SNAKE Ransomware Is the Next Threat Targeting Business Networks

bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/

Lawrence Abrams

By
Lawrence Abrams

- January 8, 2020
- 03:30 AM
- 2

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.

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.

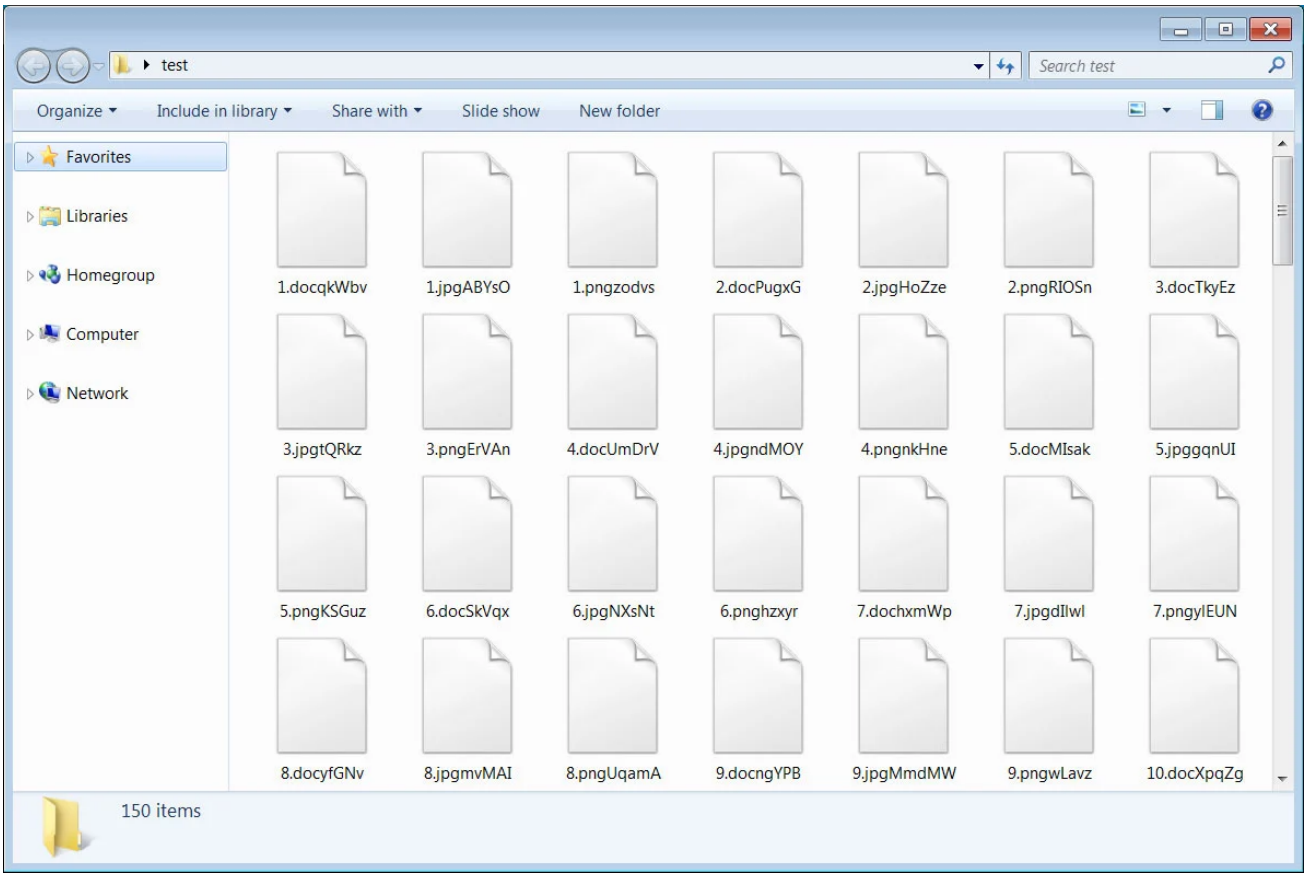
"The ransomware contains a level of routine obfuscation not previously and typically seen coupled with the targeted approach," Kremez, Head of SentinelLabs, told BleepingComputer in a conversation.

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:

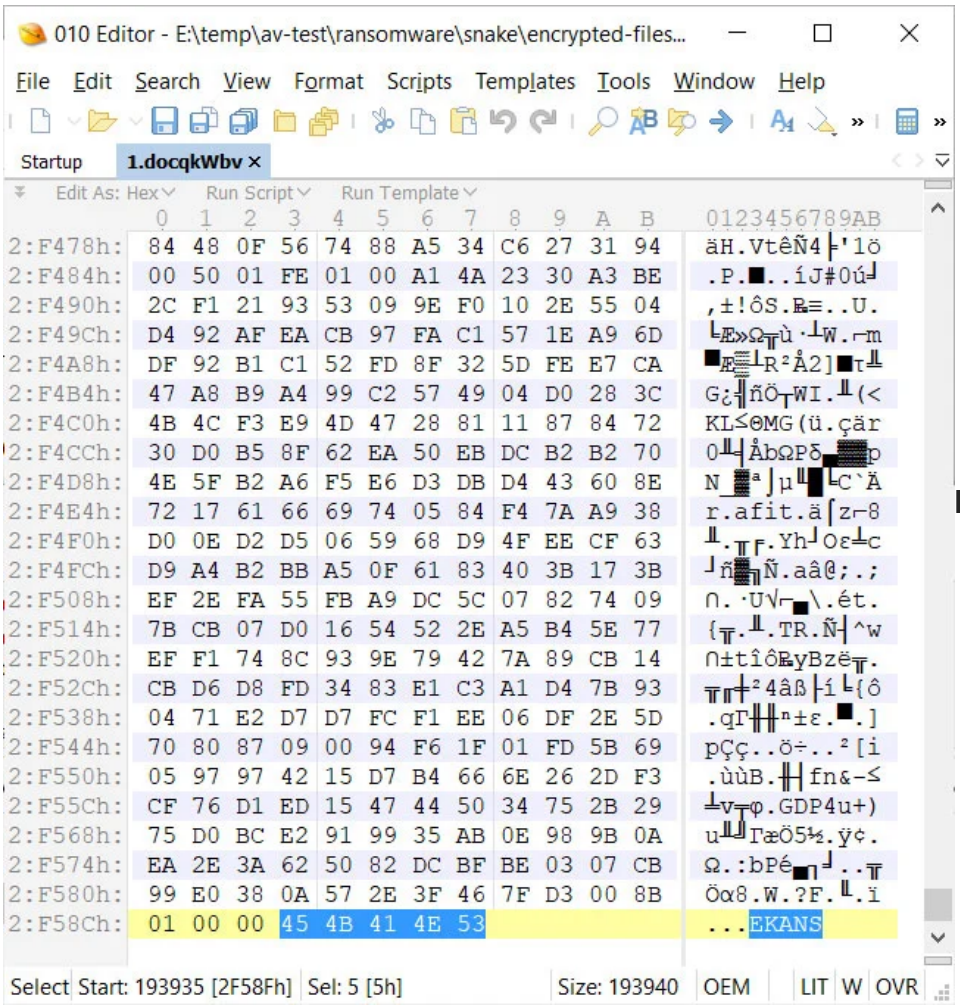
```
windir
SystemDrive
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery
\AppData\
```

When encrypting a file it will append a ransom 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

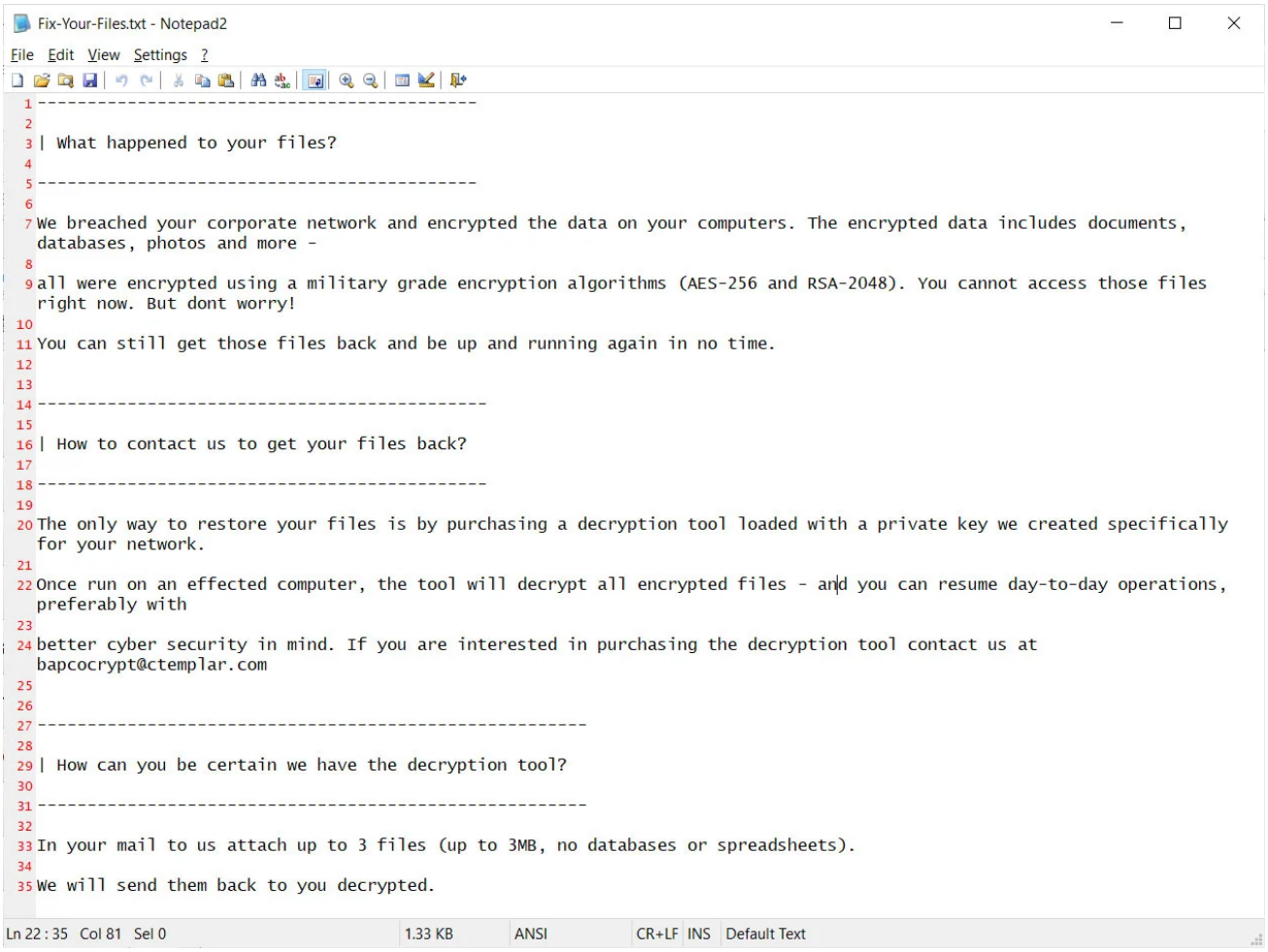
In each file that is encrypted, the SNAKE Ransomware will append the '**EKANS**' file marker shown below. EKANS is SNAKE in reverse.



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 bapcocrypt@ctemplar.com.



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, 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 bapcocrypt@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
```

- Enterprise
- Network
- Ransomware
- Snake

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 
  adammitz123 - 2 years ago
  -
  -
  Do this ransomware also blackmail the organization into paying with a threat of leaking their files?

- 
  Lawrence Abrams - 2 years ago
  -
  -
  Unknown at this time.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: