The Snake Attacks Holding the Industrial Sector Ransom

By Maxim Smoliansky

Published: 2020-06-29 · Archived: 2026-04-06 00:06:05 UTC

For years ransomware attacks are a significant threat to any organization, no matter its size, field of expertise, yearly revenue or geographical location. The year 2020 is no exception. Ransomware attacks became more sophisticated, crews operating them learned how to take better advantage of their presence in the victim's network and new ransomware strains were brought into the world to run havoc and make their creators rich.

One such ransomware is Snake (aka Ekans). It became well known in January after its first sample was uploaded to VirusTotal. The initial sample, found by the MalwareHunterTeam crew, raised a lot of concern as the malware was designed to kill computer processes related to Industrial Control Systems, implying that it was built with victims from the industrial sector in mind. Unfortunately, this concern was justified as after a few months of relative silence, Snake operators deployed the ransomware in a series of targeted and devastating attacks. The crescendo was an attack on the Japanese car manufacturer Honda on June 8th, an attack that made Honda's operations in Japan and Europe grind to a halt.

Fortunately, Deep Instinct prevents all versions of Snake ransomware. The ransomware is prevented pre-execution, using Deep Instinct's deep learning-based static prevention engine, and during on-execution, using advanced ransomware behavioral protection.

Moreover, Deep Instinct's unique deep learning approach ensured Snake ransomware was prevented with a version of our prediction model (D-Brain) that was released over a year before the malware's release.

Watch the demo of how Deep Instinct prevents Snake Ransomware

Less is More

Snake joins Maze, DopplePaymer, Ako, and others in the lucrative group of ransomware families that target corporations. Instead of relying on sporadic means of distribution, in which the quantity of infections is more important than the “quality” of each infection, Snake chooses specific targets in the corporate world so that each infection will yield much more revenue.

The goal of such ransomware is much more ambitious. Instead of encrypting one machine and demanding the ransom for its contents, they strive to encrypt all the workstations connected to a network. The ransomware takes the time to explore the environment’s topology and critical systems to exploit vulnerabilities, stolen credentials, and poor security hygiene to propagate through the network. The ransom for decrypting all the machines in a corporate network can be millions of dollars, compared to “just” thousands of dollars from an infection of a single workstation.

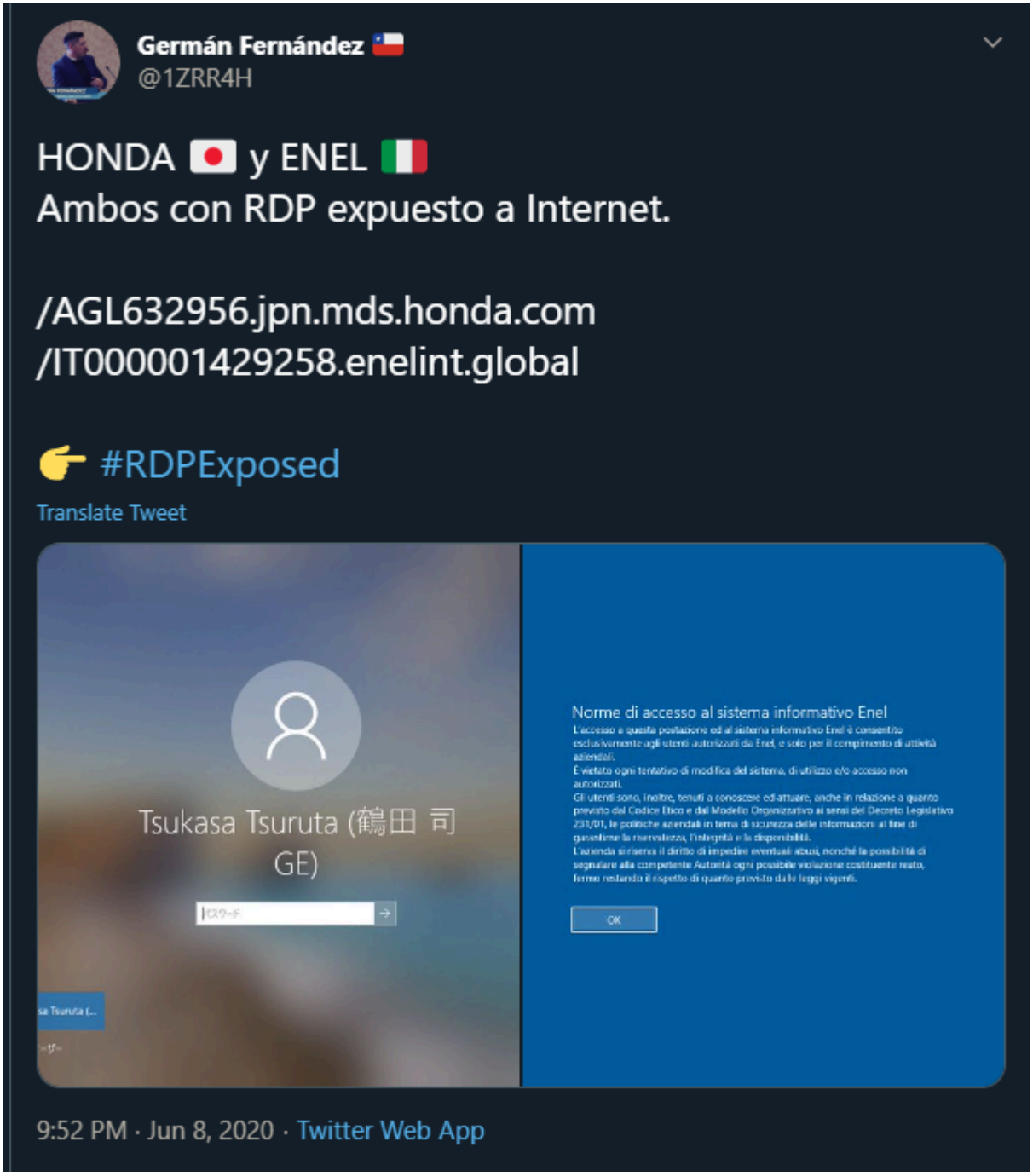
Snake also belongs to a more niche part of the ransomware world. Together with Megacortex, Snake contains a list of ICS related processes to stop before encryption. Killing these processes allows the ransomware to encrypt the files these programs use and deny the target access to its production-related assets, thus inflicting much greater damage and increasing the possibility of ransom payment.

The Subtle Serpent

These three alleged Snake ransomware attacks became public:

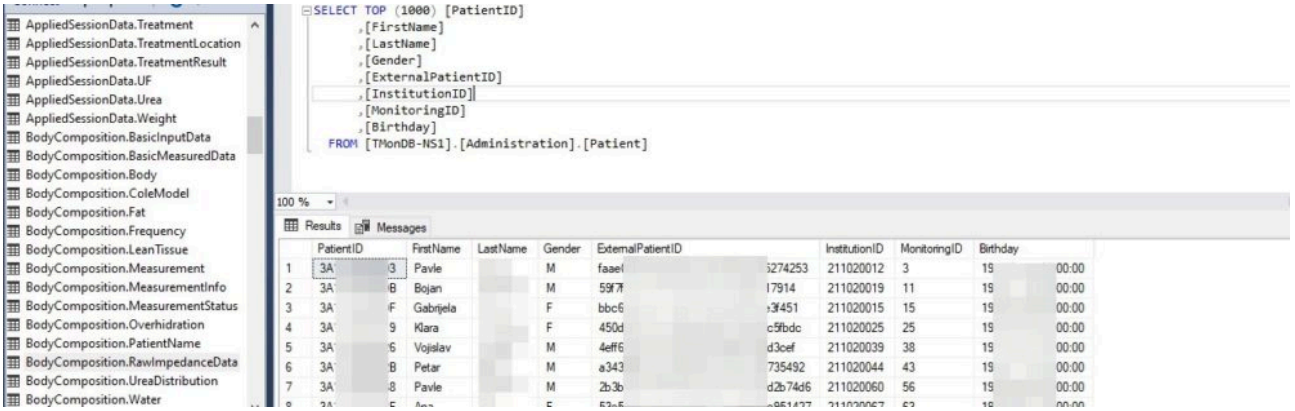
- An attack on the largest private hospital in Europe, Fresenius, on May 6th.
- The Italian energy company Enel, that operates in several parts of Europe, on June 7th.
- The Japanese car manufacturer Honda on June 8th.

And according to several sources, there are possibly more that were kept secret.
Although it is currently unclear how it found its way into the networks of its victims, bad security practices as shown in the tweet below might give us a hint.



This screenshot shows computers belonging to Honda and Enel with RDP services openly exposed and accessible from the Internet. An exposed RDP port might be easily exploited using a vulnerability or a brute-force attack.

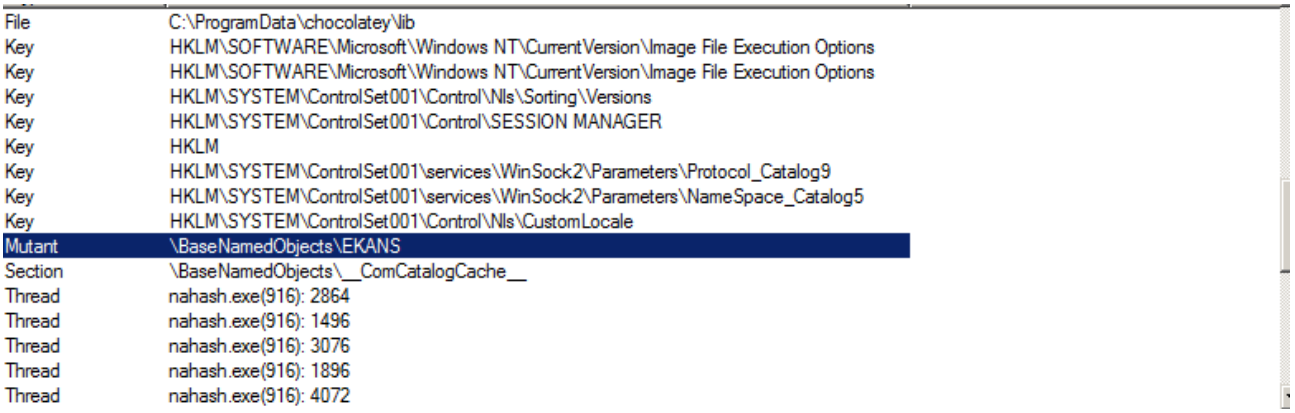
Other means might have been used by the threat actors, such as phishing attacks, malicious documents or previous malware infections, potentially with several of them used together. It is also unknown what were the specific actions performed by the malicious actors before initiating the encryption process. But we do know, based on the images published by the Snake crew, that in the case of Fresenius, the data was exfiltrated before being encrypted.



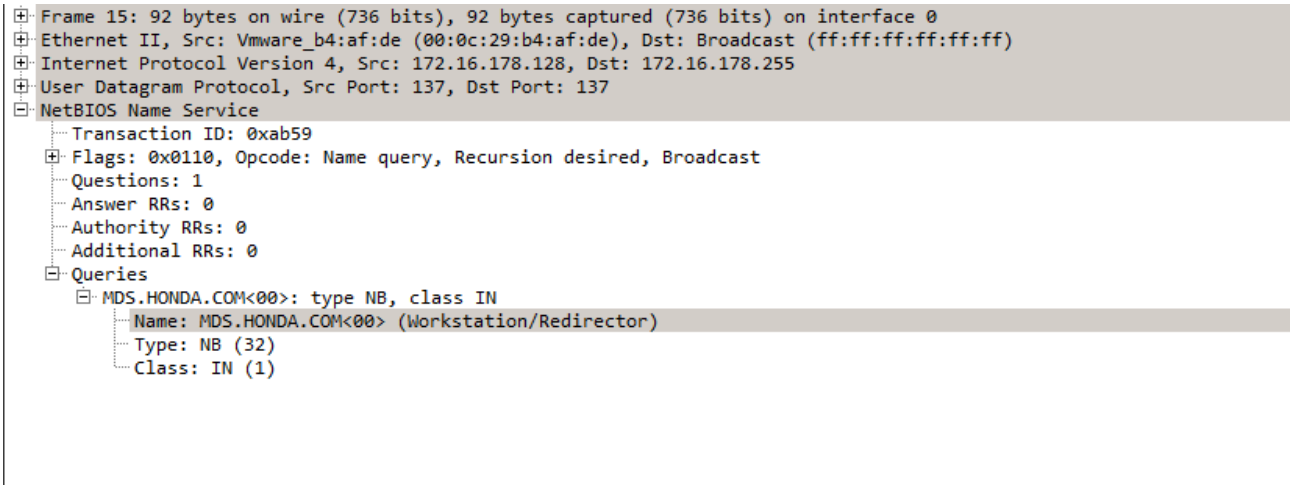
Credit: BleepingComputer.com

Snake executables are 3-4MB, unsigned, 32-bit EXE files written in the Go programming language.
There are several Snake samples publicly available. We chose to focus on the sample that was allegedly used in the attack on Honda (SHA256: d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1) and was initially uploaded with the name nmon.exe to VirusTotal which may indicate the name the attackers chose.

Upon execution, the ransomware will make sure that it is being run only once by using a mutex named “EKANS”.



Then, it will try to verify that it is running in the victim’s network by trying to resolve Honda’s internal domain name *mds.honda.com* using DNS and NetBIOS. In the case of Enel the domain name is *enelint.global*.



If the resolution is unsuccessful the ransomware will exit without any encryption done. Editing the Windows hosts file in order to provide Snake with a random IP address will not yield any results, which indicates that the malware is not only checking the availability of the domain but also expects it to have a specific IP address.

Looking for the domain name in the strings the malware stores in the computer's RAM we were able to see what seemed to be an IP address 170[.]108.71.153 or 170[.]108.71.15. We were then able to run the malware using the IP address 170[.]108.71.15 as the resolution for the domain.

```
wkp)170.108.71.1538146972656253Co
B+*7gi`Oo
eAiC
CertOpenStoreDQ
FindFirstFileFindNextFileWFreeAddrInfoWGC sweep waitG
MDS.HONDA.COMMapViewOfFileMasaram_GondiMende_KikakuiN
```

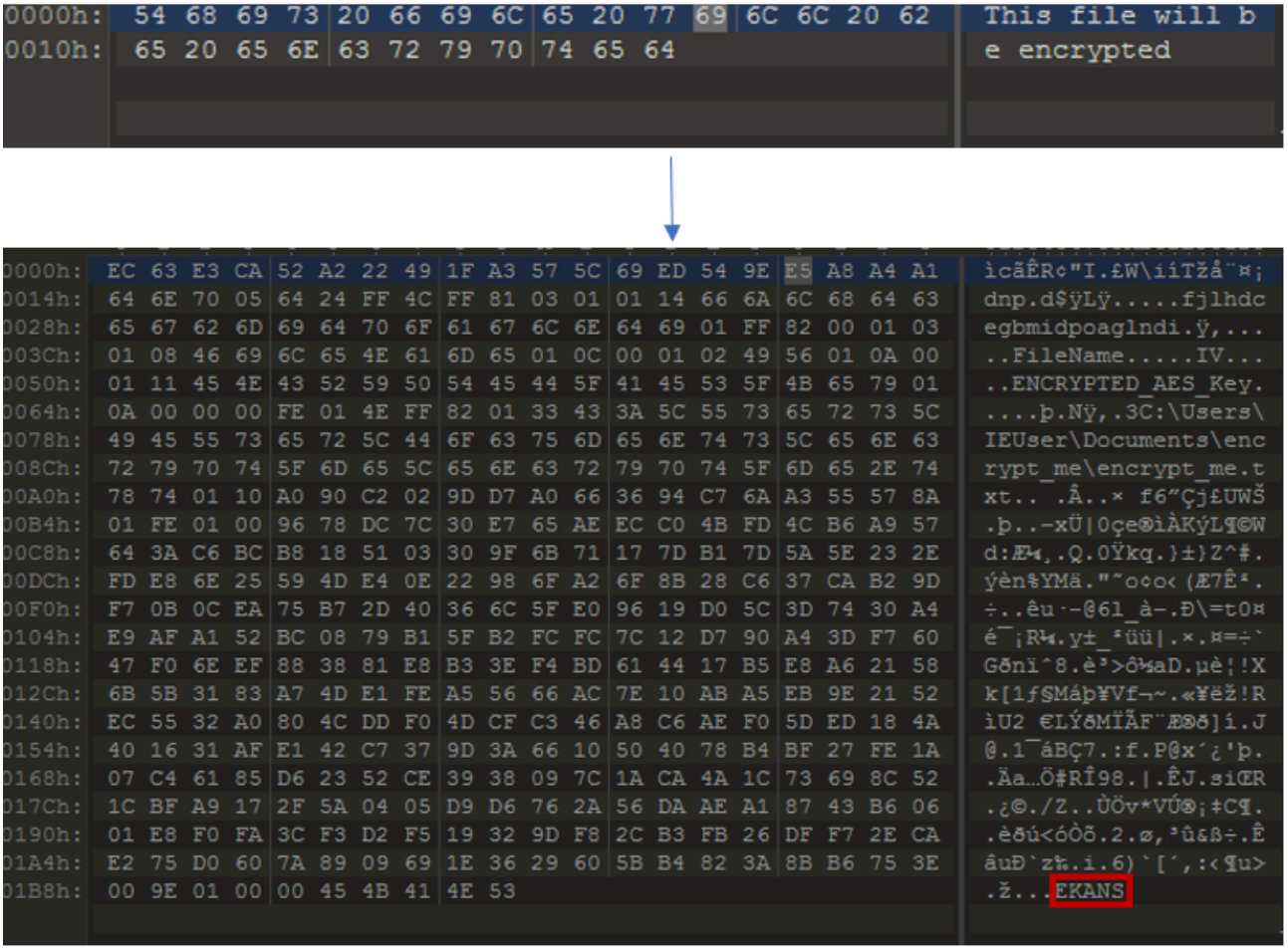
Before initiating the encryption, Snake will utilize the Windows firewall in order to block any incoming and outgoing network connections on the victim's machine that aren't configured in the firewall. Windows built-in netsh tool will be used for this purpose.

```
Path:       C:\Windows\SysWOW64\netsh.exe
Command:    netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound
Path:       C:\Windows\SysWOW64\netsh.exe
Command:    netsh advfirewall set allprofiles state on
```

Disconnected from the outside world, Snake will kill the hardcoded processes that may interfere with the encryption. This list contains processes related to the industrial world and several security and backup solutions.

Once all the preparations are completed, the ransomware can initiate the encryption process.
Excluding several system-critical folders and files, all files with extensions included in Snake's hardcoded list are included. The list includes document, virtualization, database, and archive extensions among others.

Every encrypted file will have a random five-character string appended to its extension and the word EKANS appended to the end of the file. For example, our *encrypt_me.txt* file was changed to *encrypt_me.txtDwtwx* and the word "EKANS" was added to the end of the encrypted content.



After all, files have been encrypted, netsh is called again in order to disable the firewall.

```
Path:       C:\Windows\SysWOW64\netsh.exe
Command:    netsh advfirewall set allprofiles state off
```

According to several reports, once the encryption is finished a ransom note should be dropped to C drive and the desktop. In our case, after running the malware several times with different configurations, it didn't write the ransom note to the disk.

Conclusion

The concept of ransomware is rather simple - you encrypt your victims' files and wait for them to pay. Although this concept hasn't changed in recent years, ransomware attacks have become more and more sophisticated and targeted, as we witness the gradual change in the priorities, tactics and scale of attacks.

If the attackers are changing their *modus operandi*, we should change the way we think about ransomware attacks. We should think of the ransomware itself as part of a bigger attack. The attackers might have been present on the network for a while, stealing confidential data that will later be sold to the highest bidder, they might even be there after the ransomware attack is successful. Ransomware is not just an attack on data, but also an attack on confidentiality, the privacy of customers, financial status and company reputation.

Snake ransomware possesses all the above in a single executable. It is also an example of ransomware operators' entrance into the industrial domain that was previously dominated by state-sponsored APT groups.

We should presume that the ever-growing greed of ransomware creators and operators will drive them to choose bigger and bigger targets with emphasis on critical infrastructures as their victims.

IOCs

e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60

a5a7e6ddf99634a253a060adb1f0871a5a861624382e8ca6d086e54f03bed493

b17863d41c0b915052fea85a354ec985280f4d38b46d64158a75b17ef89d76da

a8f0ff40d1e624dd2aad4d689ed47a900e4f719923647cacb58d1a4809c7bd31

d4da69e424241c291c173c8b3756639c654432706e7def5025a649730868c4a1

09133f97793186542546f439e518554a5bb17117689c83bc3978cc532ae2f138

edef8b955468236c6323e9019abb10c324c27b4f5667bc3f85f3a097b2e5159a

---