

# Honda and Enel impacted by cyber attack suspected to be ransomware

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

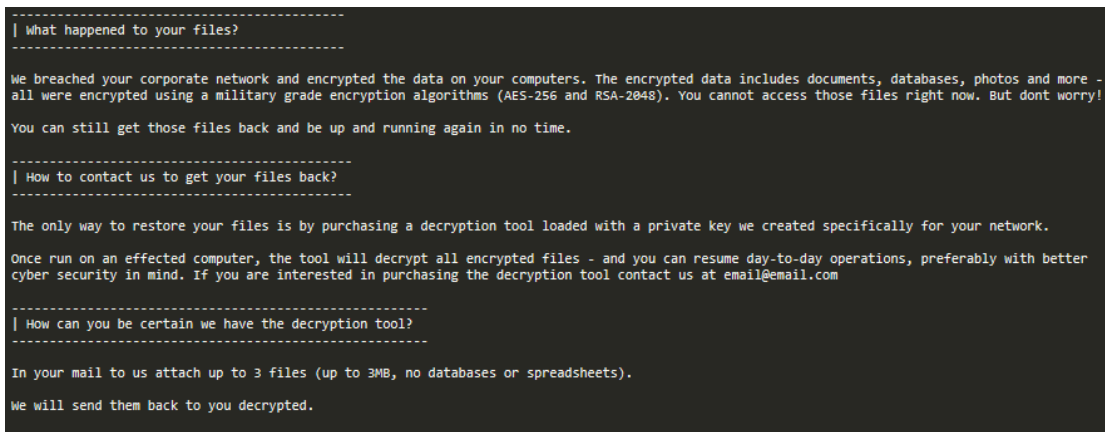
Car manufacturer Honda has been hit by a cyber attack, according to a [report](#) published by the BBC, and later confirmed by the company in a [tweet](#). Another similar attack, also [disclosed on Twitter](#), hit Edesur S.A., one of the companies belonging to Enel Argentina which operates in the business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

---

Article continues below this ad.

---

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.

The screenshot displays a debugger window with the following assembly code:

```

83 EC 4C      sub esp,4C
8D 05 01 F3 61 00 lea eax,dword ptr ds:[61F301]
89 04 24      mov dword ptr ss:[esp],eax
C7 44 24 04 0D 00 mov dword ptr ss:[esp+4],D
E8 01 7F F5 FF call honda.4ABC80
8B 44 24 08   mov eax,dword ptr ss:[esp+8]
8B 4C 24 14   mov ecx,dword ptr ss:[esp+14]
8B 54 24 0C   mov edx,dword ptr ss:[esp+C]
85 C9        test ecx,ecx
0F 85 14 01 00 00 jne honda.553EA7
85 D2        test edx,edx
0F 84 0C 01 00 00 je honda.553EA7
89 54 24 20   mov dword ptr ss:[esp+20],edx
31 C9        xor ecx,ecx
31 DB        xor ebx,ebx
EB 16        jmp honda.553DBB
8B 6C 24 48   mov ebp,dword ptr ss:[esp+48]
83 C5 0C      add ebp,C
8B 74 24 24   mov esi,dword ptr ss:[esp+24]
8D 4E 01      lea ecx,dword ptr ds:[esi+1]
8B 54 24 20   mov edx,dword ptr ss:[esp+20]
89 C3        mov ebx,eax
89 E8        mov eax,ebp
39 D1        cmp ecx,edx
7D 5E        jge honda.553E1D
89 4C 24 24   mov dword ptr ss:[esp+24],ecx
88 5C 24 1F   mov byte ptr ss:[esp+1F],b1
89 44 24 48   mov dword ptr ss:[esp+48],eax
8B 48 04      mov ecx,dword ptr ds:[eax+4]
8B 10        mov edx,dword ptr ds:[eax]
8B 58 08      mov ebx,dword ptr ds:[eax+8]
89 14 24      mov dword ptr ss:[esp],edx
89 4C 24 04   mov dword ptr ss:[esp+4],ecx
89 5C 24 08   mov dword ptr ss:[esp+8],ebx
    
```

Below the assembly code, a memory dump is visible, showing the ASCII string "MDS. HONDA. COM" at address 0046FDF3.

**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**

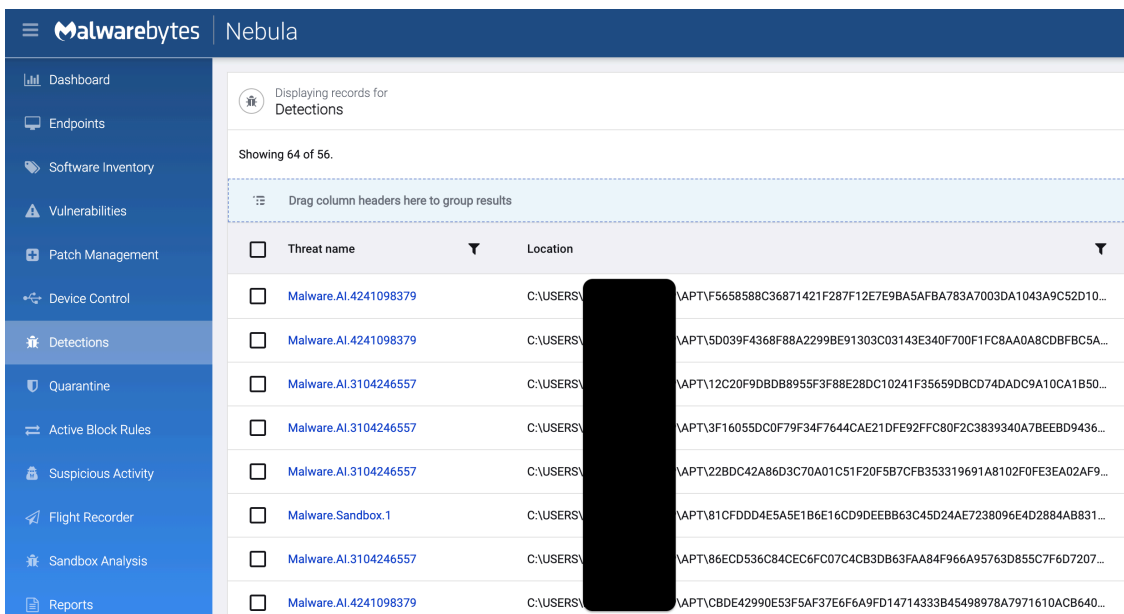
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference [here](#)). RDP attacks are one of the main entry points when it comes to targeted ransomware operations.

- 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.

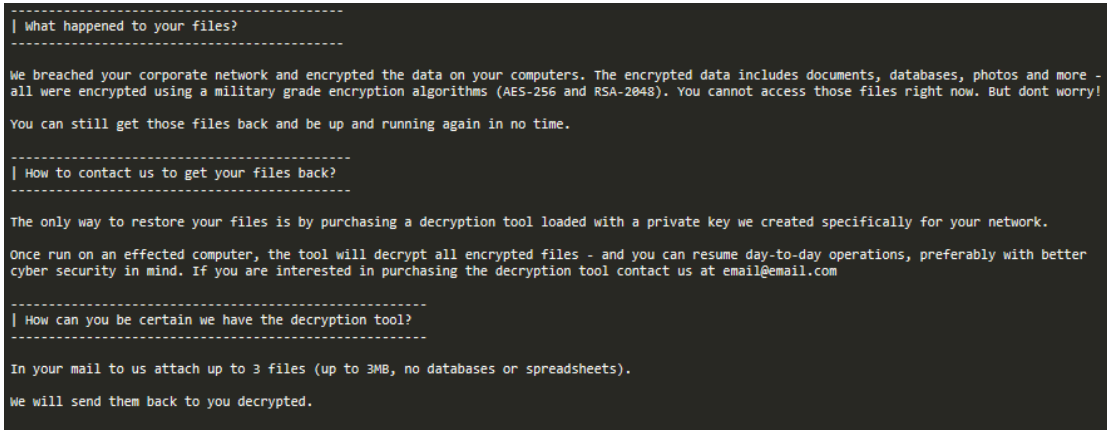
## Indicators of Compromise (IOCs)

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.

83 EC 4C sub esp,4C  
 8D 05 01 F3 61 00 lea eax,dword ptr ds:[61F301]  
 89 04 24 mov dword ptr ss:[esp],eax  
 C7 44 24 04 0D 00 mov dword ptr ss:[esp+4],D  
 E8 01 7F F5 FF call honda.4ABC80  
 8B 44 24 08 mov eax,dword ptr ss:[esp+8]  
 8B 4C 24 14 mov ecx,dword ptr ss:[esp+14]  
 8B 54 24 0C mov edx,dword ptr ss:[esp+C]  
 85 C9 test ecx,ecx  
 0F 85 14 01 00 00 jne honda.553EA7  
 85 D2 test edx,edx  
 0F 84 0C 01 00 00 je honda.553EA7  
 89 54 24 20 mov dword ptr ss:[esp+20],edx  
 31 C9 xor ecx,ecx  
 31 DB xor ebx,ebx  
 EB 16 jmp honda.553DBB  
 8B 6C 24 48 mov ebp,dword ptr ss:[esp+48]  
 83 C5 0C add ebp,C  
 8B 74 24 24 mov esi,dword ptr ss:[esp+24]  
 8D 4E 01 lea ecx,dword ptr ds:[esi+1]  
 8B 54 24 20 mov edx,dword ptr ss:[esp+20]  
 89 C3 mov ebx,eax  
 89 E8 mov eax,ebp  
 39 D1 cmp ecx,edx  
 7D 5E jge honda.553E1D  
 89 4C 24 24 mov dword ptr ss:[esp+24],ecx  
 88 5C 24 1F mov byte ptr ss:[esp+1F],b1  
 89 44 24 48 mov dword ptr ss:[esp+48],eax  
 8B 48 04 mov ecx,dword ptr ds:[eax+4]  
 8B 10 mov edx,dword ptr ds:[eax]  
 8B 58 08 mov ebx,dword ptr ds:[eax+8]  
 89 14 24 mov dword ptr ss:[esp],edx  
 89 4C 24 04 mov dword ptr ss:[esp+4],ecx  
 89 5C 24 08 mov dword ptr ss:[esp+8],ebx

0046FDF3  
 #15316F

ASCII  
 41 2E 43 4F 4D 4D MDS. HONDA. COM  
 59 6C 65 4D 61 73 61 ViewOfFileMasar  
 4D 65 6E 64 65 5F 4B m Gondimende K

**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**

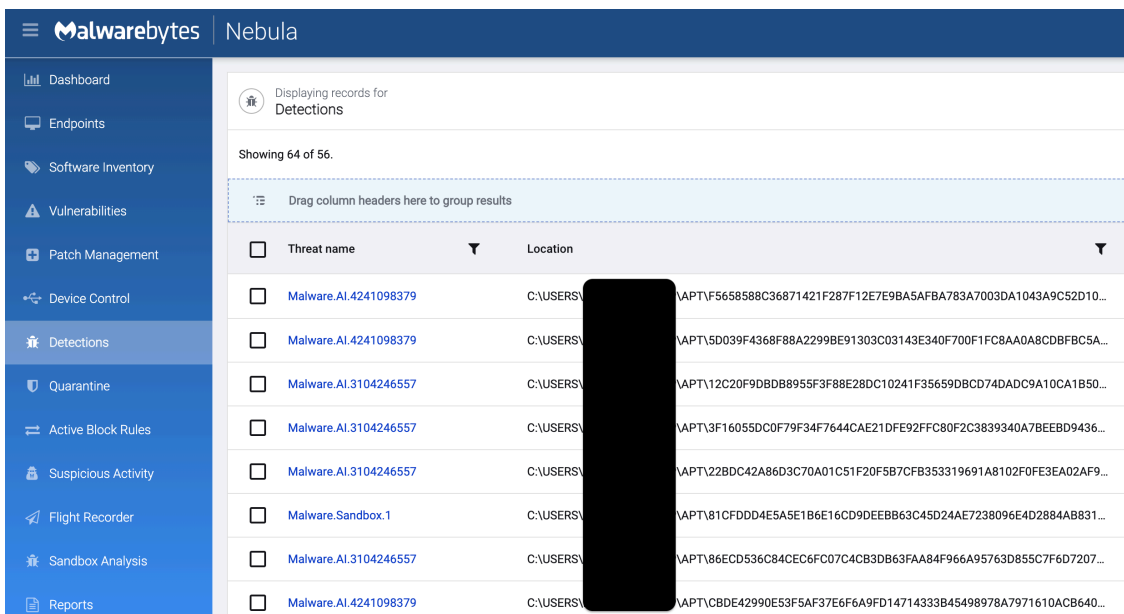
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference [here](#)). RDP attacks are one of the main entry points when it comes to targeted ransomware operations.

- 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.

The screenshot displays a debugger window with the following assembly code:

```

83 EC 4C      sub esp,4C
8D 05 01 F3 61 00  lea eax,dword ptr ds:[61F301]
89 04 24      mov dword ptr ss:[esp],eax
C7 44 24 04 0D 00  mov dword ptr ss:[esp+4],D
E8 01 7F F5 FF  call honda.4ABC80
8B 44 24 08  mov eax,dword ptr ss:[esp+8]
8B 4C 24 14  mov ecx,dword ptr ss:[esp+14]
8B 54 24 0C  mov edx,dword ptr ss:[esp+C]
85 C9        test ecx,ecx
0F 85 14 01 00 00  jne honda.553EA7
85 D2        test edx,edx
0F 84 0C 01 00 00  je honda.553EA7
89 54 24 20  mov dword ptr ss:[esp+20],edx
31 C9        xor ecx,ecx
31 DB        xor ebx,ebx
EB 16        jmp honda.553DBB
8B 6C 24 48  mov ebp,dword ptr ss:[esp+48]
83 C5 0C      add ebp,C
8B 74 24 24  mov esi,dword ptr ss:[esp+24]
8D 4E 01      lea ecx,dword ptr ds:[esi+1]
8B 54 24 20  mov edx,dword ptr ss:[esp+20]
89 C3        mov ebx,eax
89 E8        mov eax,ebp
39 D1        cmp ecx,edx
7D 5E        jge honda.553E1D
89 4C 24 24  mov dword ptr ss:[esp+24],ecx
88 5C 24 1F  mov byte ptr ss:[esp+1F],b1
89 44 24 48  mov dword ptr ss:[esp+48],eax
8B 48 04      mov ecx,dword ptr ds:[eax+4]
8B 10        mov edx,dword ptr ds:[eax]
8B 58 08      mov ebx,dword ptr ds:[eax+8]
89 14 24      mov dword ptr ss:[esp],edx
89 4C 24 04  mov dword ptr ss:[esp+4],ecx
89 5C 24 08  mov dword ptr ss:[esp+8],ebx
    
```

Below the assembly code, a memory dump shows the following ASCII string:

```

41 2E 43 4F 4D 4D MDS. HONDA. COM
59 6C 65 4D 61 73 61 ViewOfFileMasar
4D 65 6E 64 65 5F 4B m Gondimende K
    
```

**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**

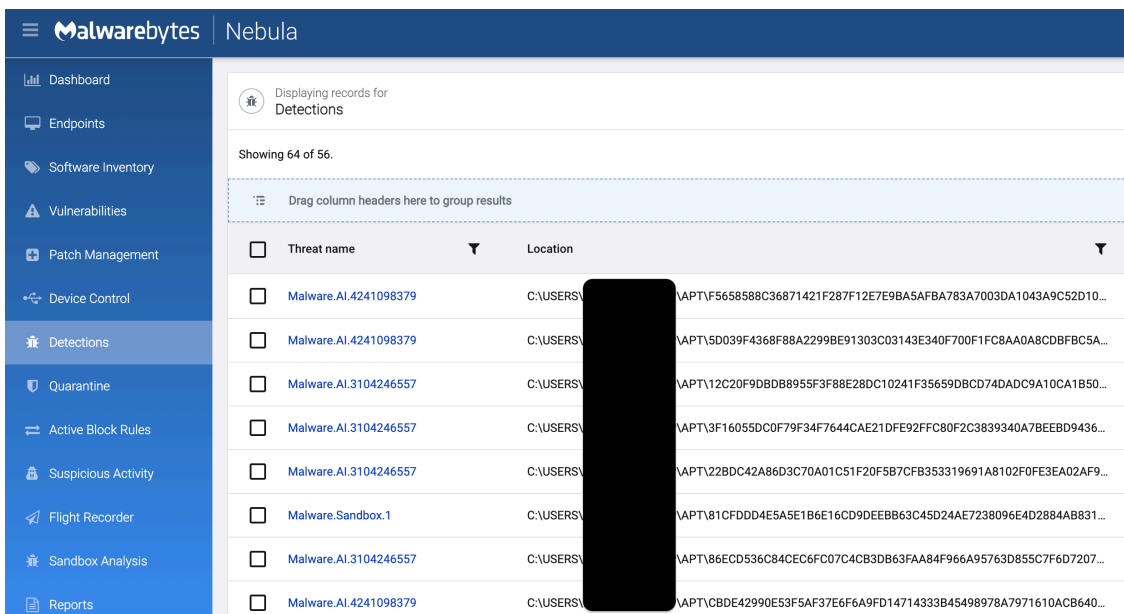
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference [here](#)). RDP attacks are one of the main entry points when it comes to targeted ransomware operations.

- 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

```

83 EC 4C      sub     esp, 4C
8D 05 01 F3 61 00  lea   eax, dword ptr ds:[61F301]
89 04 24      mov   dword ptr ss:[esp], eax
C7 44 24 04 0D 00  mov   dword ptr ss:[esp+4], D
E8 01 7F F5 FF  call  honda.4ABC80
8B 44 24 08  mov   eax, dword ptr ss:[esp+8]
8B 4C 24 14  mov   ecx, dword ptr ss:[esp+14]
8B 54 24 0C  mov   edx, dword ptr ss:[esp+C]
85 C9      test  ecx, ecx
0F 85 14 01 00 00  jne   honda.553EA7
85 D2      test  edx, edx
0F 84 0C 01 00 00  je    honda.553EA7
89 54 24 20  mov   dword ptr ss:[esp+20], edx
31 C9      xor   ecx, ecx
31 DB      xor   ebx, ebx
EB 16      jmp   honda.553DBB
8B 6C 24 48  mov   ebp, dword ptr ss:[esp+48]
83 C5 0C      add   ebp, C
8B 74 24 24  mov   esi, dword ptr ss:[esp+24]
8D 4E 01      lea  ecx, dword ptr ds:[esi+1]
8B 54 24 20  mov   edx, dword ptr ss:[esp+20]
89 C3      mov   ebx, eax
89 E8      mov   eax, ebp
39 D1      cmp   ecx, edx
7D 5E      jge  honda.553E1D
89 4C 24 24  mov   dword ptr ss:[esp+24], ecx
88 5C 24 1F  mov   byte ptr ss:[esp+1F], bl
89 44 24 48  mov   dword ptr ss:[esp+48], eax
8B 48 04      mov   ecx, dword ptr ds:[eax+4]
8B 10      mov   edx, dword ptr ds:[eax]
8B 58 08      mov   ebx, dword ptr ds:[eax+8]
89 14 24      mov   dword ptr ss:[esp], edx
89 4C 24 04  mov   dword ptr ss:[esp+4], ecx
89 5C 24 08  mov   dword ptr ss:[esp+8], ebx
    
```

Target: mds.honda.com  
 D:\r\net\_lookupIP

0046FDF3  
 #15316F

ASCII  
 41 2E 43 4F 4D 4D MDS.HONDA.COM  
 6C 65 4D 61 73 61 ViewOfFileMasat  
 D 65 6E 64 65 5F 4B m Gondimende K

**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 operations.

- 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.

Threat name	Location
<input type="checkbox"/> Malware.AI.4241098379	C:\USERS\... \APT\F5658588C36871421F287F12E7E9BA5AFBA783A7003DA1043A9C52D10...
<input type="checkbox"/> Malware.AI.4241098379	C:\USERS\... \APT\5D039F4368F88A2299BE91303C03143E340F700F1FC8AA0A8CDBFBC5A...
<input type="checkbox"/> Malware.AI.3104246557	C:\USERS\... \APT\12C20F9DB8B8955F3F88E28DC10241F35659DBCD74DADC9A10CA1B50...
<input type="checkbox"/> Malware.AI.3104246557	C:\USERS\... \APT\3F16055DC0F79F34F7644CAE21DFE92FFC80F2C3839340A7BEEBD9436...
<input type="checkbox"/> Malware.AI.3104246557	C:\USERS\... \APT\22BDC42A86D3C70A01C51F20F5B7CFB353319691A8102F0FE3EA02AF9...
<input type="checkbox"/> Malware.Sandbox.1	C:\USERS\... \APT\81CFDD4E5A5E1B6E16CD9DEEBB63C45D24AE7238096E4D2884AB831...
<input type="checkbox"/> Malware.AI.3104246557	C:\USERS\... \APT\86ECD536C84CE06FC07C4C3DB63FAA84F966A95763D855C7F6D7207...
<input type="checkbox"/> Malware.AI.4241098379	C:\USERS\... \APT\CBDE42990E53F5AF37E6F6A9FD14714333B45498978A7971610ACB640...

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
```

```
-----  
| what happened to your files?  
-----  
  
We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more -  
all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry!  
  
You can still get those files back and be up and running again in no time.  
  
-----  
| How to contact us to get your files back?  
-----  
  
The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network.  
  
Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with better  
cyber security in mind. If you are interested in purchasing the decryption tool contact us at email@email.com  
  
-----  
| How can you be certain we have the decryption tool?  
-----  
  
In your mail to us attach up to 3 files (up to 3MB, no databases or spreadsheets).  
  
We will send them back to you decrypted.
```

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.

The screenshot displays a debugger window with the following assembly code and memory dump:

```

83 EC 4C      sub esp,4C
8D 05 01 F3 61 00  lea eax,dword ptr ds:[61F301]
89 04 24      mov dword ptr ss:[esp],eax
C7 44 24 04 0D 00  mov dword ptr ss:[esp+4],D
E8 01 7F F5 FF  call honda.4ABC80
8B 44 24 08  mov eax,dword ptr ss:[esp+8]
8B 4C 24 14  mov ecx,dword ptr ss:[esp+14]
8B 54 24 0C  mov edx,dword ptr ss:[esp+C]
85 C9        test ecx,ecx
0F 85 14 01 00 00  jne honda.553EA7
85 D2        test edx,edx
0F 84 0C 01 00 00  je honda.553EA7
89 54 24 20  mov dword ptr ss:[esp+20],edx
31 C9        xor ecx,ecx
31 DB        xor ebx,ebx
EB 16        jmp honda.553DBB
8B 6C 24 48  mov ebp,dword ptr ss:[esp+48]
83 C5 0C      add ebp,C
8B 74 24 24  mov esi,dword ptr ss:[esp+24]
8D 4E 01      lea ecx,dword ptr ds:[esi+1]
8B 54 24 20  mov edx,dword ptr ss:[esp+20]
89 C3        mov ebx,eax
89 E8        mov eax,ebp
39 D1        cmp ecx,edx
7D 5E        jge honda.553E1D
89 4C 24 24  mov dword ptr ss:[esp+24],ecx
88 5C 24 1F  mov byte ptr ss:[esp+1F],b1
89 44 24 48  mov dword ptr ss:[esp+48],eax
8B 48 04      mov ecx,dword ptr ds:[eax+4]
8B 10        mov edx,dword ptr ds:[eax]
8B 58 08      mov ebx,dword ptr ds:[eax+8]
89 14 24      mov dword ptr ss:[esp],edx
89 4C 24 04  mov dword ptr ss:[esp+4],ecx
89 5C 24 08  mov dword ptr ss:[esp+8],ebx
    
```

The memory dump shows the following ASCII string:

```

41 2E 43 4F 4D 4D MDS. HONDA. COM
59 6C 65 4D 61 73 61 ViewOfFileMasar
D 65 6E 64 65 5F 4B m Gondimende K
    
```

**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**

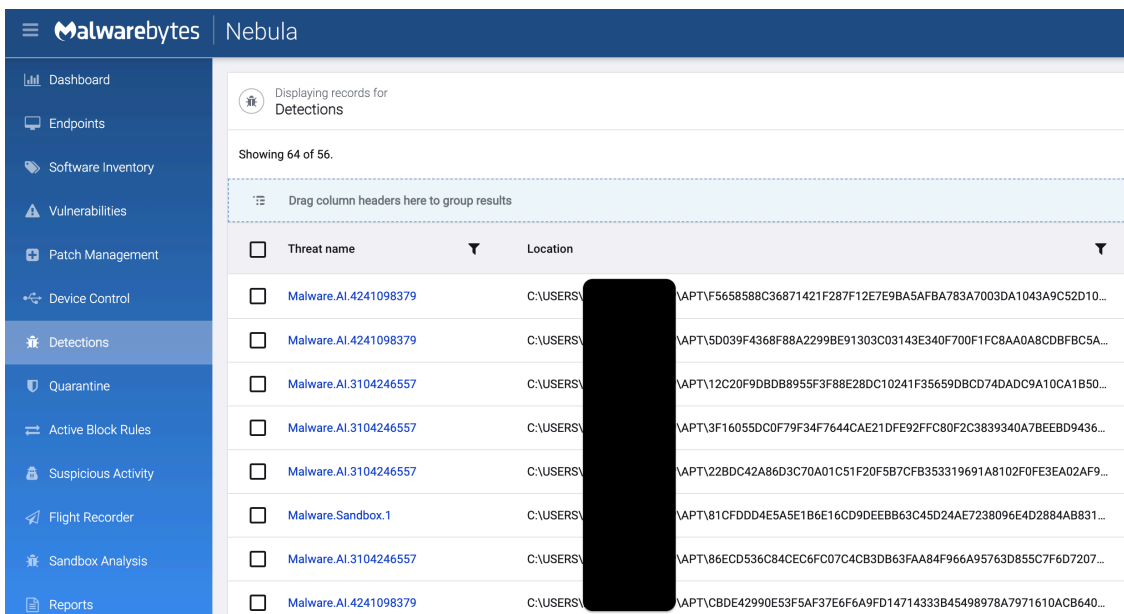
Both companies had some machines with Remote Desktop Protocol (RDP) access publicly exposed (reference [here](#)). RDP attacks are one of the main entry points when it comes to targeted ransomware operations.

- 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.

```

83 EC 4C      sub esp,4C
8D 05 01 F3 61 00 00  lea eax,dword ptr ds:[61F301]
89 04 24      mov dword ptr ss:[esp],eax
C7 44 24 04 0D 00 00  mov dword ptr ss:[esp+4],D
E8 01 7F F5 FF      call honda.4ABC80
8B 44 24 08      mov eax,dword ptr ss:[esp+8]
8B 4C 24 14      mov ecx,dword ptr ss:[esp+14]
8B 54 24 0C      mov edx,dword ptr ss:[esp+C]
85 C9          test ecx,ecx
0F 85 14 01 00 00  jne honda.553EA7
85 D2          test edx,edx
0F 84 0C 01 00 00  je honda.553EA7
89 54 24 20      mov dword ptr ss:[esp+20],edx
31 C9          xor ecx,ecx
31 DB          xor ebx,ebx
EB 16          jmp honda.553DBB
8B 6C 24 48      mov ebp,dword ptr ss:[esp+48]
83 C5 0C          add ebp,C
8B 74 24 24      mov esi,dword ptr ss:[esp+24]
8D 4E 01          lea ecx,dword ptr ds:[esi+1]
8B 54 24 20      mov edx,dword ptr ss:[esp+20]
89 C3          mov ebx,eax
89 E8          mov eax,ebp
39 D1          cmp ecx,edx
7D 5E          jge honda.553E1D
89 4C 24 24      mov dword ptr ss:[esp+24],ecx
88 5C 24 1F      mov byte ptr ss:[esp+1F],b1
89 44 24 48      mov dword ptr ss:[esp+48],eax
8B 48 04          mov ecx,dword ptr ds:[eax+4]
8B 10          mov edx,dword ptr ds:[eax]
8B 58 08          mov ebx,dword ptr ds:[eax+8]
89 14 24          mov dword ptr ss:[esp],edx
89 4C 24 04      mov dword ptr ss:[esp+4],ecx
89 5C 24 08      mov dword ptr ss:[esp+8],ebx

```

mds.honda.com  
D: '\\r'  
net\_lookupIP

0046FDF3  
#15316F

Dump 3 | Dump 4 | Dump 5 | Watch 1 | Struct

ASCII	
41 2E 43 4F 4D 4D	MDS. HONDA. COM
6C 65 4D 61 73 61	ViewOfFileMasar
65 6E 64 65 5F 4B	m Gondimende K

**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 operations.

- 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.

Threat name	Location
Malware.AI.4241098379	C:\USERSV\APT\F5658588C36871421F287F12E7E9BA5AFBA783A7003DA1043A9C52D10...
Malware.AI.4241098379	C:\USERSV\APT\5D039F4368F88A2299BE91303C03143E340F700F1FC8AA0A8CDBFBC5A...
Malware.AI.3104246557	C:\USERSV\APT\12C20F9DBDB8955F3F88E28DC10241F35659DBCD74DADC9A10CA1B50...
Malware.AI.3104246557	C:\USERSV\APT\3F16055DC0F79F34F7644CAE21DFE92FFC80F2C3839340A7BEEBD9436...
Malware.AI.3104246557	C:\USERSV\APT\22BDC42A86D3C70A01C51F20F5B7CFB353319691A8102F0FE3EA02AF9...
Malware.Sandbox.1	C:\USERSV\APT\81CFDD4E5A5E1B6E16CD9DEEBB63C45D24AE7238096E4D2884AB831...
Malware.AI.3104246557	C:\USERSV\APT\86ECD536C84CE6FC07C4CB3DB63FAA84F966A95763D855C7F6D7207...
Malware.AI.4241098379	C:\USERSV\APT\CBDE42990E53F5AF37E6F6A9FD14714333B45498978A7971610ACB640...

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
```

---

Source: <https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/>