Snatch Ransomware Reboots to Windows Safe Mode to Bypass AV Tools

bleepingcomputer.com/news/security/snatch-ransomware-reboots-to-windows-safe-mode-to-bypass-av-tools/

Sergiu Gatlan

By
Sergiu Gatlan

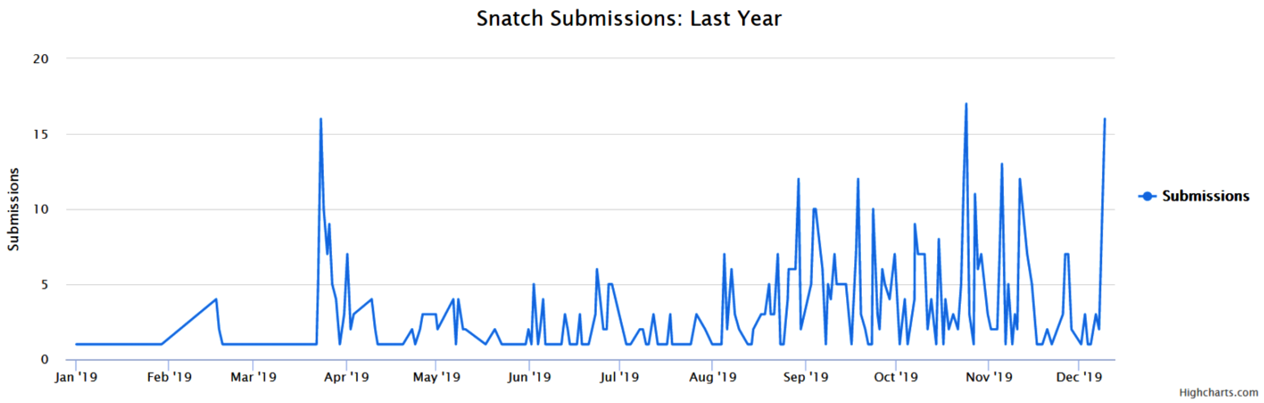
- December 9, 2019
- 06:08 PM
- 0

Researchers discovered a new Snatch ransomware strain that will reboot computers it infects into Safe Mode to disable any resident security solutions and immediately starts encrypting files once the system loads.

Encrypting the victim's files is possible because most security tools are automatically disabled when Windows devices boot in Safe Mode as the Sophos Managed Threat Response (MTR) team and SophosLabs researchers found.

"Snatch can run on most common versions of Windows, from 7 through 10, in 32- and 64-bit versions," they add. "The samples we’ve seen are also packed with the open-source packer UPX to obfuscate their contents."

Snatch ransomware came out towards the end of 2018 and it became noticeably active during April 2019 as shown by a spike in ransom notes and encrypted file samples submitted to Michael Gillespie's ID Ransomware platform.



Snatch ransomware 2019 activity (*ID Ransomware*)

Persistence, stealing data, and payload delivery

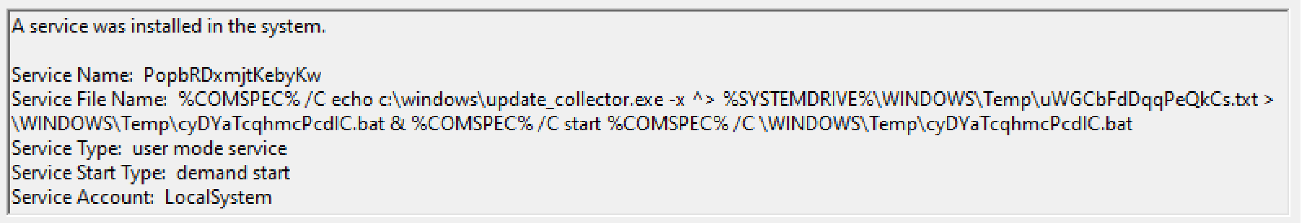
A suspected member of the Snatch ransomware team was observed by Sophos' researchers while "looking for affiliate partners with access to RDP\VNC\TeamViewer\WebShell\SQL inj [SQL injection] in corporate networks, stores, and other companies."

This hints at the group or its affiliates abusing this type of security holes into organizations' computing systems, as shown by logs the researchers discovered on one the victims' encrypted servers pointing at the threat actors brute-forcing a server's Microsoft Azure admin account and logging in via Remote Desktop (RDP).

"Subsequent hunts for related files revealed several other attacks in which precisely the same collection of tools was used in what appear to be opportunistic attacks against organizations located around the world, including the United States, Canada, and several European countries," Sophos says.

"All the organizations where these same files were found also were later discovered to have one or more computers with RDP exposed to the internet."

After the initial intrusion, the attackers logged into the domain controller (DC) machine using the same admin account and maintained access, collecting and exfiltrating information, as well as monitoring the victim's network for a few weeks.



```
A service was installed in the system.

Service Name:  PopbRDxmjtKebyKw
Service File Name:  %COMSPEC% /C echo c:\windows\update_collector.exe -x ^> %SYSTEMDRIVE%\WINDOWS\Temp\uWGCbFdDqqPeQkCs.txt >
\WINDOWS\Temp\cyDYaTcqhmcPcdlC.bat & %COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\cyDYaTcqhmcPcdlC.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

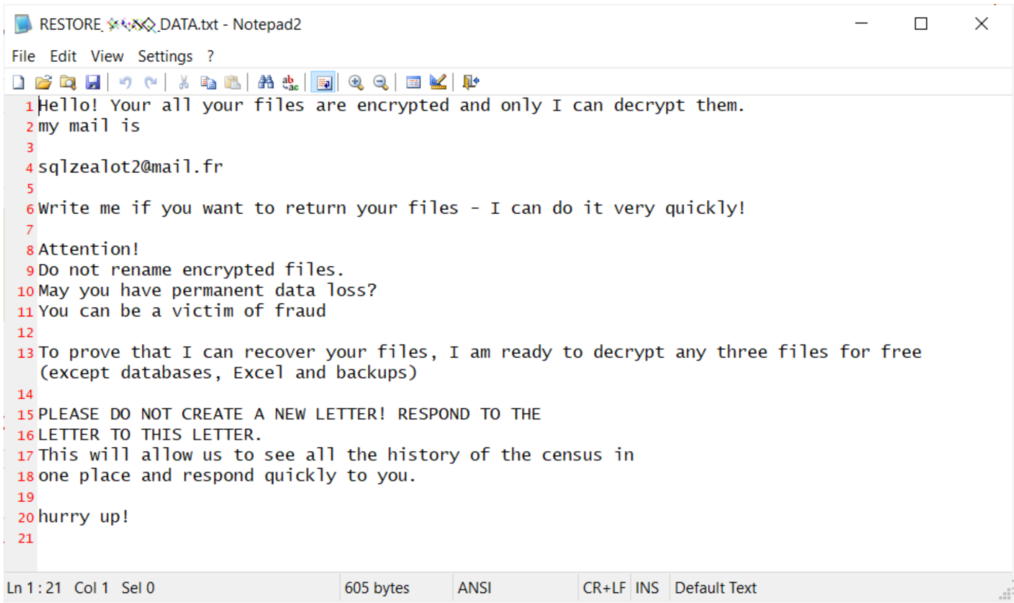
Installing a service to exfiltrate stolen data *(Image: Sophos)*

They also installed surveillance software on around 5% of all machines on the network (roughly 200 computers), which also allowed for remote access making it possible to maintain persistence on the compromised network even if the compromised Azure server would've been taken down.

"The threat actors have also innovated their crime in another important way: one piece of malware used in the Snatch attacks is capable of, and has been, stealing vast amounts of information from the target organizations," Sophos adds.

The group behind it has also been observed while dropping a series of other tools including Process Hacker, IObit Uninstaller, PowerTool, and PsExec that would also help them disable security tools on devices they compromise.

Dropping the Snatch ransomware component payload on the compromised network happens following a seemingly random timeline, in some cases taking just a few days while in others it can take weeks.


RESTORE_[redacted]_DATA.txt - Notepad2
File Edit View Settings ?

```
Hello! Your all your files are encrypted and only I can decrypt them.
my mail is

sqlzealot2@mail.fr

Write me if you want to return your files - I can do it very quickly!

Attention!
Do not rename encrypted files.
May you have permanent data loss?
You can be a victim of fraud

To prove that I can recover your files, I am ready to decrypt any three files for free (except databases, Excel and backups)

PLEASE DO NOT CREATE A NEW LETTER! RESPOND TO THE
LETTER TO THIS LETTER.
This will allow us to see all the history of the census in
one place and respond quickly to you.

hurry up!

```

Snatch ransomware ransom note sample

Disabling anti-malware solutions and encrypting devices

To take advantage of anti-malware solutions not loading in Safe Mode, the Snatch ransomware component installs itself as a Windows service dubbed SuperBackupMan capable of running in Safe Mode that can't be stopped or paused, and then force restarts the compromised machine.

After the device enters Windows Safe Mode, Snatch ransomware will delete "all the Volume Shadow Copies on the system" as the researchers discovered, preventing "forensic recovery of the files encrypted by the ransomware."

In the next stage, the malware will start encrypting its victims' files, with the attackers now being sure that recovery without payment is impossible.

The researchers made a video demo showing one of the Snatch ransomware samples rebooting an infected system and encrypting files once the Windows Safe Mode is loaded.

Coveware, a company specialized in intermediating ransomware negotiations, told Sophos that they negotiated with the Snatch team "on 12 occasions between July and October on behalf of their clients" with the ransom demands ranging between $2,000 to $35,000 worth of bitcoins, going up over those four months.

To avoid getting breached and infected with Snatch ransomware, companies are advised by Sophos not to expose RDP services to the Internet or protect them by using a VPN.

Since the group behind this ransomware is also actively looking for affiliates with access to exposed VNC and TeamViewer endpoints, as well as with experience in SQL server hacking and deploying/using web shells, exposing this type of services could also expose potential victims to attacks.

Last but least, Sophos recommends organizations to use multifactor authentication (MFA) for protecting administrator accounts to prevent brute force attacks.

An extensive list of indicators of compromise (IOCs) including malware sample hashes, exfiltration server addresses, commands used in the attacks, and more, are available here.

Related Articles:

NVIDIA fixes ten vulnerabilities in Windows GPU display drivers

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Eternity malware kit offers stealer, miner, worm, ransomware tools

New Raspberry Robin worm uses Windows Installer to drop malware

- Malware
- Ransomware
- Security
- Snatch
- Windows

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

You may also like: