Honda and Enel impacted by cyber attack suspected to be ransomware

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

Threat Intelligence Team June 10, 2020

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.

Honda Ransomware Attack 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.

```
-------------------------------------------
| 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.
```

Figure 1: EKANS ransom note

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.

```
89 E6              mov esi,esp
E8 95 89 EF FF     call honda.44B3EE
8B 05 14 99 7C 00  mov eax,dword ptr ds:[7C9914]
8B 0D 10 99 7C 00  mov ecx,dword ptr ds:[7C9910]   ecx:"EKANS", 7C9910:&"EKANS"
89 0C 24           mov dword ptr ss:[esp],ecx      [esp]:"EKANS"
89 44 24 04        mov dword ptr ss:[esp+4],eax
E8 DF 12 00 00     call honda.553D50               DNS_Resolver_Mutex_check
0F B6 44 24 08     movzx eax,byte ptr ss:[esp+8]
84 C0              test al,al
0F 84 3D 01 00 00  je honda.552BBB
E8 7D 16 00 00     call honda.554100
E8 78 91 02 00     call honda.57BC00
8B 04 24           mov eax,dword ptr ss:[esp]      [esp]:"EKANS"
8B 4C 24 04        mov ecx,dword ptr ss:[esp+4]
C7 04 24 00 00 00  mov dword ptr ss:[esp],0        [esp]:"EKANS"
89 44 24 04        mov dword ptr ss:[esp+4],eax
89 4C 24 08        mov dword ptr ss:[esp+8],ecx
E8 ED 7E EE FF     call honda.43A990
8B 44 24 14        mov eax,dword ptr ss:[esp+14]
8B 4C 24 10        mov ecx,dword ptr ss:[esp+10]
8B 54 24 0C        mov edx,dword ptr ss:[esp+C]
89 14 24           mov dword ptr ss:[esp],edx      [esp]:"EKANS"
89 4C 24 04        mov dword ptr ss:[esp+4],ecx
89 44 24 08        mov dword ptr ss:[esp+8],eax
E8 B1 6B F9 FF     call honda.4E9670
8B 44 24 0C        mov eax,dword ptr ss:[esp+C]
89 44 24 1C        mov dword ptr ss:[esp+1C],eax
85 C0              test eax,eax
0F 84 C5 00 00 00  je honda.552B94
E8 4C 93 02 00     call honda.57BE20
8B 04 24           mov eax,dword ptr ss:[esp]      [esp]:"EKANS"
8B 4C 24 04        mov ecx,dword ptr ss:[esp+4]
8B 54 24 1C        mov edx,dword ptr ss:[esp+1C]
8B 1A              mov ebx,dword ptr ds:[edx]
```

Figure 2: Mutex check

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.

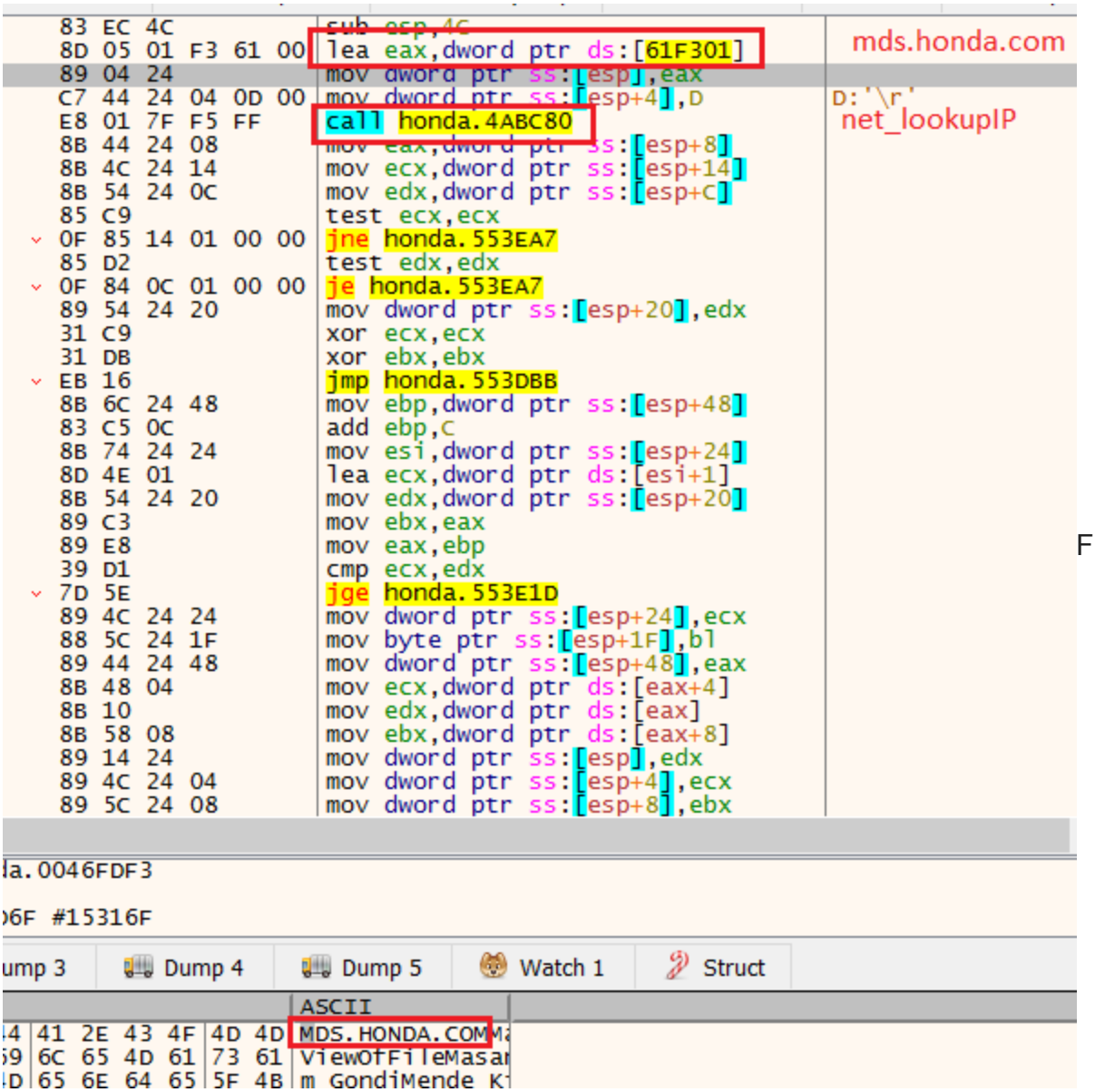

Figure 3: Function responsible for performing DNS query

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.

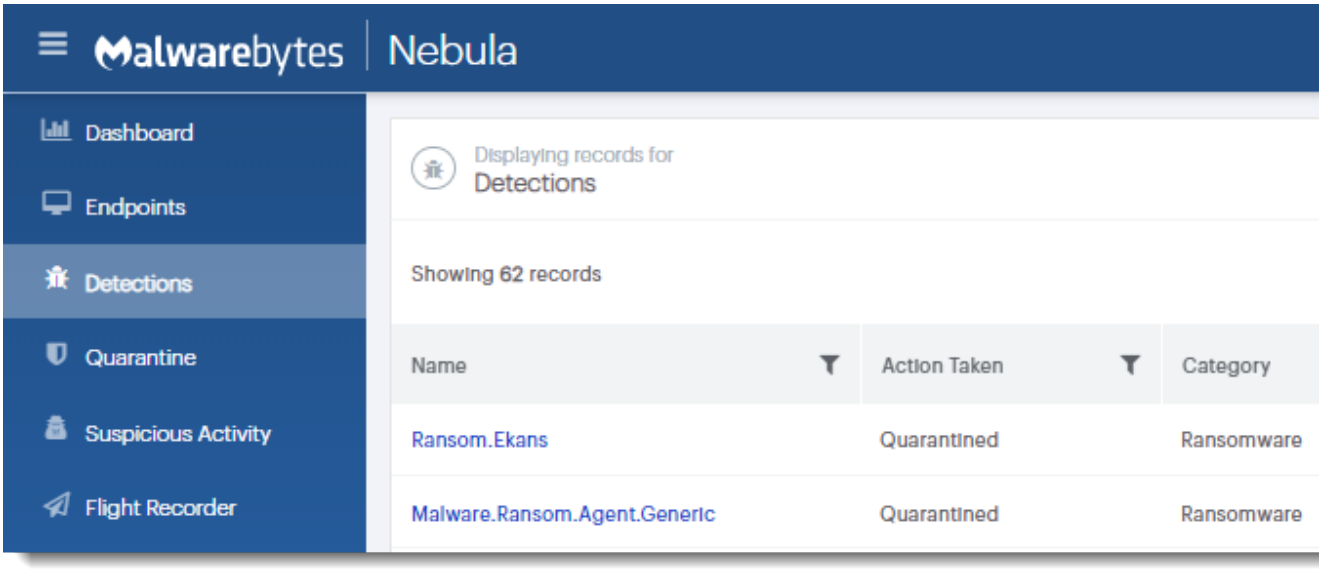

Figure 4: Malwarebytes Nebula dashboard showing detections

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
```