

SNAKE Ransomware Is the Next Threat Targeting Business Networks

By Lawrence Abrams

Published: 2020-01-08 · Archived: 2026-04-05 21:33:22 UTC



Since network administrators didn't already have enough on their plate, they now have to worry about a new ransomware called SNAKE that is targeting their networks and aiming to encrypt all of the devices connected to it.

Enterprise targeting, or big-game hunting, ransomware are used by threat actors that infiltrate a business network, gather administrator credentials, and then use post-exploitation tools to encrypt the files on all of the computers on the network.

The list of enterprise targeting ransomware is slowly growing and include [Ryuk](#), [BitPaymer](#), [DoppelPaymer](#), [Sodinokibi](#), [Maze](#), [MegaCortex](#), [LockerGoga](#), and now the Snake Ransomware.



Visit Advertiser website [GO TO PAGE](#)

What we know about the Snake Ransomware

Snake Ransomware was discovered by [MalwareHunterTeam](#) last week who shared it with [Vitali Kremez](#) to reverse engineer and learn more about the infection.

Based on the analysis performed by Kremez, this ransomware is written in Golang and contains a much higher level of obfuscation than is commonly seen with these types of infections.

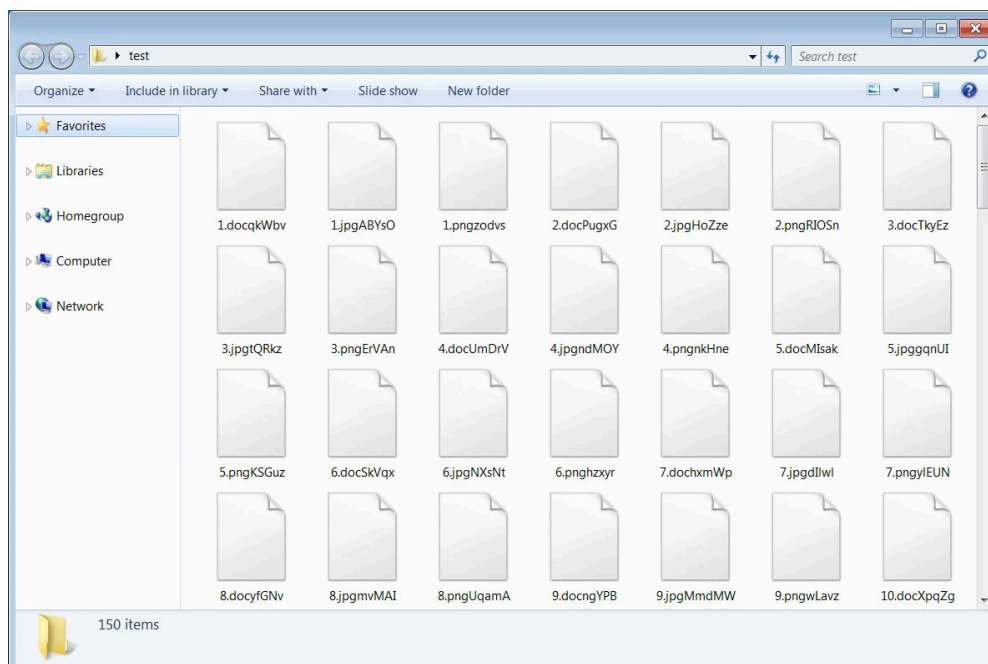
"The ransomware contains a level of routine obfuscation not previously and typically seen coupled with the targeted approach," Kremez, Head of [SentinelLabs](#), told BleepingComputer in a conversation.

When started Snake will remove the computer's Shadow Volume Copies and then kill numerous processes related to SCADA systems, virtual machines, industrial control systems, remote management tools, network management software, and more.

It then proceeds to encrypt the files on the device, while skipping any that are located in Windows system folders and various system files. The list of system folders that are skipped can be found below:

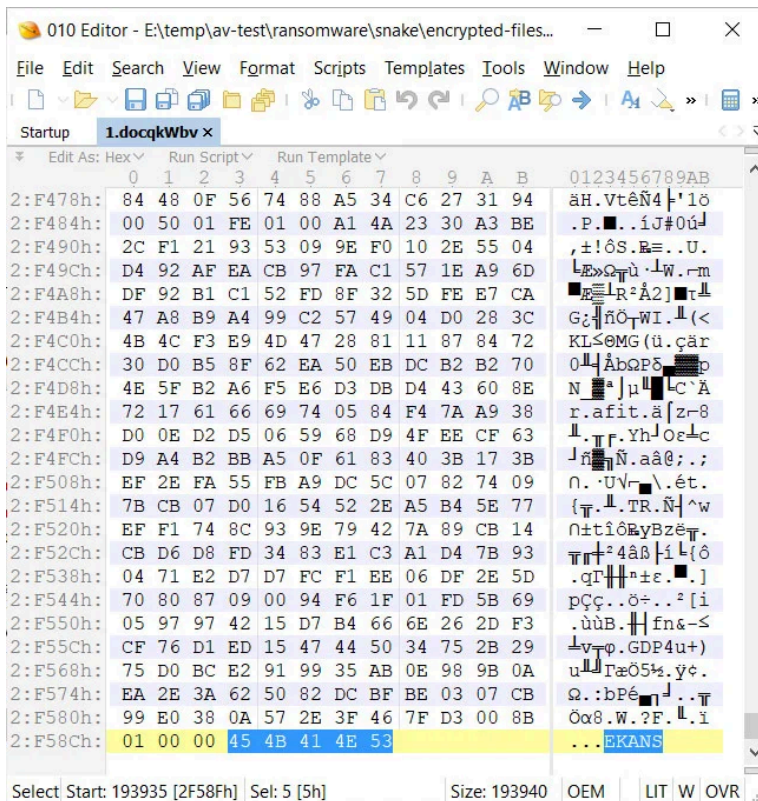
```
windir
SystemDrive
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery
\AppData\
```

When encrypting a file it will append a random 5 character string to the files extension. For example, a file named **1.doc** will be encrypted and renamed like **1.docqkWbv**.



Folder of Encrypted Files

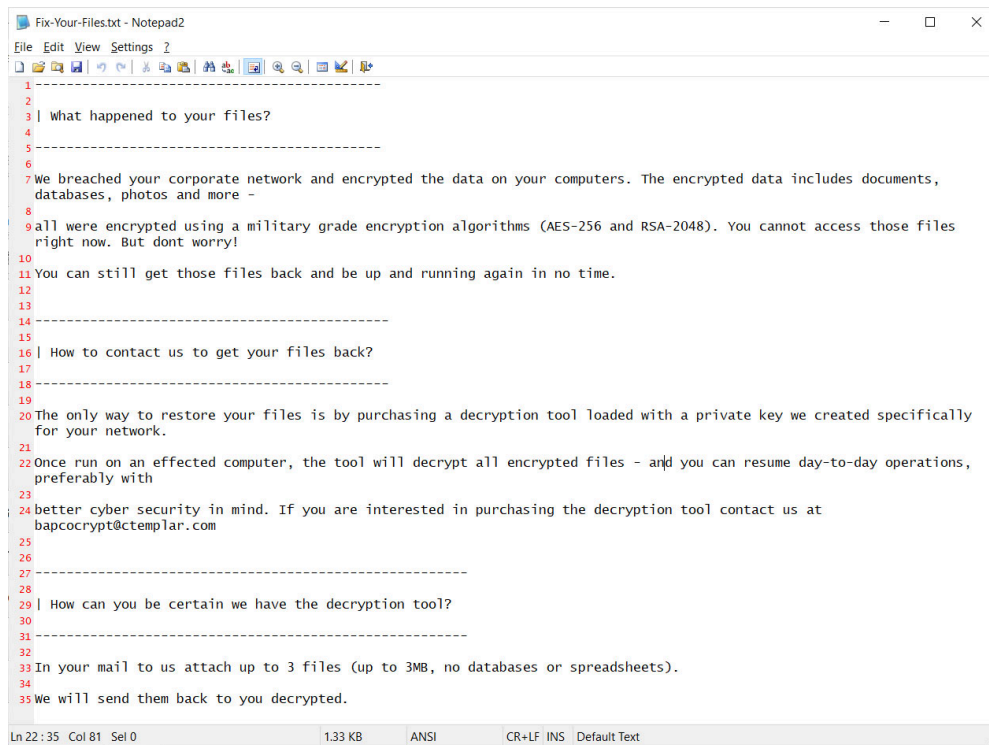
In each file that is encrypted, the SNAKE Ransomware will append the 'EKANS' file marker shown below. EKANS is SNAKE in reverse.



EKANS File Marker

BleepingComputer has tested many ransomware infections since 2013 and for some reason, it took Snake particularly long time to encrypt our small test box compared to many other ransomware infections. As this is targeted ransomware that is executed at the time of the attacker's choosing, this may not be that much of a problem as the encryption will most likely occur after hours.

When done encrypting the computer, the ransomware will create a ransom note in the C:\Users\Public\Desktop folder named **Fix-Your-Files.txt**. This ransom note contains instructions to contact a listed email address for payment instructions. This email address is currently bapcocypt@ctemplar.com.



```
Fix-Your-Files.txt - Notepad2
File Edit View Settings ?
| What happened to your files?
-----
7 We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents,
databases, photos and more -
8
9 all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files
right now. But dont worry!
10
11 You can still get those files back and be up and running again in no time.
12
13
14 -----
15
16 | How to contact us to get your files back?
17
18 -----
19
20 The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically
for your network.
21
22 Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations,
preferably with
23
24 better cyber security in mind. If you are interested in purchasing the decryption tool contact us at
bapccrypt@ctemplar.com
25
26 -----
27
28 | How can you be certain we have the decryption tool?
29
30 -----
31
32 In your mail to us attach up to 3 files (up to 3MB, no databases or spreadsheets).
33
34 We will send them back to you decrypted.
35
Ln 22, Col 1, Sel 0 1.33 KB ANSI CR+LF INS Default Text
```

SNAKE Ransom Note

As you can see from the language in the ransom note, this ransomware specifically targets the entire network rather than individual workstations. They further indicate that any decryptor that is purchased will be for the network and not individual machines, but it is too soon to tell if they would make an exception.

This ransomware is still being analyzed for weaknesses and it is not known if it can be decrypted for free. At this time, though, it looks secure.

IOCs:

Hash:

```
e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60
```

Ransom note text:

```
-----

| What happened to your files?

-----

We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databa

all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files rig

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 you. Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, please have better cyber security in mind. If you are interested in purchasing the decryption tool contact us at bapccrypt@ctemplar.com.

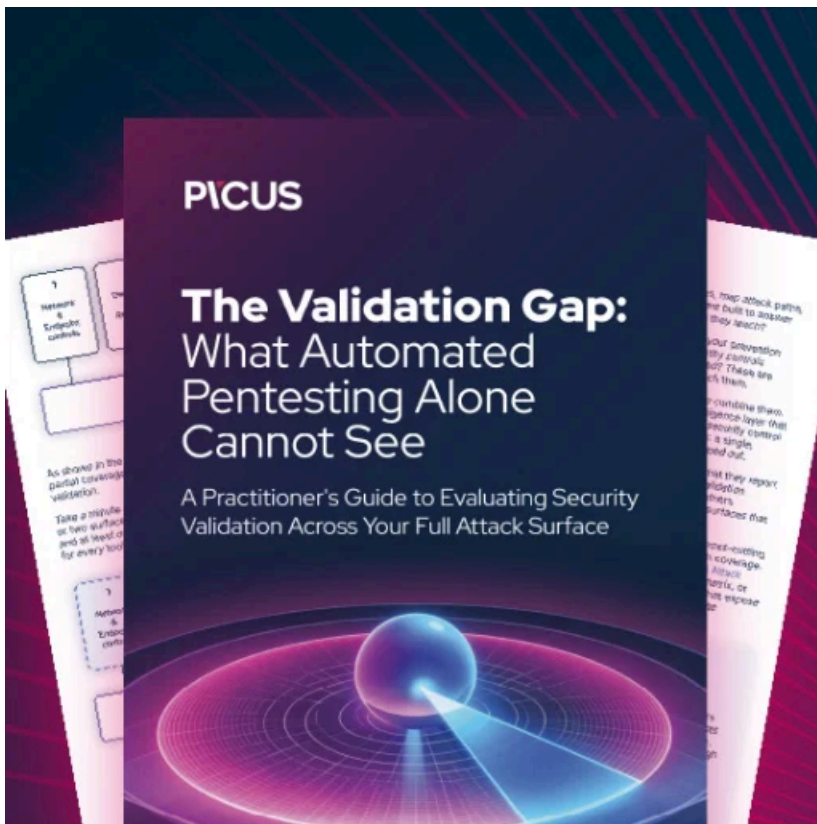
| How can you be certain we have the decryption tool?

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.

Associated file names:

Fix-Your-Files.txt



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/>