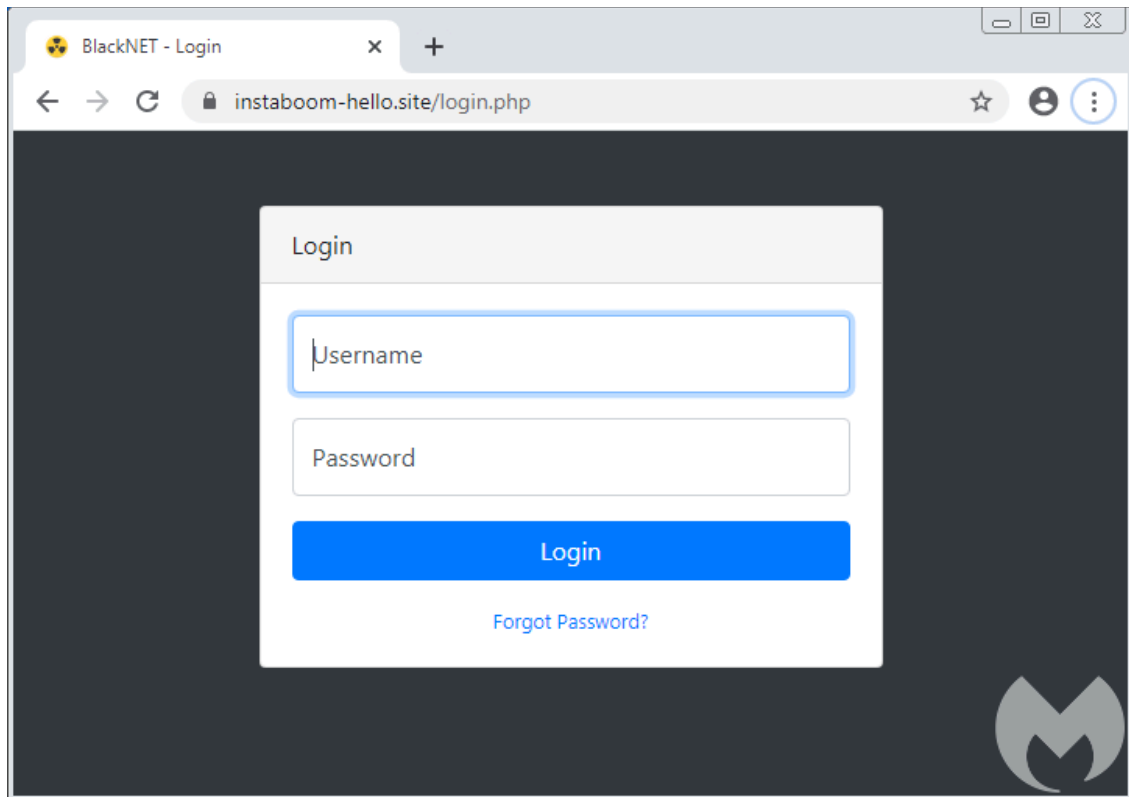


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

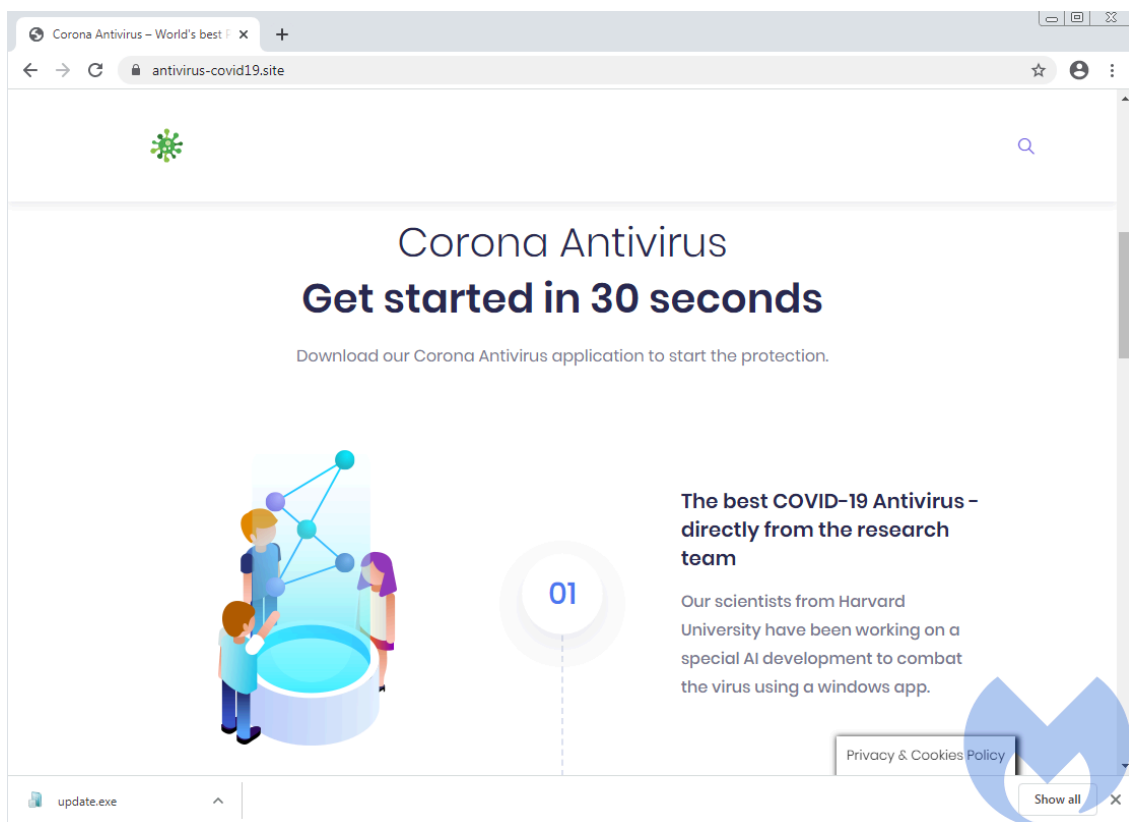
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

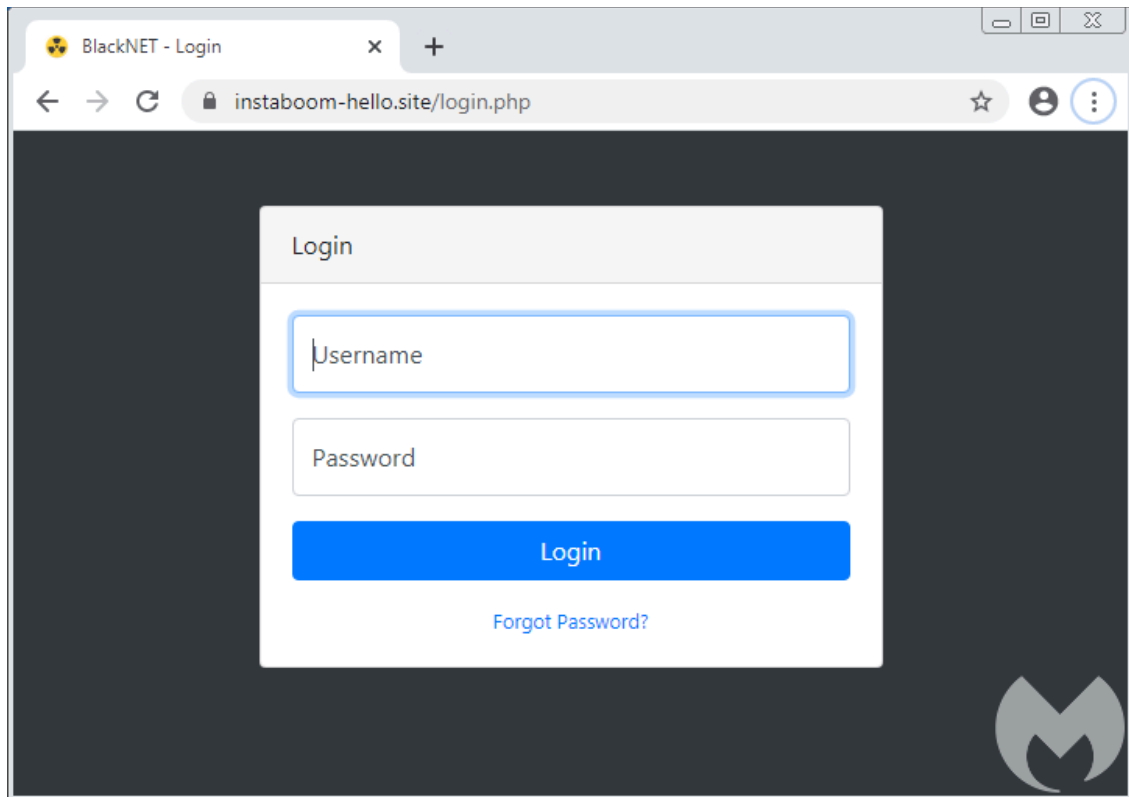


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

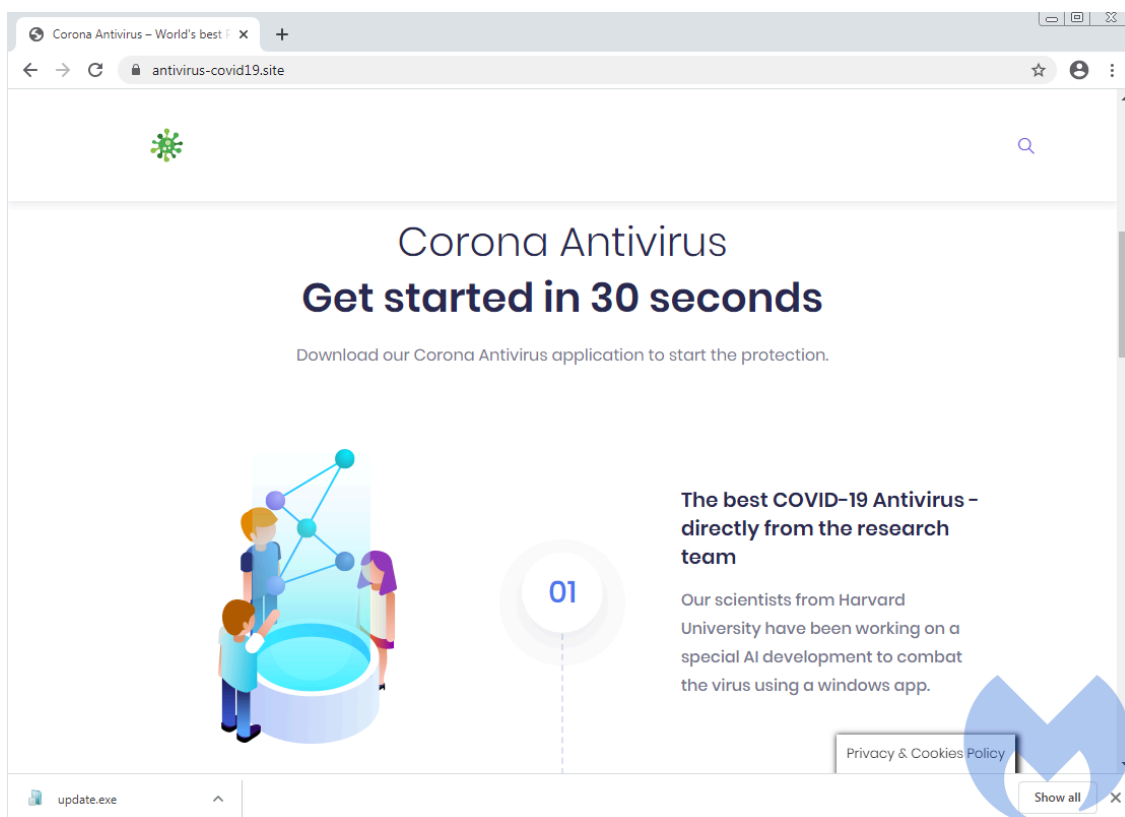
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

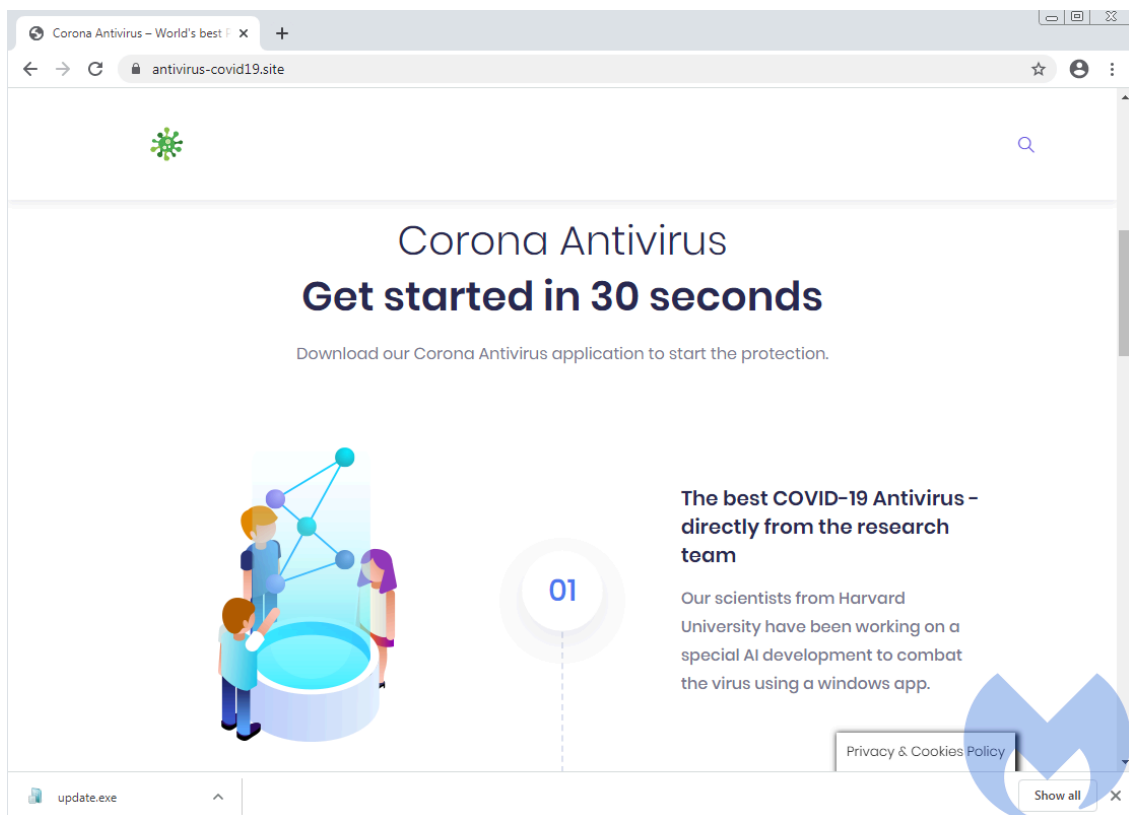
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

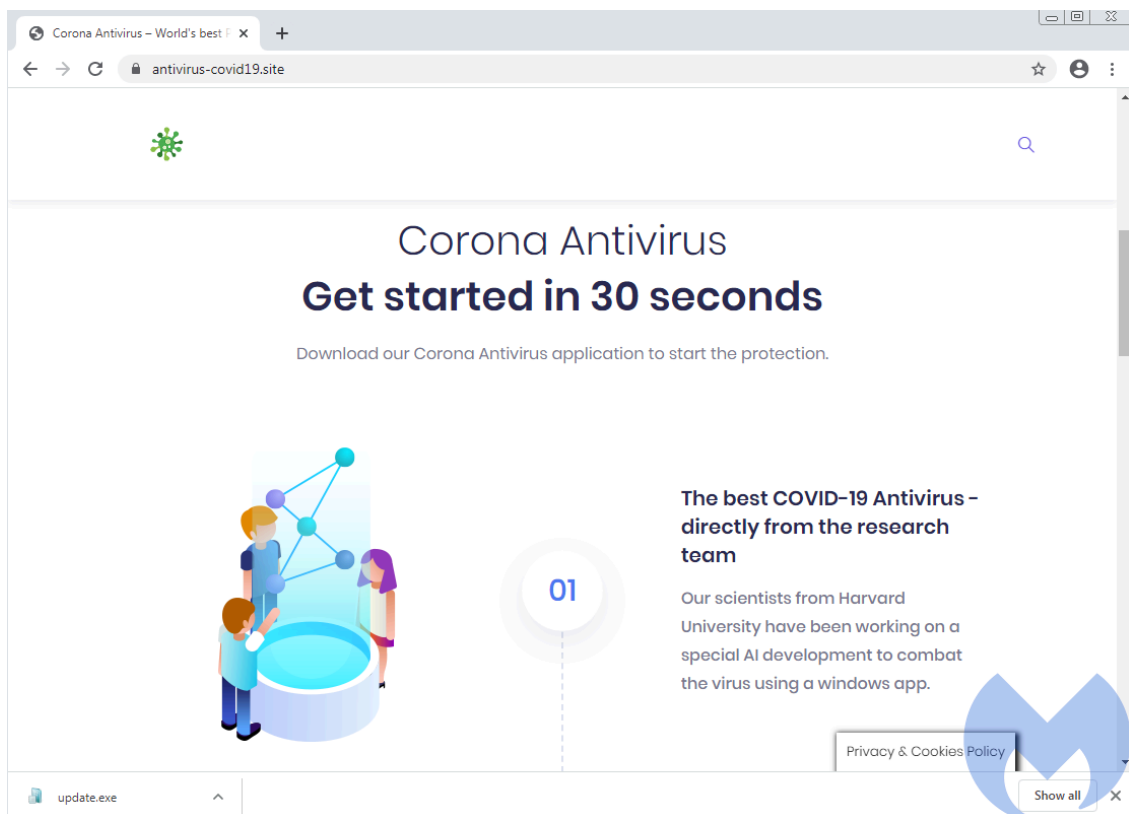
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

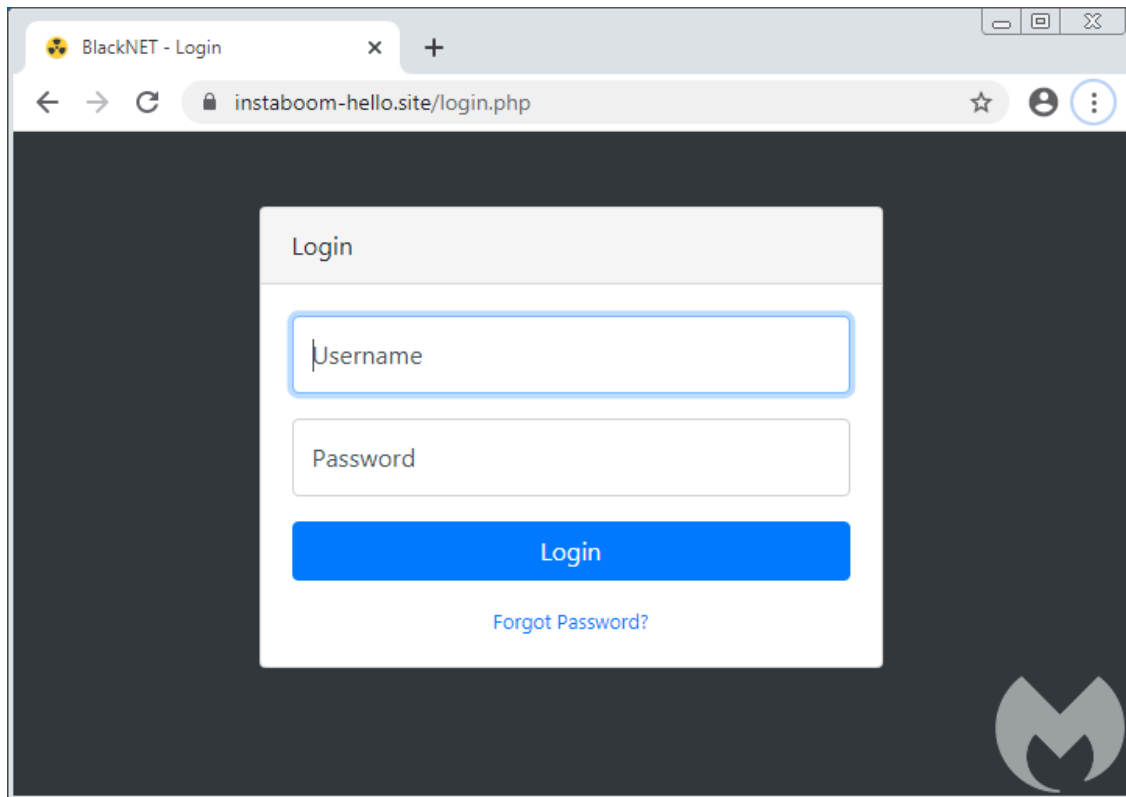


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

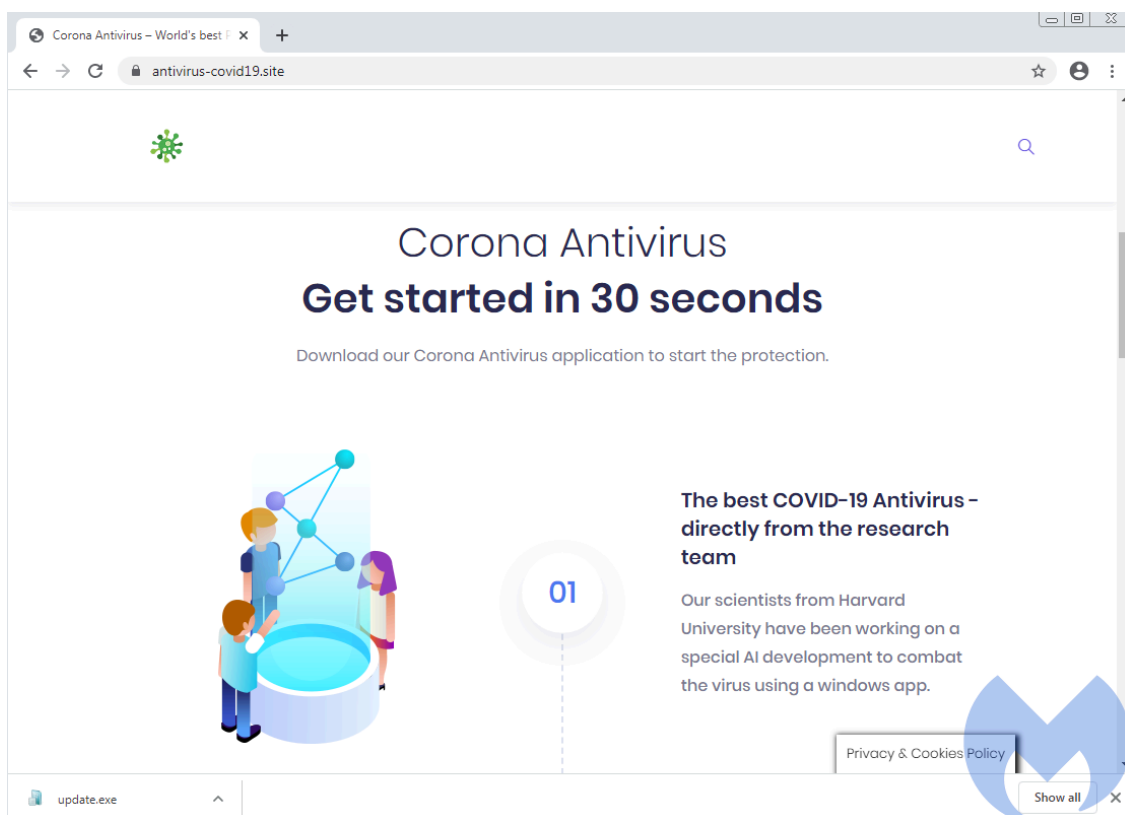
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four status cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below these is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the table is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" showing a world map with blue markers. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

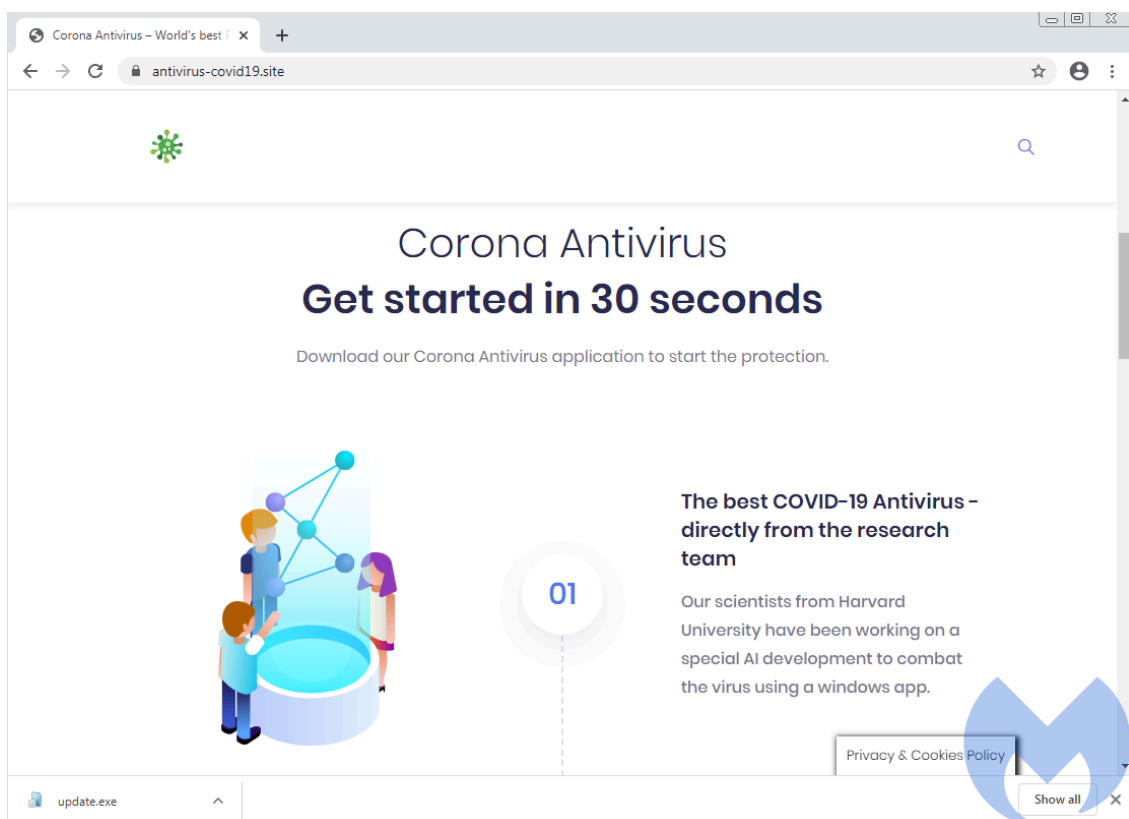
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

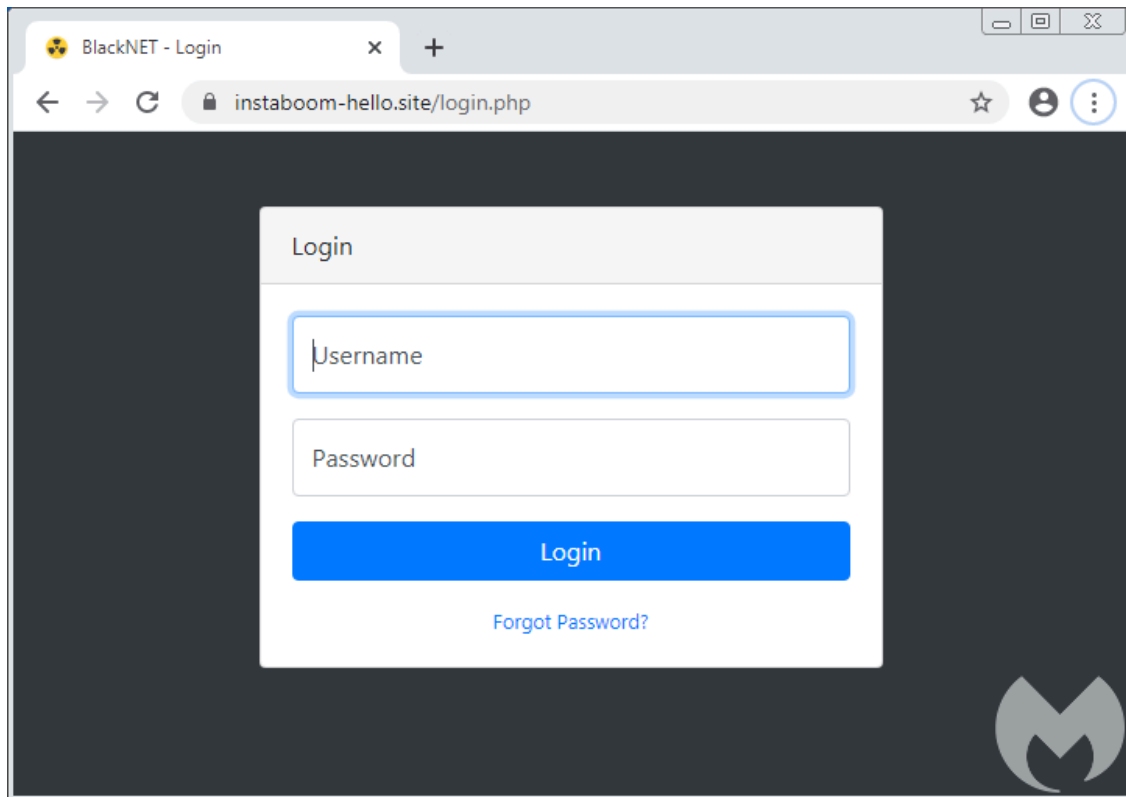


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[:]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[:]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

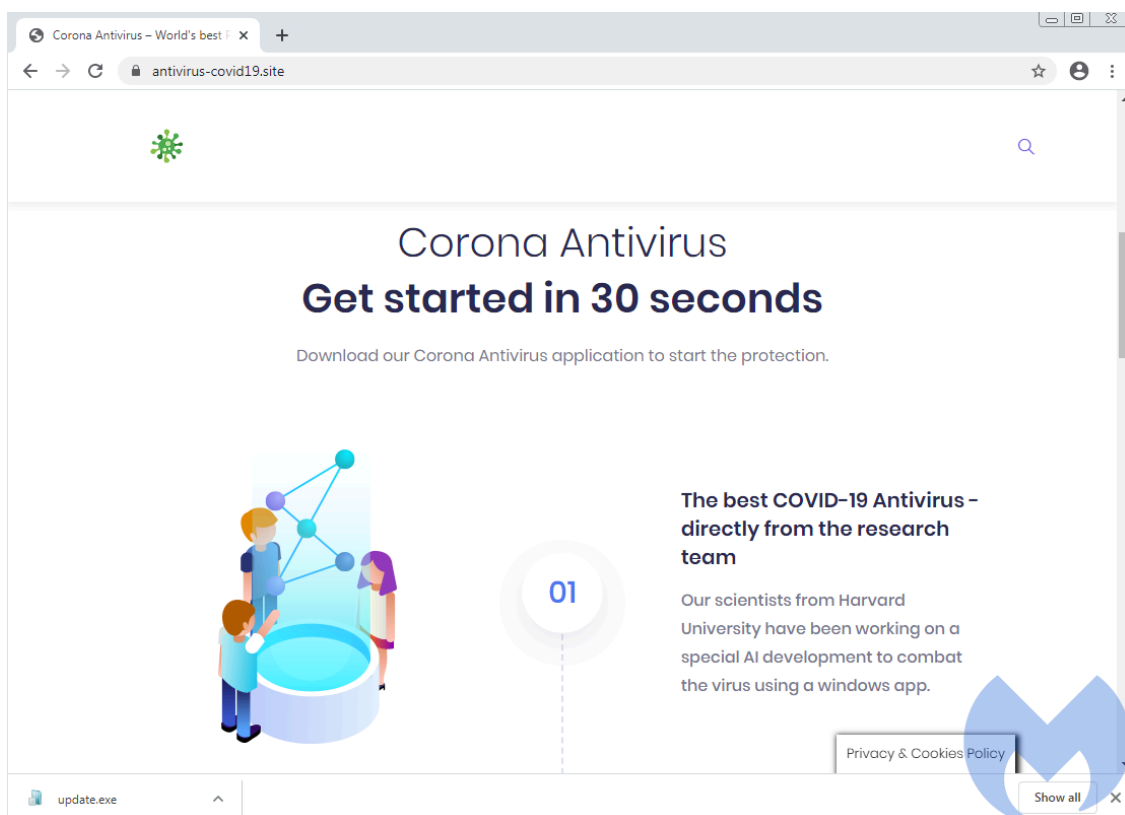
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

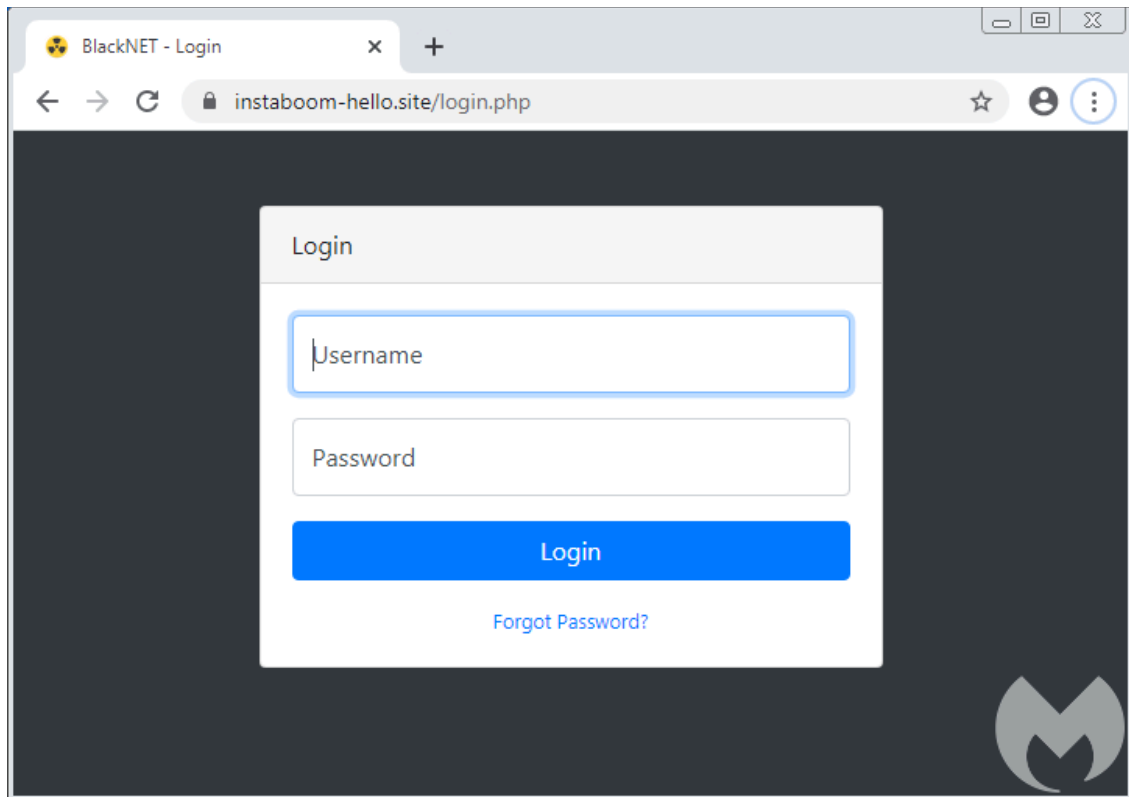


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

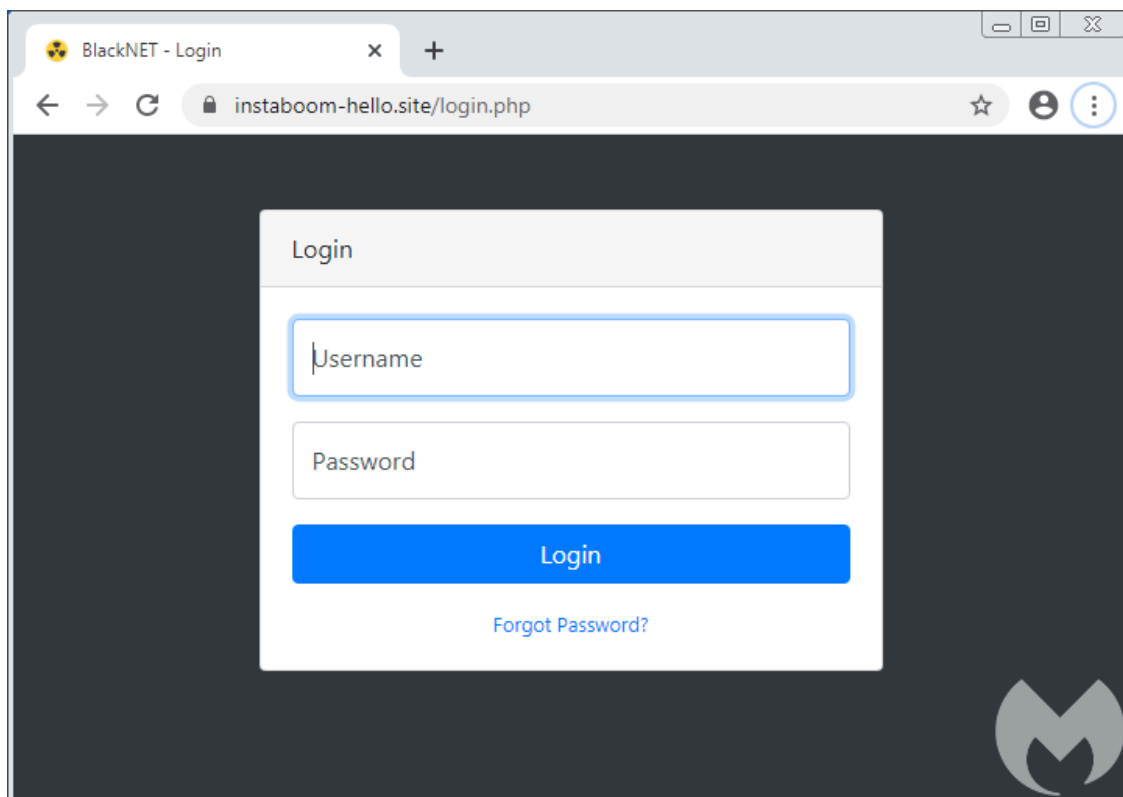
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

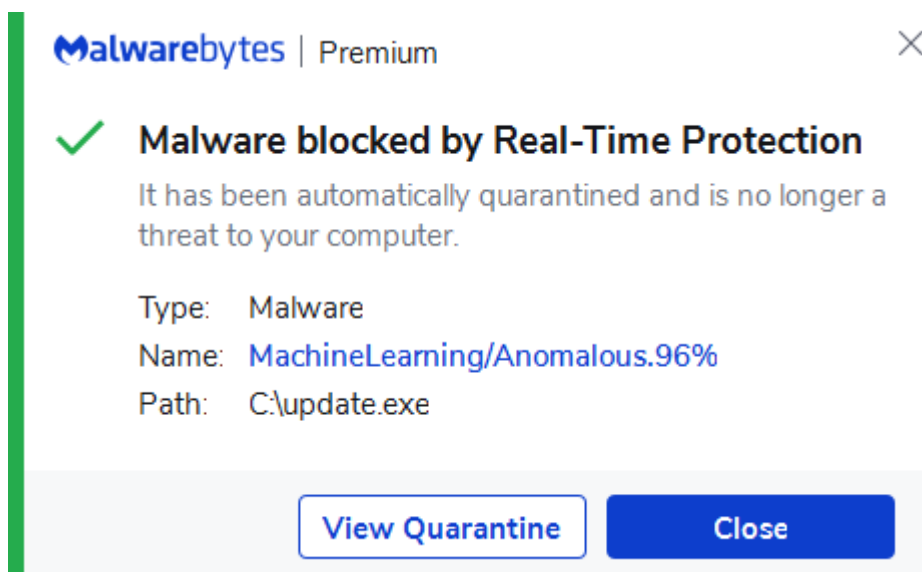
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

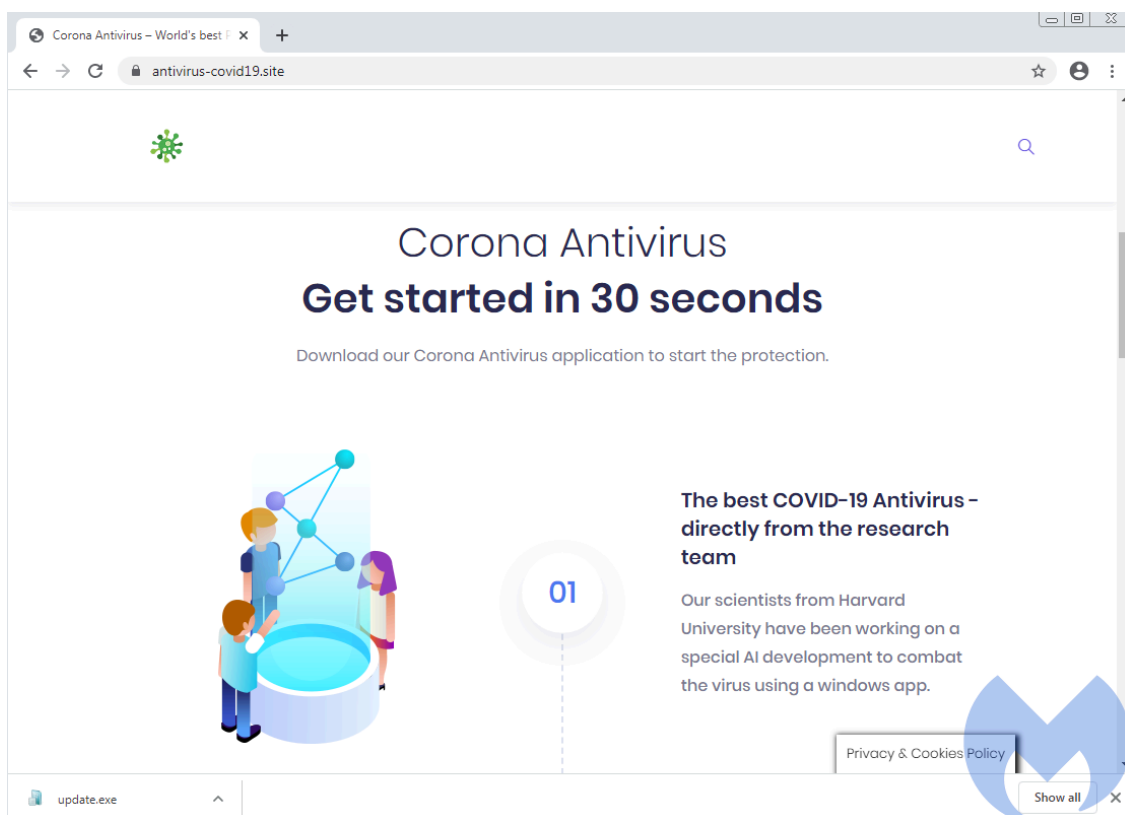
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

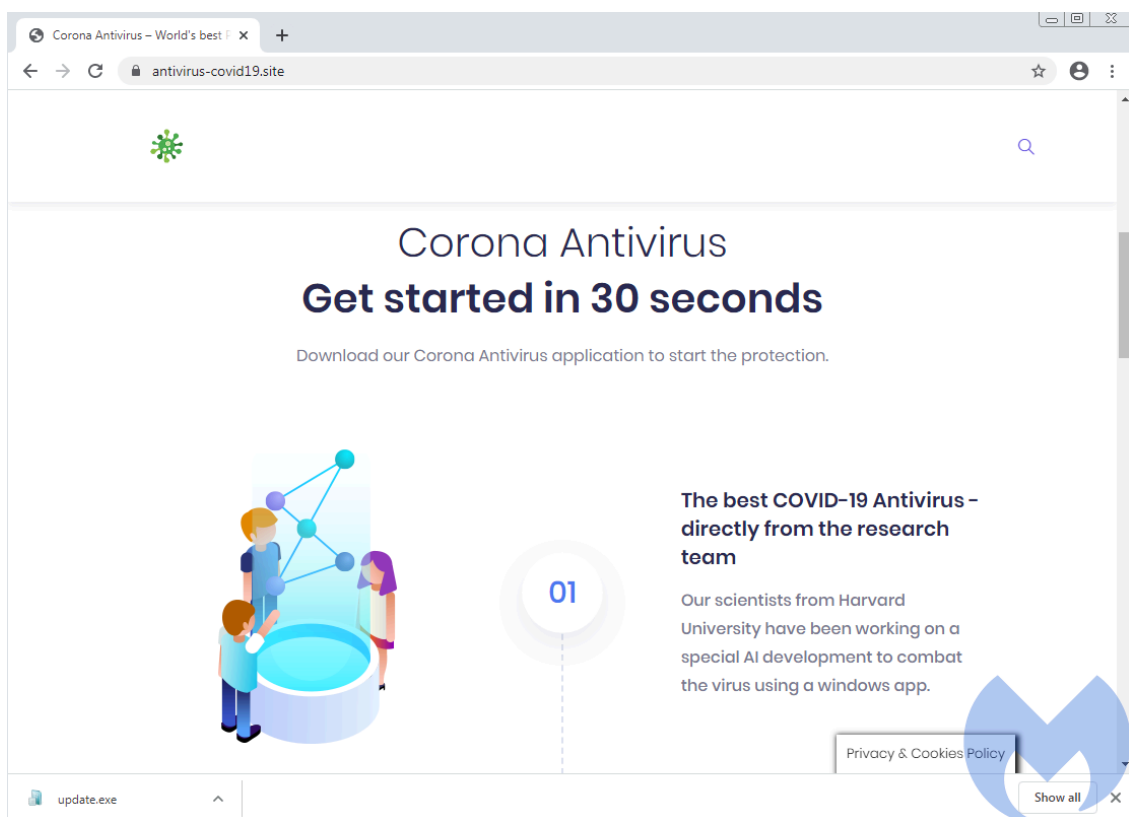
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

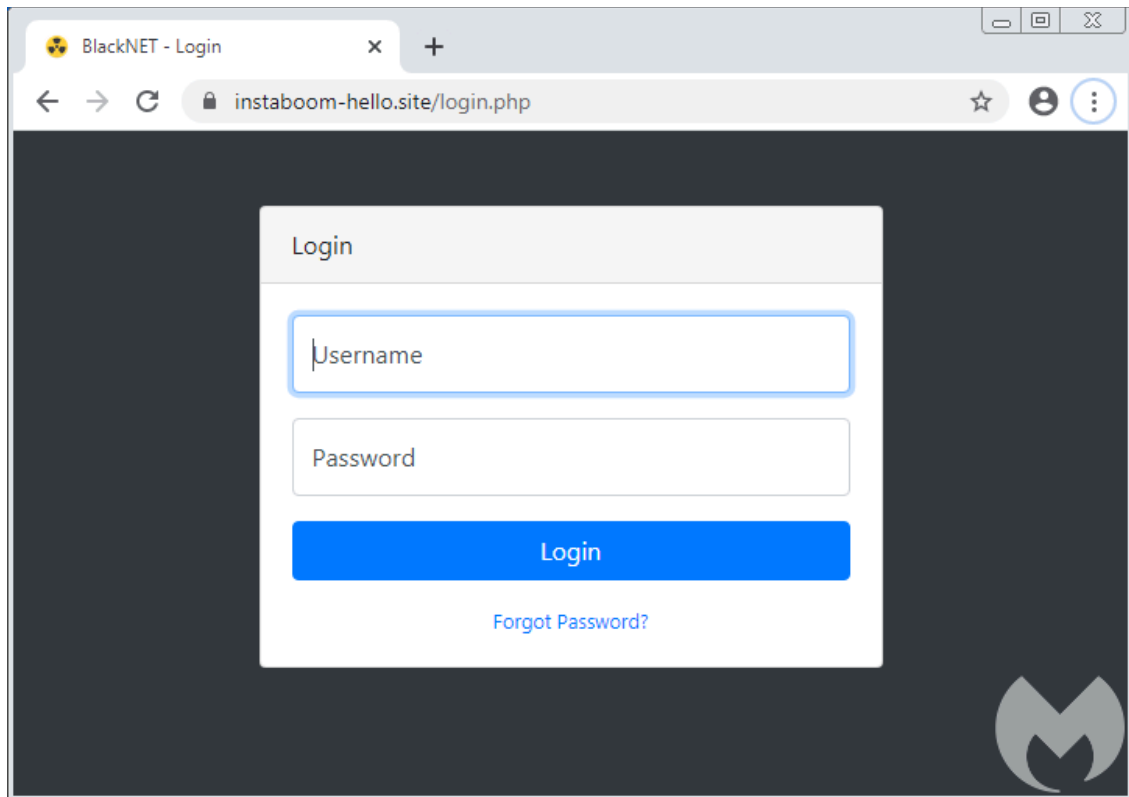


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. Below this, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

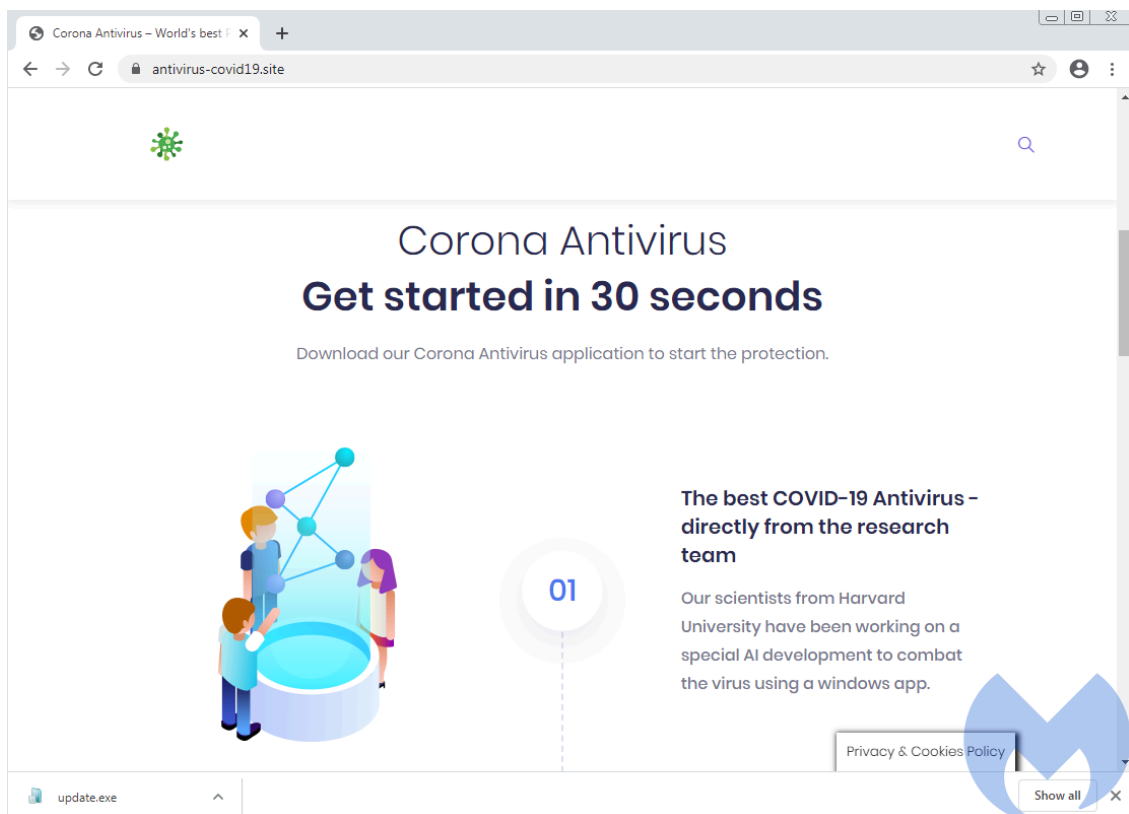
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

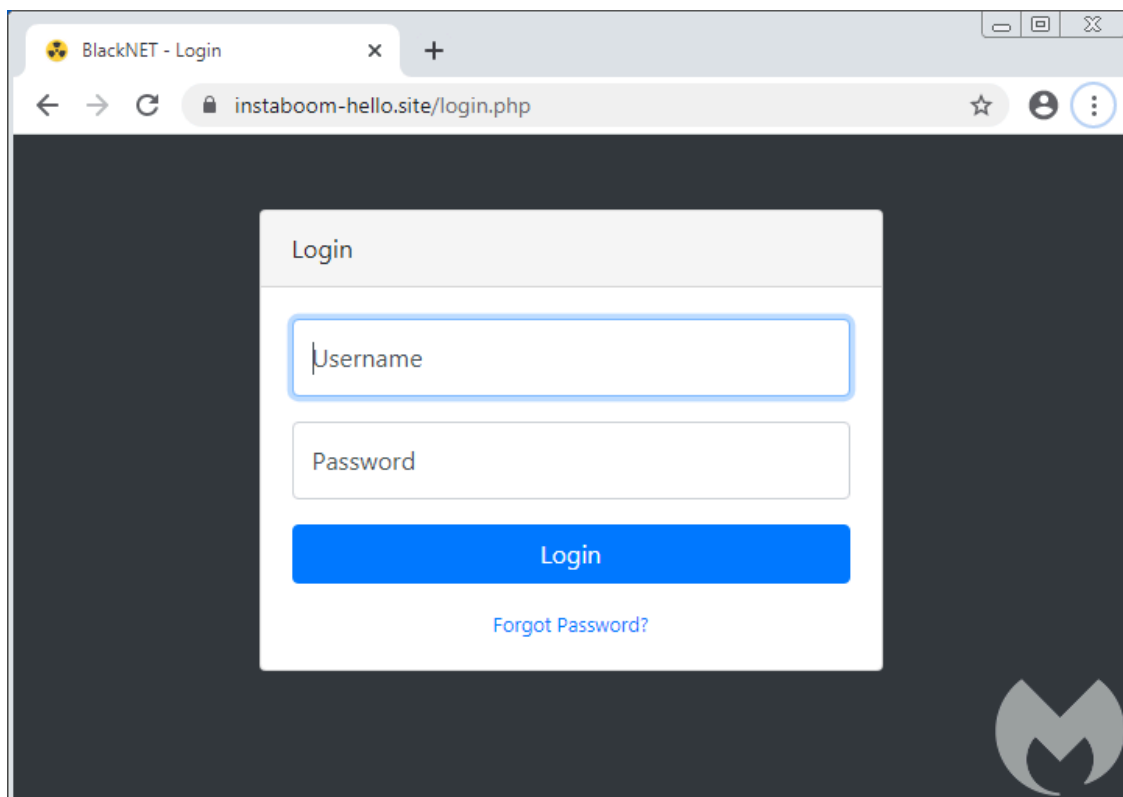


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a blue overlay. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

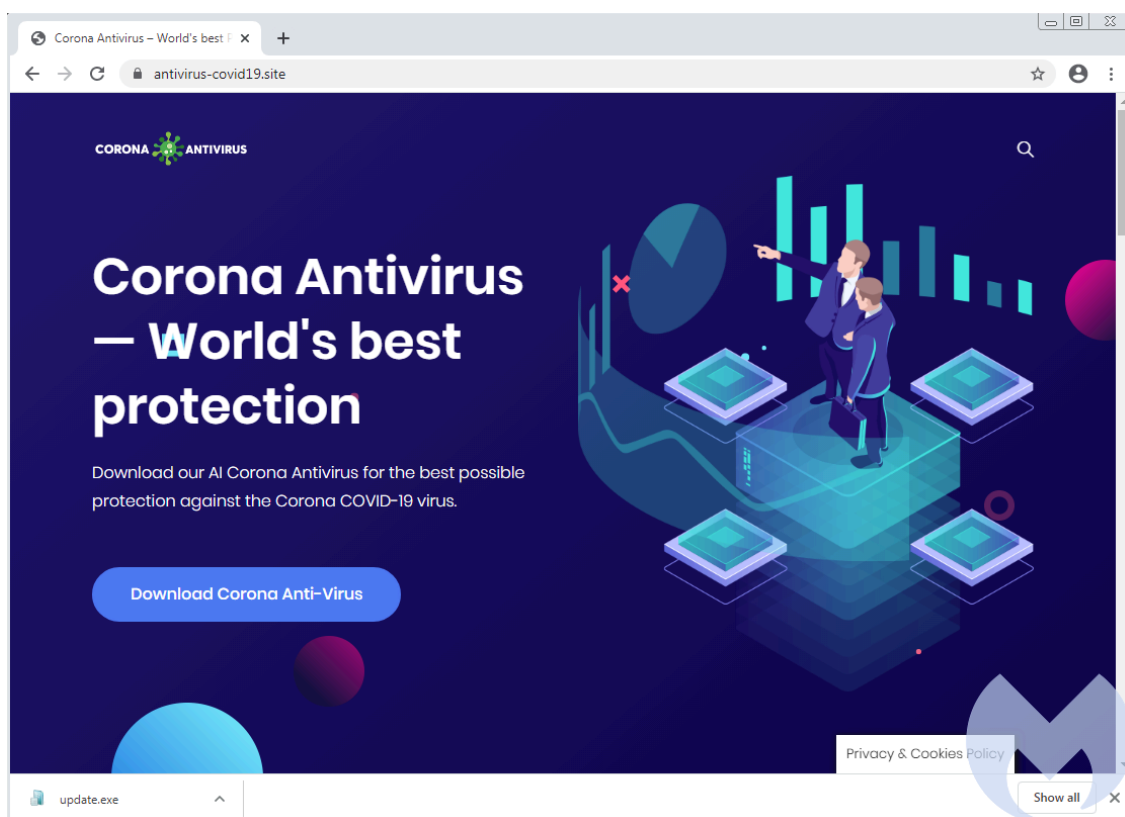
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

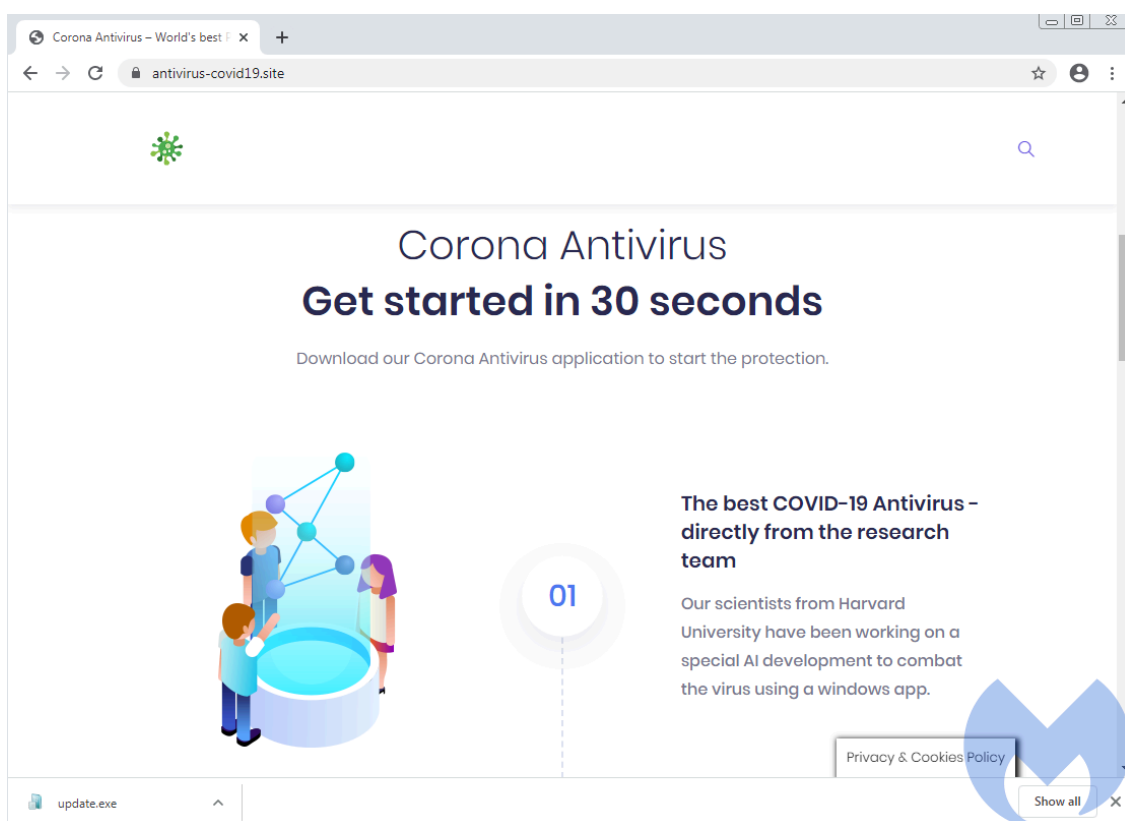
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

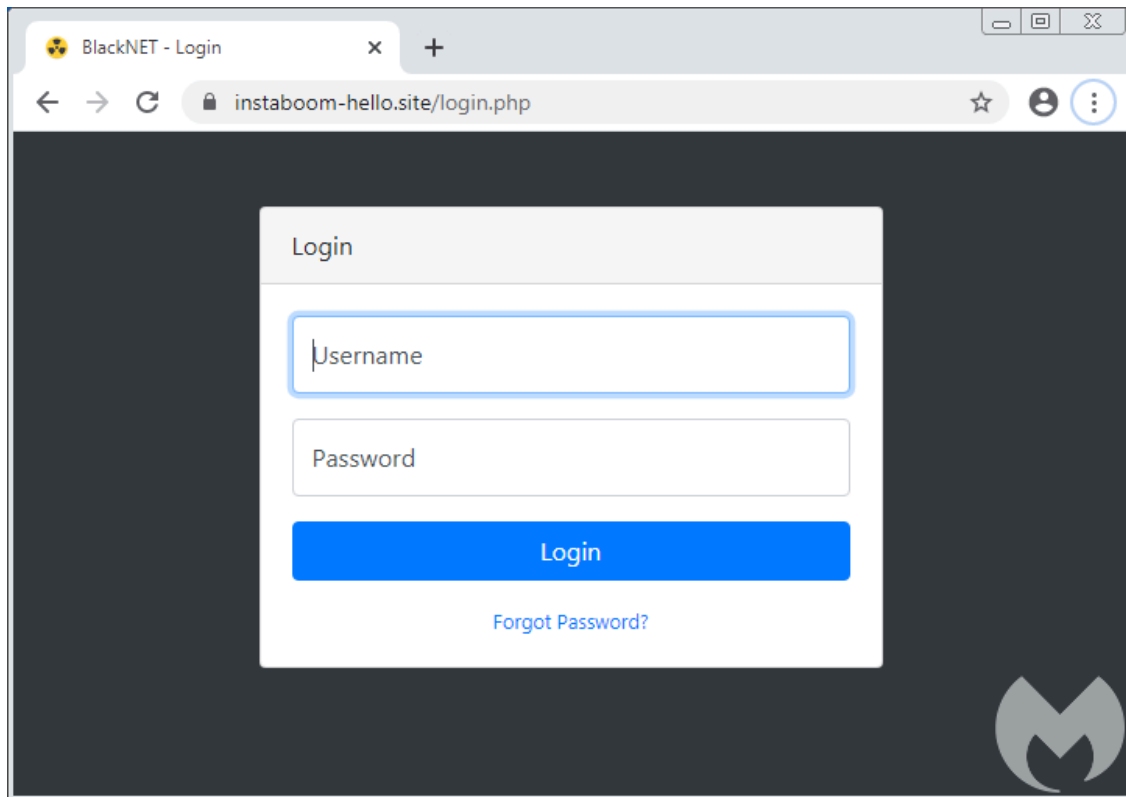


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

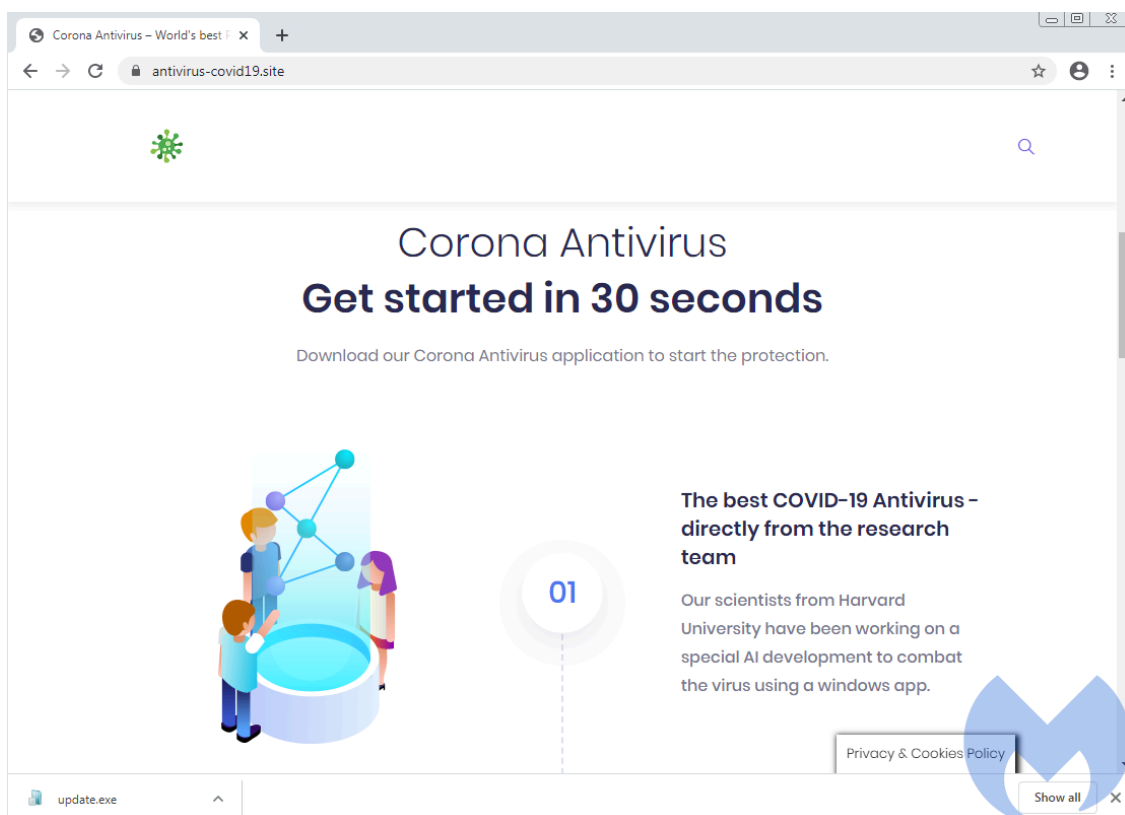
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

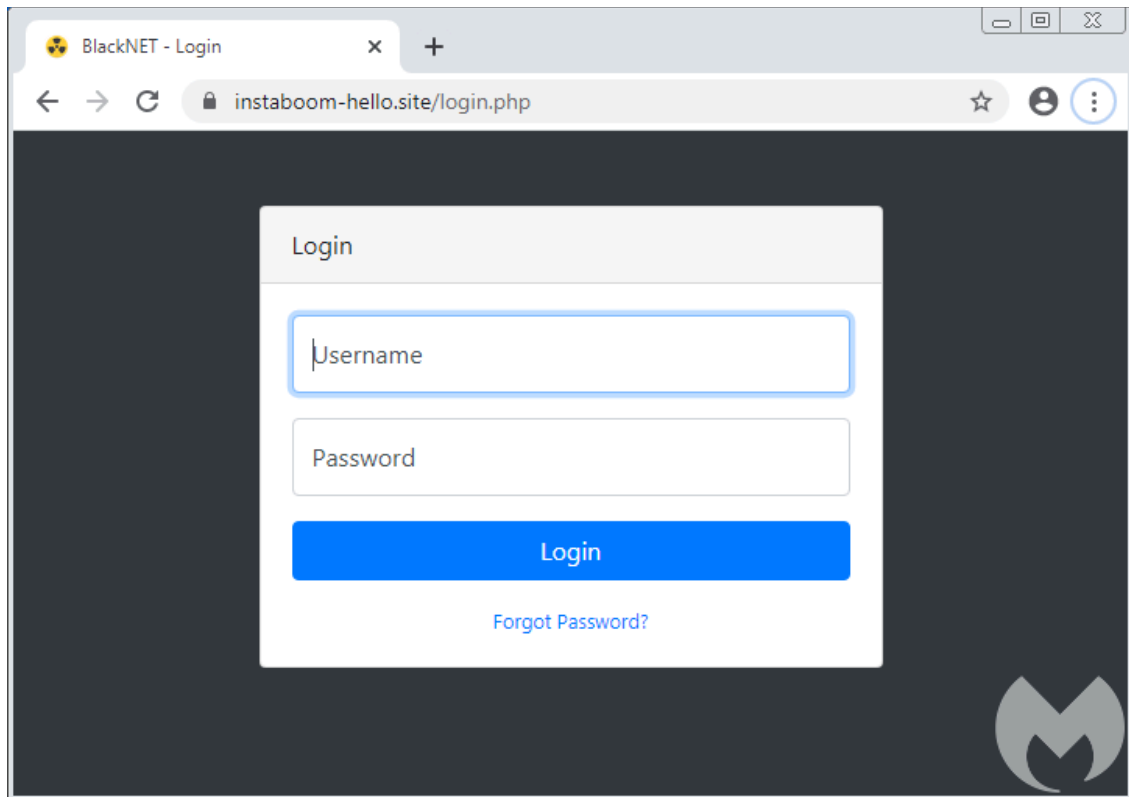


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

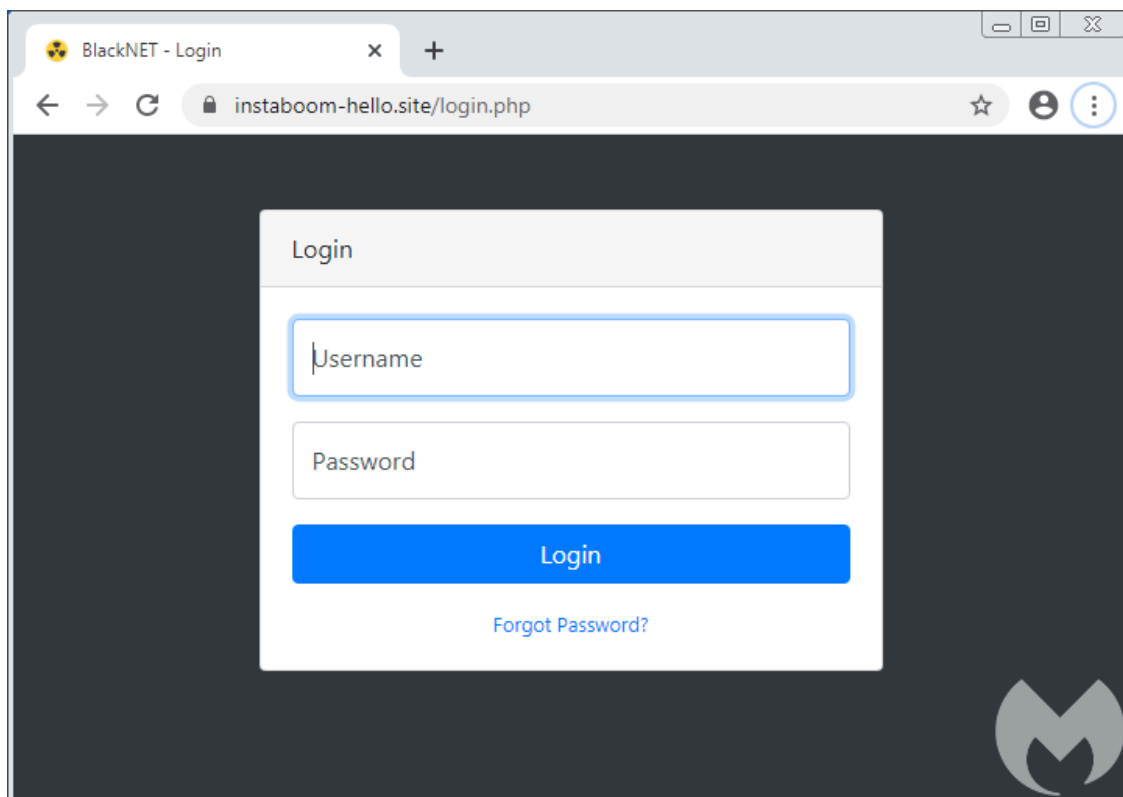
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

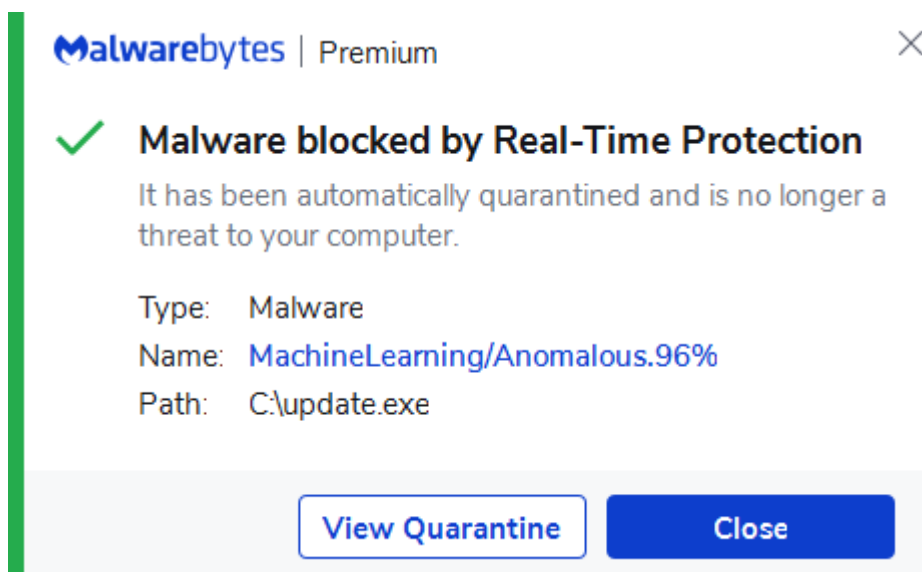
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

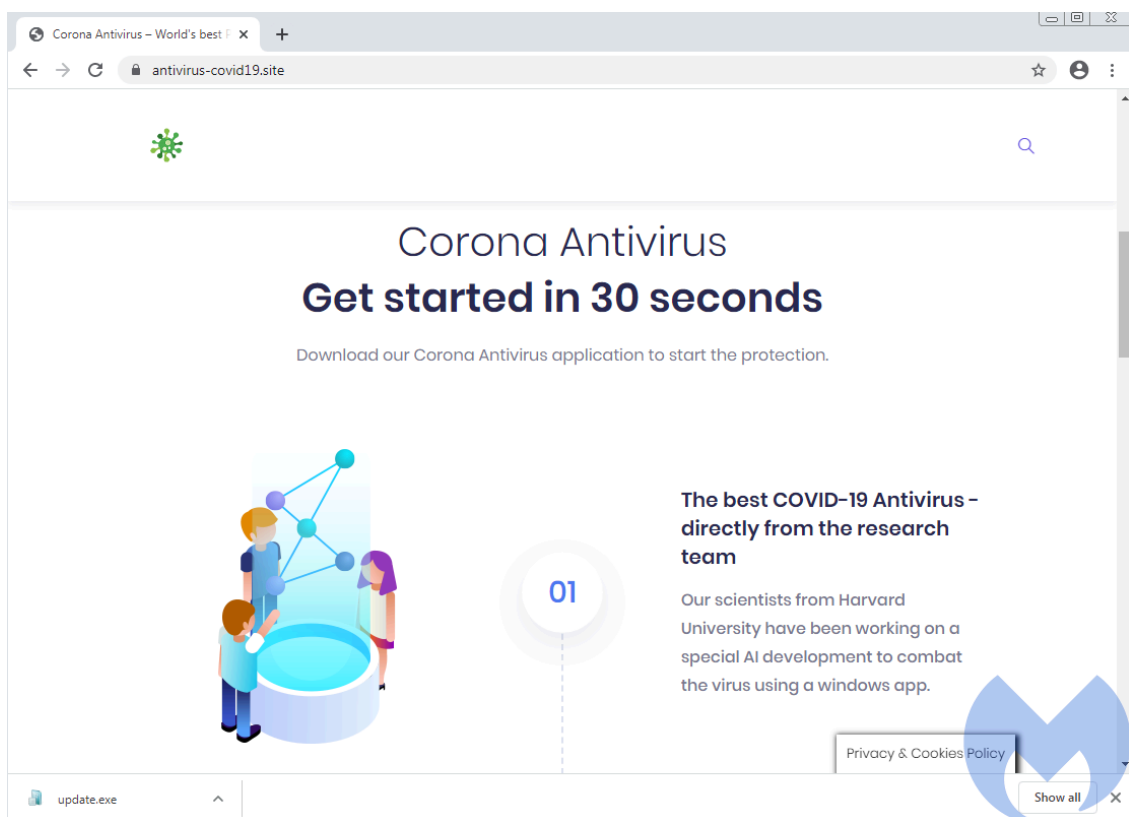
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

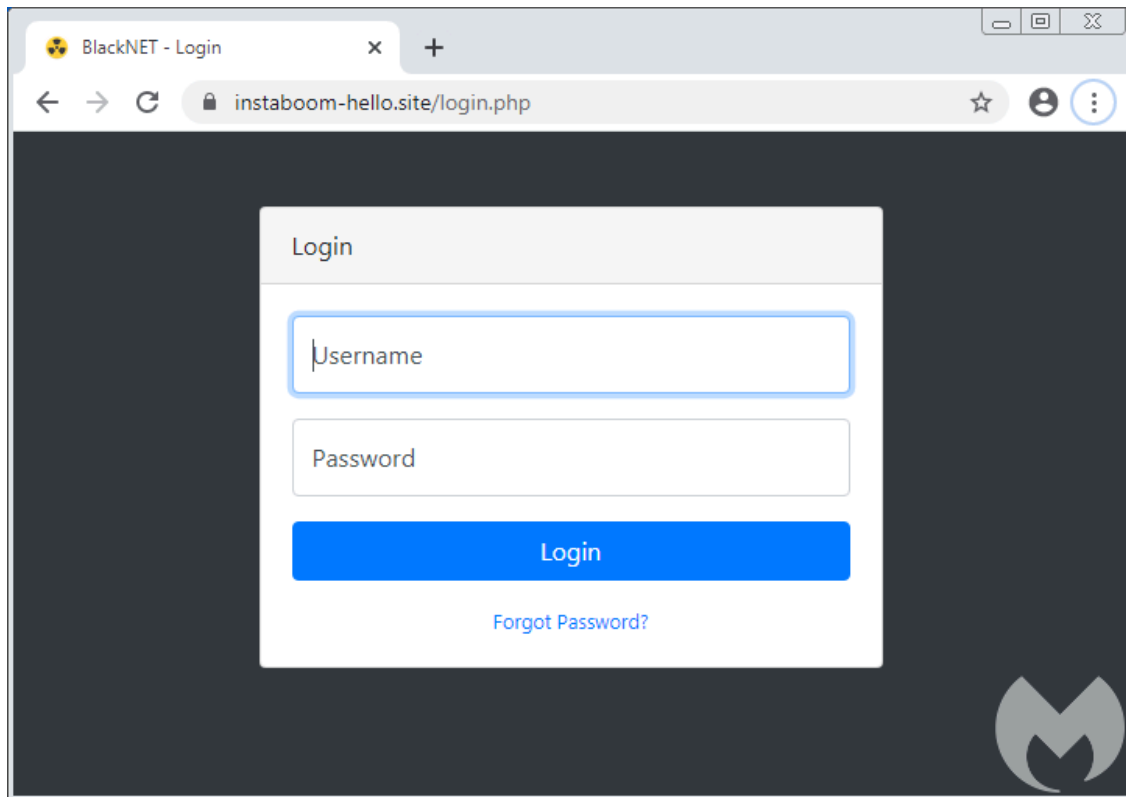


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

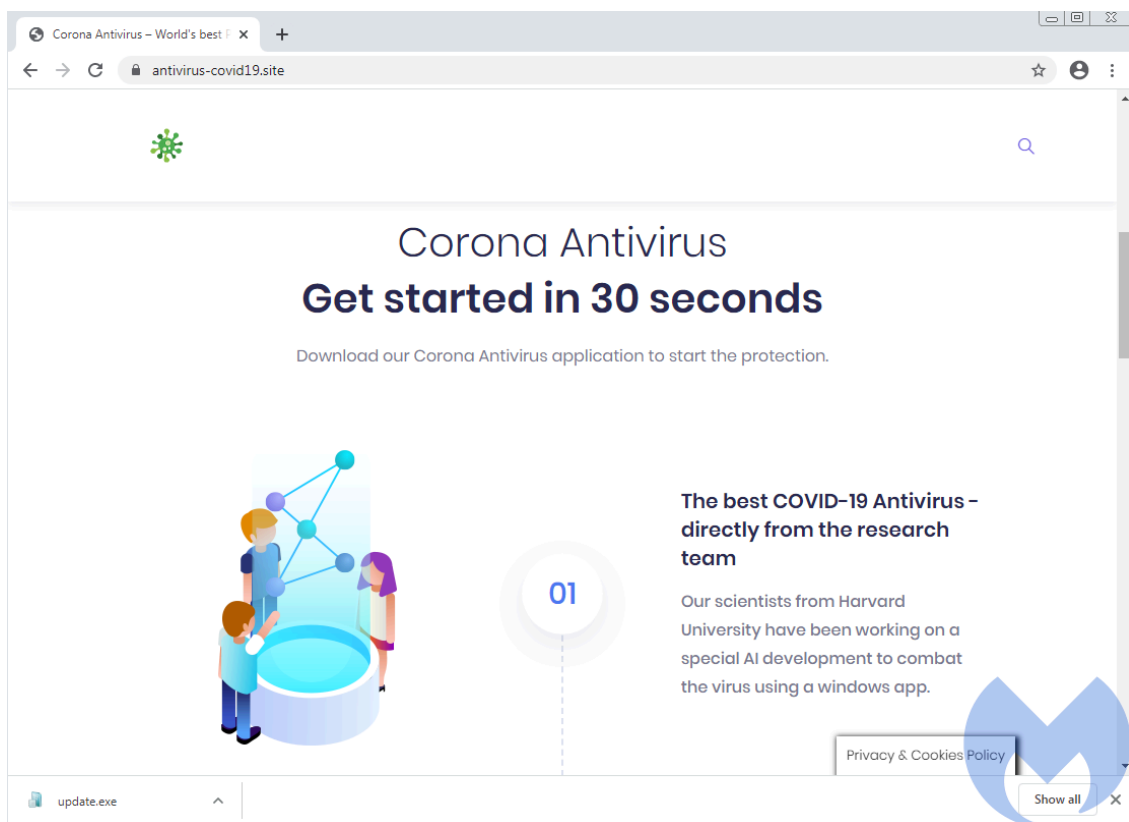
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

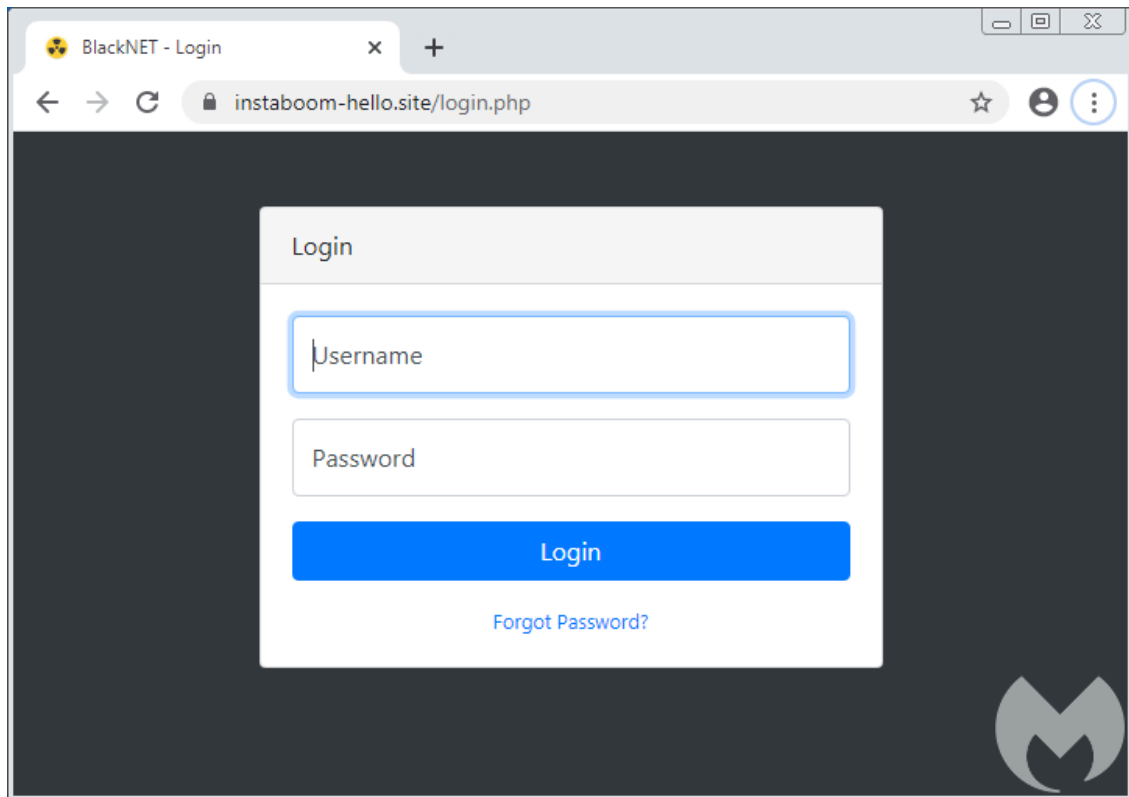


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a few blue dots representing clients. At the bottom, there's a footer with the text "Copyright © BLACKNET by Black.Hacker - 2020" and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, it lists the details: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

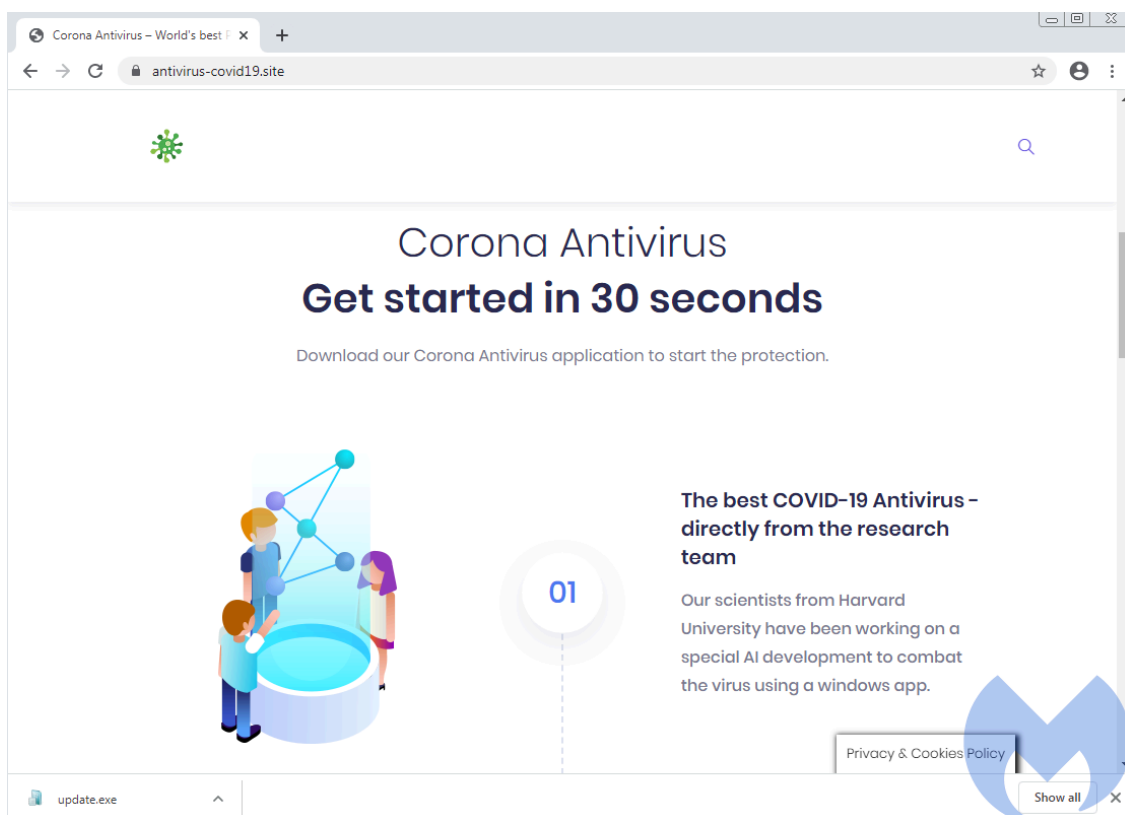
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

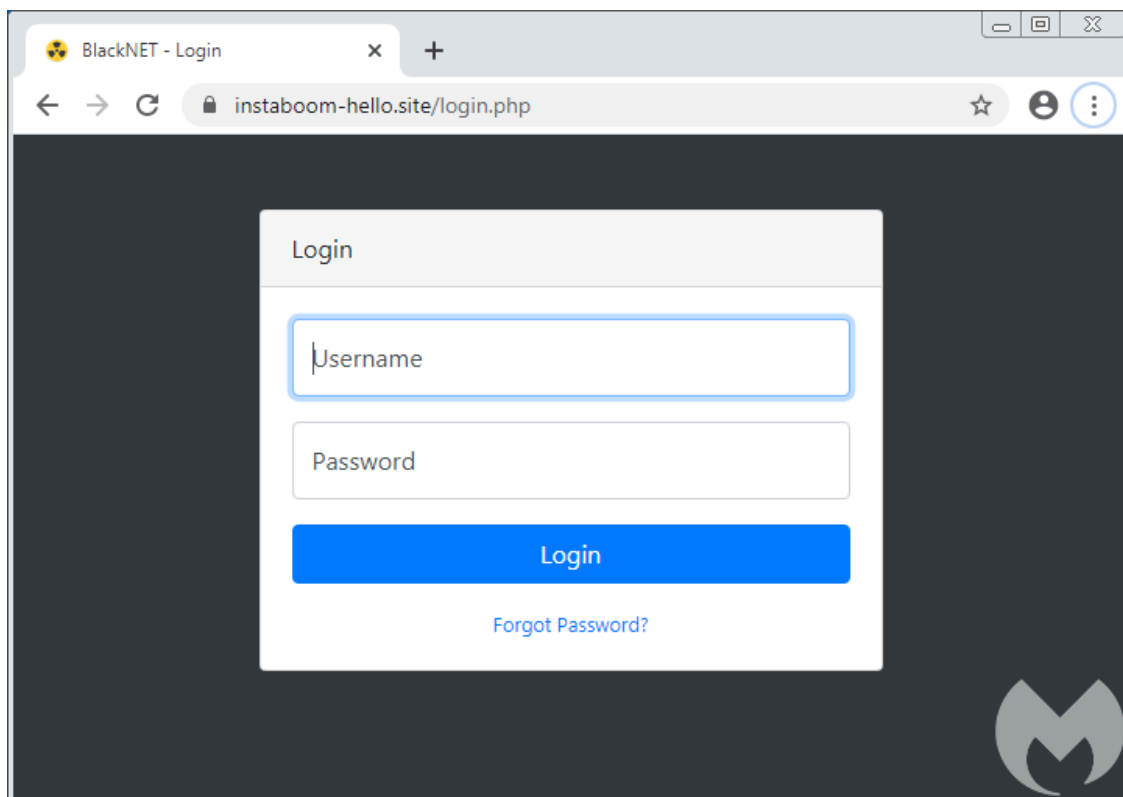
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

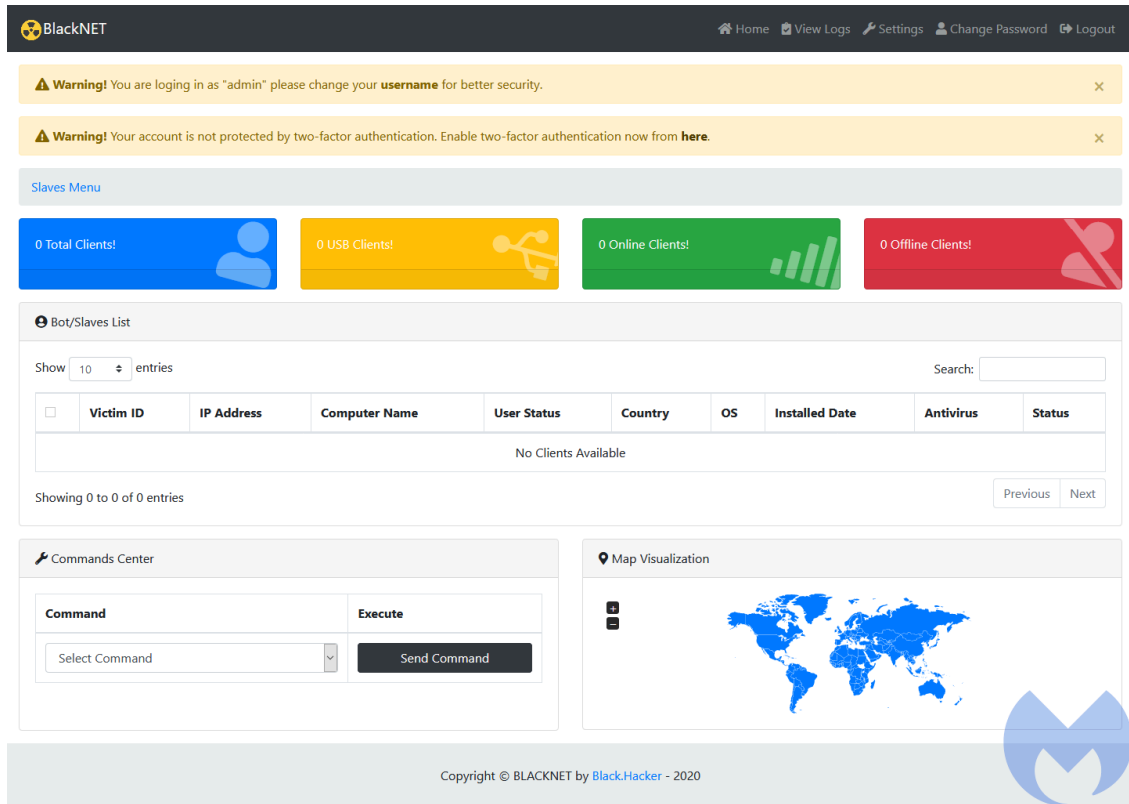
```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

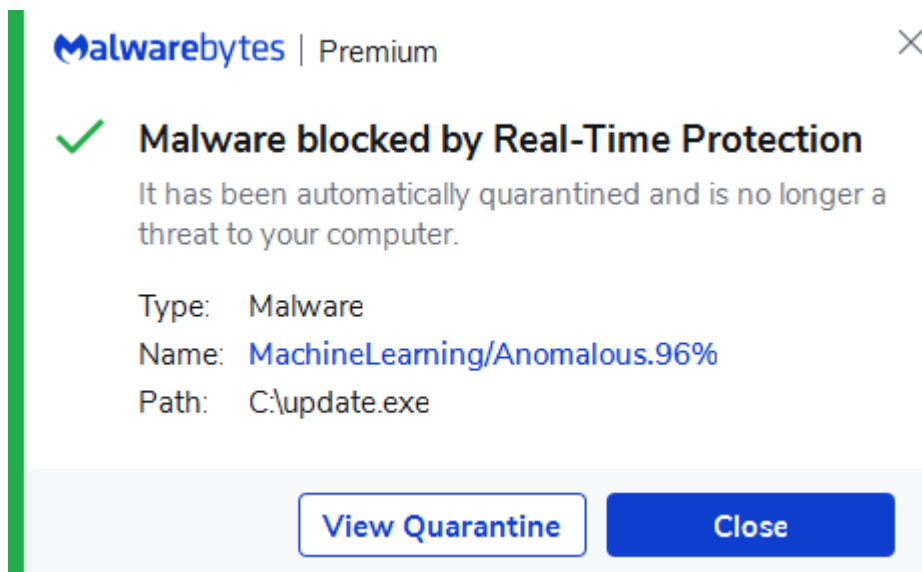


Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

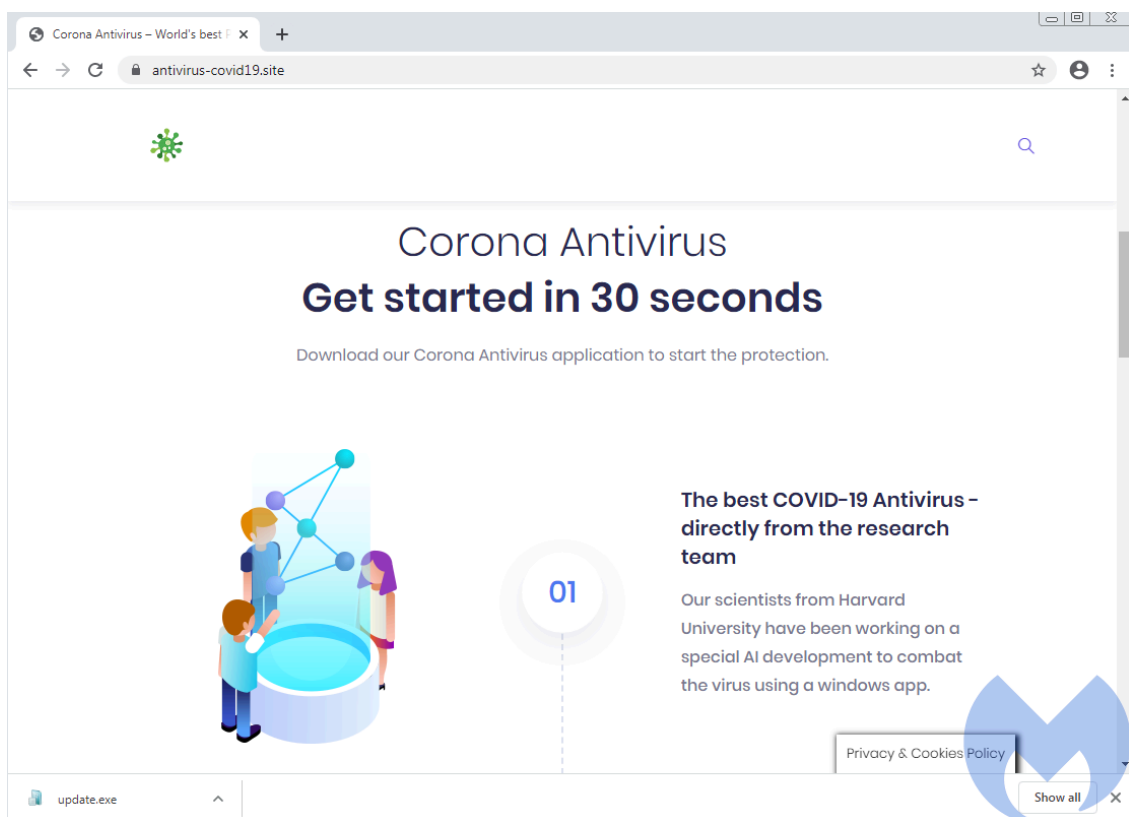
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

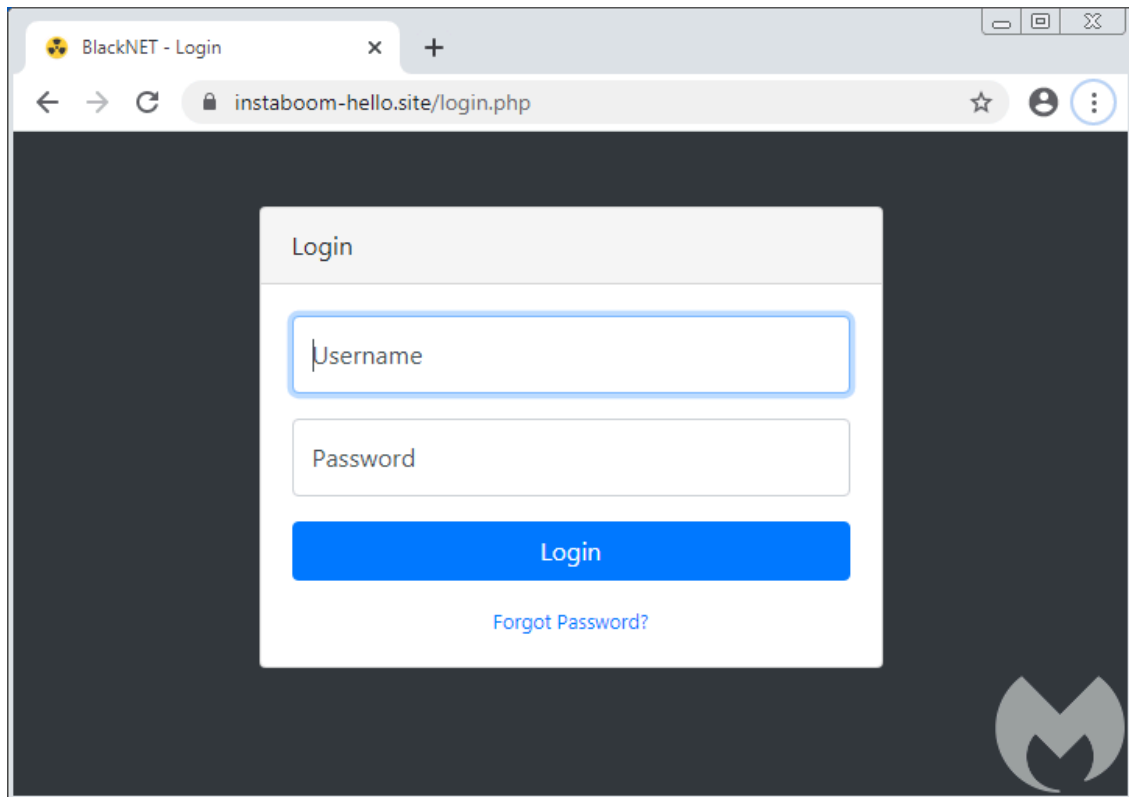


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

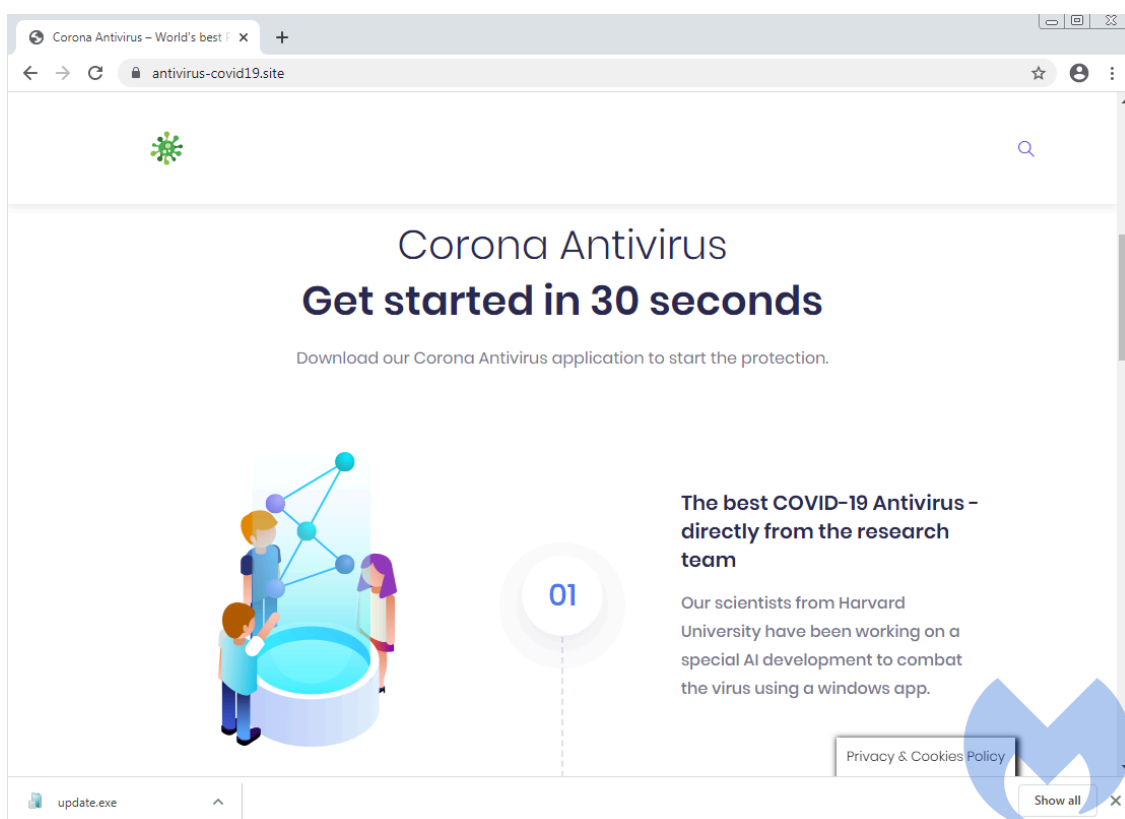
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

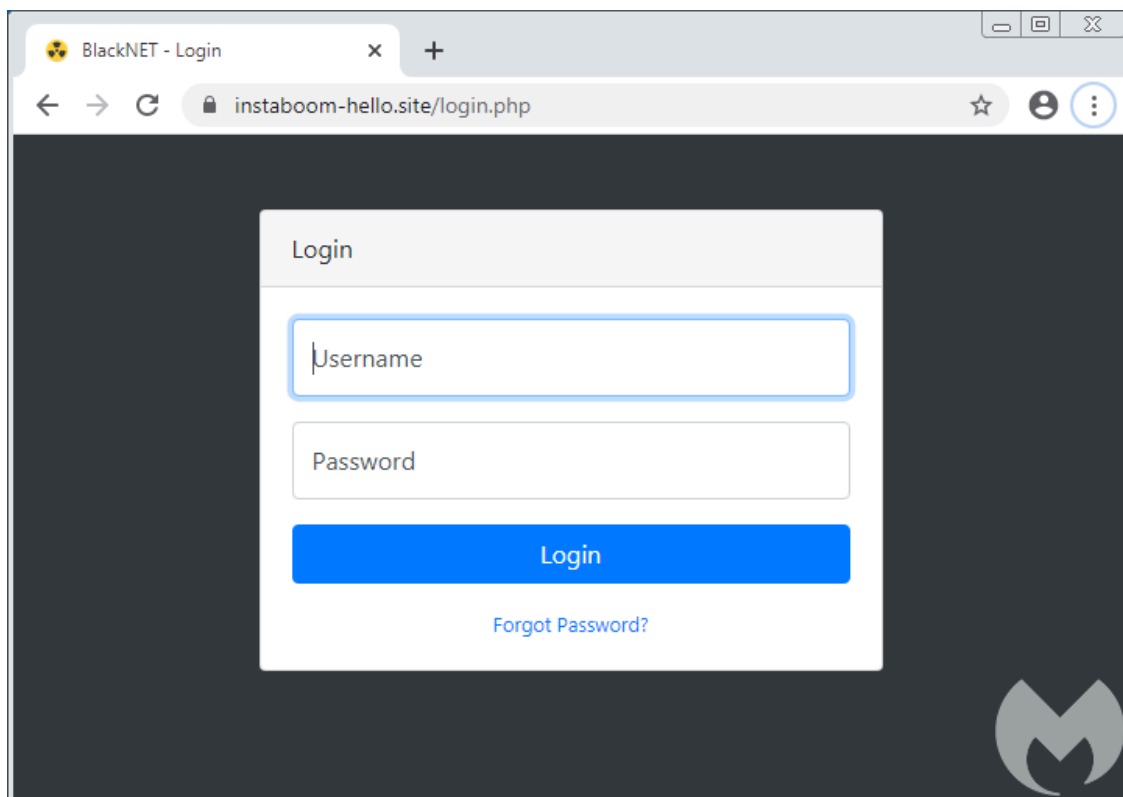


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

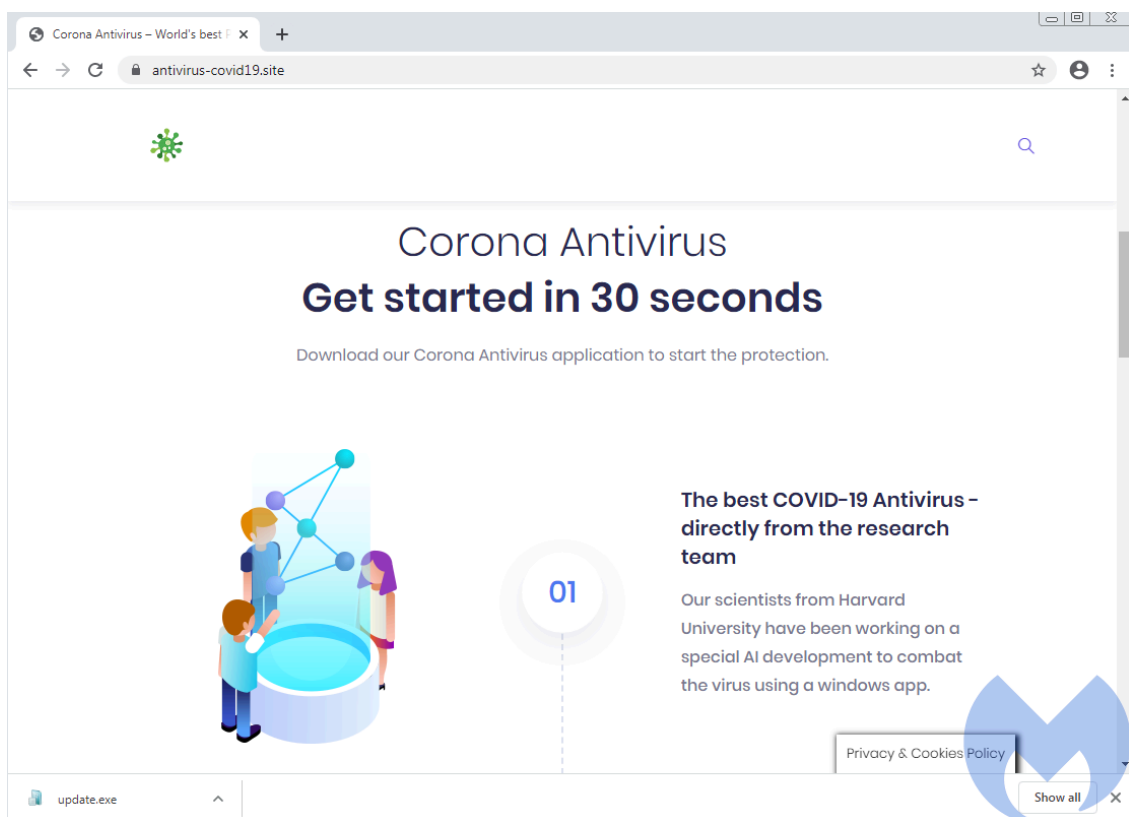
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

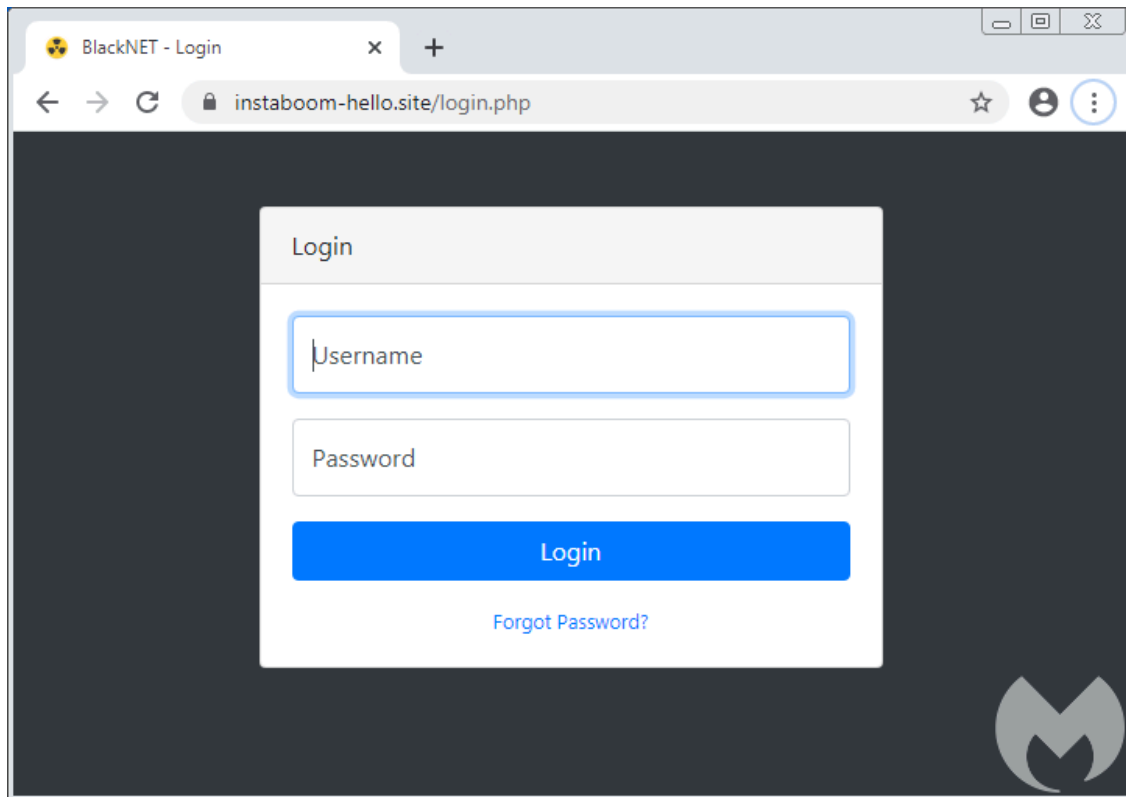


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

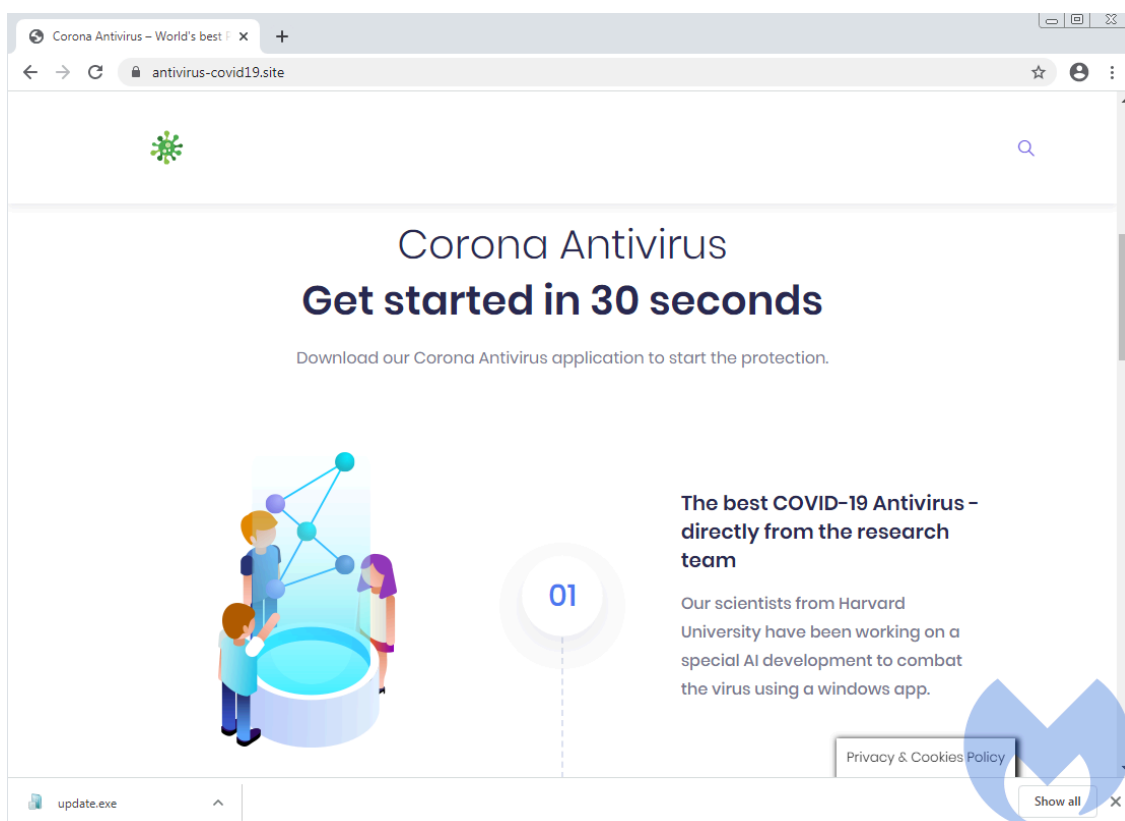
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

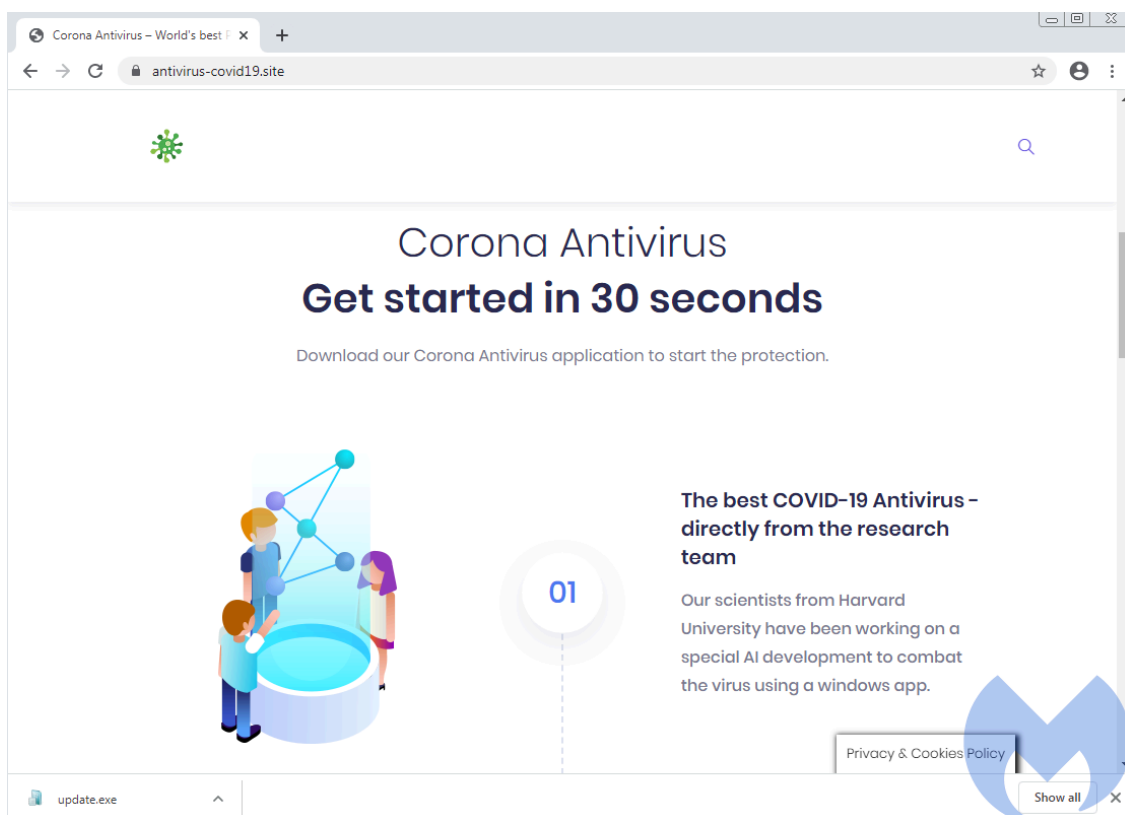
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

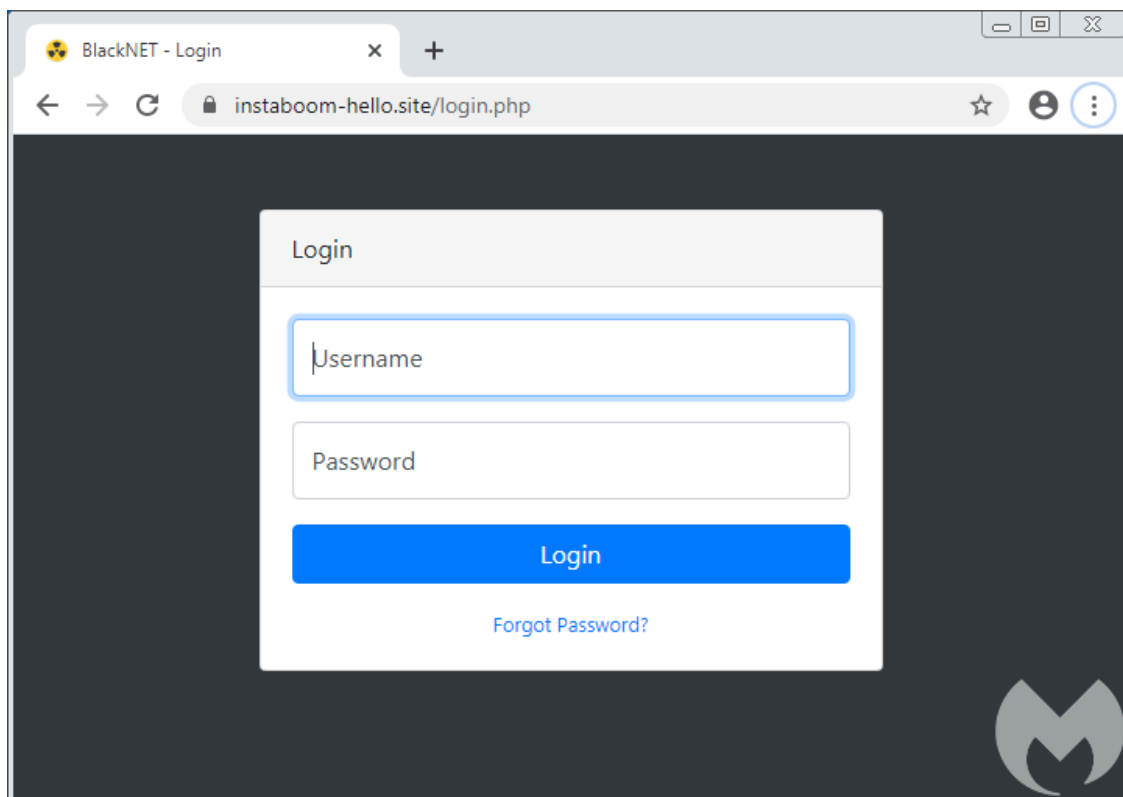
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

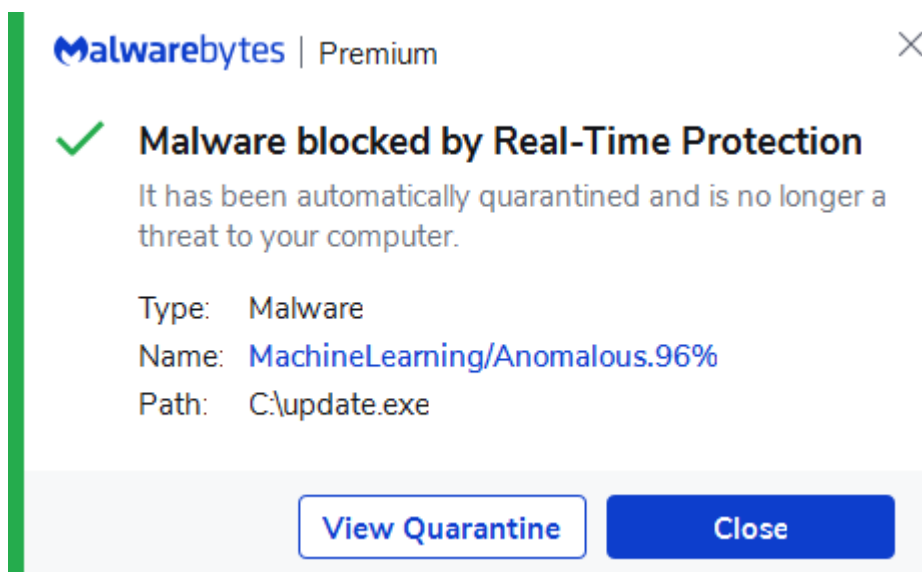
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

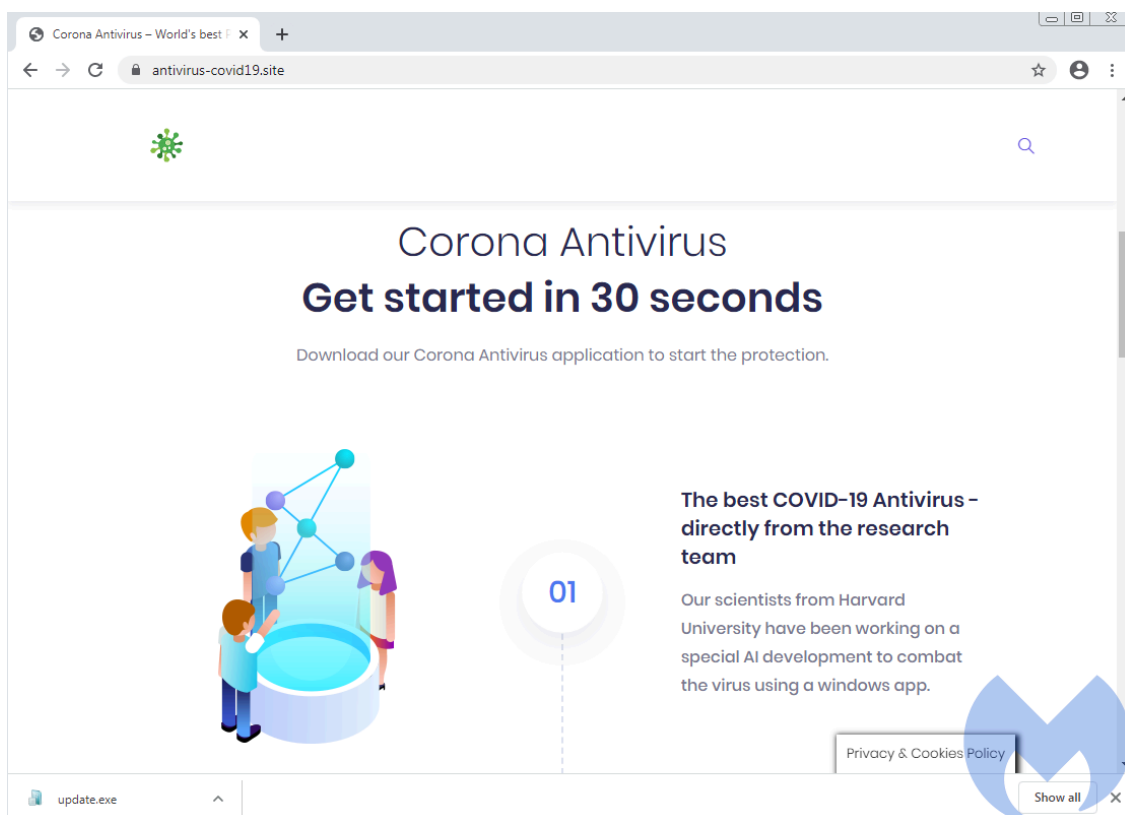
C2 panel

```
instaboom-hello[.]site
```




To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

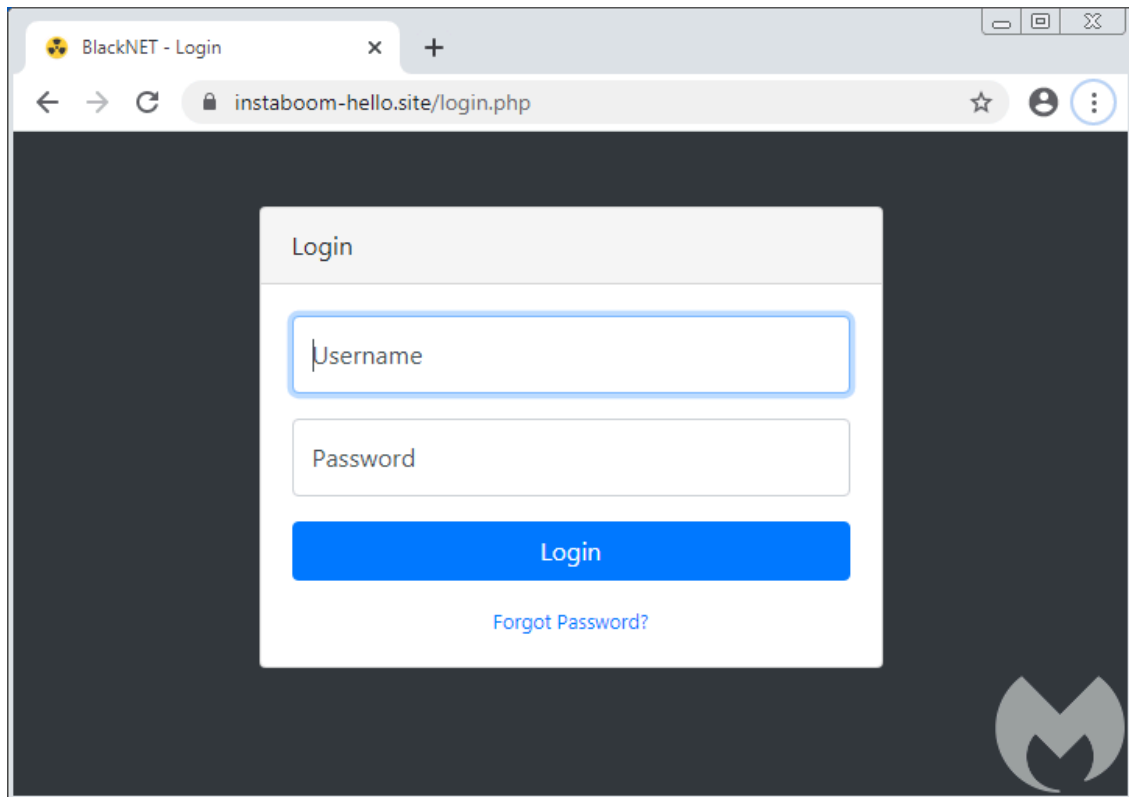


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

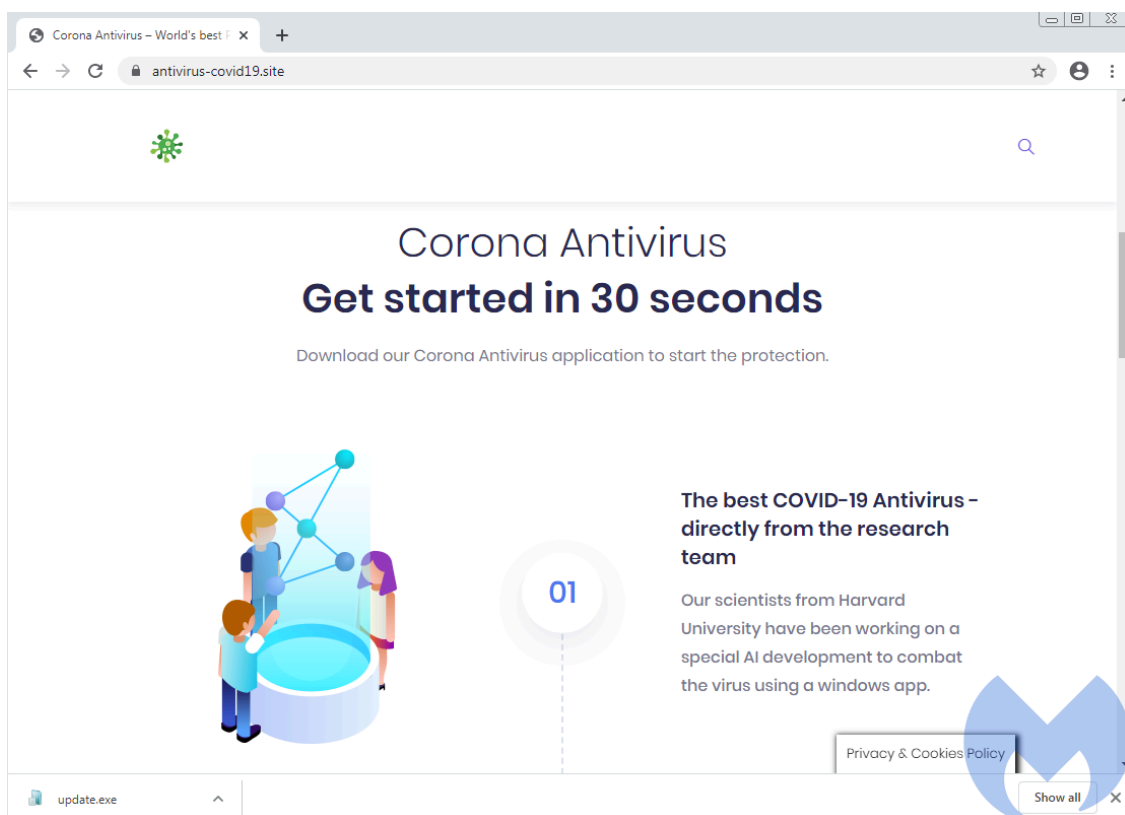
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

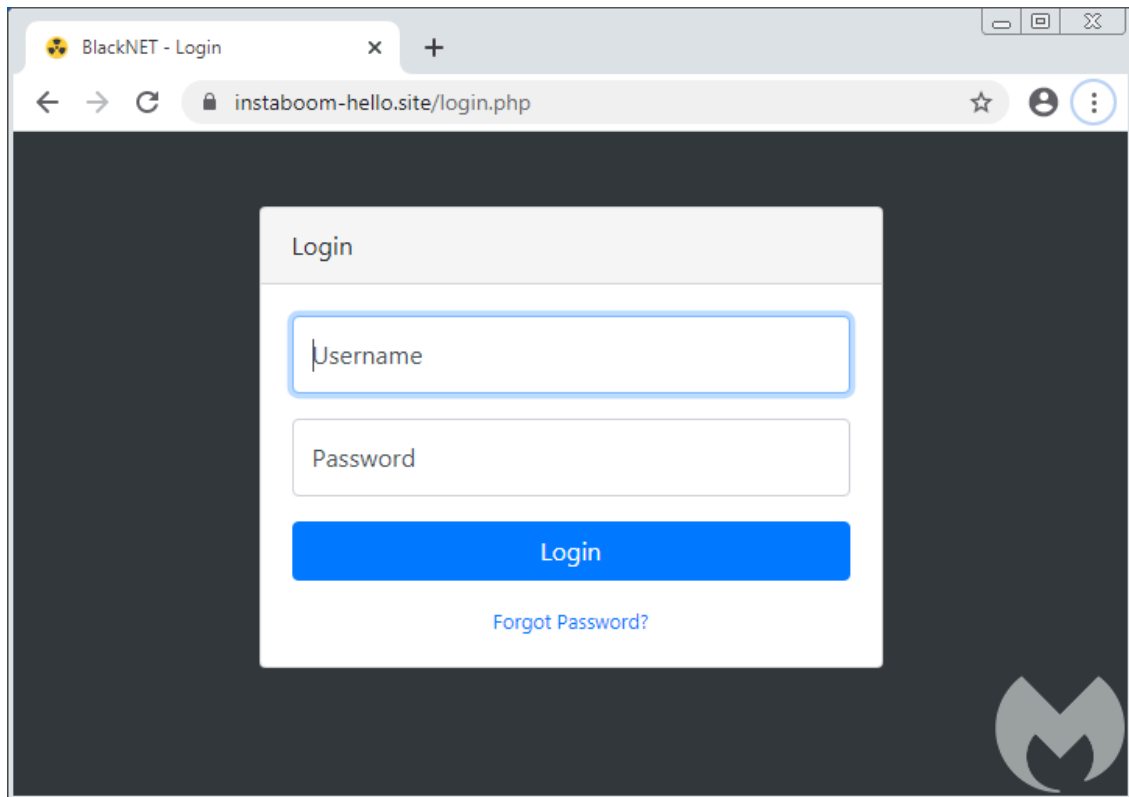


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

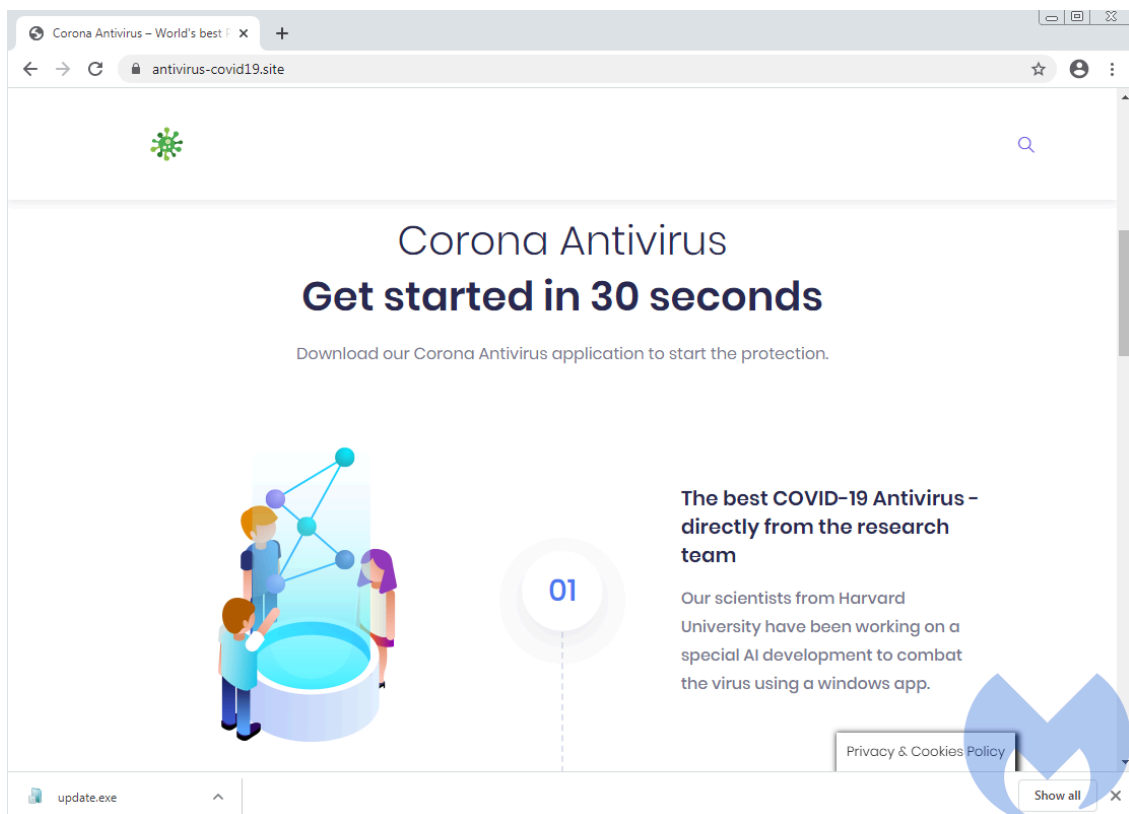
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

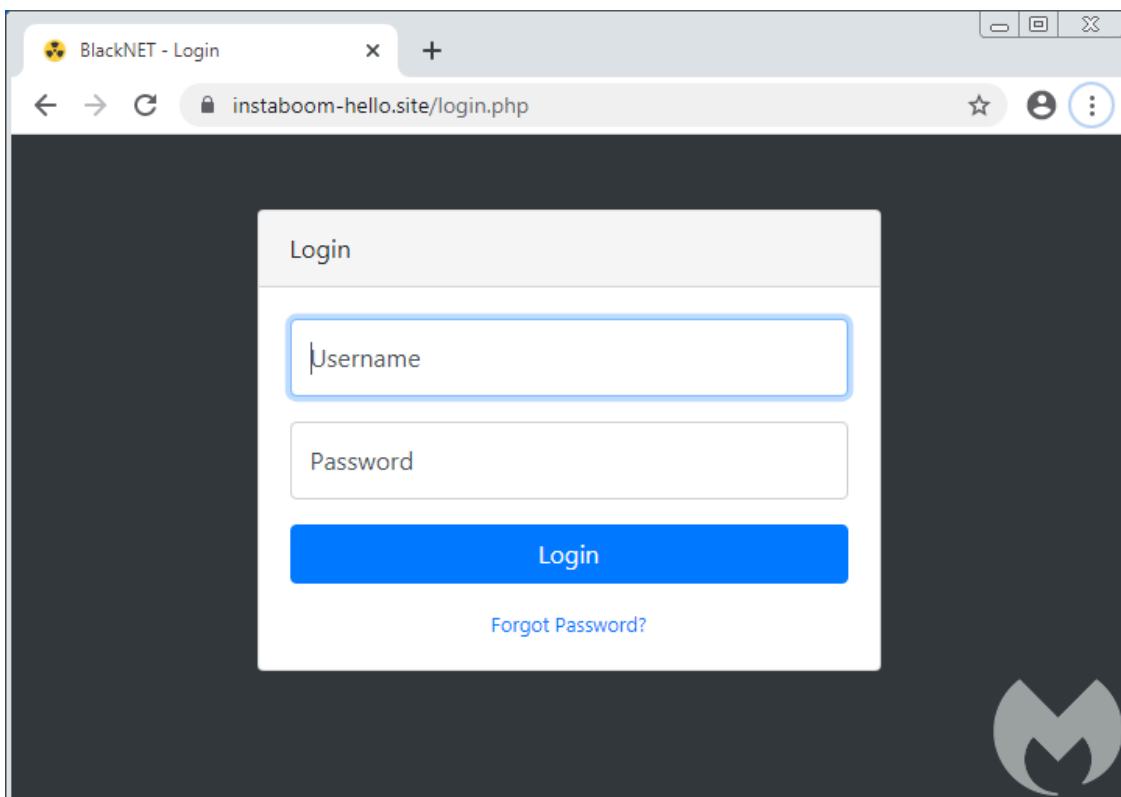


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

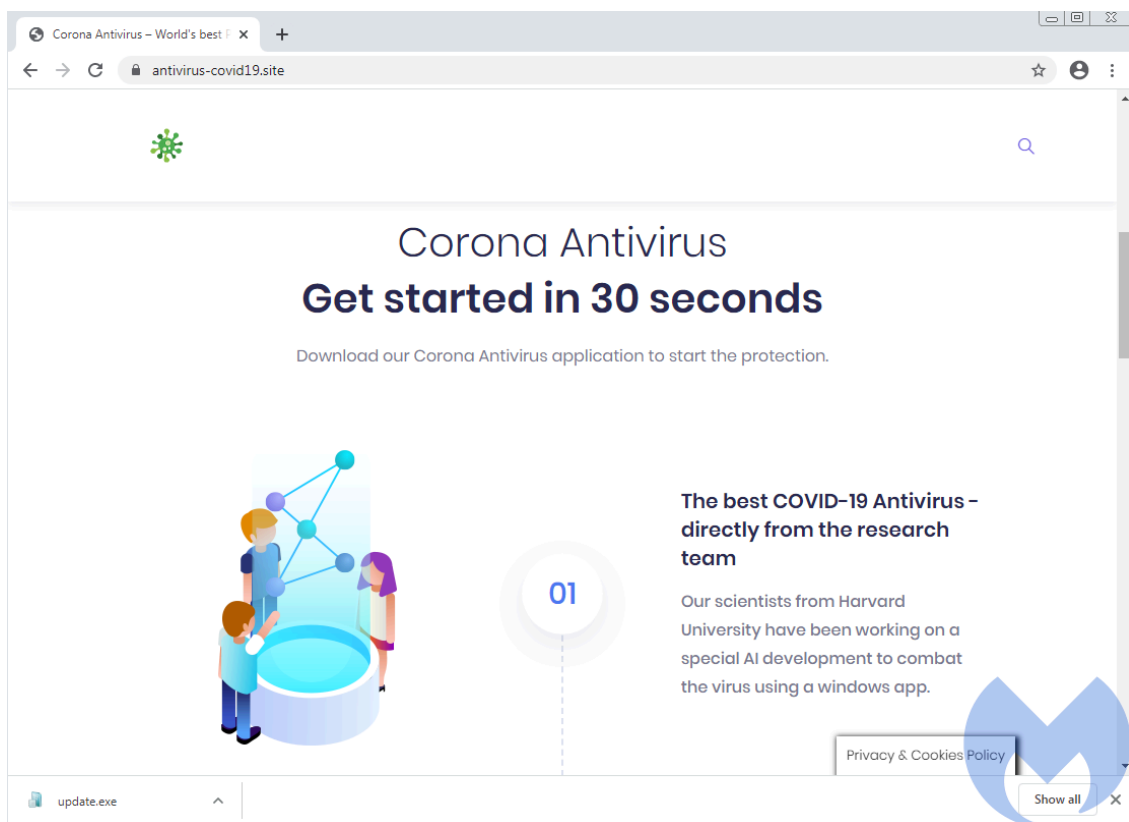
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

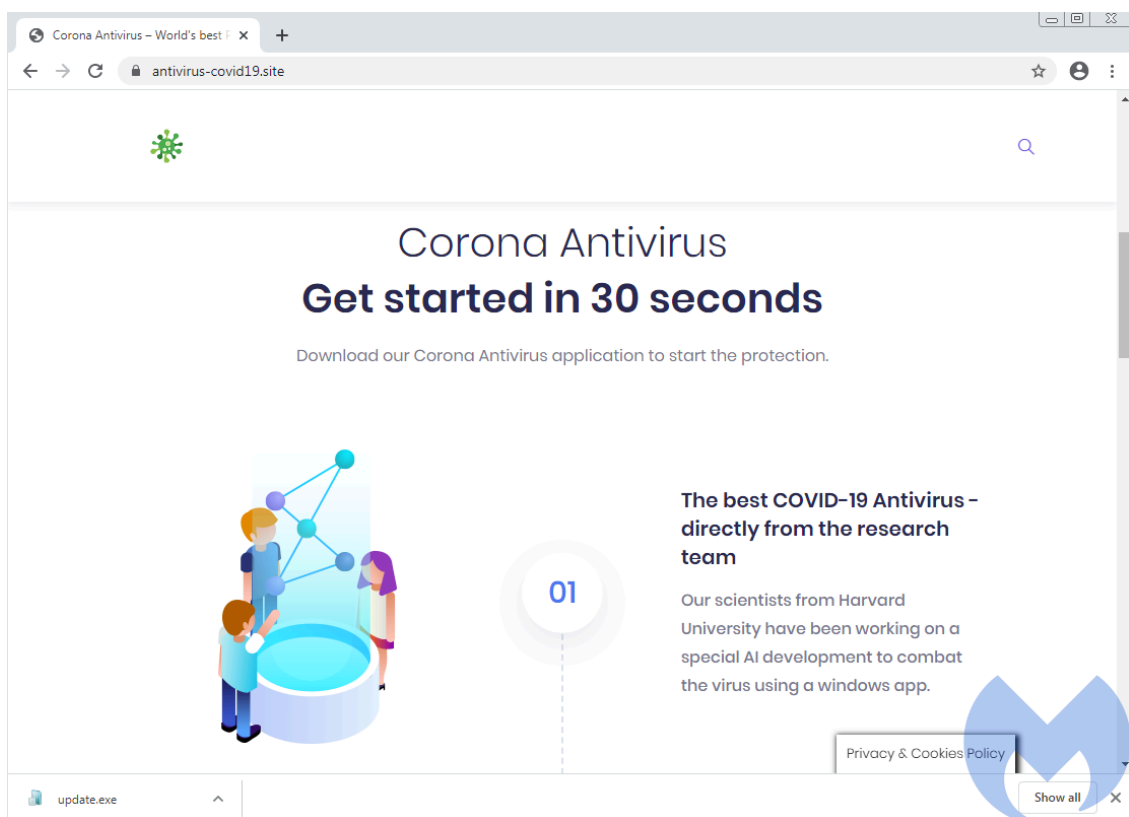
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

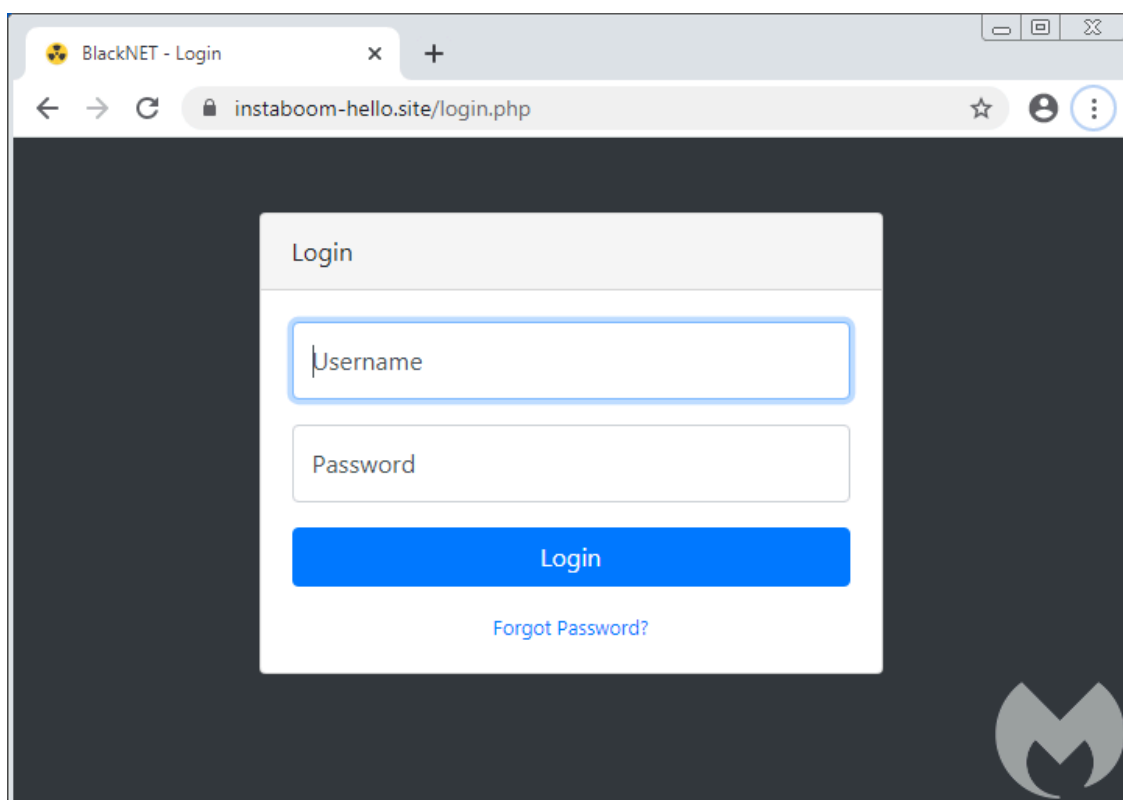
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

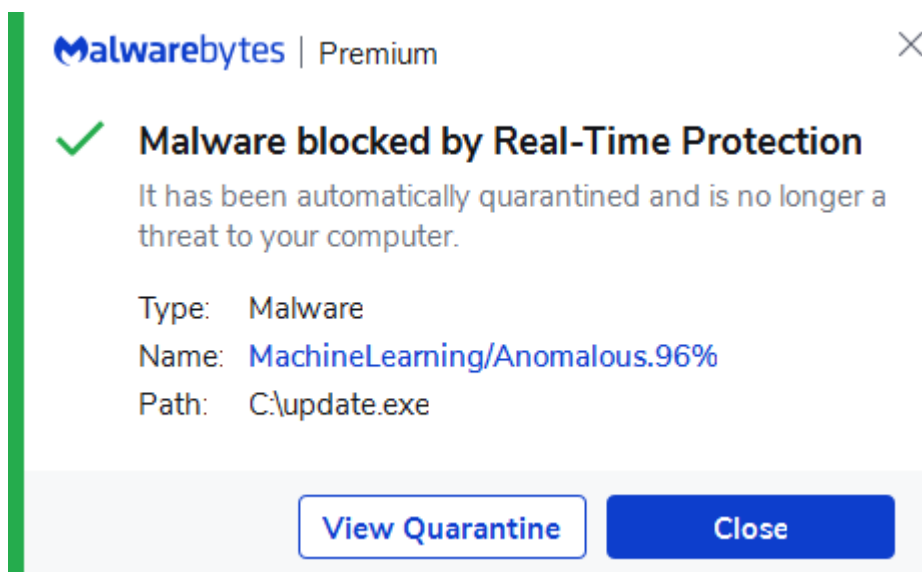
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

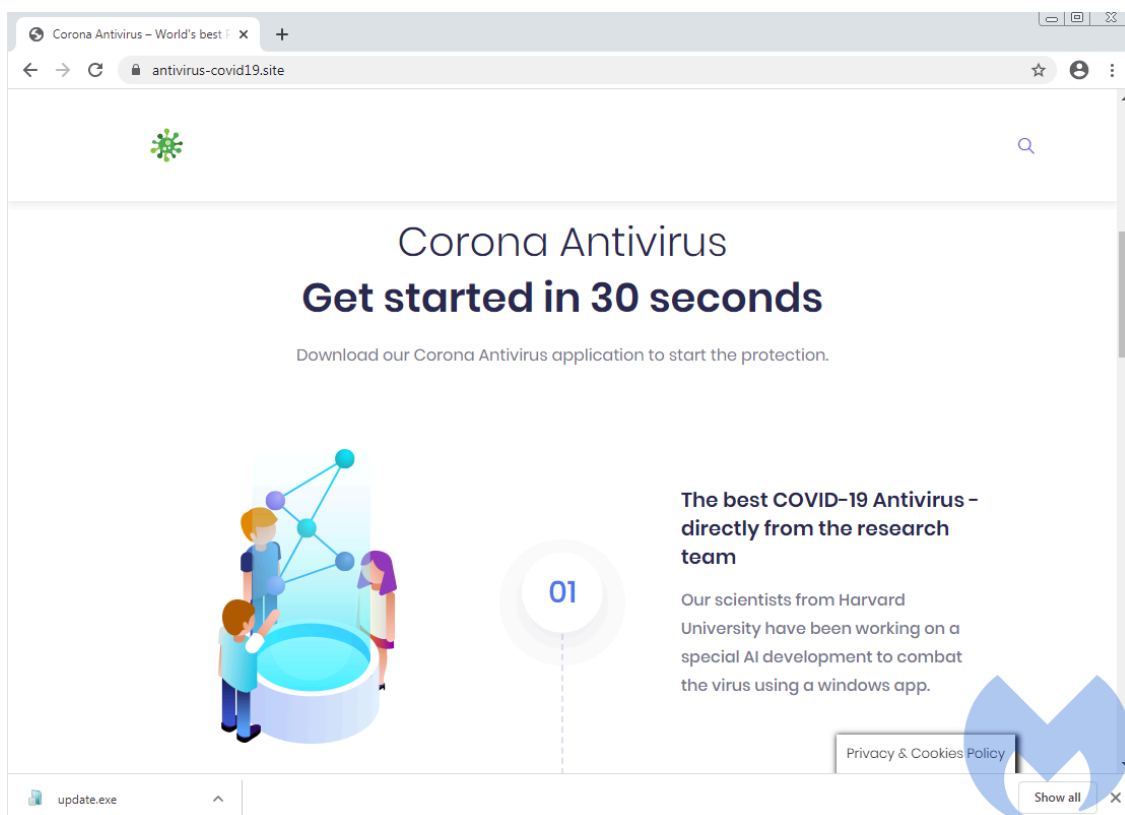
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

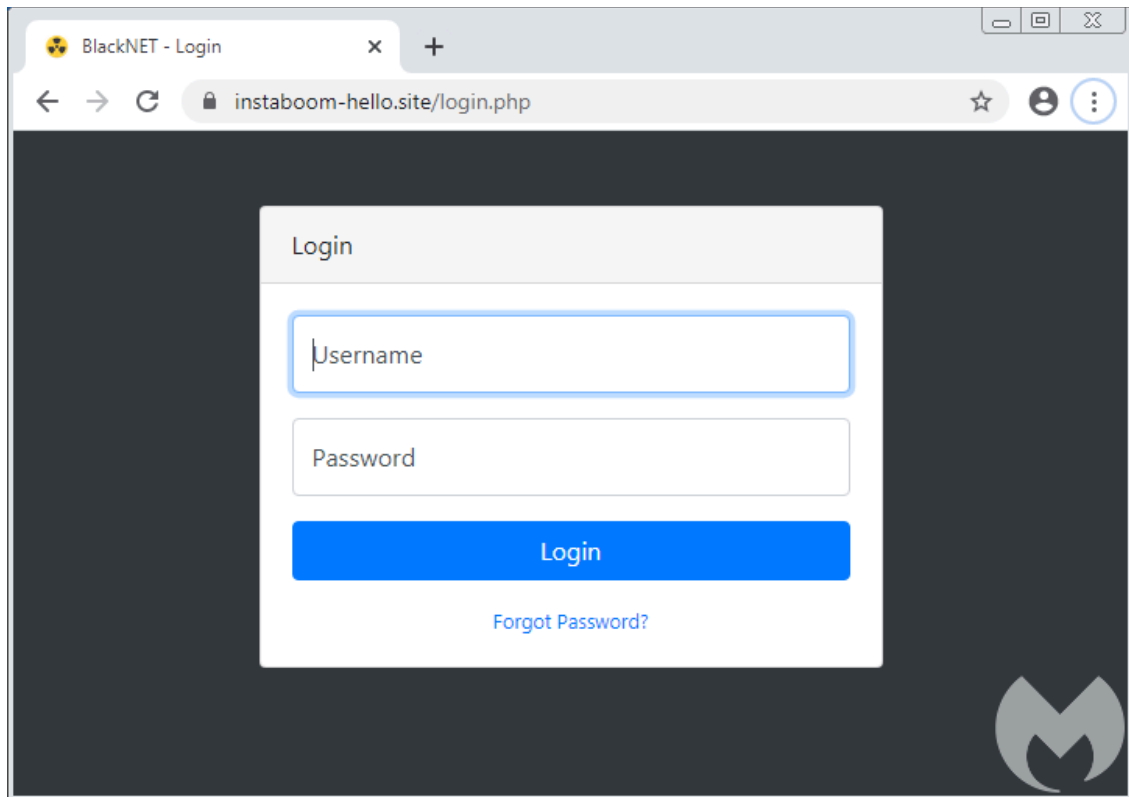



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a few blue dots indicating client locations. At the bottom, a copyright notice reads "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, the details are listed: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

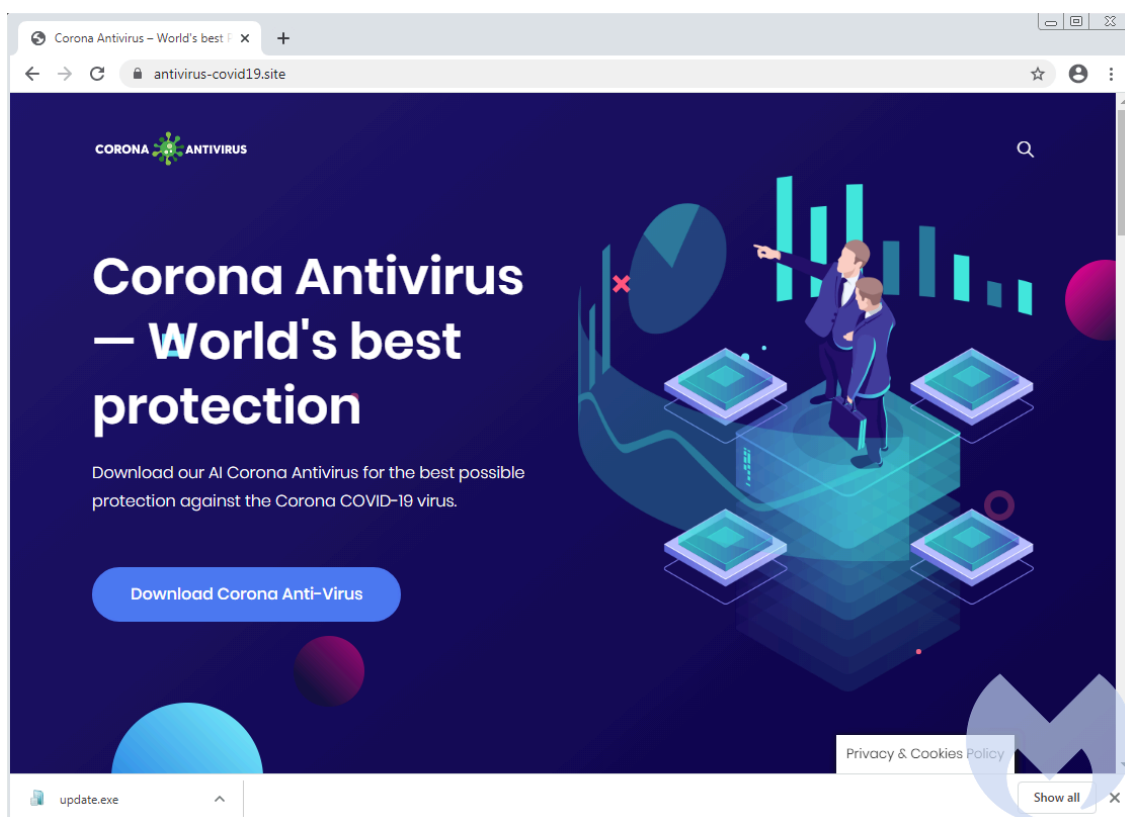
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

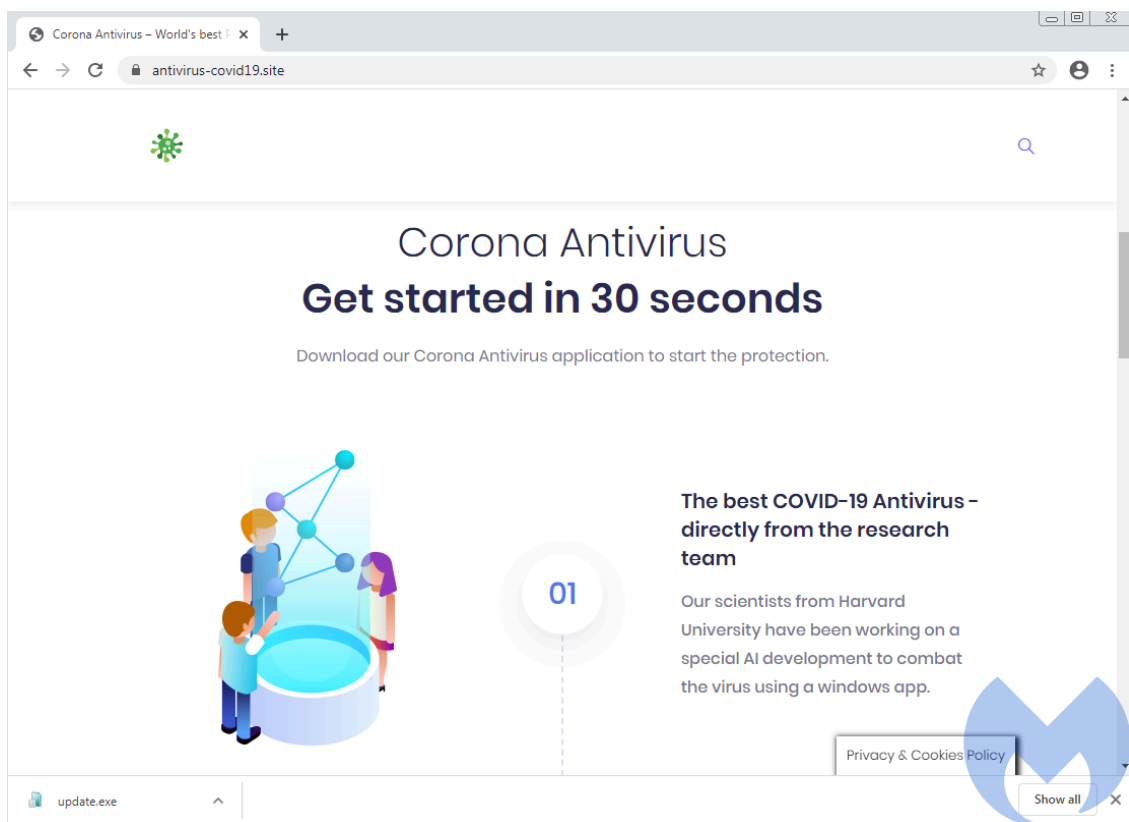
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

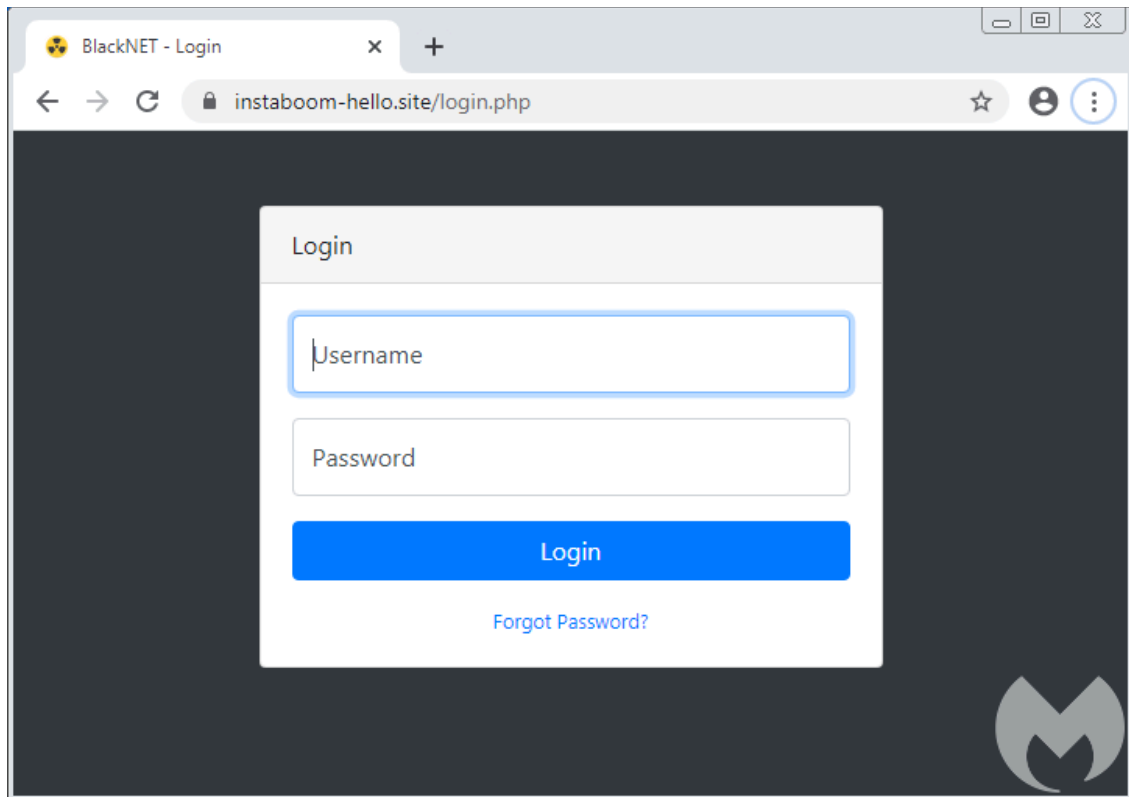


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

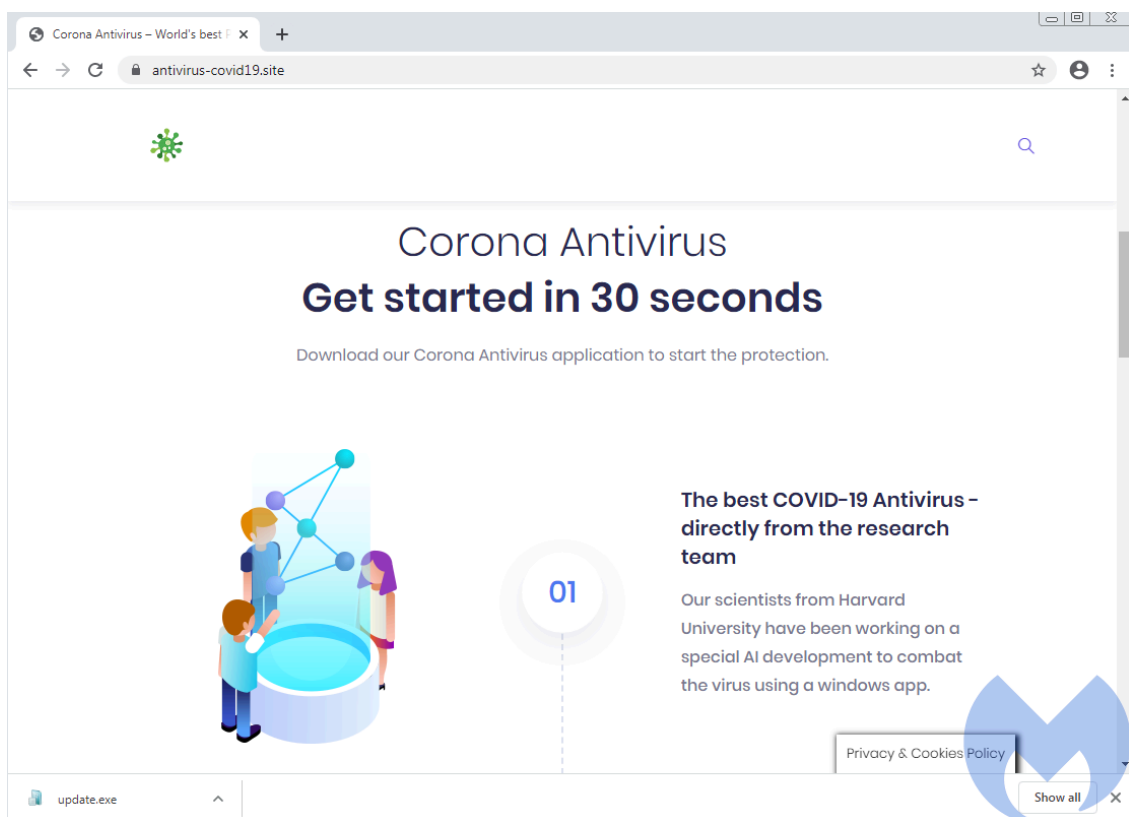
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

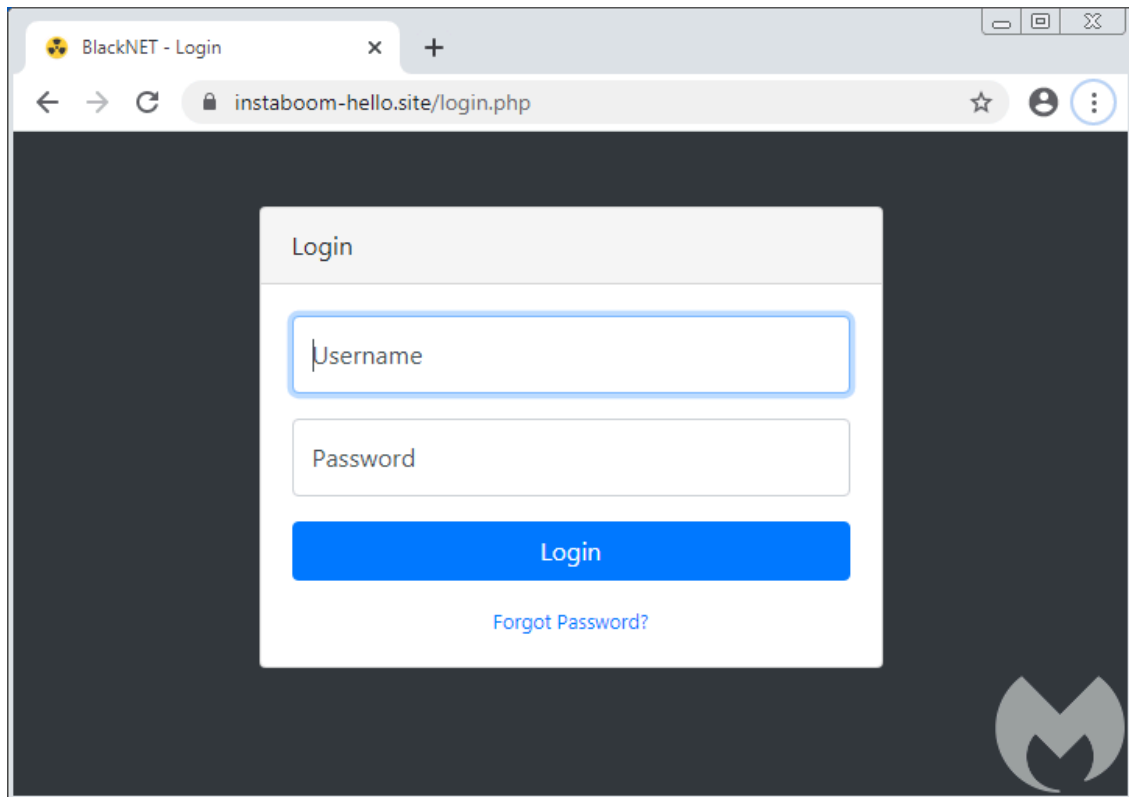


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

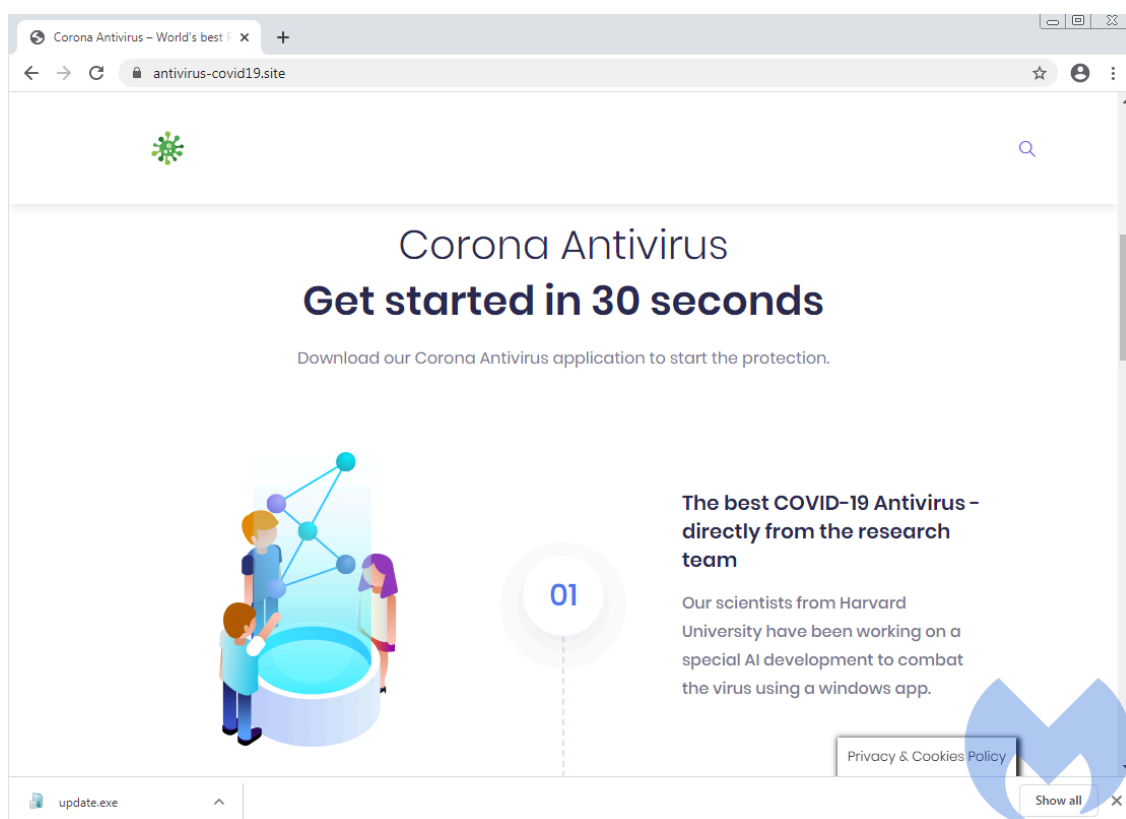
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

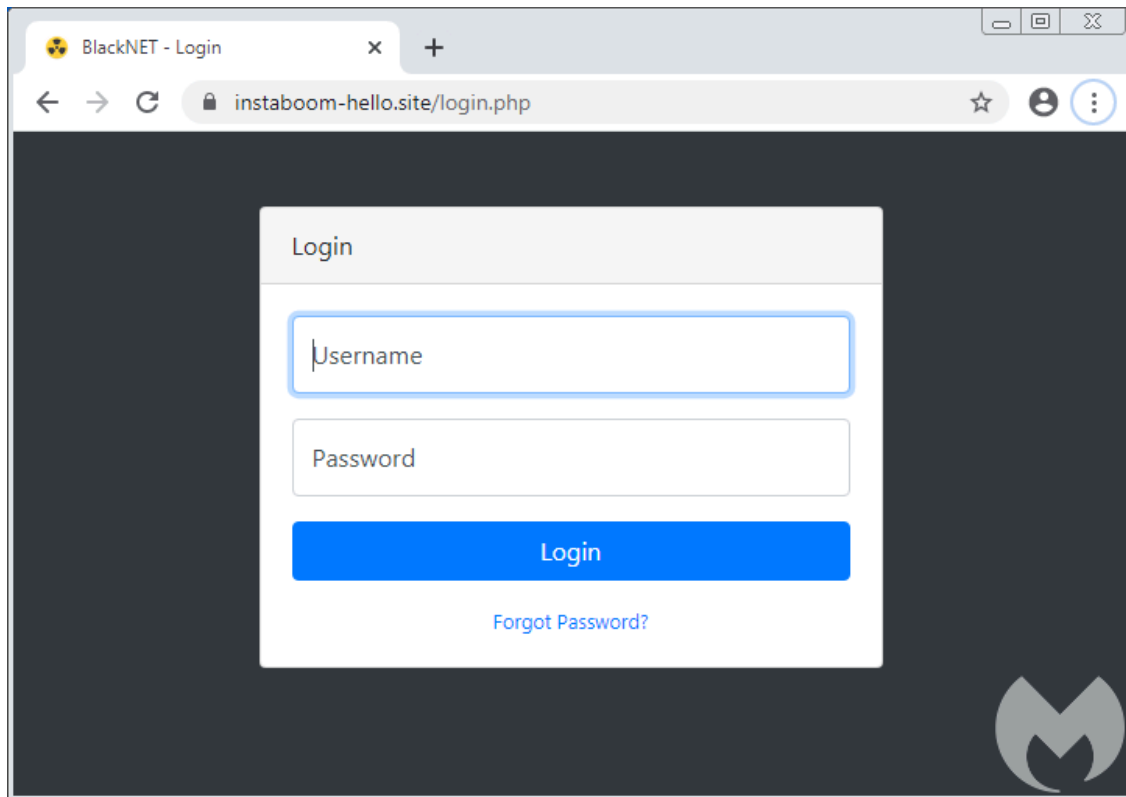


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

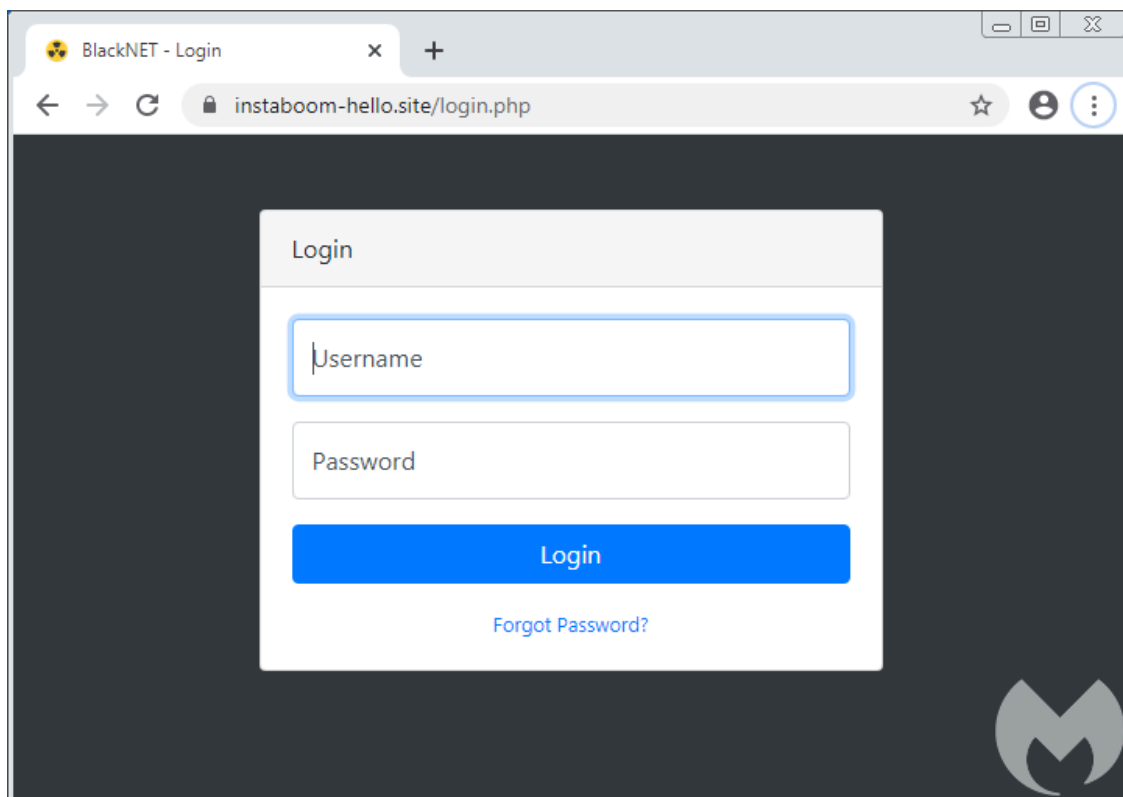
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

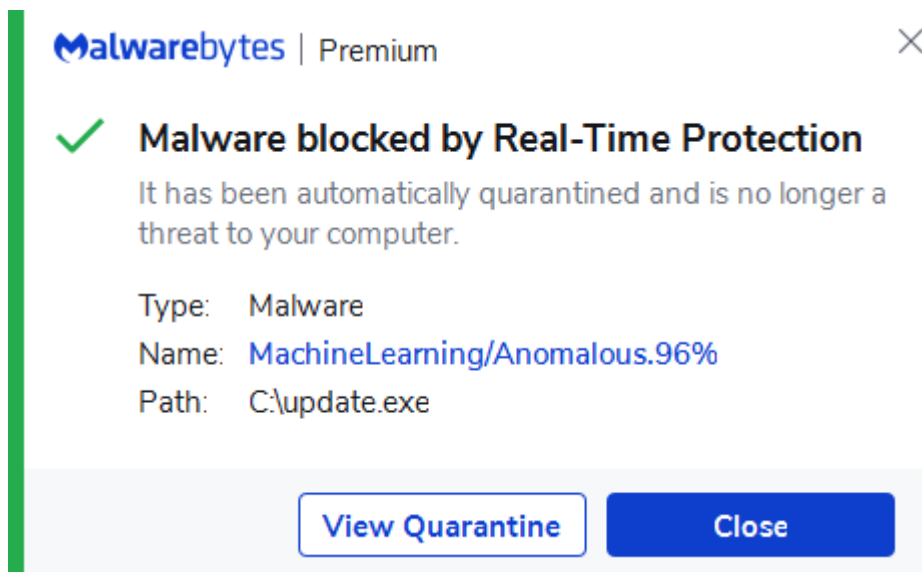
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

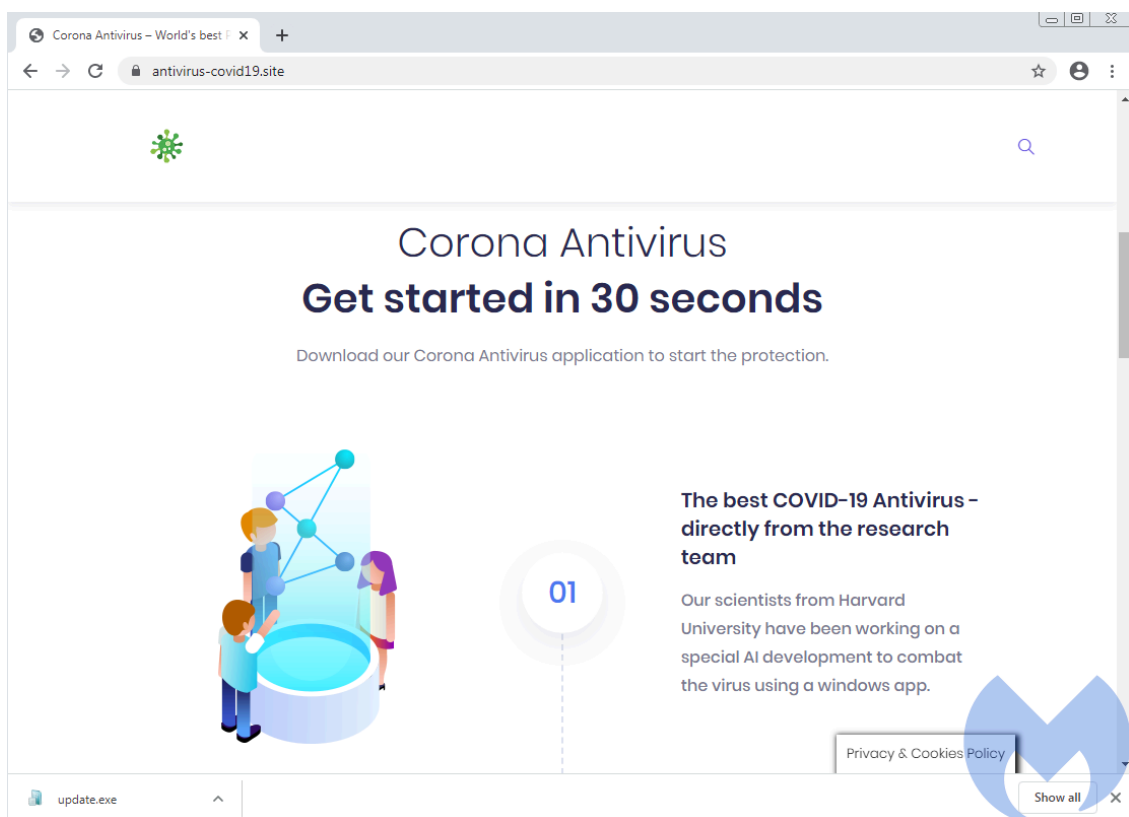
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

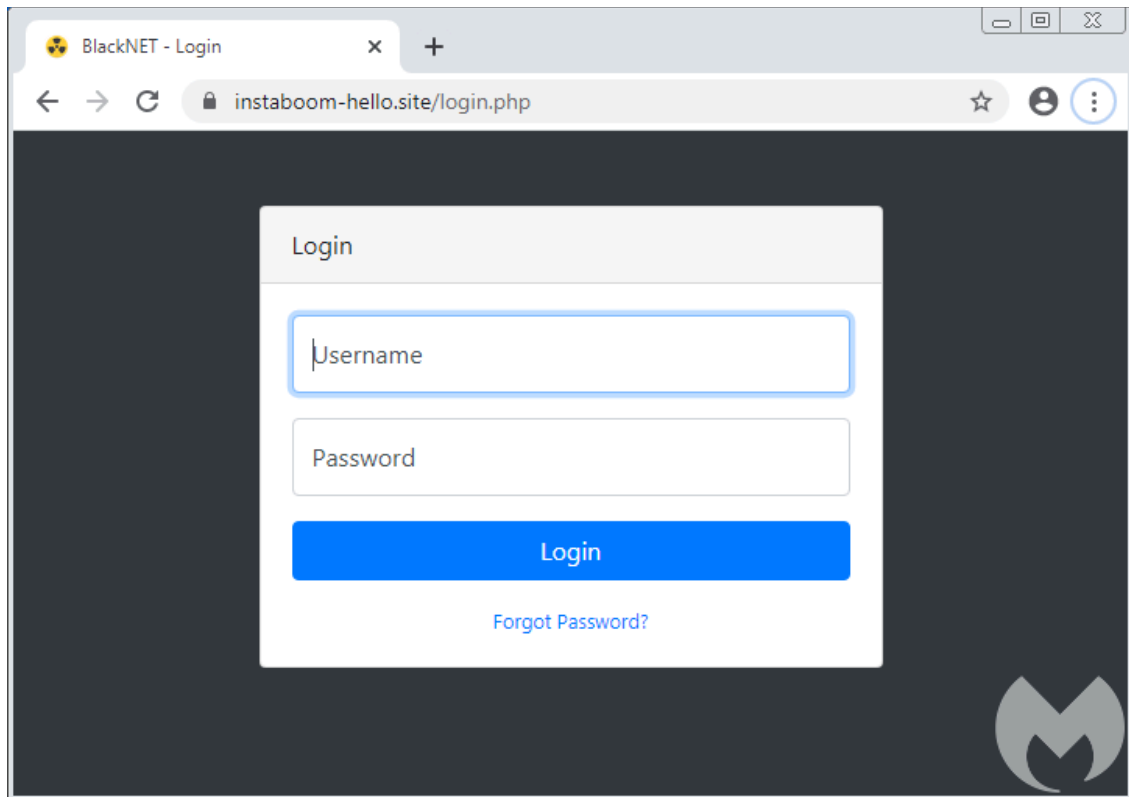


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

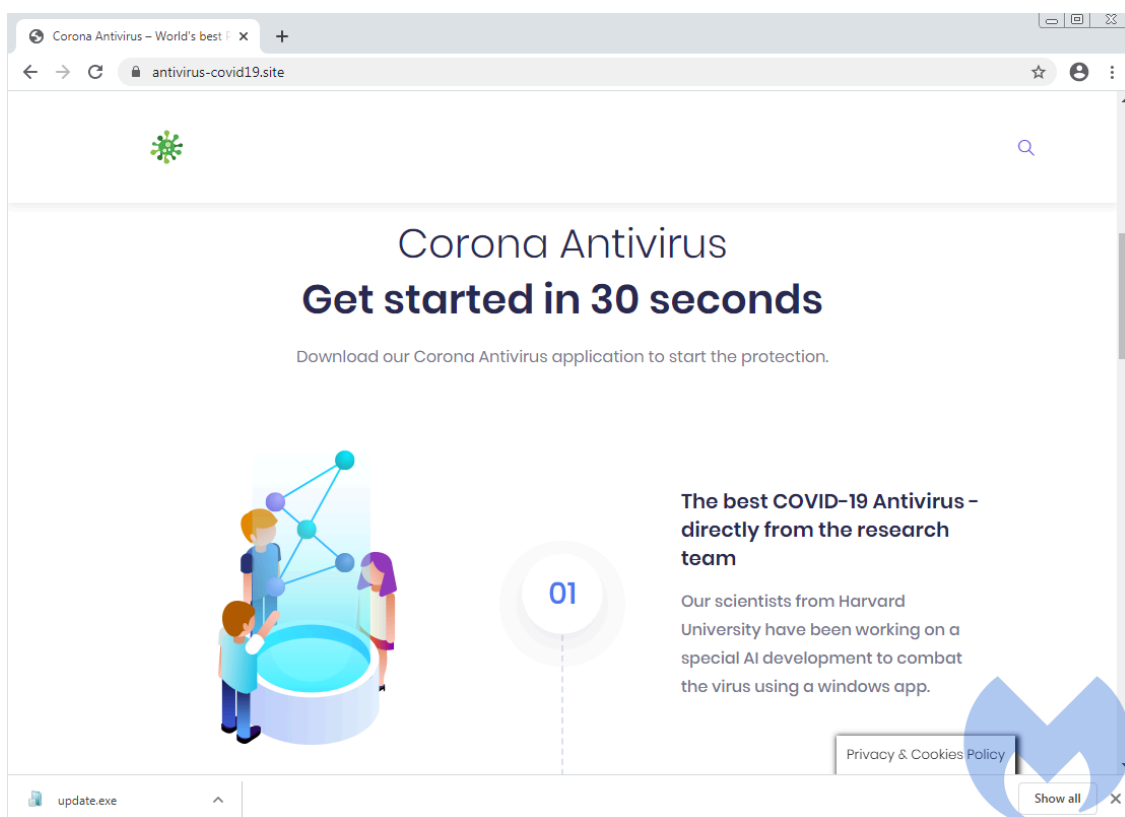
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

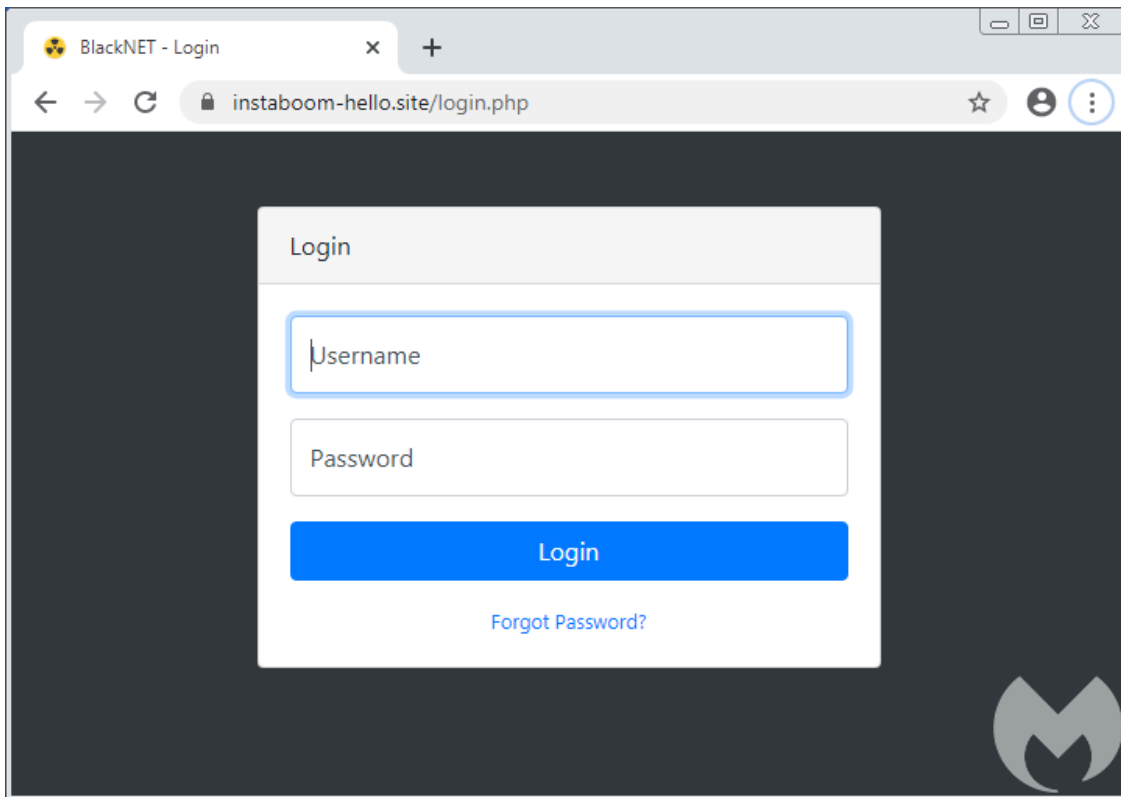


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots representing clients. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

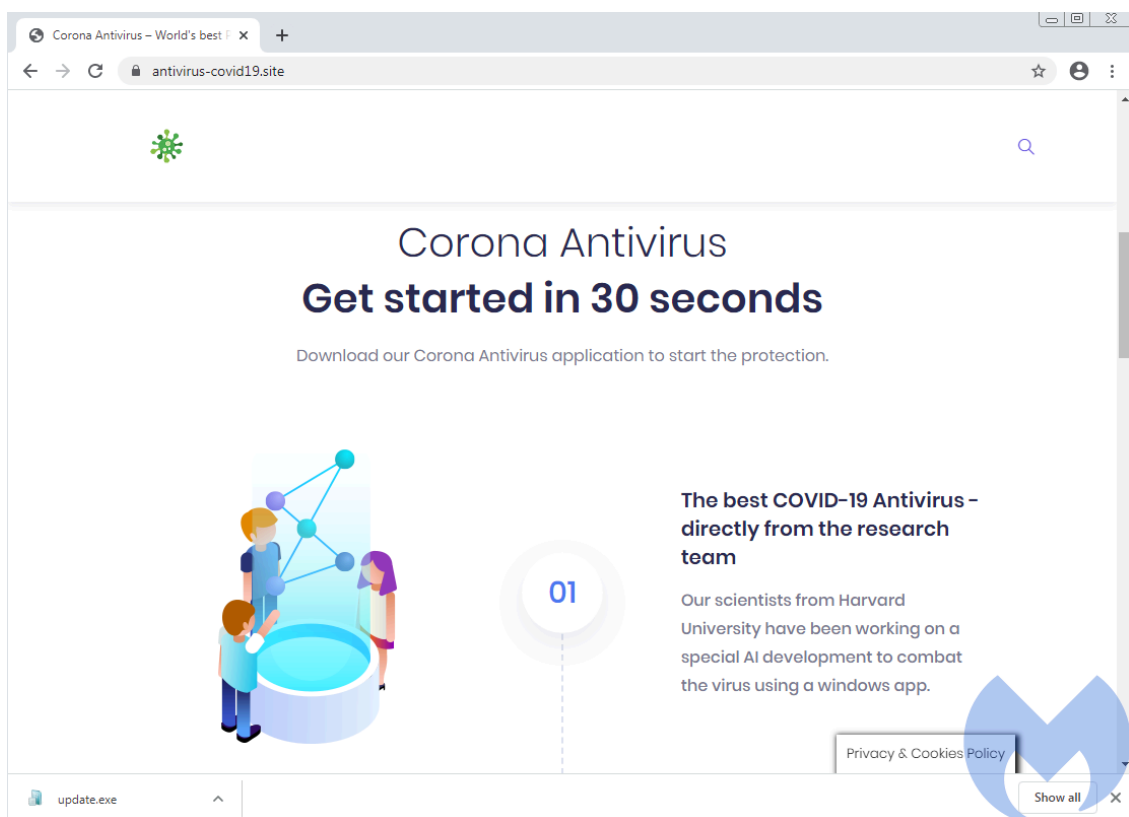
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

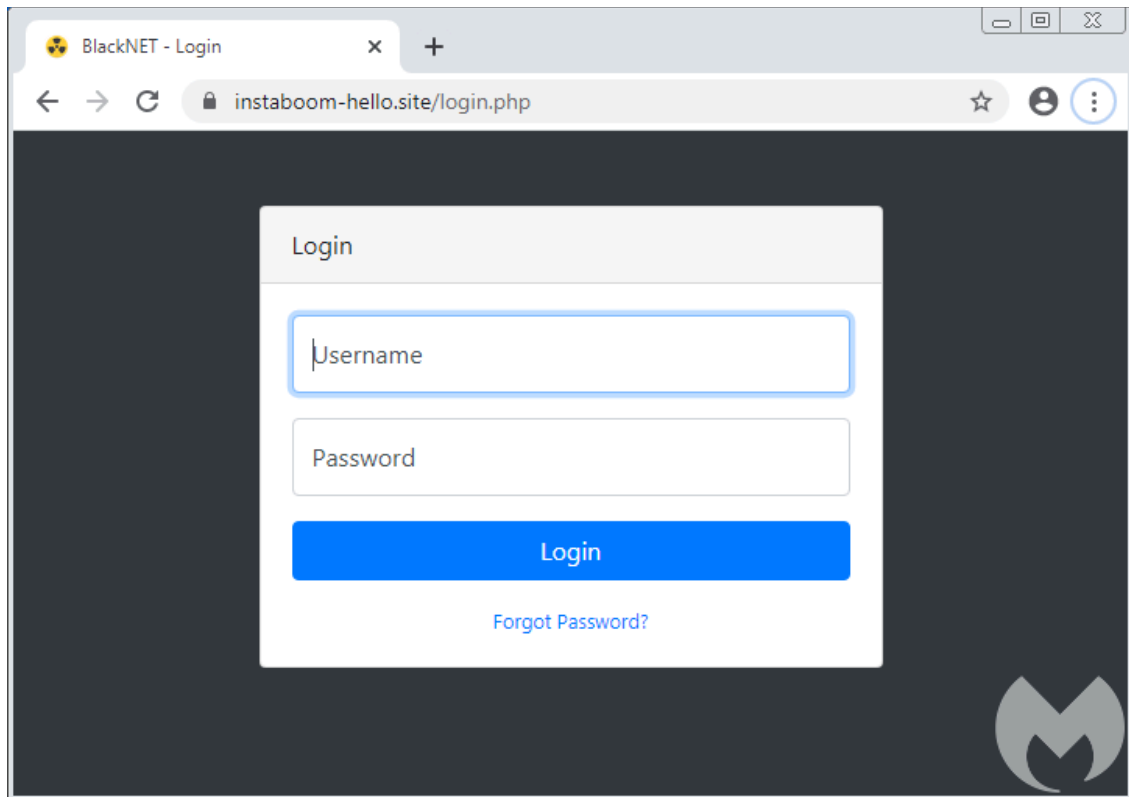


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

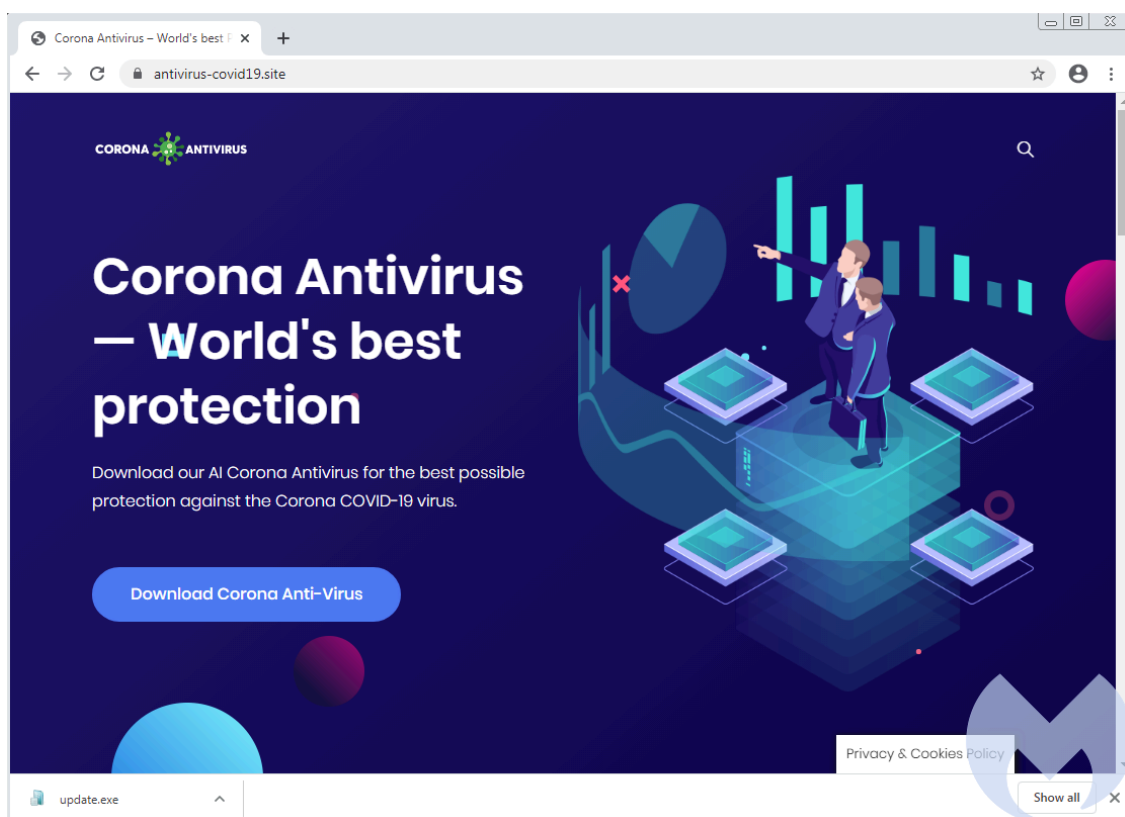
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

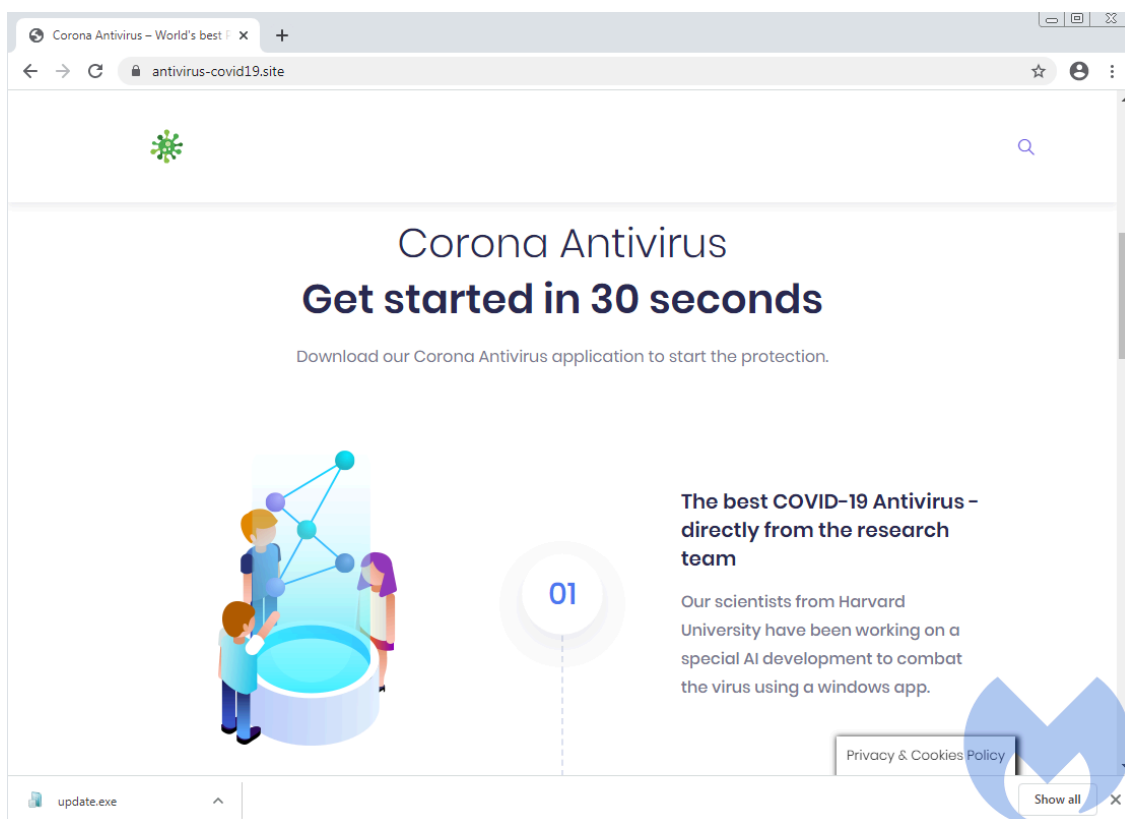
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

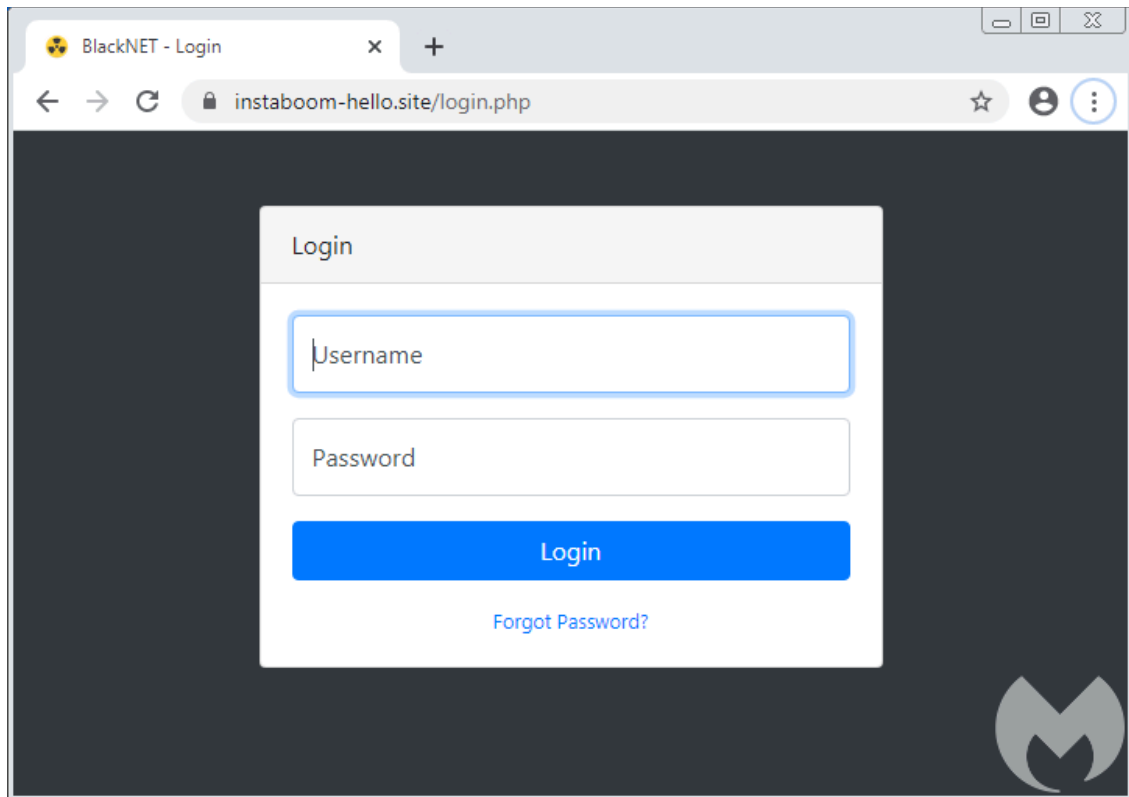


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

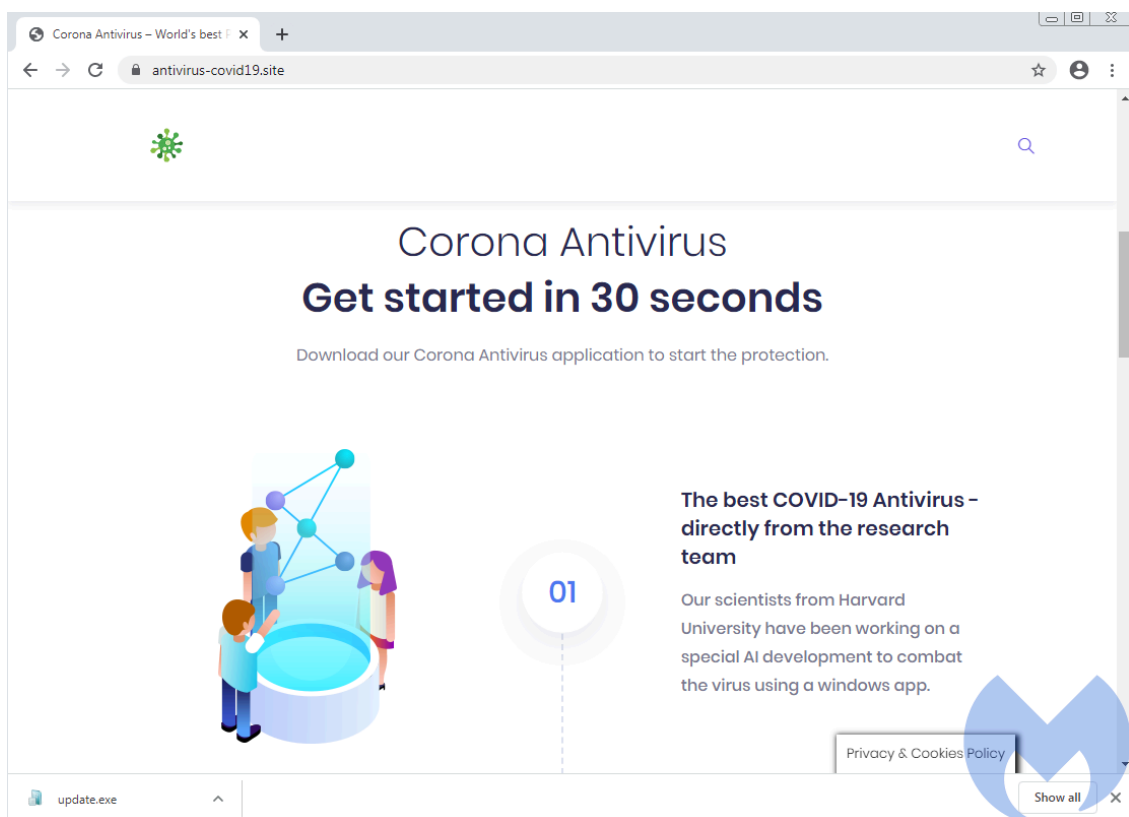
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

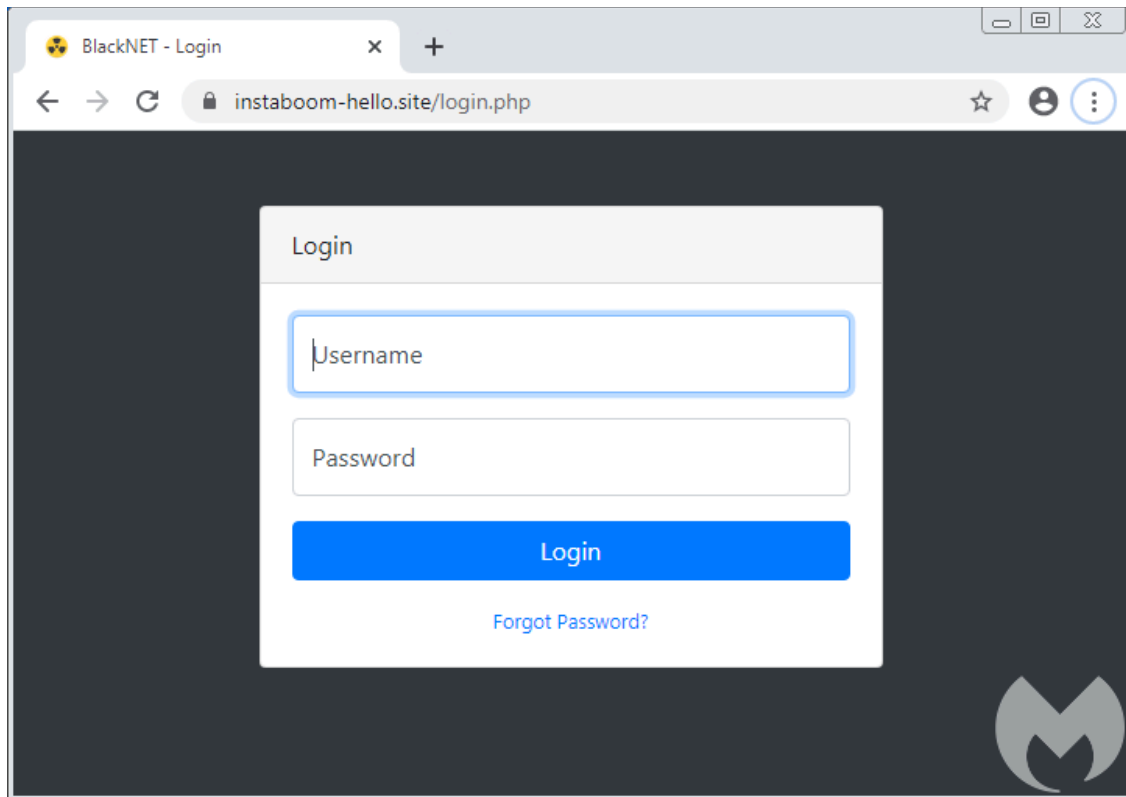


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

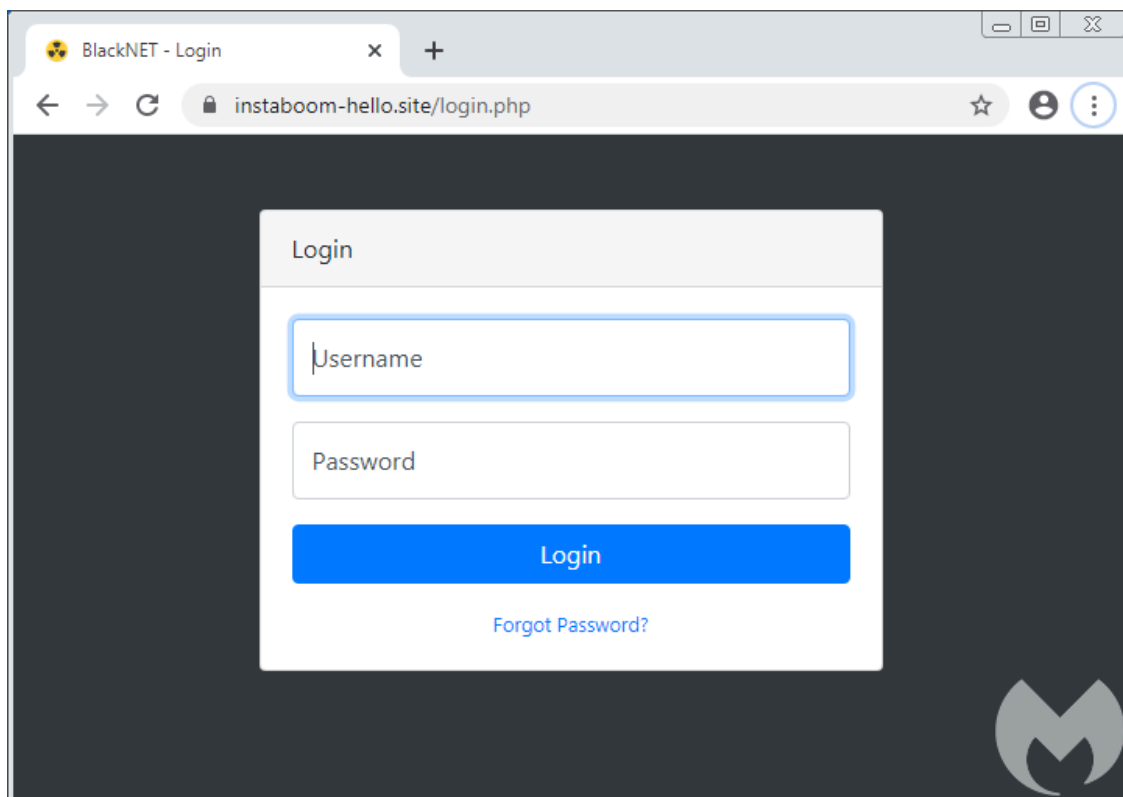
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

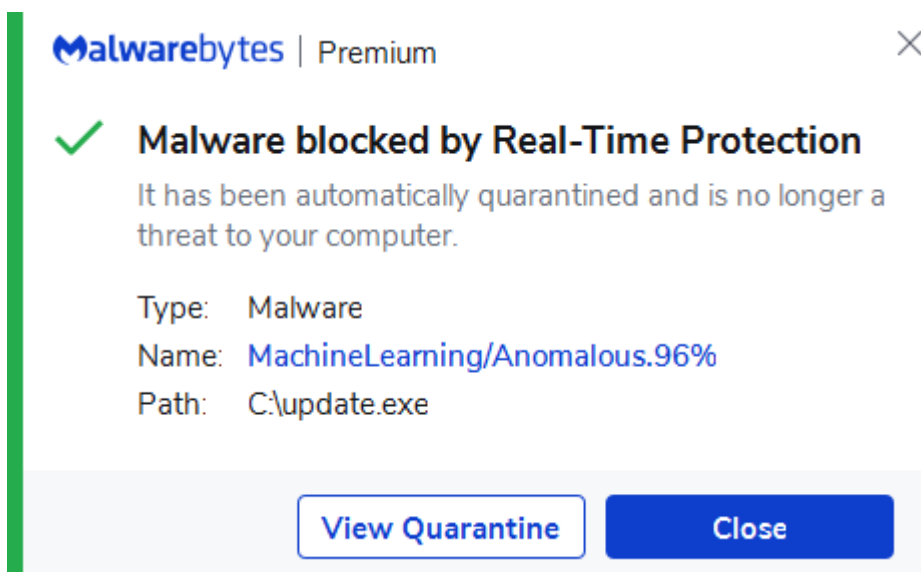
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

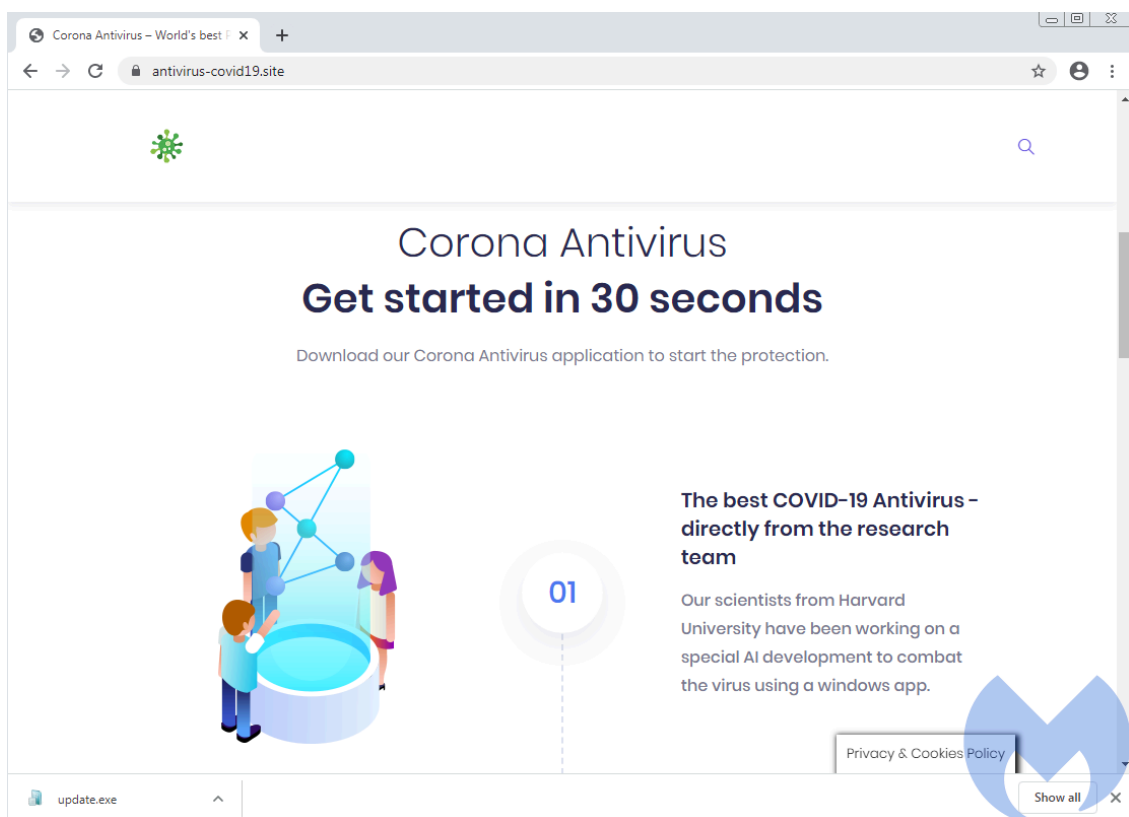
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

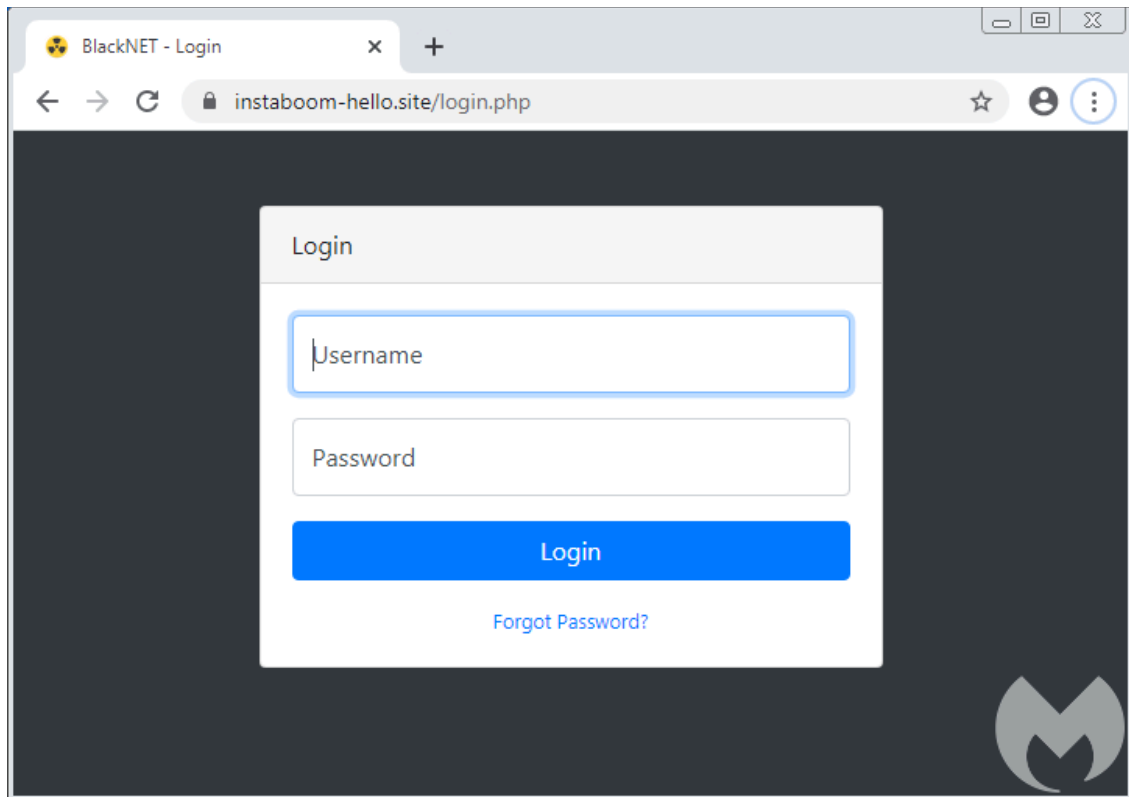


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

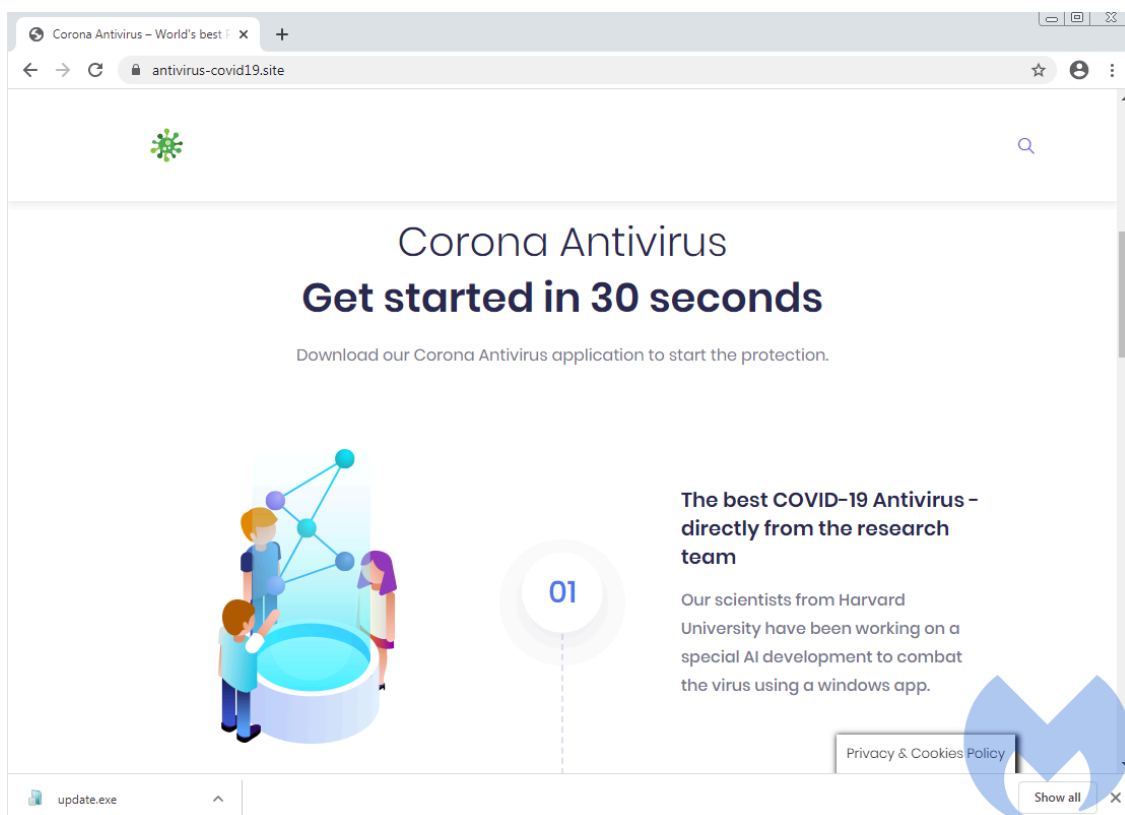
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

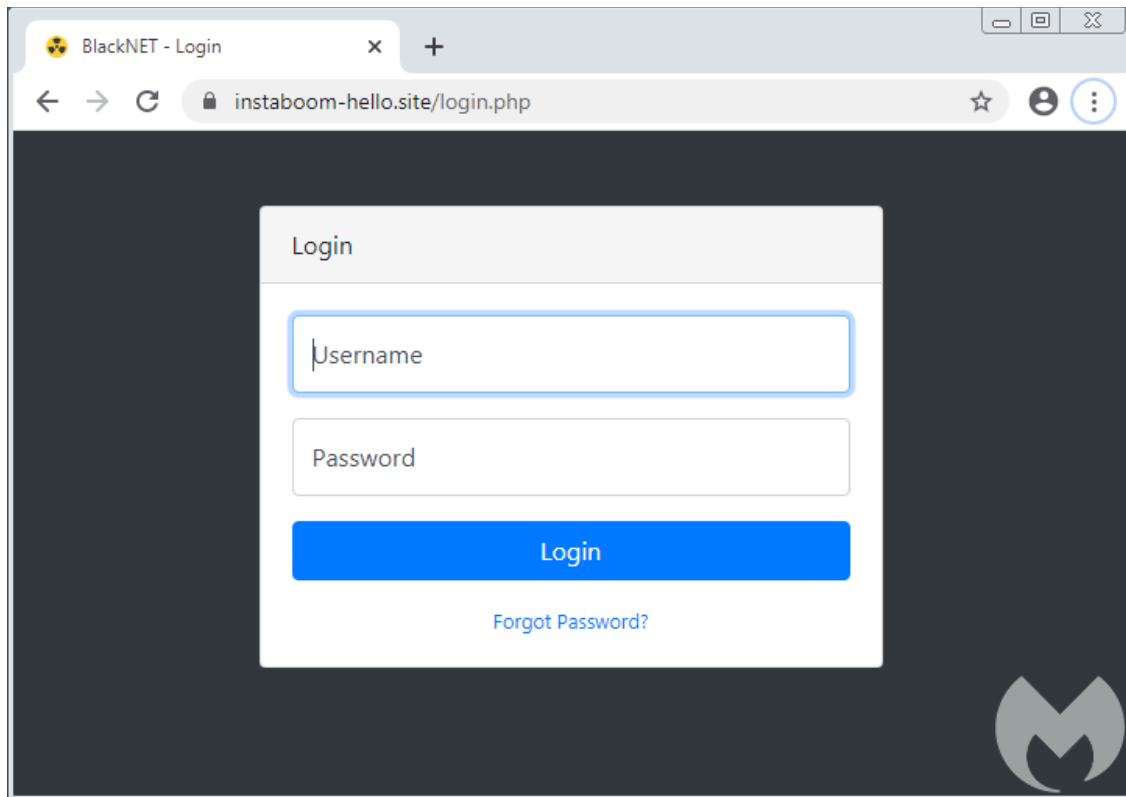


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

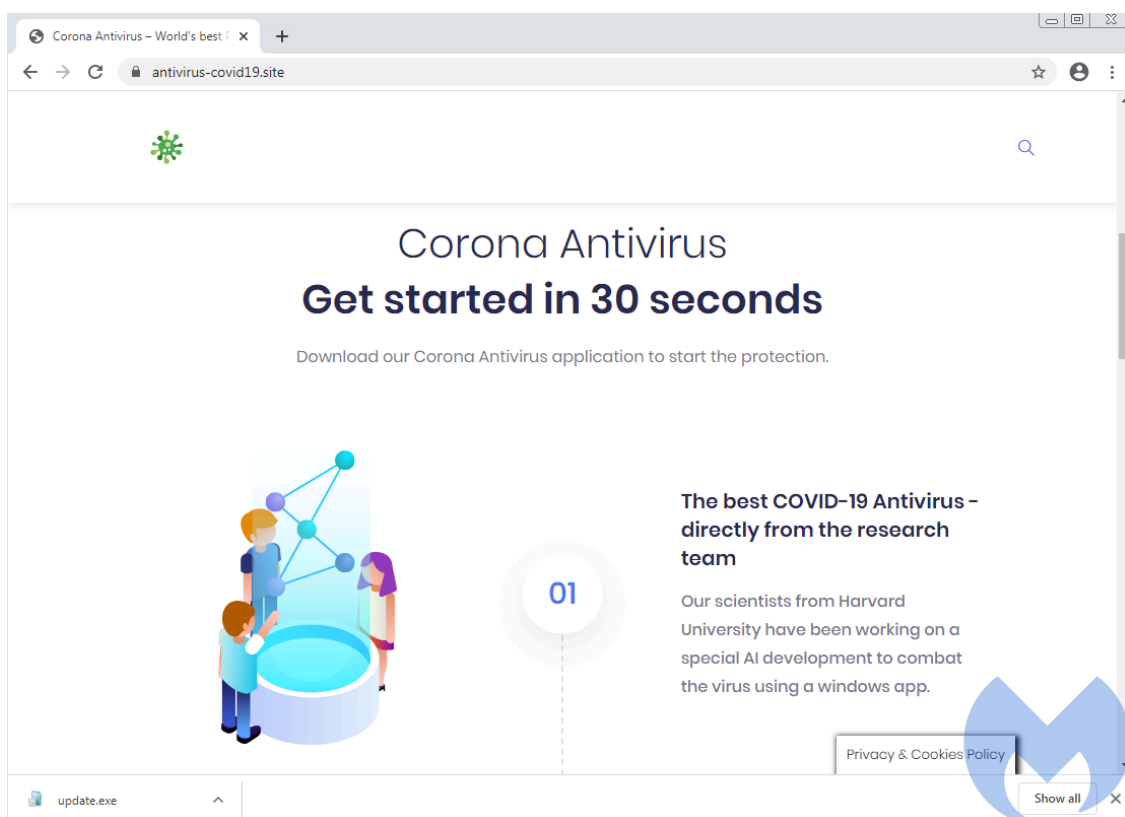
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

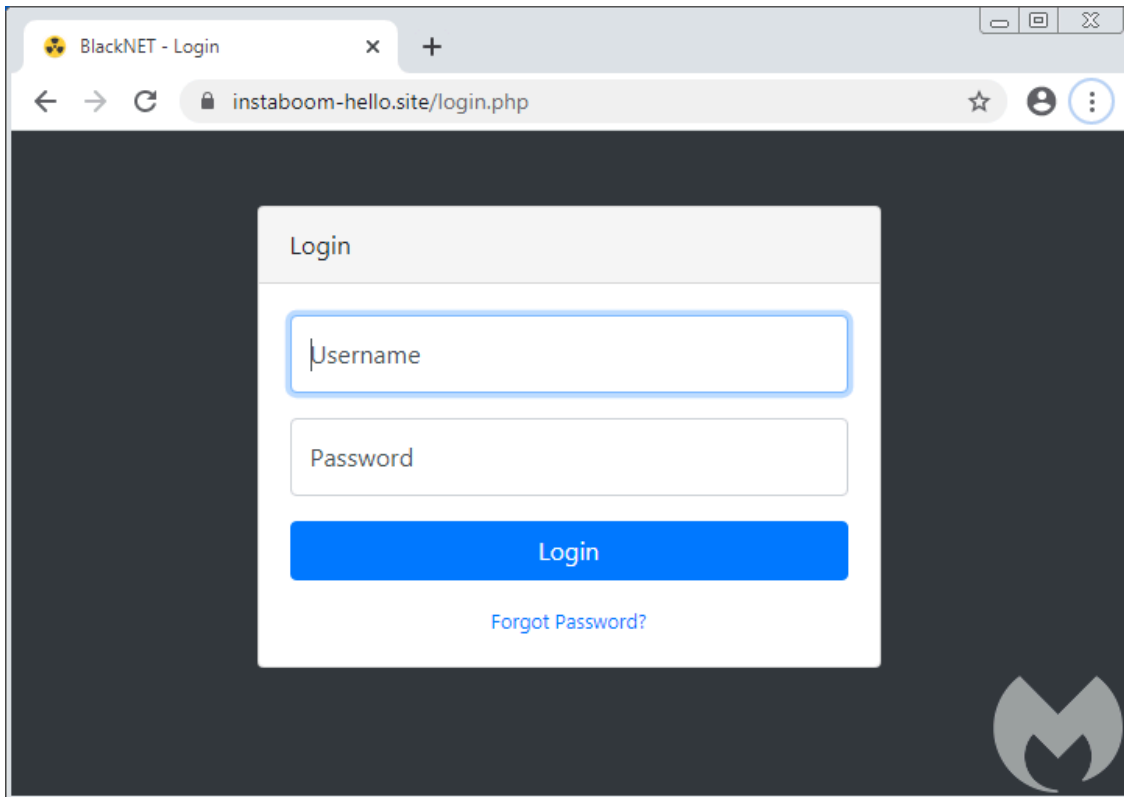


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

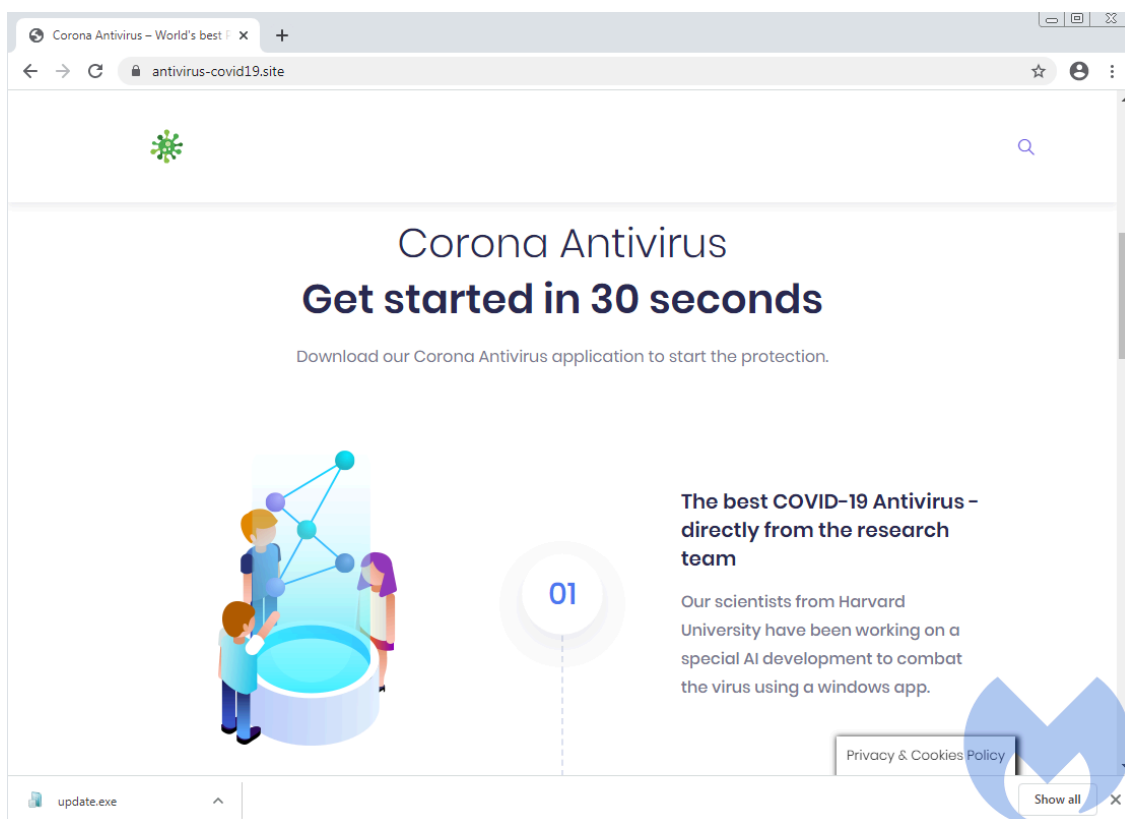
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

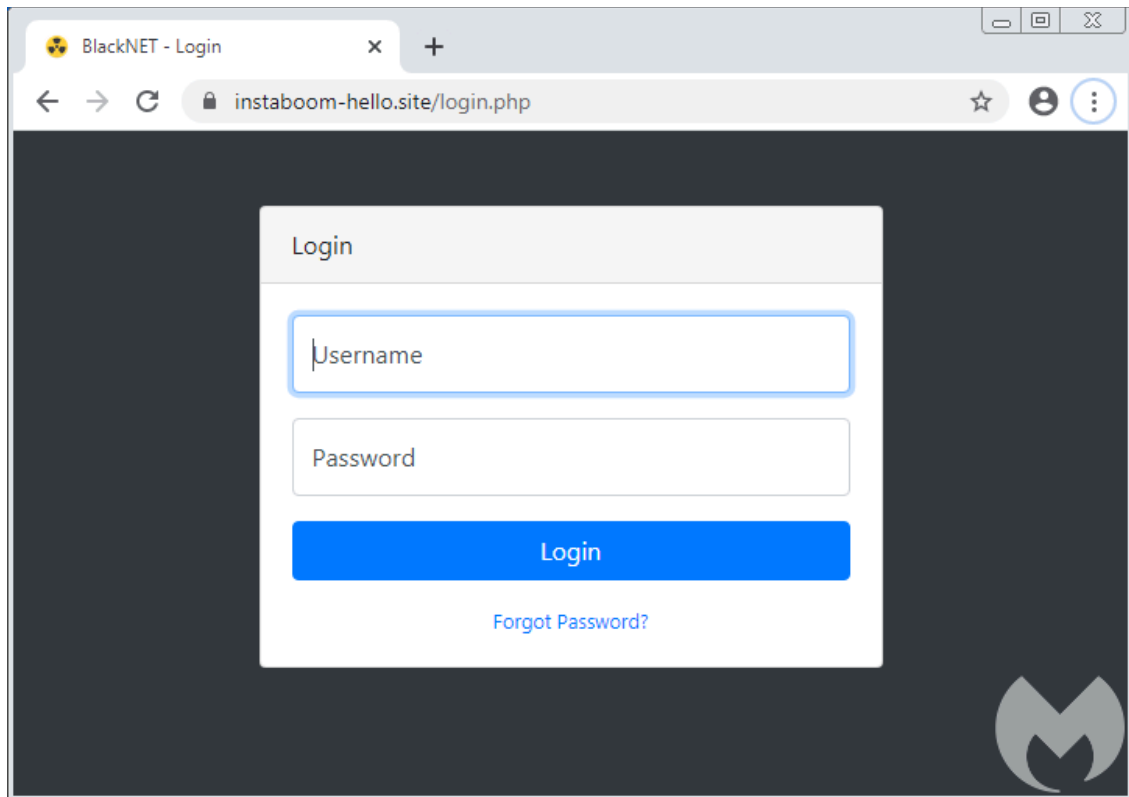


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

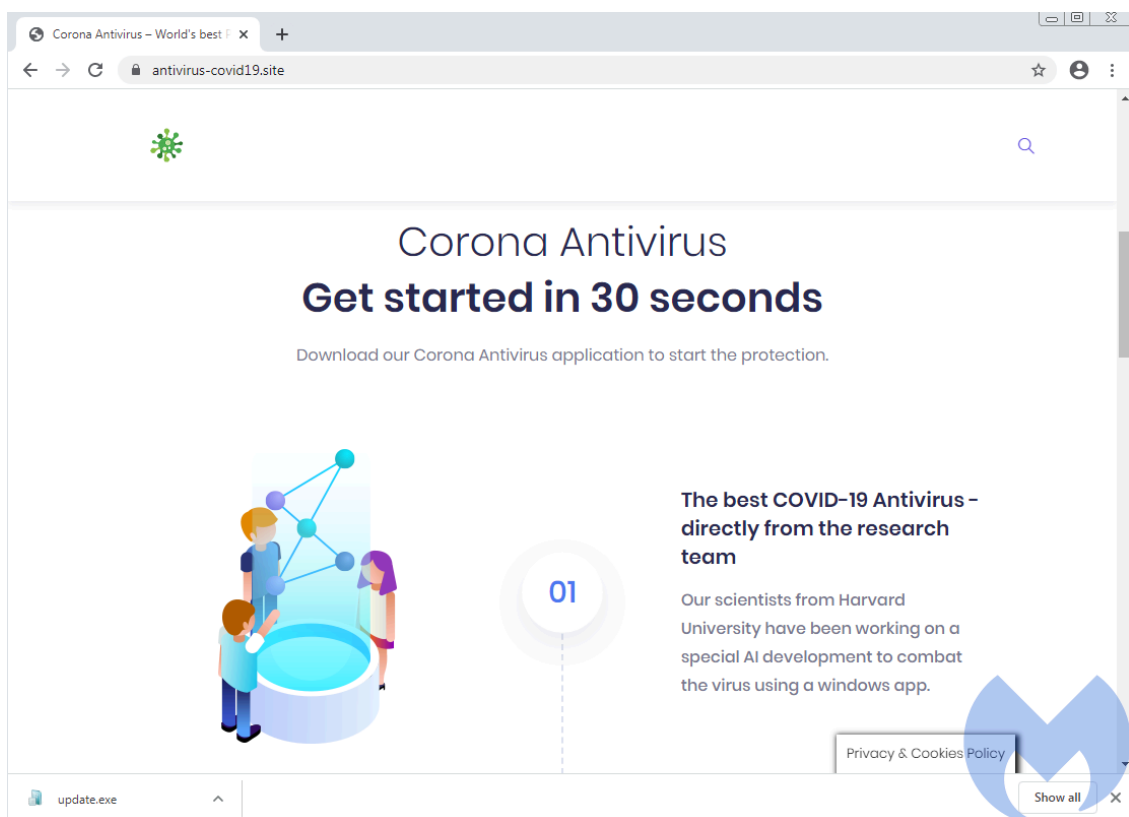
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

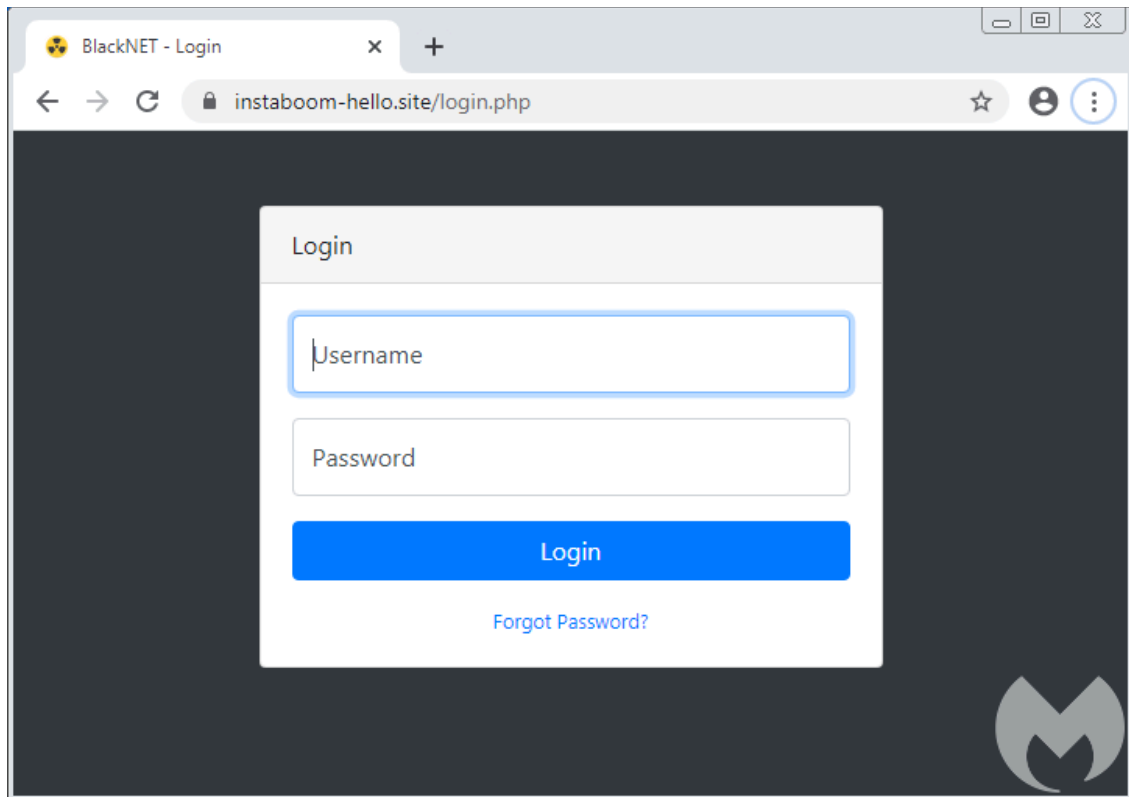


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

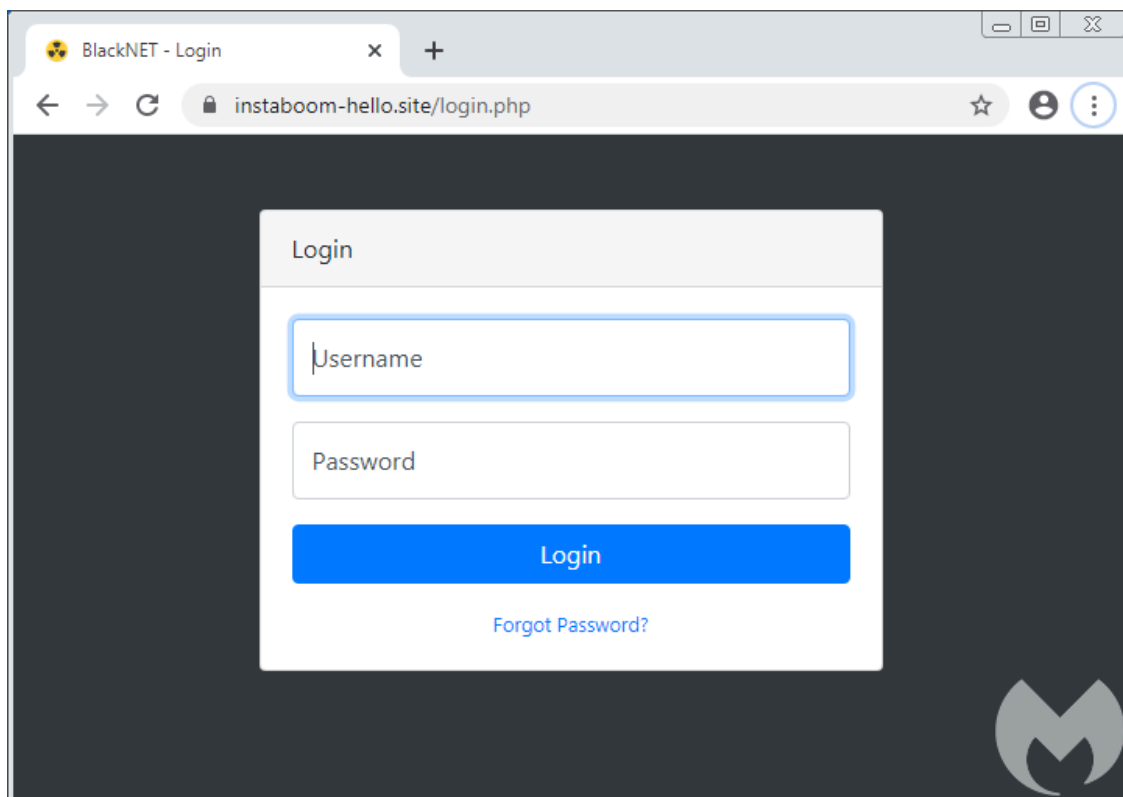
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

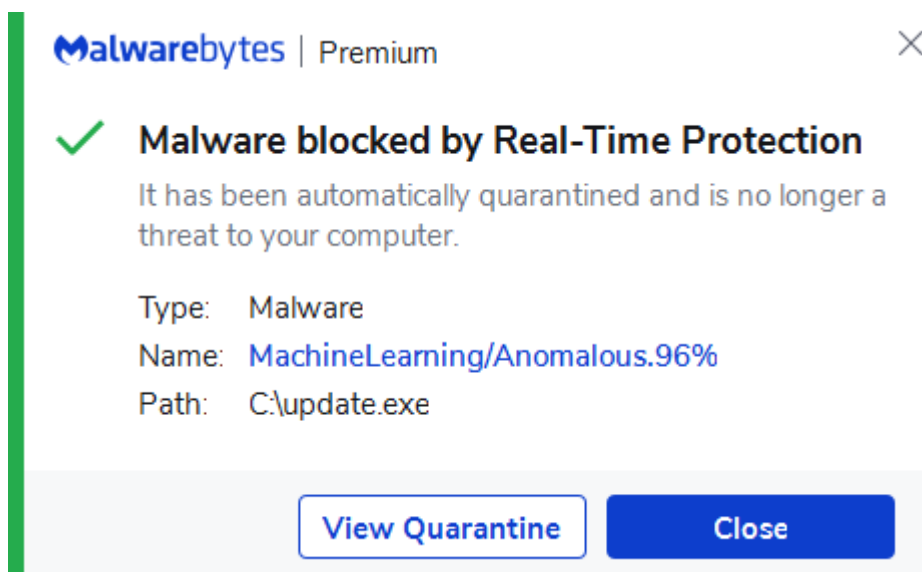
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

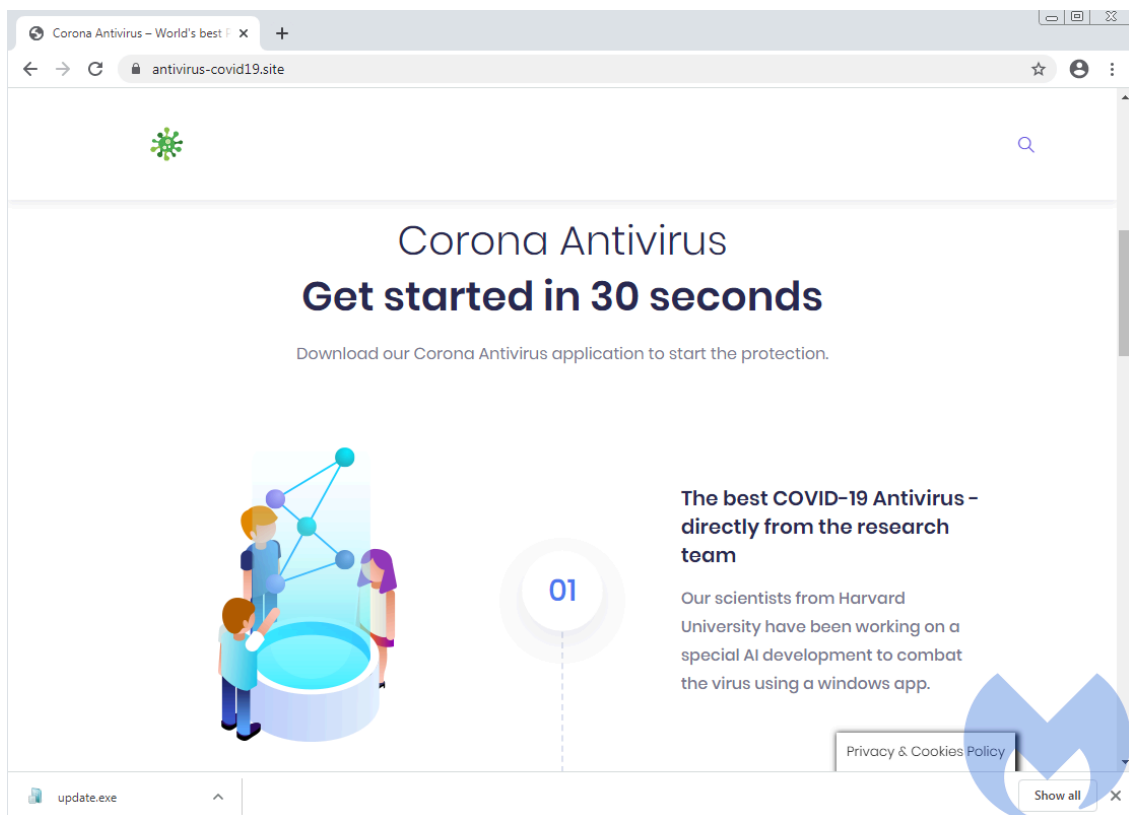
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

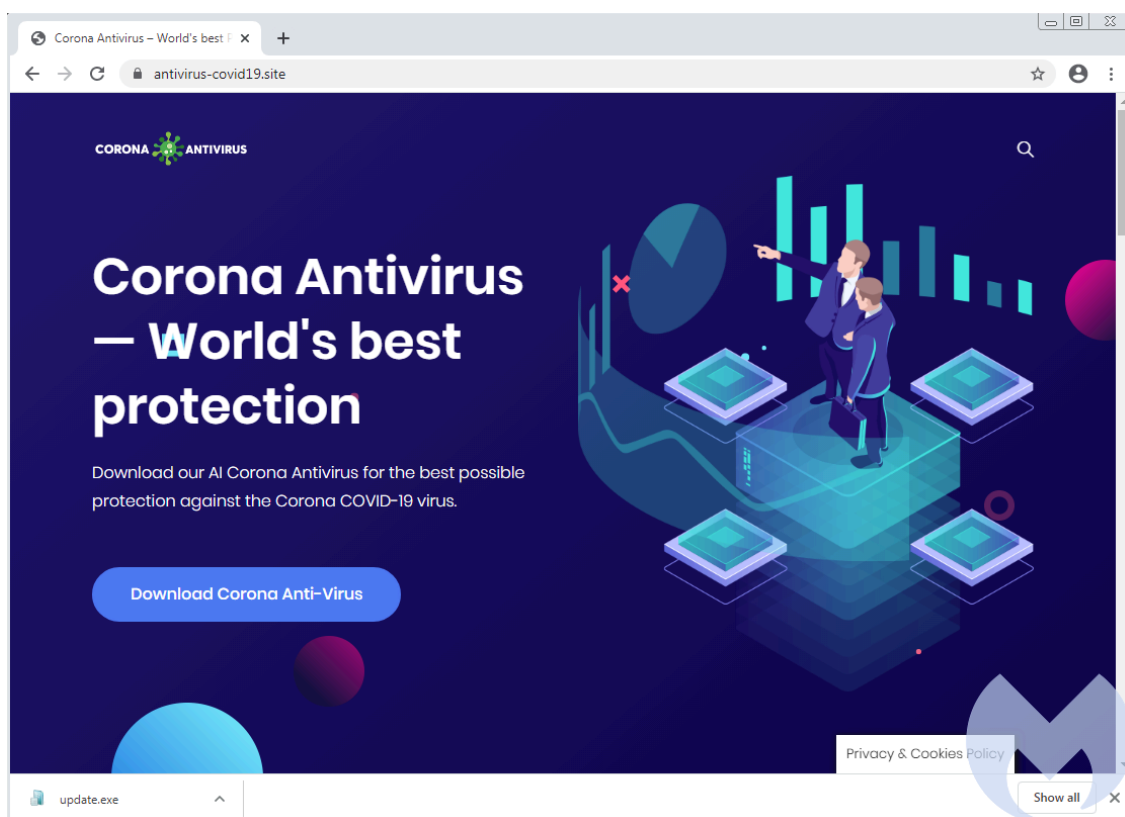
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

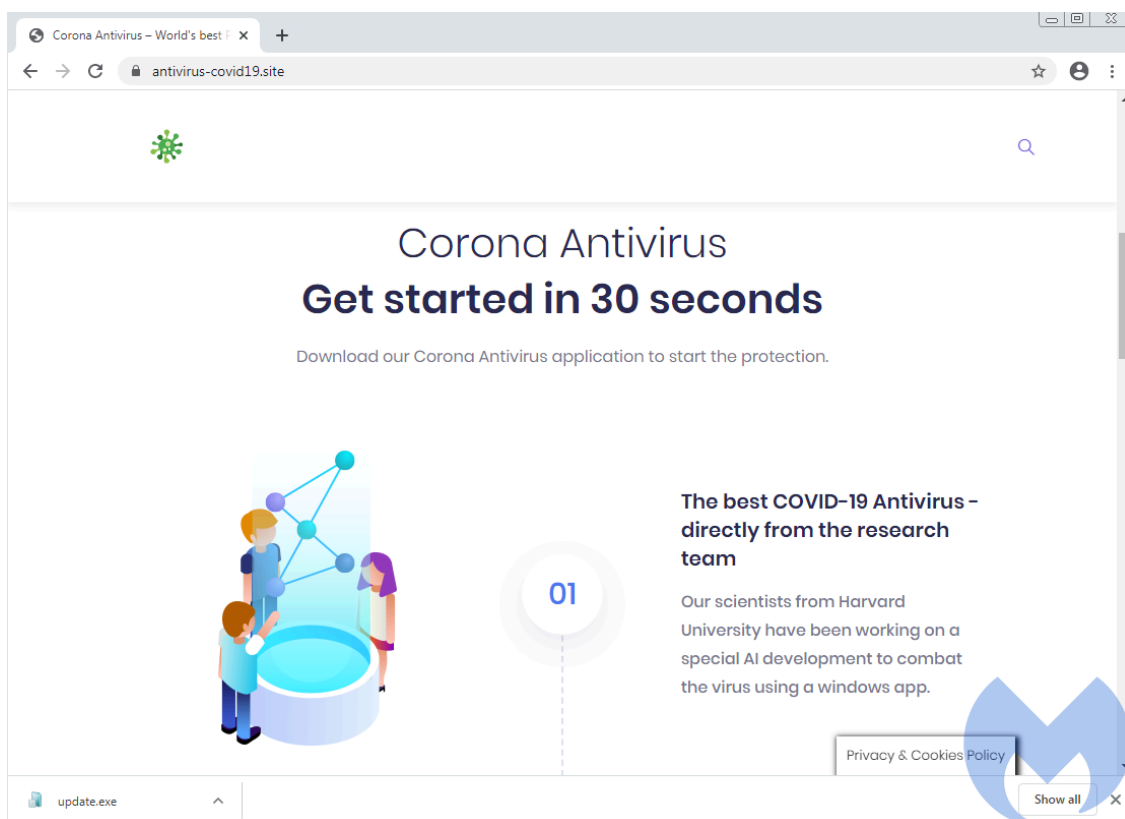
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

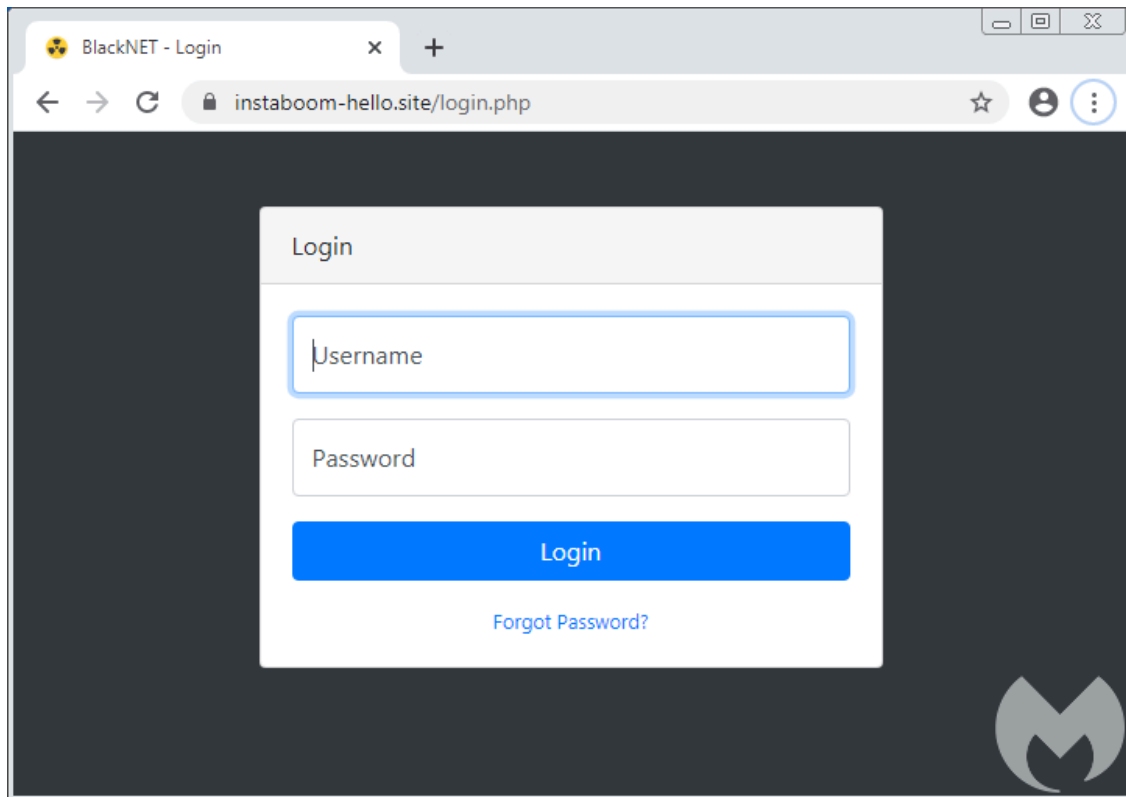


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

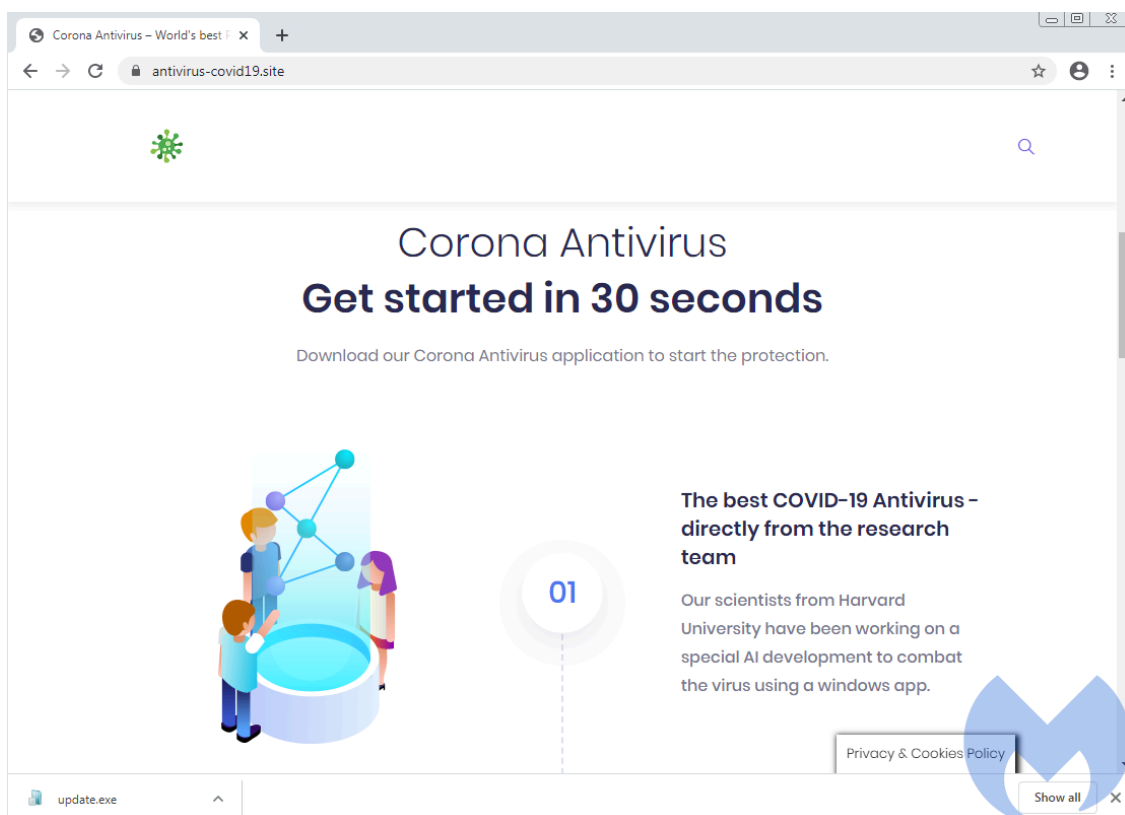
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

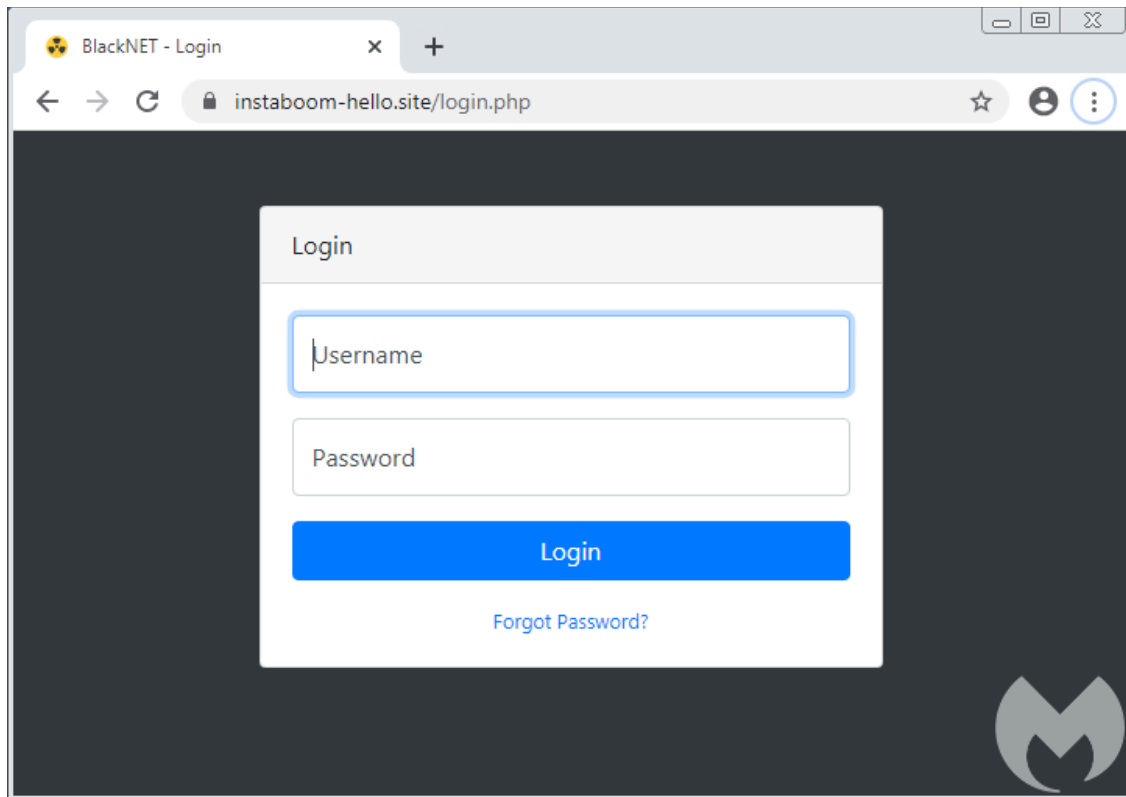


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

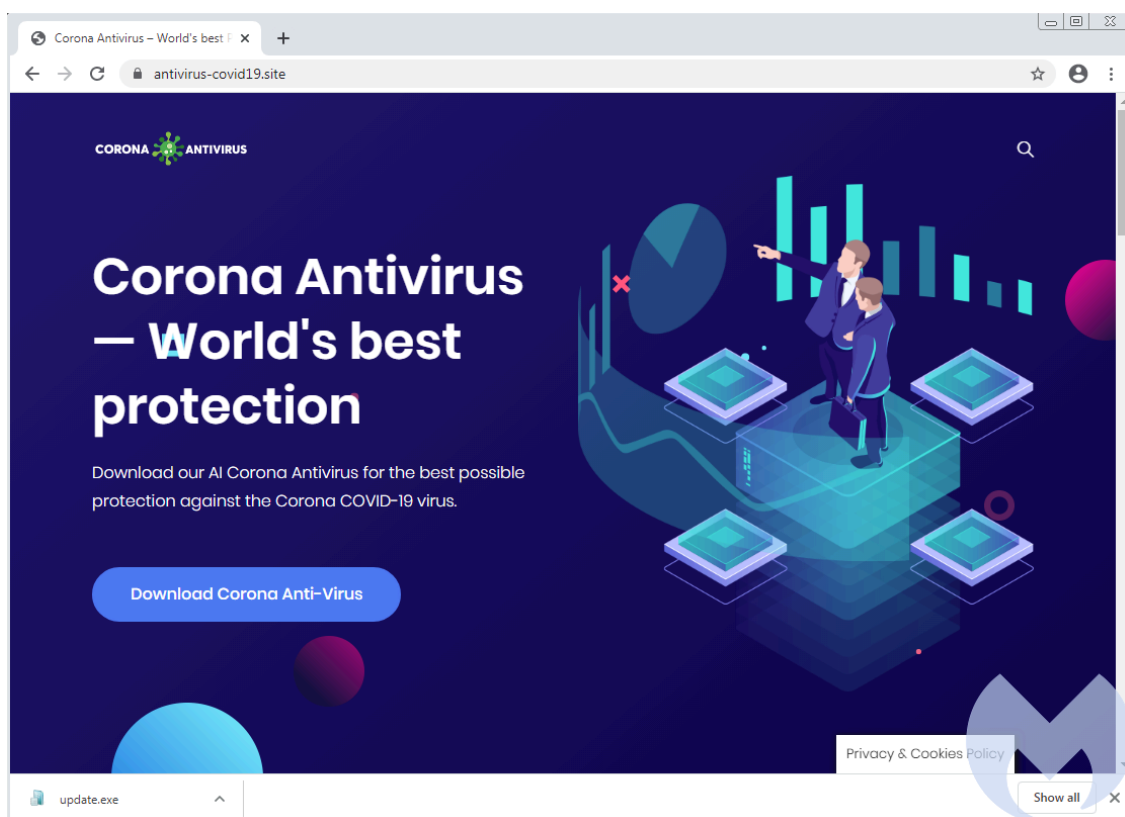
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

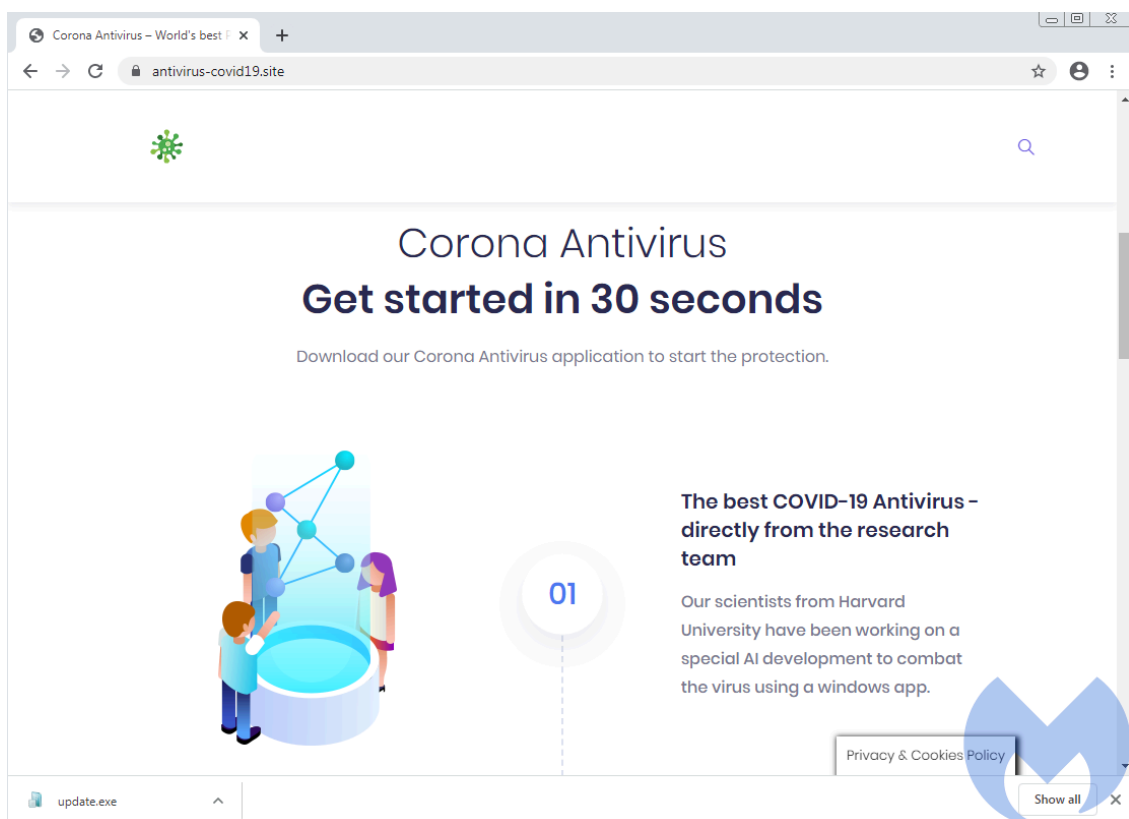
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

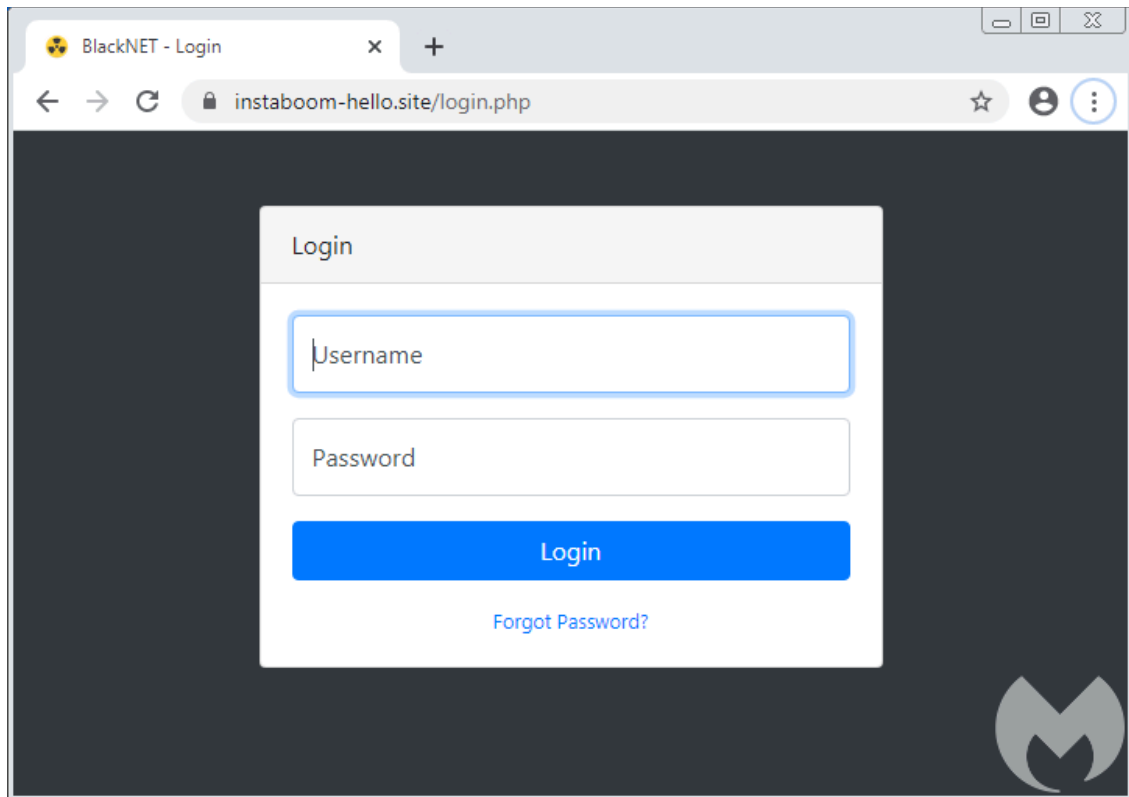


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

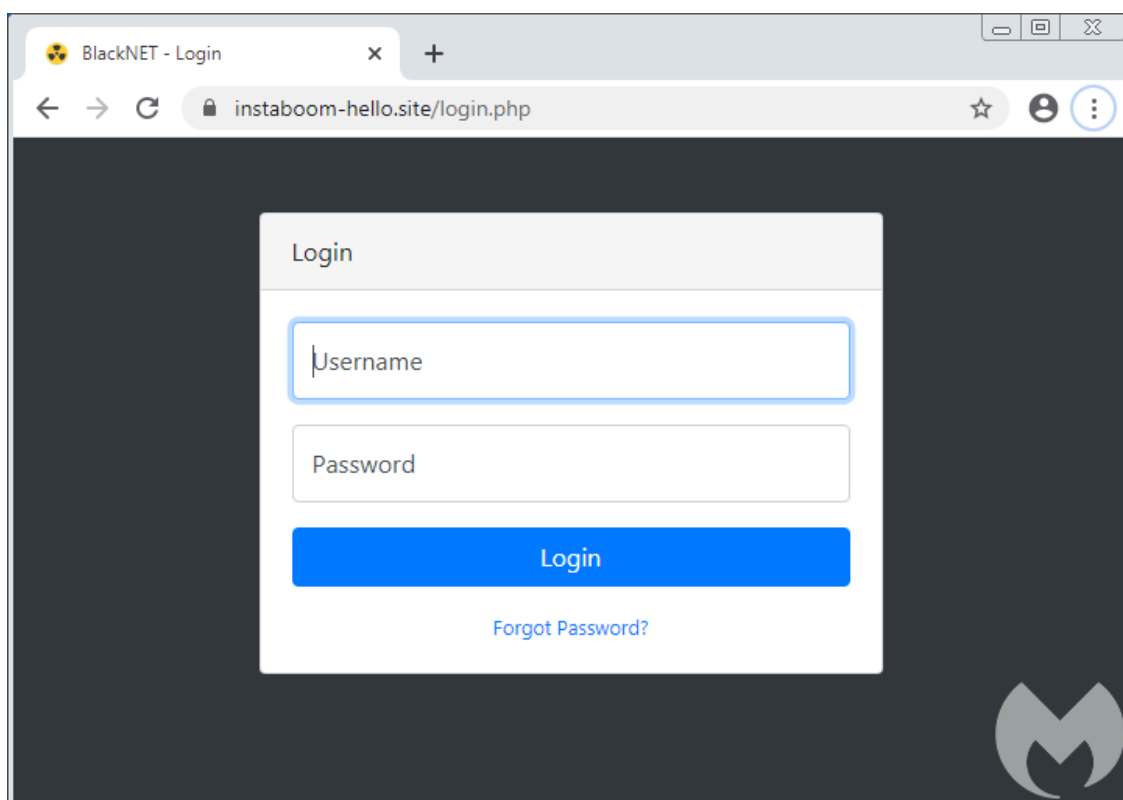
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

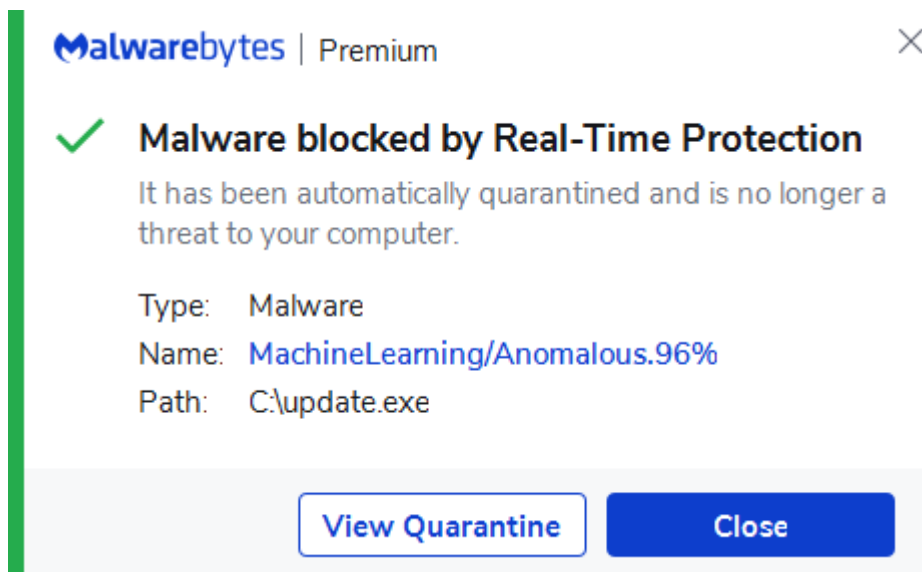
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

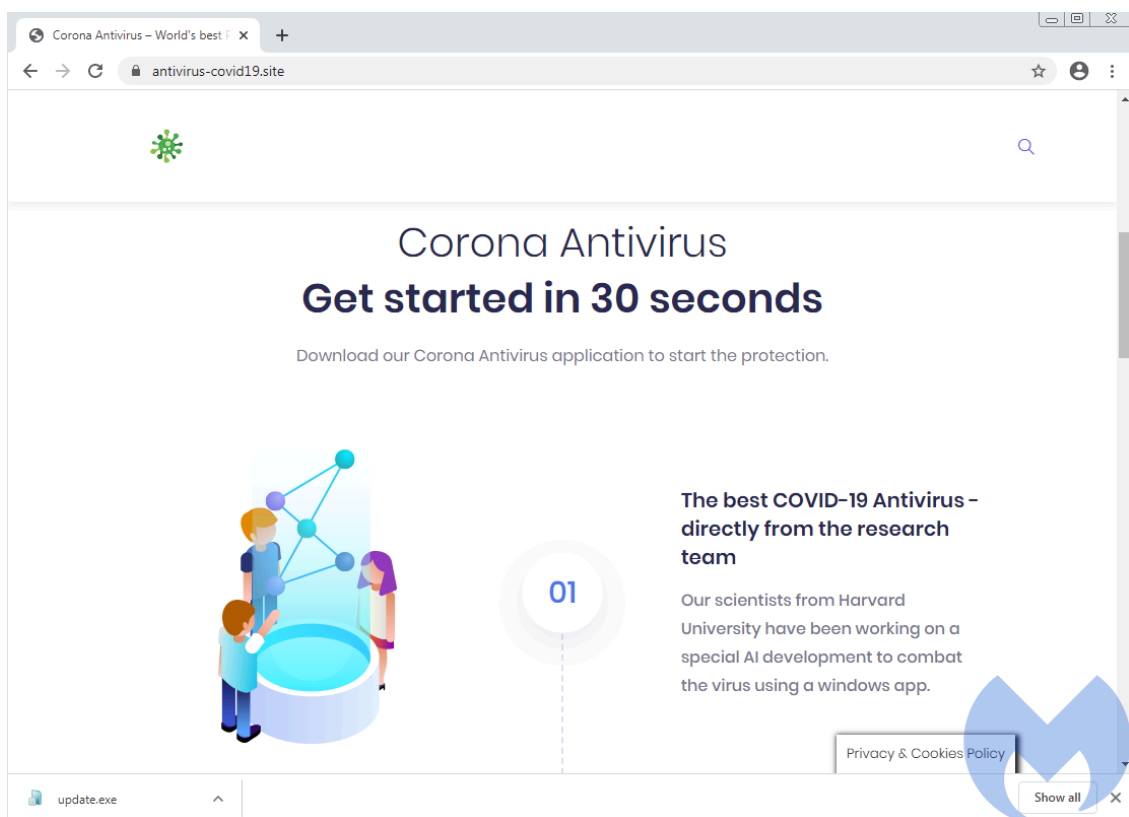
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

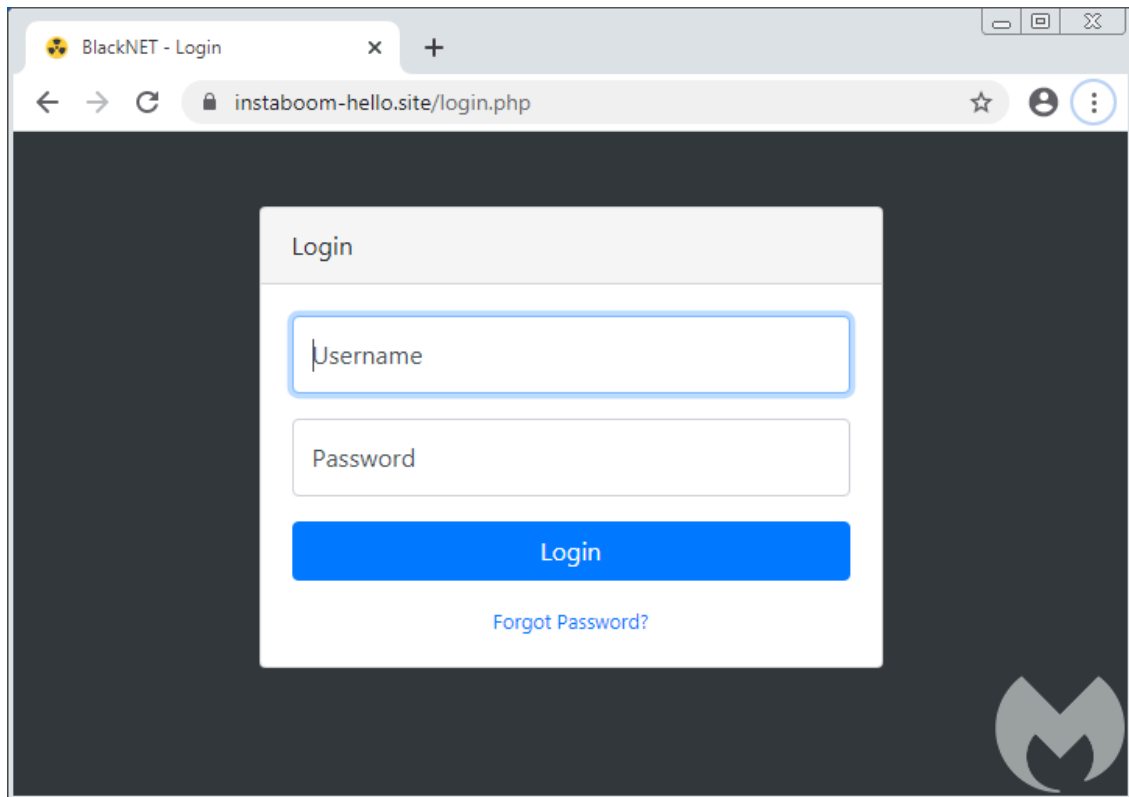


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer." Below this, the details are listed: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

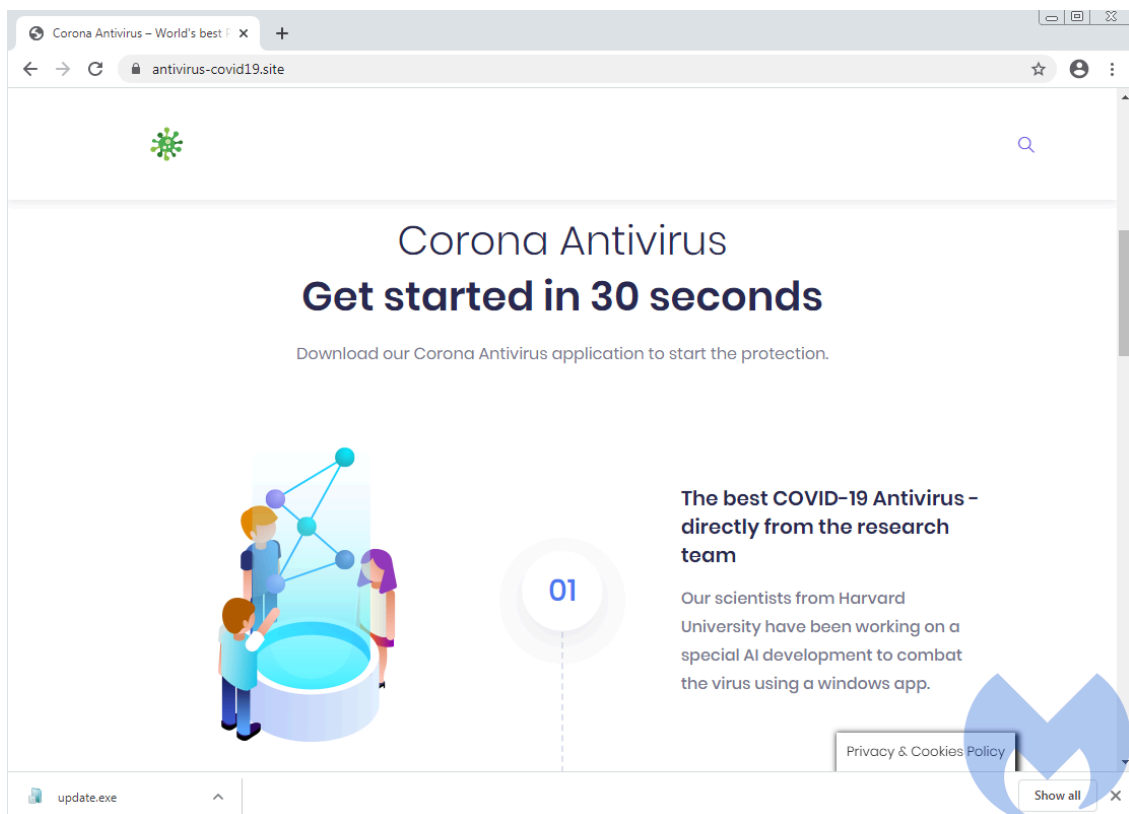
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

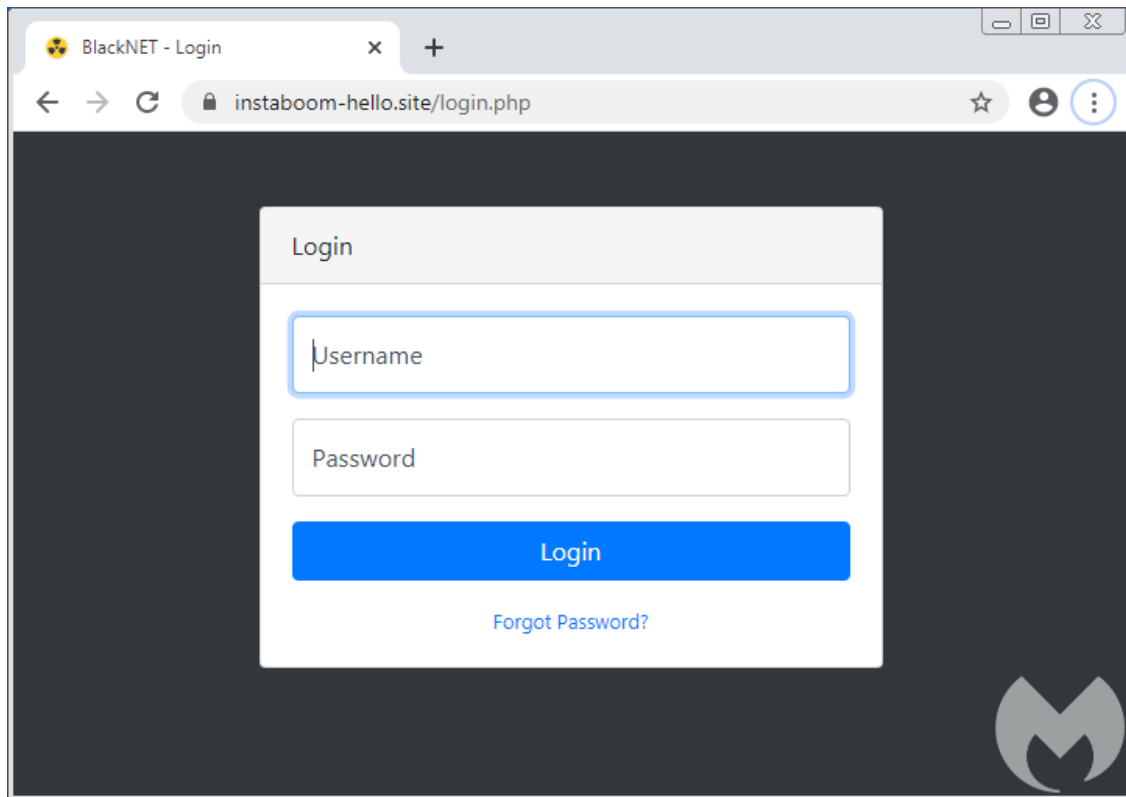


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table is a "Commands Center" with a dropdown menu for "Select Command" and a "Send Command" button. Further right is a "Map Visualization" section showing a world map with a few blue dots indicating client locations. At the bottom, a copyright notice reads "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

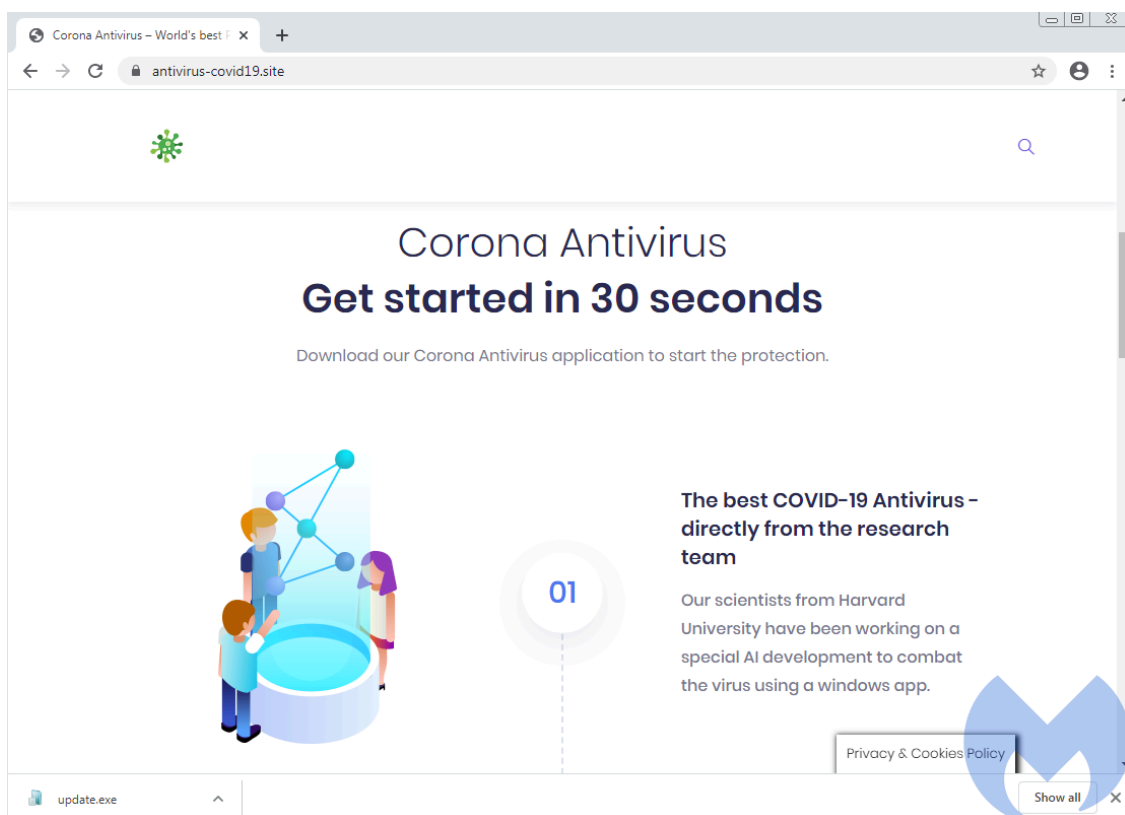
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

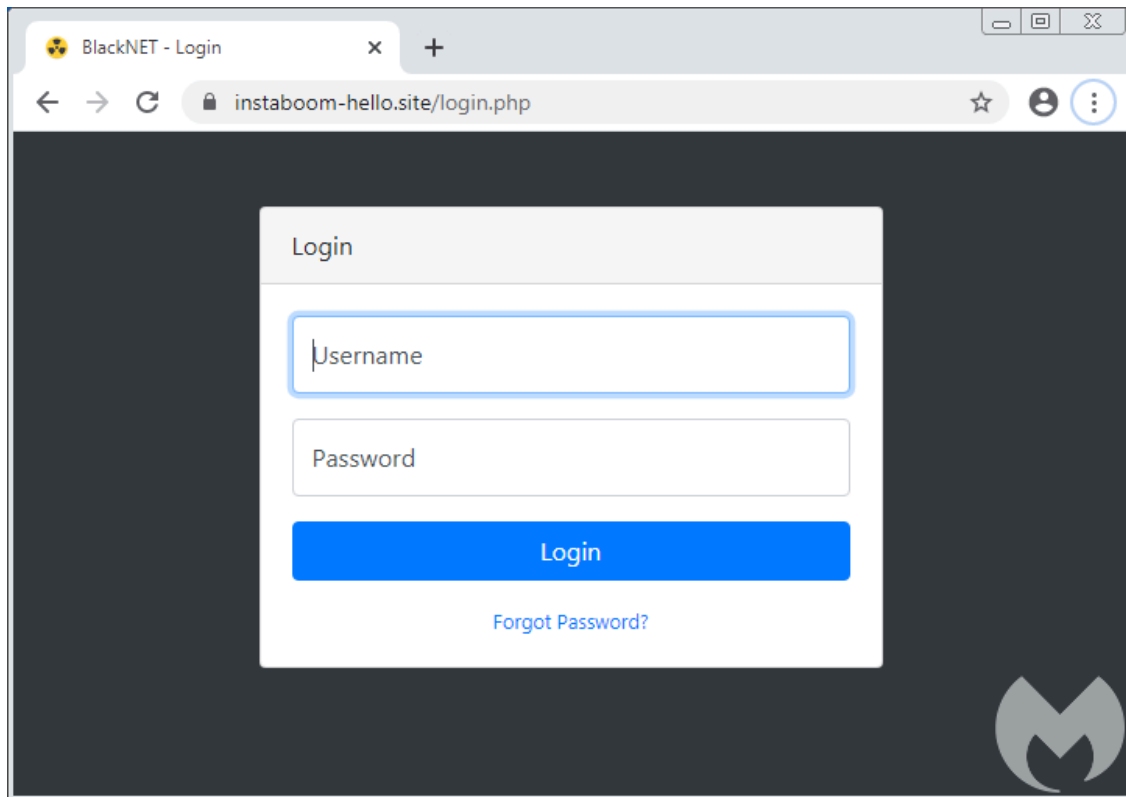


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

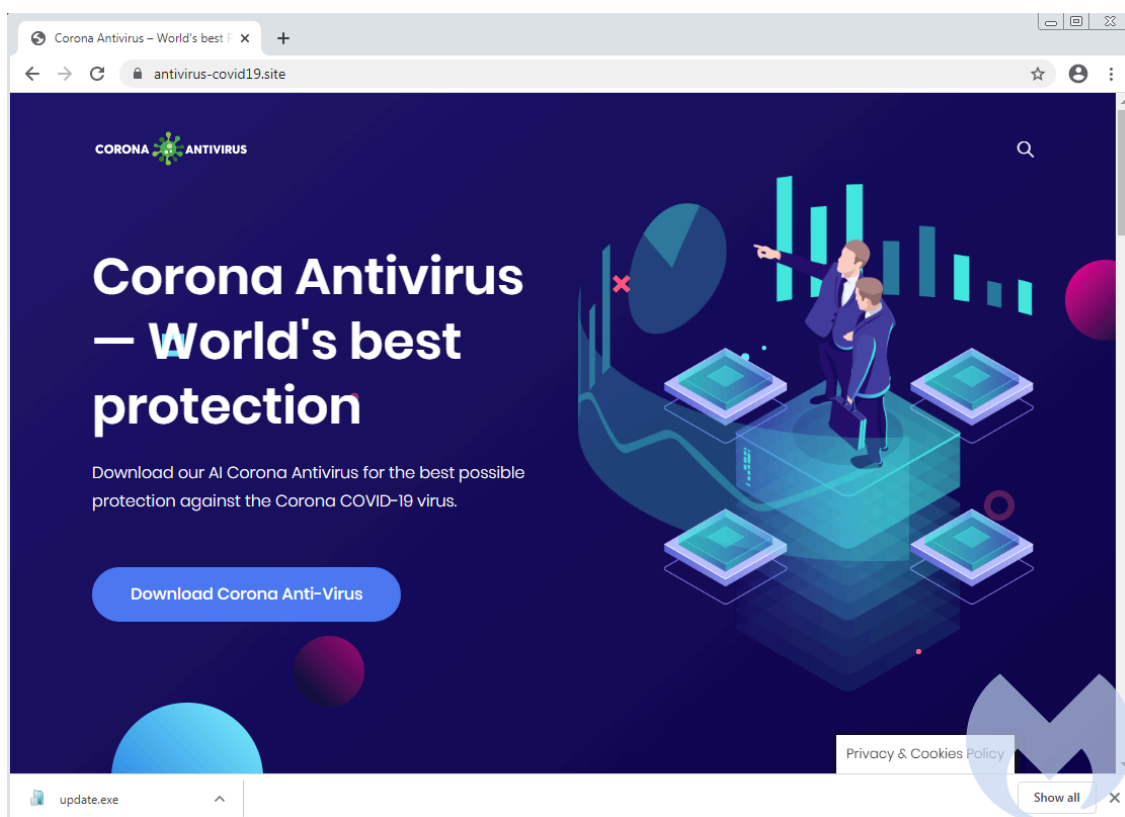
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

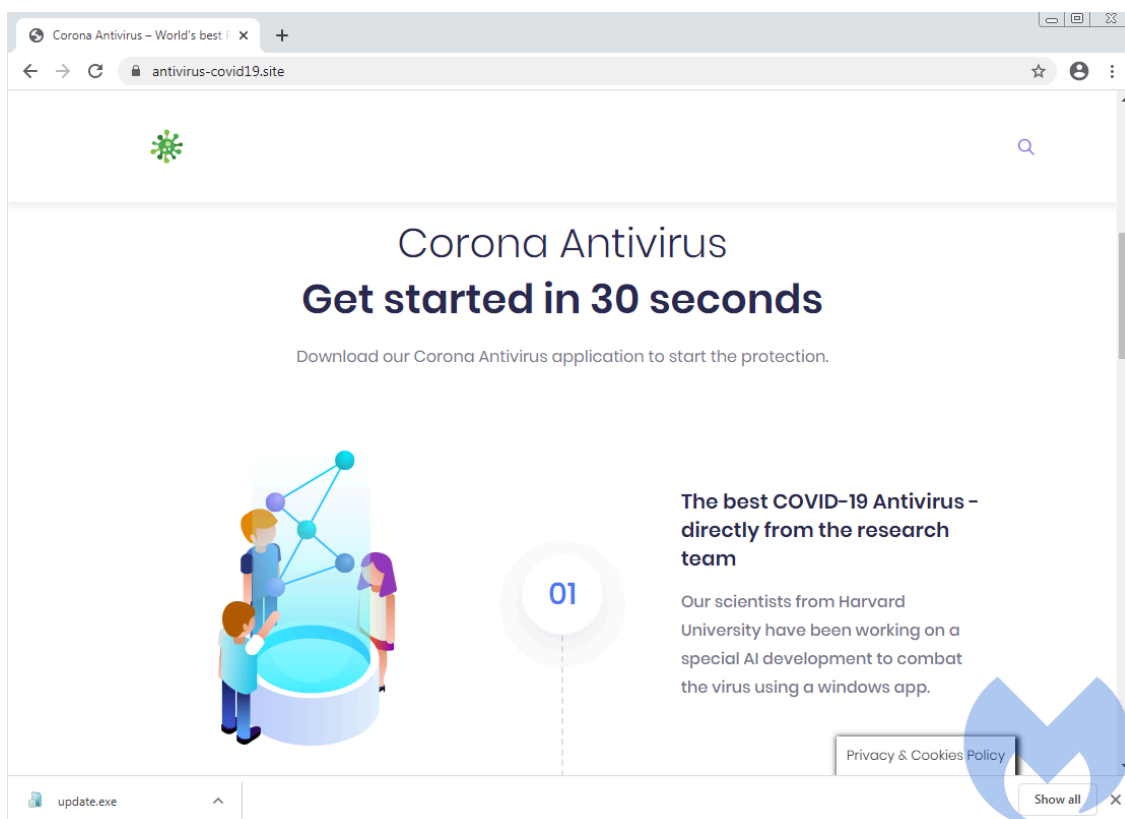
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

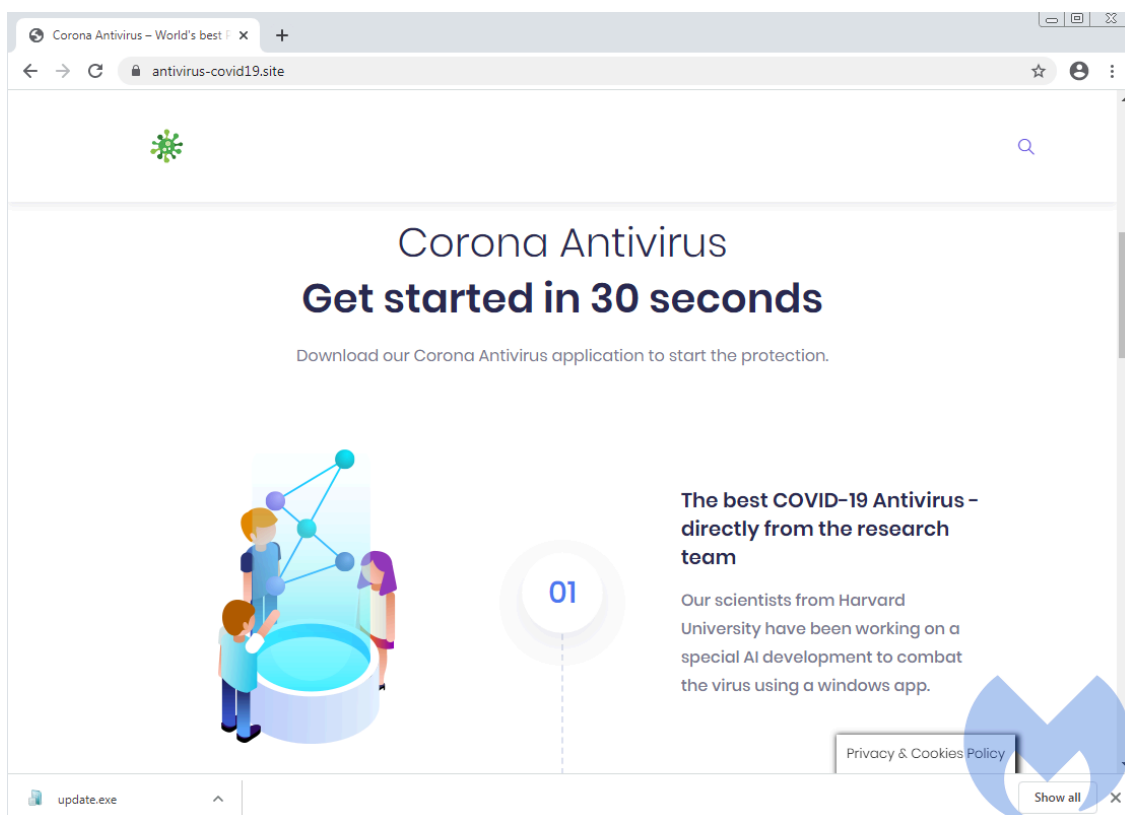
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

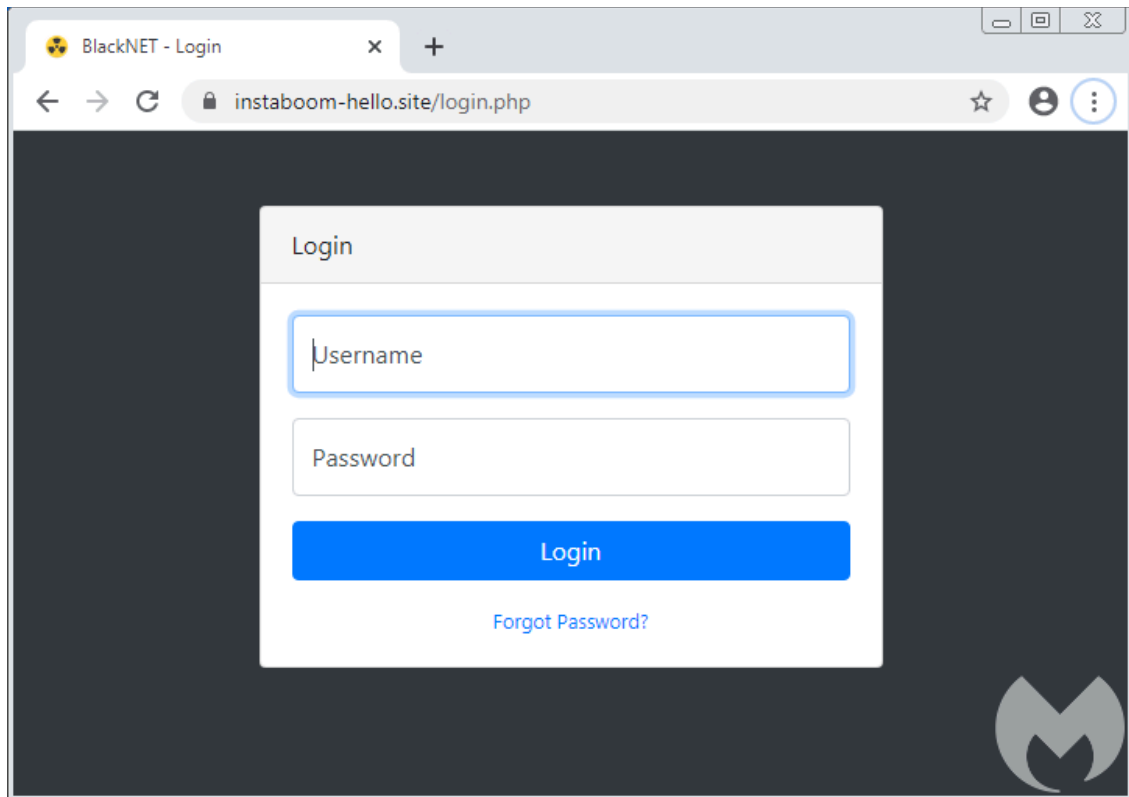


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

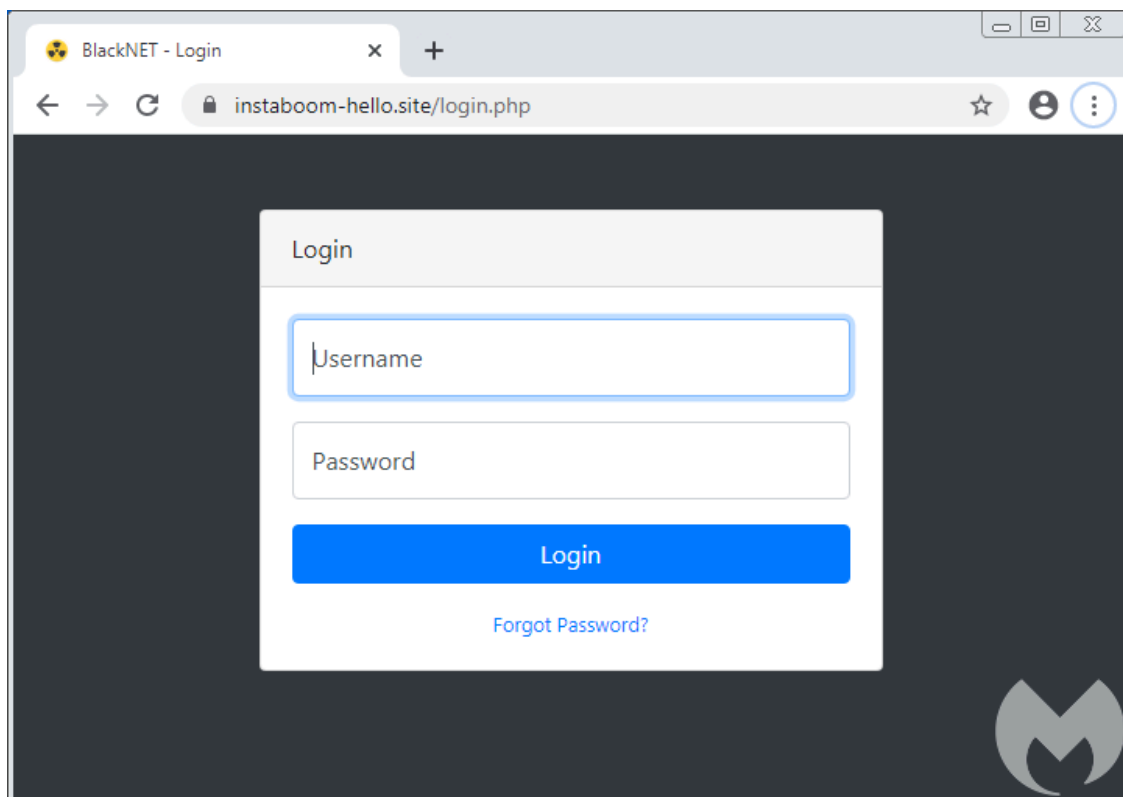
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

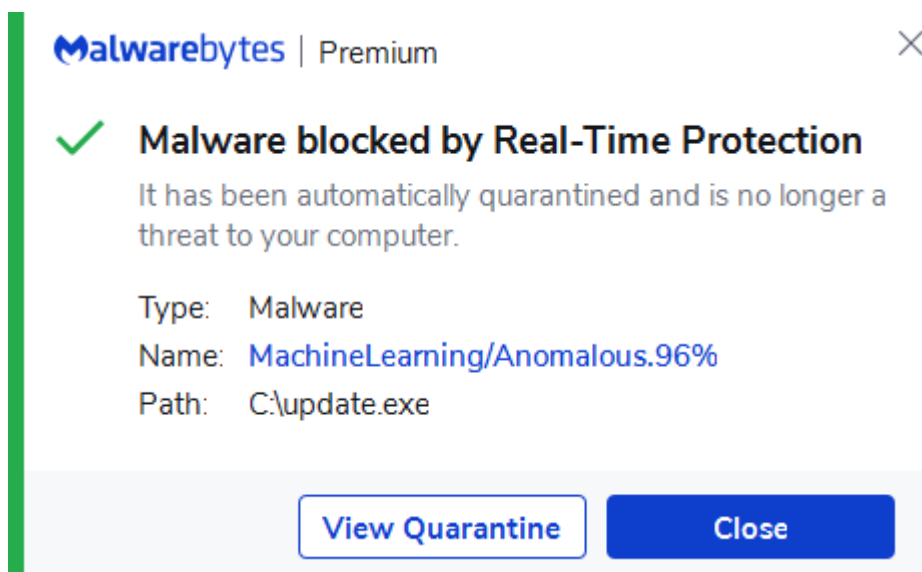
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

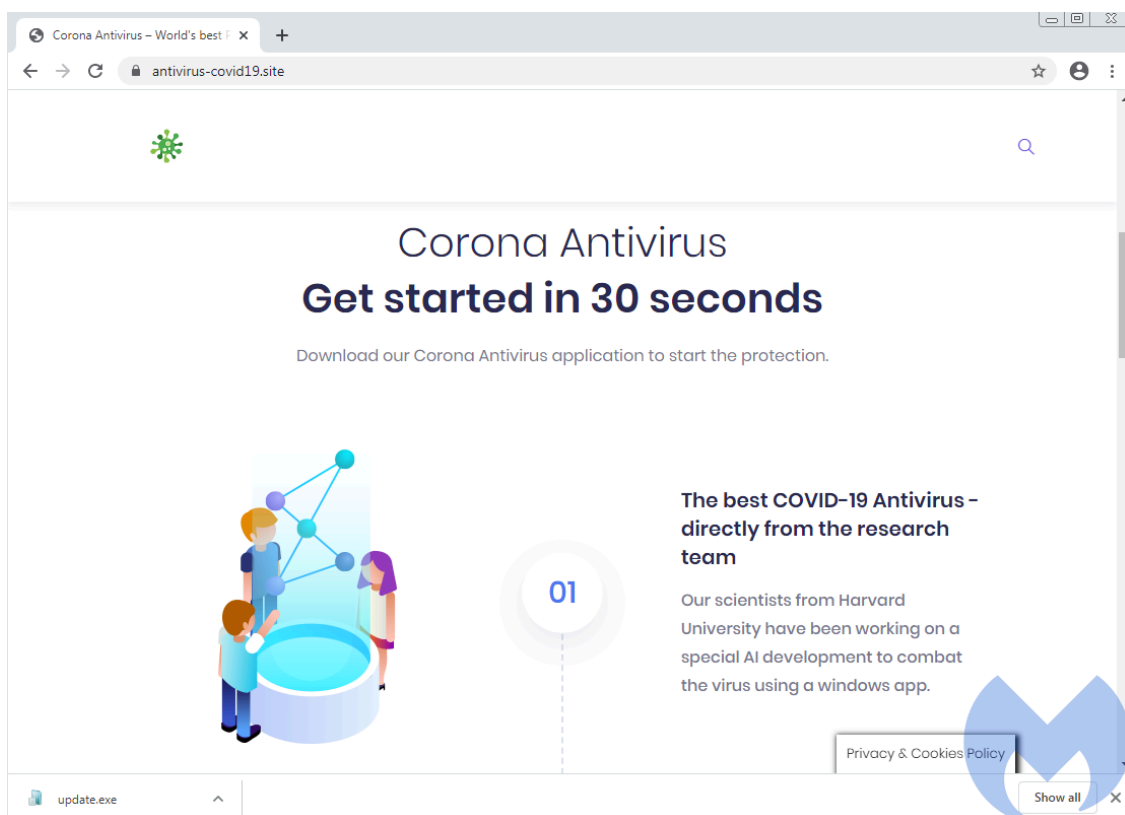
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

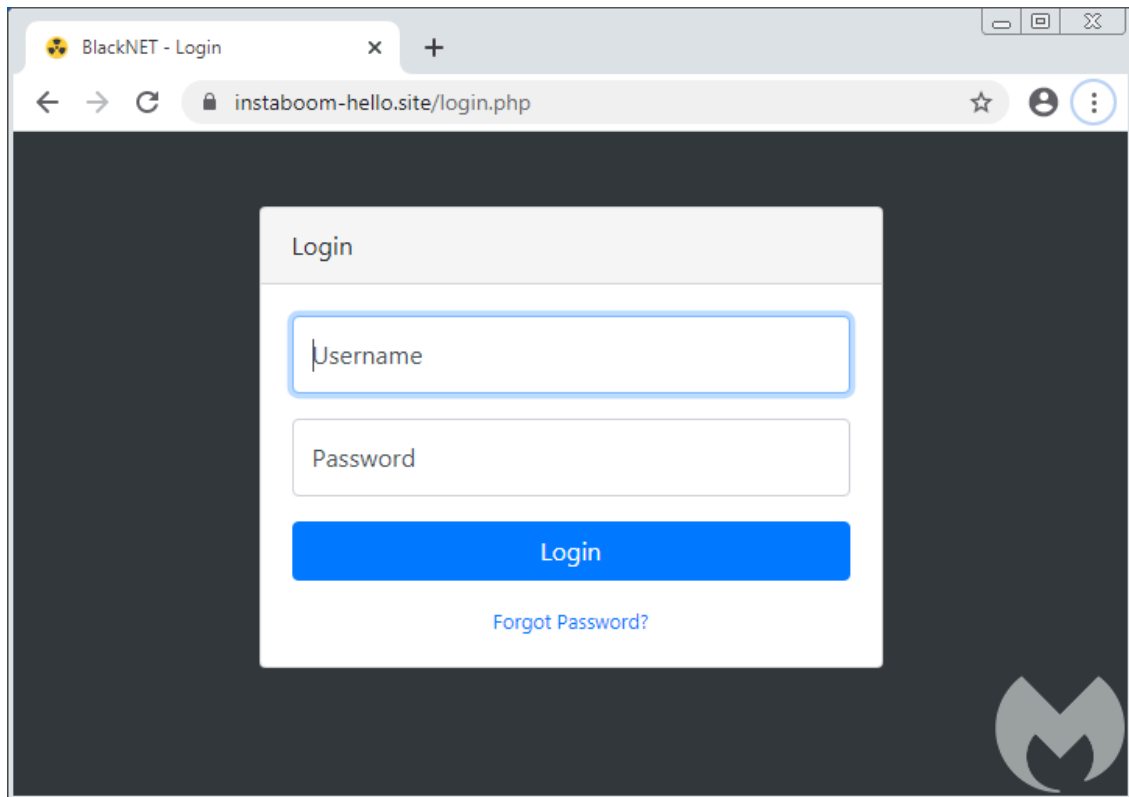


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

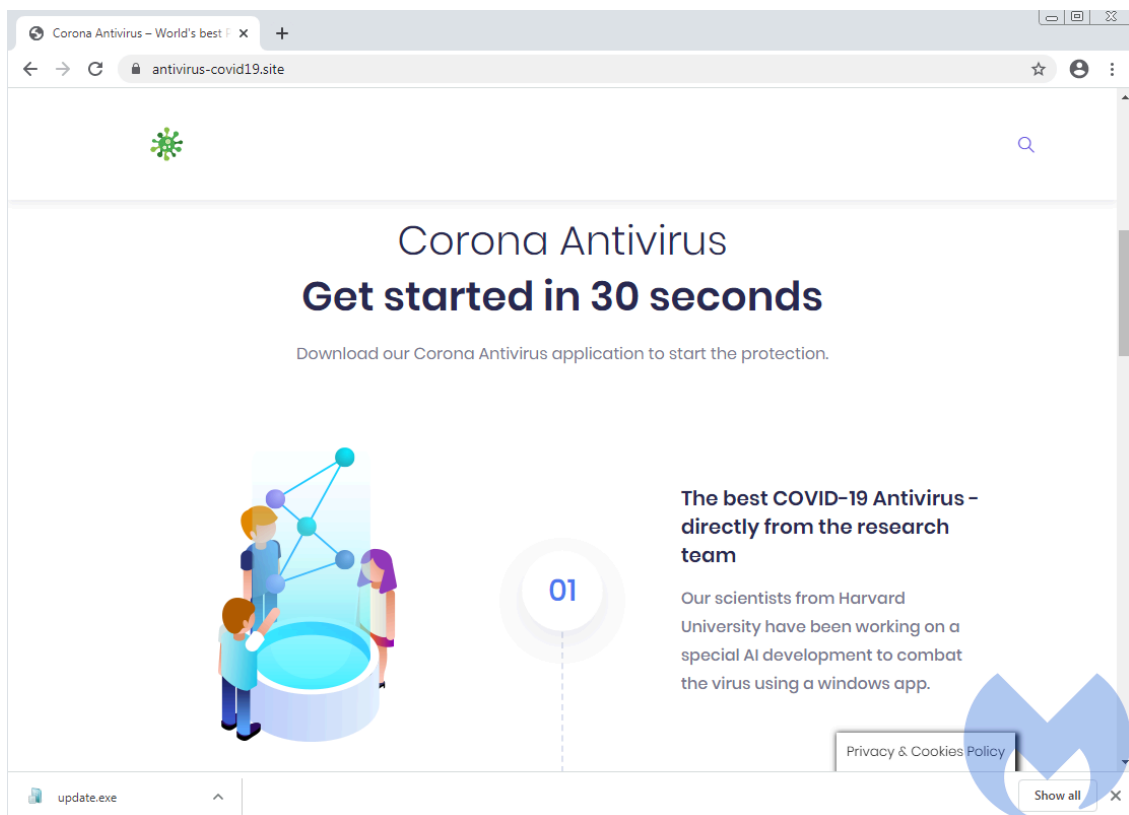
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

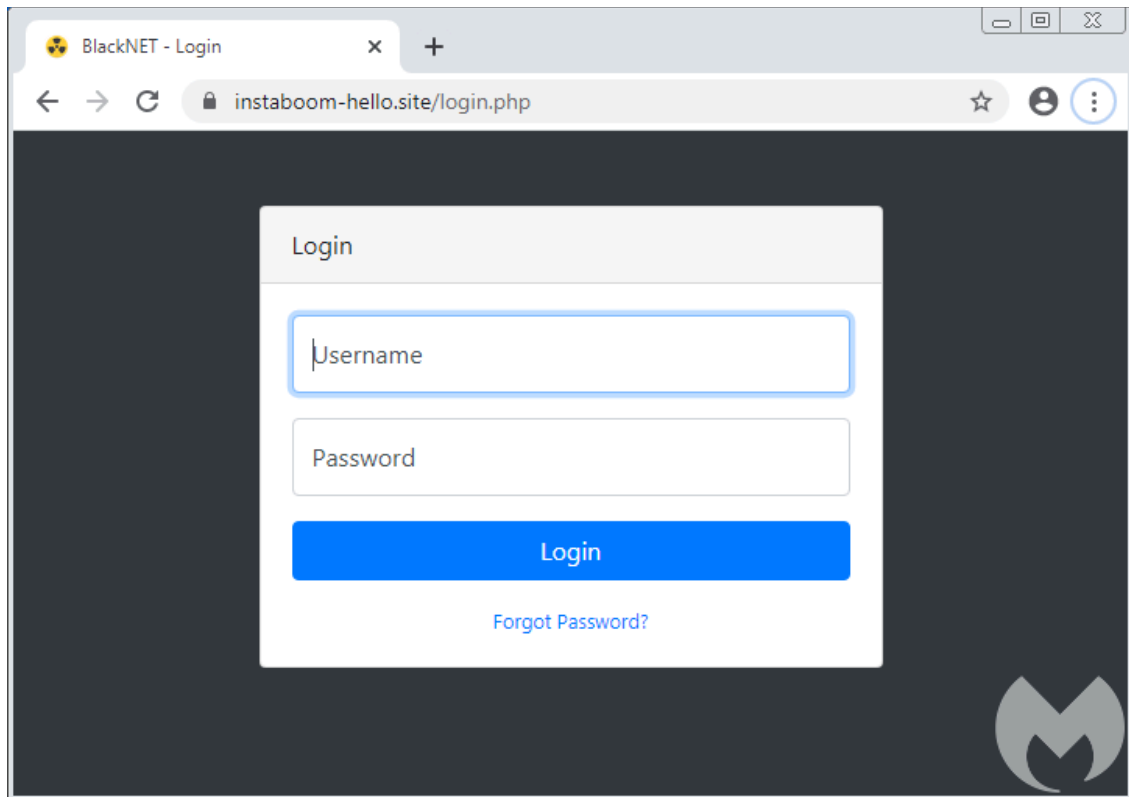


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored tiles: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

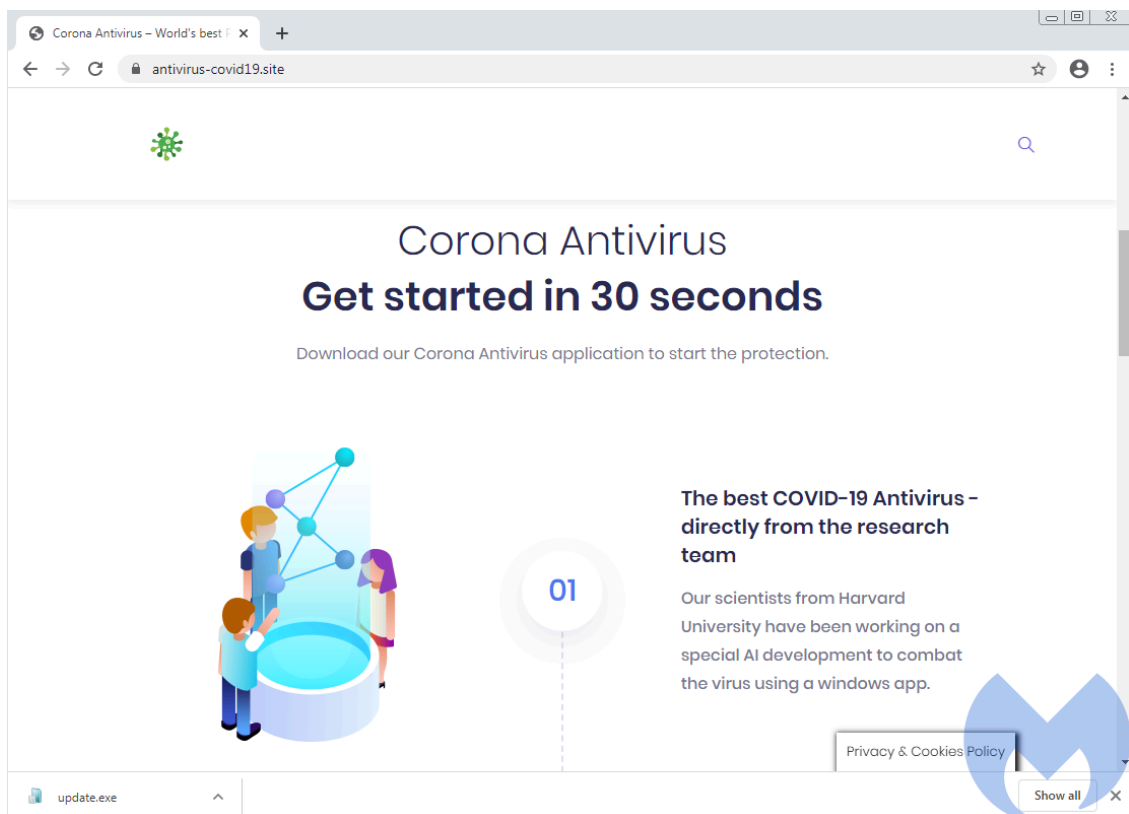
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

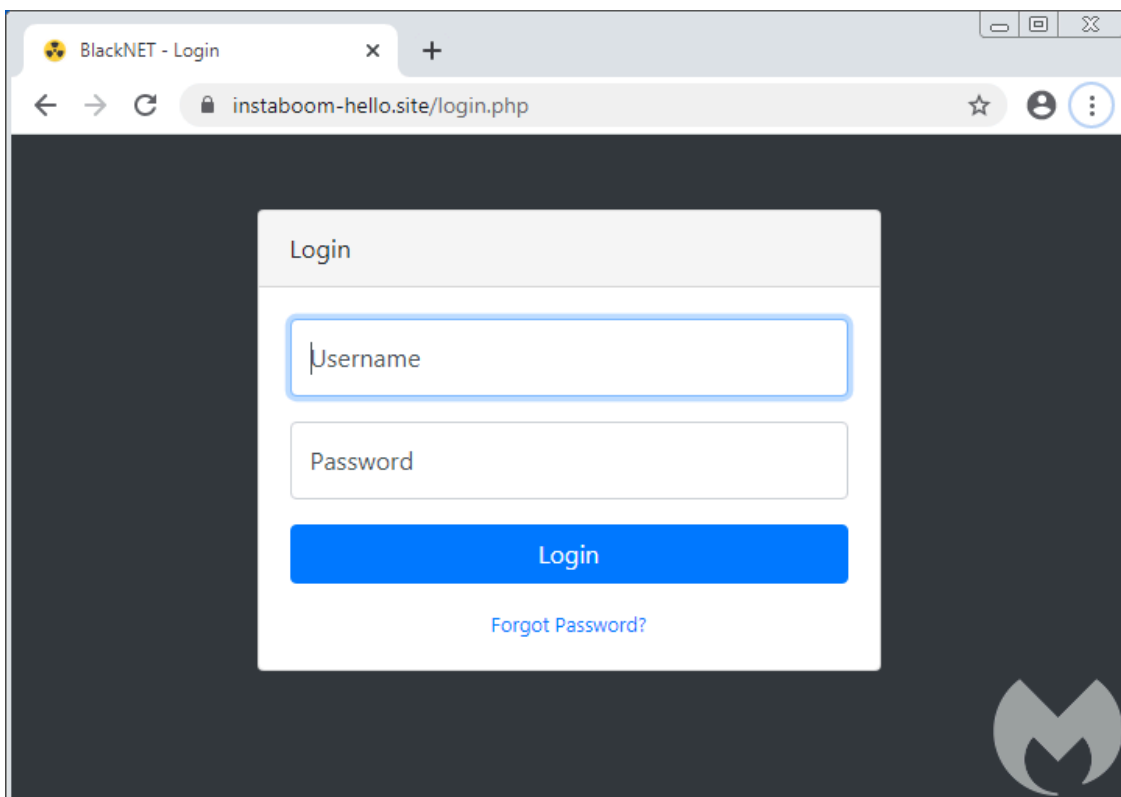


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

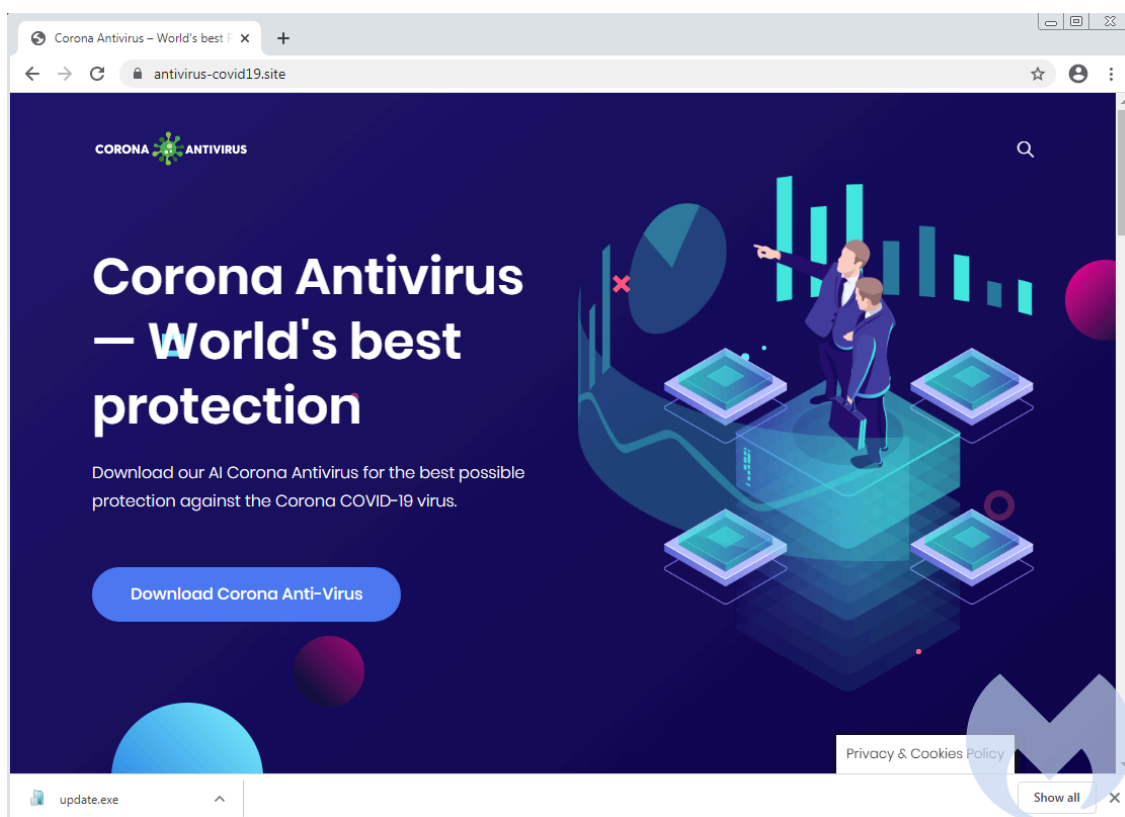
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

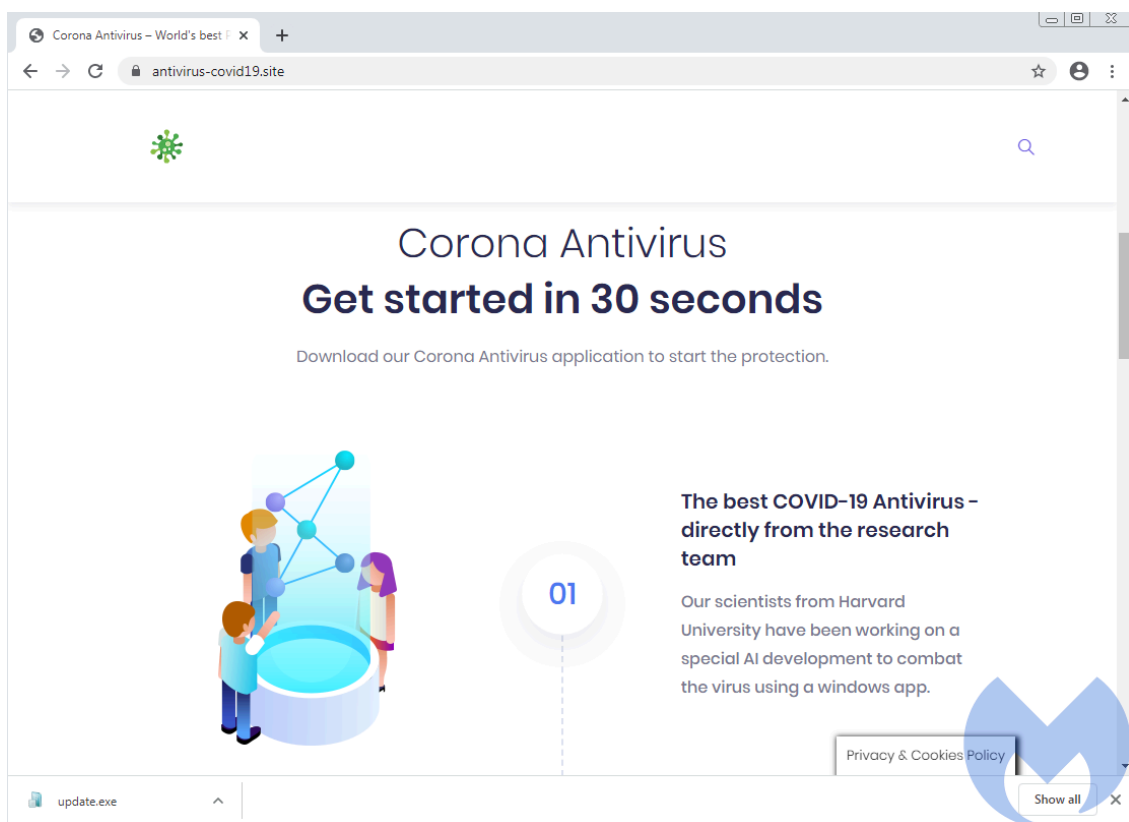
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

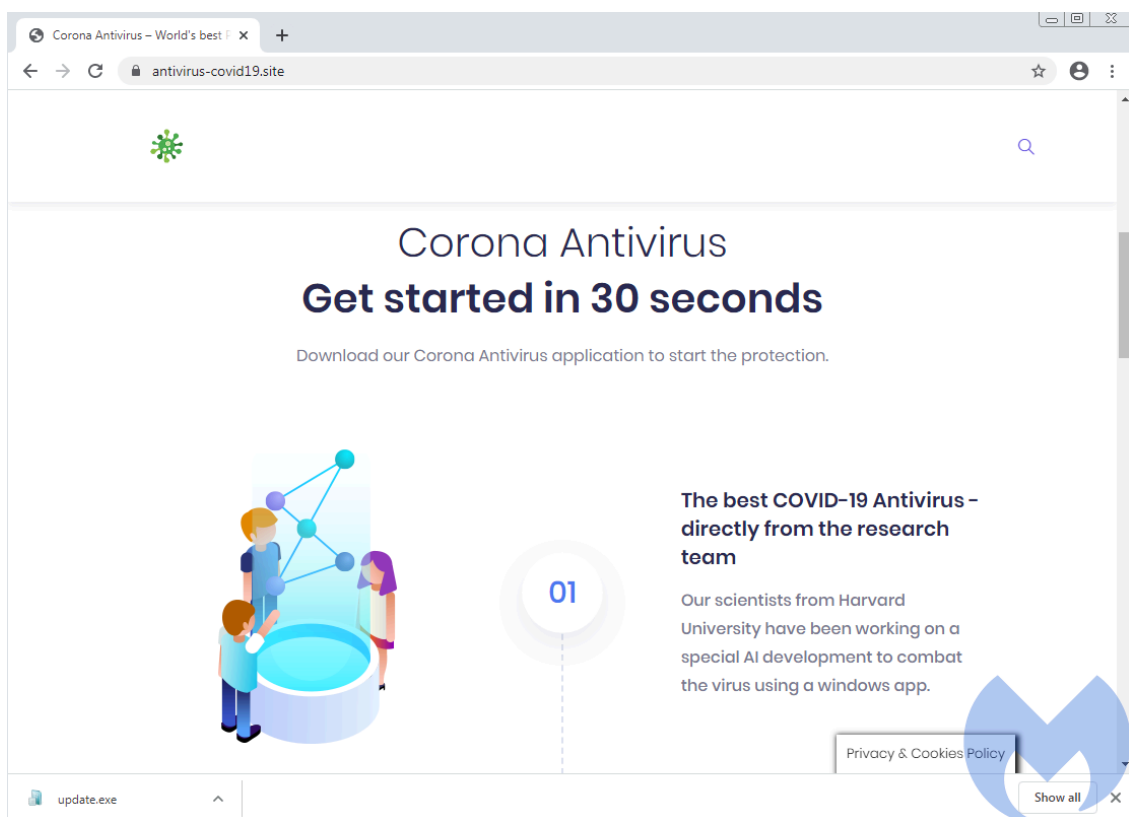
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

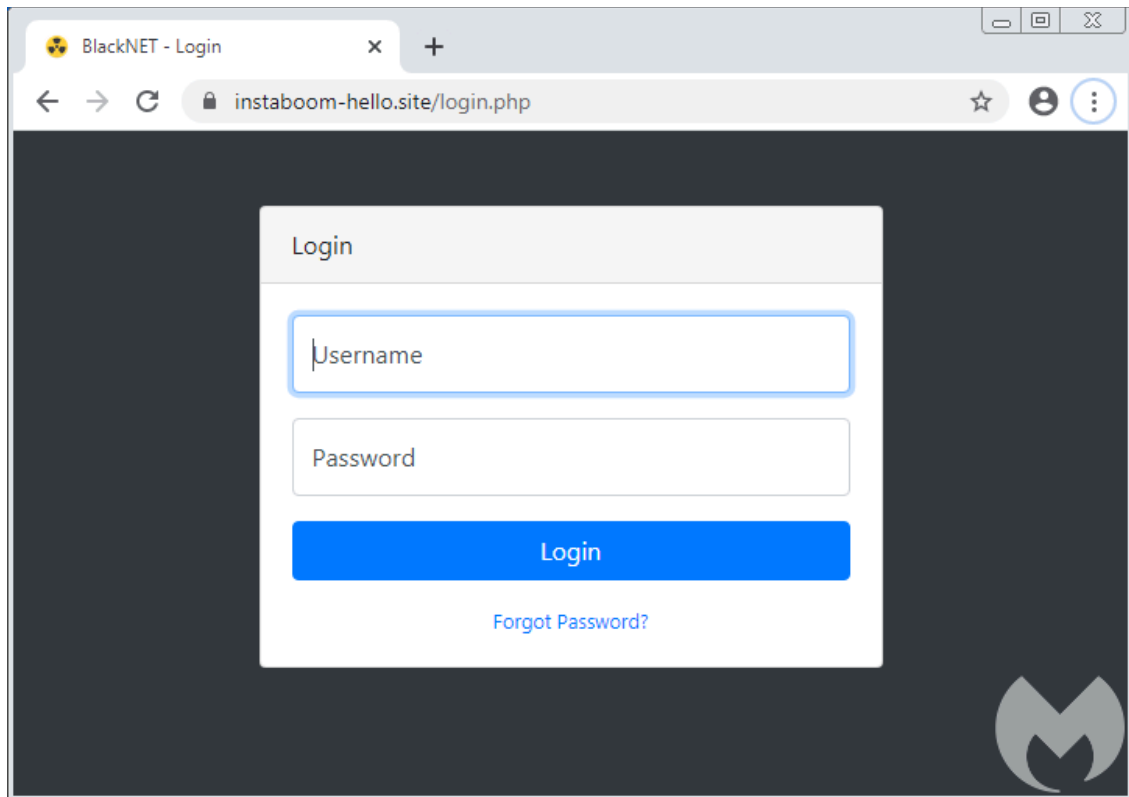


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

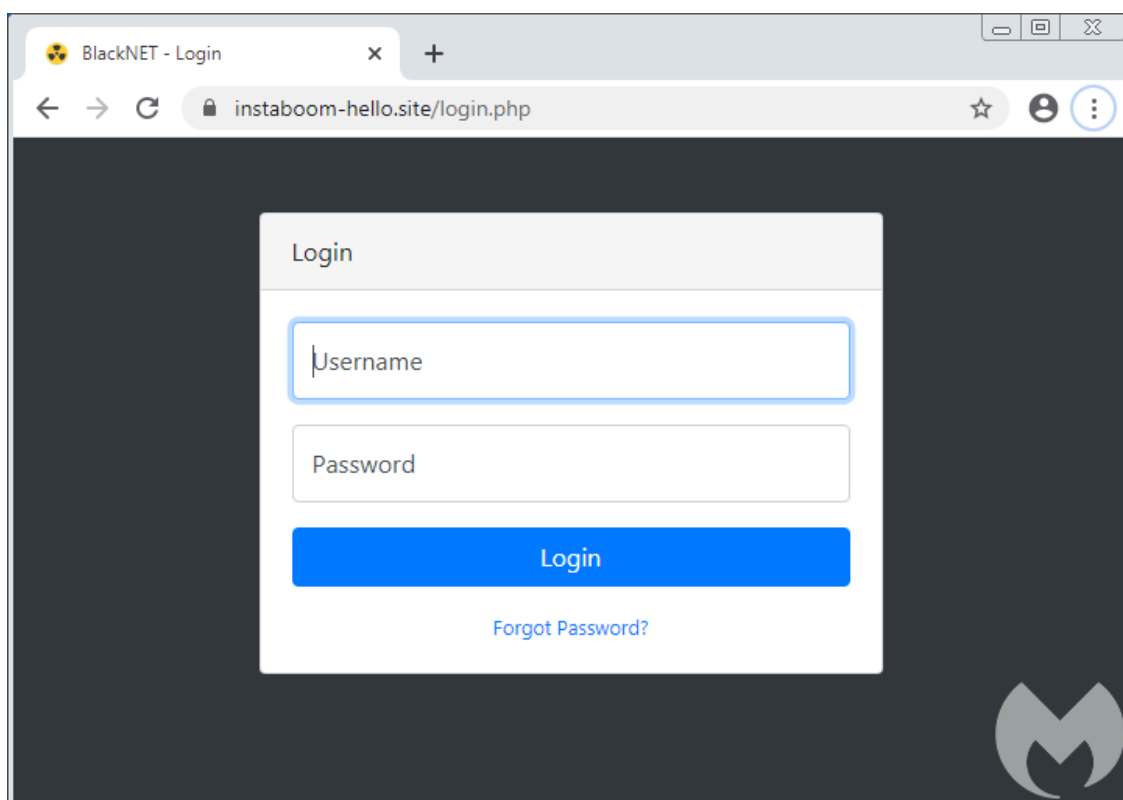
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

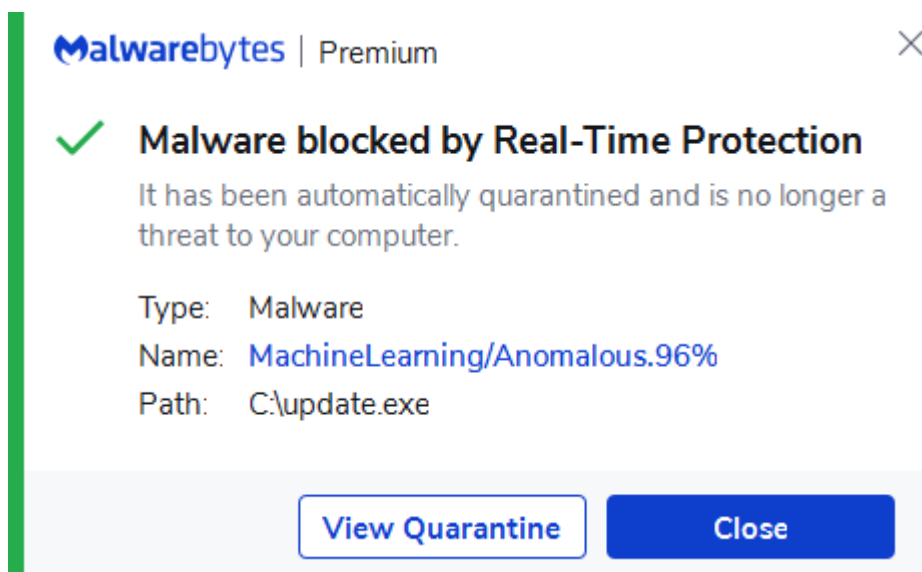
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' pagination buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

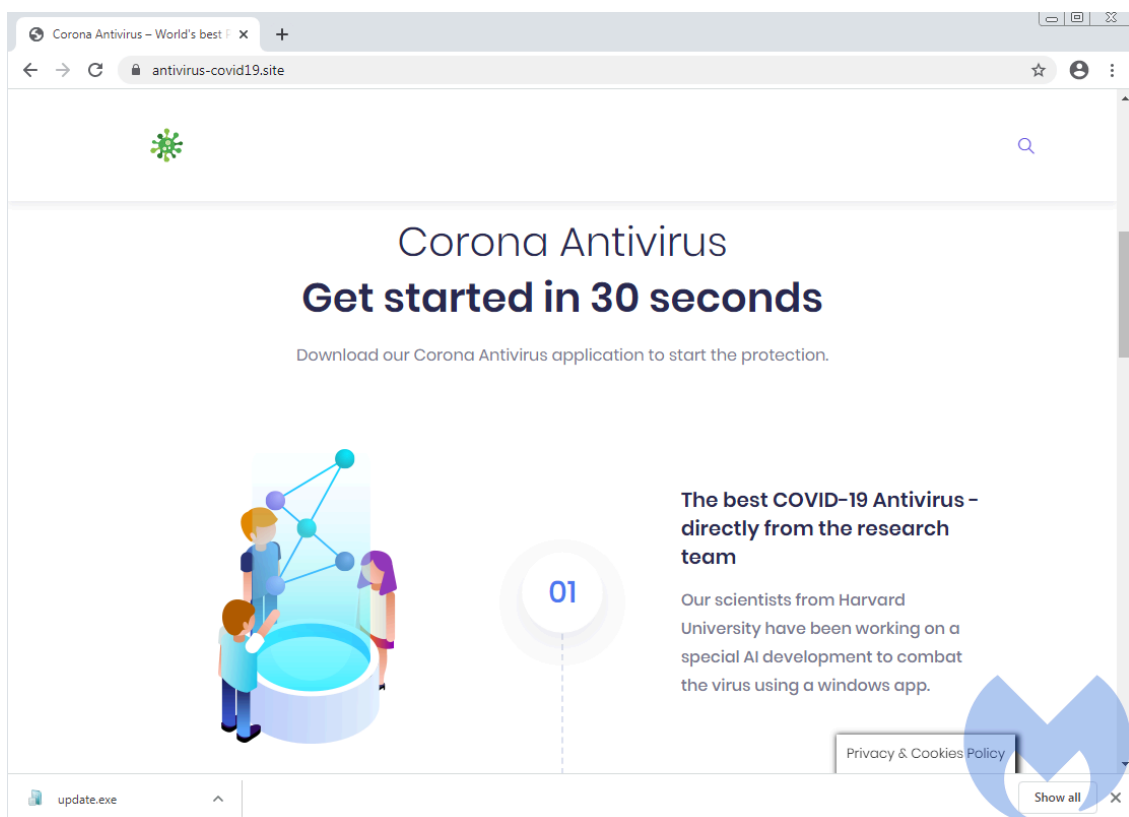
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

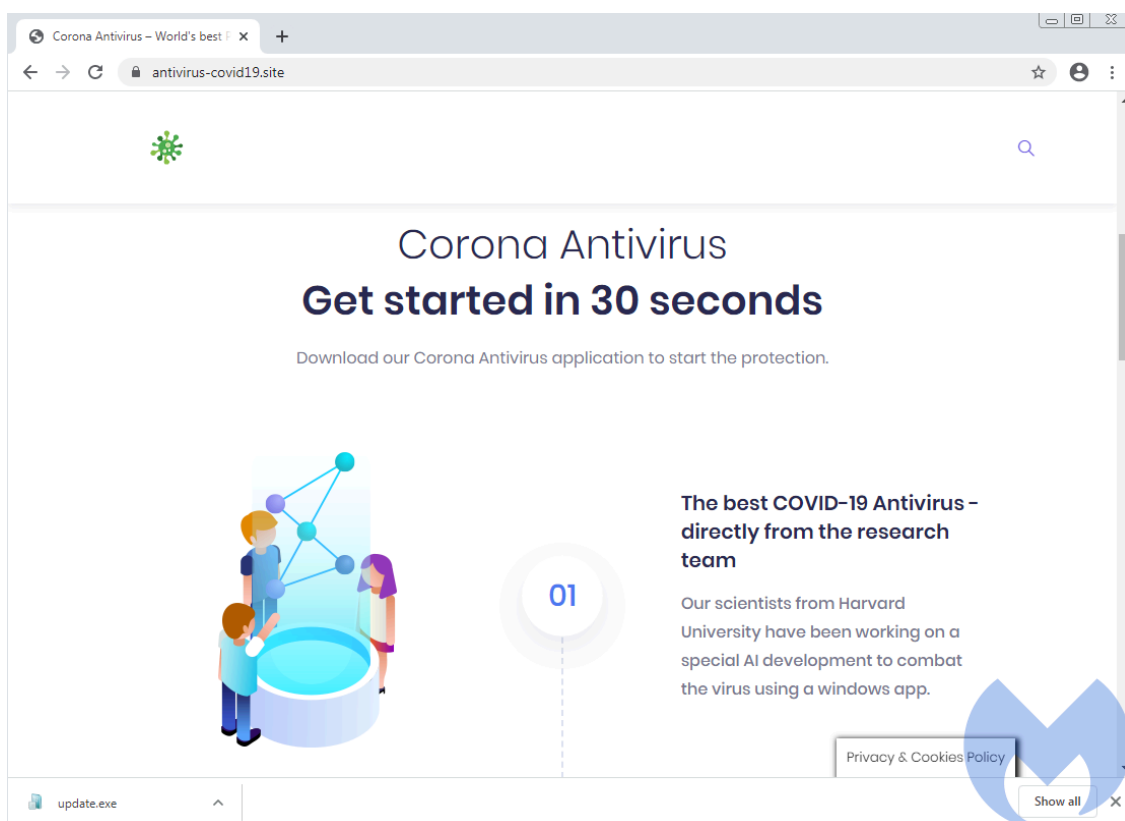
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

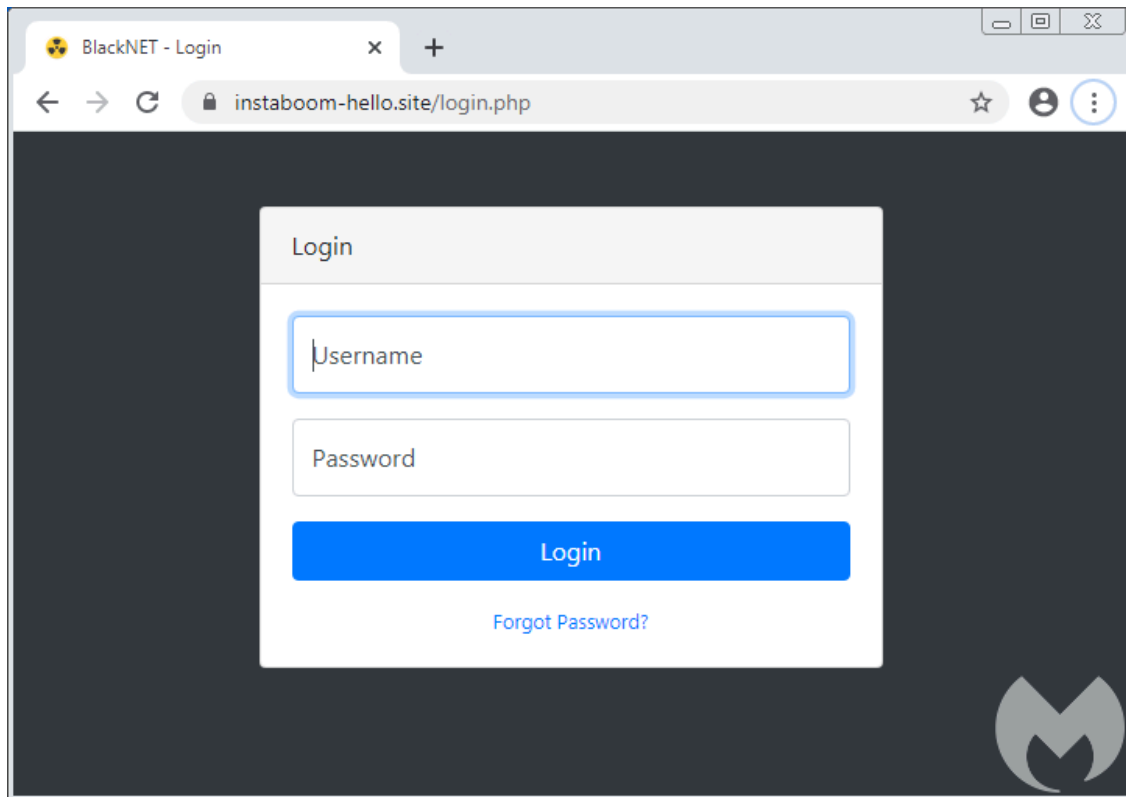


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

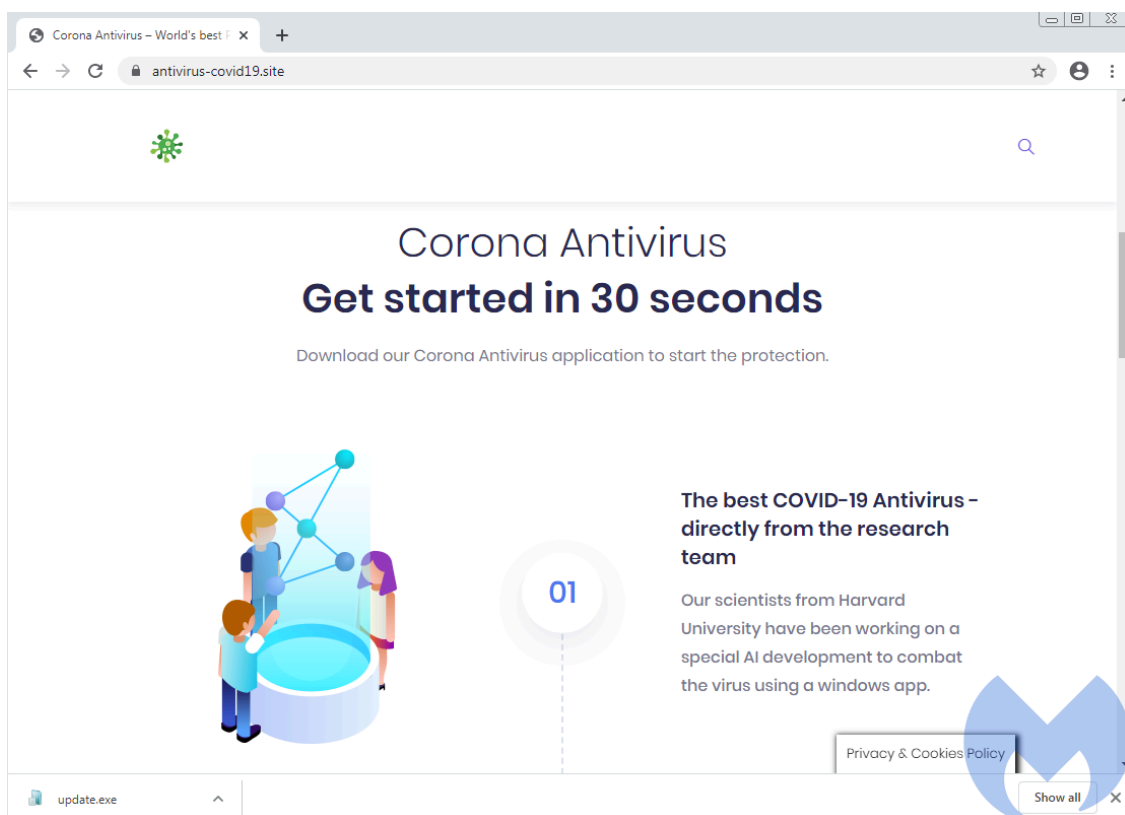
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

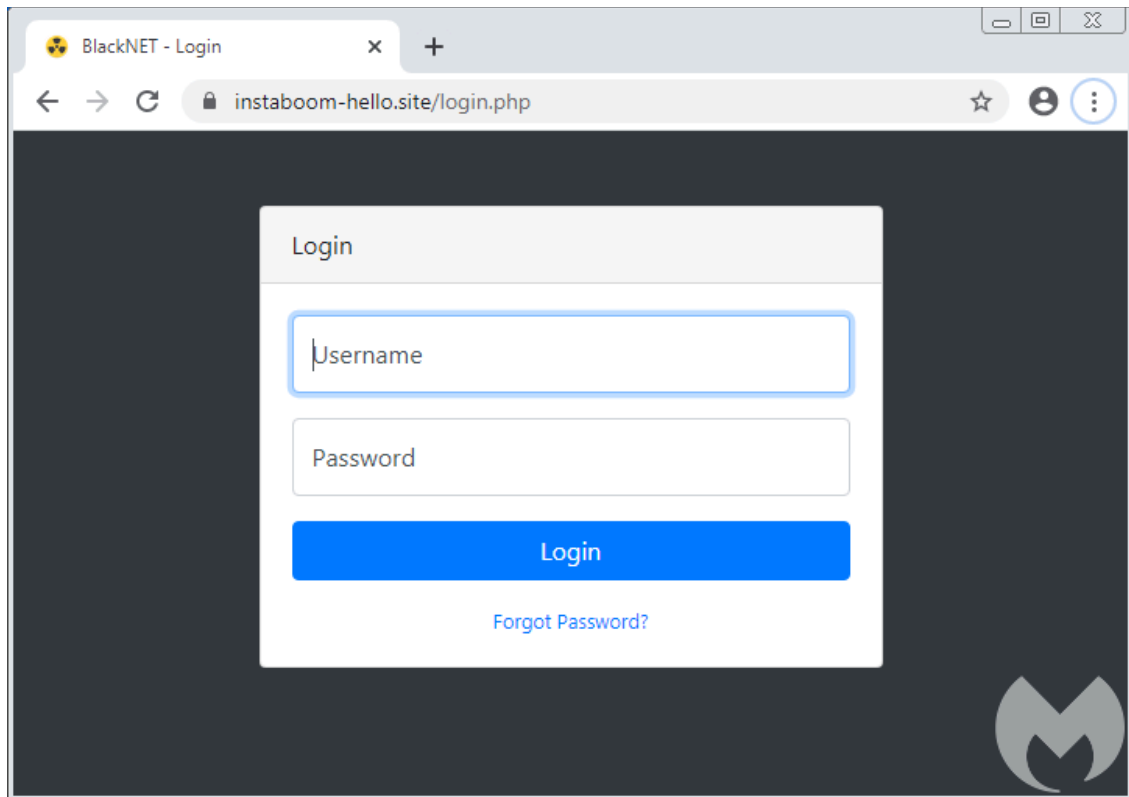


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

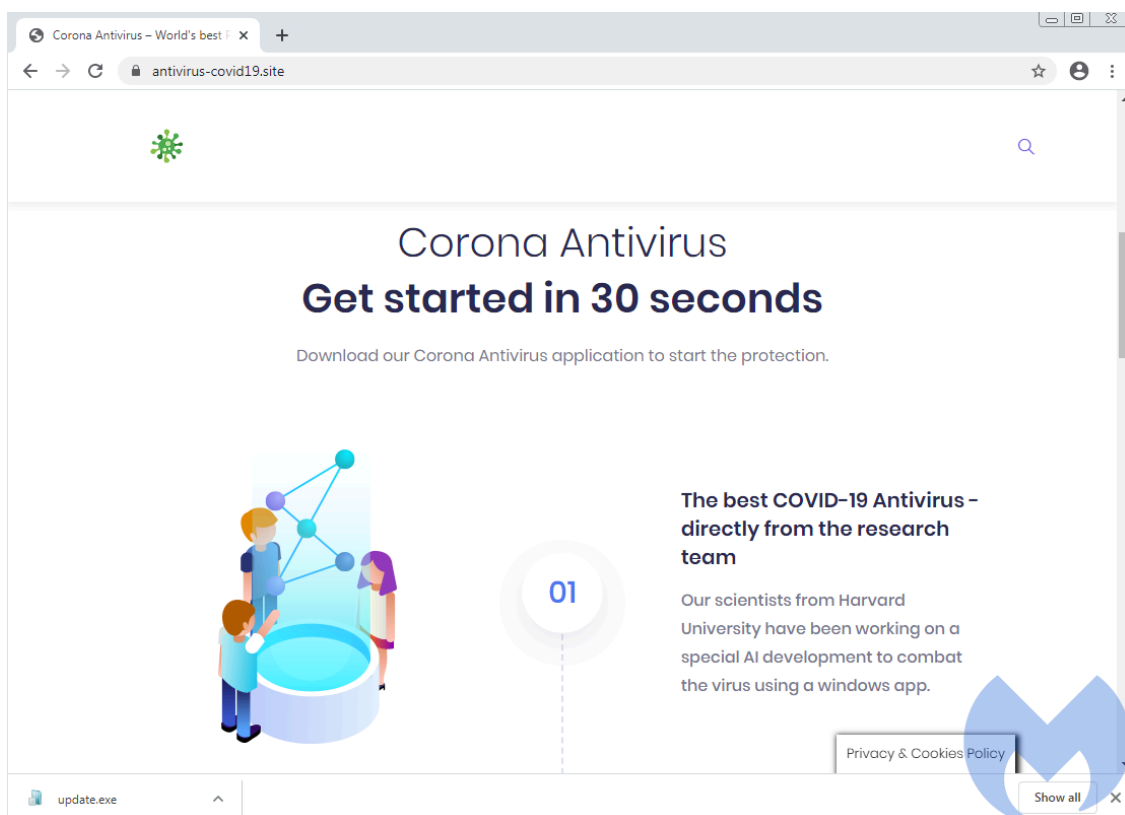
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

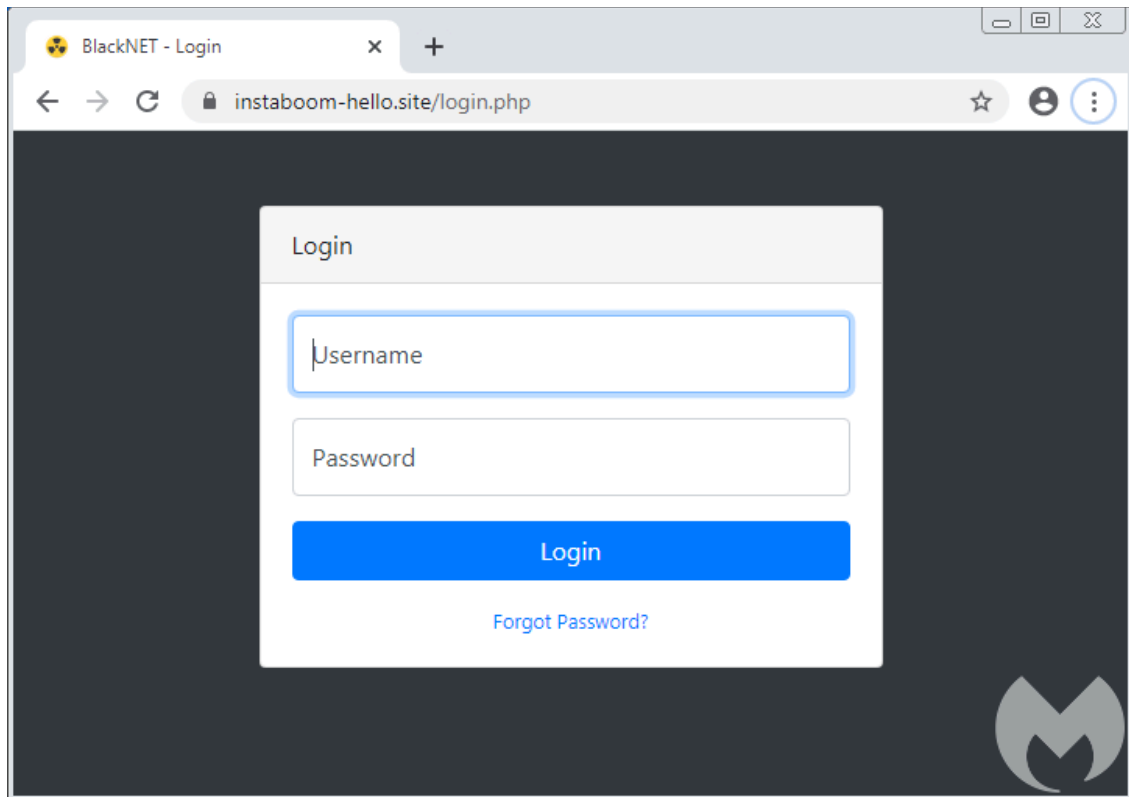


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients!

0 USB Clients!

0 Online Clients!

0 Offline Clients!

Bot/Slaves List

Show 10 entries
Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries

Previous Next

Commands Center

Command

Execute

Select Command

Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Premium

Malware blocked by Real-Time Protection

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: MachineLearning/Anomalous.96%
Path: C:\update.exe

View Quarantine

Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

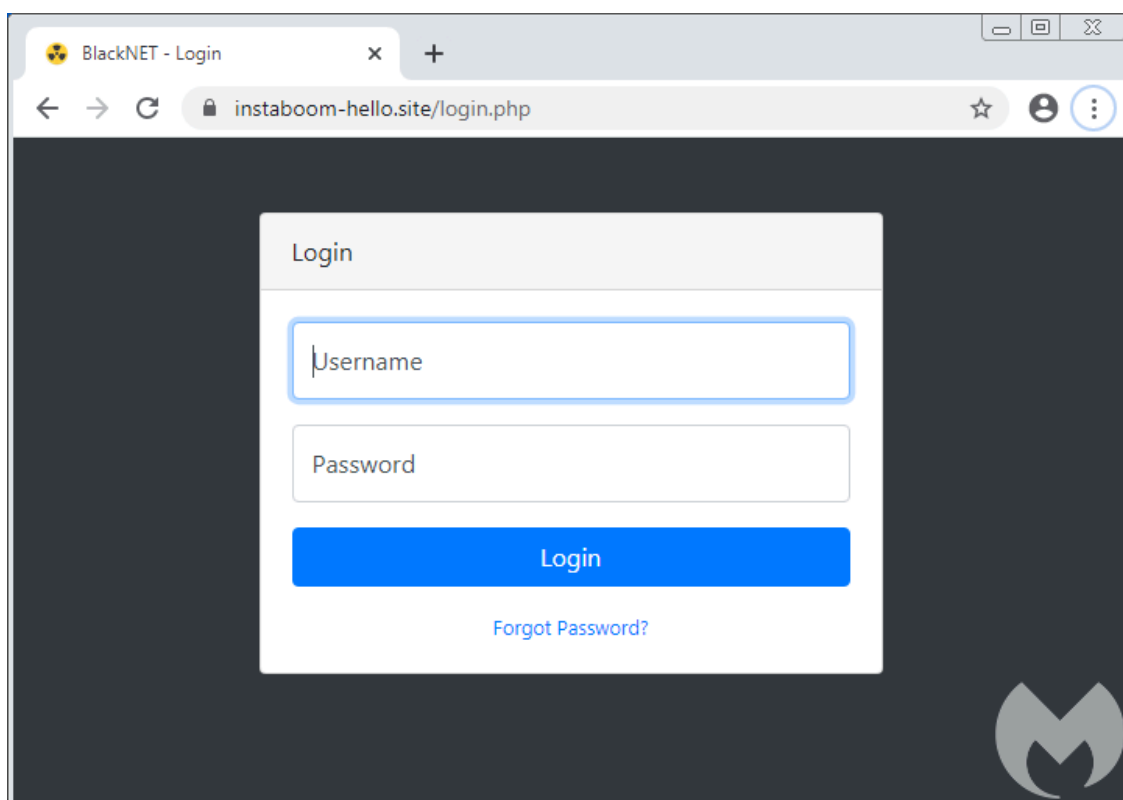
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

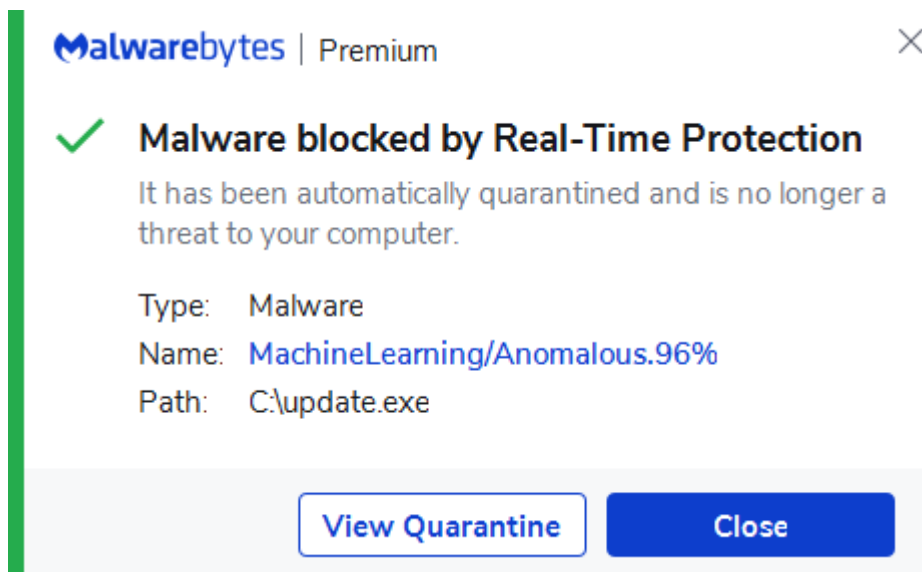
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

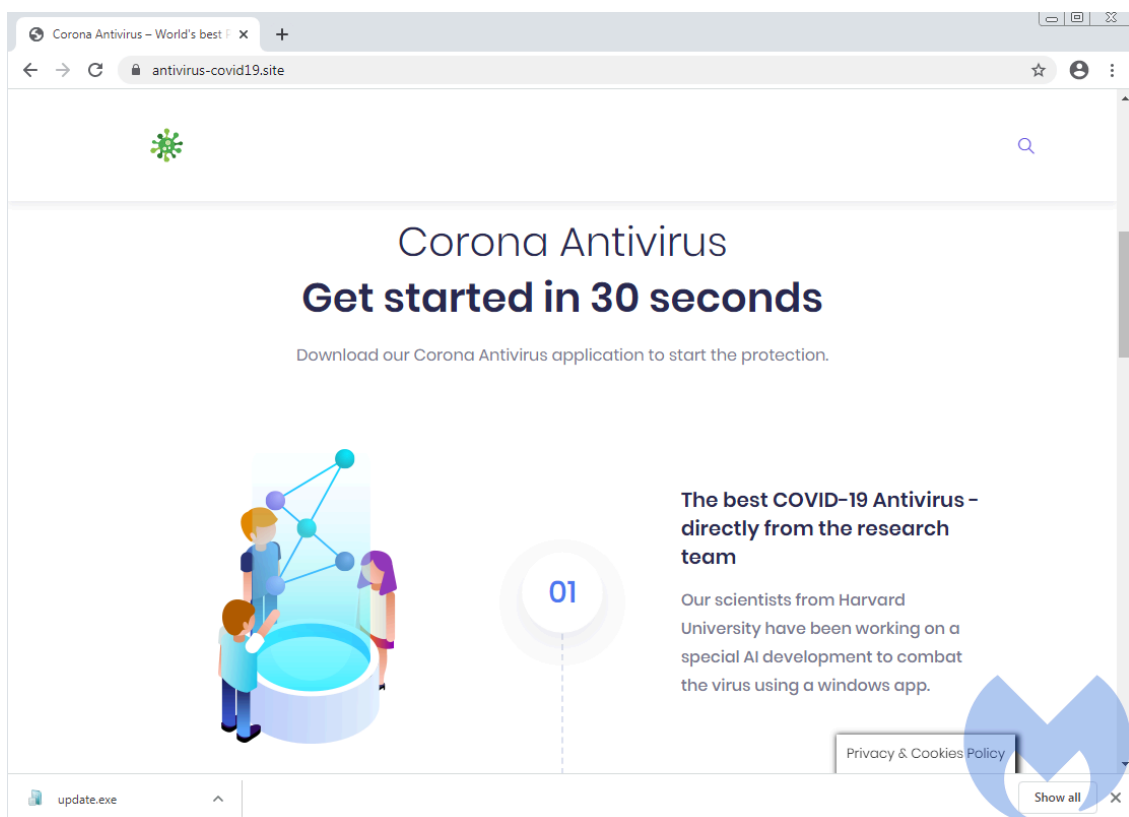
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

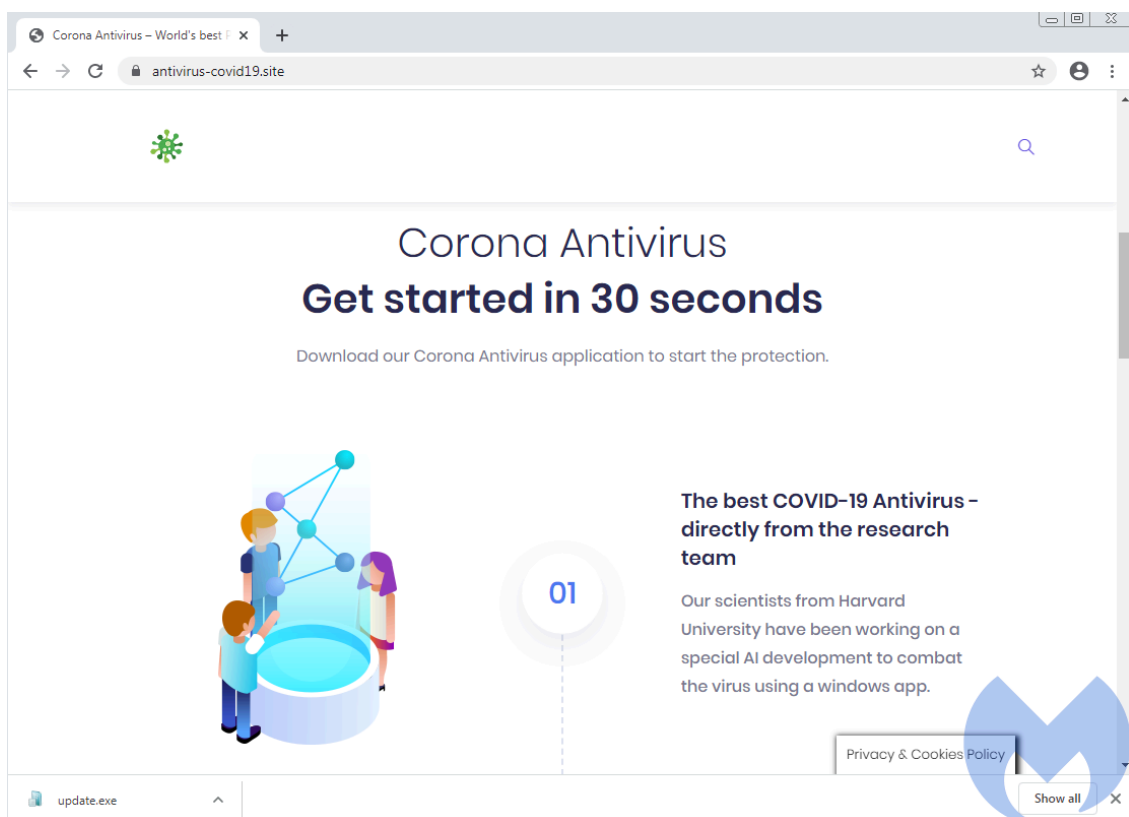
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

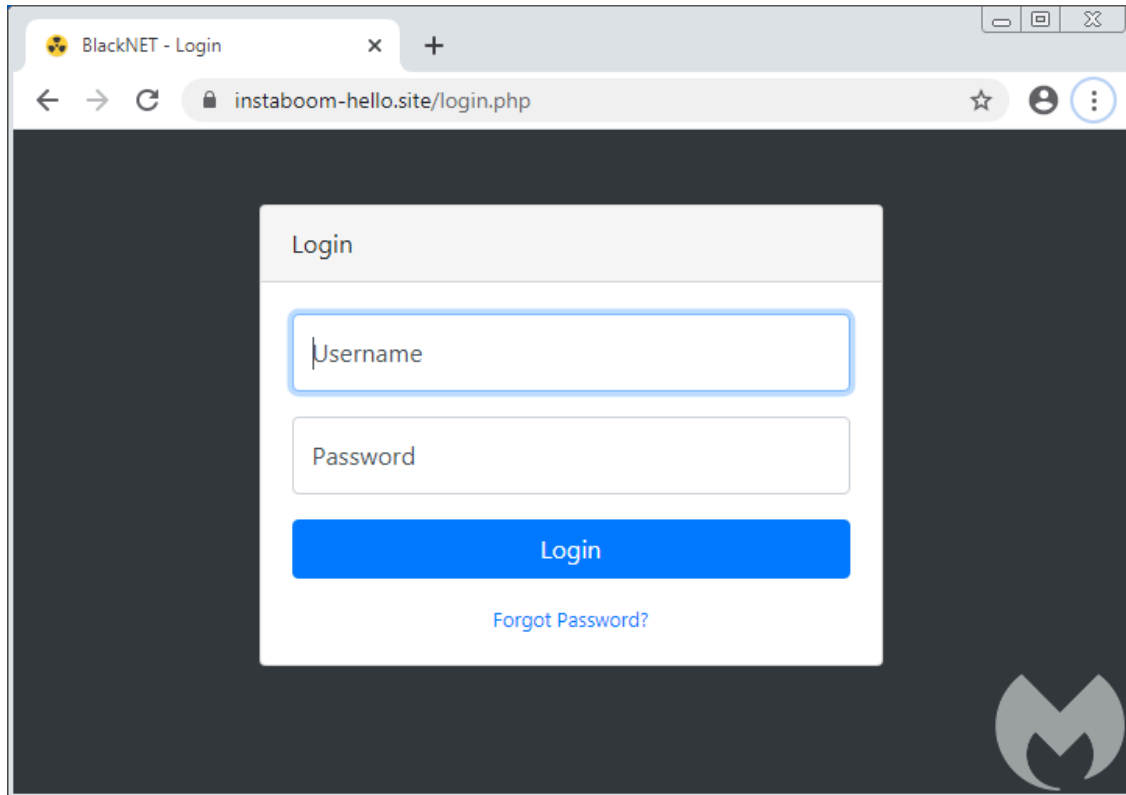


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

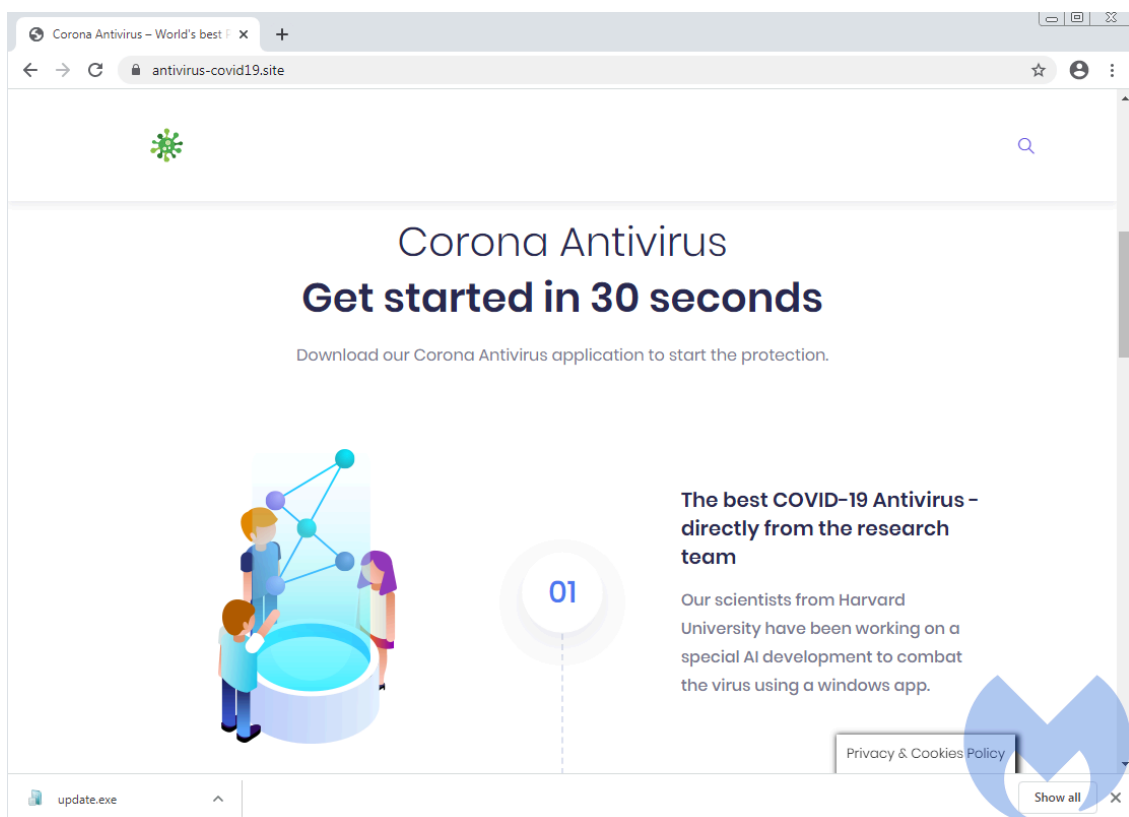
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with blue dots representing clients. At the bottom of the interface is a footer with the text "Copyright © BLACKNET by Black.Hacker - 2020" and a large blue logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. The window has a green vertical bar on the left and a close button (X) in the top right corner. The main content area has a green checkmark icon and the text "Malware blocked by Real-Time Protection". Below this, it says "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following information: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

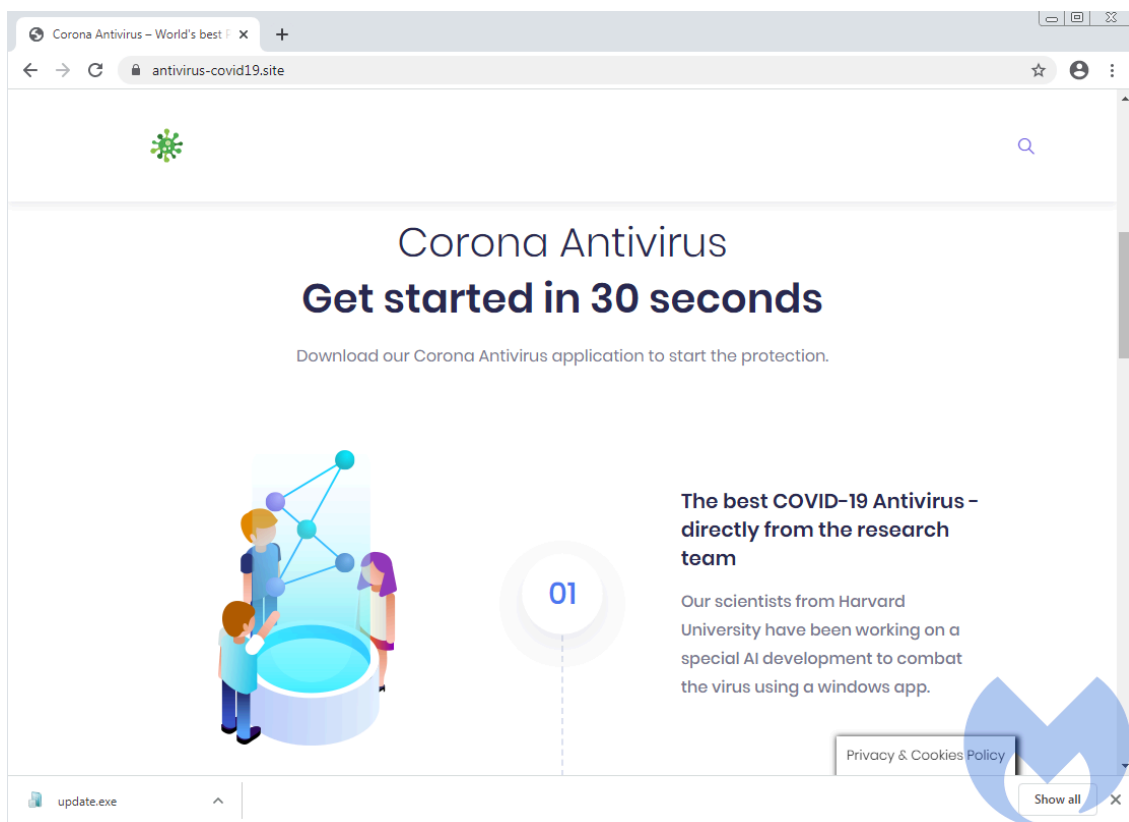
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

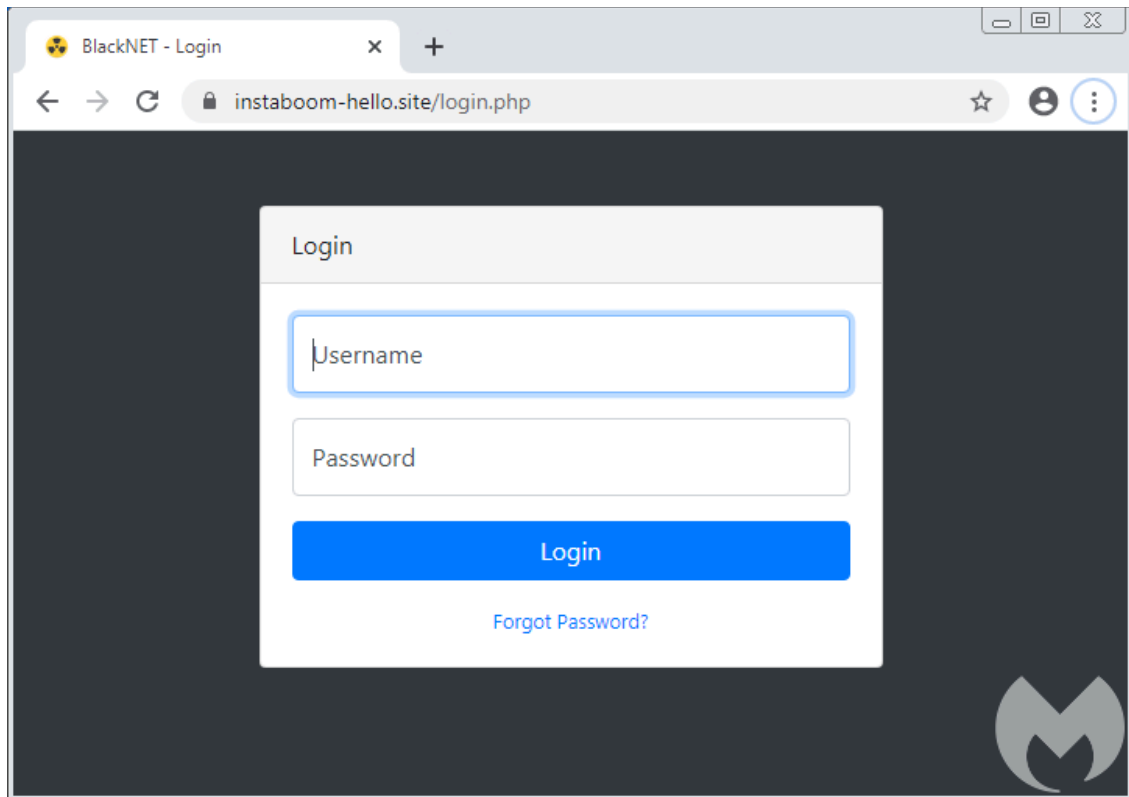


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

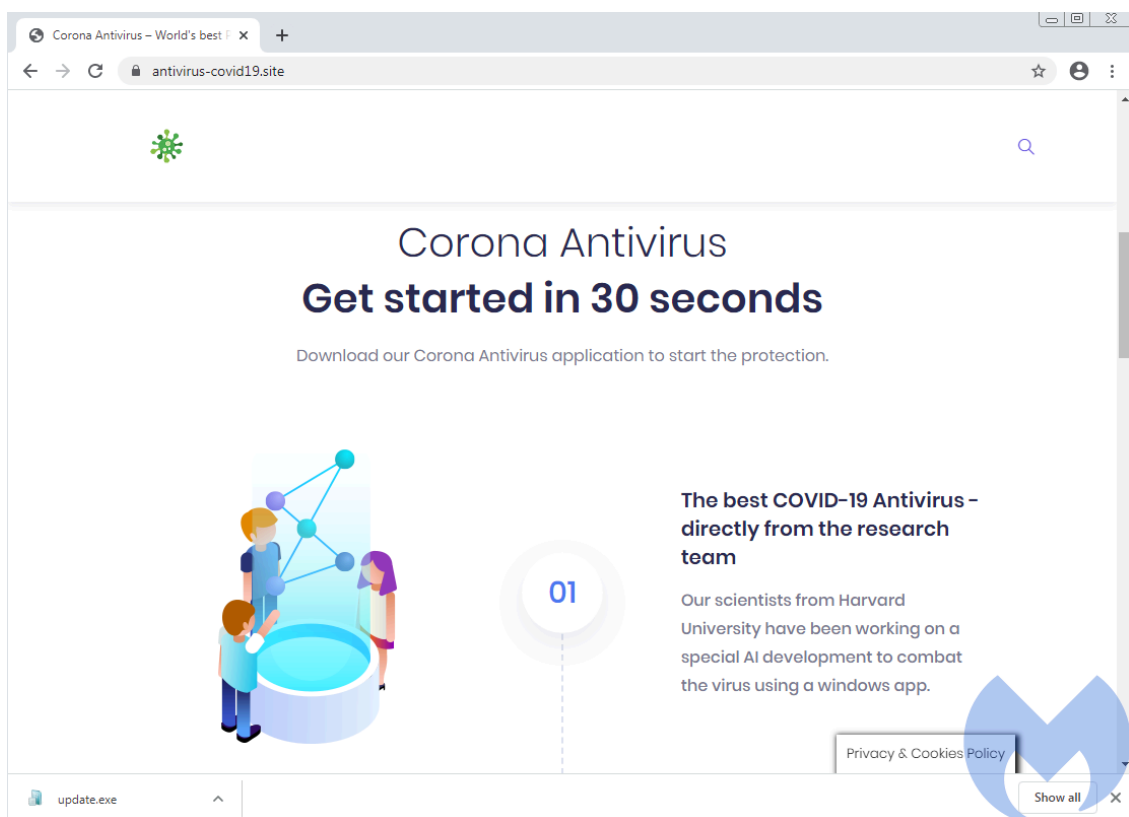
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

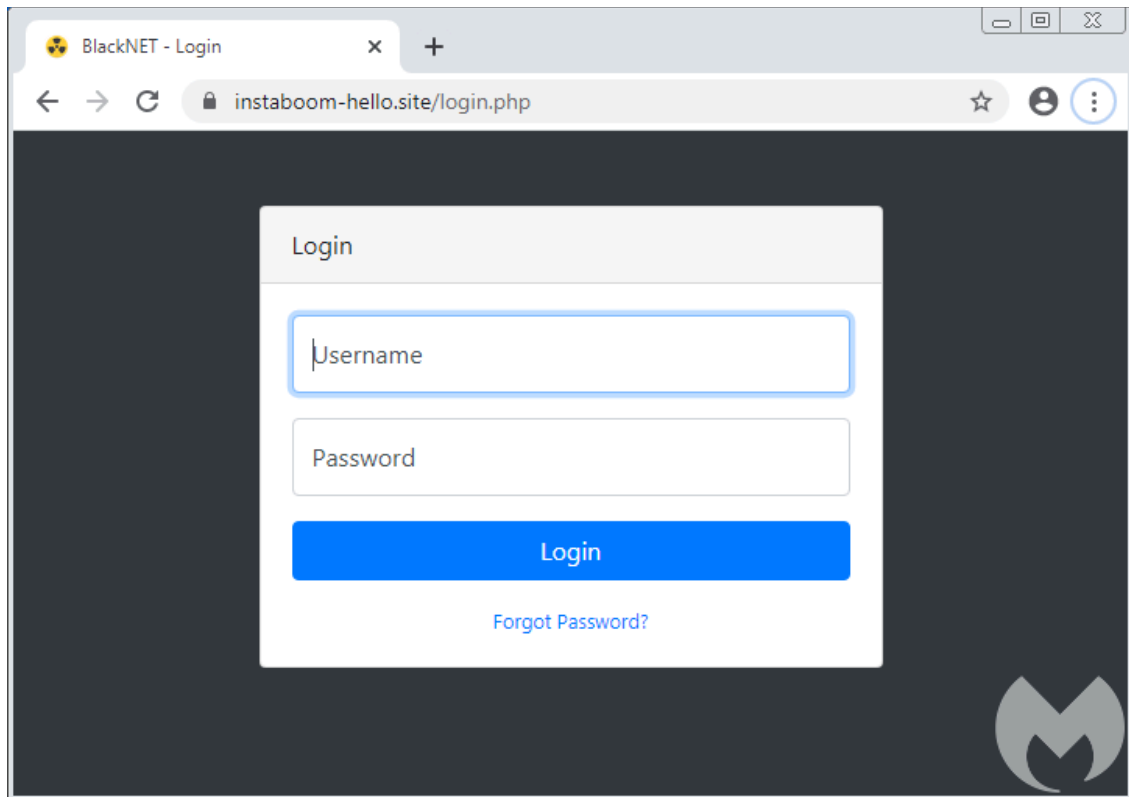


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

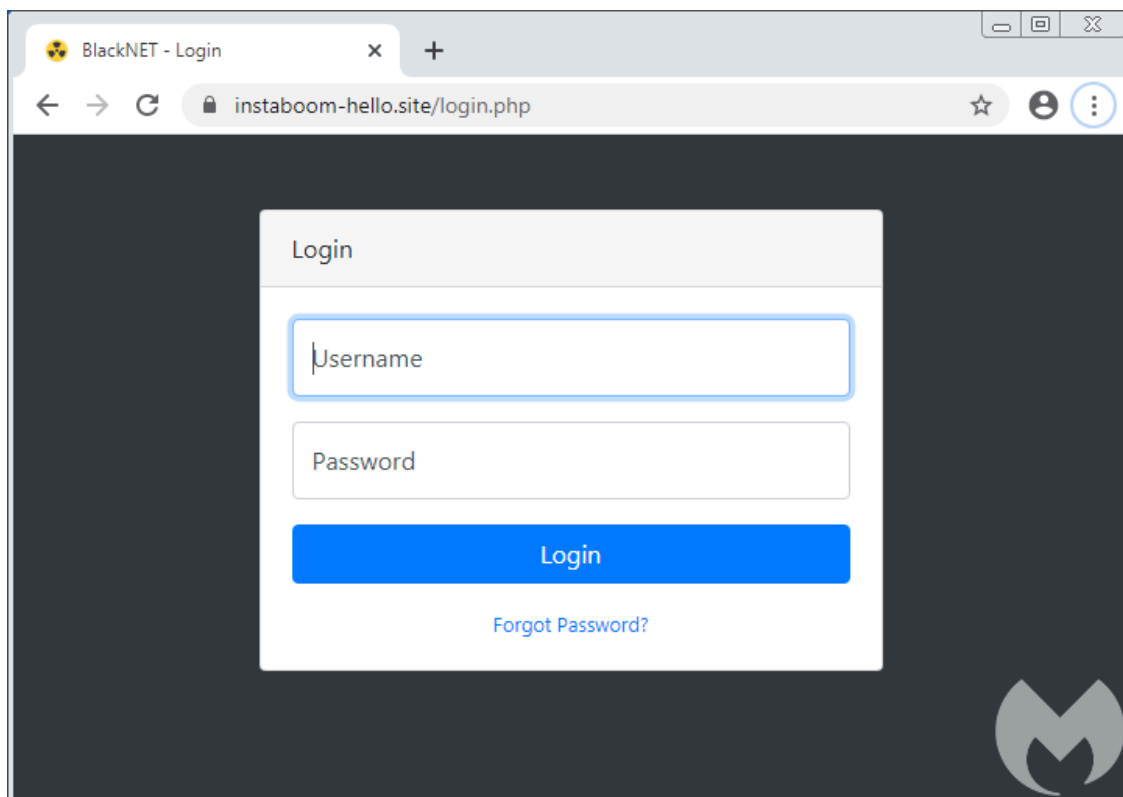
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

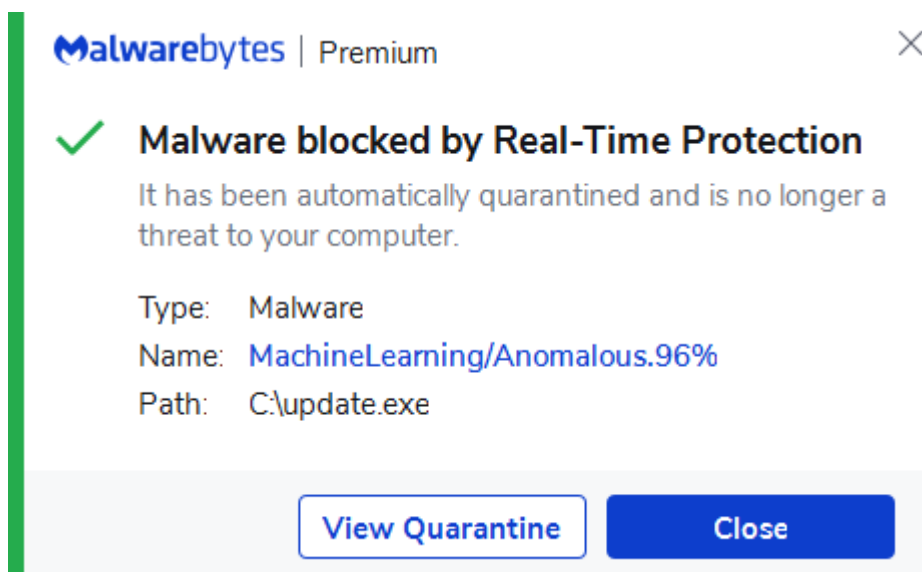
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

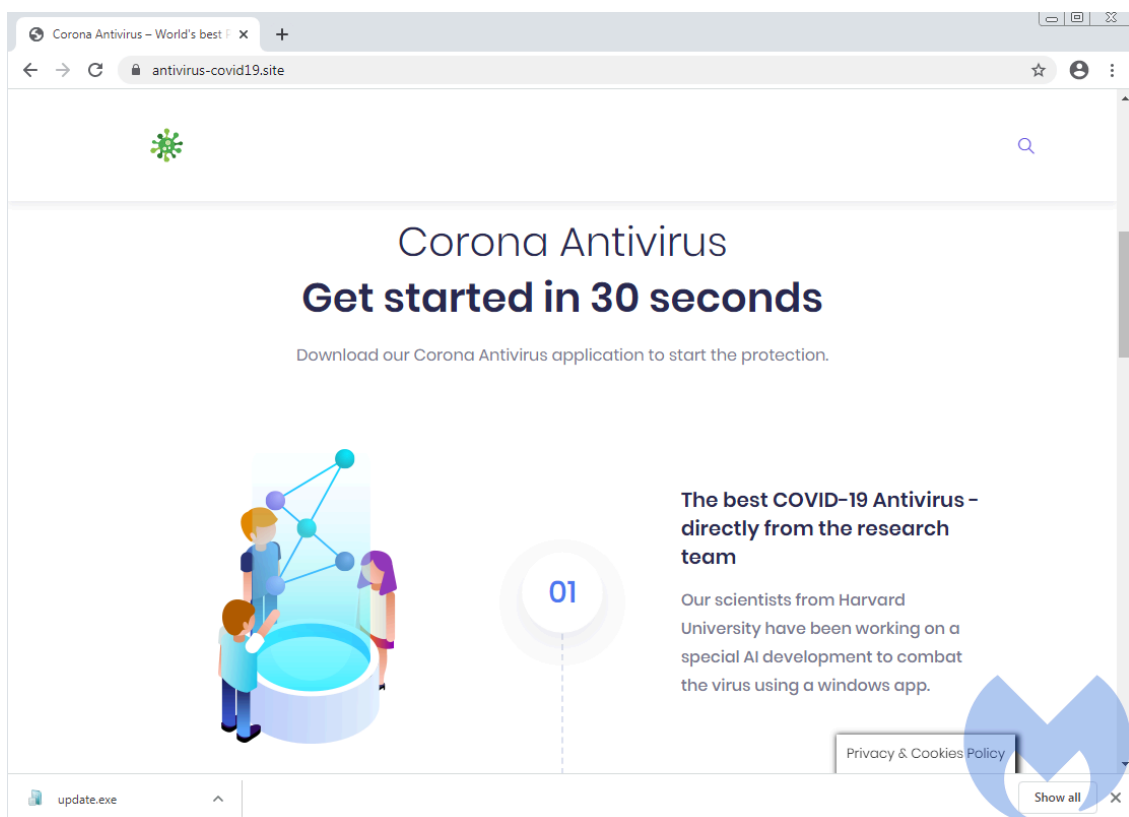
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

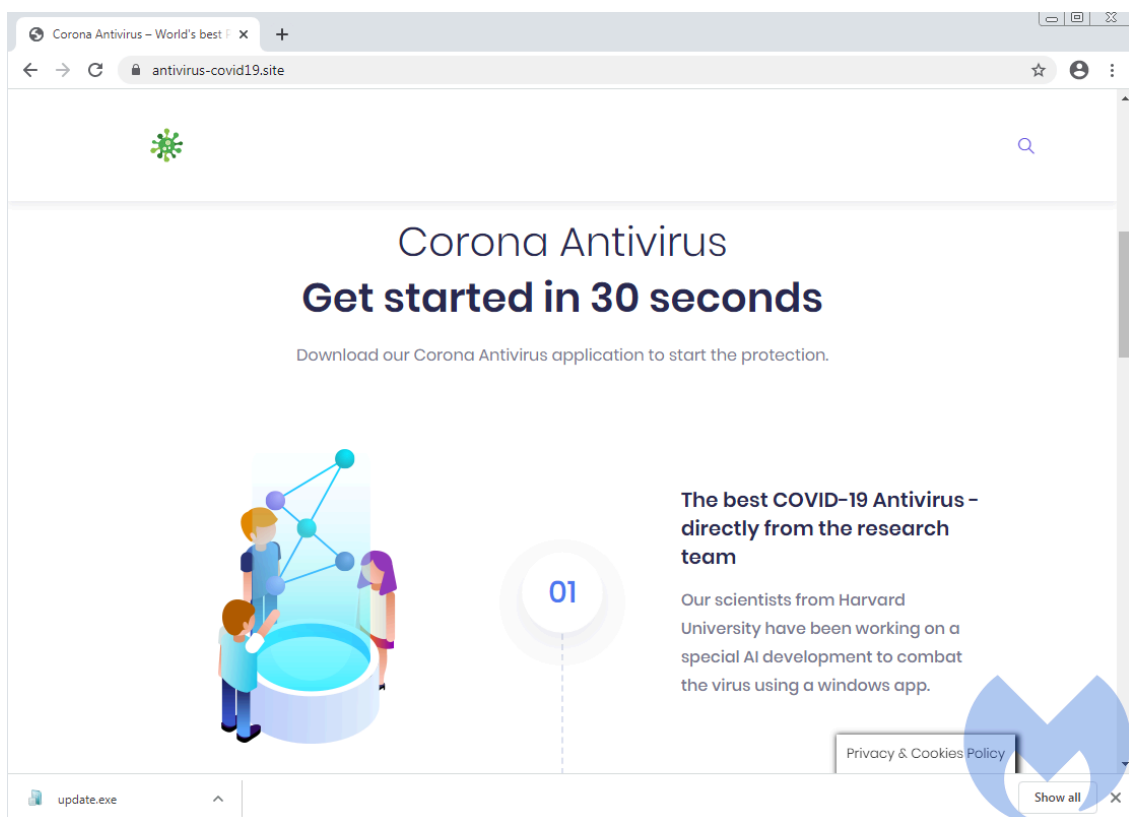
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

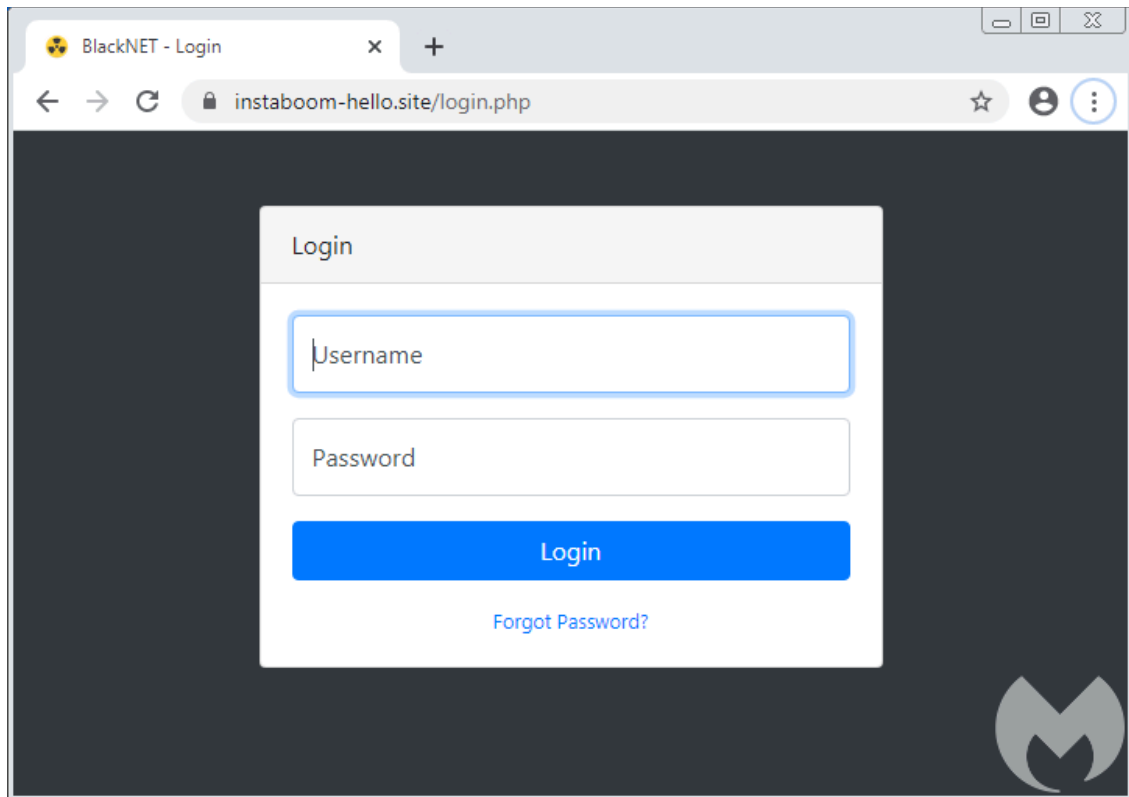


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

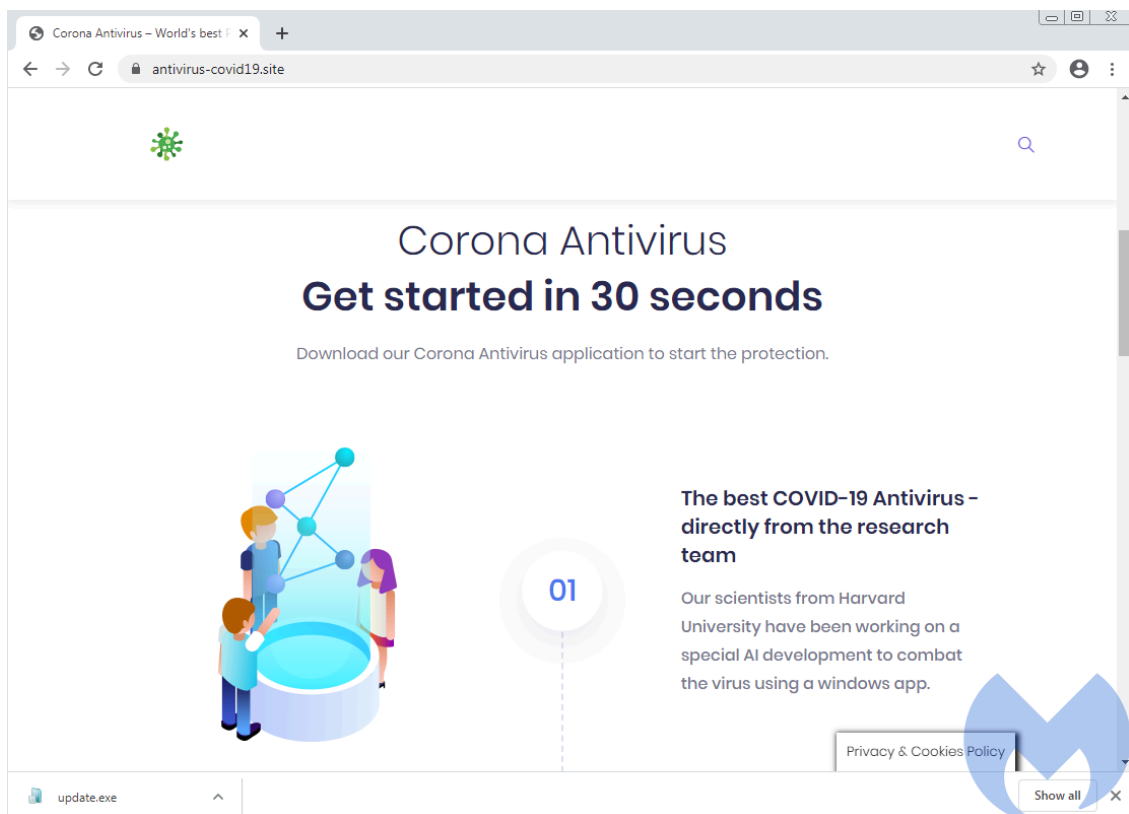
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

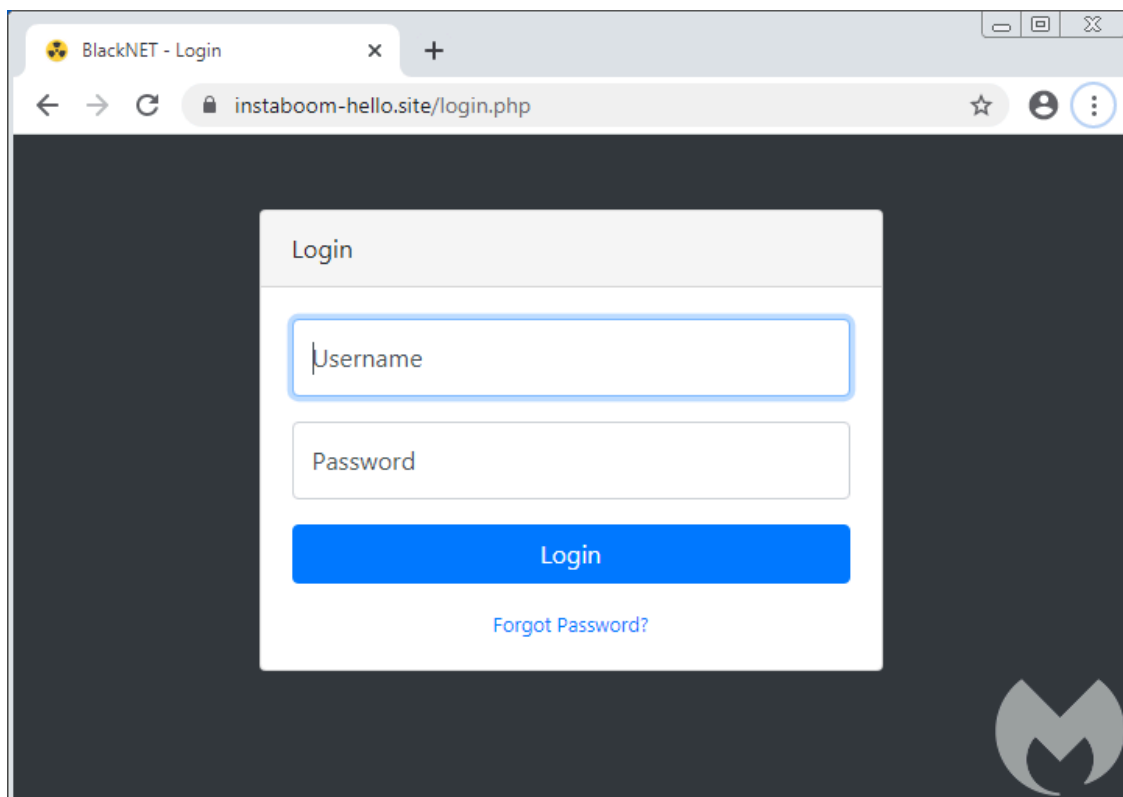


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

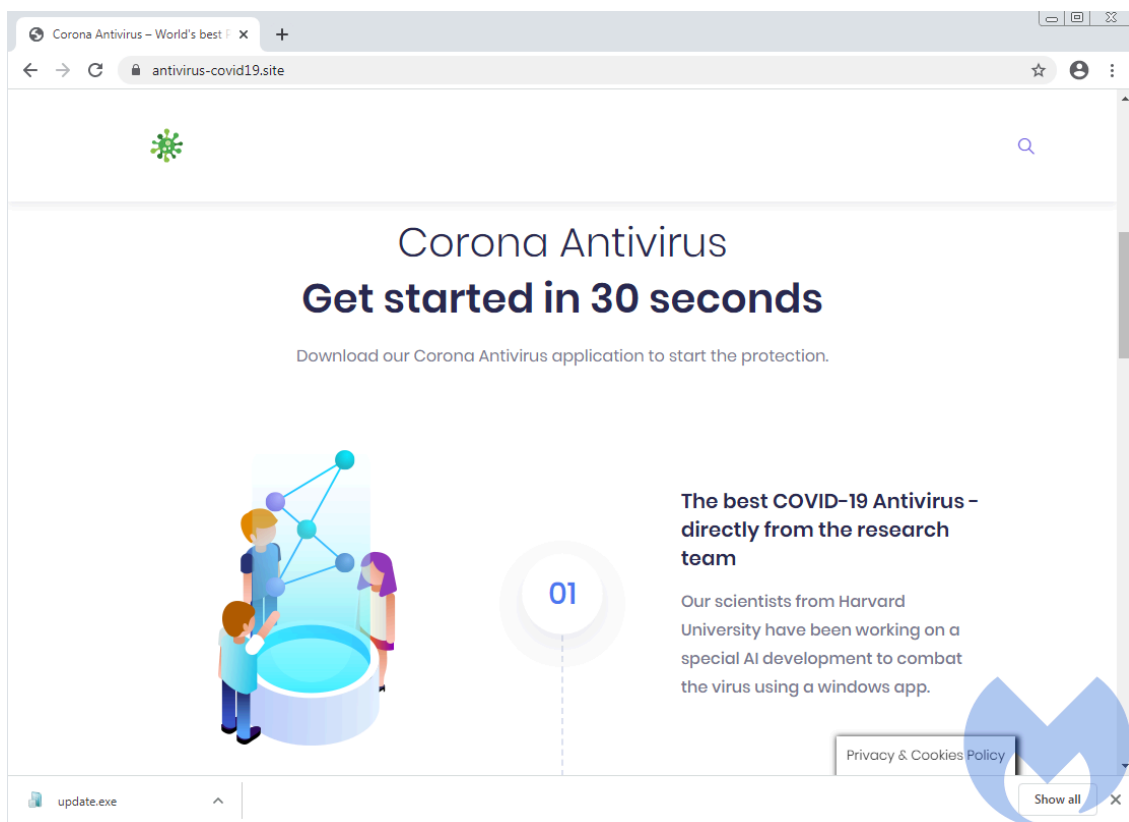
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

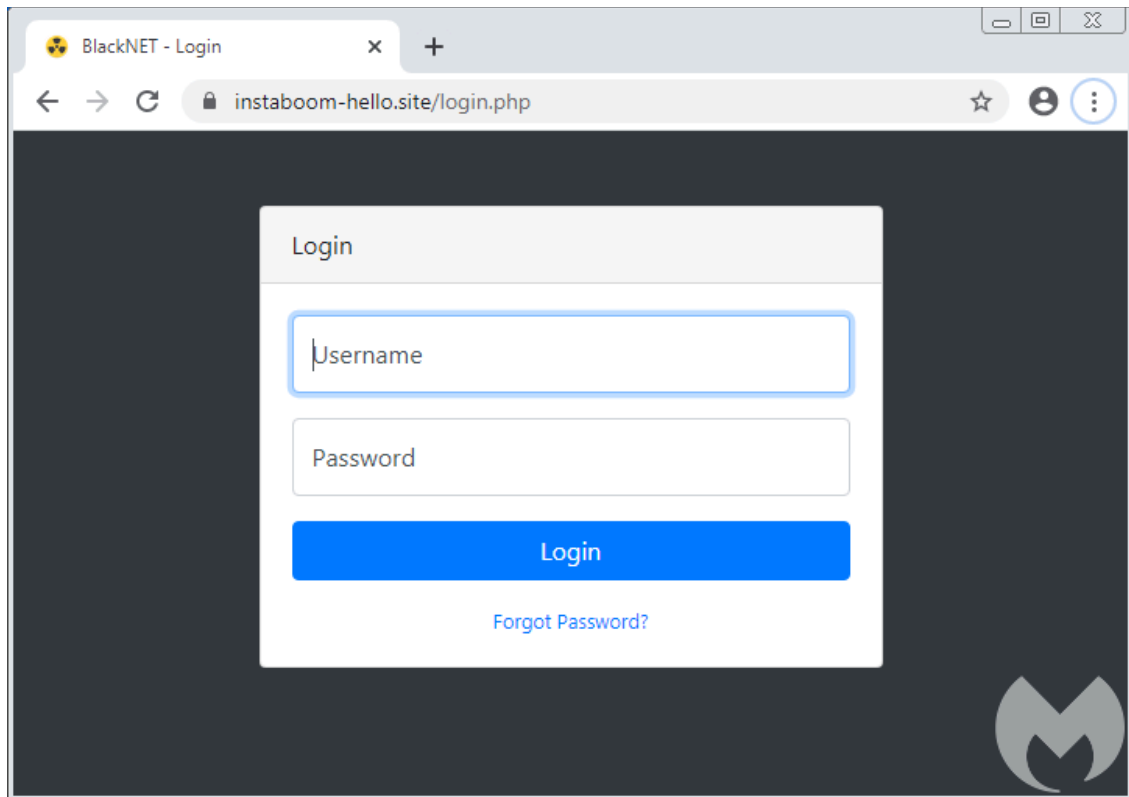


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

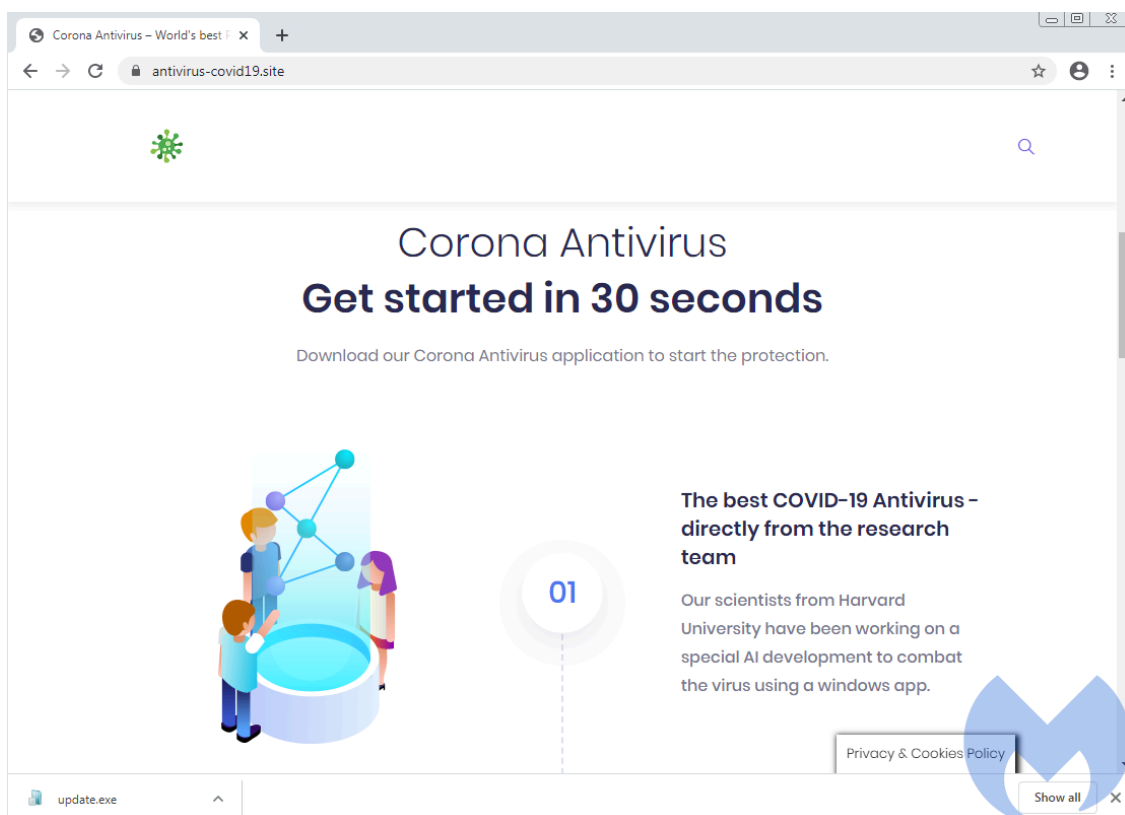
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

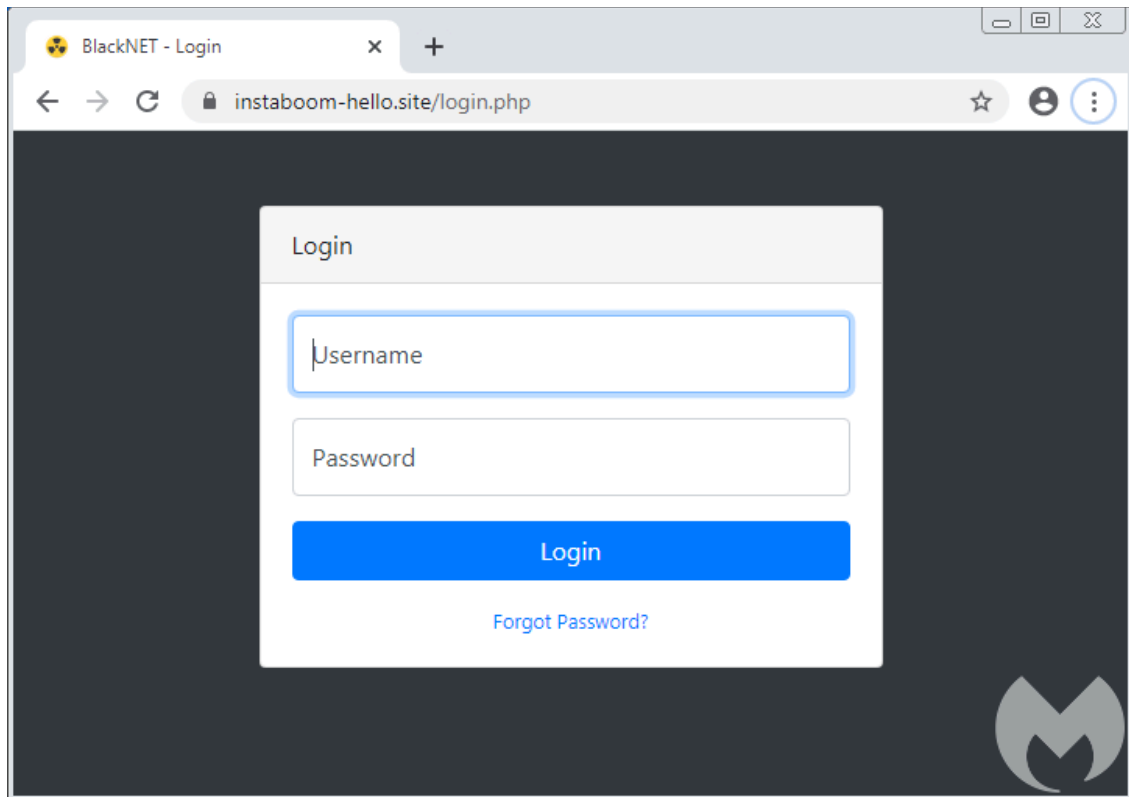


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

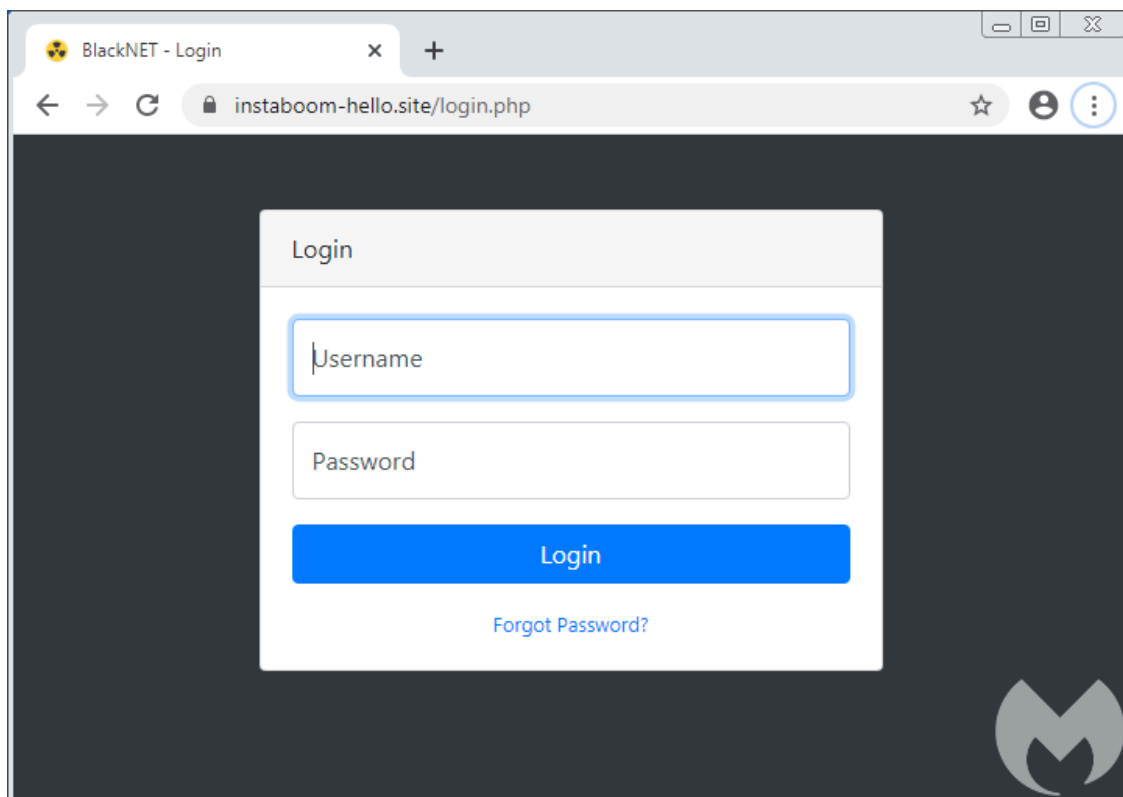
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

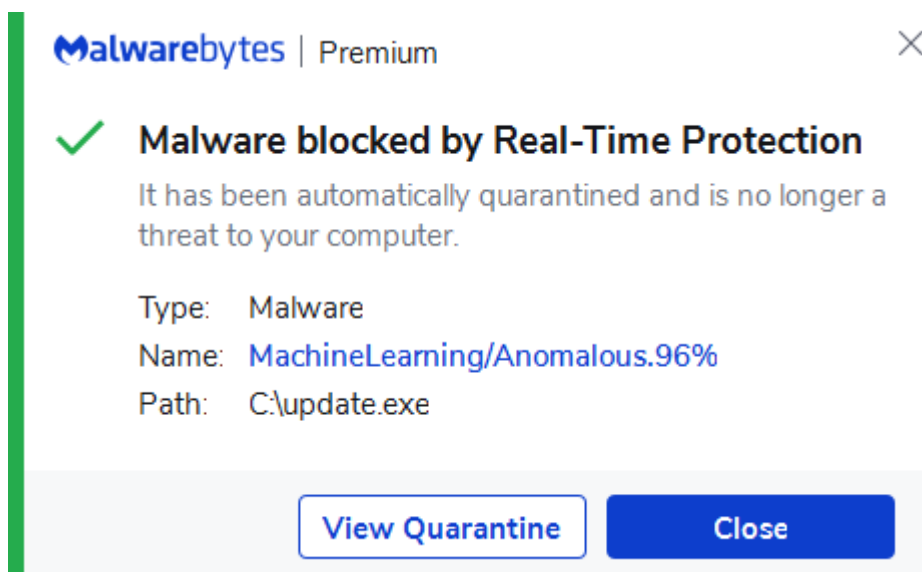
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

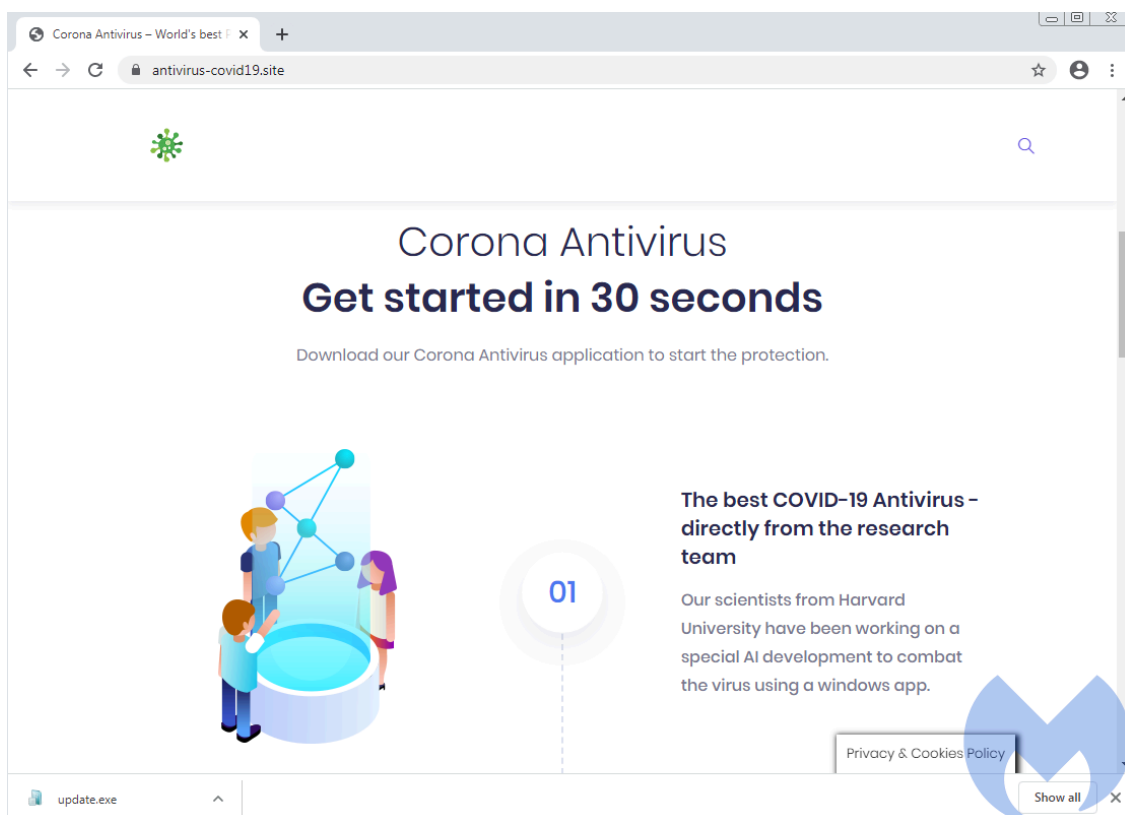
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

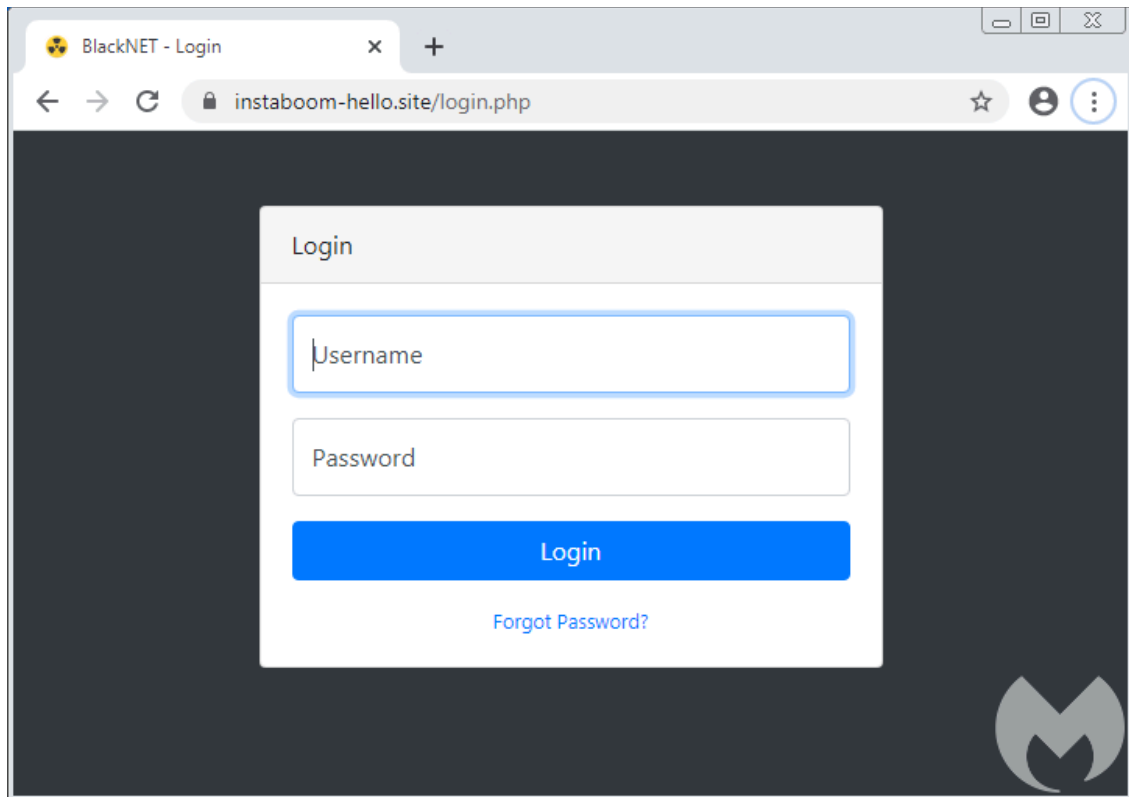


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

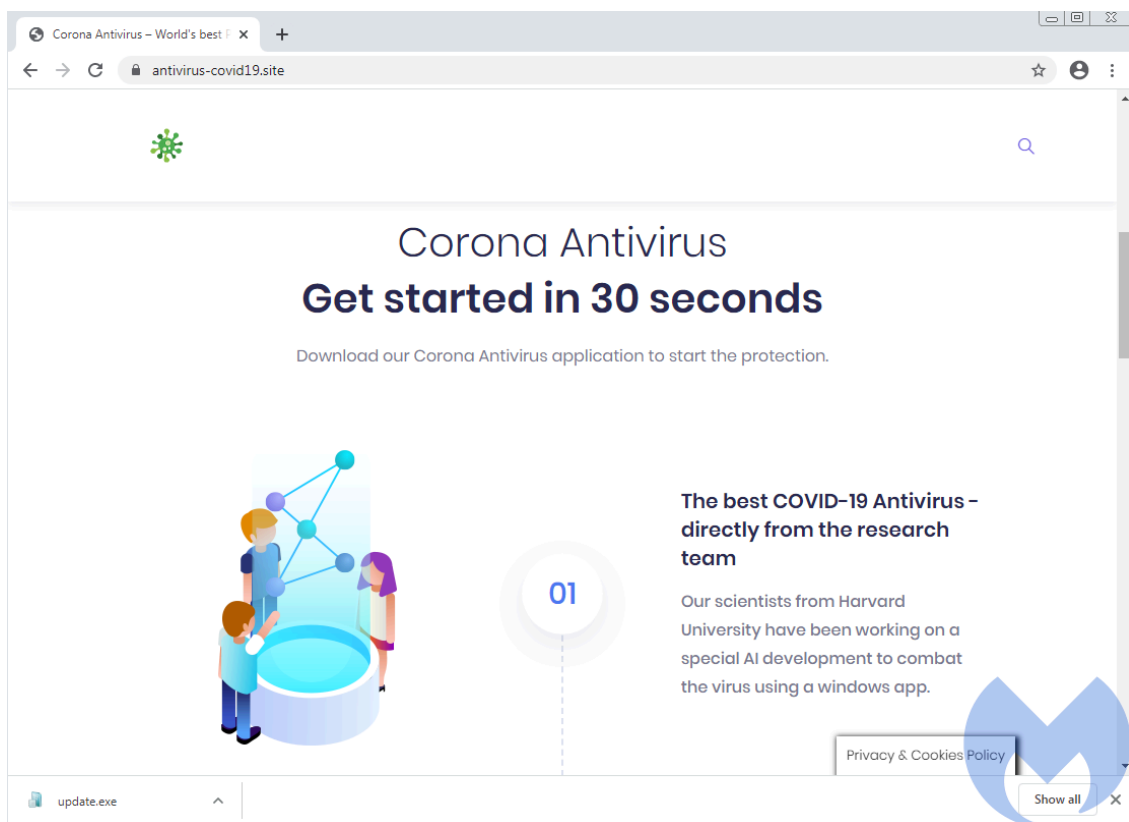
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

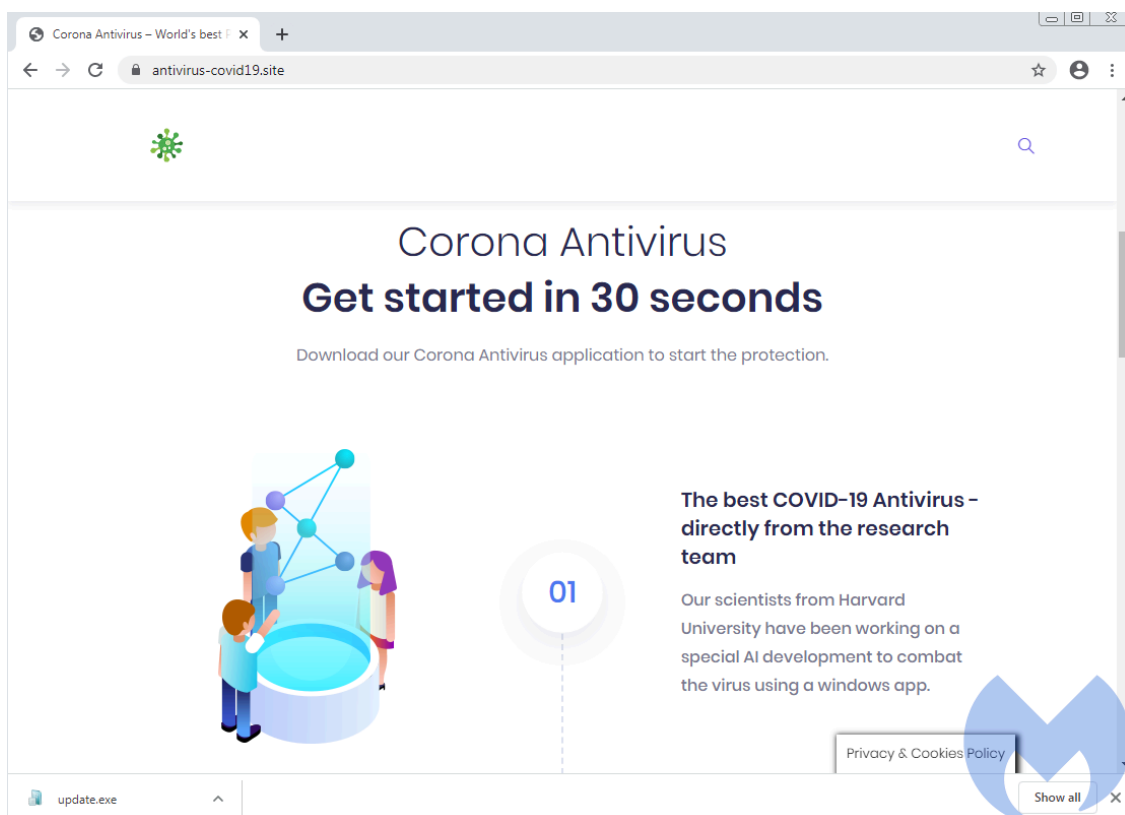
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

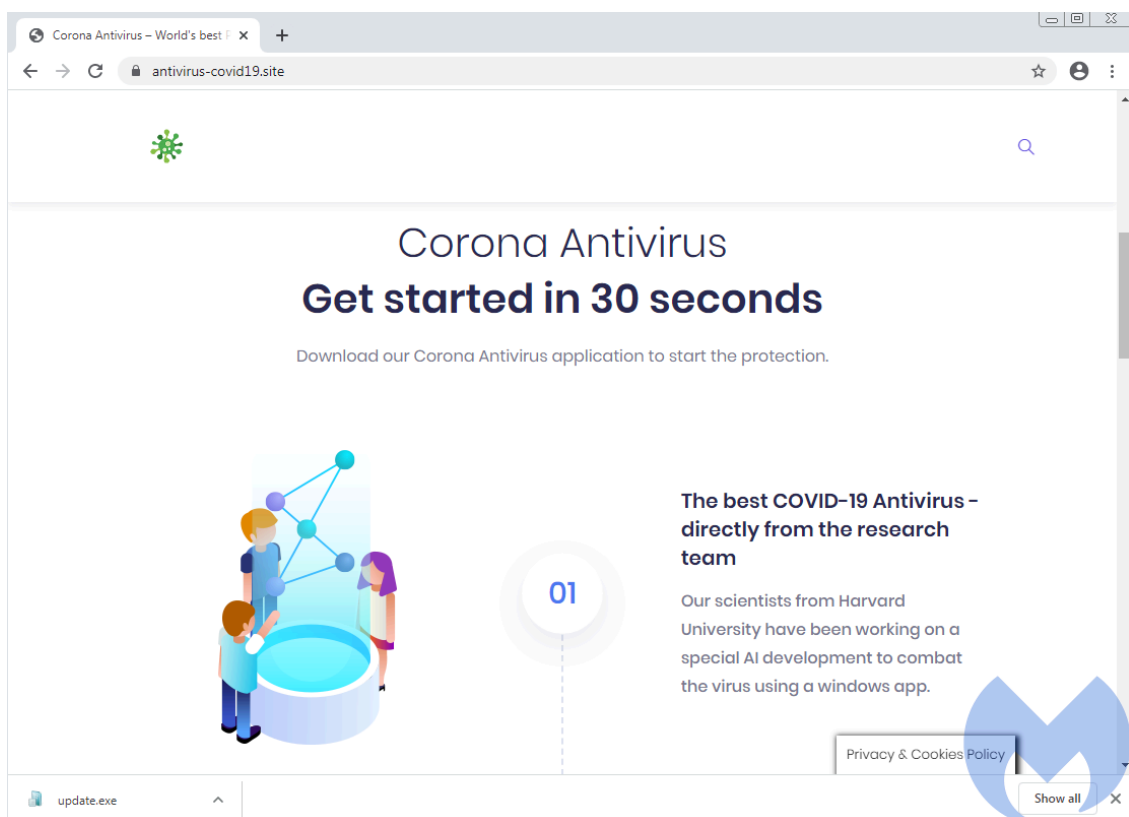
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

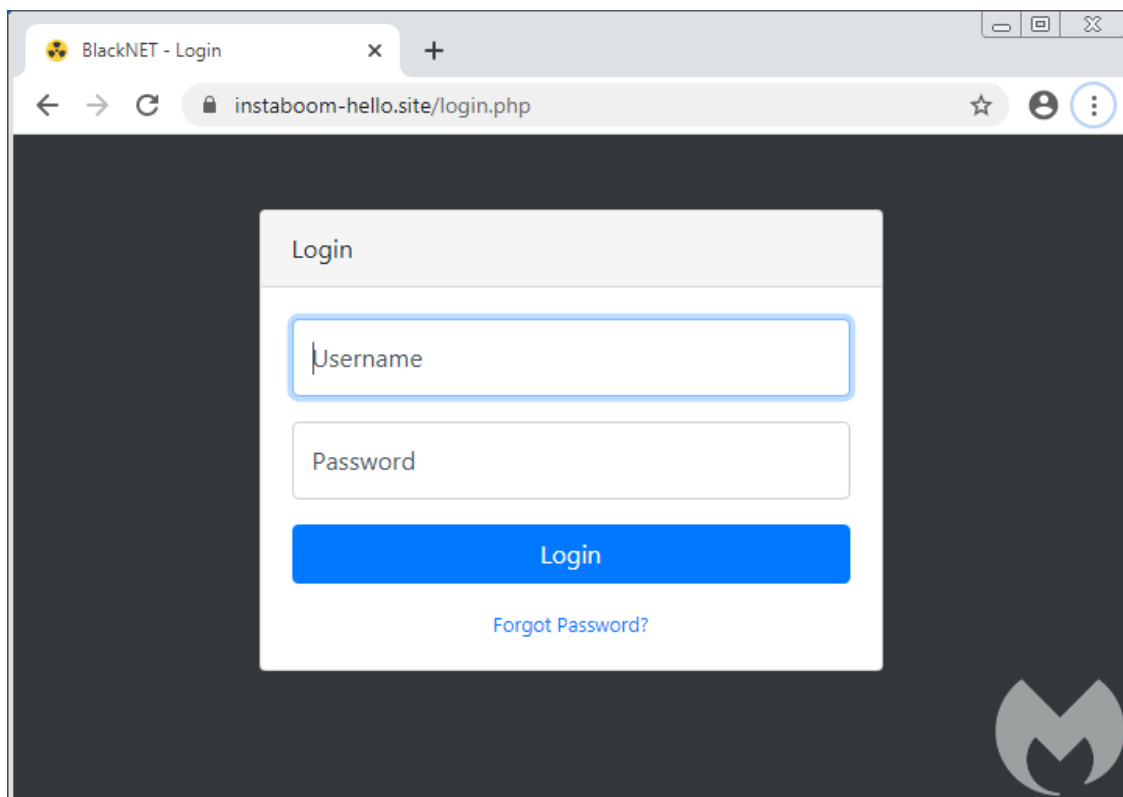


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

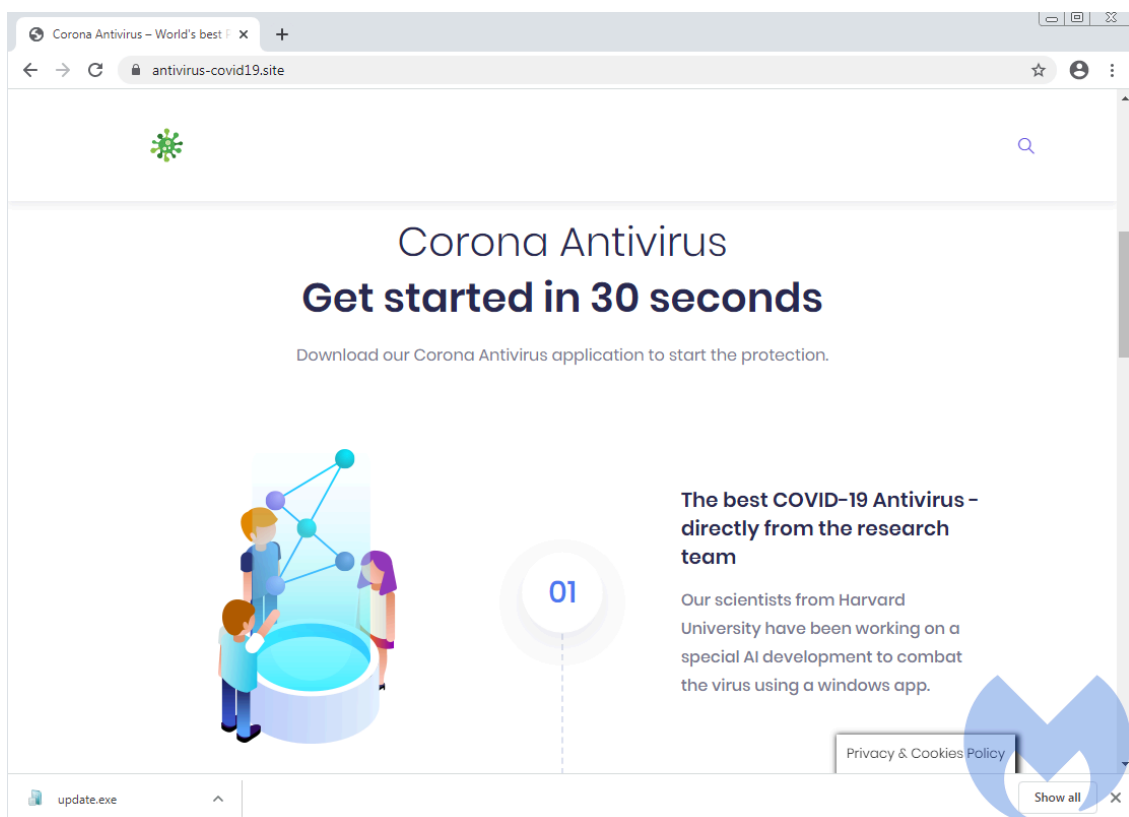
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four colored cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the list is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom, there's a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

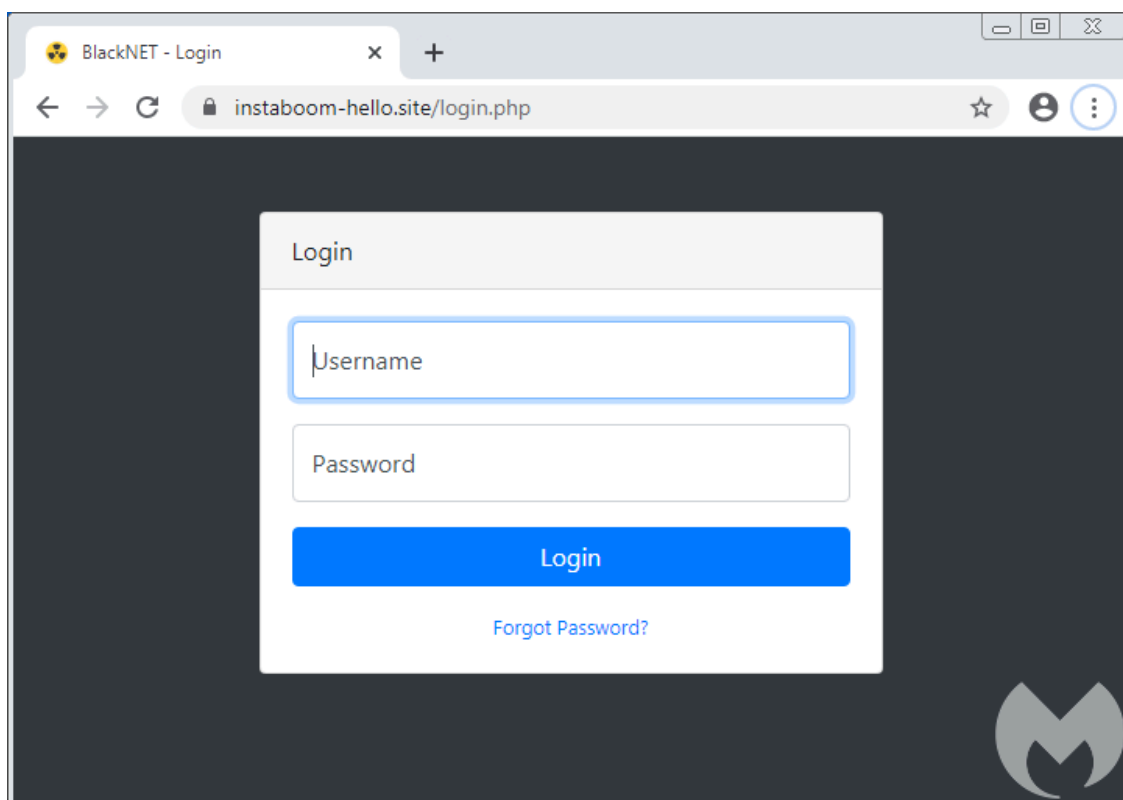
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

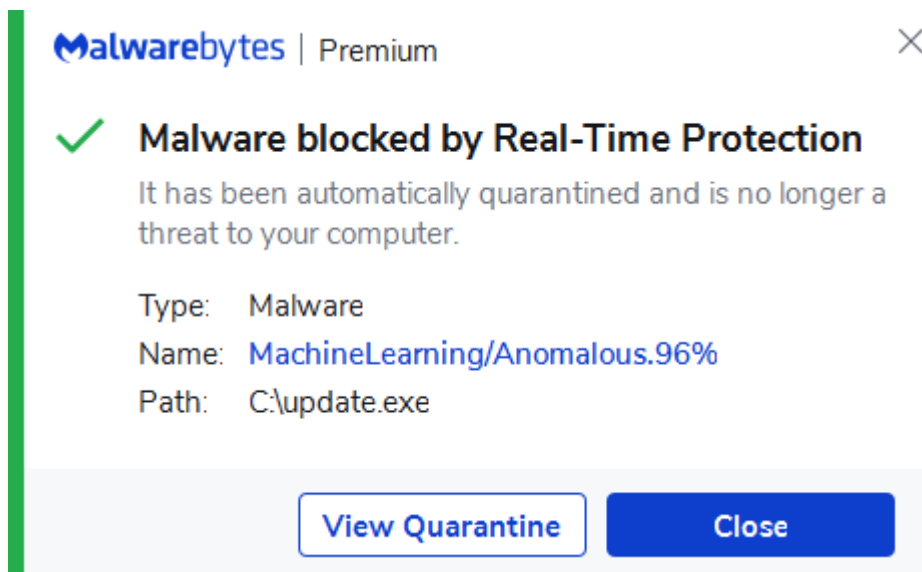
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

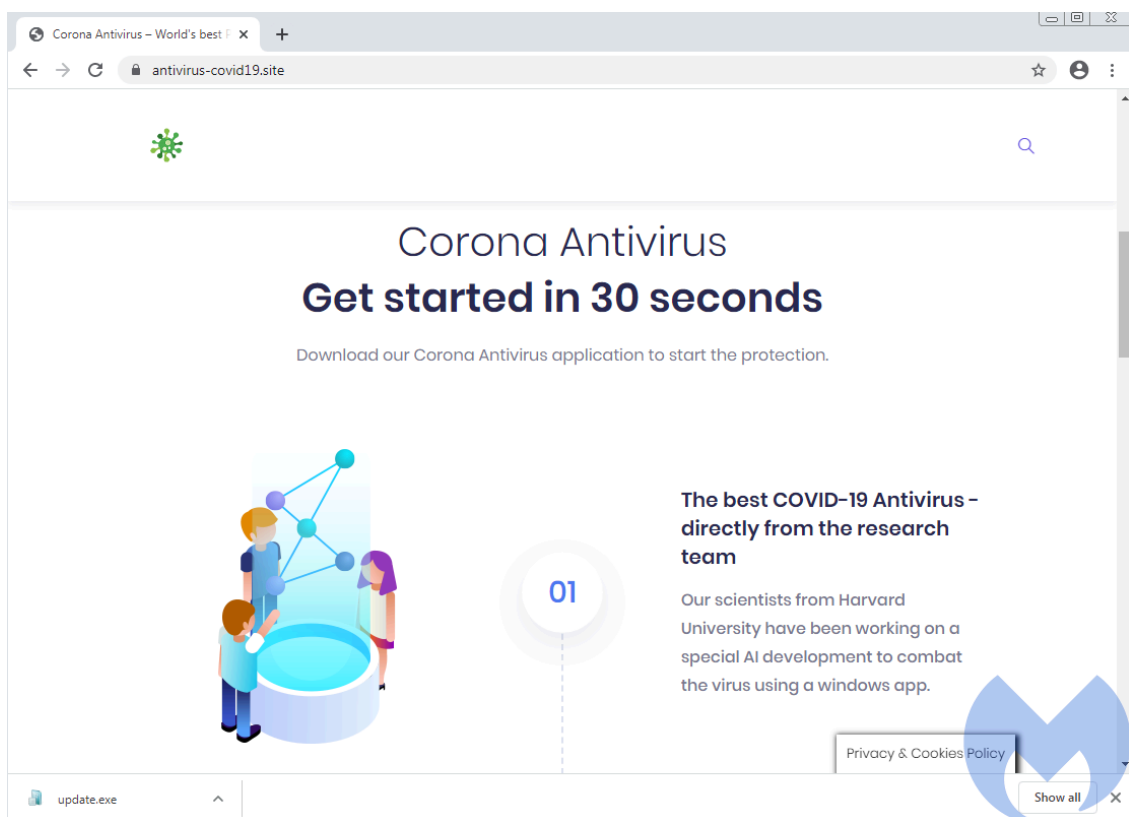
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

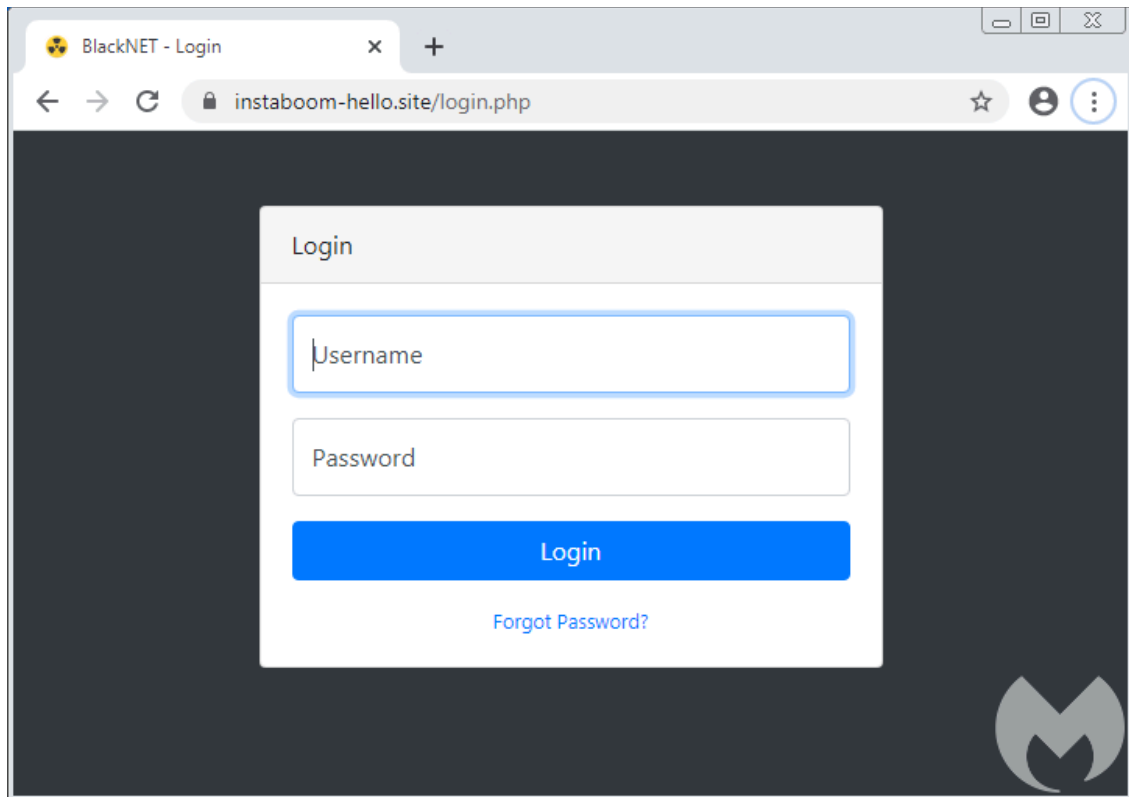


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue dot indicating a client location. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. The window has a green vertical bar on the left and a close button (X) in the top right corner. The main content area has a green checkmark icon and the text: "Malware blocked by Real-Time Protection". Below this, it says: "It has been automatically quarantined and is no longer a threat to your computer." The notification also displays the following information: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

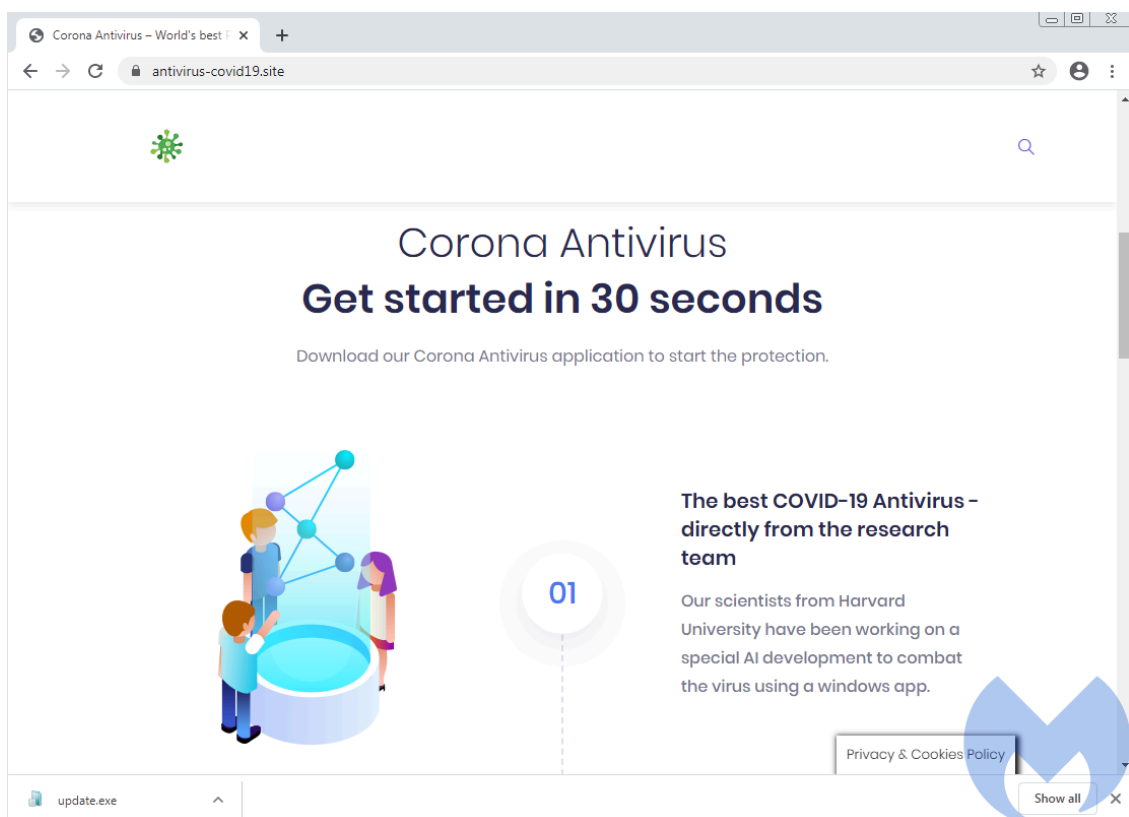
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

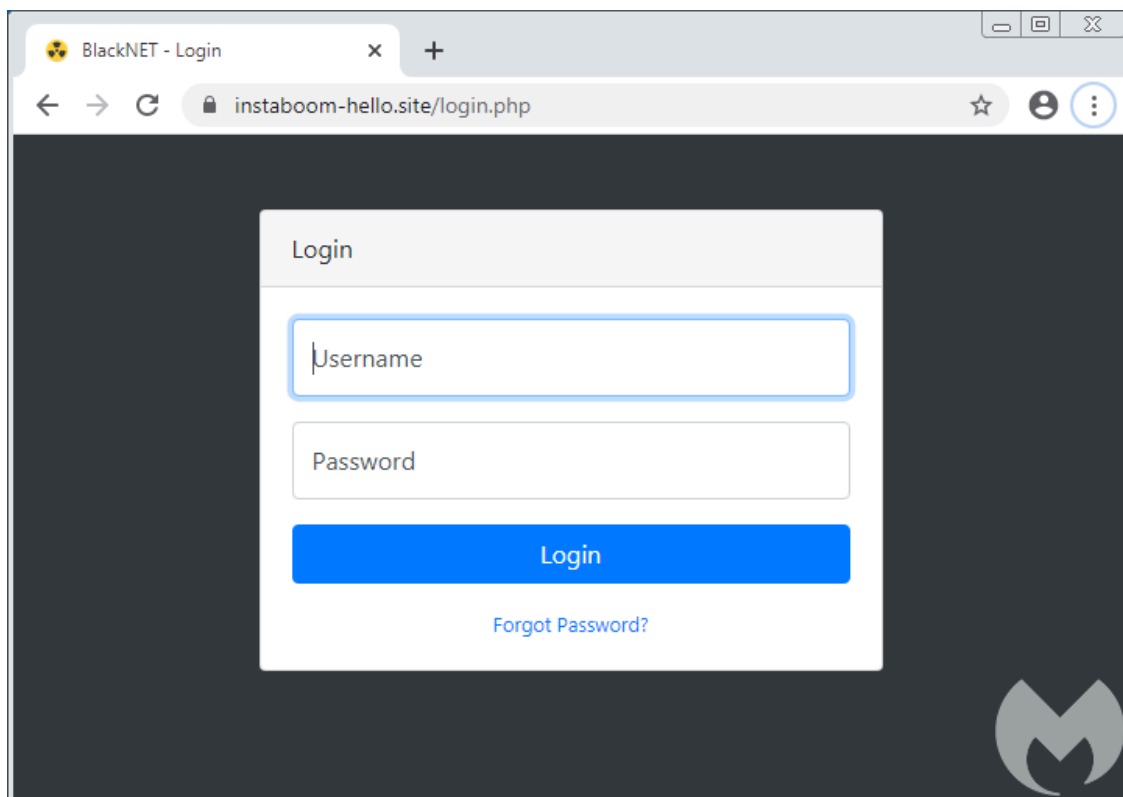


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

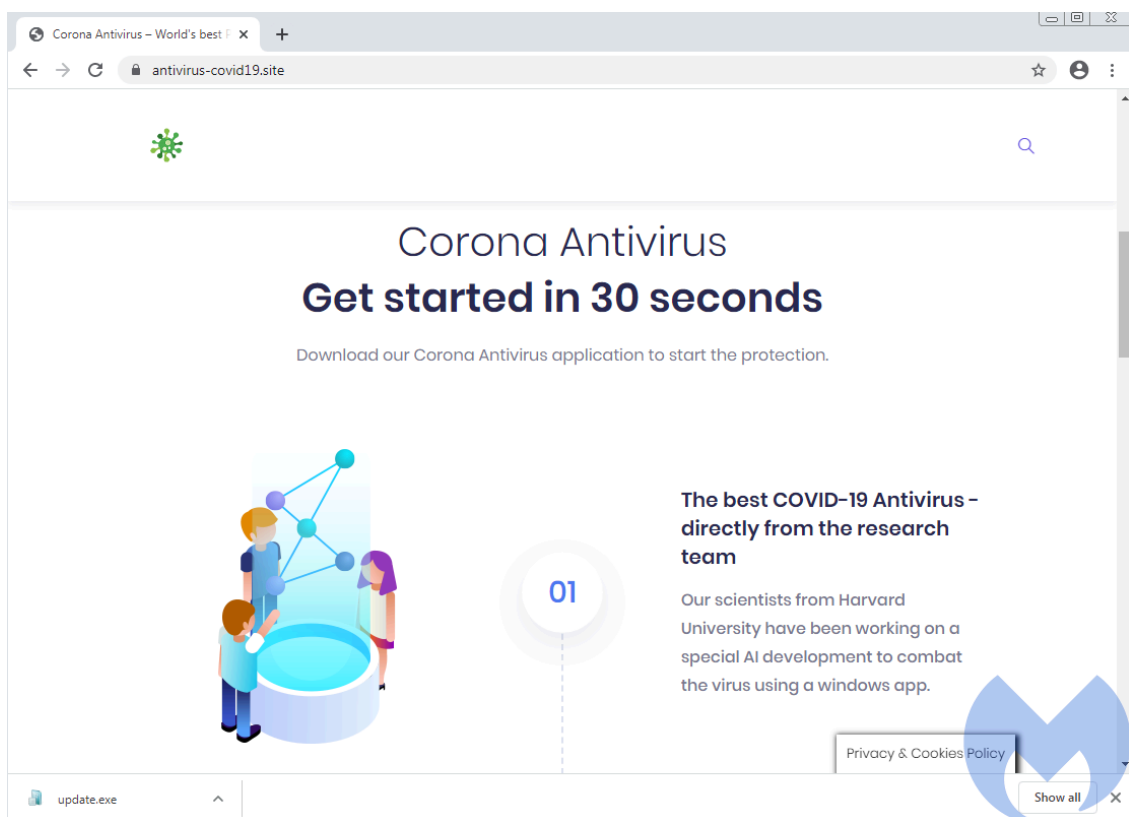
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

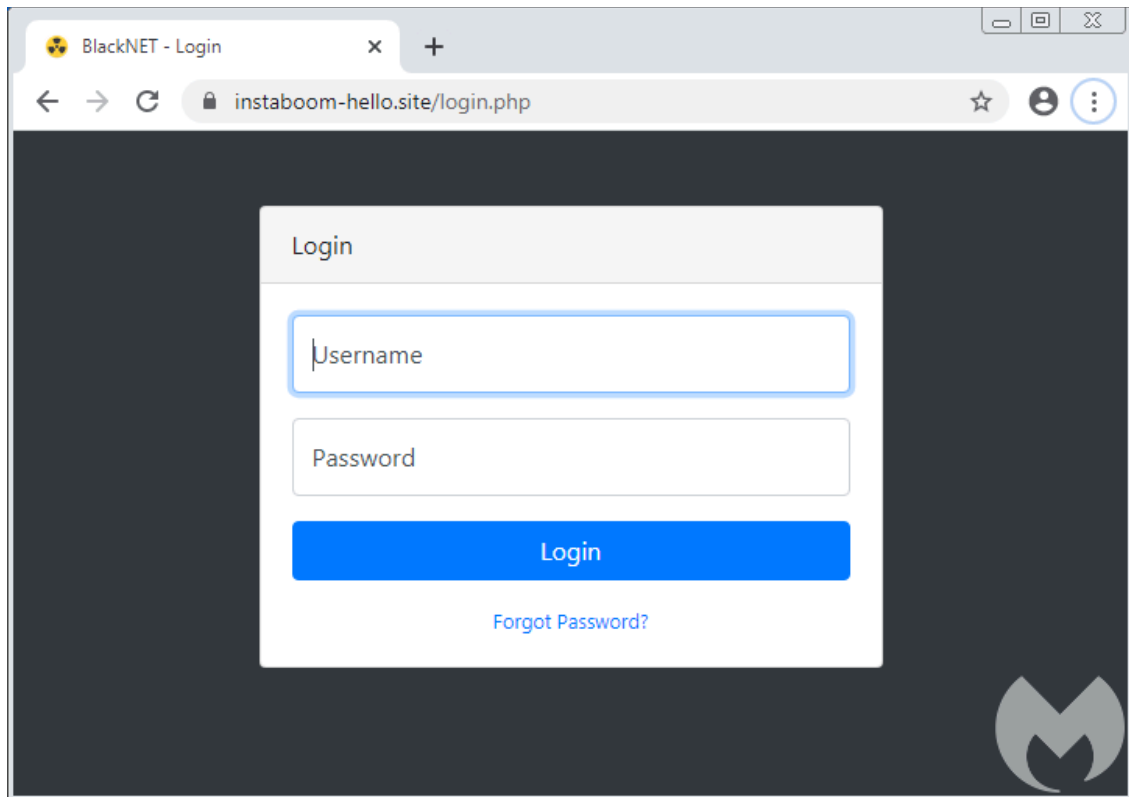


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

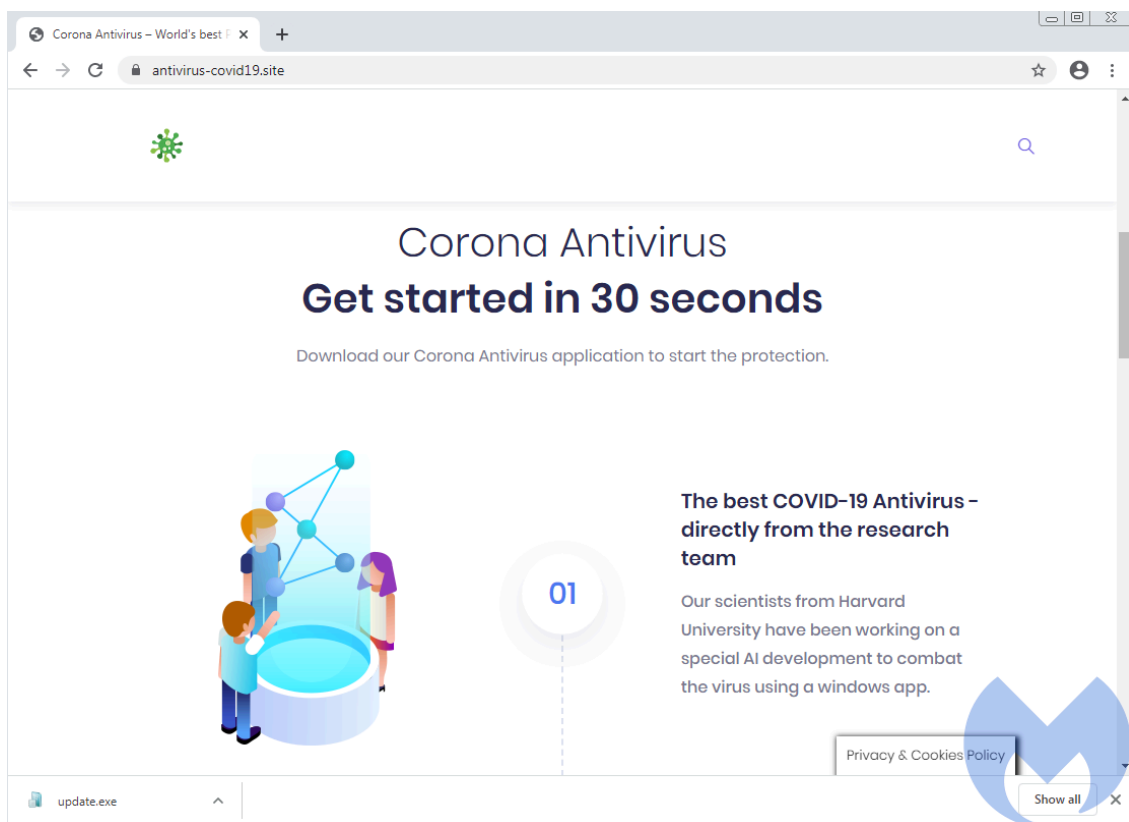
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

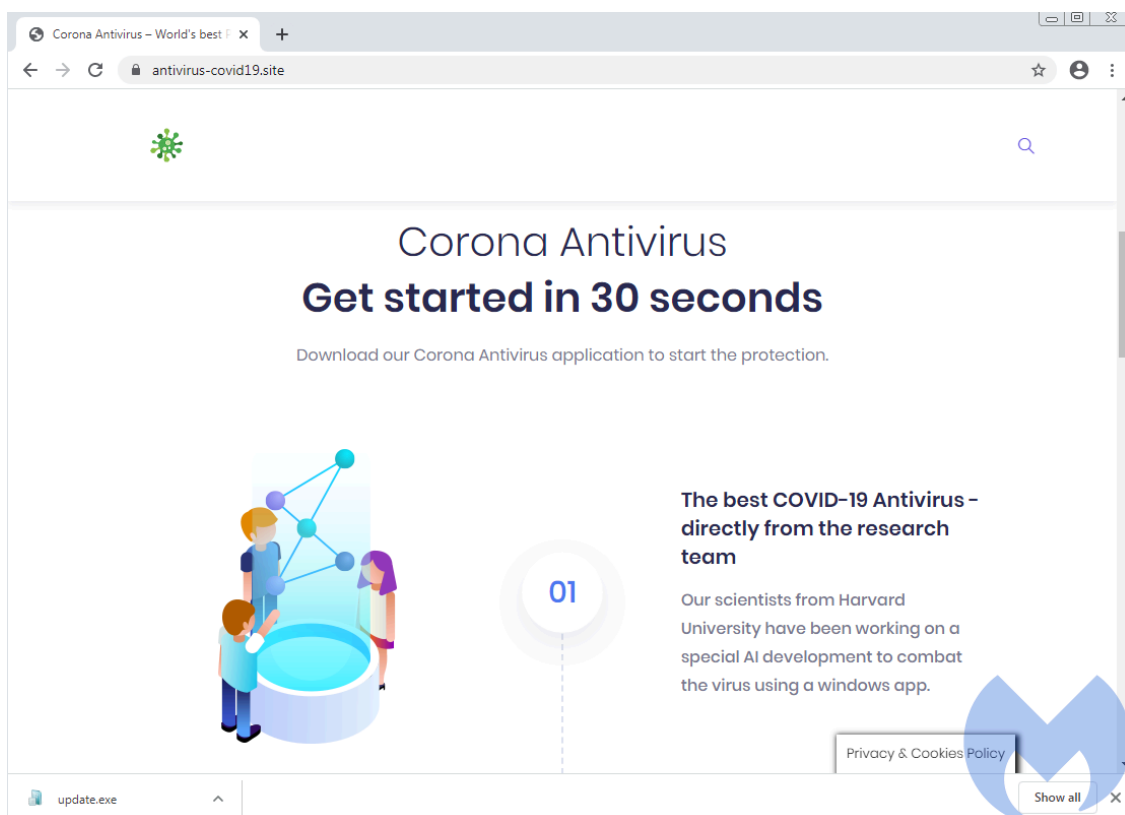
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

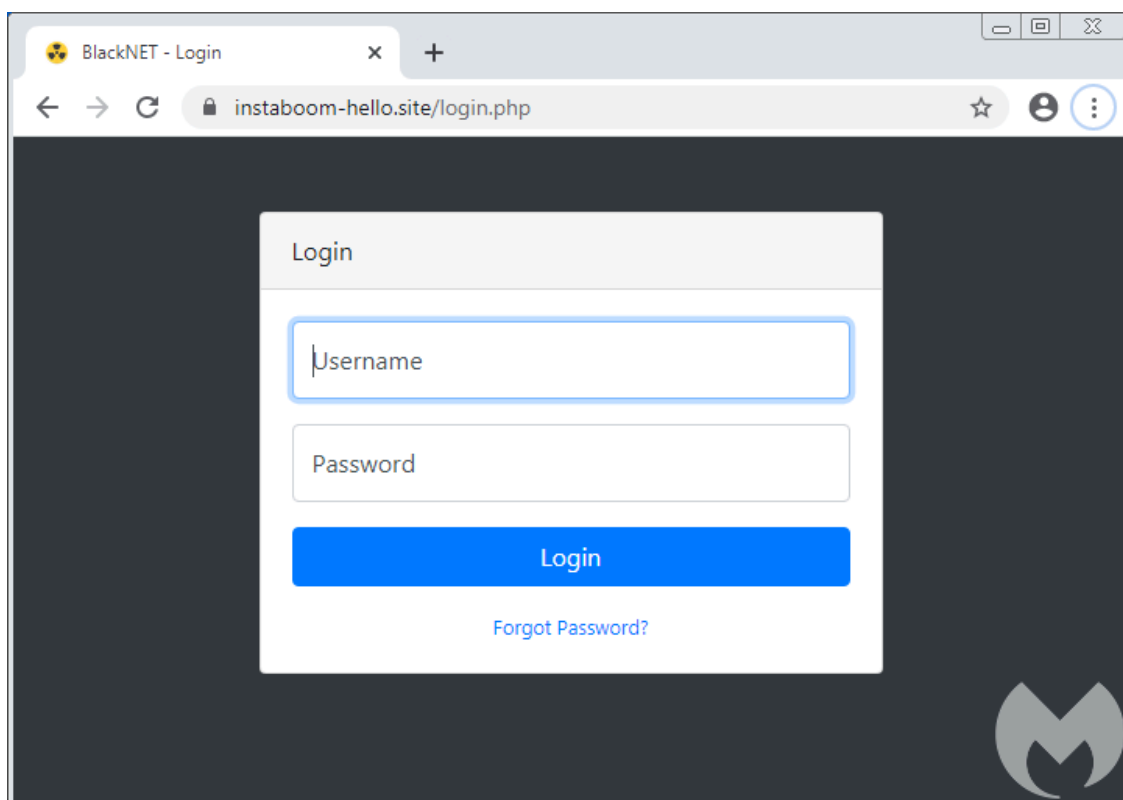
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

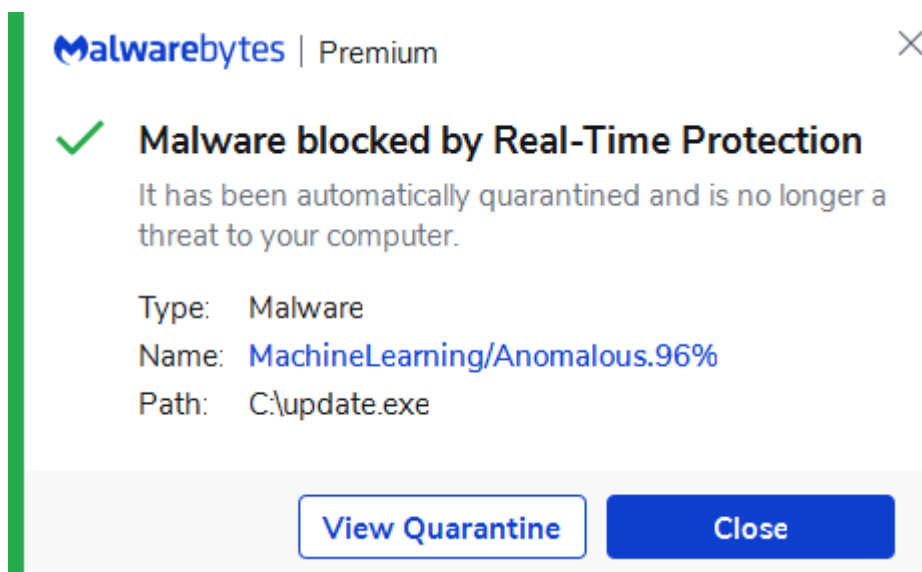
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. Below the table are 'Previous' and 'Next' buttons. To the left of the table is a 'Commands Center' with a 'Command' dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

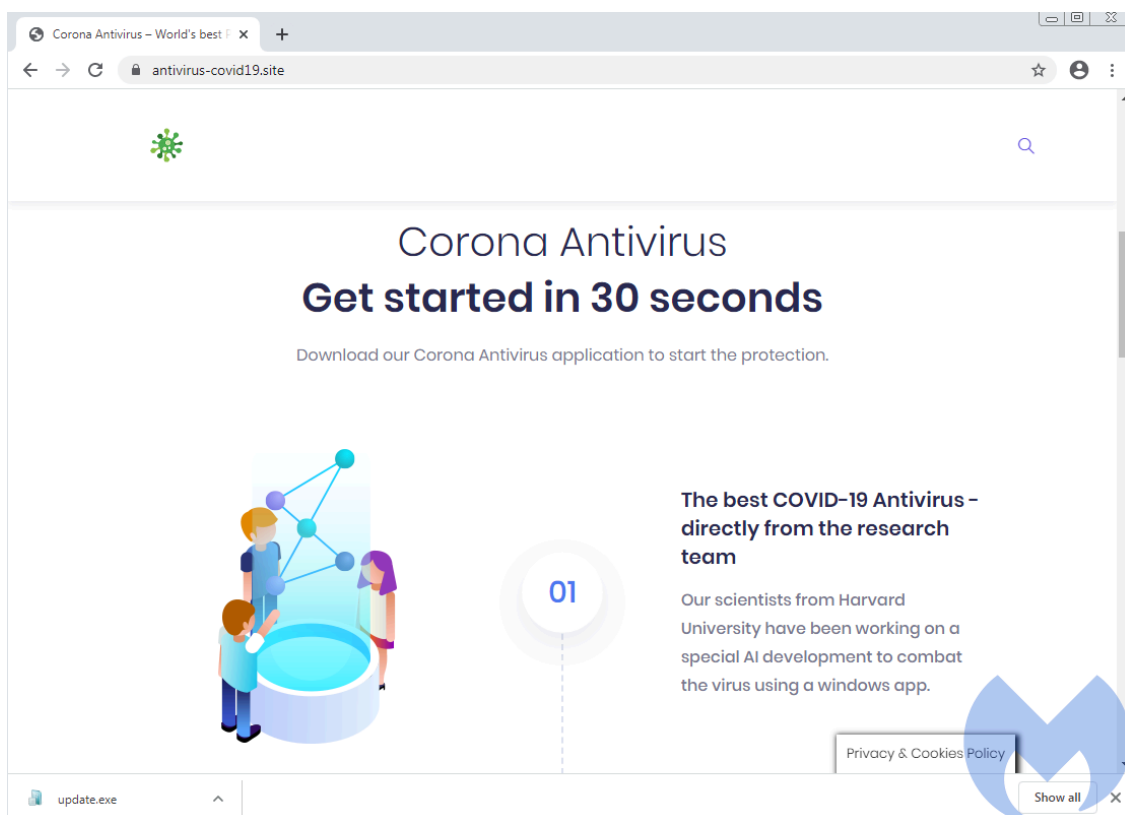
C2 panel

```
instaboom-hello[.]site
```




To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

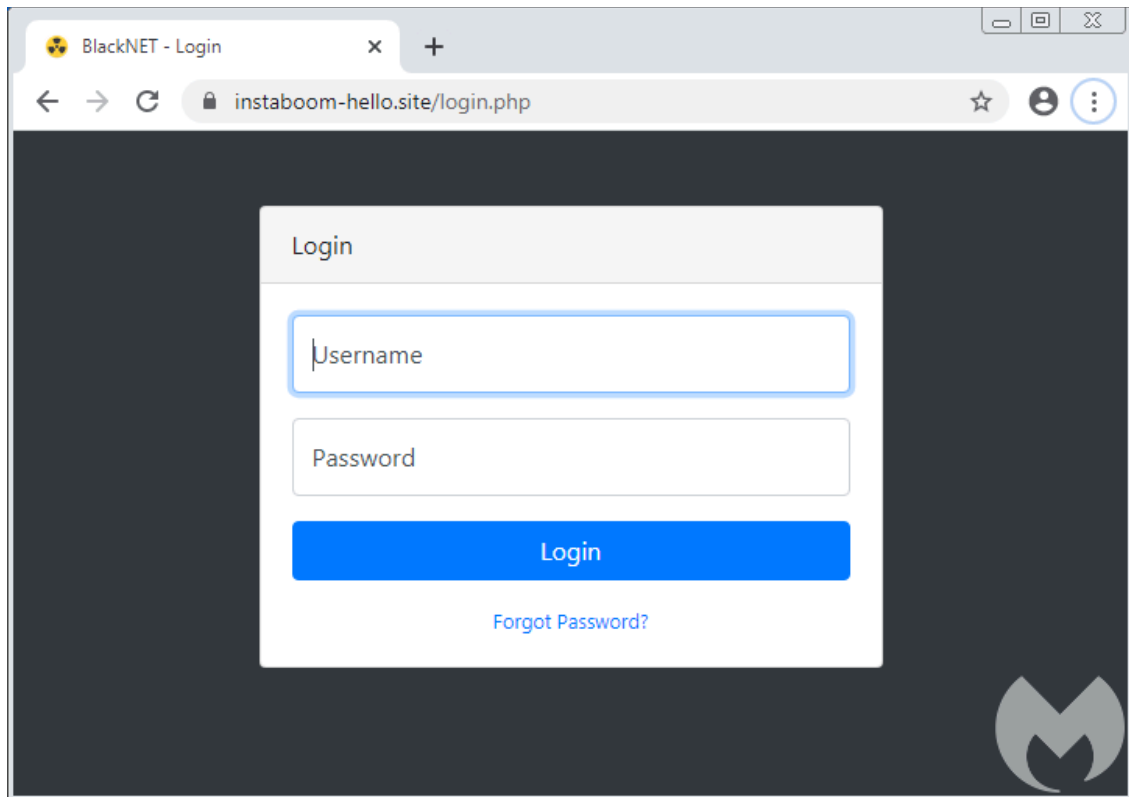


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a table header including Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table is a 'Map Visualization' showing a world map with a few blue dots. At the bottom left, there's a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

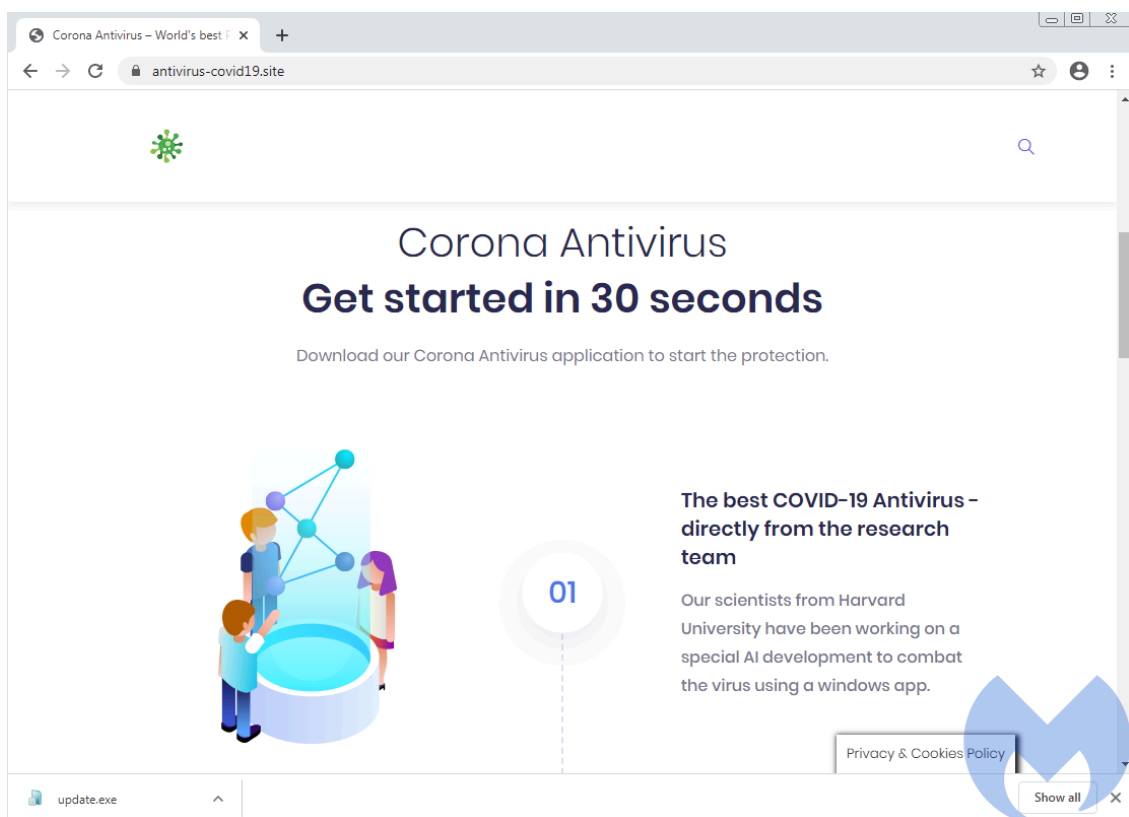
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

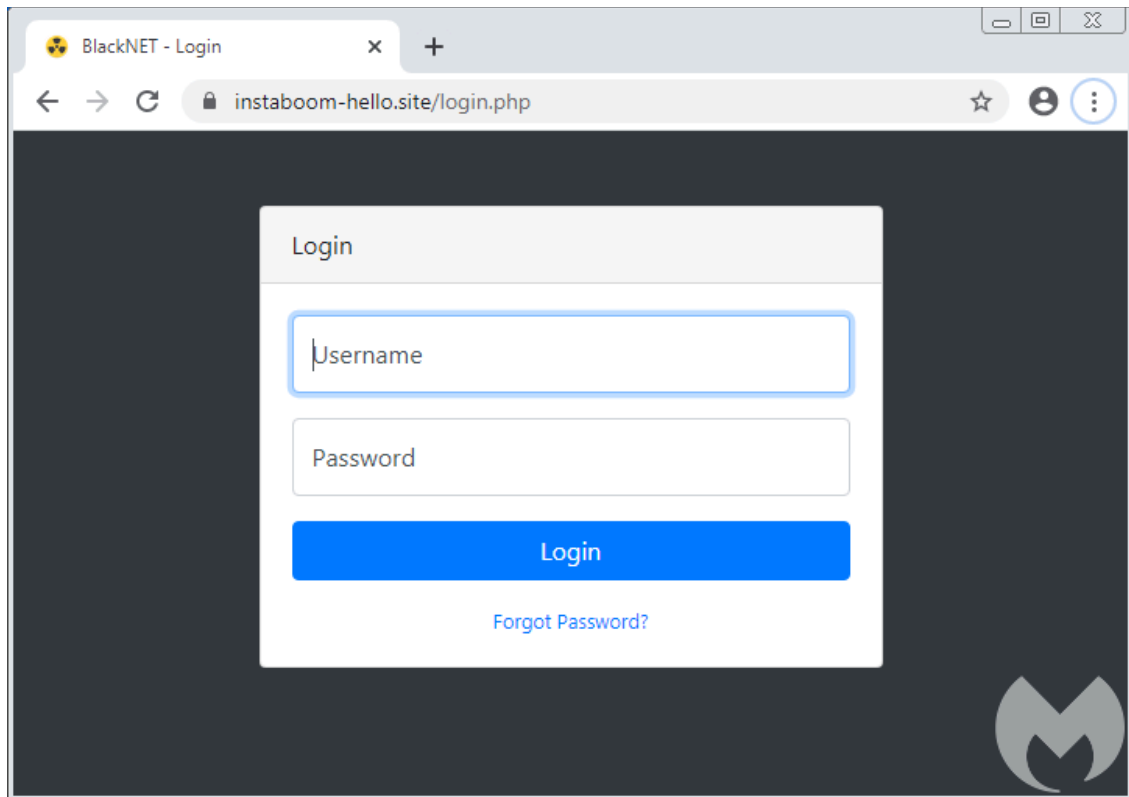


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

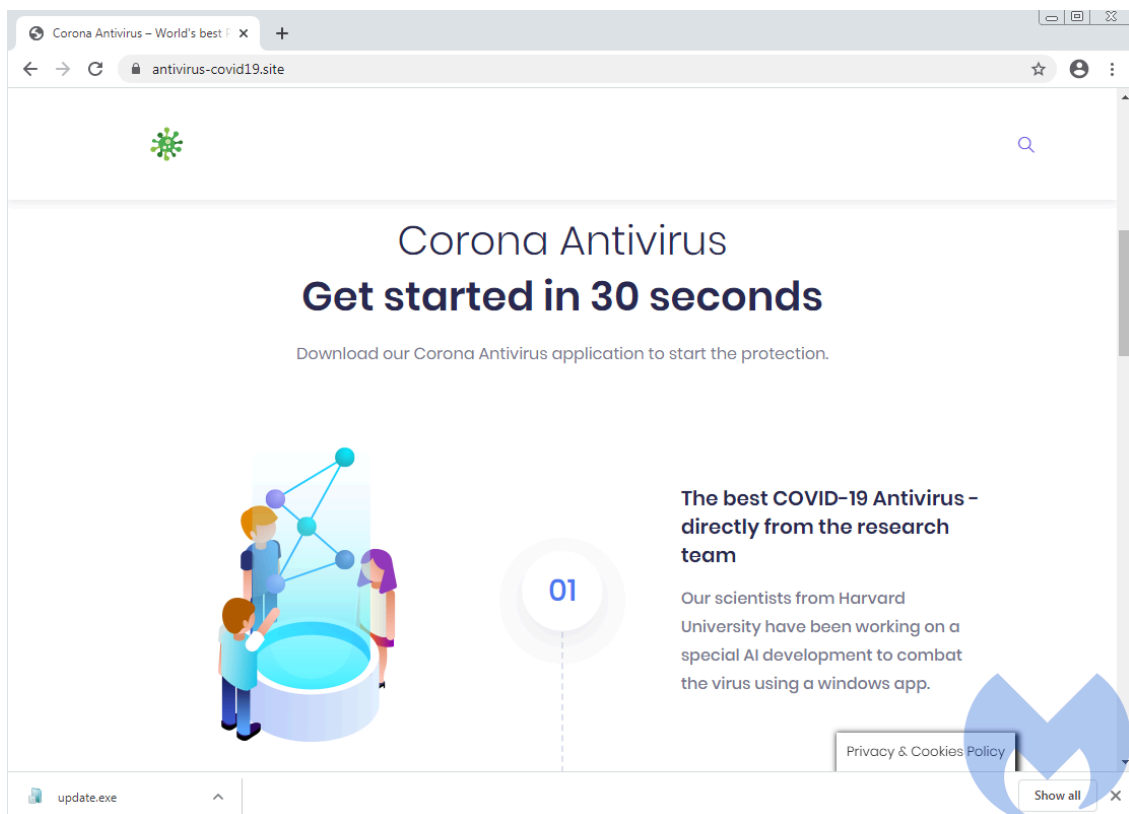
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

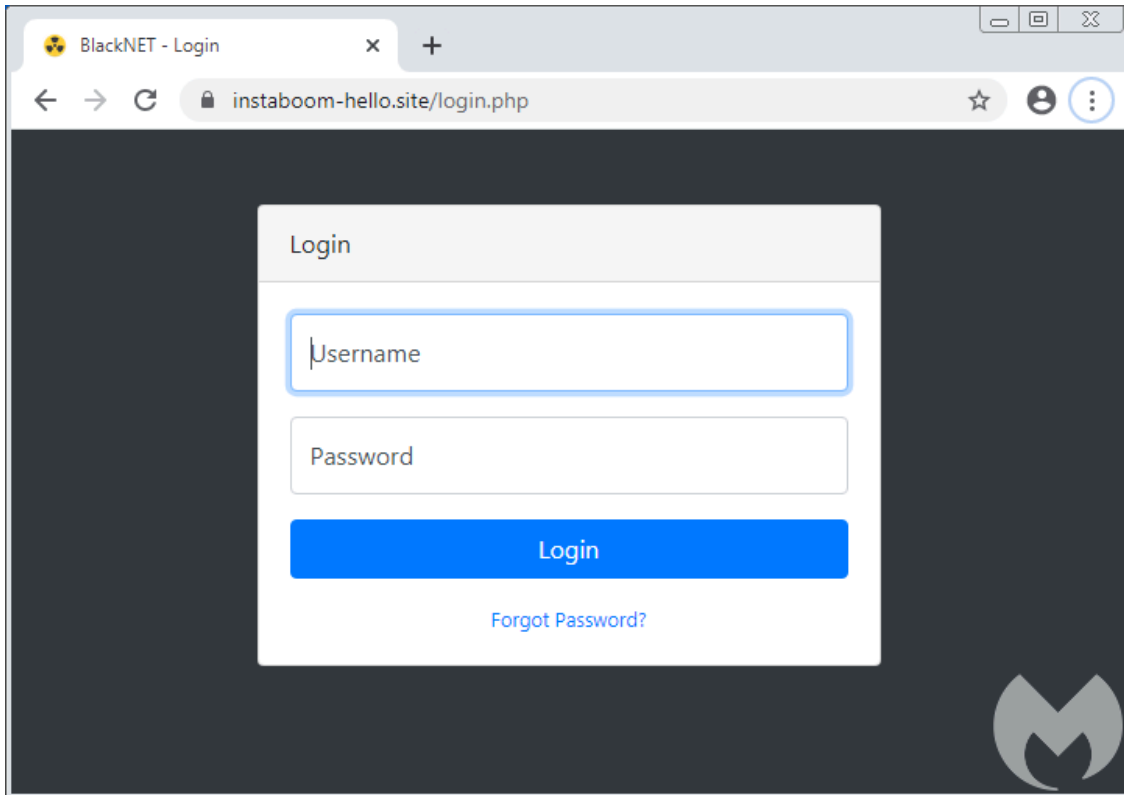


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

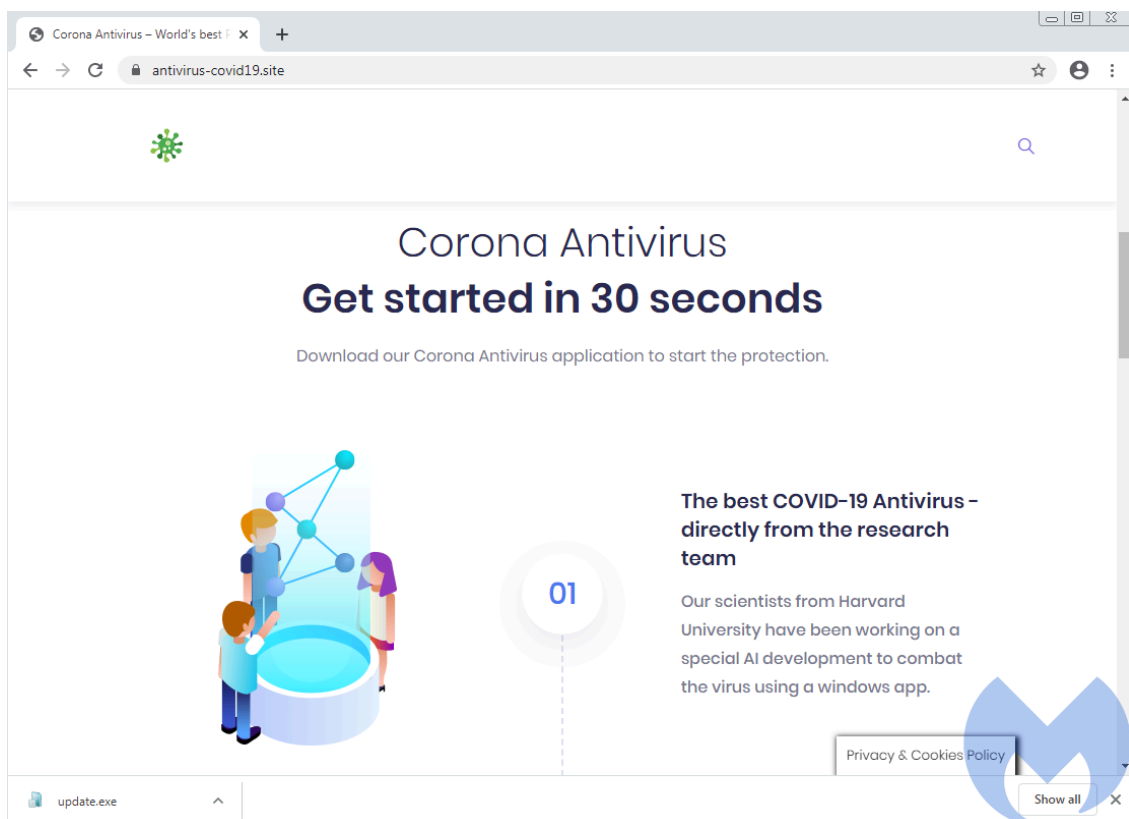
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue Malwarebytes logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

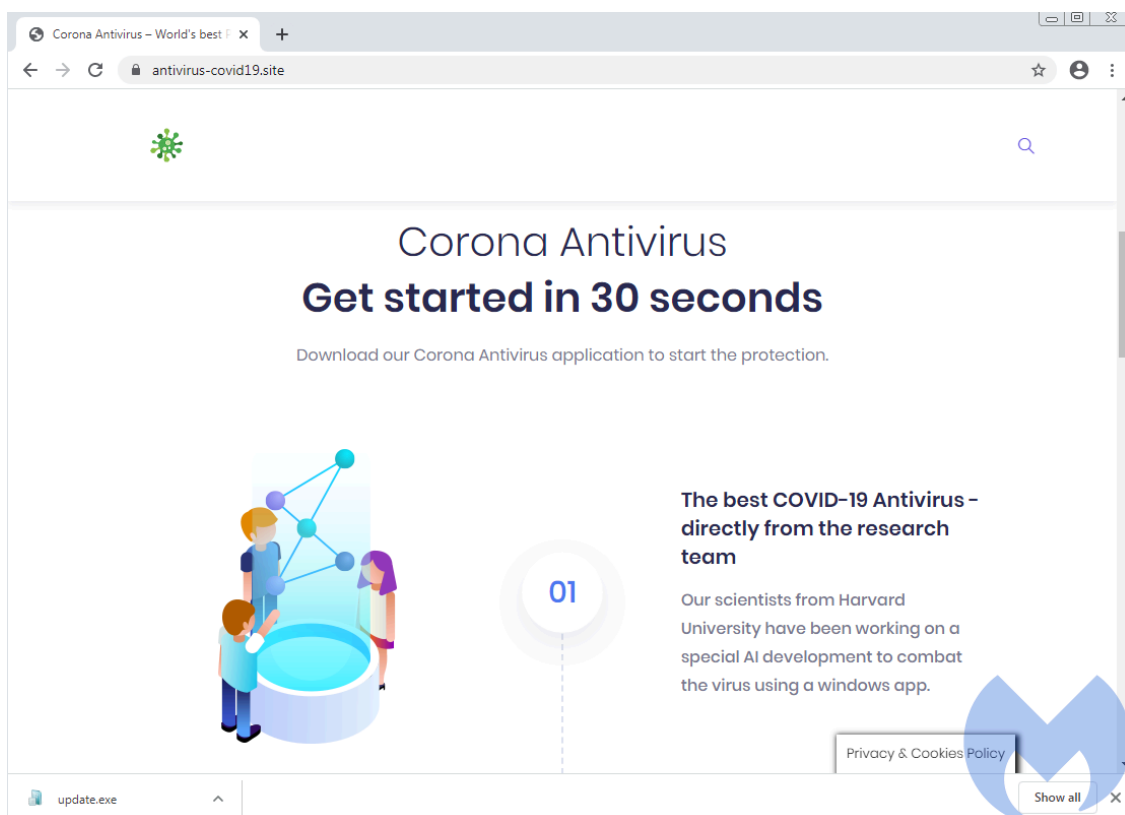
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." The main dashboard features a "Slaves Menu" with four status cards: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below these is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows "No Clients Available". To the right of the table are "Previous" and "Next" buttons. Below the table is a "Commands Center" with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" showing a world map with blue markers. At the bottom, a copyright notice reads "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: "Malware blocked by Real-Time Protection". Below this, it states: "It has been automatically quarantined and is no longer a threat to your computer." The details provided are: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

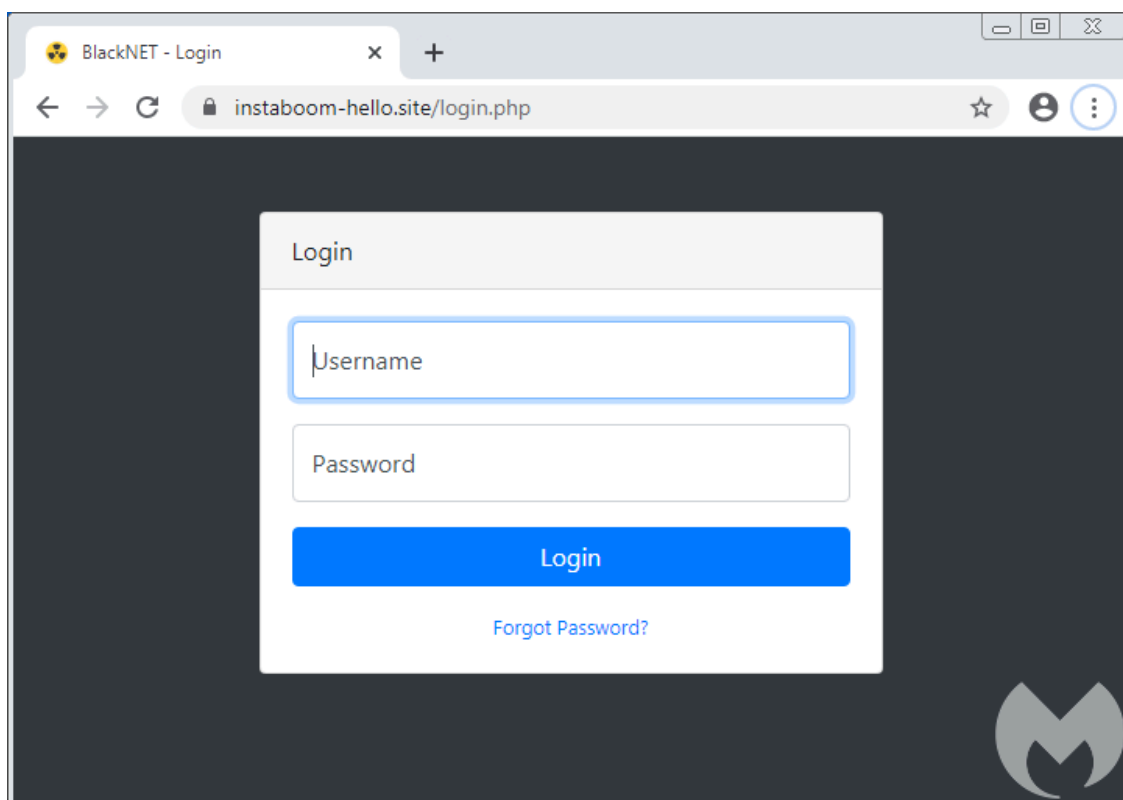
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

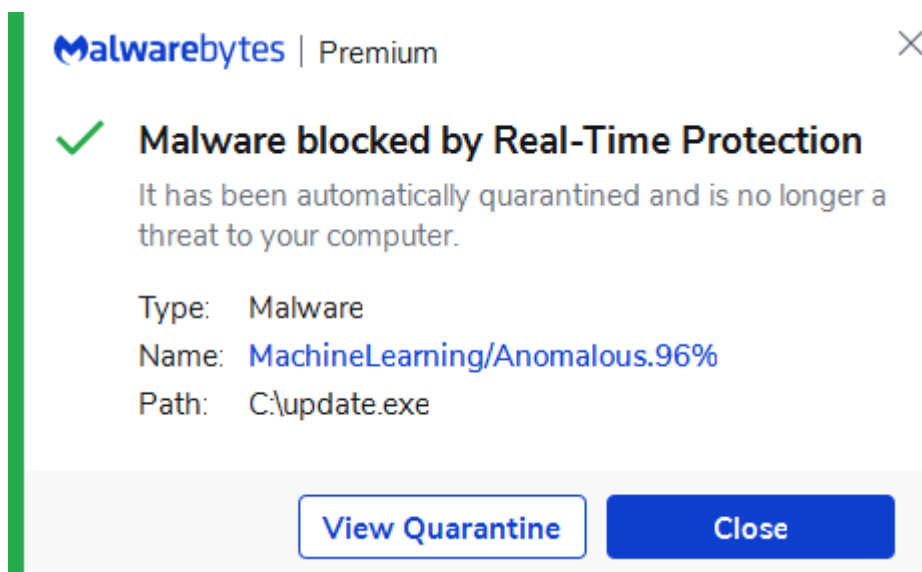
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

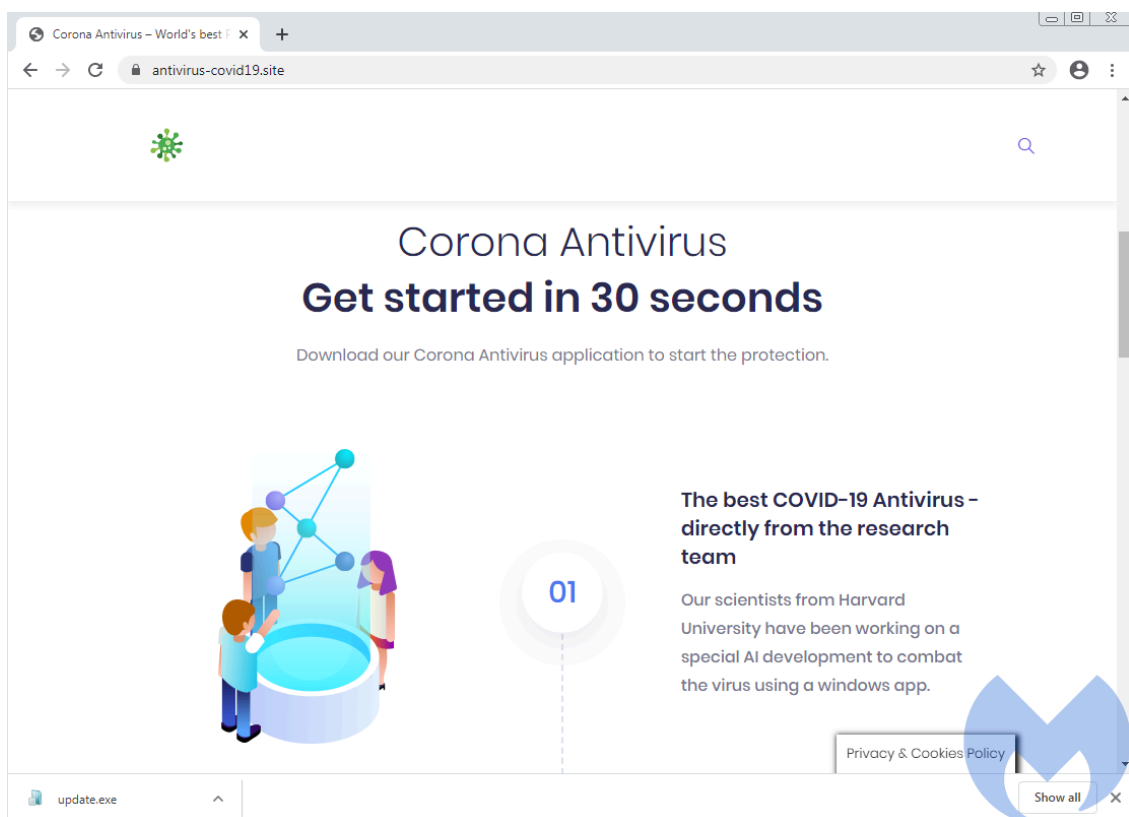
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

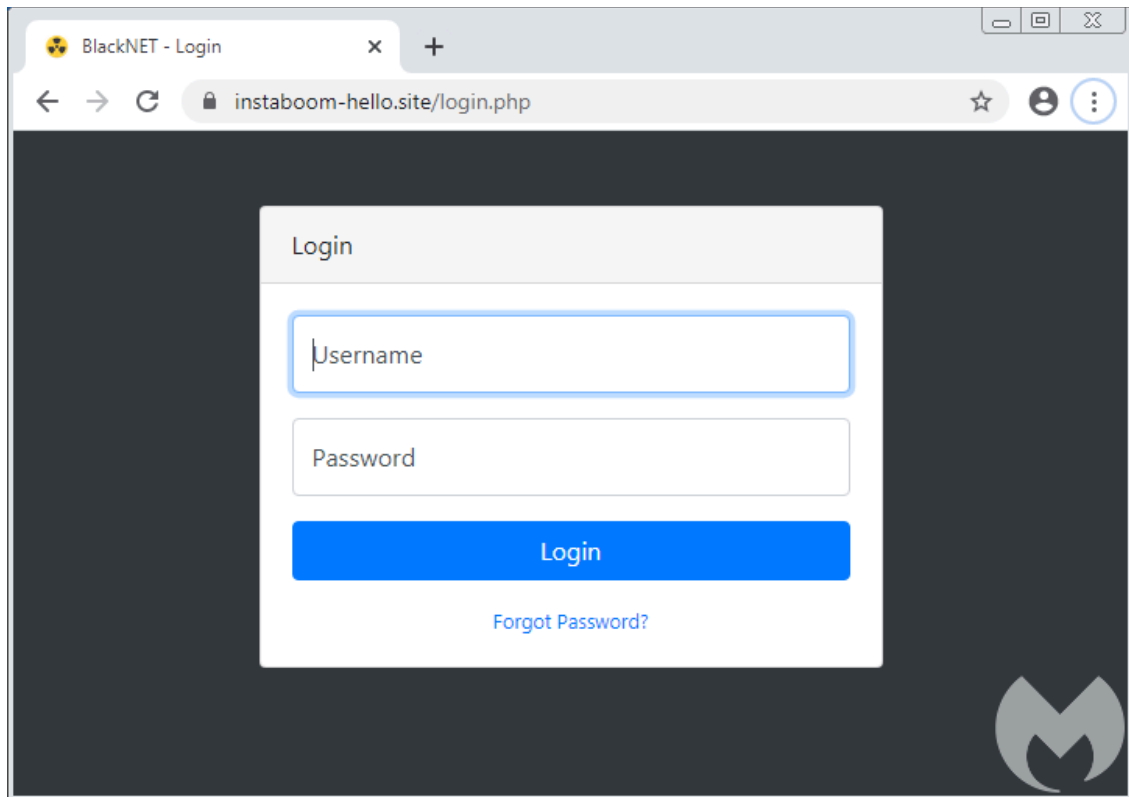



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored tiles: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

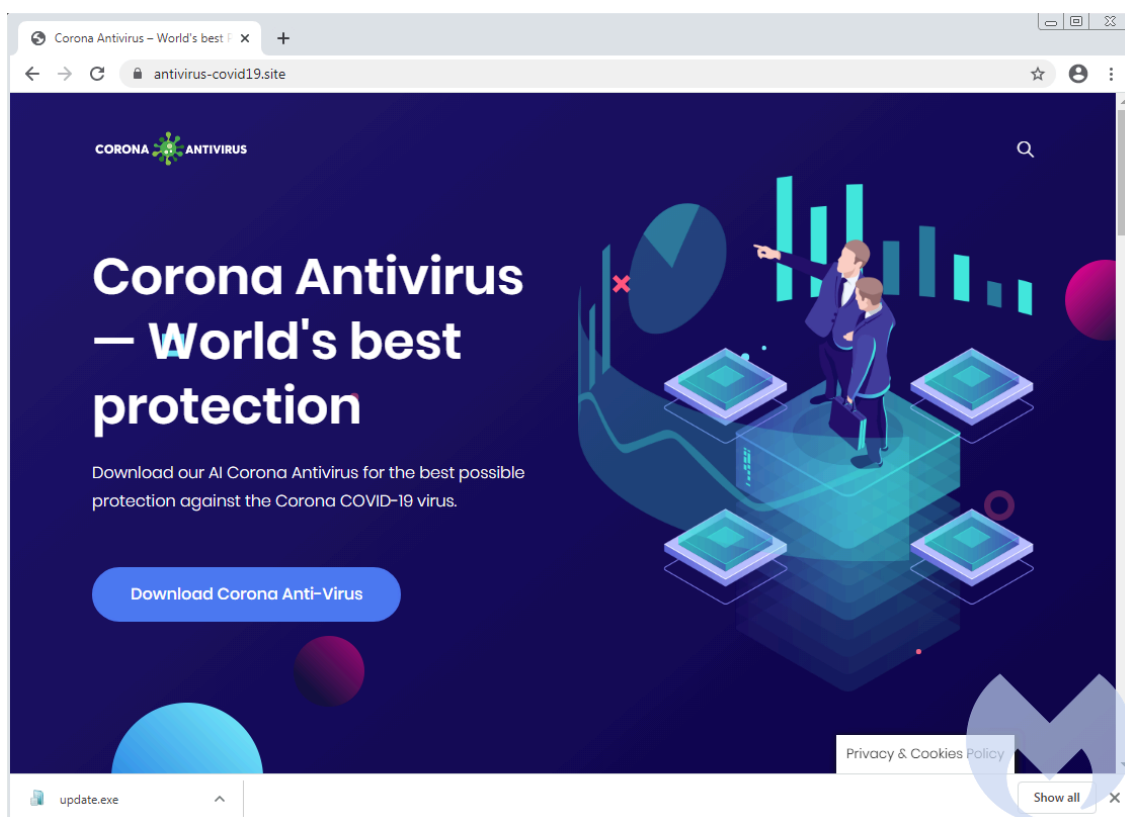
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

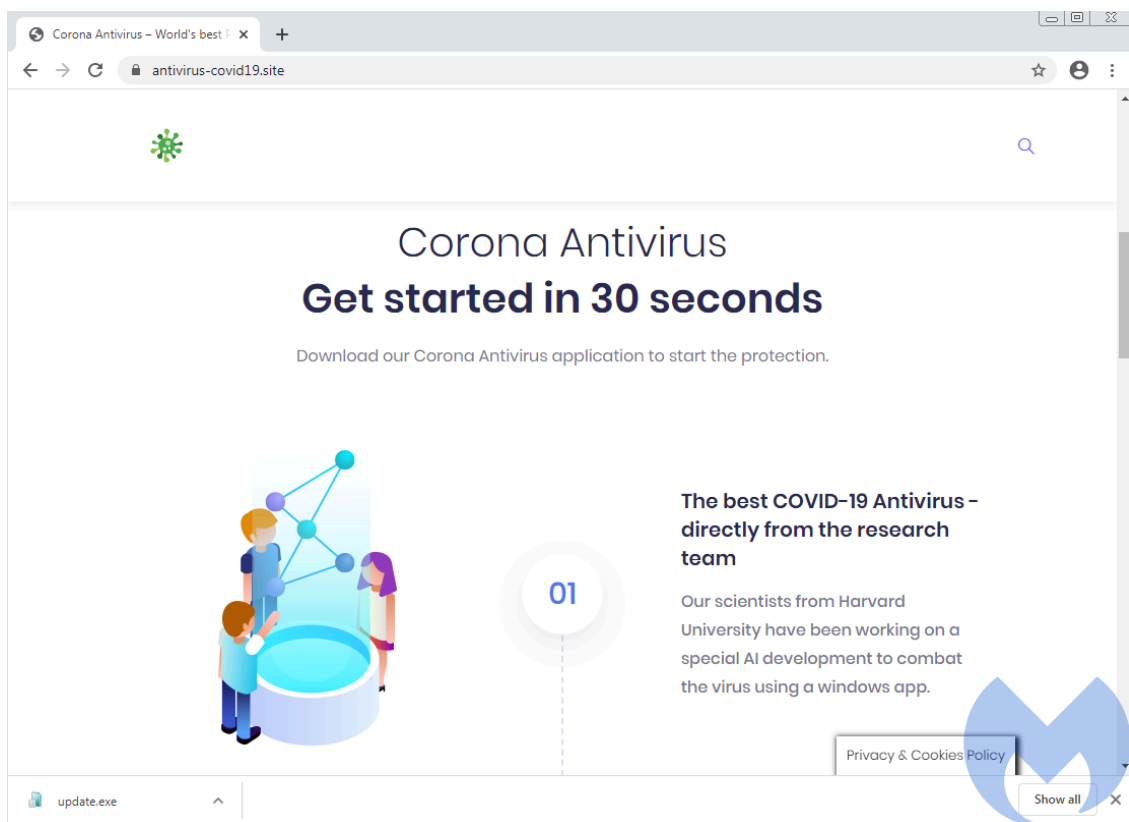
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

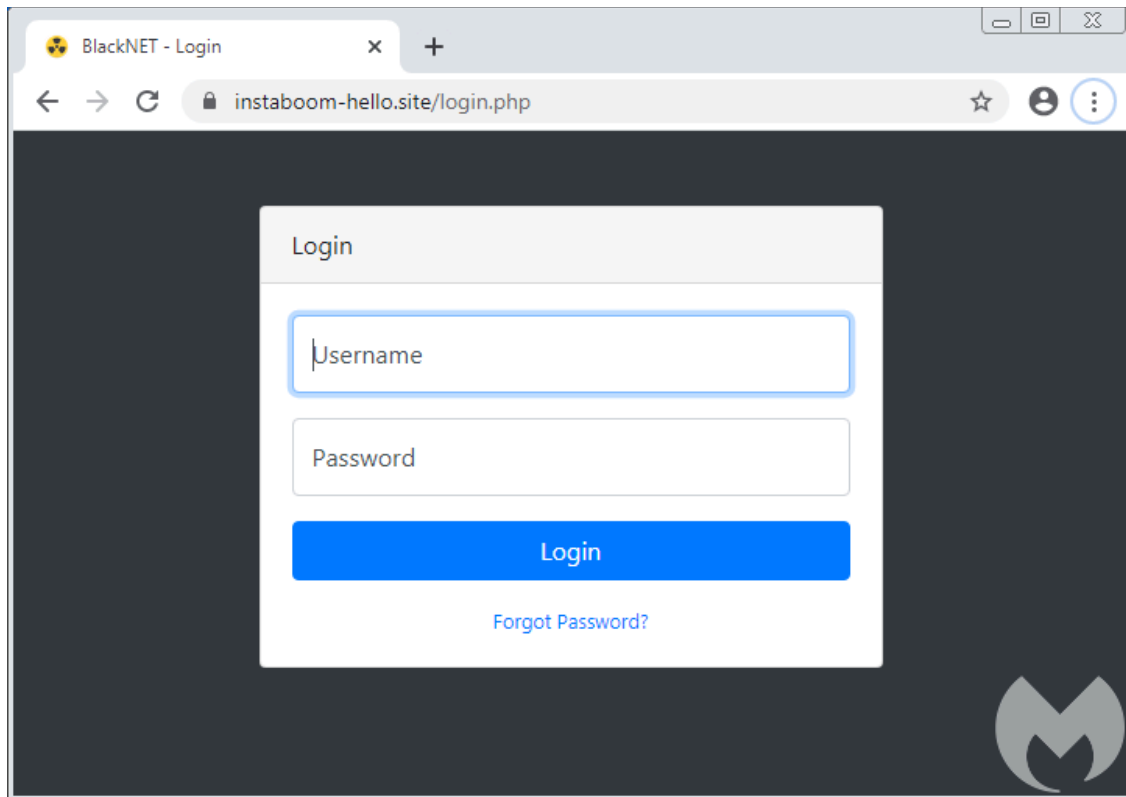


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

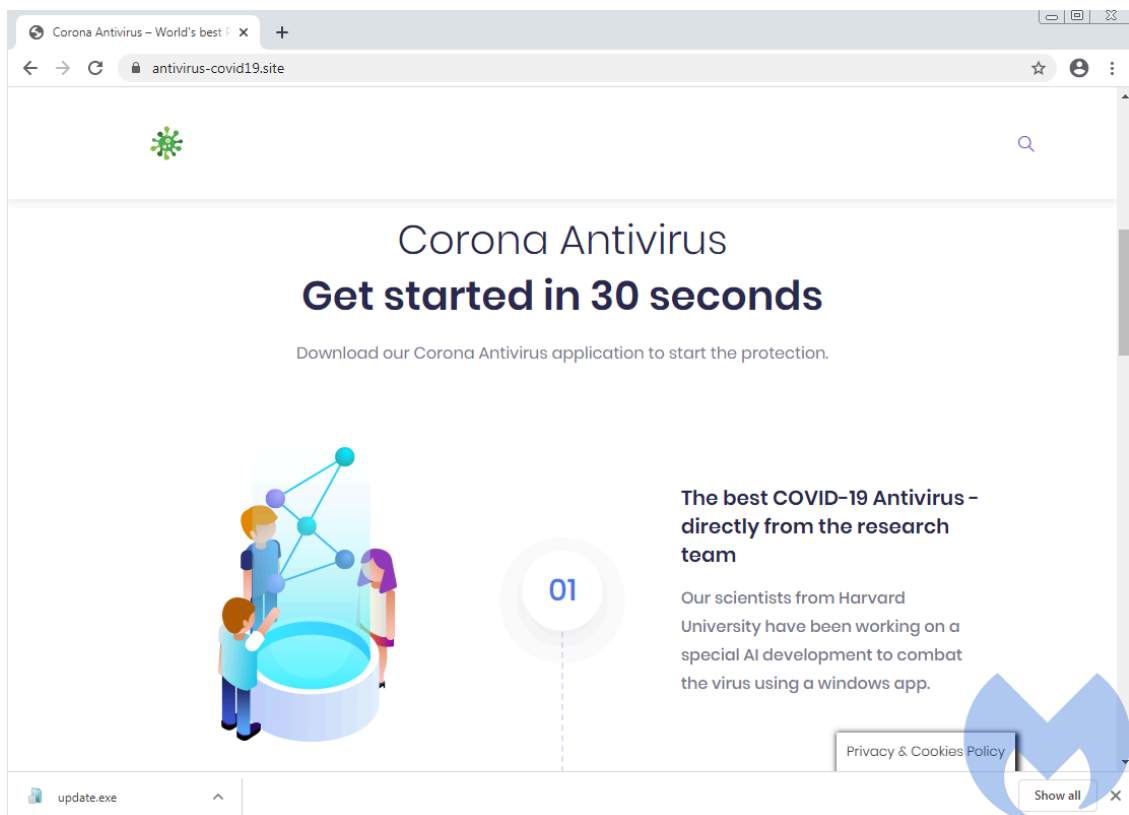
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

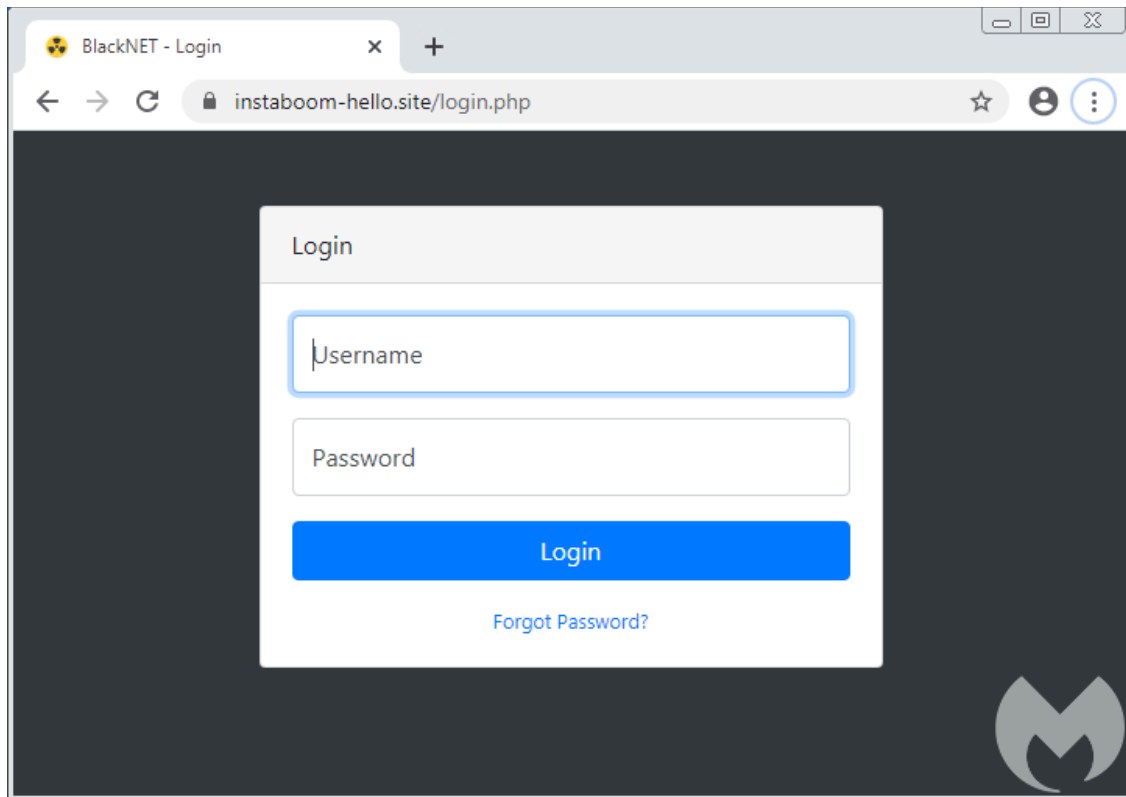


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

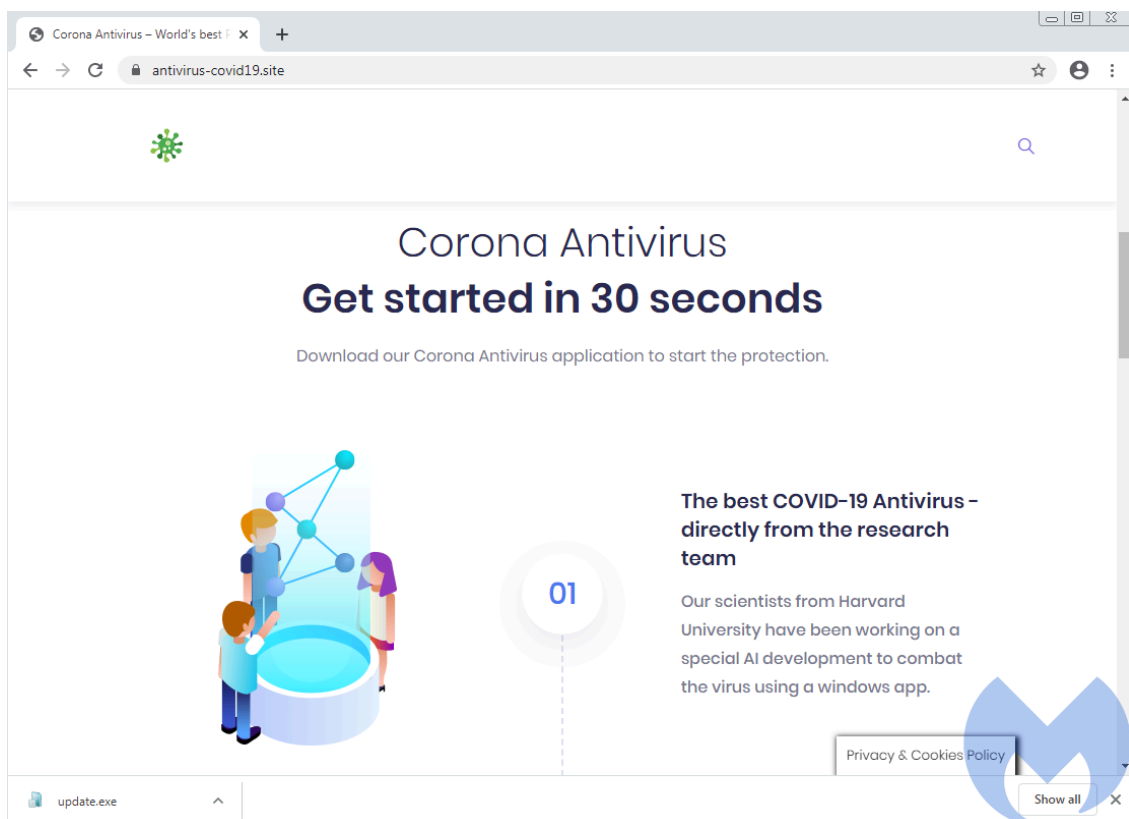
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

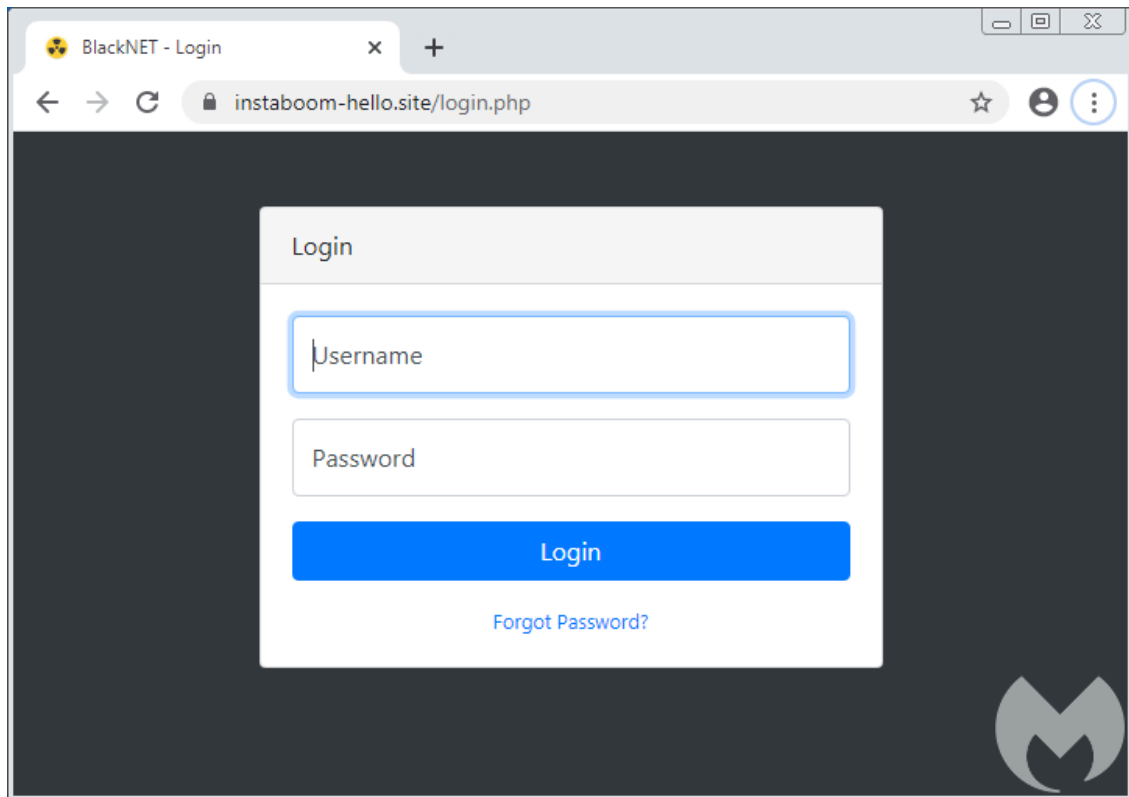


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

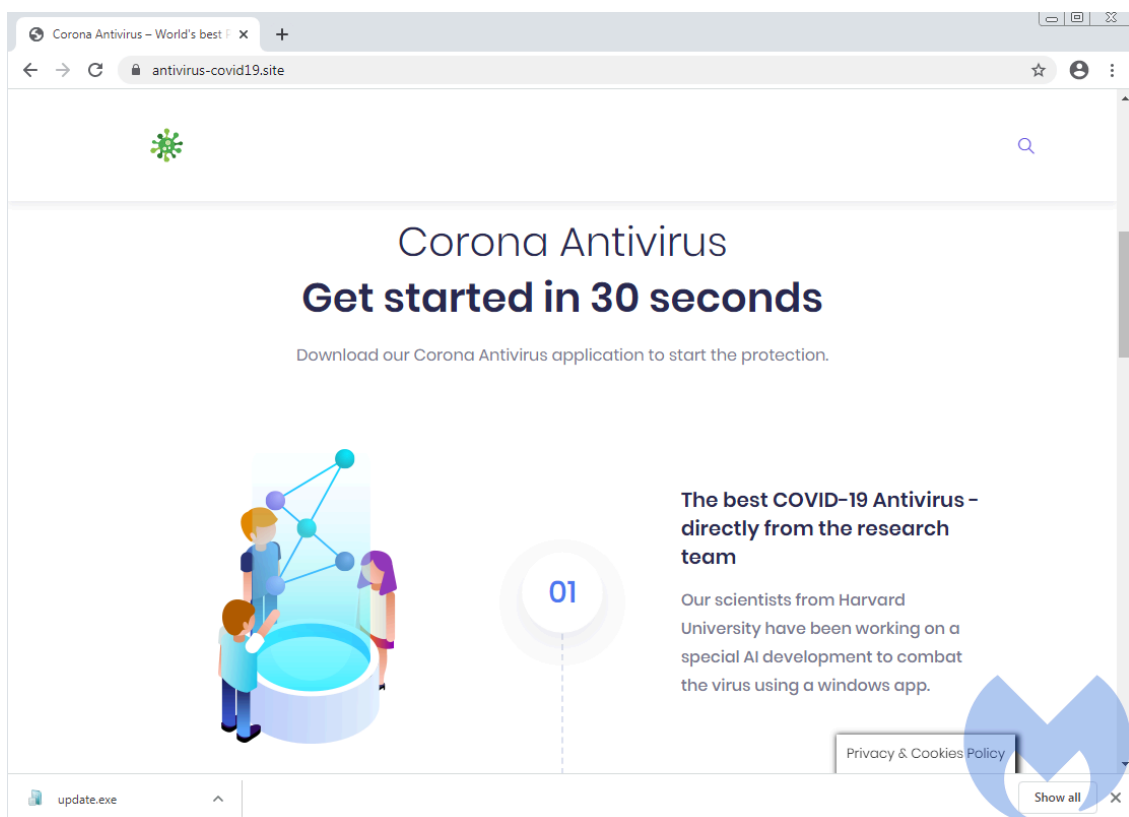
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

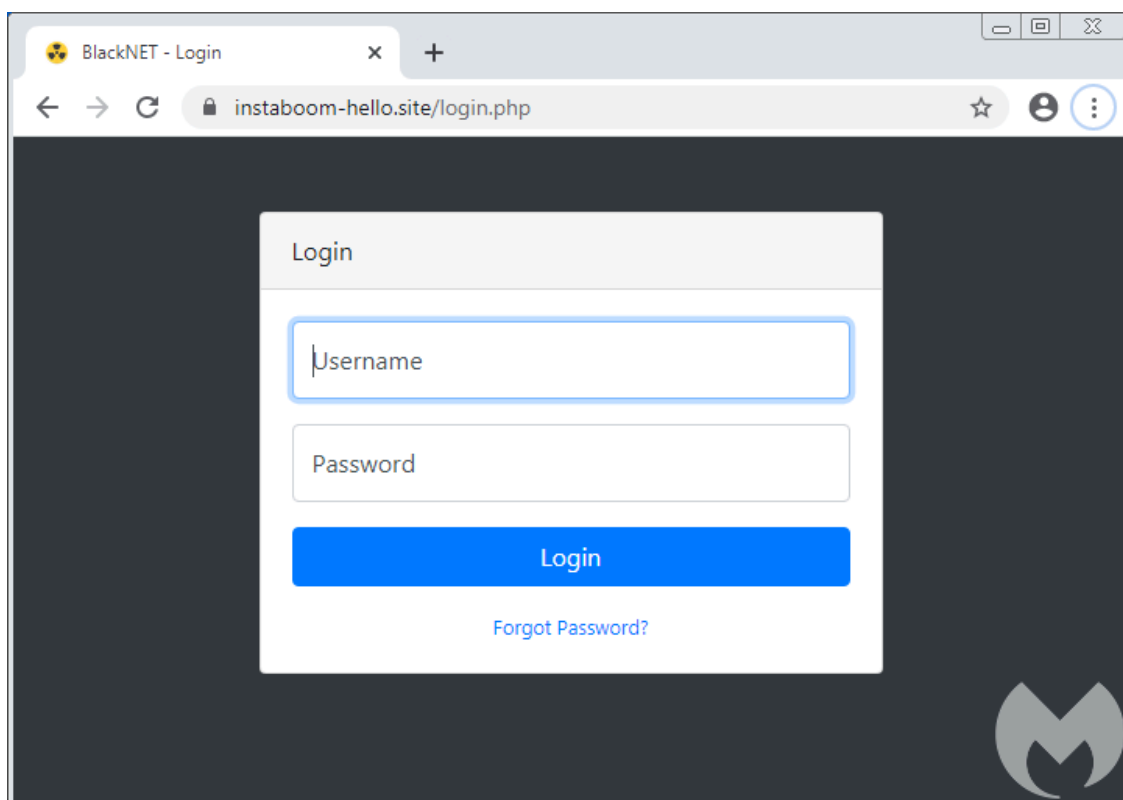
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

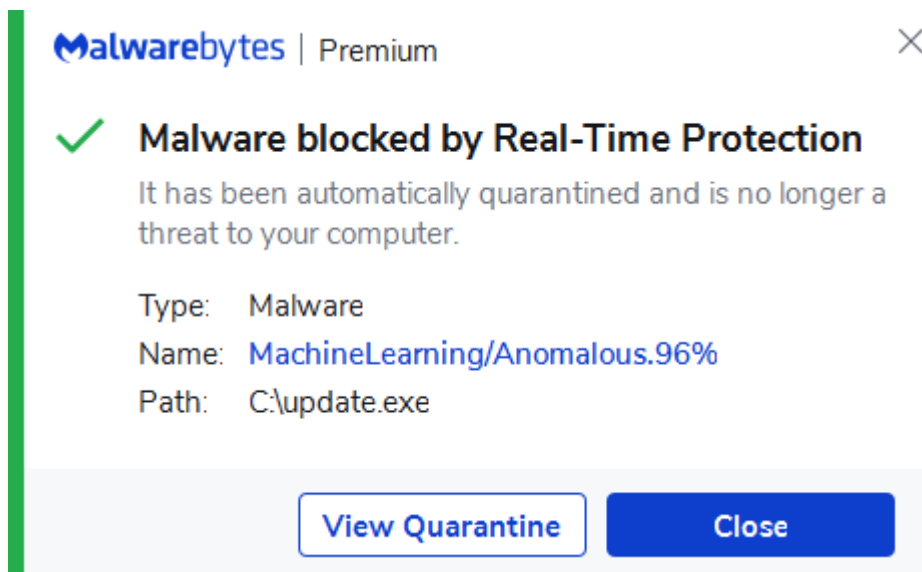
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a 'Command' dropdown and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

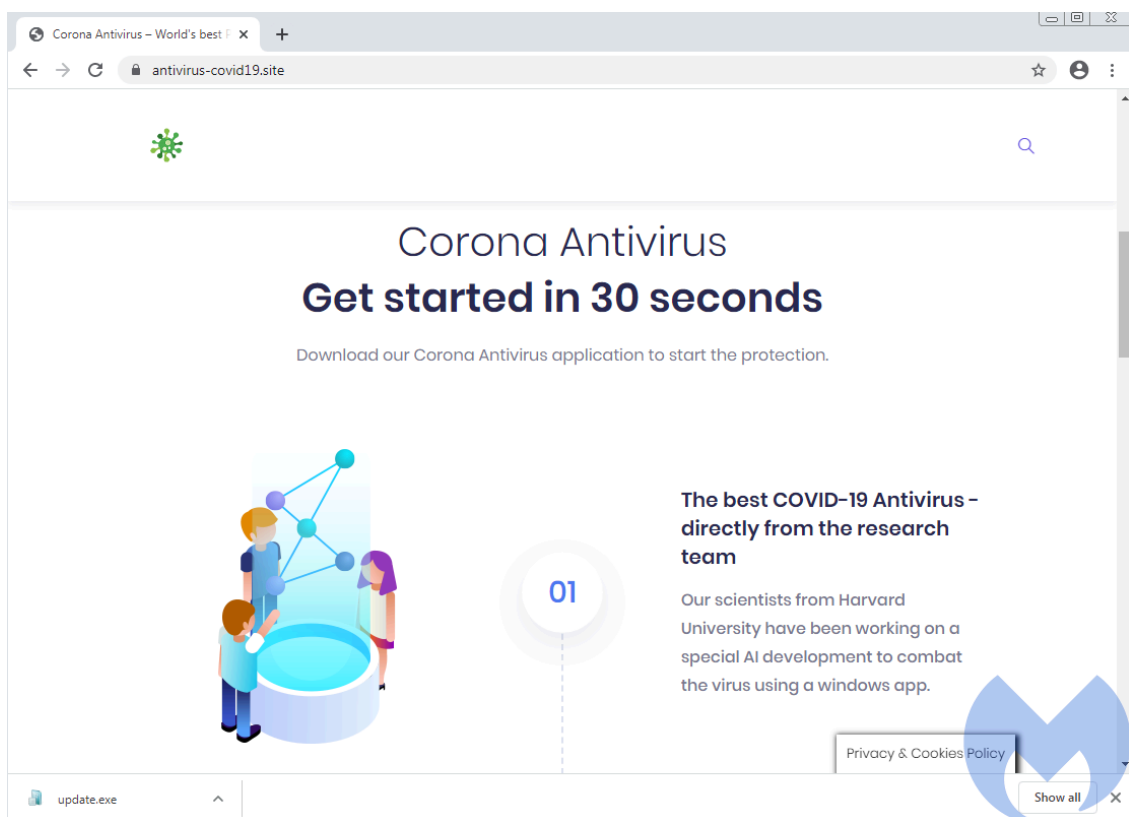
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

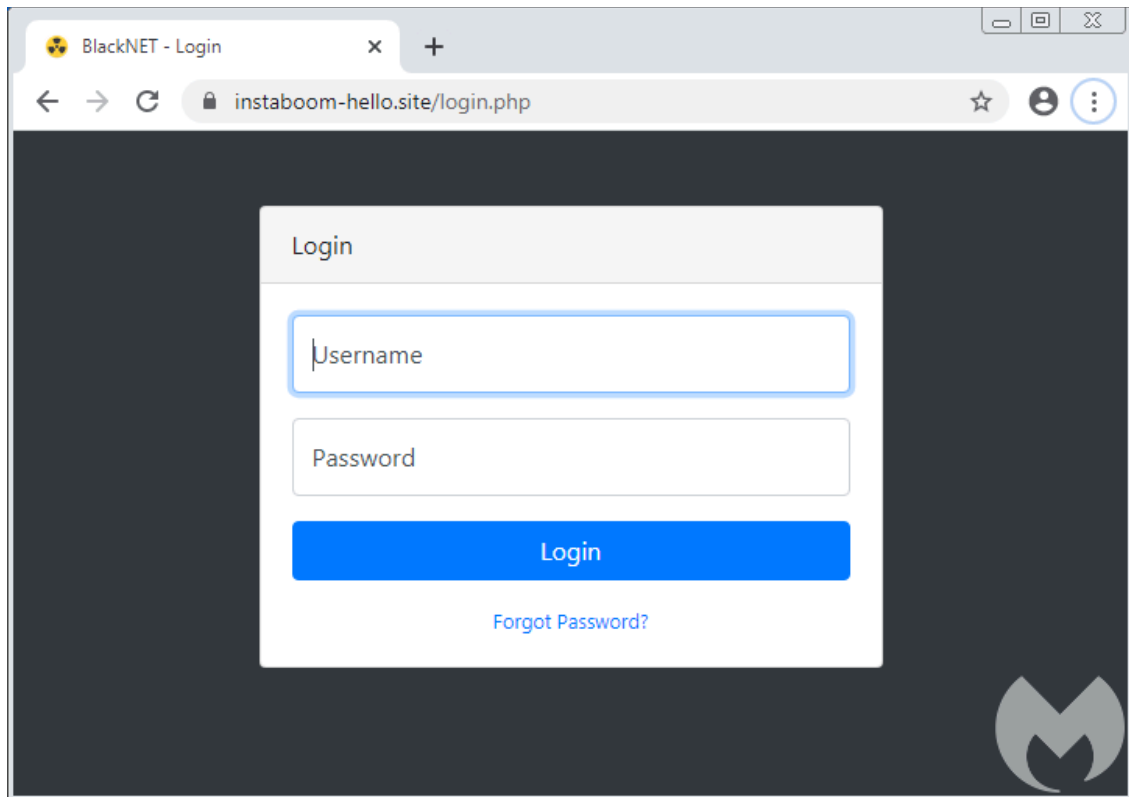


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Malwarebytes | Premium

✓ **Malware blocked by Real-Time Protection**

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: MachineLearning/Anomalous.96%

Path: C:\update.exe

View Quarantine Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

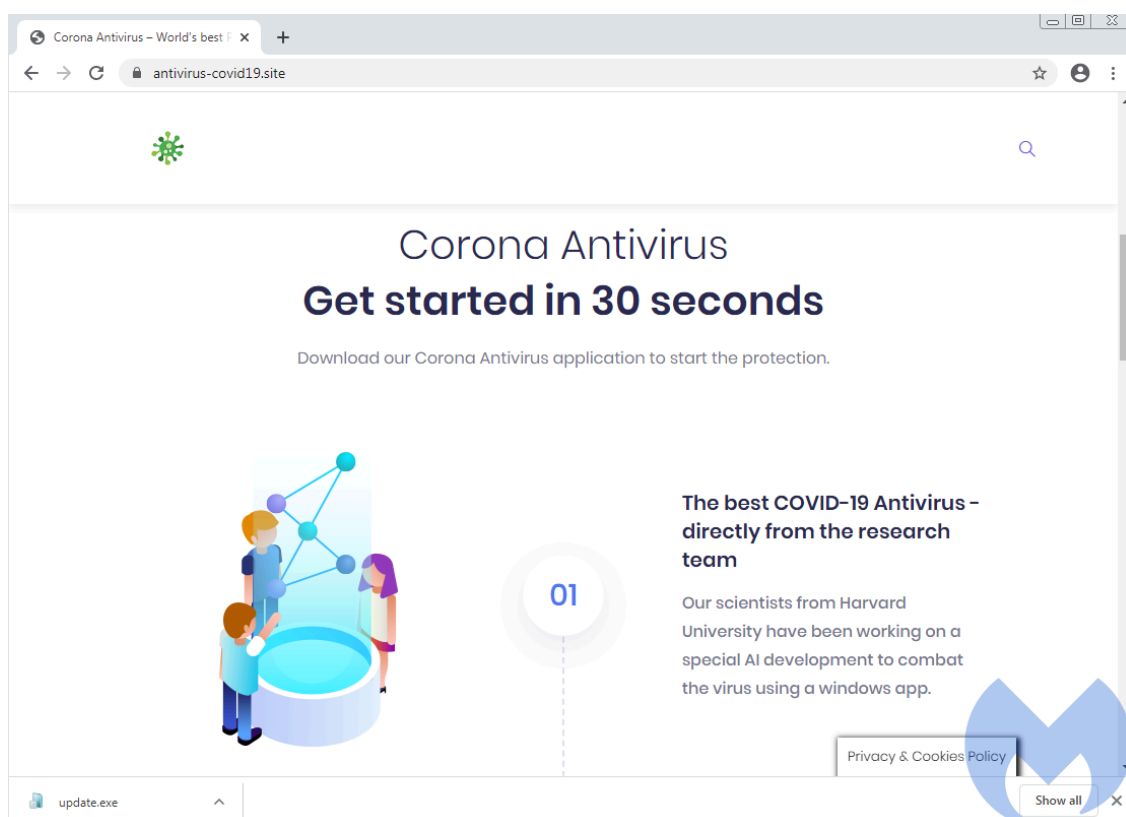
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

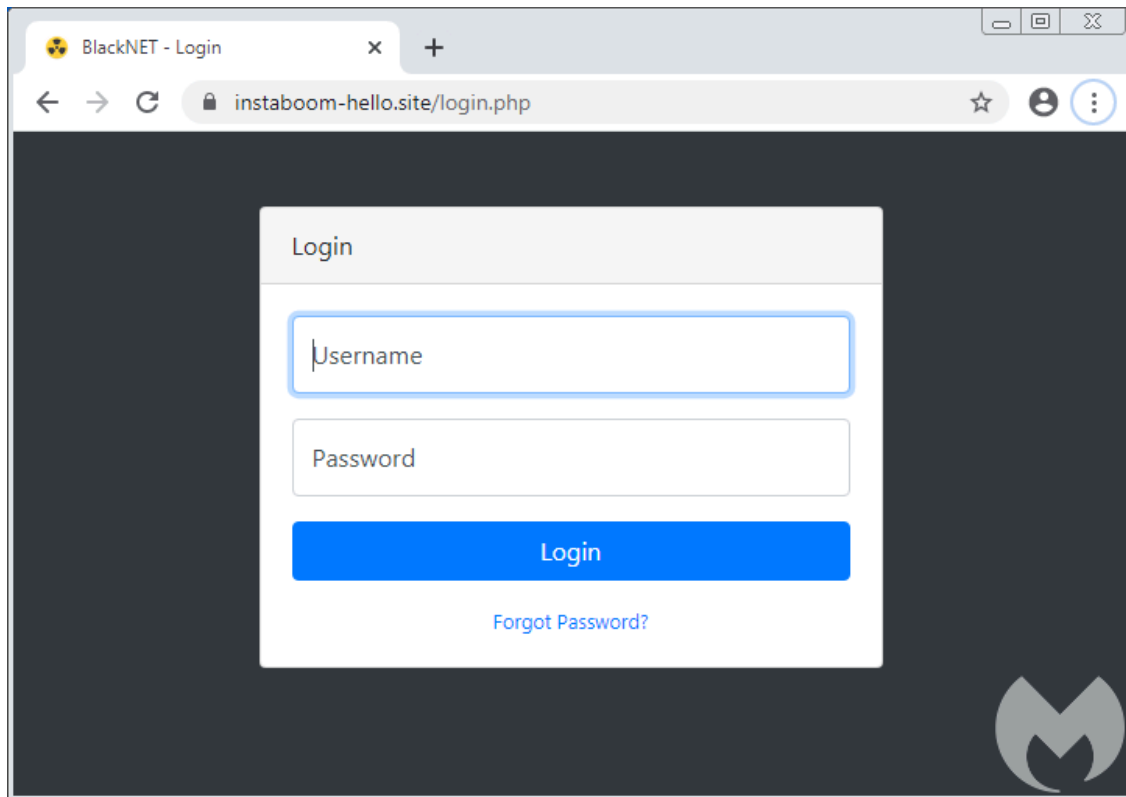


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

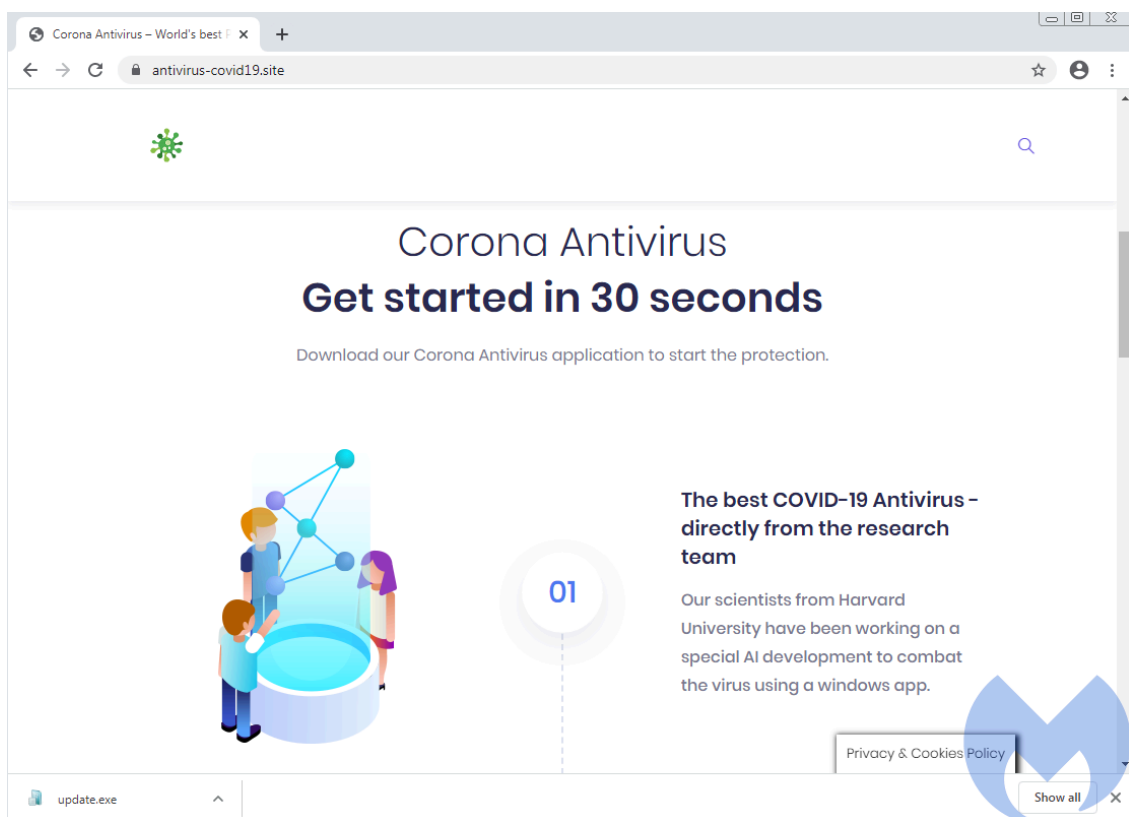
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

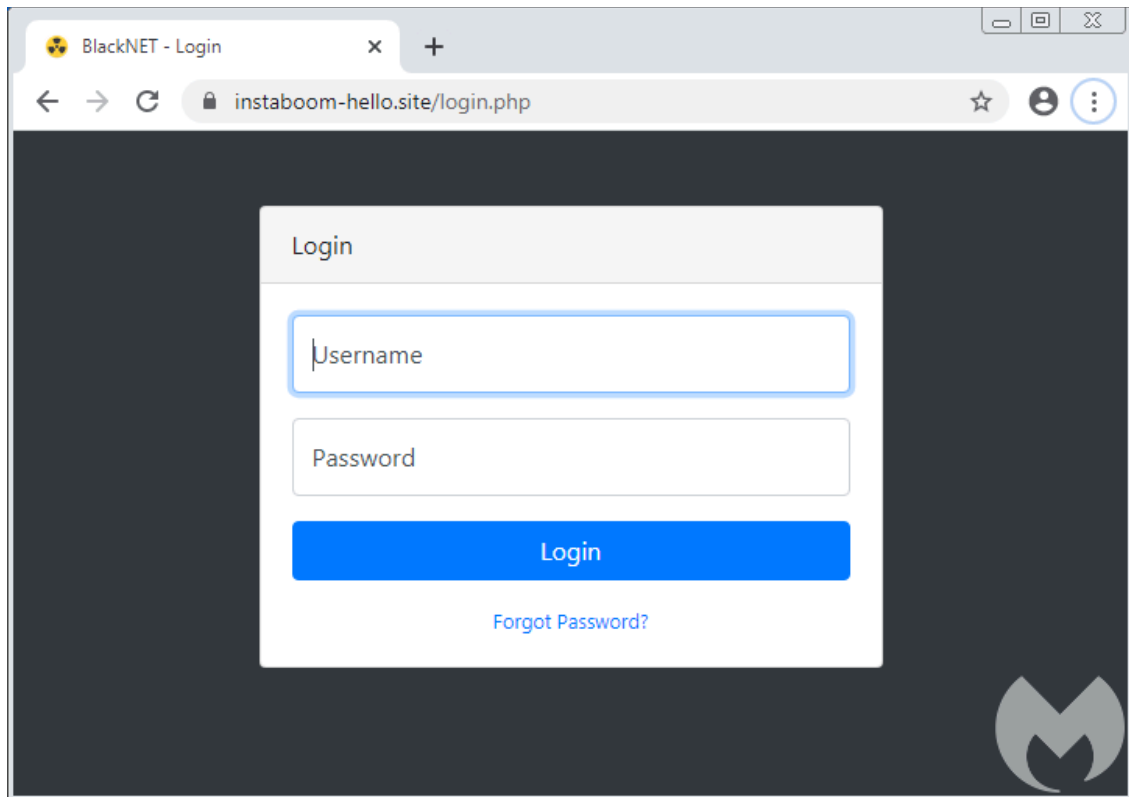


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

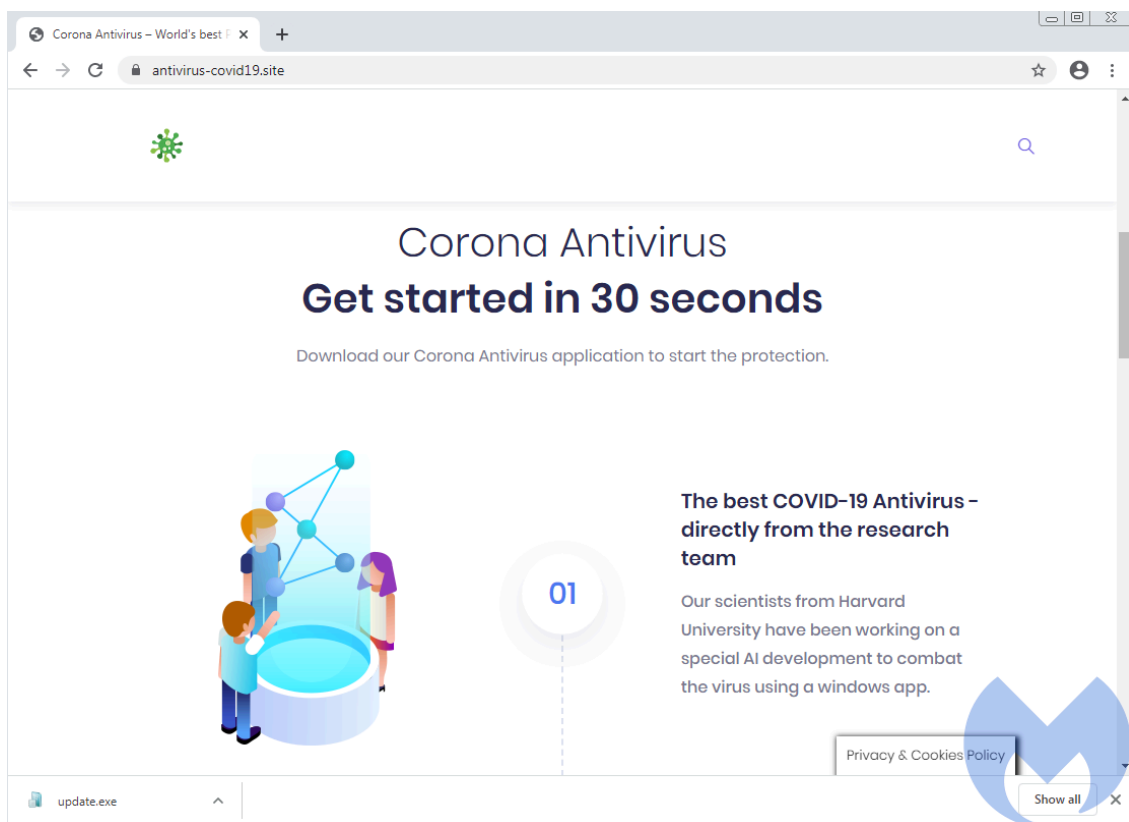
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

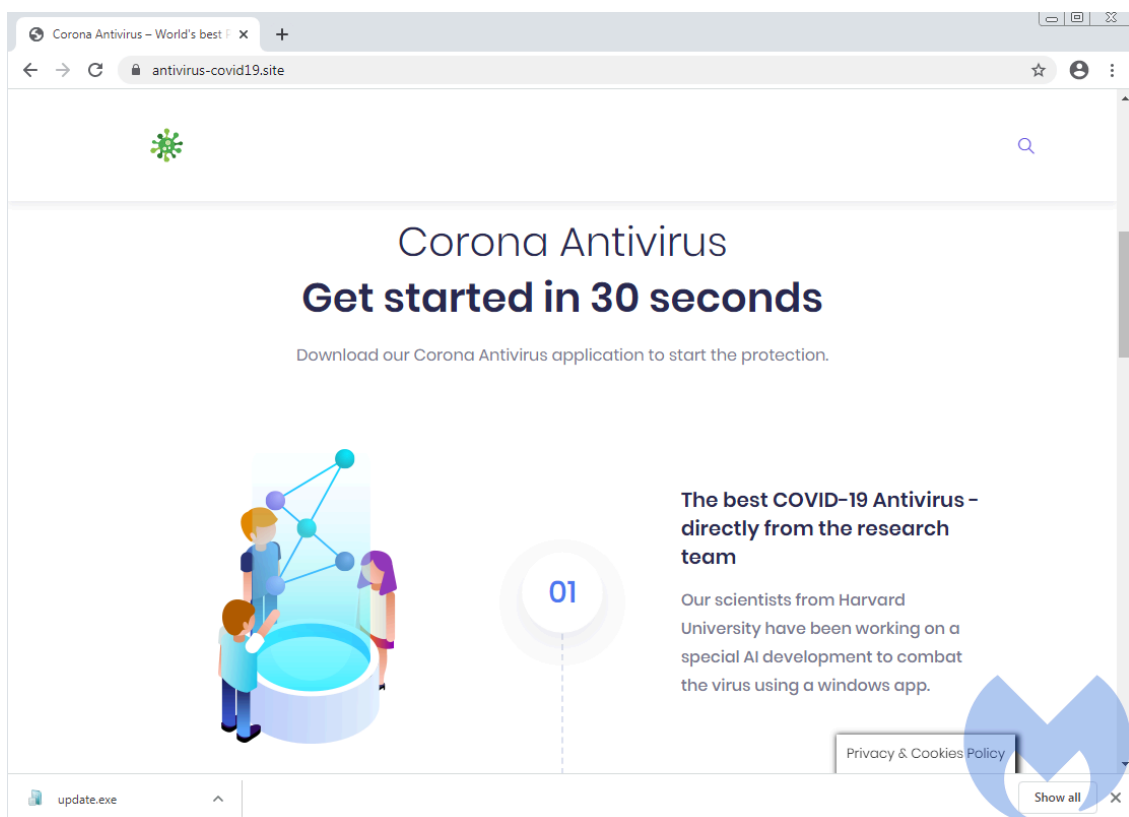
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

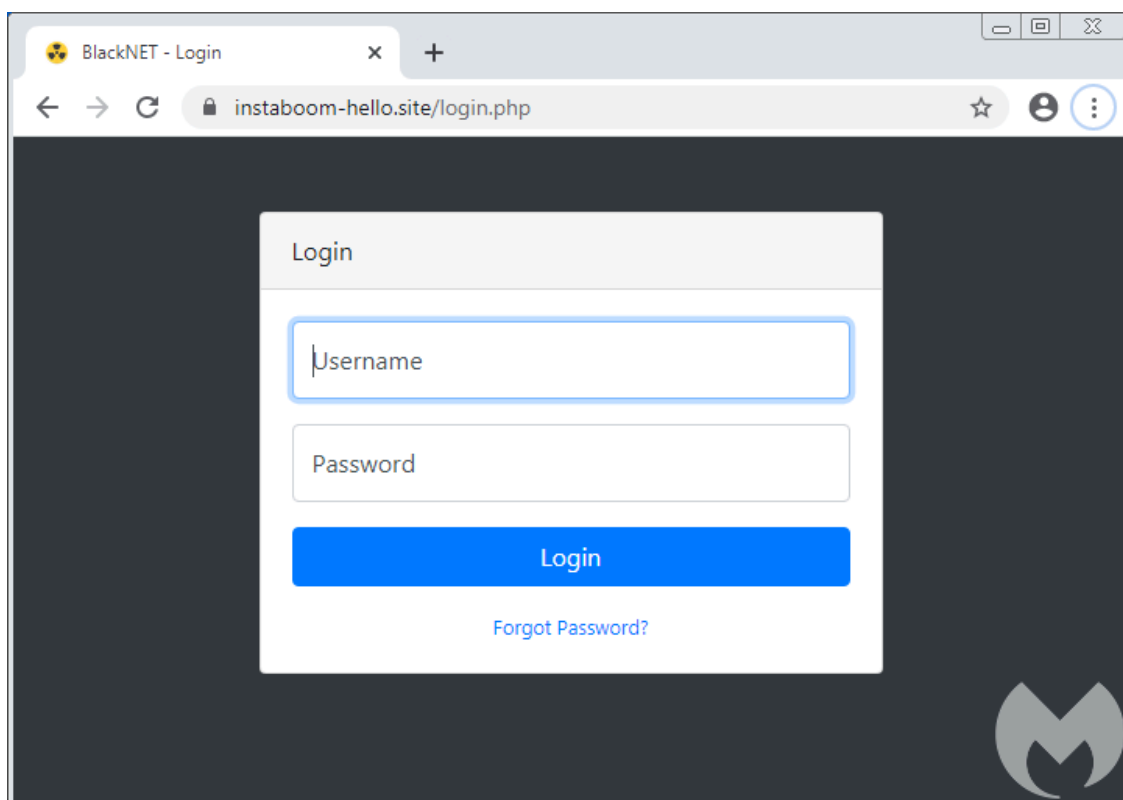
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

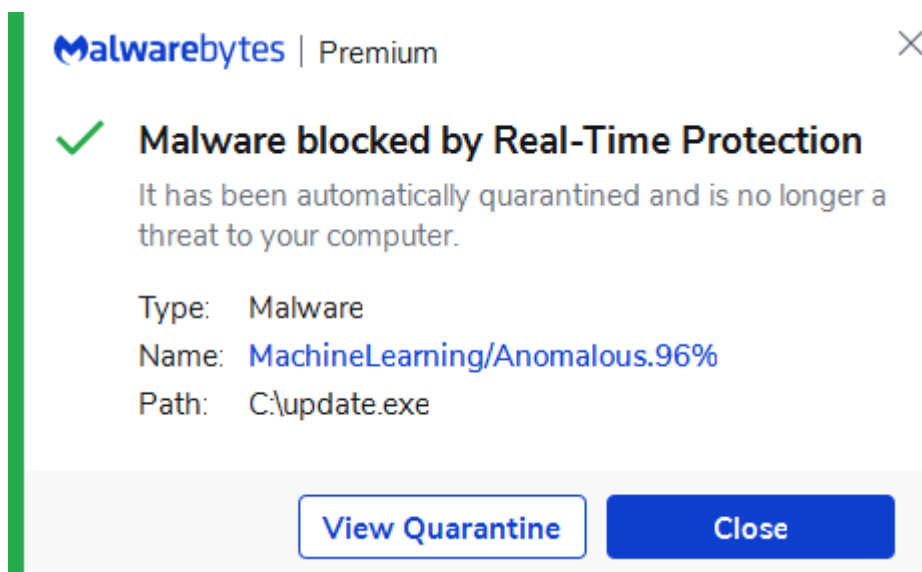
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

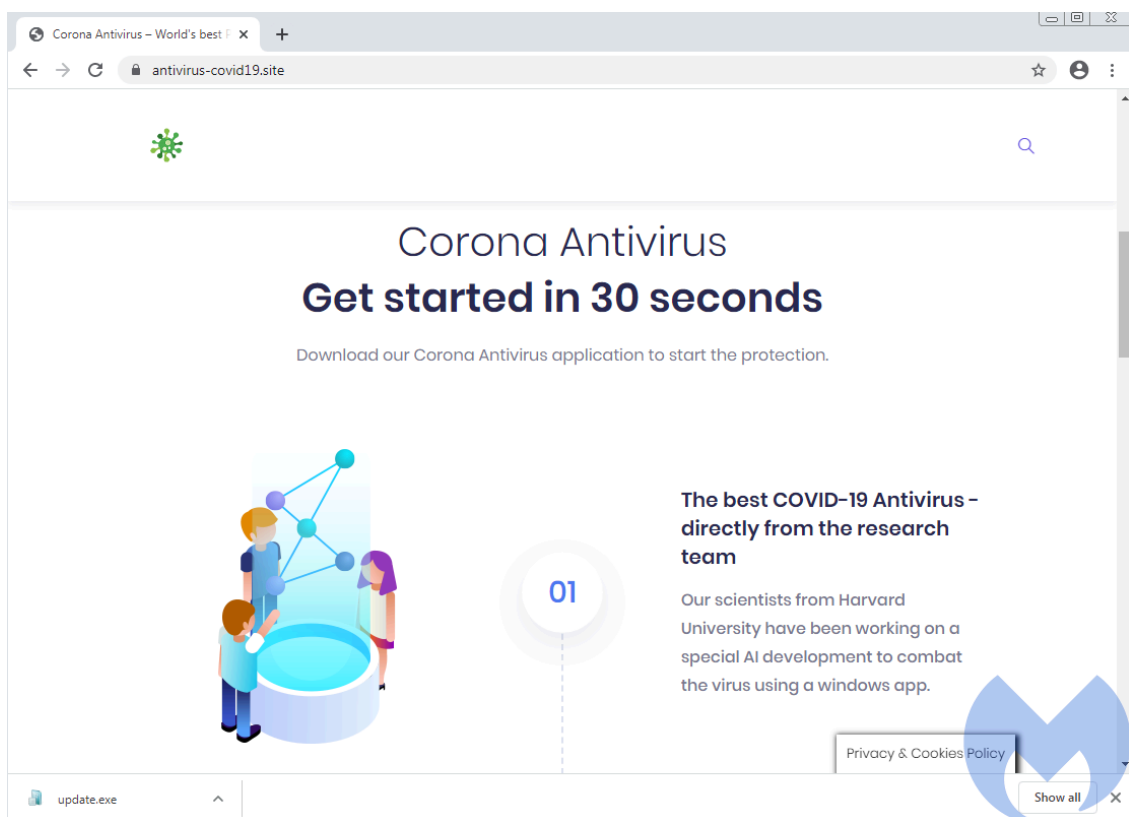
C2 panel

```
instaboom-hello[.]site
```




To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

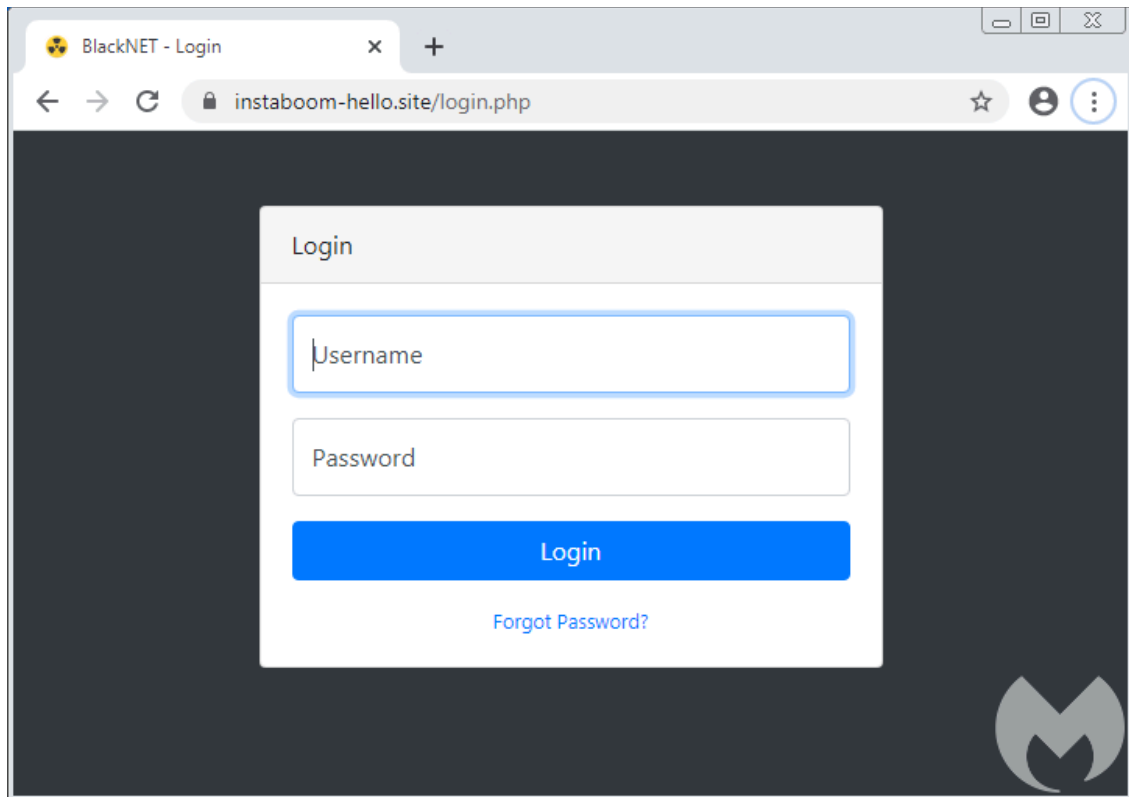


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

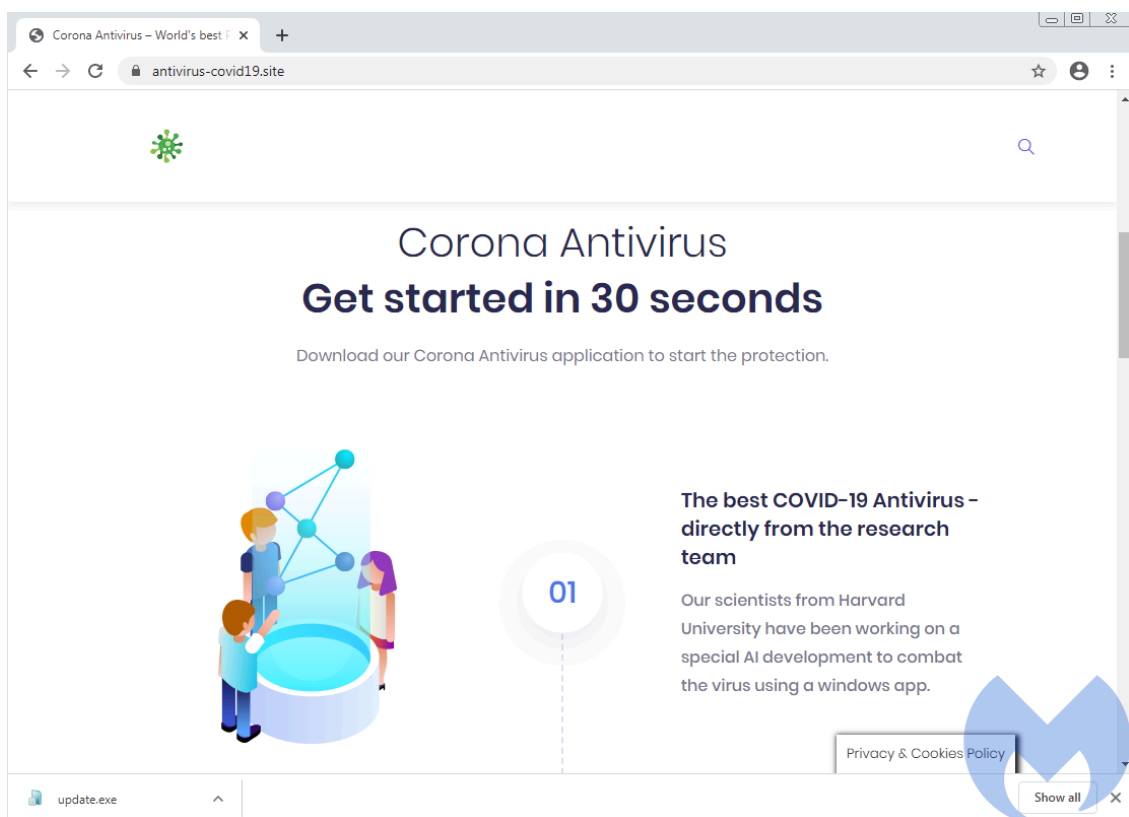
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

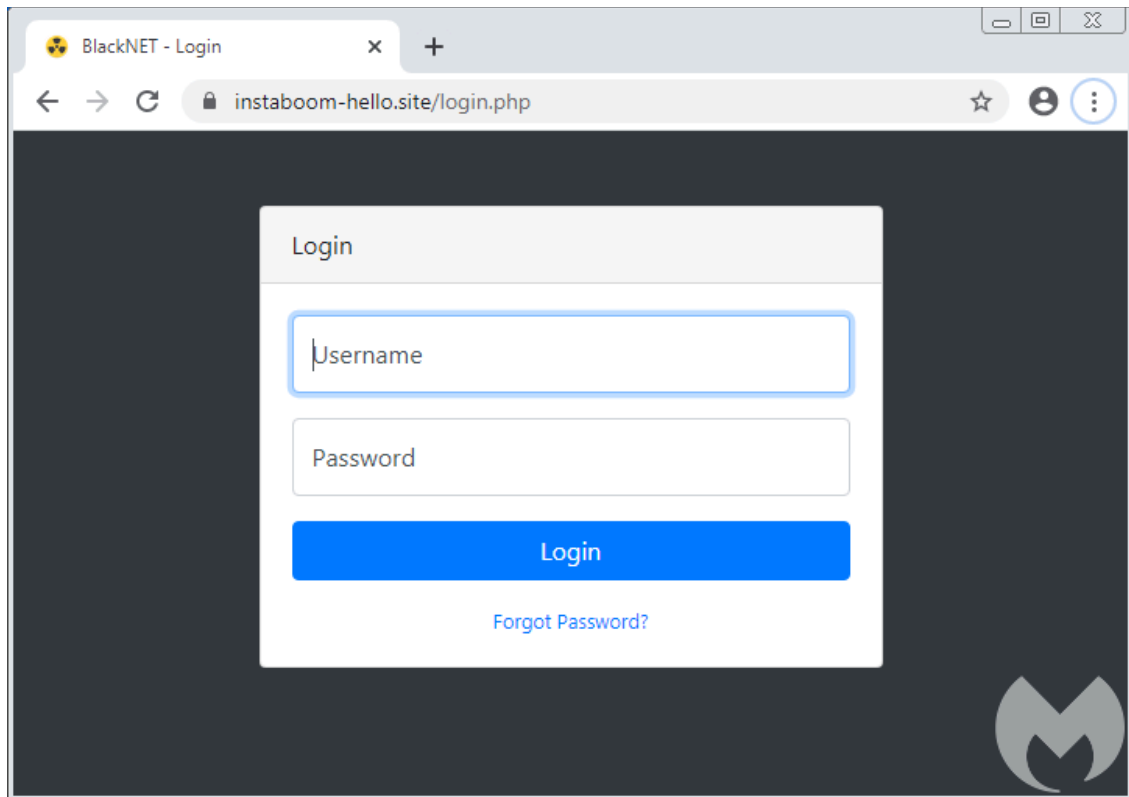


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

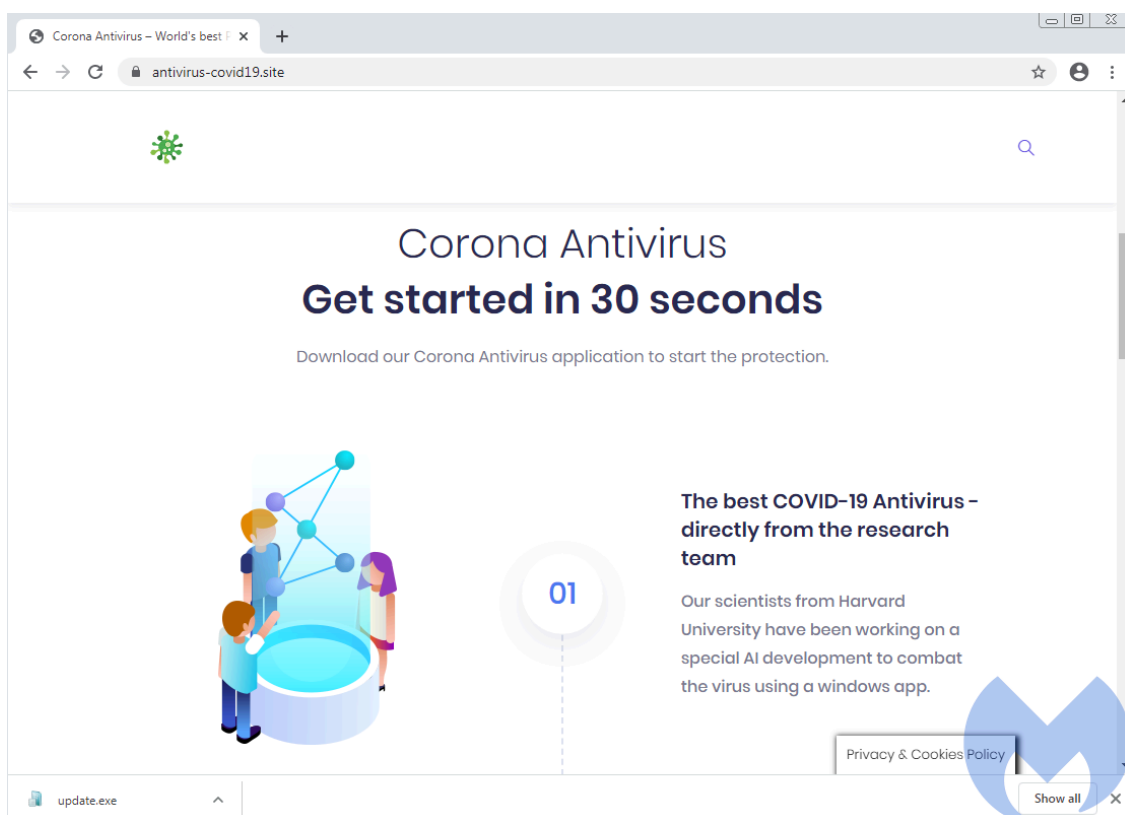
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

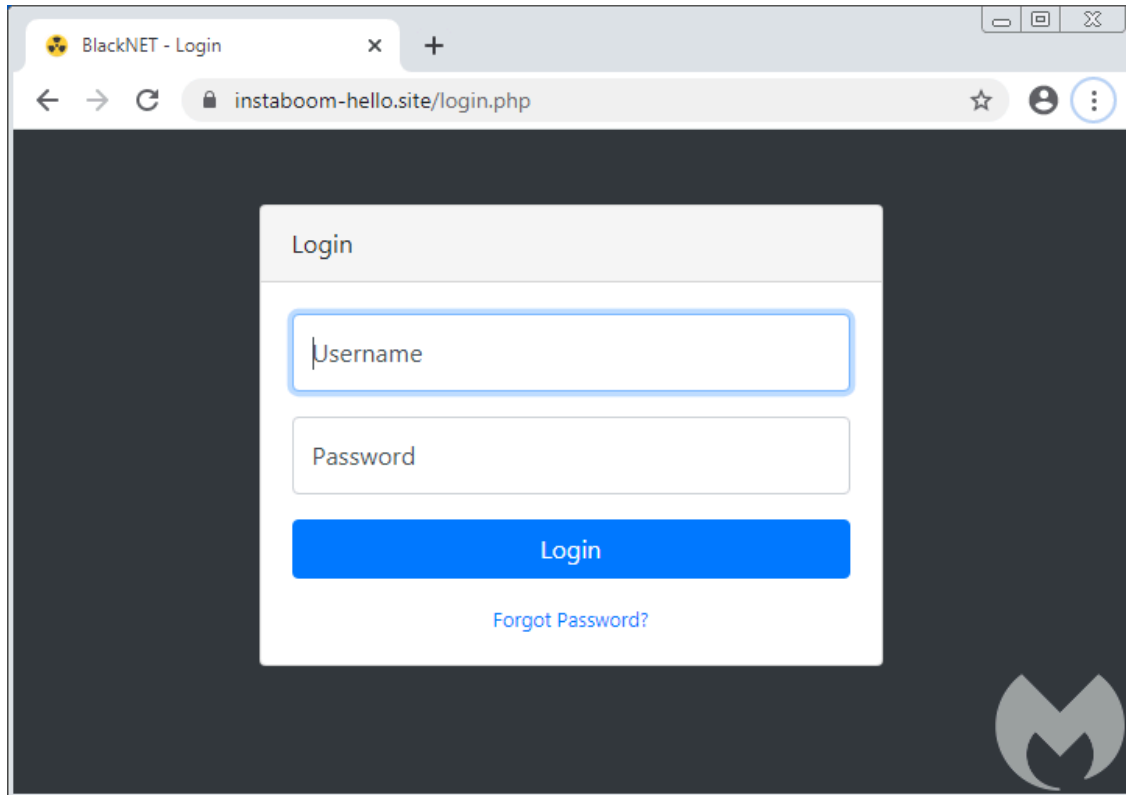


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a table header including Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the right of the table is a 'Map Visualization' showing a world map with a few blue dots. At the bottom left, there's a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

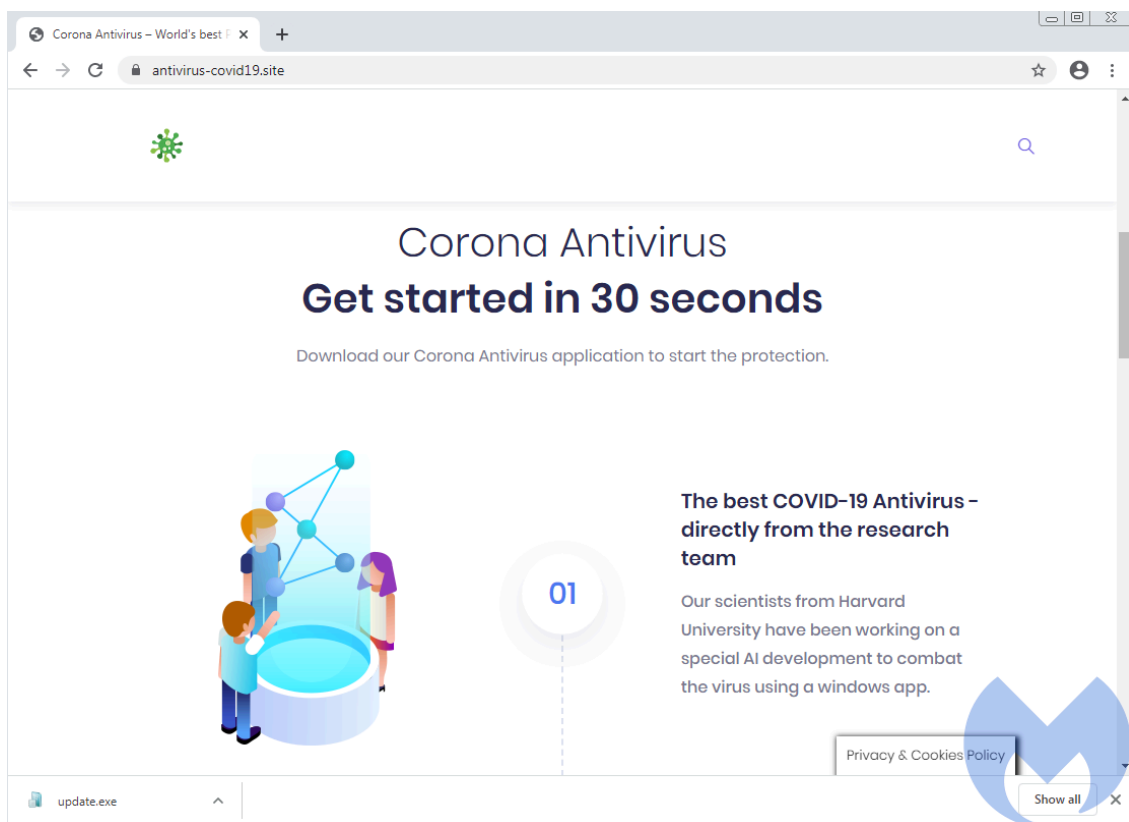
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

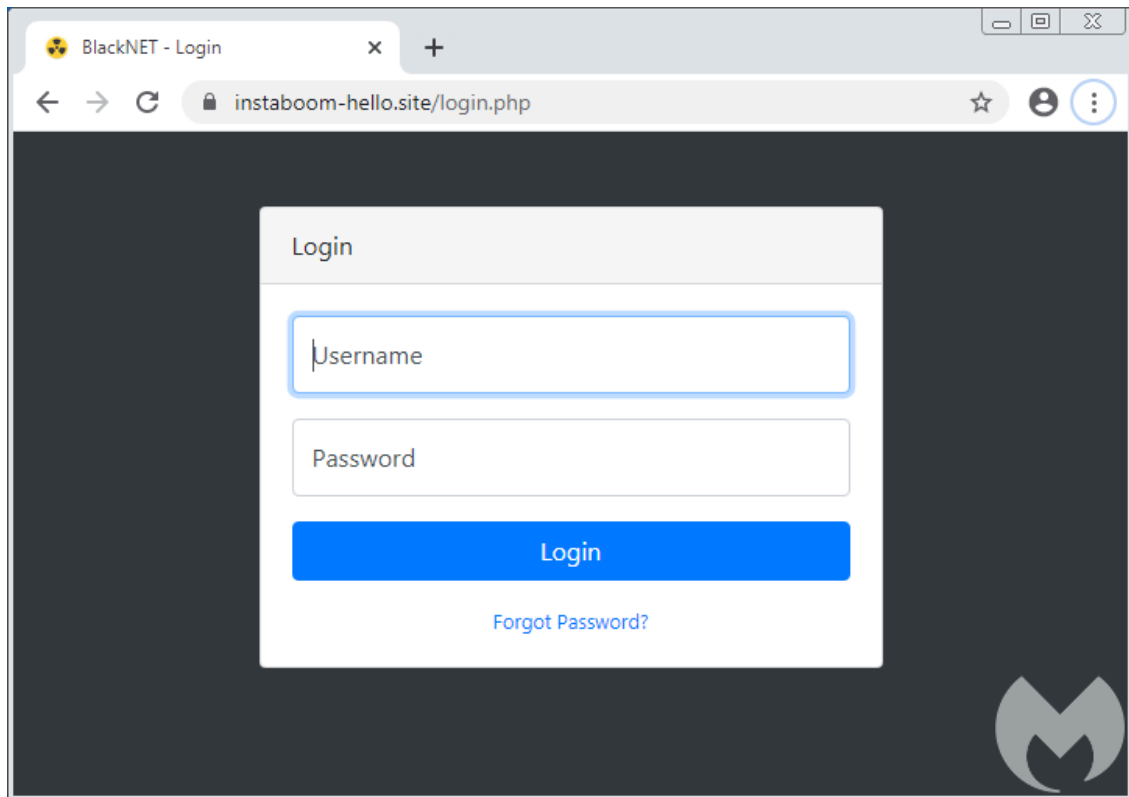


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

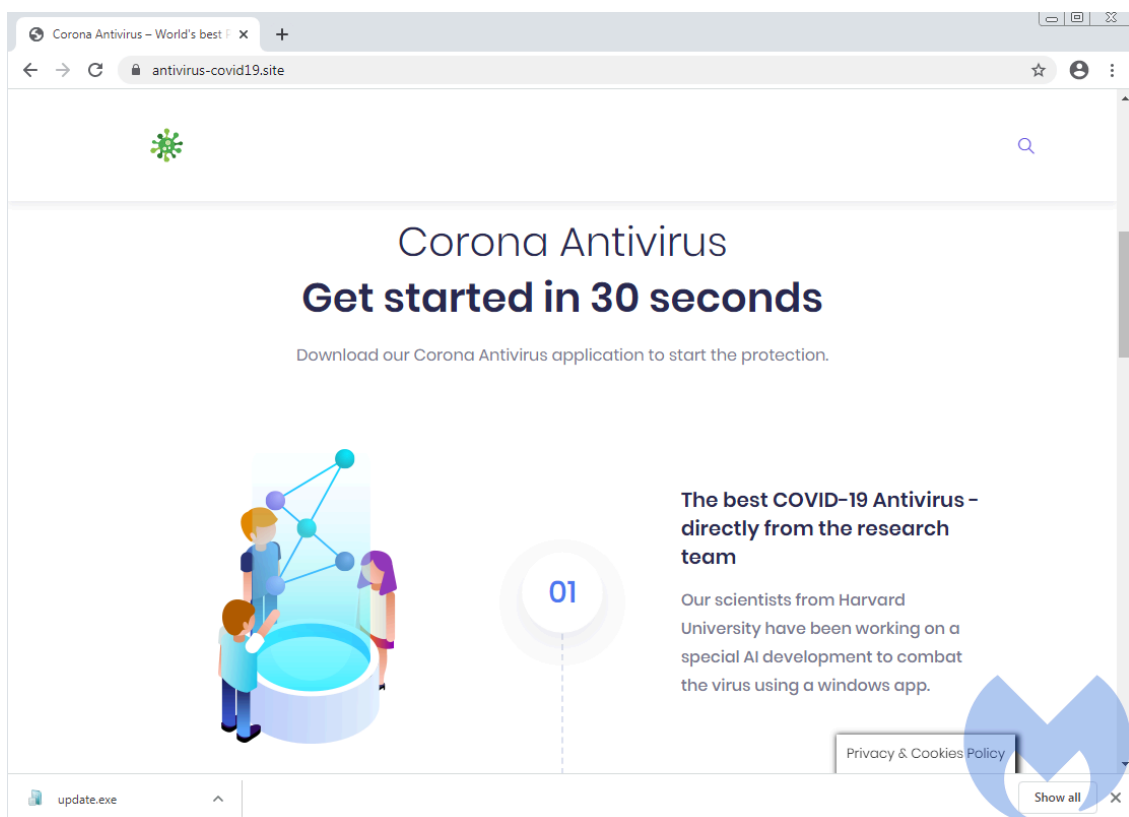
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

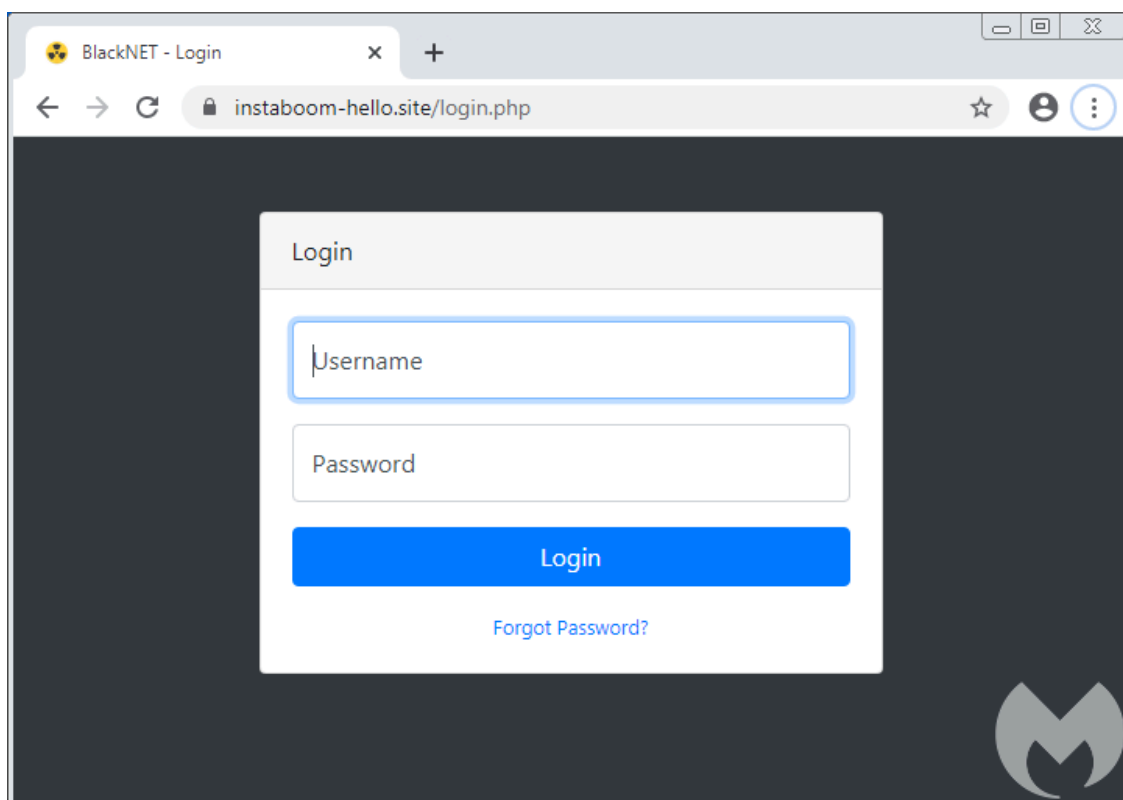
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

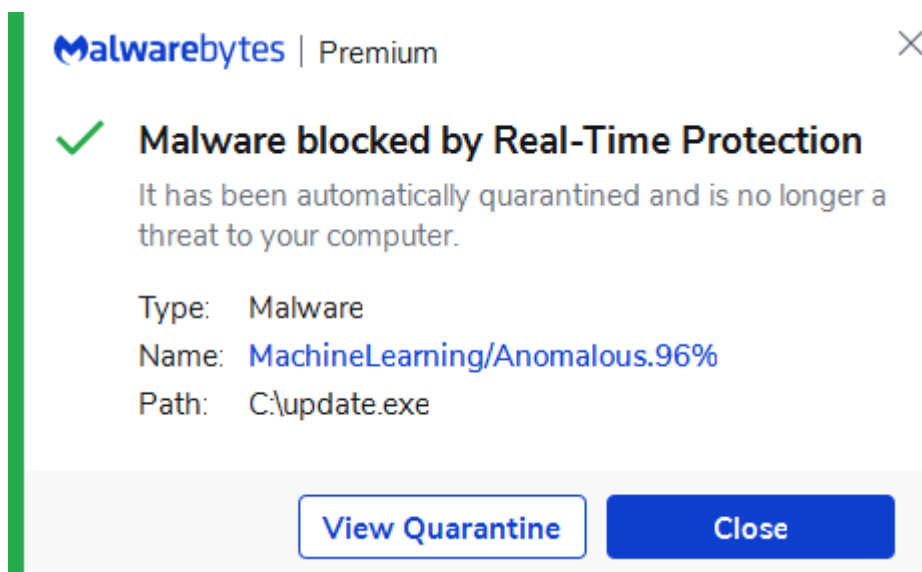
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below this is a 'Commands Center' with a dropdown menu for selecting a command and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

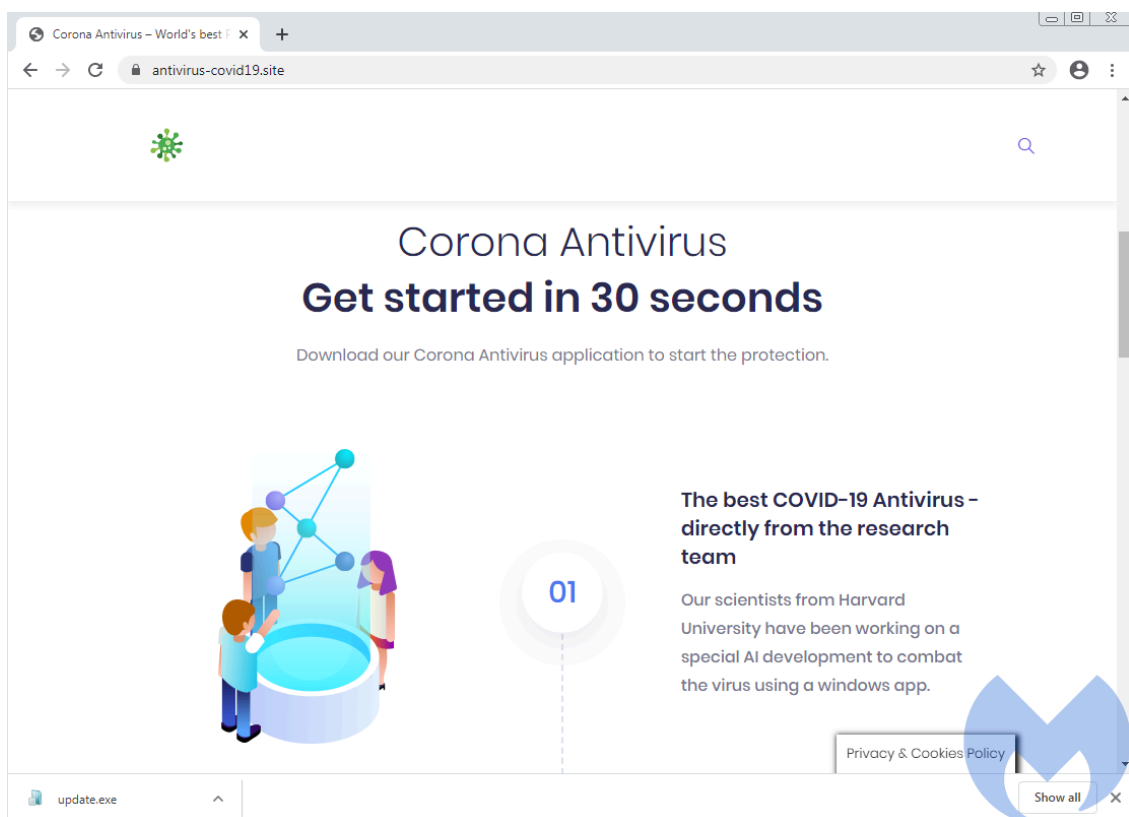
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

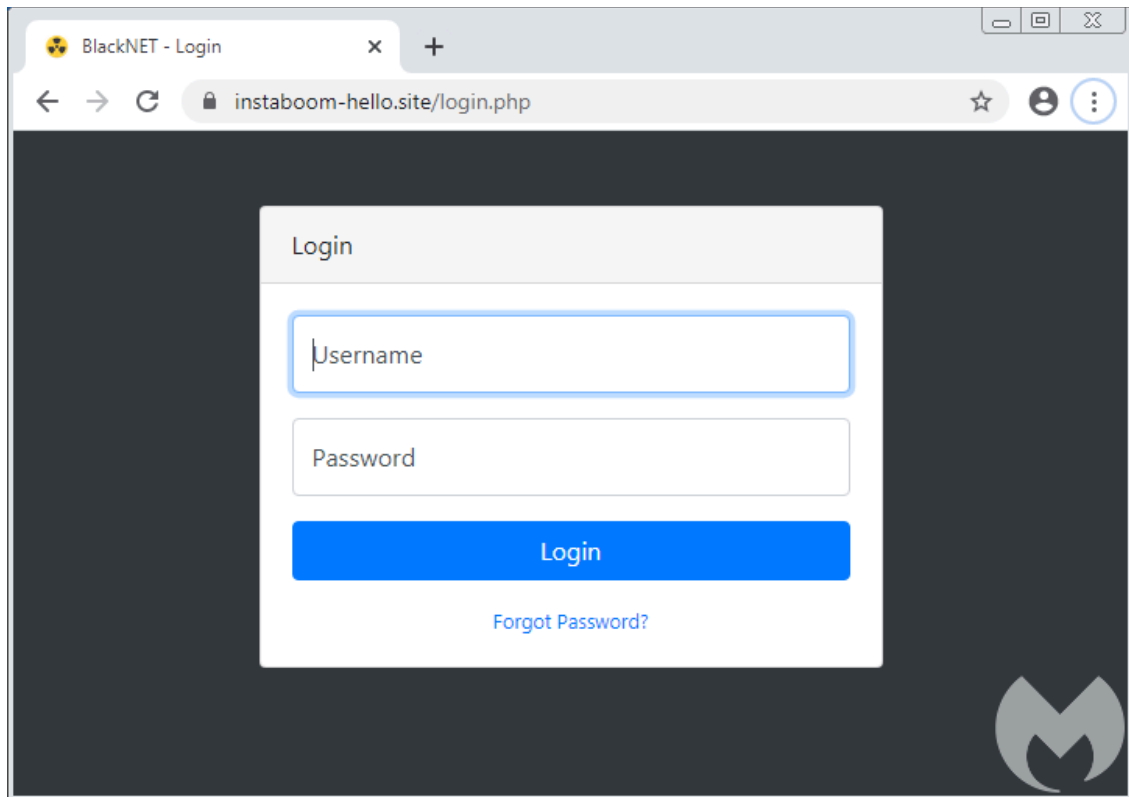



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

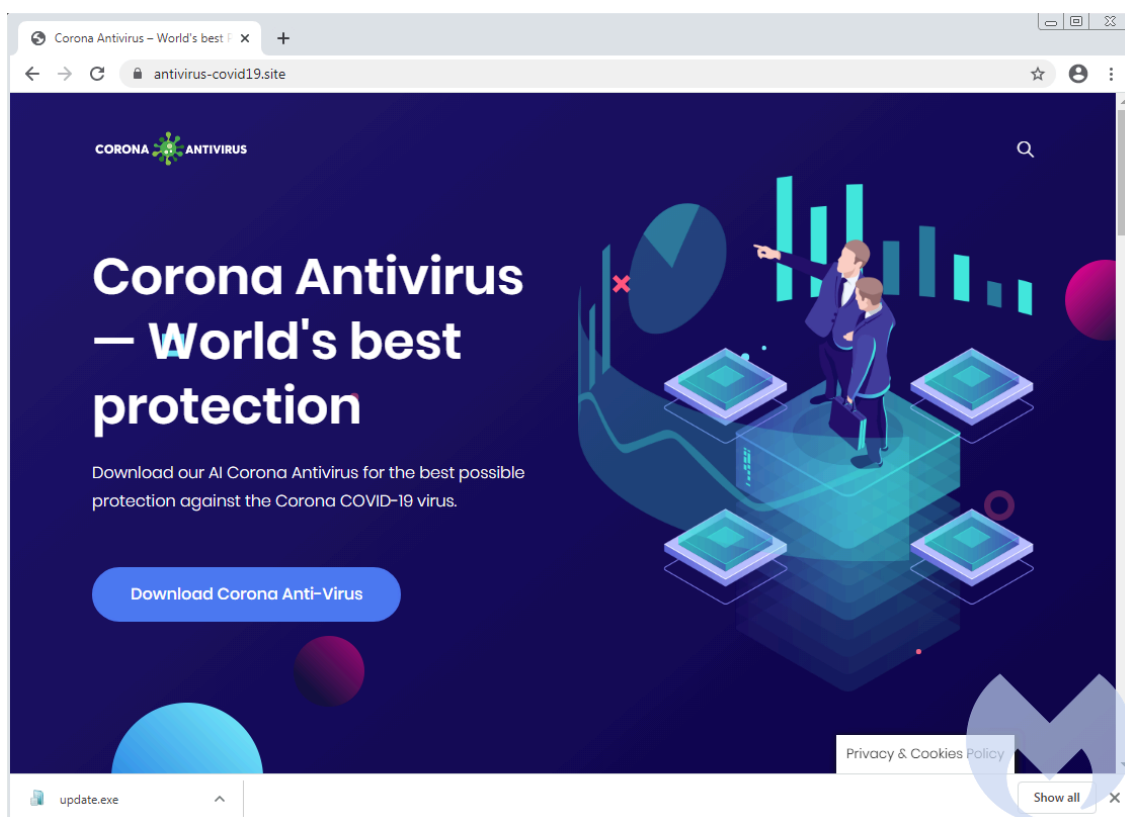
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

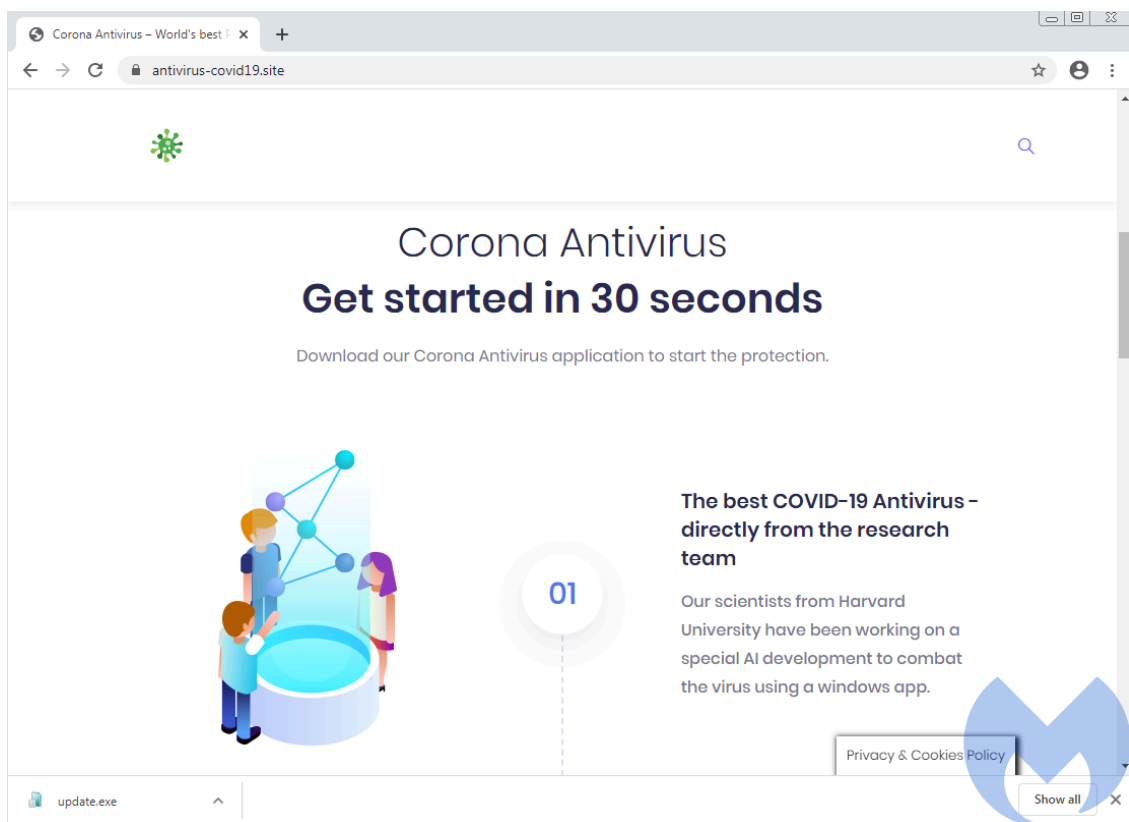
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

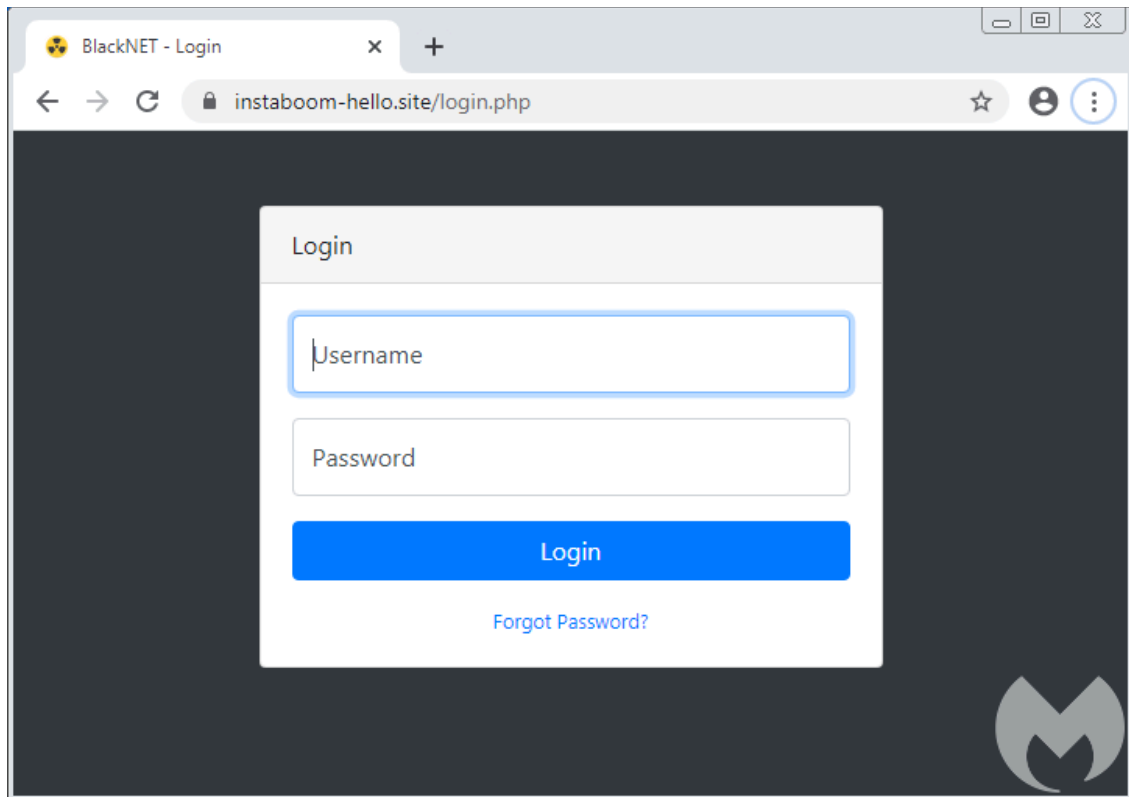


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

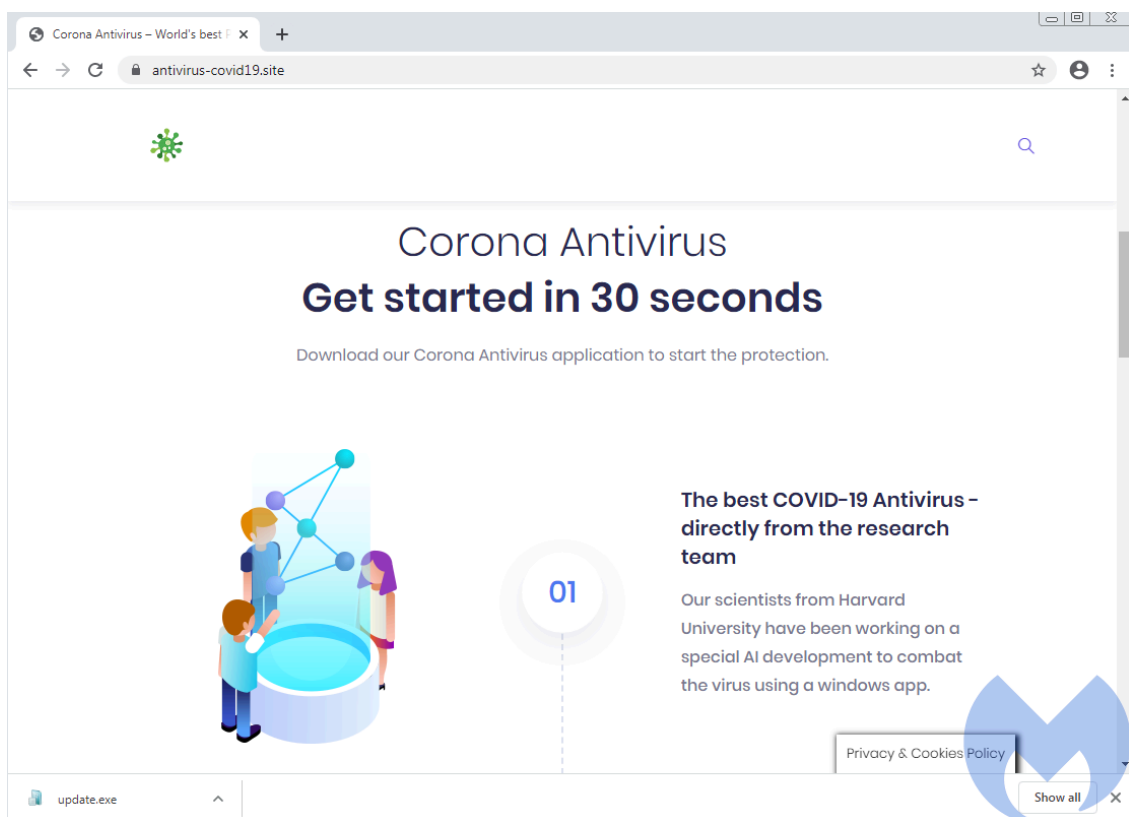
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

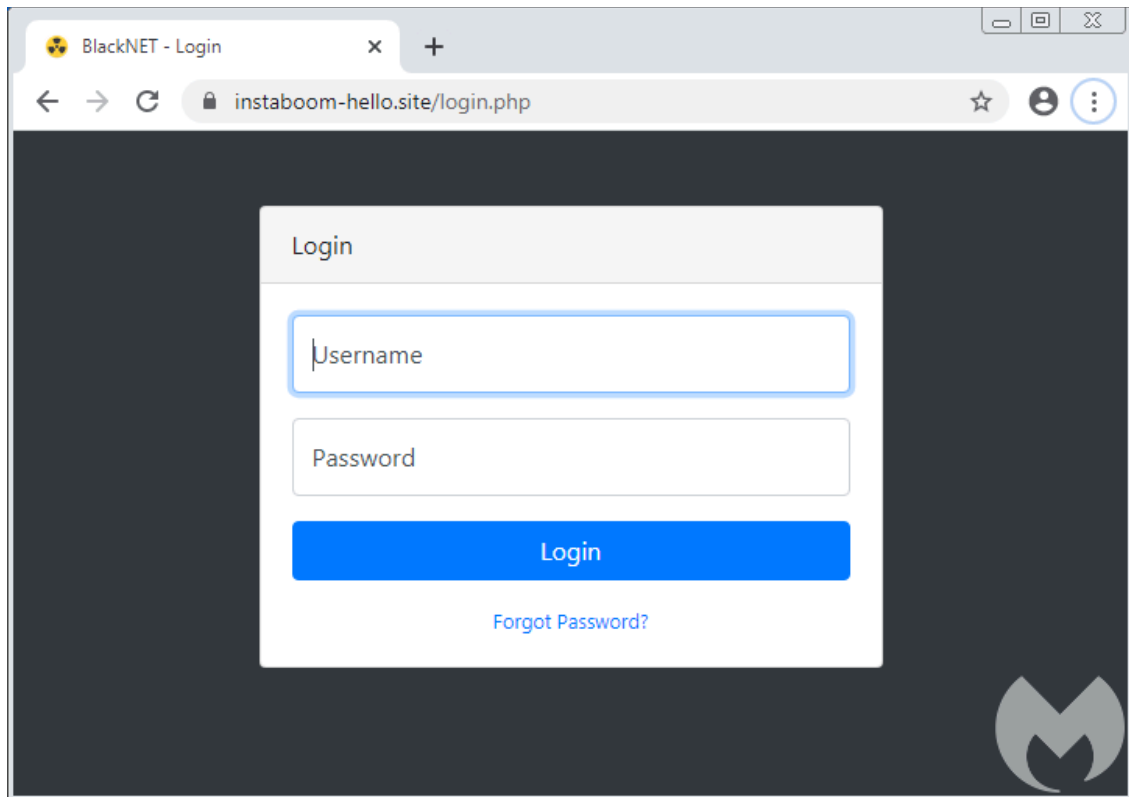


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

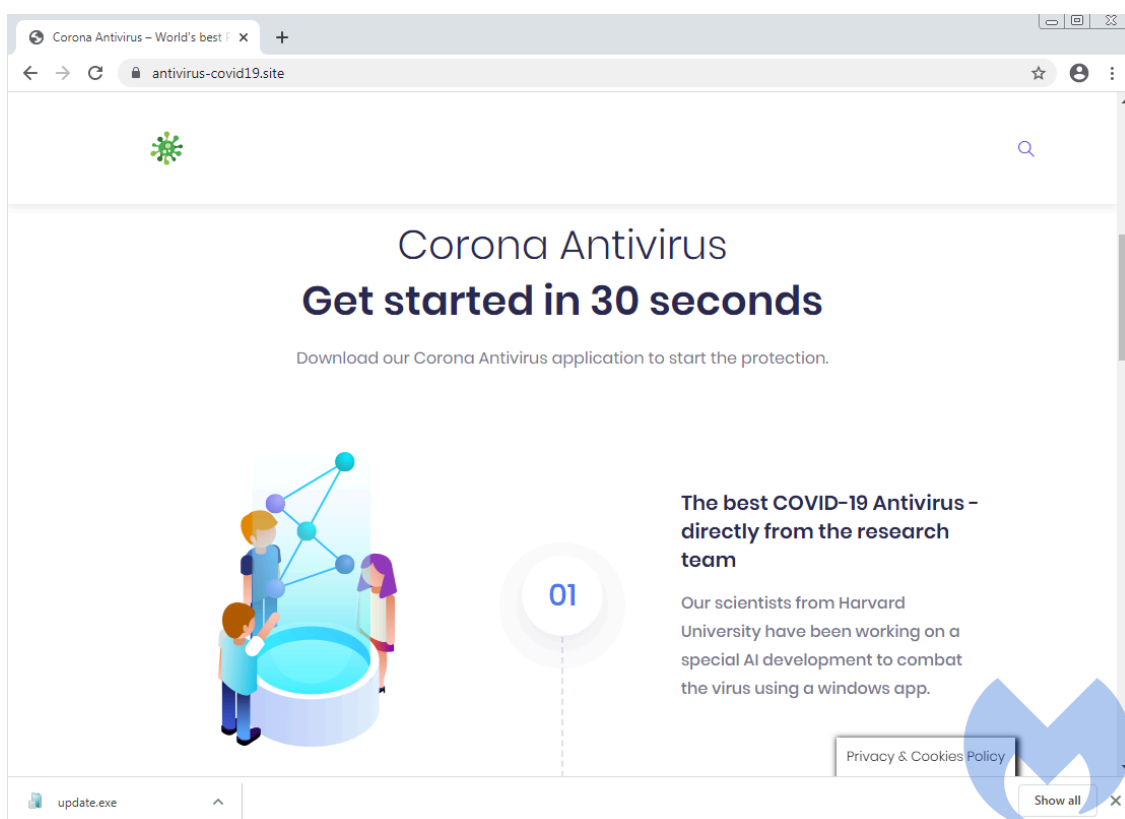
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

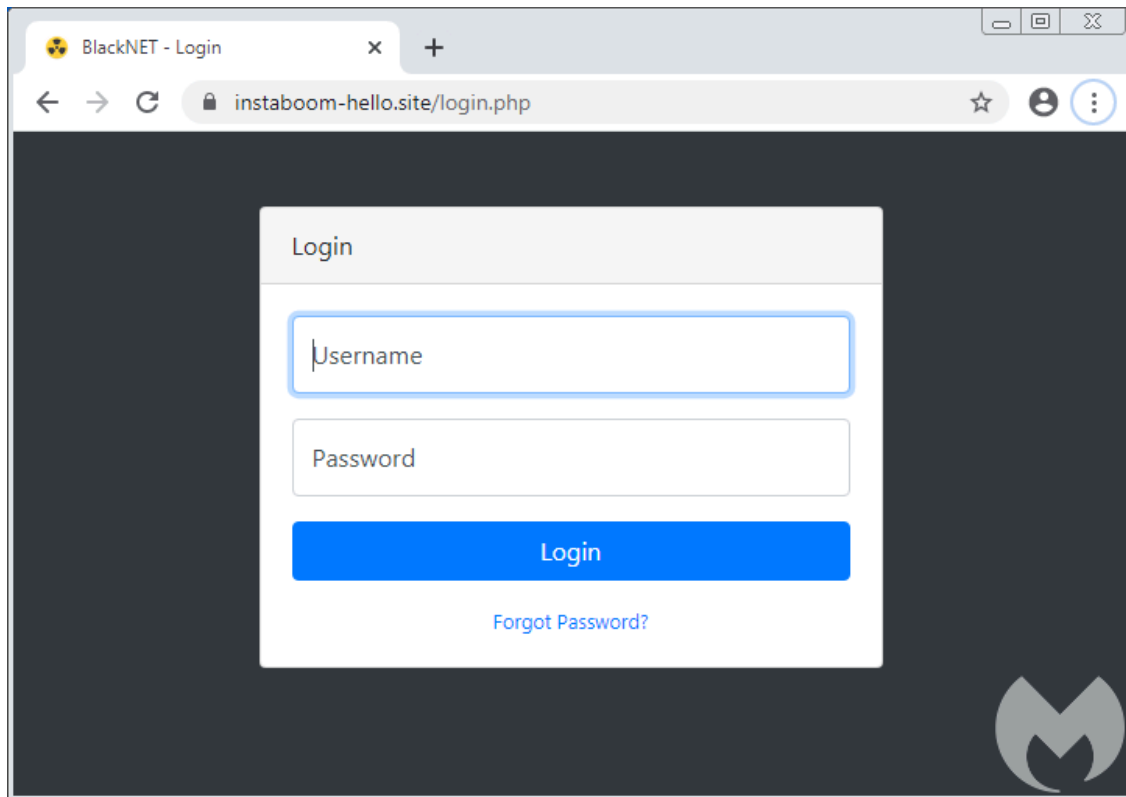


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below the navigation bar are two warning messages: "Warning! You are logging in as 'admin' please change your username for better security." and "Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from here." Below the warnings is a "Slaves Menu" section with four colored buttons: "0 Total Clients!" (blue), "0 USB Clients!" (yellow), "0 Online Clients!" (green), and "0 Offline Clients!" (red). Below the menu is a "Bot/Slaves List" section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing "No Clients Available". Below the table is a "Commands Center" section with a "Command" dropdown menu and a "Send Command" button. To the right of the commands center is a "Map Visualization" section showing a world map with a blue overlay. At the bottom of the interface is a copyright notice: "Copyright © BLACKNET by Black.Hacker - 2020".

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. At the top left is the Malwarebytes logo and "Premium" text. At the top right is a close button (X). Below the header is a green checkmark icon followed by the text "Malware blocked by Real-Time Protection". Below this is a message: "It has been automatically quarantined and is no longer a threat to your computer." Below the message are three lines of information: "Type: Malware", "Name: MachineLearning/Anomalous.96%", and "Path: C:\update.exe". At the bottom of the window are two buttons: "View Quarantine" and "Close".

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

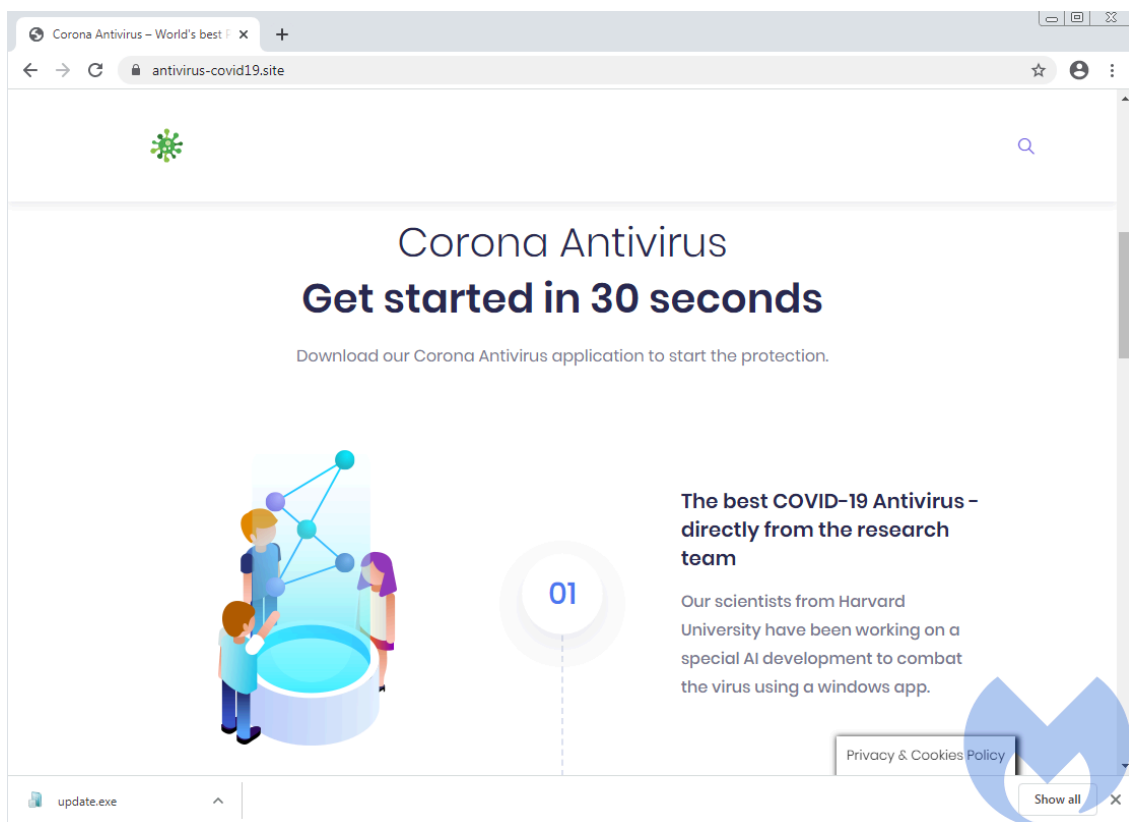
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

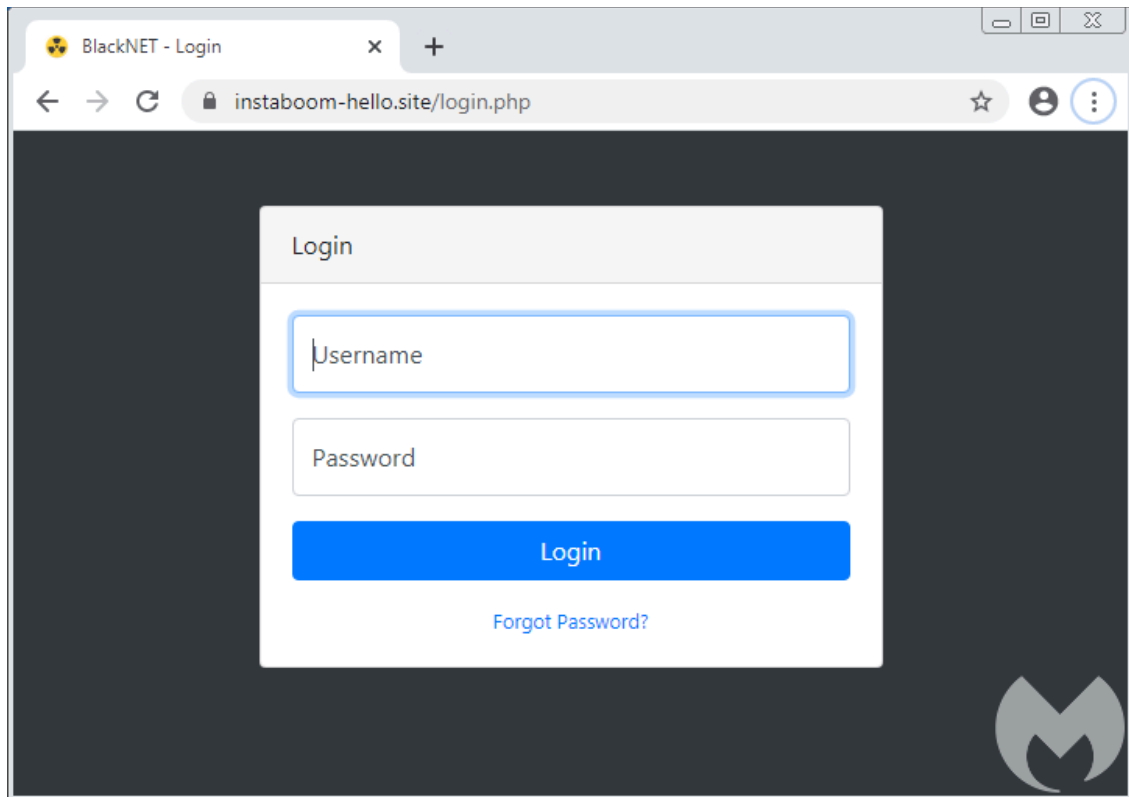


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with a blue overlay. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

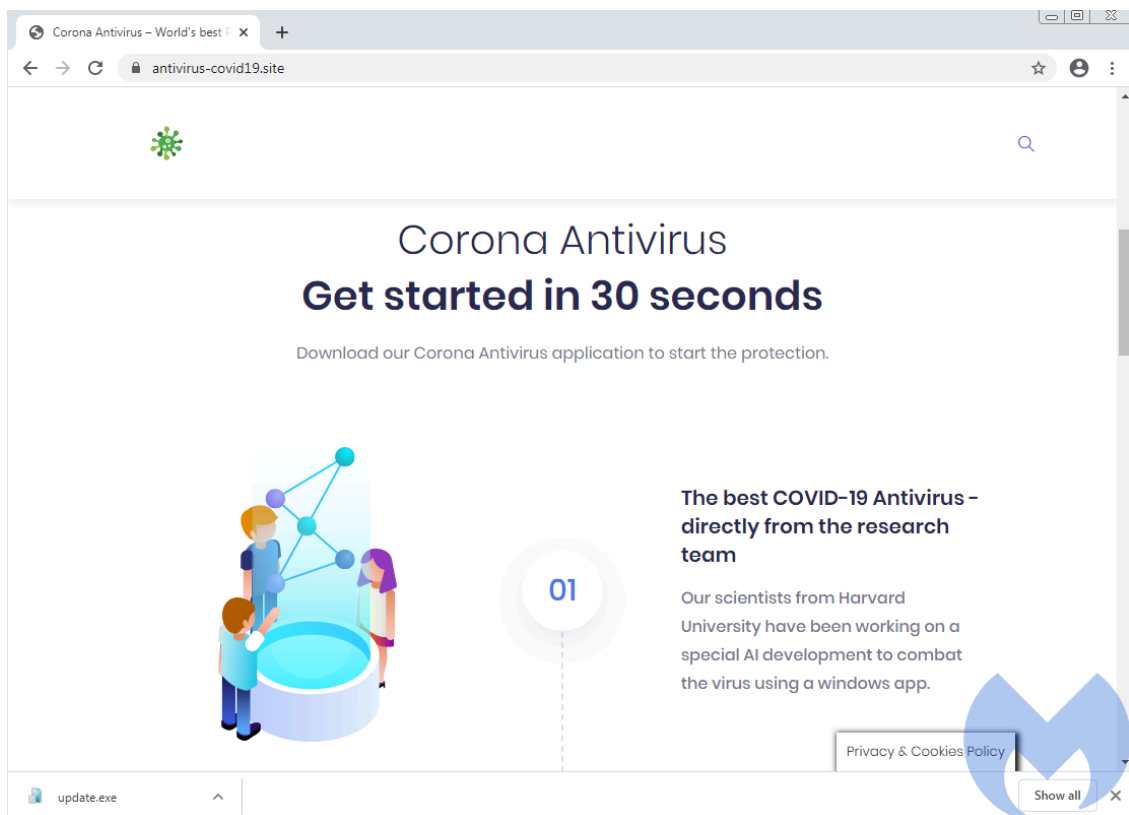
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

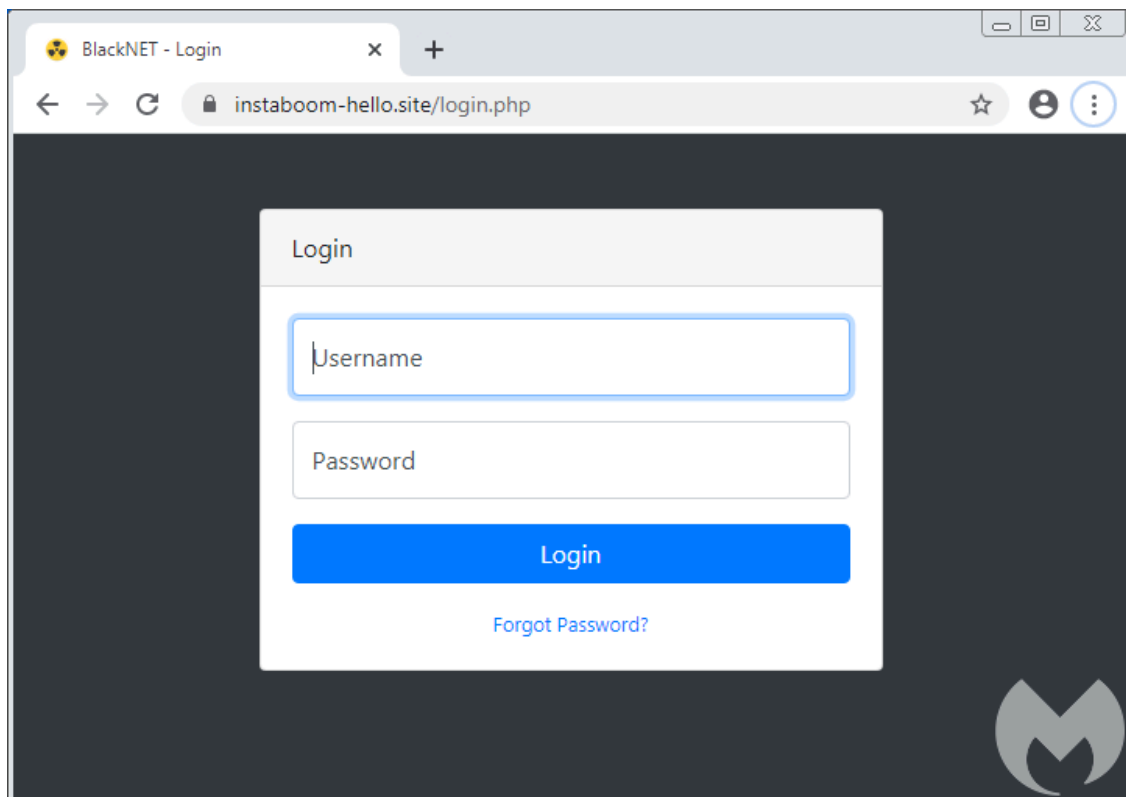
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

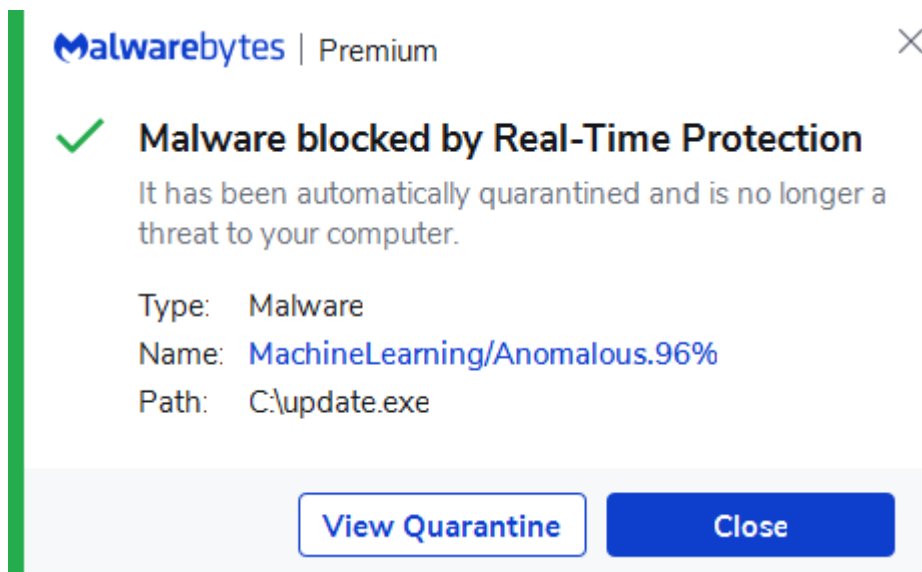
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

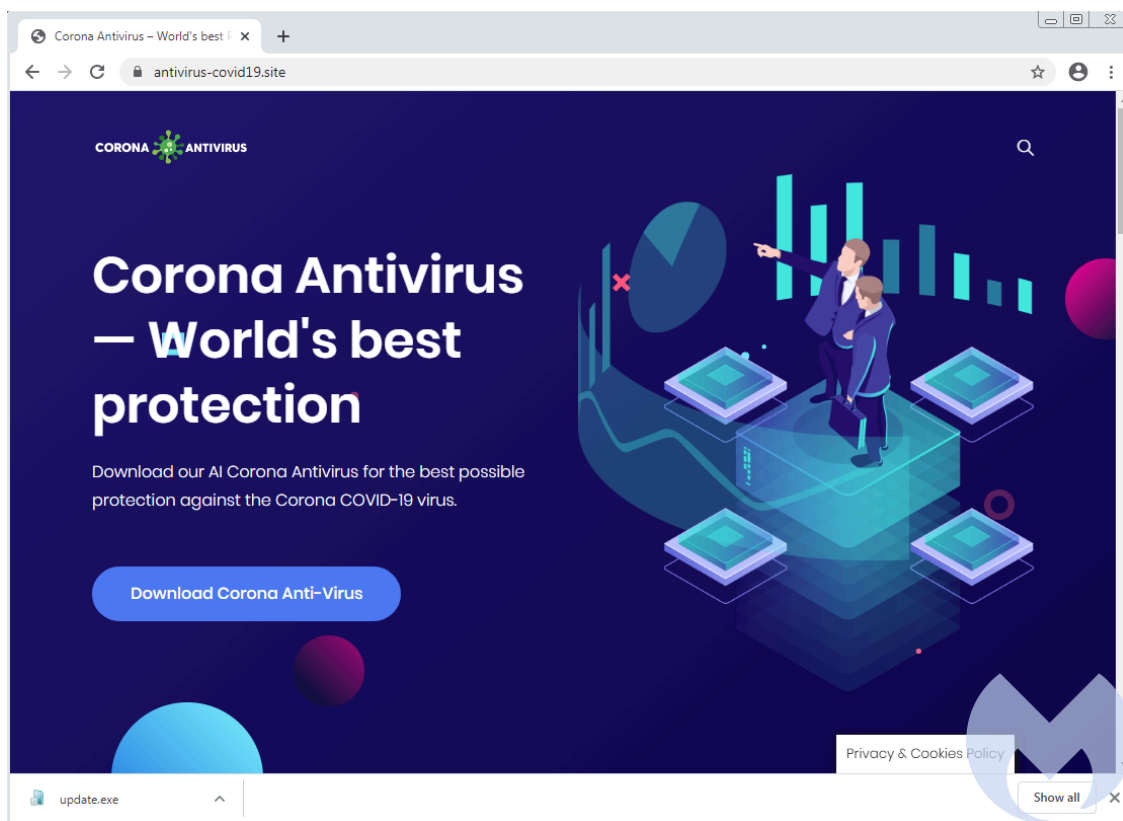
```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

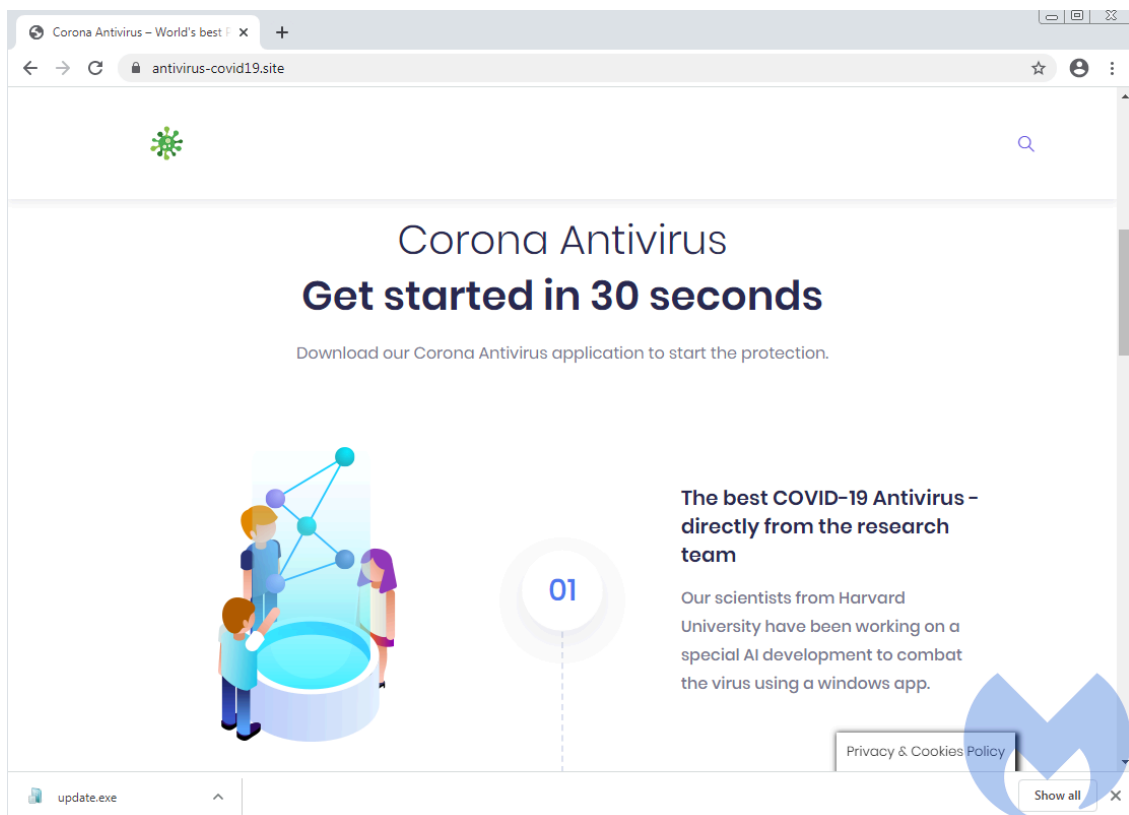
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising “Corona Antivirus -World’s best protection.” That’s right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

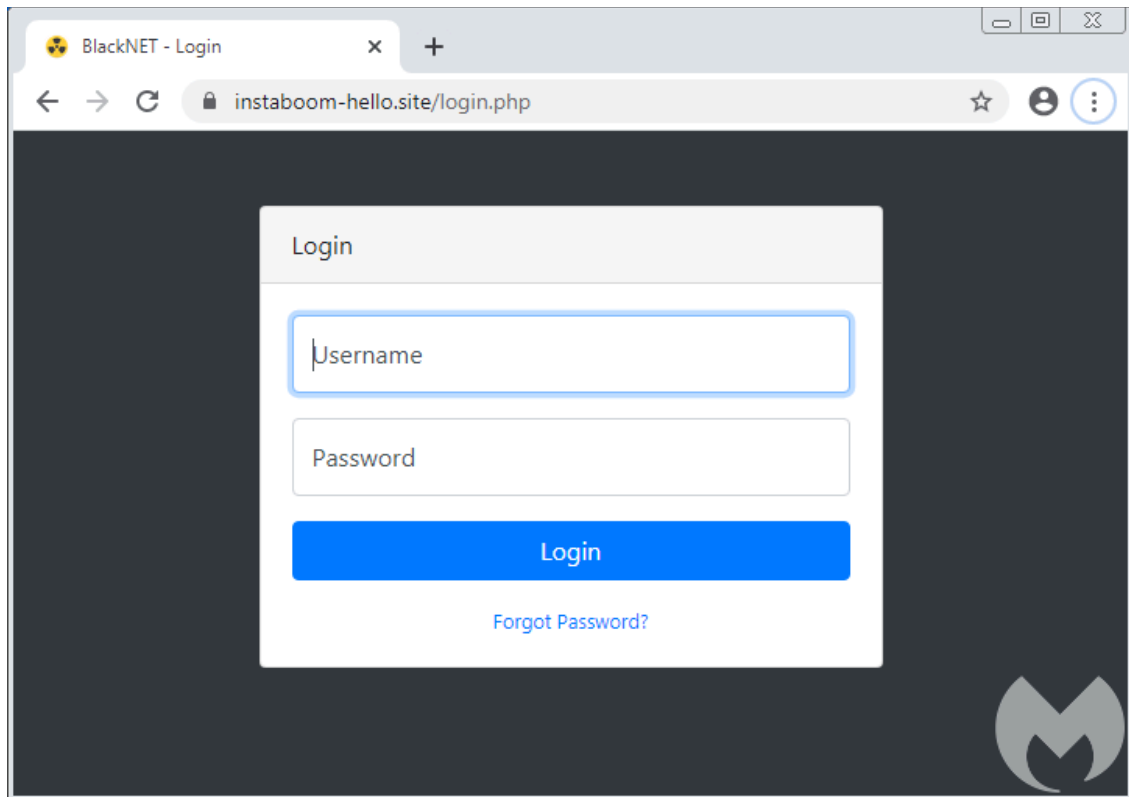


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

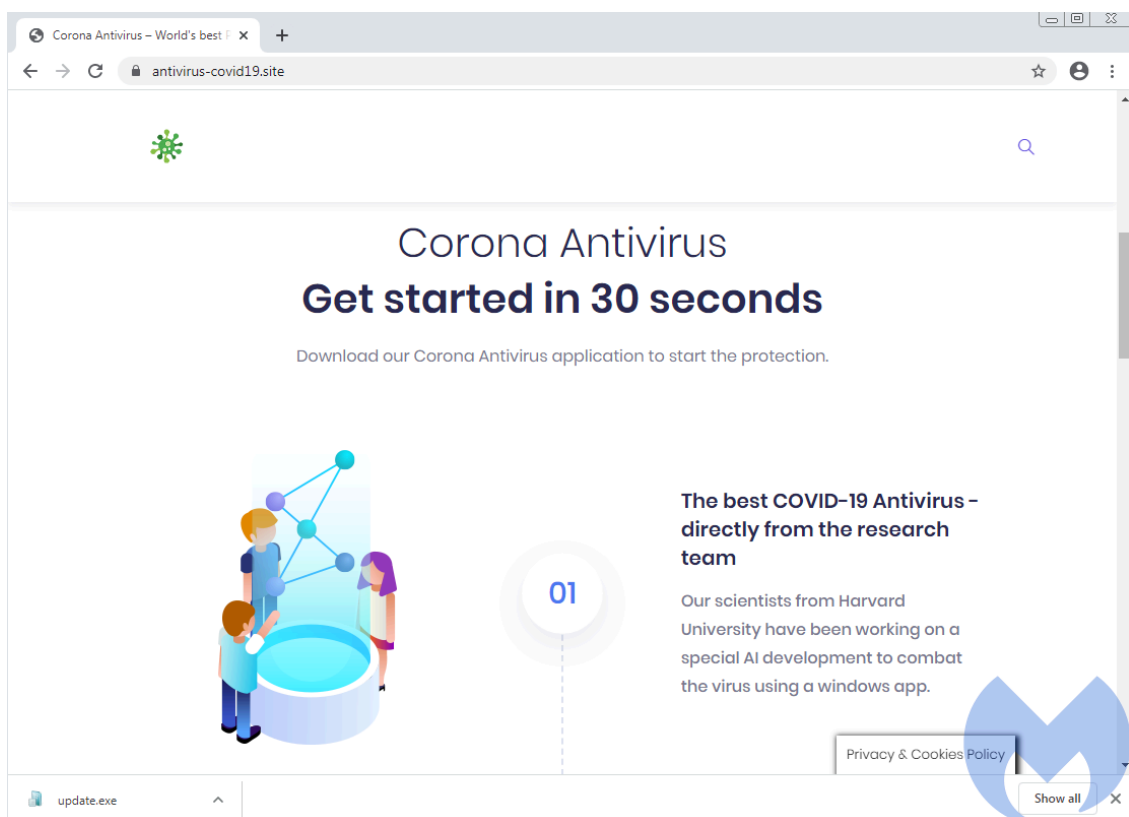
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

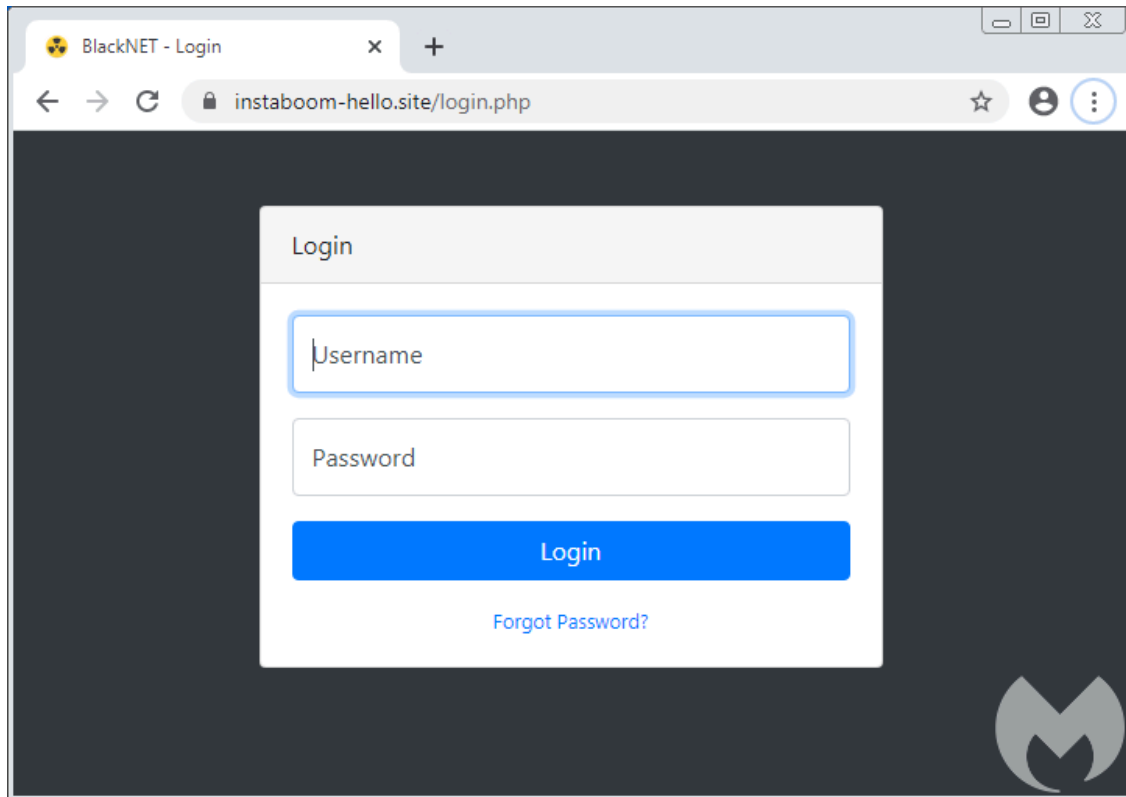


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:


```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

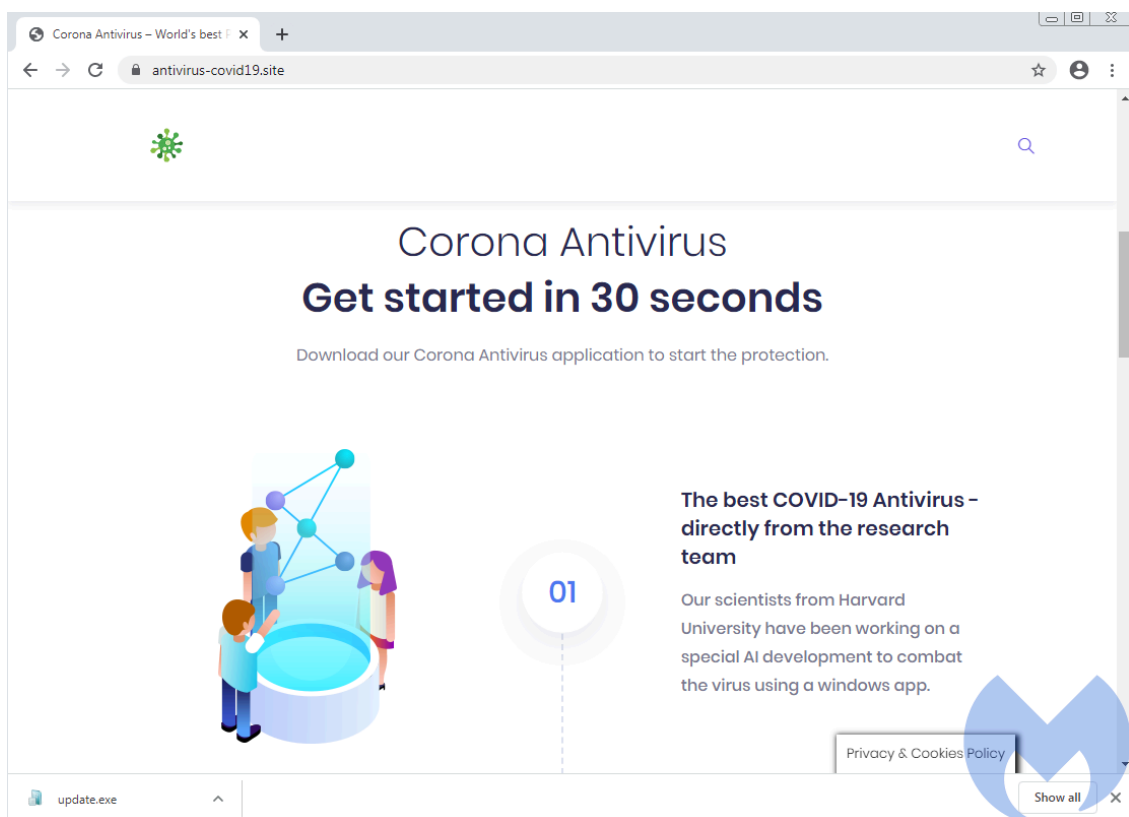
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

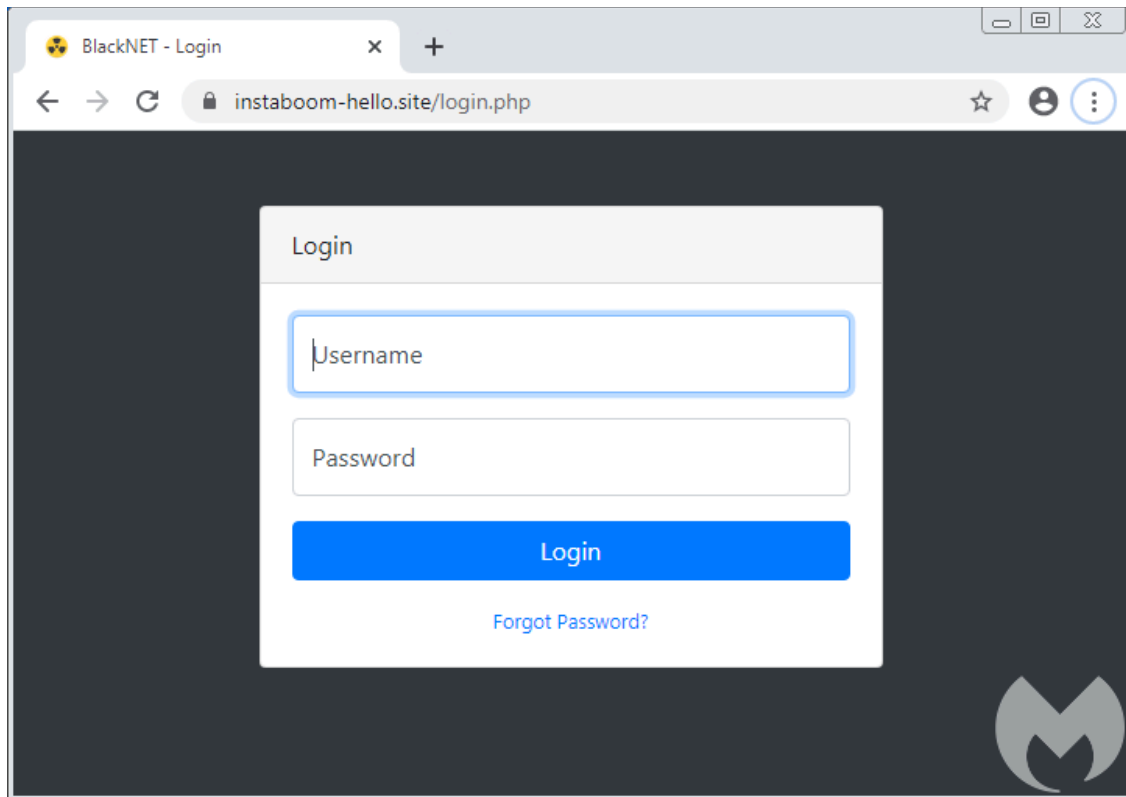


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

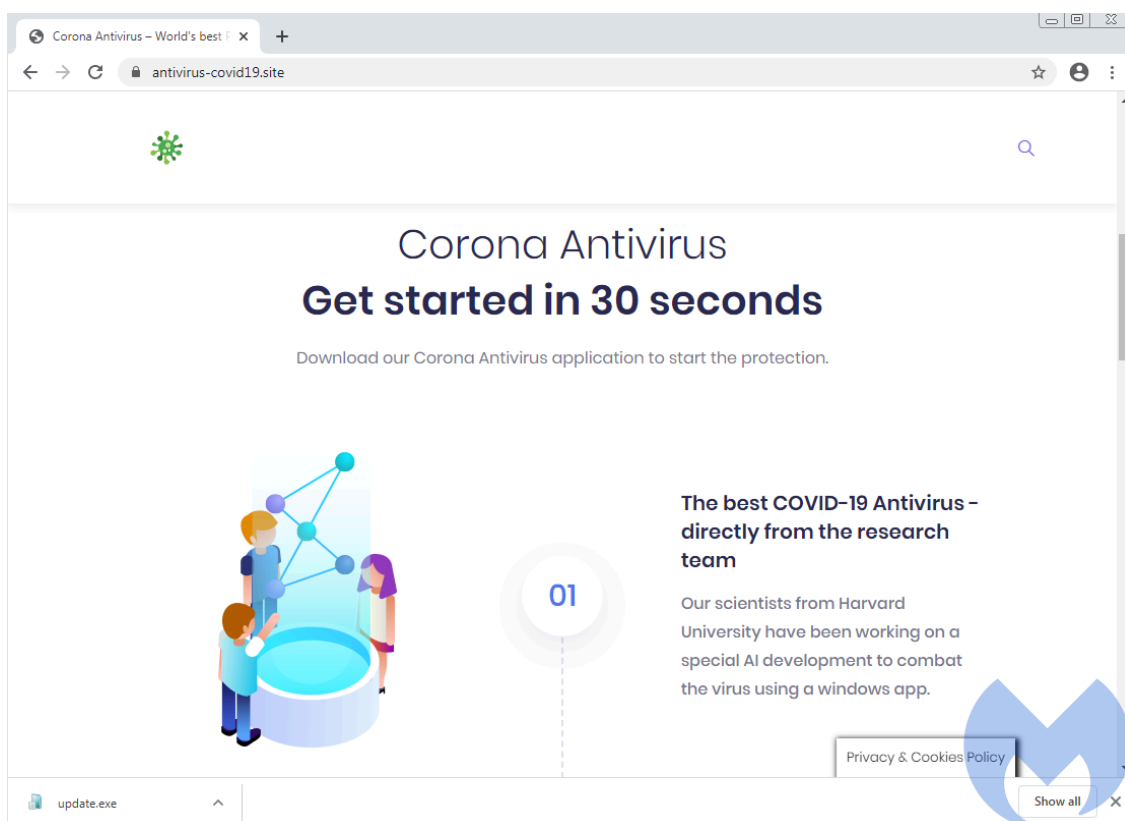
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

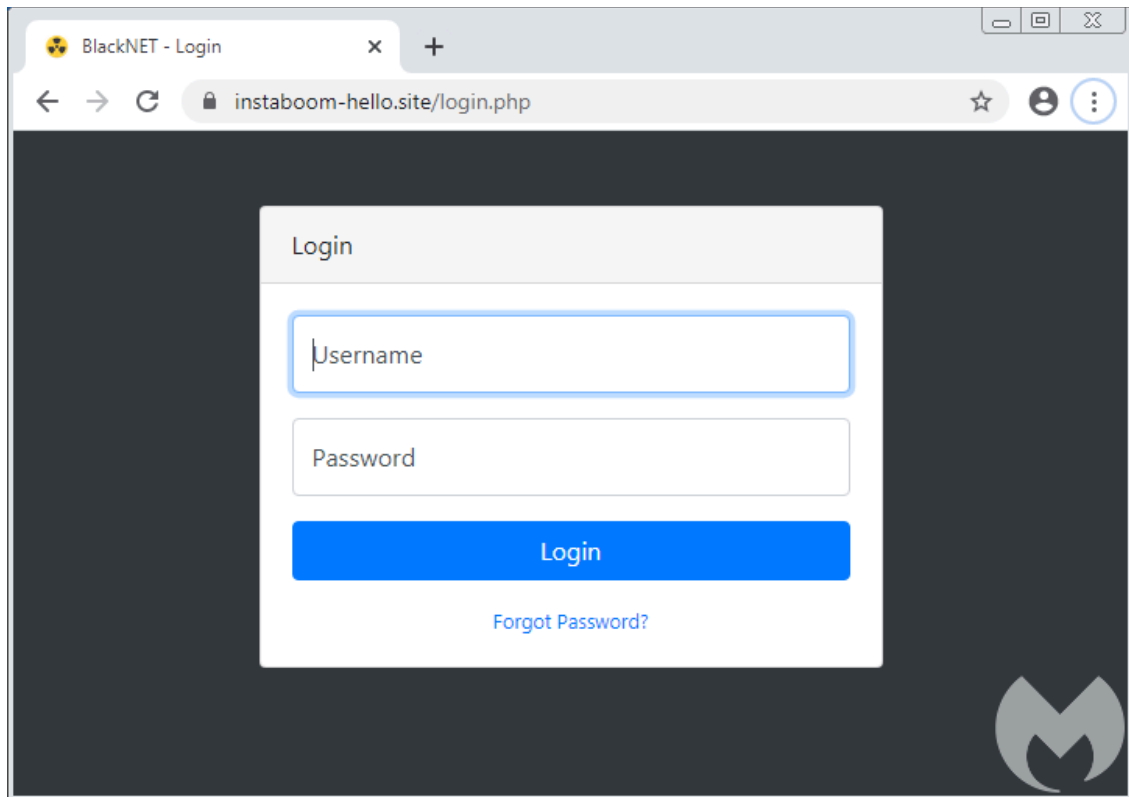


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

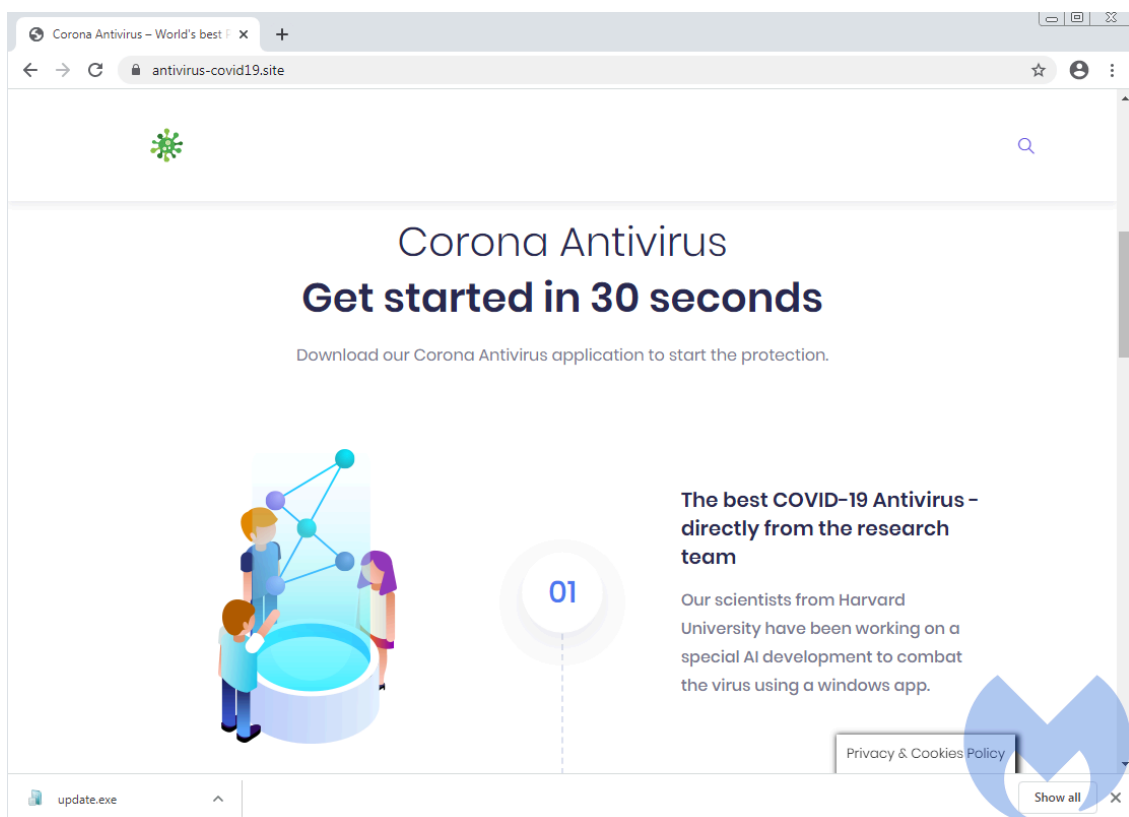
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.



Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

BlackNET Home View Logs Settings Change Password Logout

Warning! You are logging in as "admin" please change your **username** for better security.

Warning! Your account is not protected by two-factor authentication. Enable two-factor authentication now from [here](#).

Slaves Menu

0 Total Clients! 0 USB Clients! 0 Online Clients! 0 Offline Clients!

Bot/Slaves List

Show 10 entries Search:

☐	Victim ID	IP Address	Computer Name	User Status	Country	OS	Installed Date	Antivirus	Status
No Clients Available									

Showing 0 to 0 of 0 entries Previous Next

Commands Center

Command Execute

Select Command Send Command

Map Visualization

Copyright © BLACKNET by Black.Hacker - 2020

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

Malwarebytes | Premium

✓ **Malware blocked by Real-Time Protection**

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware

Name: MachineLearning/Anomalous.96%

Path: C:\update.exe

View Quarantine Close

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

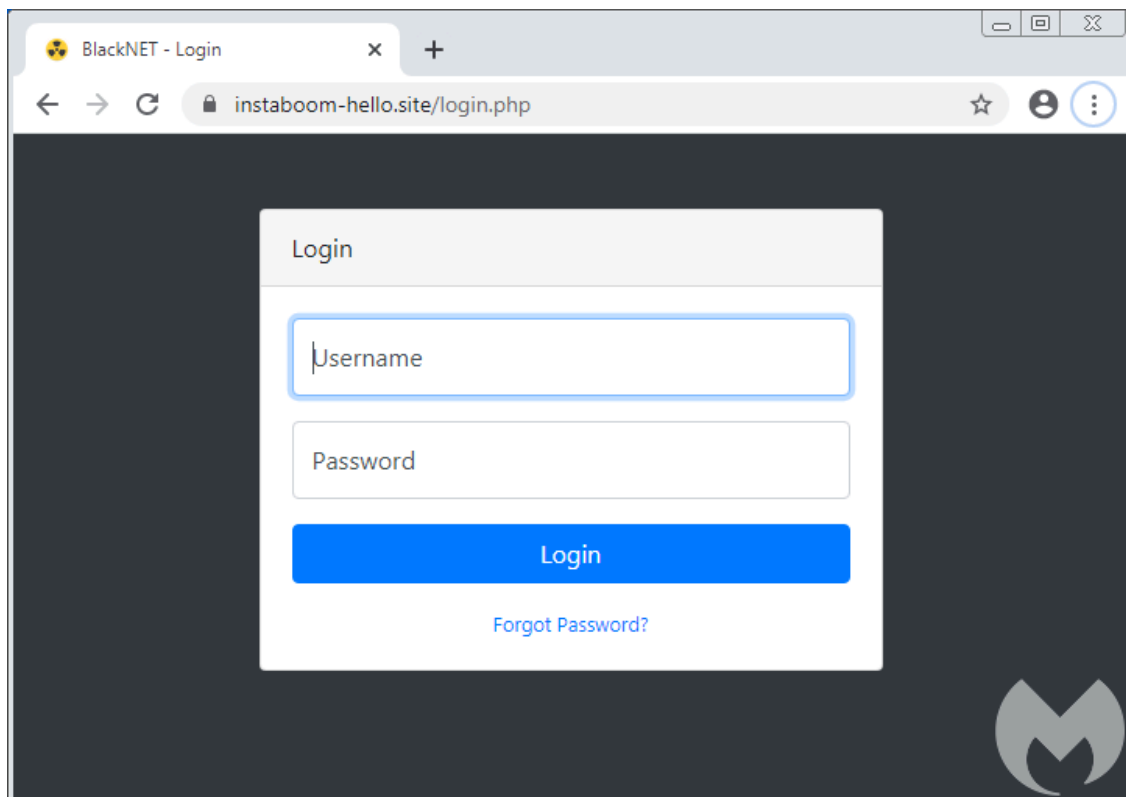
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

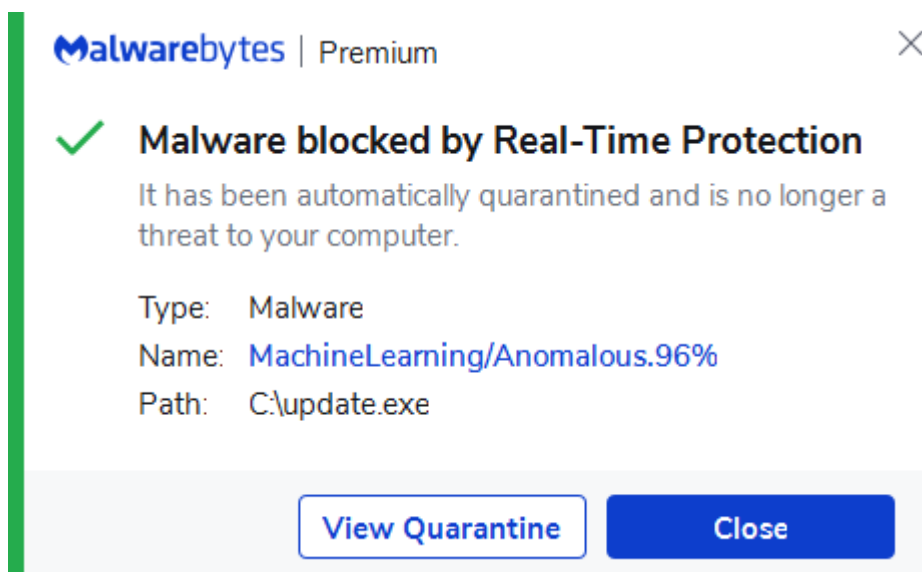
The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored buttons: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a message 'No Clients Available'. Below this is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' section showing a world map with blue dots representing clients. The footer contains the copyright notice 'Copyright © BLACKNET by Black.Hacker - 2020' and a large blue stylized 'M' logo.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

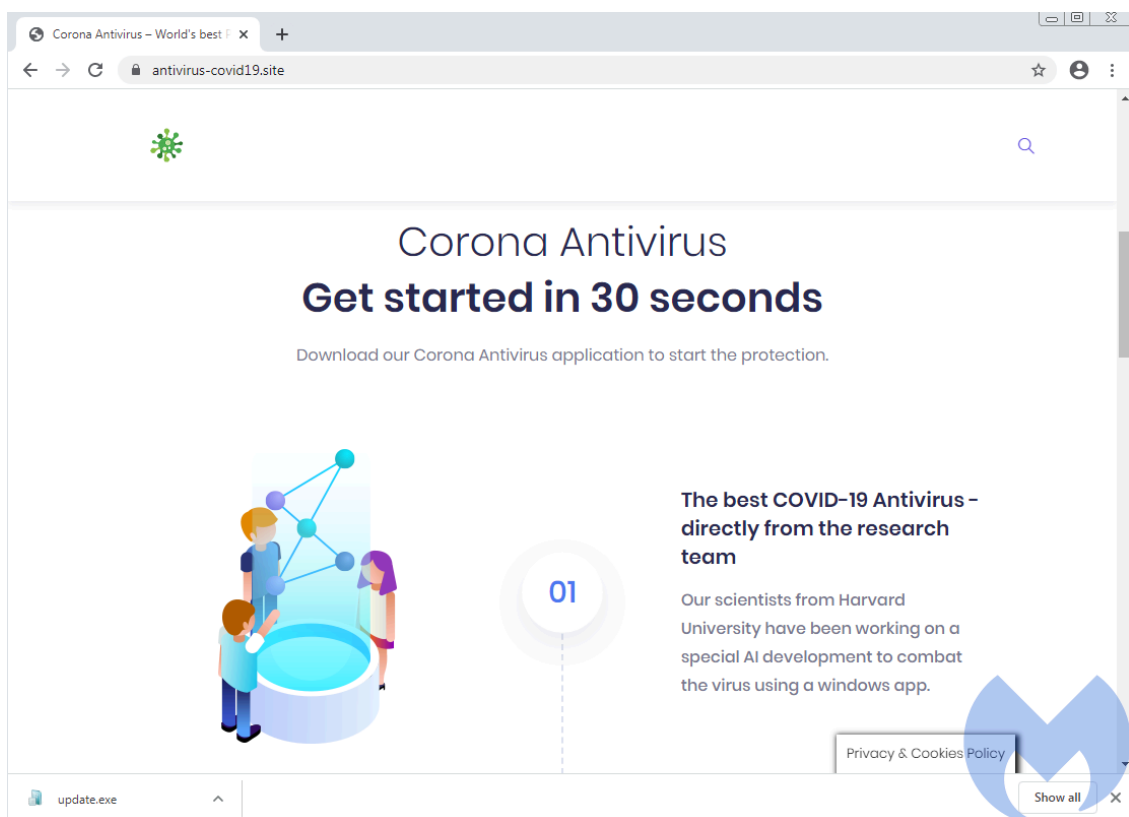
C2 panel

```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

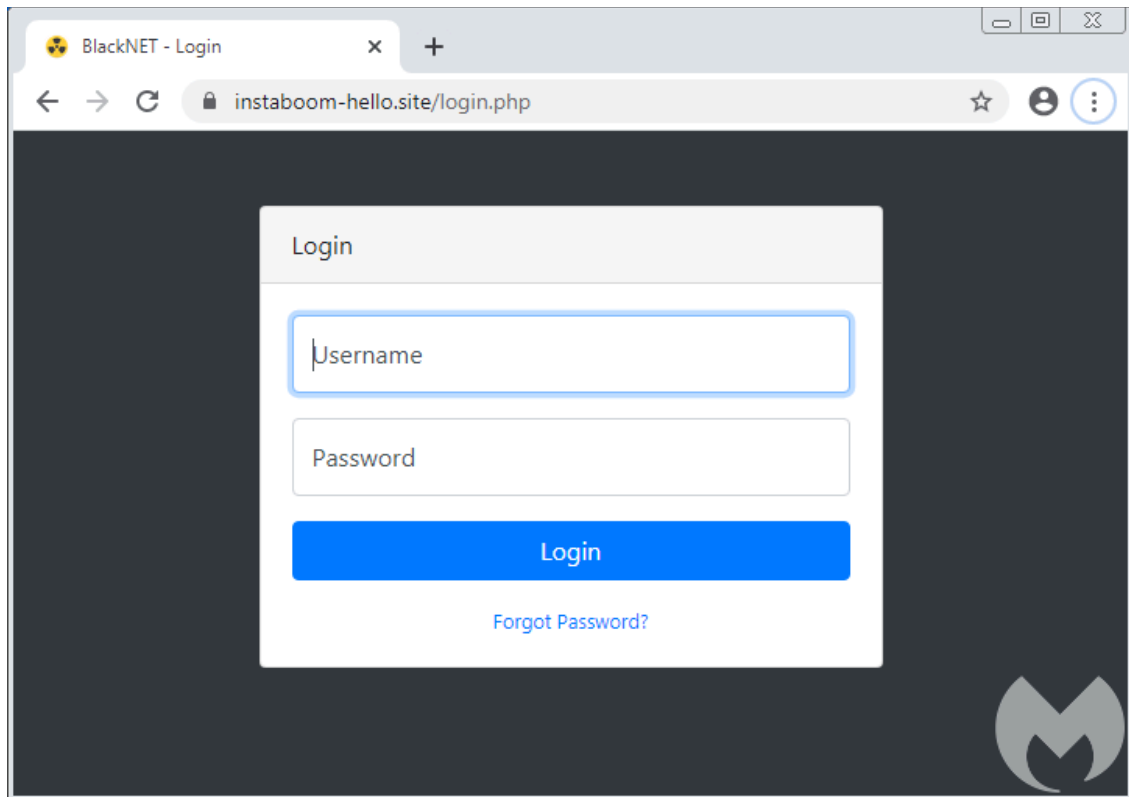


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with a few blue dots. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

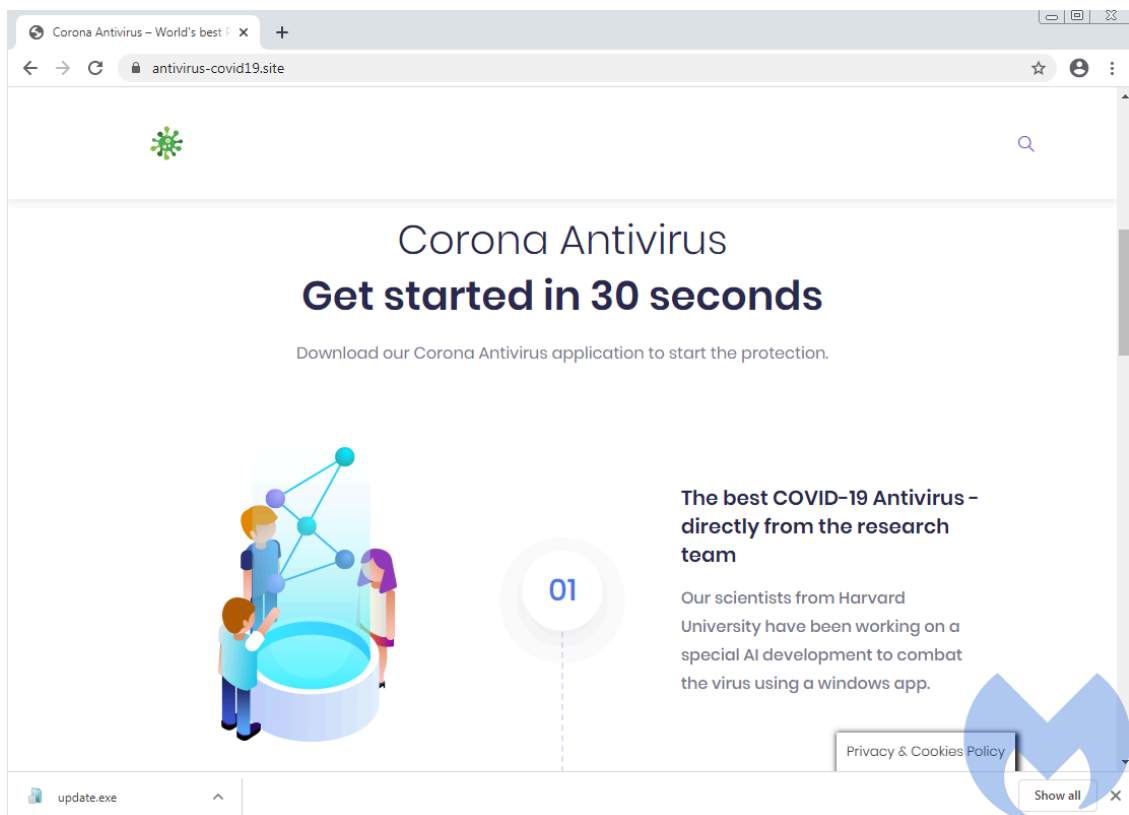
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

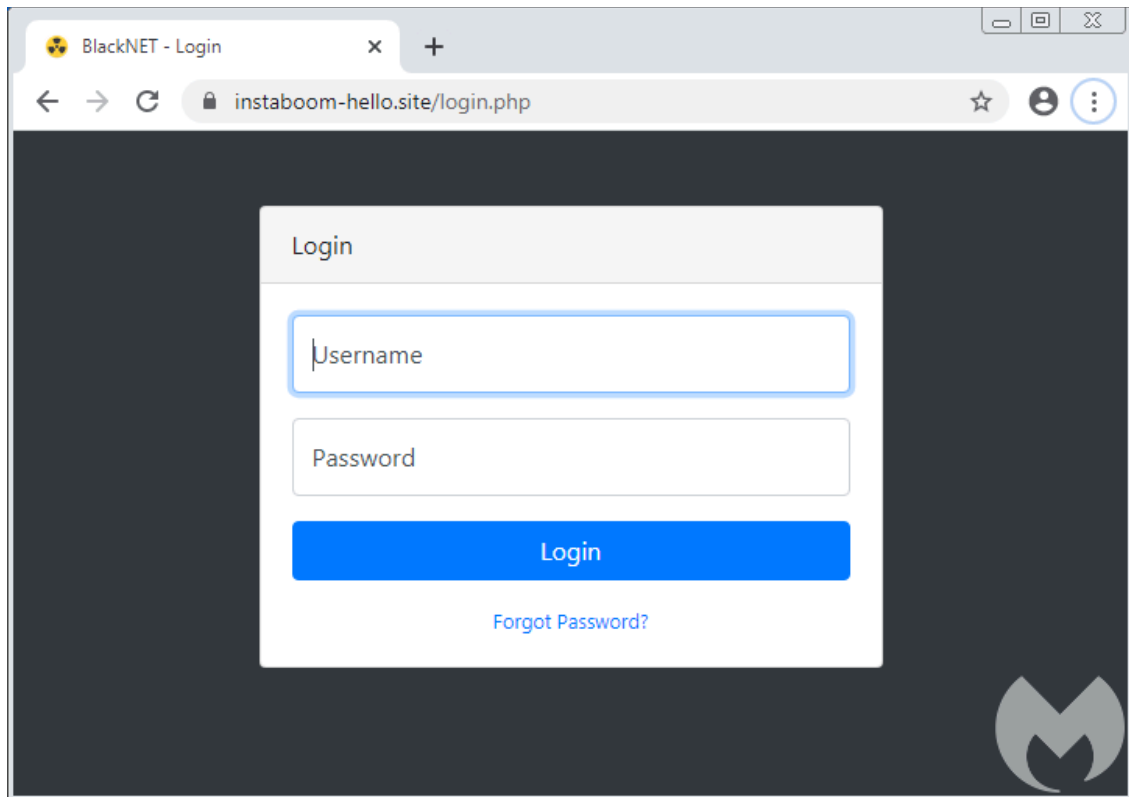


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning messages are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a table header including Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table is currently empty, showing 'No Clients Available'. To the right of the table is a 'Map Visualization' showing a world map with blue dots representing clients. At the bottom left, there's a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

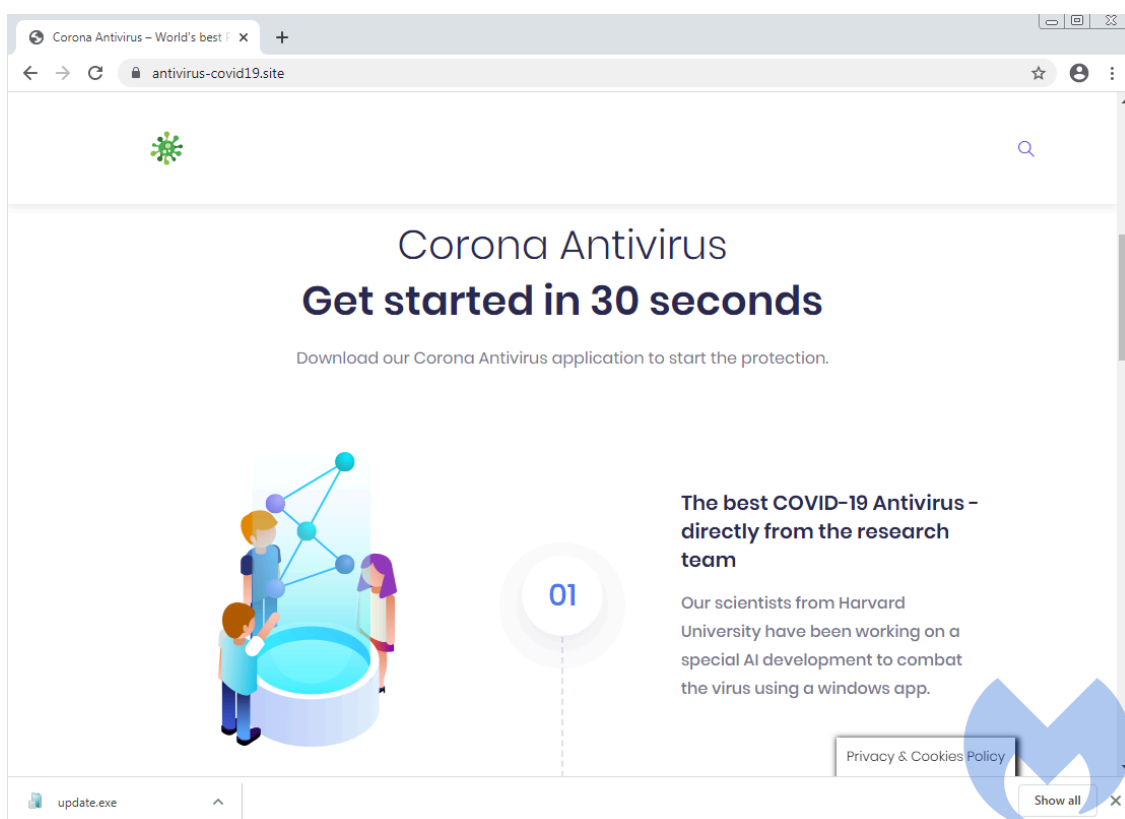
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

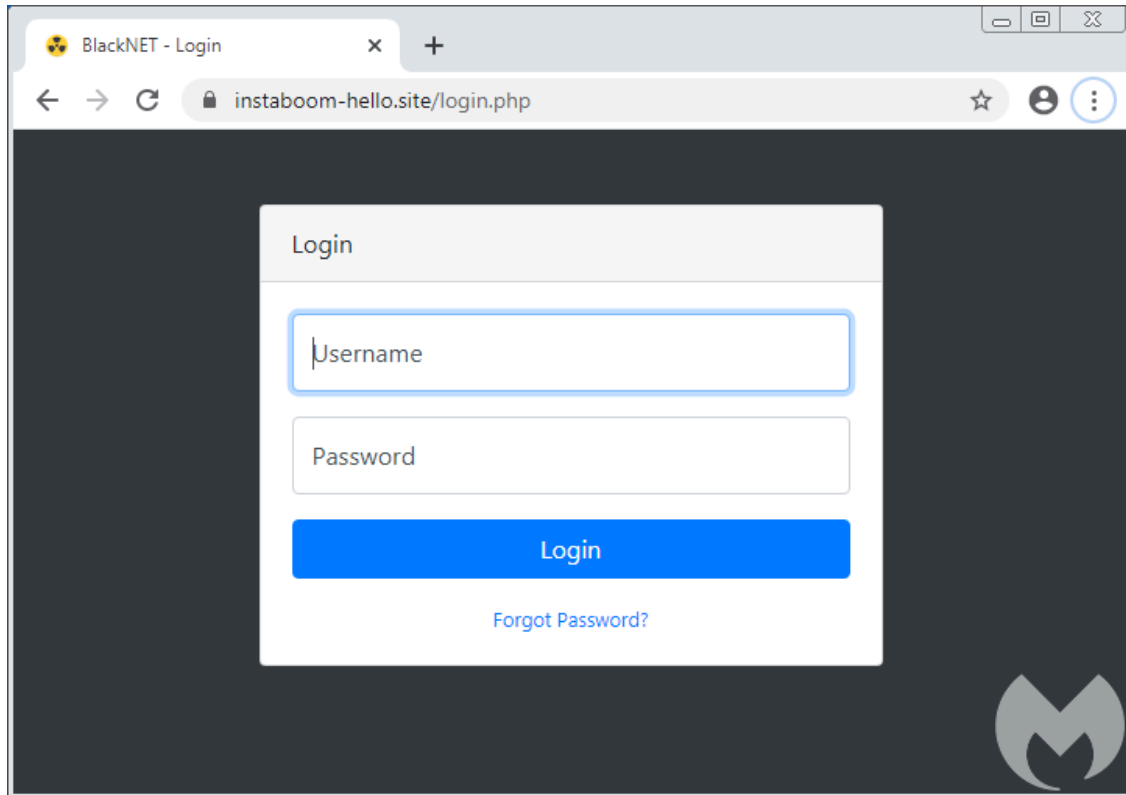


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

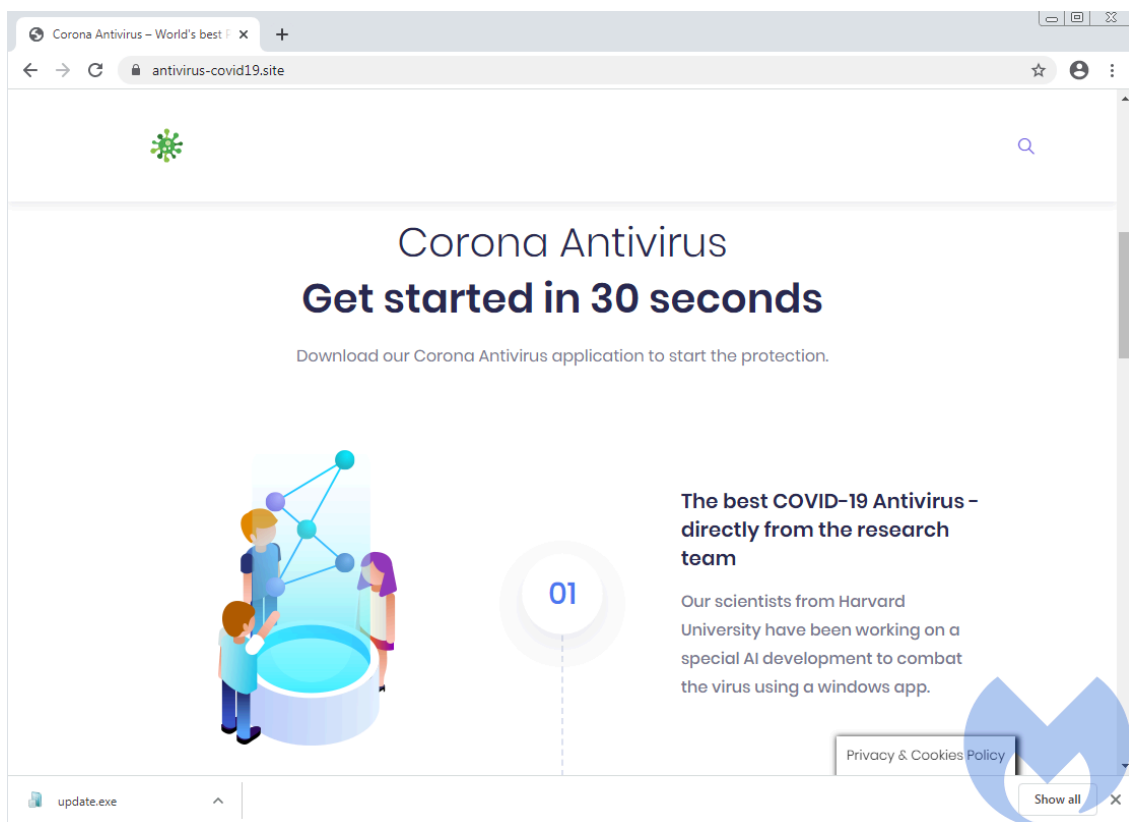
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

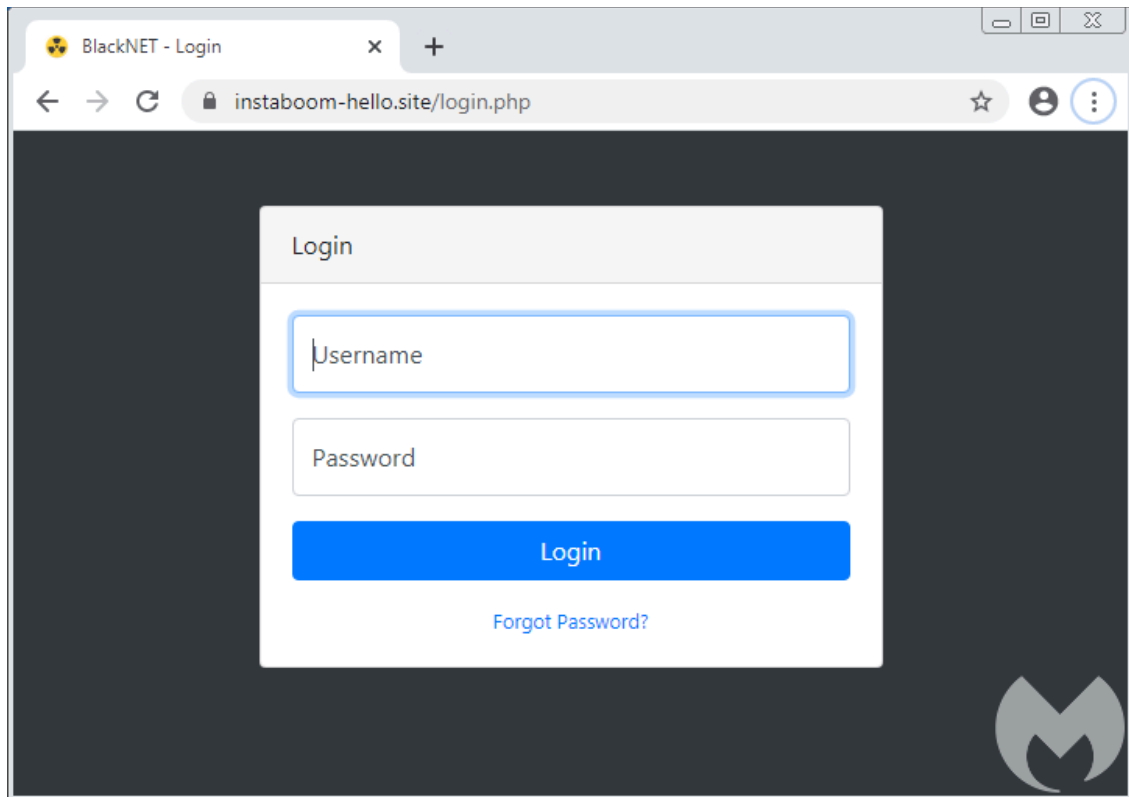


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features a 'Slaves Menu' with four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below the menu is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the right of the table are 'Previous' and 'Next' buttons. Below the list is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right of the commands center is a 'Map Visualization' section showing a world map with a blue overlay. At the bottom, there's a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The screenshot shows a Malwarebytes Premium notification window. It features the Malwarebytes logo and the word 'Premium' in the top left corner. A green checkmark icon is next to the heading 'Malware blocked by Real-Time Protection'. Below the heading, it states: 'It has been automatically quarantined and is no longer a threat to your computer.' The notification also displays the following details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

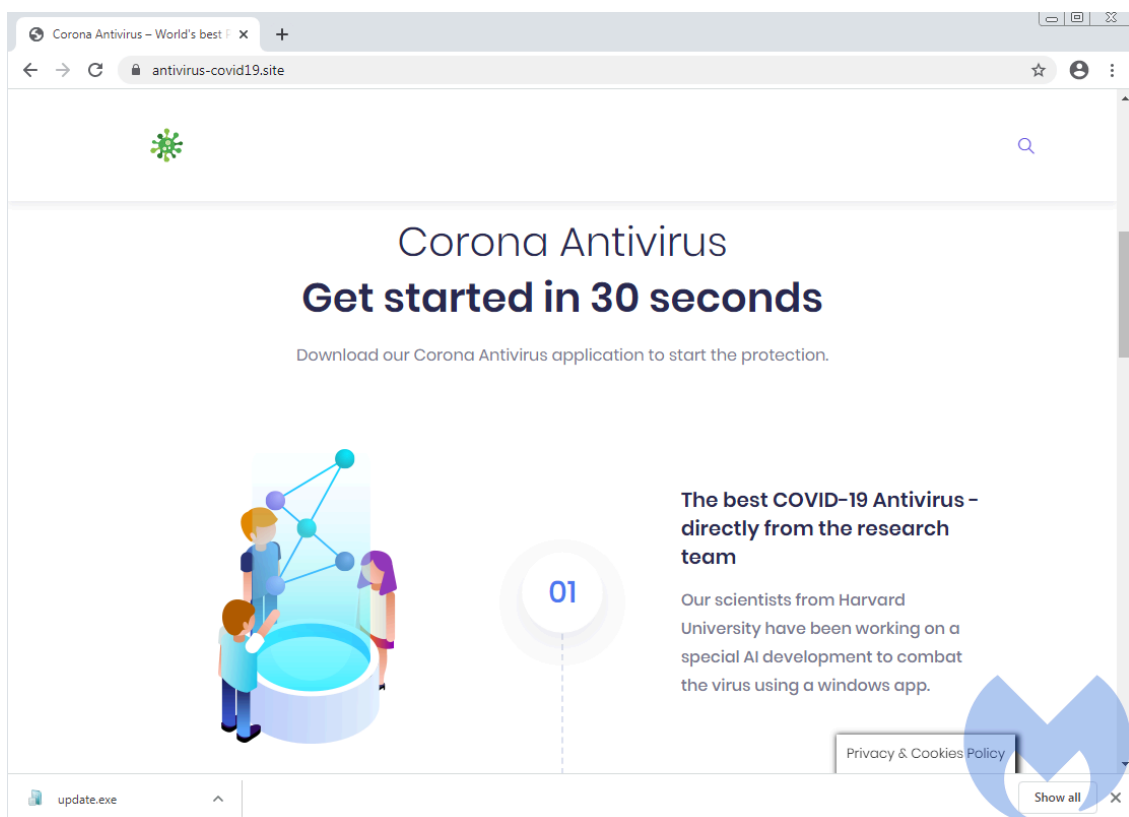
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

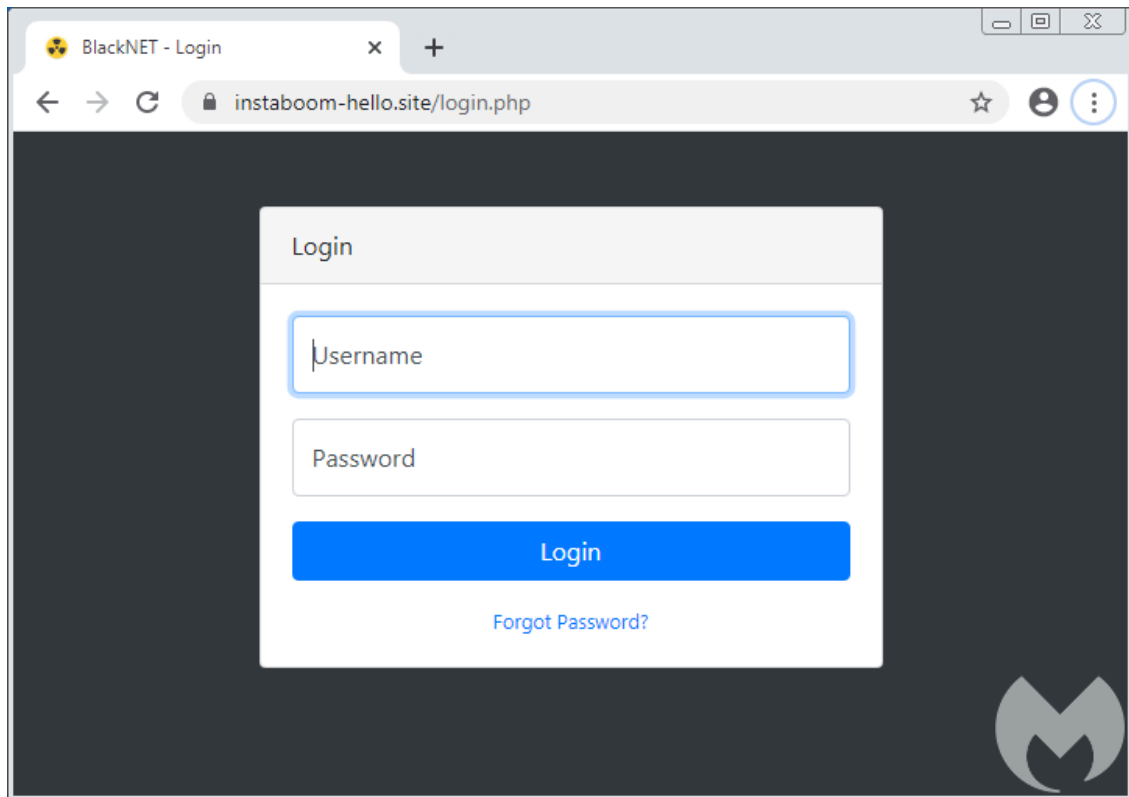


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

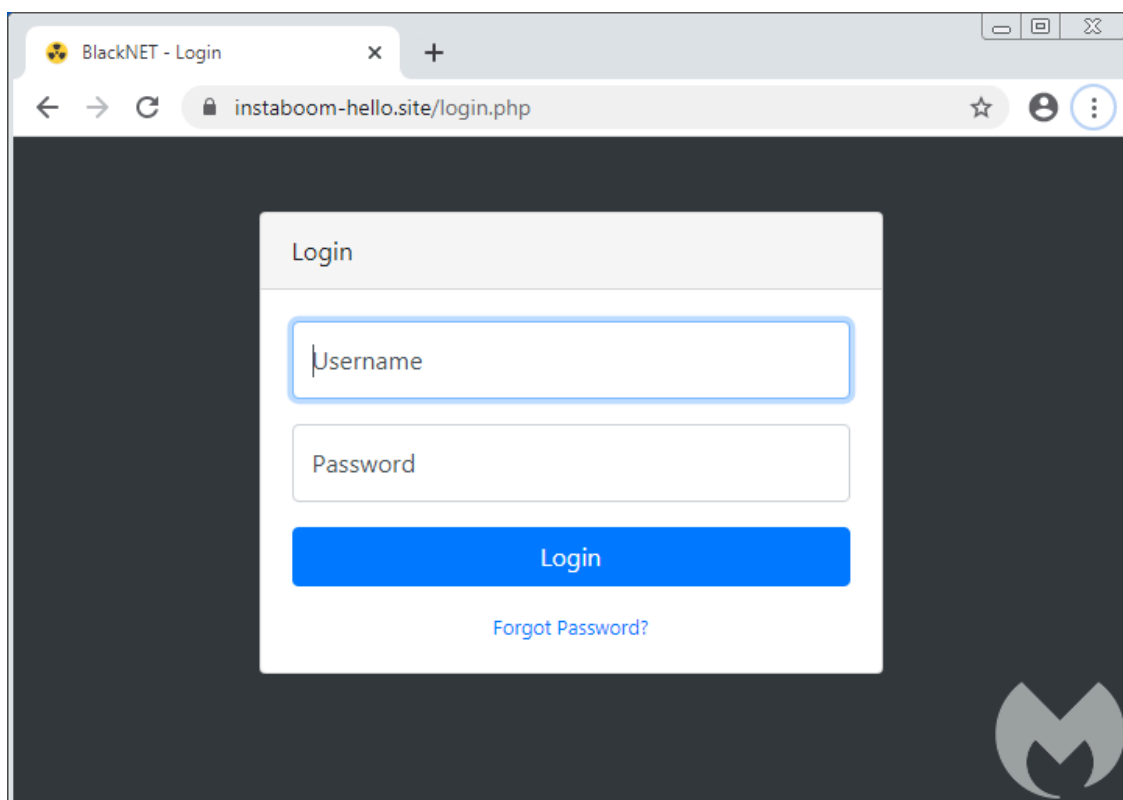
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots

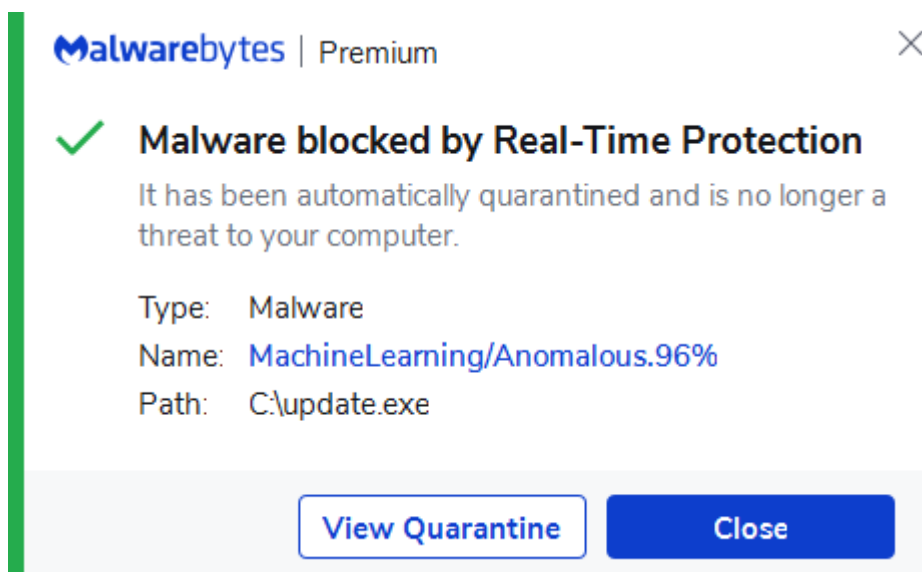
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.



We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

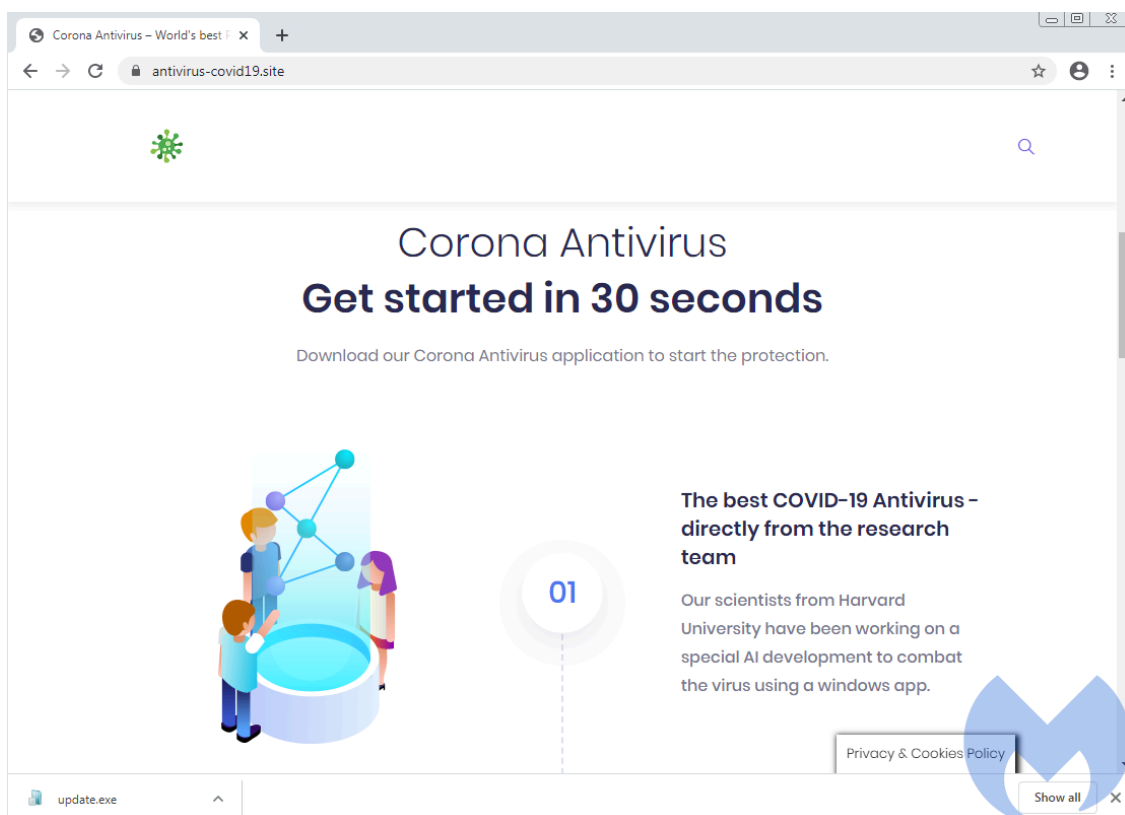
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

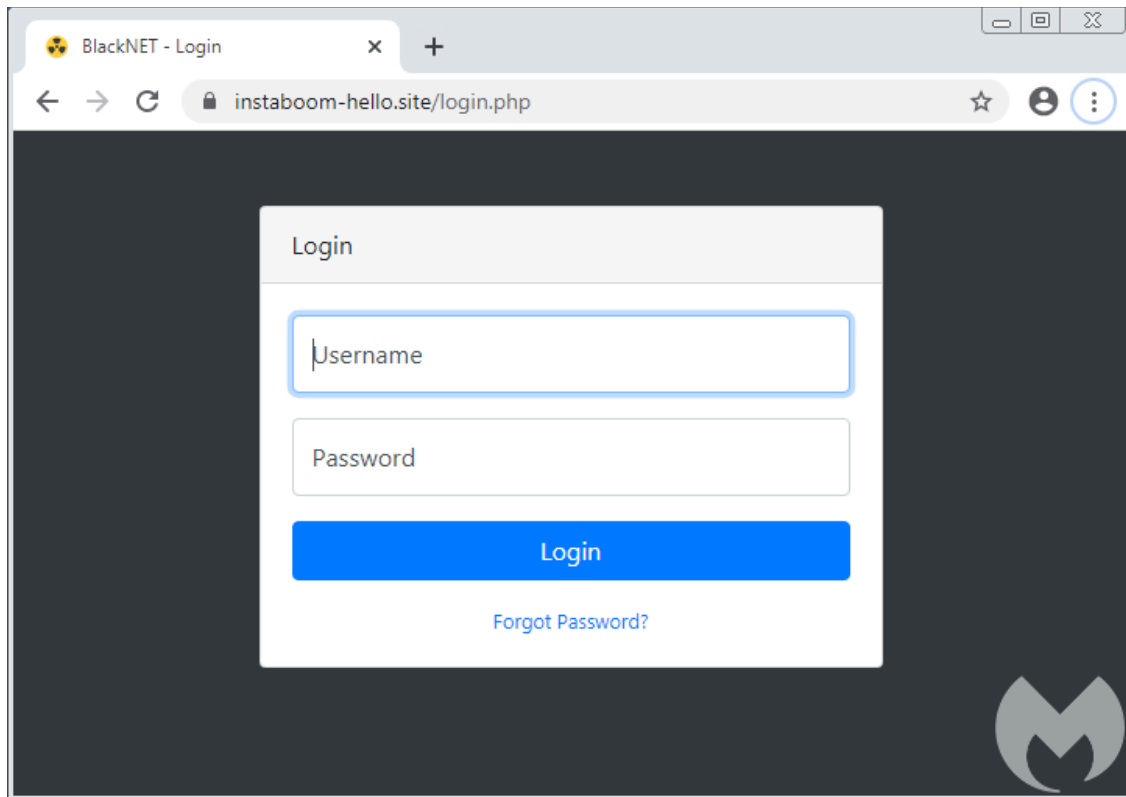


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top, there's a navigation bar with links: Home, View Logs, Settings, Change Password, and Logout. Below this, two warning banners are displayed: one about logging in as 'admin' and another about two-factor authentication. The main dashboard features four colored boxes: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). Below these is a 'Bot/Slaves List' section with a search bar and a table with columns: Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status. The table currently shows 'No Clients Available'. To the left of the table is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains the copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection'. It states: 'It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: Type: Malware, Name: MachineLearning/Anomalous.96%, and Path: C:\update.exe. At the bottom, there are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

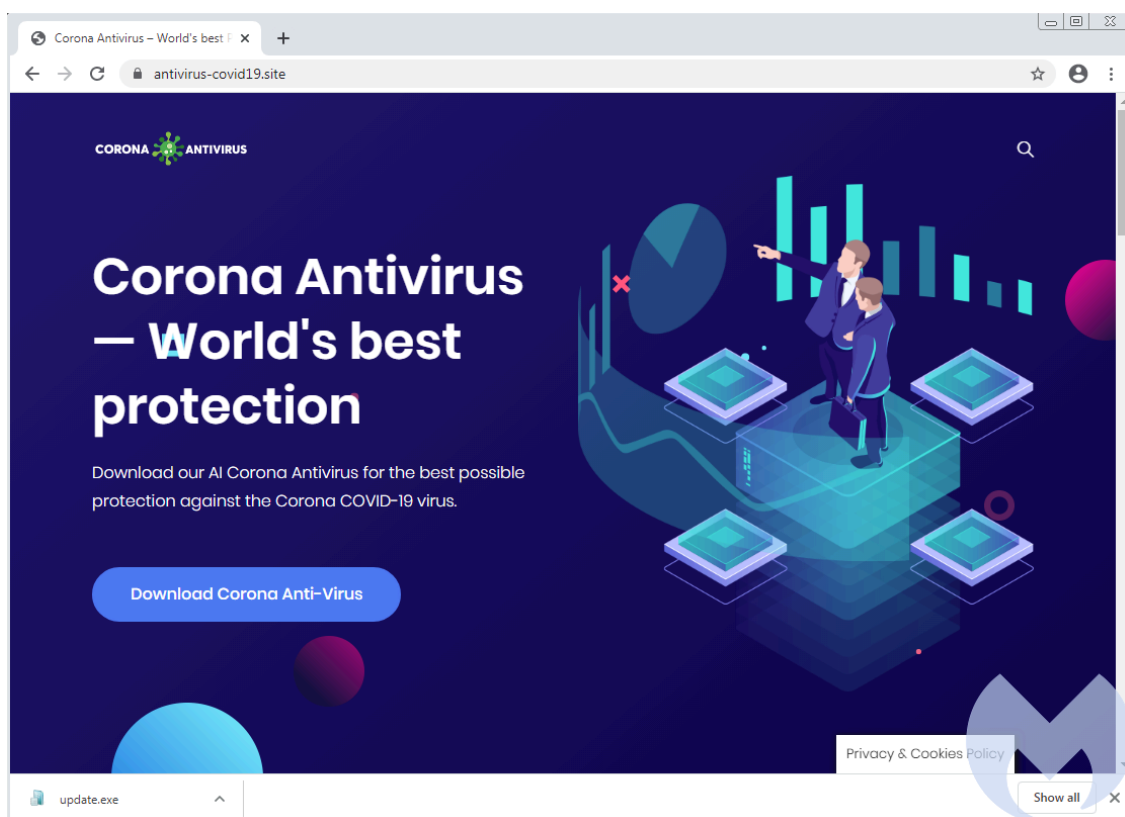
Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

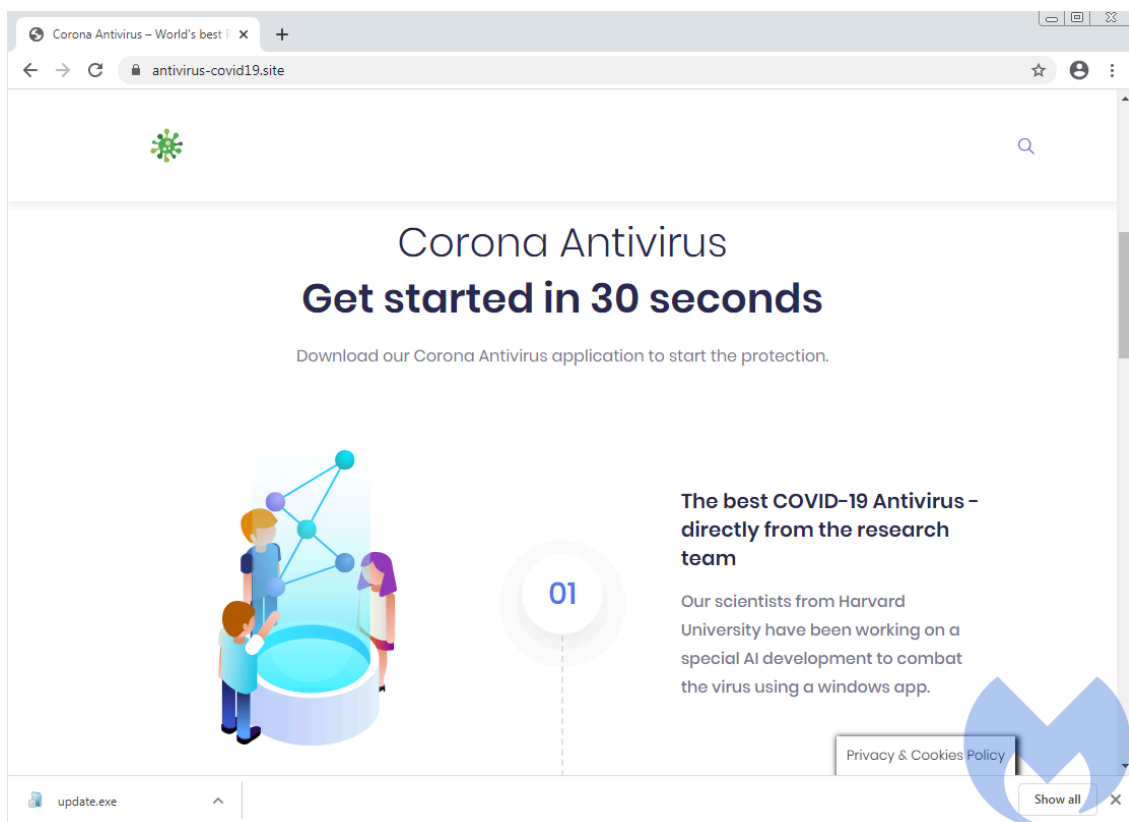
```
instaboom-hello[.]site
```



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the

app is running.

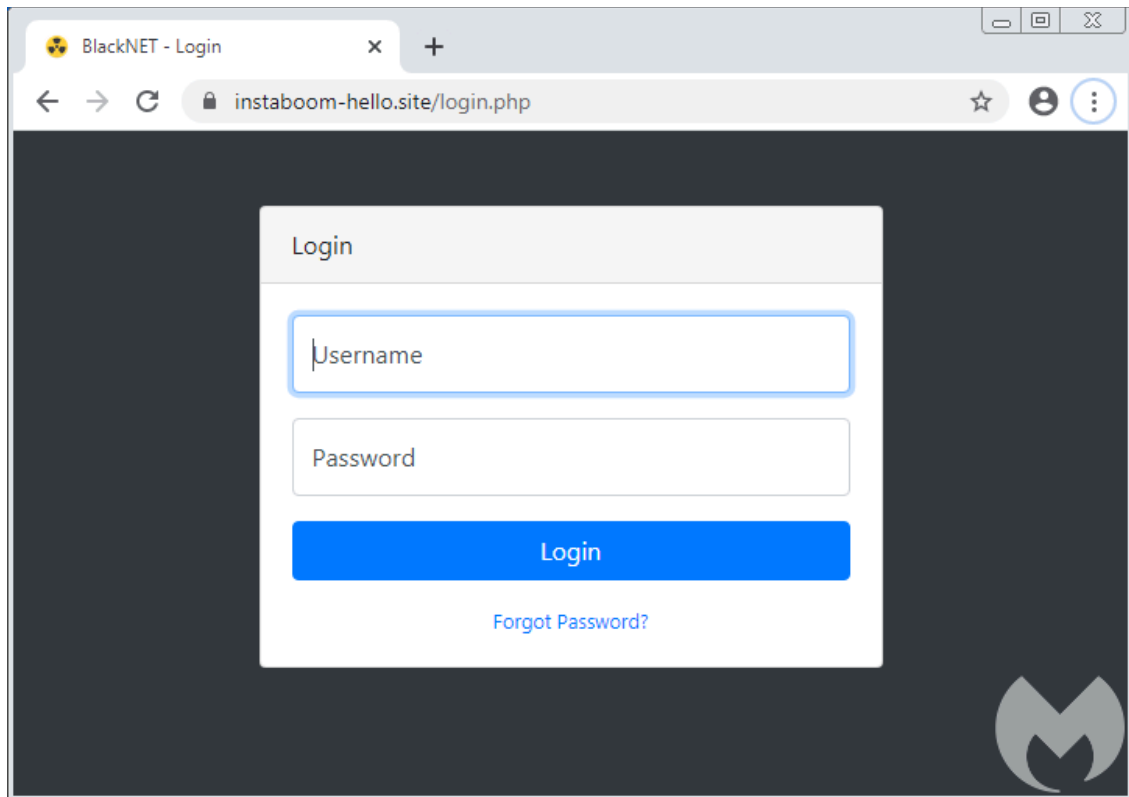


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

The screenshot shows the BlackNET web interface. At the top is a dark navigation bar with the BlackNET logo and links for Home, View Logs, Settings, Change Password, and Logout. Below this are two yellow warning banners: one about logging in as 'admin' and another about two-factor authentication. A 'Slaves Menu' section contains four colored cards: '0 Total Clients!' (blue), '0 USB Clients!' (yellow), '0 Online Clients!' (green), and '0 Offline Clients!' (red). The main section is titled 'Bot/Slaves List' and includes a search bar, a table with columns for Victim ID, IP Address, Computer Name, User Status, Country, OS, Installed Date, Antivirus, and Status, and a 'No Clients Available' message. Below the table are 'Previous' and 'Next' buttons. To the left is a 'Commands Center' with a dropdown menu for 'Select Command' and a 'Send Command' button. To the right is a 'Map Visualization' showing a world map with blue markers. The footer contains a copyright notice: 'Copyright © BLACKNET by Black.Hacker - 2020'.

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

The notification window from Malwarebytes Premium shows a green checkmark and the text: 'Malware blocked by Real-Time Protection. It has been automatically quarantined and is no longer a threat to your computer.' Below this, it lists the details: 'Type: Malware', 'Name: MachineLearning/Anomalous.96%', and 'Path: C:\update.exe'. At the bottom are two buttons: 'View Quarantine' and 'Close'.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Scammers and malware authors are taking advantage of the coronavirus crisis in full swing. We have seen a number of spam campaigns using COVID-19 as a lure to trick people into installing a variety of malware, but especially data stealers.

As more of us work from home, the need to secure your computer, especially if you are connecting to your company's network, becomes more important. However, you should be extra careful of bogus security software, especially if it tries to use the coronavirus as a selling point.

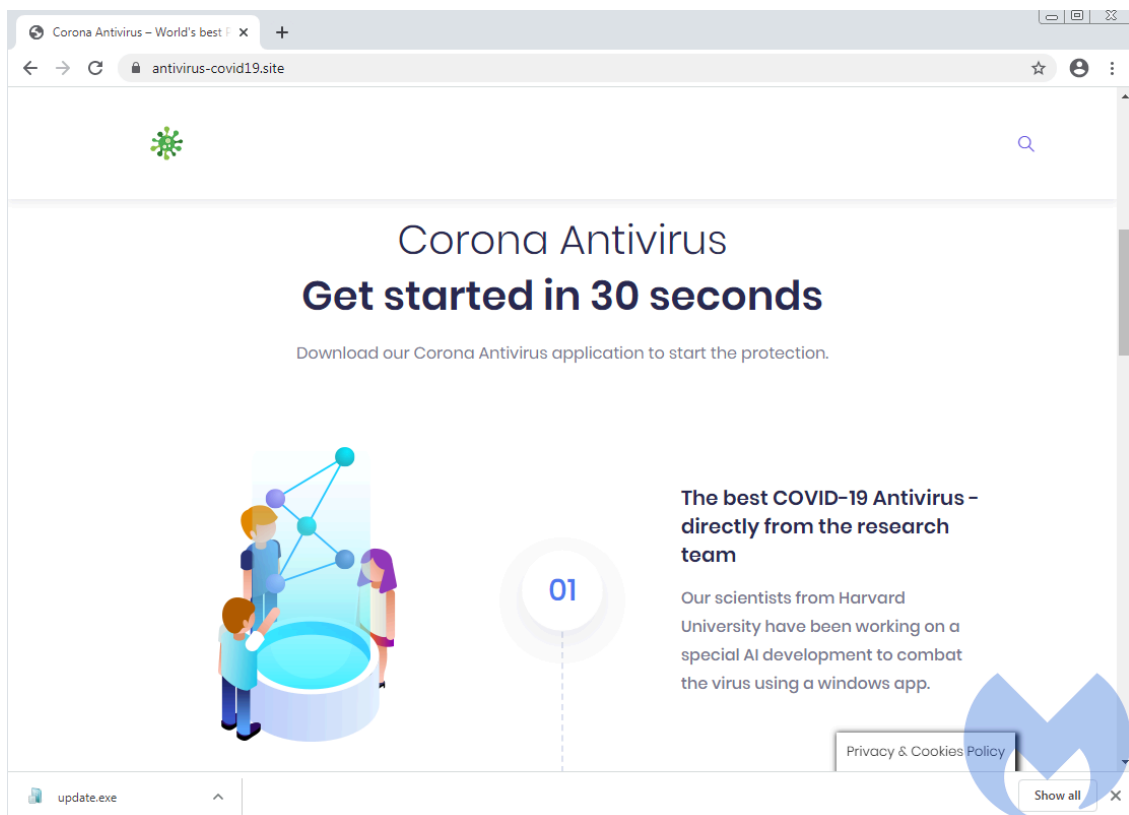
Corona antivirus: 100% fake

The latest scam we found is a website (antivirus-covid19[.]site) advertising "Corona Antivirus -World's best protection." That's right, scammers are trying to get you to install a digital antivirus that supposedly protects against the actual COVID-19 virus infecting people across the world.



To add to the nonsense, the site goes on by adding:

Our scientists from Harvard University have been working on a special AI development to combat the virus using a windows app. Your PC actively protects you against the Coronaviruses (Cov) while the app is running.

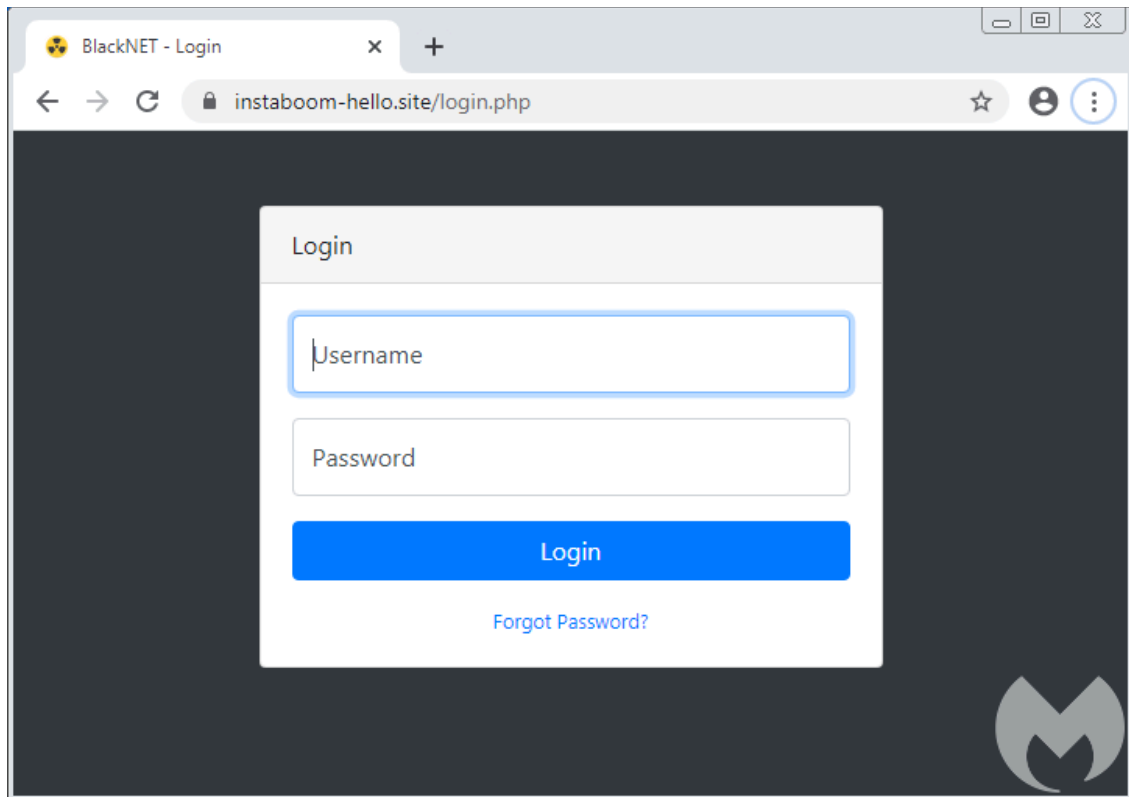


Infected victims added to BlackNET RAT

Upon installing this application, your computer will be infected with malware. The file, packed with the commercial packer Themida turns your PC into a bot ready to receive commands:

```
hxxps[://]instaboom-hello[.]site//connection[.]php?data=[removed] hxxps[://]instaboom-hello[.]site//
```

The command and control server hosted at instaboom-hello[.]site reveals the control panel for the BlackNET botnet.



The full source code for this toolkit was [published](#) on GitHub a month ago. Some of its features include:

- Deploying DDOS attacks
- Taking screenshots
- Stealing Firefox cookies
- Stealing saved passwords
- Implementing a keylogger
- Executing scripts
- Stealing Bitcoin wallets

Choose the right protection

During this period, it is important to stay safe both at home and online. The number of scams we have seen during these past few weeks shows that criminals will take advantage of any situation, no matter how dire it is.

We recommend that you keep your computer up to date and use extra caution when downloading new programs. Beware of instant notifications and other messages, even if they appear to come from friends.

Malwarebytes users were already protected even though we had not seen this malware sample before, thanks to our Machine learning engine.

We also informed CloudFlare since the threat actors were abusing their service and they took immediate action to flag this website as a phish.

Indicators of compromise

Malicious site

```
antivirus-covid19[.]site
```

Bogus corona antivirus

```
antivirus-covid19[.]site/update.exe
```

```
146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
```

C2 panel

```
instaboom-hello[.]site
```

Source: <https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/>