Honda and Enel impacted by cyber attack suspected to be ransomware

Published: 2020-06-08 · Archived: 2026-04-05 18:21:20 UTC

Car manufacturer Honda has been hit by a cyber attack, according to a report published by the BBC, and later confirmed by the company in a tweet. Another similar attack, also disclosed on Twitter, hit Edesur S.A., one of the companies belonging to Enel Argentina which operates in the business of energy distribution in the City of Buenos Aires.

Based on samples posted online, these incidents may be tied to the EKANS/SNAKE ransomware family. In this blog post, we review what is known about this ransomware strain and what we have been able to analyze so far.

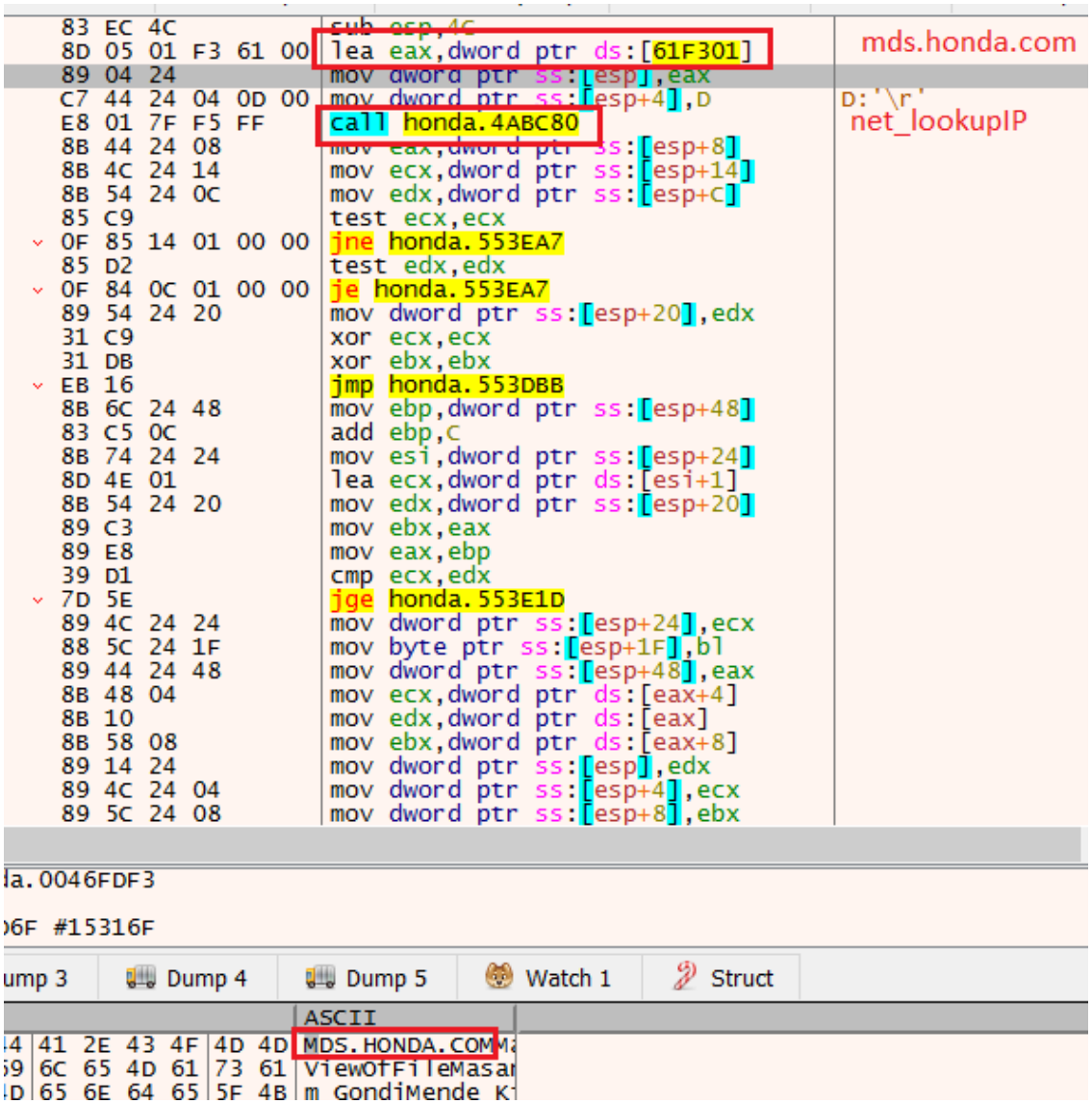
Targeted ransomware with a liking for ICS

First public mentions of EKANS ransomware date back to January 2020, with security researcher Vitali Kremez sharing information about a new targeted ransomware written in GOLANG.

The group appears to have a special interest for Industrial Control Systems (ICS), as detailed in this blog post by security firm Dragos.

On June 8, a researcher shared samples of ransomware that supposedly was aimed at Honda and ENEL INT. When we started looking at the code, we found several artefacts that corroborate this possibility.

When the malware executes, it will try to resolve to a hardcoded hostname (mds.honda.com). If, and only if it does, will the file encryption begin. The same logic, with a specific hostname, also applied to the ransomware allegedly tied to Enel.



Target: Honda

- Resolving internal domain: mds.honda.com
- Ransom e-mail: CarrolBidell@tutanota[.]com

Target: Enel

- Resolving internal domain: enelint.global
- Ransom e-mail: CarrolBidell@tutanota[.]com

RDP as a possible attack vector

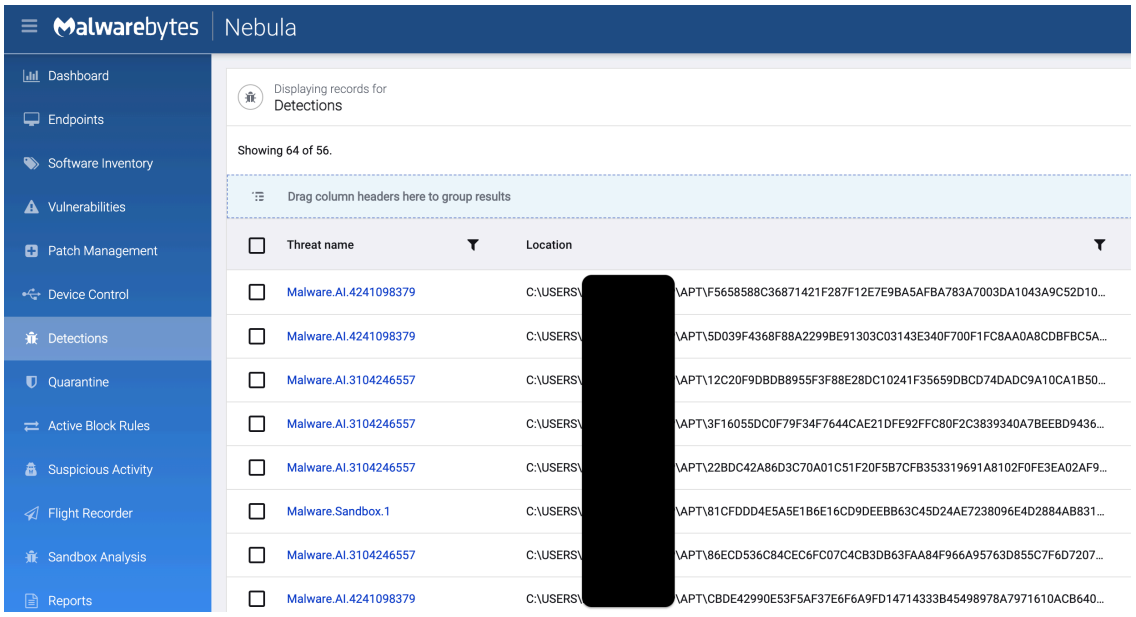
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference here). RDP attacks are one of the main entry points when it comes to targeted ransomware opertaions.

- RDP Exposed: /AGL632956.jpn.mds.honda.com
- RDP Exposed: /IT000001429258.enelint.global

However, we cannot say conclusively that this is how threat actors may have gotten in. Ultimately, only a proper internal investigation will be able to determine exactly how the attackers were able to compromise the affected networks.

Detection

We tested the ransomware samples publicly available in our lab by creating a fake internal server that would respond to the DNS query made by the malware code with the same IP address it expected. We then ran the sample alleged to be tied to Honda against Malwarebytes Nebula, our cloud-based endpoint protection for businesses.



We detect this payload as ‘Ransom.Ekans’ when it attempts to execute. In order to test another of our protection layers, we also disabled (not recommended) the malware protection to let the behavior engine do its thing. Our anti-ransomware technology was able to quarantine the malicious file without the use of any signature.

Ransomware gangs have shown no mercy, even in this period of dealing with a pandemic. They continue to target big companies in order to extort large sums of money.

RDP has been called out as some of the lowest hanging fruit preferred by attackers. However, we also recently learned about a new SMB vulnerability allowing remote execution. It is important for defenders to properly map out all assets, patch them, and never allow them to be publicly exposed.

We will update this blog post if we come across new relevant information.

Indicators of Compromise (IOCs)

Honda related sample:

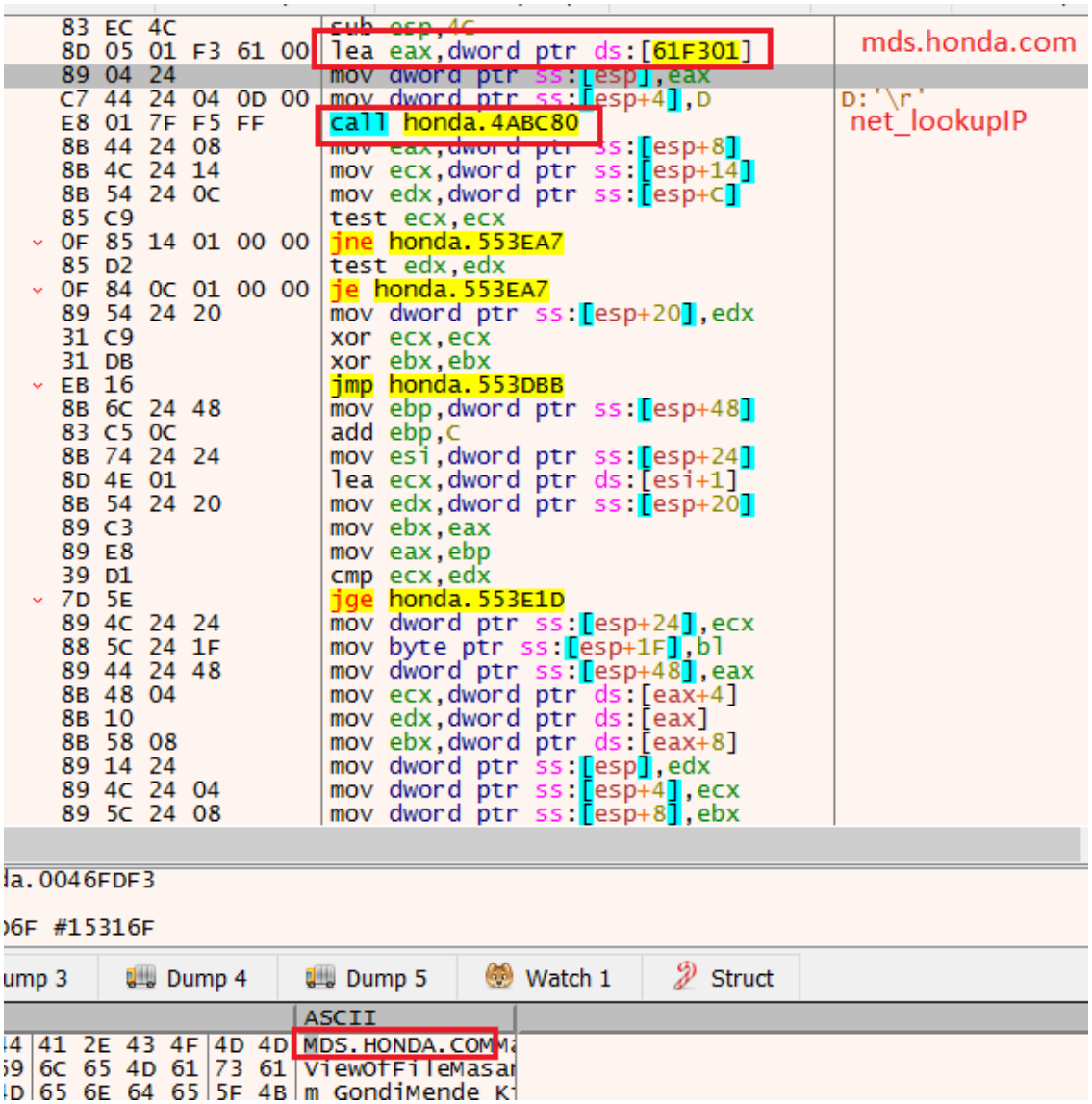
```
d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1 mds.honda.com
```

Enel related sample:

```
edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a
enelint.global
```

On June 8, a researcher shared samples of ransomware that supposedly was aimed at Honda and ENEL INT. When we started looking at the code, we found several artefacts that corroborate this possibility.

When the malware executes, it will try to resolve to a hardcoded hostname (mds.honda.com). If, and only if it does, will the file encryption begin. The same logic, with a specific hostname, also applied to the ransomware allegedly tied to Enel.



Target: Honda

- Resolving internal domain: mds.honda.com
- Ransom e-mail: CarrolBidell@tutanota[.]com

Target: Enel

- Resolving internal domain: enelint.global
- Ransom e-mail: CarrolBidell@tutanota[.]com

RDP as a possible attack vector

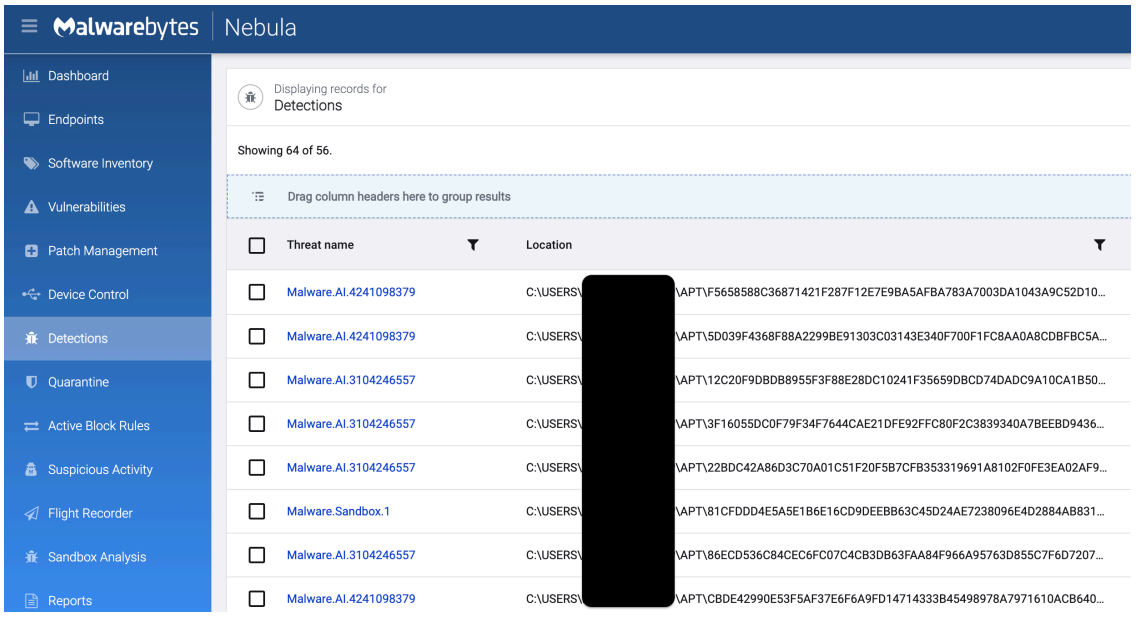
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference here). RDP attacks are one of the main entry points when it comes to targeted ransomware opertaions.

- RDP Exposed: /AGL632956.jpn.mds.honda.com
- RDP Exposed: /IT000001429258.enelint.global

However, we cannot say conclusively that this is how threat actors may have gotten in. Ultimately, only a proper internal investigation will be able to determine exactly how the attackers were able to compromise the affected networks.

Detection

We tested the ransomware samples publicly available in our lab by creating a fake internal server that would respond to the DNS query made by the malware code with the same IP address it expected. We then ran the sample alleged to be tied to Honda against Malwarebytes Nebula, our cloud-based endpoint protection for businesses.



We detect this payload as ‘Ransom.Ekans’ when it attempts to execute. In order to test another of our protection layers, we also disabled (not recommended) the malware protection to let the behavior engine do its thing. Our anti-ransomware technology was able to quarantine the malicious file without the use of any signature.

Ransomware gangs have shown no mercy, even in this period of dealing with a pandemic. They continue to target big companies in order to extort large sums of money.

RDP has been called out as some of the lowest hanging fruit preferred by attackers. However, we also recently learned about a new SMB vulnerability allowing remote execution. It is important for defenders to properly map out all assets, patch them, and never allow them to be publicly exposed.

We will update this blog post if we come across new relevant information.

Indicators of Compromise (IOCs)

Honda related sample:

```
d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1 mds.honda.com
```

Enel related sample:

```
edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a
enelint.global
```

Car manufacturer Honda has been hit by a cyber attack, according to a report published by the BBC, and later confirmed by the company in a tweet. Another similar attack, also disclosed on Twitter, hit Edesur S.A., one of the companies belonging to Enel Argentina which operates in the business of energy distribution in the City of Buenos Aires.

Based on samples posted online, these incidents may be tied to the EKANS/SNAKE ransomware family. In this blog post, we review what is known about this ransomware strain and what we have been able to analyze so far.

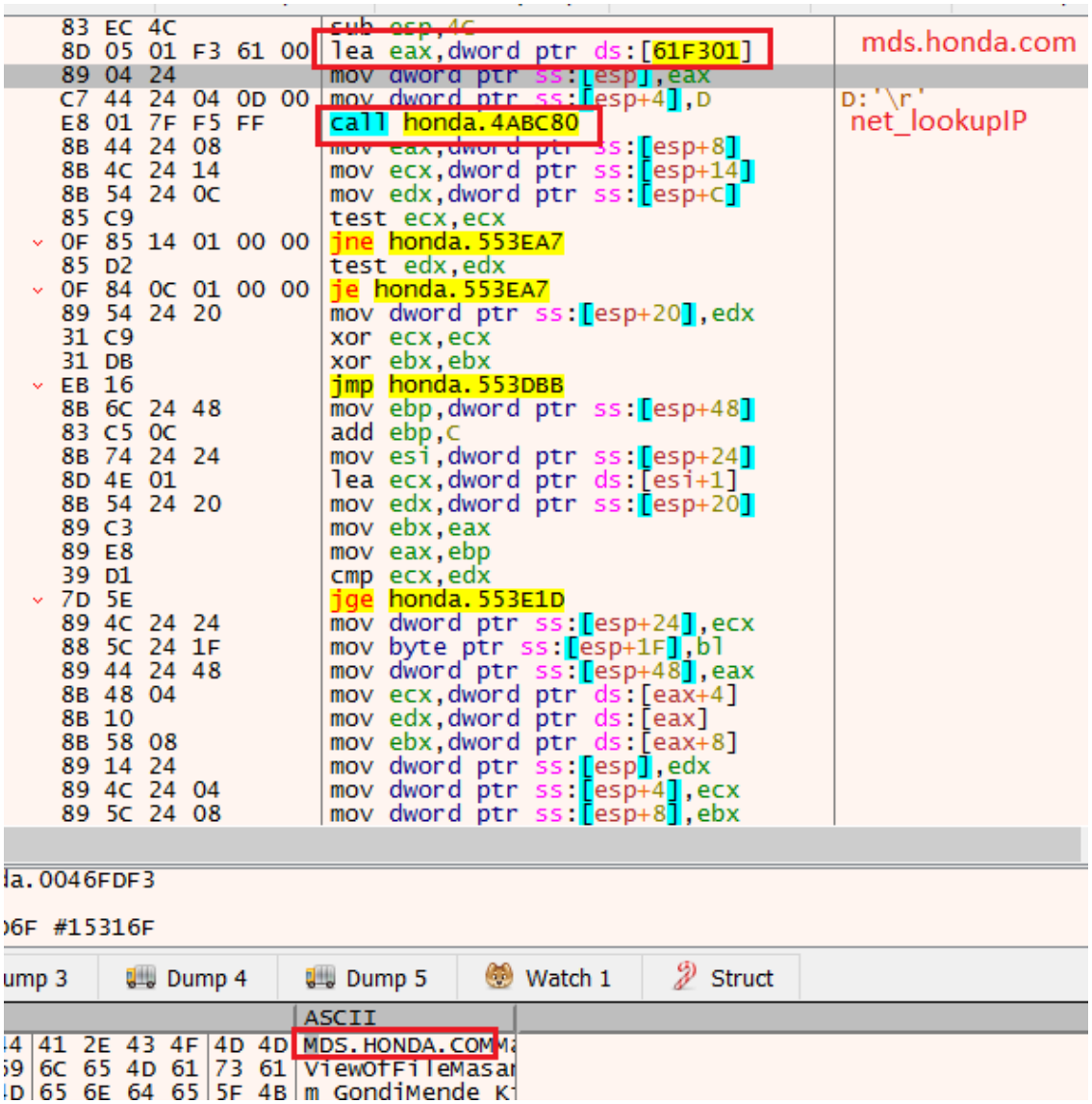
Targeted ransomware with a liking for ICS

First public mentions of EKANS ransomware date back to January 2020, with security researcher Vitali Kremez sharing information about a new targeted ransomware written in GOLANG.

The group appears to have a special interest for Industrial Control Systems (ICS), as detailed in this blog post by security firm Dragos.

On June 8, a researcher shared samples of ransomware that supposedly was aimed at Honda and ENEL INT. When we started looking at the code, we found several artefacts that corroborate this possibility.

When the malware executes, it will try to resolve to a hardcoded hostname (mds.honda.com). If, and only if it does, will the file encryption begin. The same logic, with a specific hostname, also applied to the ransomware allegedly tied to Enel.



Target: Honda

- Resolving internal domain: mds.honda.com
- Ransom e-mail: CarrolBidell@tutanota[.]com

Target: Enel

- Resolving internal domain: enelint.global
- Ransom e-mail: CarrolBidell@tutanota[.]com

RDP as a possible attack vector

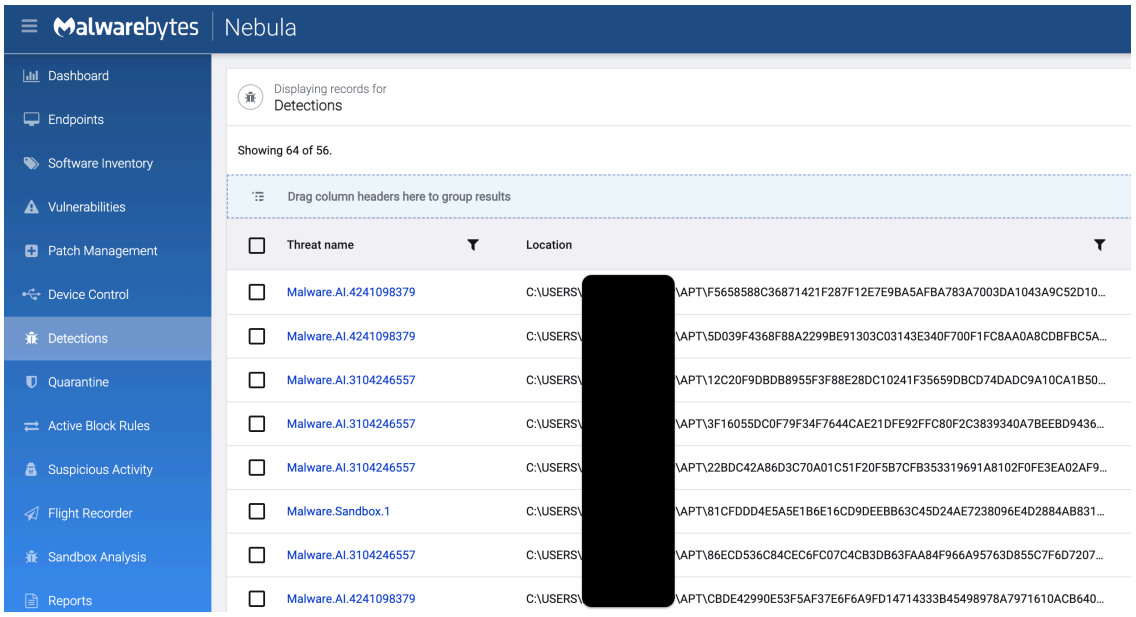
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference here). RDP attacks are one of the main entry points when it comes to targeted ransomware opertaions.

- RDP Exposed: /AGL632956.jpn.mds.honda.com
- RDP Exposed: /IT000001429258.enelint.global

However, we cannot say conclusively that this is how threat actors may have gotten in. Ultimately, only a proper internal investigation will be able to determine exactly how the attackers were able to compromise the affected networks.

Detection

We tested the ransomware samples publicly available in our lab by creating a fake internal server that would respond to the DNS query made by the malware code with the same IP address it expected. We then ran the sample alleged to be tied to Honda against Malwarebytes Nebula, our cloud-based endpoint protection for businesses.



We detect this payload as ‘Ransom.Ekans’ when it attempts to execute. In order to test another of our protection layers, we also disabled (not recommended) the malware protection to let the behavior engine do its thing. Our anti-ransomware technology was able to quarantine the malicious file without the use of any signature.

Ransomware gangs have shown no mercy, even in this period of dealing with a pandemic. They continue to target big companies in order to extort large sums of money.

RDP has been called out as some of the lowest hanging fruit preferred by attackers. However, we also recently learned about a new SMB vulnerability allowing remote execution. It is important for defenders to properly map out all assets, patch them, and never allow them to be publicly exposed.

We will update this blog post if we come across new relevant information.

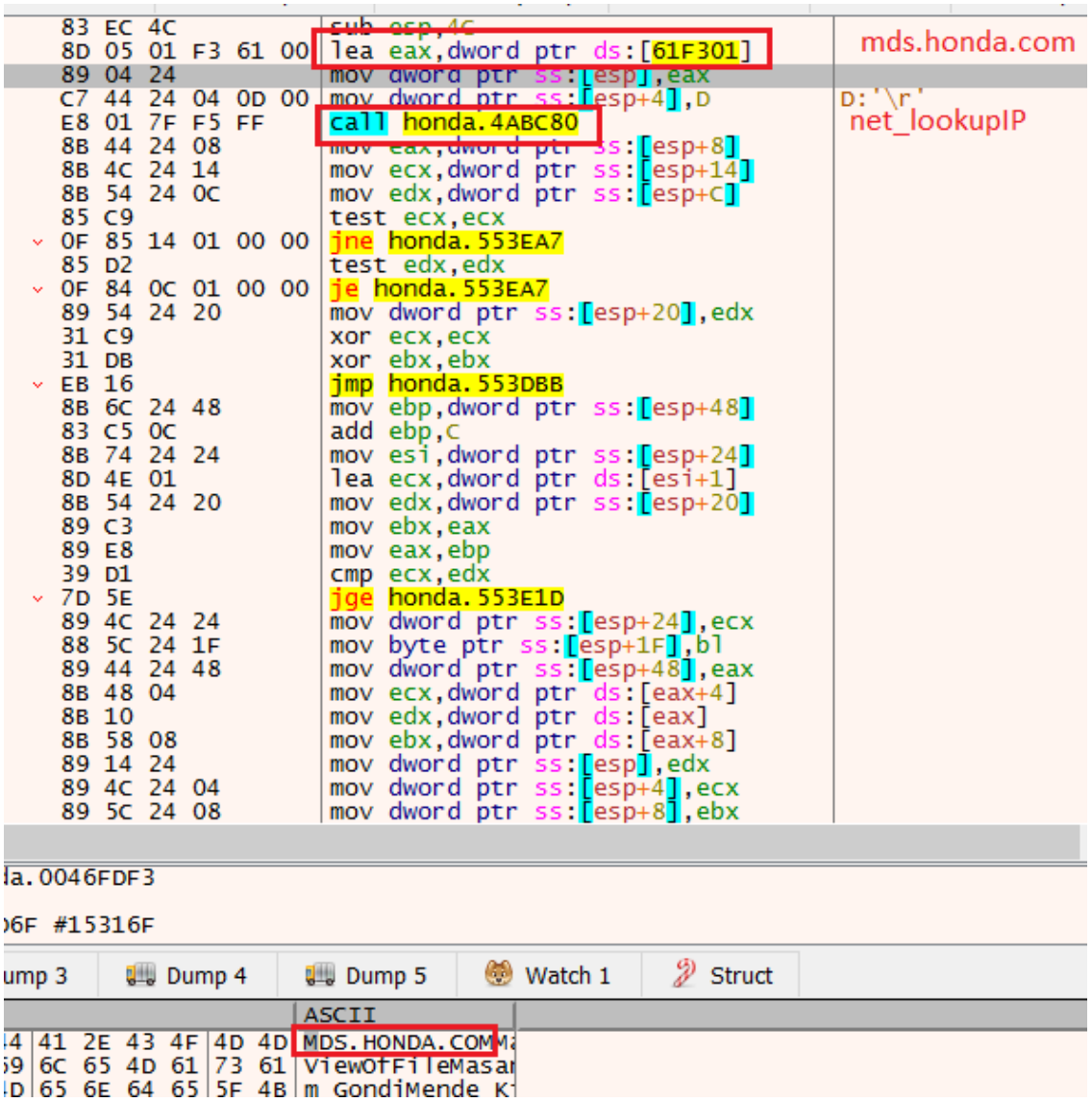
Indicators of Compromise (IOCs)

Honda related sample:

```
d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1 mds.honda.com
```

Enel related sample:

```
edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a
enelint.global
```



Target: Honda

- Resolving internal domain: mds.honda.com
- Ransom e-mail: CarrolBidell@tutanota[.]com

Target: Enel

- Resolving internal domain: enelint.global
- Ransom e-mail: CarrolBidell@tutanota[.]com

RDP as a possible attack vector

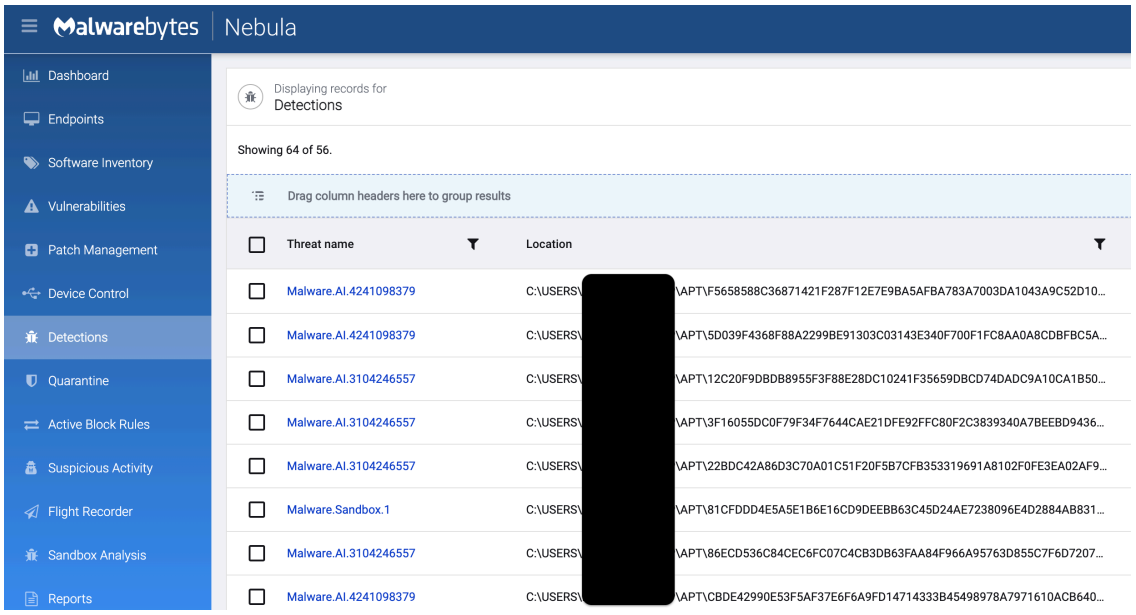
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference here). RDP attacks are one of the main entry points when it comes to targeted ransomware opertaions.

- RDP Exposed: /AGL632956.jpn.mds.honda.com
- RDP Exposed: /IT000001429258.enelint.global

However, we cannot say conclusively that this is how threat actors may have gotten in. Ultimately, only a proper internal investigation will be able to determine exactly how the attackers were able to compromise the affected networks.

Detection

We tested the ransomware samples publicly available in our lab by creating a fake internal server that would respond to the DNS query made by the malware code with the same IP address it expected. We then ran the sample alleged to be tied to Honda against Malwarebytes Nebula, our cloud-based endpoint protection for businesses.



We detect this payload as ‘Ransom.Ekans’ when it attempts to execute. In order to test another of our protection layers, we also disabled (not recommended) the malware protection to let the behavior engine do its thing. Our anti-ransomware technology was able to quarantine the malicious file without the use of any signature.

Ransomware gangs have shown no mercy, even in this period of dealing with a pandemic. They continue to target big companies in order to extort large sums of money.

RDP has been called out as some of the lowest hanging fruit preferred by attackers. However, we also recently learned about a new SMB vulnerability allowing remote execution. It is important for defenders to properly map out all assets, patch them, and never allow them to be publicly exposed.

We will update this blog post if we come across new relevant information.

Indicators of Compromise (IOCs)

Honda related sample:

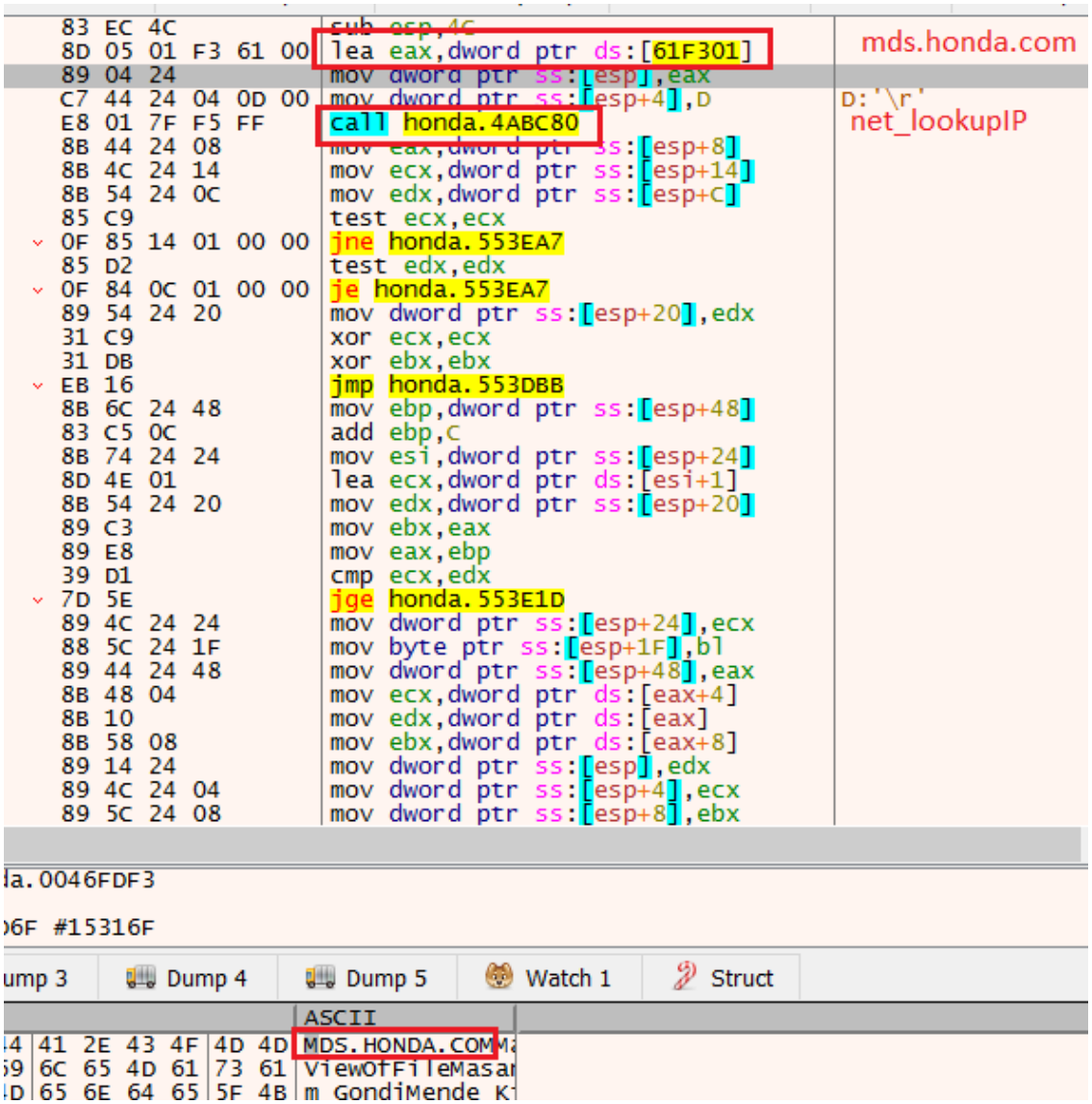
```
d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1 mds.honda.com
```

Enel related sample:

```
edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a
enelint.global
```

On June 8, a researcher shared samples of ransomware that supposedly was aimed at Honda and ENEL INT. When we started looking at the code, we found several artefacts that corroborate this possibility.

When the malware executes, it will try to resolve to a hardcoded hostname (mds.honda.com). If, and only if it does, will the file encryption begin. The same logic, with a specific hostname, also applied to the ransomware allegedly tied to Enel.



Target: Honda

- Resolving internal domain: mds.honda.com
- Ransom e-mail: CarrolBidell@tutanota[.]com

Target: Enel

- Resolving internal domain: enelint.global
- Ransom e-mail: CarrolBidell@tutanota[.]com

RDP as a possible attack vector

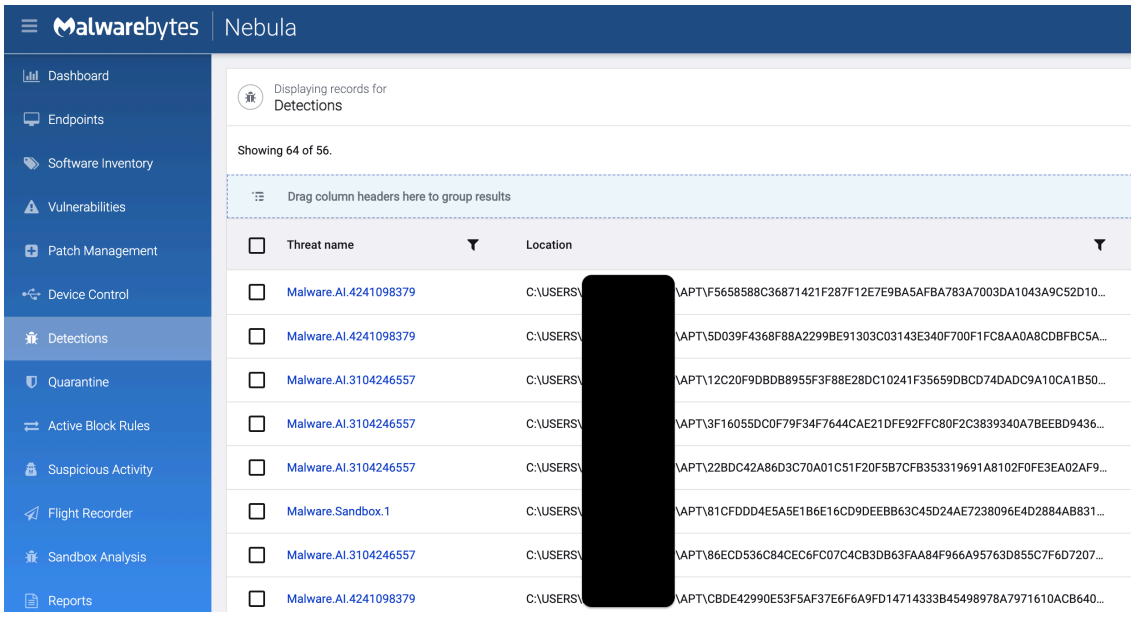
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference here). RDP attacks are one of the main entry points when it comes to targeted ransomware opertaions.

- RDP Exposed: /AGL632956.jpn.mds.honda.com
- RDP Exposed: /IT000001429258.enelint.global

However, we cannot say conclusively that this is how threat actors may have gotten in. Ultimately, only a proper internal investigation will be able to determine exactly how the attackers were able to compromise the affected networks.

Detection

We tested the ransomware samples publicly available in our lab by creating a fake internal server that would respond to the DNS query made by the malware code with the same IP address it expected. We then ran the sample alleged to be tied to Honda against Malwarebytes Nebula, our cloud-based endpoint protection for businesses.



We detect this payload as ‘Ransom.Ekans’ when it attempts to execute. In order to test another of our protection layers, we also disabled (not recommended) the malware protection to let the behavior engine do its thing. Our anti-ransomware technology was able to quarantine the malicious file without the use of any signature.

Ransomware gangs have shown no mercy, even in this period of dealing with a pandemic. They continue to target big companies in order to extort large sums of money.

RDP has been called out as some of the lowest hanging fruit preferred by attackers. However, we also recently learned about a new SMB vulnerability allowing remote execution. It is important for defenders to properly map out all assets, patch them, and never allow them to be publicly exposed.

We will update this blog post if we come across new relevant information.

Indicators of Compromise (IOCs)

Honda related sample:

```
d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1 mds.honda.com
```

Enel related sample:

```
edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a
enelint.global
```

Car manufacturer Honda has been hit by a cyber attack, according to a report published by the BBC, and later confirmed by the company in a tweet. Another similar attack, also disclosed on Twitter, hit Edesur S.A., one of the companies belonging to Enel Argentina which operates in the business of energy distribution in the City of Buenos Aires.

Based on samples posted online, these incidents may be tied to the EKANS/SNAKE ransomware family. In this blog post, we review what is known about this ransomware strain and what we have been able to analyze so far.

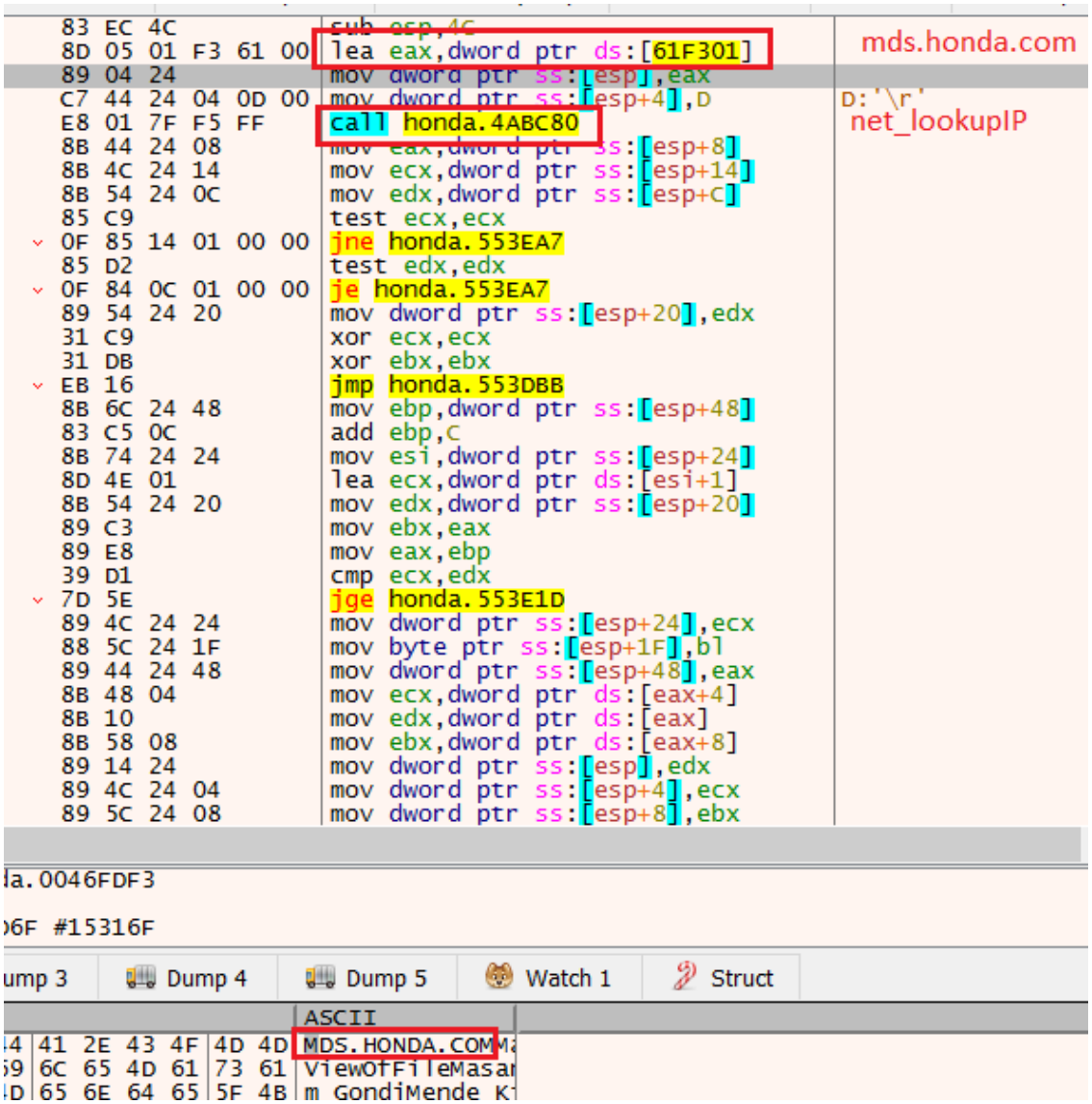
Targeted ransomware with a liking for ICS

First public mentions of EKANS ransomware date back to January 2020, with security researcher Vitali Kremez sharing information about a new targeted ransomware written in GOLANG.

The group appears to have a special interest for Industrial Control Systems (ICS), as detailed in this blog post by security firm Dragos.

On June 8, a researcher shared samples of ransomware that supposedly was aimed at Honda and ENEL INT. When we started looking at the code, we found several artefacts that corroborate this possibility.

When the malware executes, it will try to resolve to a hardcoded hostname (mds.honda.com). If, and only if it does, will the file encryption begin. The same logic, with a specific hostname, also applied to the ransomware allegedly tied to Enel.



Target: Honda

- Resolving internal domain: mds.honda.com
- Ransom e-mail: CarrolBidell@tutanota[.]com

Target: Enel

- Resolving internal domain: enelint.global
- Ransom e-mail: CarrolBidell@tutanota[.]com

RDP as a possible attack vector

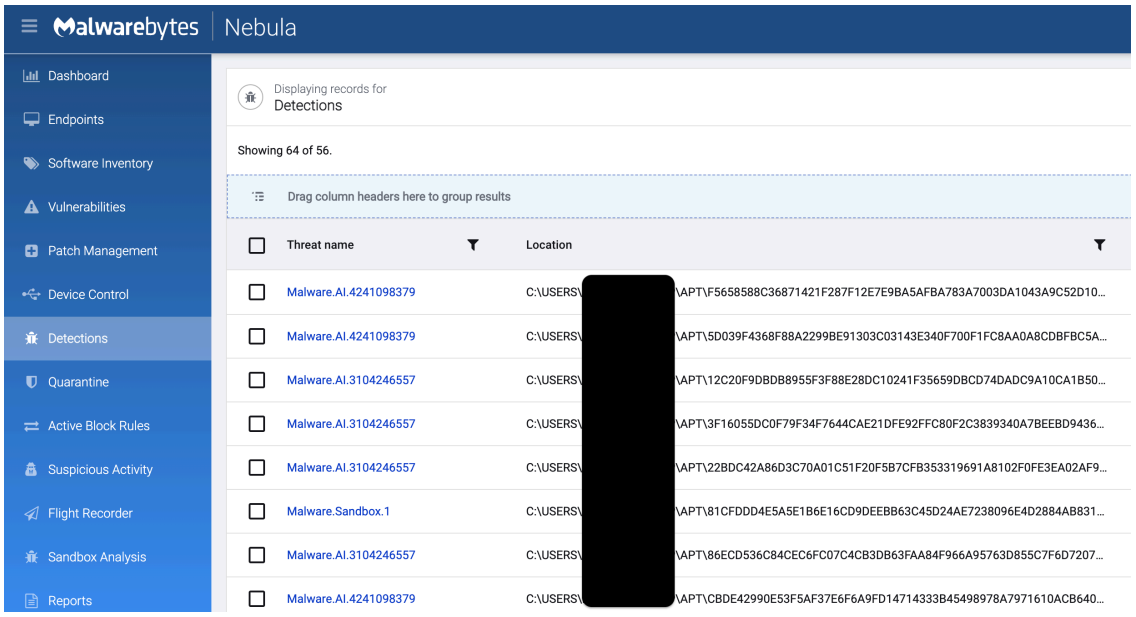
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference here). RDP attacks are one of the main entry points when it comes to targeted ransomware opertaions.

- RDP Exposed: /AGL632956.jpn.mds.honda.com
- RDP Exposed: /IT000001429258.enelint.global

However, we cannot say conclusively that this is how threat actors may have gotten in. Ultimately, only a proper internal investigation will be able to determine exactly how the attackers were able to compromise the affected networks.

Detection

We tested the ransomware samples publicly available in our lab by creating a fake internal server that would respond to the DNS query made by the malware code with the same IP address it expected. We then ran the sample alleged to be tied to Honda against Malwarebytes Nebula, our cloud-based endpoint protection for businesses.



We detect this payload as ‘Ransom.Ekans’ when it attempts to execute. In order to test another of our protection layers, we also disabled (not recommended) the malware protection to let the behavior engine do its thing. Our anti-ransomware technology was able to quarantine the malicious file without the use of any signature.

Ransomware gangs have shown no mercy, even in this period of dealing with a pandemic. They continue to target big companies in order to extort large sums of money.

RDP has been called out as some of the lowest hanging fruit preferred by attackers. However, we also recently learned about a new SMB vulnerability allowing remote execution. It is important for defenders to properly map out all assets, patch them, and never allow them to be publicly exposed.

We will update this blog post if we come across new relevant information.

Indicators of Compromise (IOCs)

Honda related sample:

```
d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1 mds.honda.com
```

Enel related sample:

```
edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a
enelint.global
```
