Targeted attacks on industrial companies using Snake ransomware

Date: June 17, 2020

Updated: July 7, 2020

According to Kaspersky ICS CERT data, a number of industrial companies are currently experiencing targeted attacks involving the Snake encryption ransomware.

On June 8, 2020 issues were reported which affected the computer networks of Honda, a Japanese motorcycle and auto manufacturer, in Europe and Japan. Specifically, it was announced that Honda Customer Service and Honda Financial Services were experiencing technical difficulties. Information security experts believe that, in all likelihood, one of the company's servers was infected with Snake (EKANS) ransomware.

A sample of the Snake malware discovered by some researchers on VirusTotal checked for Honda's domain name, "mds.honda.com" (which is probably used on the company's internal network). If the domain name cannot be resolved (i.e., if the corresponding IP address cannot be determined), the ransomware terminates without encrypting any files. According to the researchers, this could indicate that the attackers' activity is targeted.

Kaspersky ICS CERT experts used their own telemetry data do identify other samples that were similar to the sample uploaded to VirusTotal. Based on the findings of our research:

1. The malware was launched using a "nmon.bat" file detected by Kaspersky products in domain policy script folders.
2. The only difference between all of the Snake samples identified is the domain name and IP address embedded in the code.
3. The IP address embedded in the malware code is compared with the IP address resolved from the domain name, if the malware was able to resolve it.
4. The malware encrypts data only if the IP address embedded in the malware code matches the IP address resolved from the domain name that is also embedded in the malware code.
5. The IP address and domain name combination embedded in the malware code is unique for each attack we have identified and is apparently valid for the internal network of the organization targeted by that specific attack.
6. In some cases, the domain names may have been obtained from public sources (DNS), while information on IP addresses associated with these domain names is apparently stored on internal DNS servers and is only available when sending DNS requests from the victim organizations' internal networks.
7. In addition to the domain name and IP address of the organization under attack, which are embedded into the malware code, new Snake samples are different from those identified in December 2019 in that they include an extended list of file extensions (types) that the malware should encrypt. The new samples include extensions for virtual drive files, Microsoft Access, source code in C/C#/ASP/JSP/PHP/JS, as well as the corresponding files of projects/solutions and other extensions that were unsupported by earlier samples.

The results of our research clearly indicate that the attackers carry out multistage hacker attacks, each attack targeting a specific organization. Encrypting files using Snake is the final stage of these attacks.

Each Snake sample was apparently compiled after the attackers had gained the knowledge of the relevant domain name and its associated IP address on the company's internal network. In the malware samples analyzed, the IP address and domain name are stored as strings. This means that the executable file cannot be easily changed (patched) after compilation because the length of these strings varies.

Clearly, checking that the domain name matches the IP address is a technique designed to prevent the malware from running outside the local network for which the sample was created.

It is most likely that the attackers used domain policies to spread the ransomware across the local network. In that case, they had access to the domain administrator's account, compromised in the attack's earlier stages.

It is known that, in addition to Honda, victims include power company Enel Group. According to Kaspersky ICS CERT data, attack targets also include a German company that supplies its products to auto makers and other industrial manufacturers and a German manufacturer of medical equipment and supplies. Apparently, other auto makers and manufacturing companies have also been attacked: similar Snake samples have been detected on computers in China, Japan and Europe. We believe the attack may have gone beyond the victims' IT systems. Specifically, in one case, the malware was detected and blocked on the video surveillance server of an organization attacked in China.

All malware samples were proactively blocked by Kaspersky products using the heuristic signature Trojan-Ransom.Win32.Snake.a, which was created using the original Snake sample that appeared in December 2019.

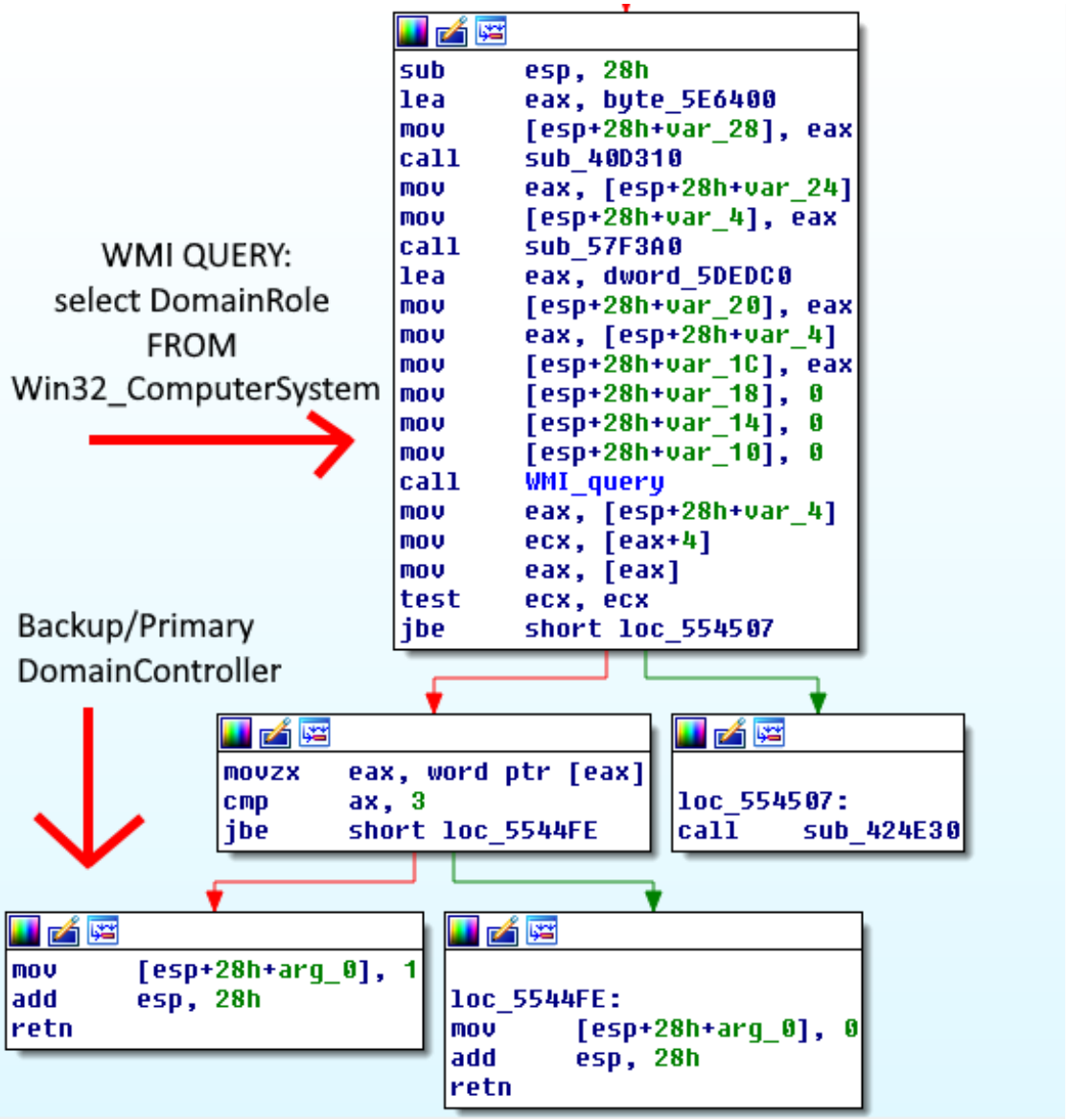
It is worth reminding that an important distinguishing feature of Snake is that it targets, among other things, industrial automation systems – specifically that it is designed to encrypt files used by General Electric ICS. This is evidenced by the fact that the malware attempts to terminate the processes of General Electric software before starting the file encryption process.

Attacks similar to those described above continue. If you have encountered an attack of this kind, you can report it via a special form on our website.

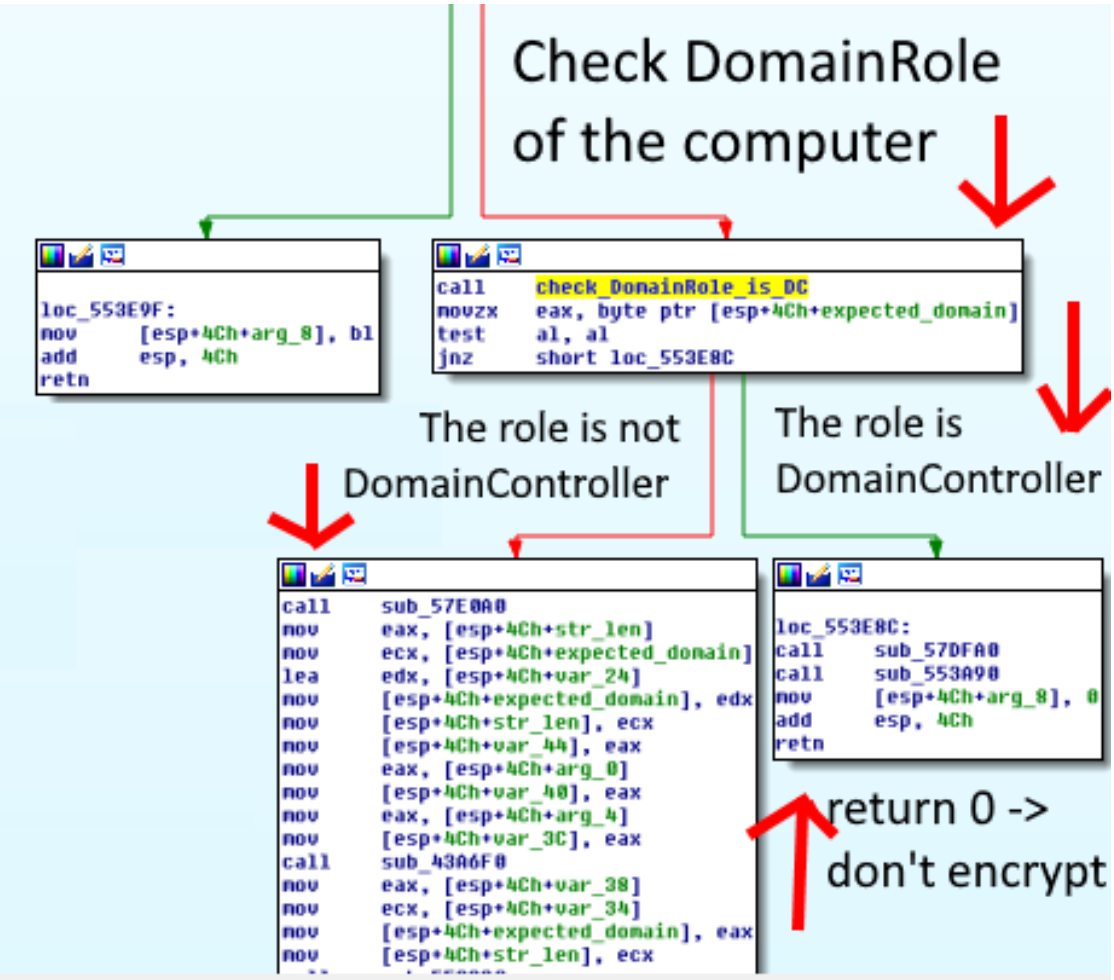
July 7, 2020 update

Our hypothesis that the attackers used the attacked company's domain controller to spread the ransomware across the local network is supported by one more curious fact.

The malware checks the domain role of the computer on which it is running. If the computer has the domain controller role (DomainController), the function returns the value "1".



If the function that checks the attacked computer's domain role returns "1" (i.e., the computer has the role of a primary or backup domain controller), the function that calls it returns "0". This results in the malware terminating without performing any encryption. The calling function also checks whether the domain's IP address matches the hard-coded IP address.



This means that if, as we believe, the attackers used the domain controller to spread the malware across the victim's local network, the domain controller exclusion logic described above would certainly work for them, since they needed the domain controller to be operational and unencrypted.

Recommendations

To identify traces of an attack and prevent possible damage, Kaspersky ICS CERT recommends:

- Using the indicators of compromise provided to identify infections on Windows workstations and servers;
- Checking active domain policies and scripts for malicious code;
- Checking active tasks in the Windows Task Scheduler on workstations and servers for malicious code;
- Changing the passwords of all accounts in the domain administrator group.

Indicators of compromise

MD5

- ED3C05BDE9F0EA0F1321355B03AC42D0
- 7DDB09DB3FB9B01FA931C2A1A41E13E1
- C547141B8A690EEE313C0F6CE6B5CCA6
- 47EBE9F8F5F73F07D456EC12BB49C75D
- D659325EA3491708820A2BEFFE9362B8
- C7C39967E16500C37638AB24F1BB3FF9
- F58A00D132205045F8AA4C765239301F
- D1277A10494B5D2D5B21B2488C650D3A
- 1E296139AF94AFC2F6002969E8EA750E
- E52927F8E4A22B4D9FD463637A8696EE
- 6DDD81BE14DFC8354AEB63220CFE112E
- DC68AE3CC7BDB1EC80C72FC9F0E93255

File names

- nmon.exe
- nmon.bat
- KB3020369.exe
- KB[7 random numbers].exe

Folders in which malicious objects can be located

- %WinTemp%
- \sysvol\[domain name]\scripts\

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com