

New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware - SentinelLabs

By Jim Walter

Published: 2020-01-23 · Archived: 2026-04-05 13:34:23 UTC

We are just about 1 month into 2020, and so far, there has been no break in the ongoing flurry of new or varied ransomware campaigns. Amongst the well-established families (Ryuk, Maze, REvil) we now have another to add to the list... "Snake".

SentinelLabs has [observed](#) the Snake ransomware in targeted campaigns over the last month. While it contains all the hallmarks of standard ransomware, there are a few traits that make it stand out as more aggressive and more complex.

Snake is written in Golang, which has been seen in many recent ransomware families. Golang is an open-source programming language, with a degree of cross-platform support. It is for these same reasons that some RaaS (Ransomware as a Service) offerings utilize the language as well. One such example would be [Project Root](#).

Upon infection, relevant files are overwritten with encrypted data. Each modified file is also 'tagged' at the end of the file with the string "EKANS" (Snake backwards).

```
03a0820 03 01 08 46 69 6c 65 4e 61 6d 65 01 0c 00 01 02 GY&M1
03a0830 49 56 01 0a 00 01 11 45 4e 43 52 59 50 54 45 44 vi [K
03a0840 5f 41 45 53 5f 4b 65 79 01 0a 00 00 00 fe 01 3f ='xN
03a0850 ff 82 01 24 43 3a 5c 55 73 65 72 73 5c 61 64 6d Xby<
03a0860 69 6e 31 5c 44 6f 77 6e 6c 6f 61 64 73 5c 73 6e X<"Qo+
03a0870 61 6b 65 31 2e 65 78 65 01 10 c4 6f 89 80 bf 1b tv(J
03a0880 d5 3b 3d 1f b1 0f 02 99 ad 64 01 fe 01 00 40 7b un_0
03a0890 a1 a6 92 09 43 21 b7 e5 18 d9 9b 3d f1 33 89 6e R!>}i
03a08a0 05 31 43 6d f1 96 02 87 fb 7d e9 dc 1d b6 ab 87 5(k,<
03a08b0 cc b0 c4 86 78 bc a2 bd 71 b5 d8 38 db 89 e6 a5 s/E>^M
03a08c0 2f 2d 9b 5b 25 3e 27 59 02 ef 06 6e 44 34 1a 9e yB'M
03a08d0 87 35 4b 28 9f d4 d6 4c 11 1d 33 4f b5 90 54 84 yKj`
03a08e0 e3 a8 a0 90 8e 5a 67 d4 43 cc 3b 21 07 1c 38 c6 >yH7|
03a08f0 16 d5 e3 63 8e e1 b1 d6 90 62 c2 95 95 d3 d5 1b 1SD1
03a0900 3b 56 0a 0f 39 cb f7 ce e4 fd 85 ba 18 f8 2c dd -e-i
03a0910 27 32 9e cb 95 b8 77 cc 63 3e 2f bd fc 54 9e c4 'uZ!L
03a0920 93 fd 6a 8d 13 99 56 98 a9 6d c3 50 91 34 7d c5 /9'X
03a0930 f4 03 56 4e 09 96 61 23 66 57 65 6c 14 78 85 9c nodceikemblegmpmkc1o
03a0940 45 30 bb d9 6b 14 51 f2 6b 21 06 d8 be 97 f9 7b FileName
03a0950 8d 30 41 7c fc b9 7a 47 4c 40 91 8a 71 76 41 e8 ENCRYPTED_AES_Key
03a0960 6b 76 7a cc 56 c4 00 35 84 15 75 04 f8 e3 56 2a $C:\Users\...Downloads\snake1.exe
03a0970 e4 90 cb a2 77 0e 46 3e 74 96 0f 94 5a f5 d3 2e [%>'Y
03a0980 da 01 a0 b4 93 6a ed 36 8a 16 bb 96 11 40 00 8f a#fWel
03a0990 01 00 00 45 4b 41 4e 53 zGL@
03a0998 EKANS
```

In addition, the names of modified files are appended with random characters, rather than a singular or uniform extension change. This, in theory, makes it more difficult to identify the specific ransomware family simply by the file extensions.

Name	Date modified	Type
7z1900-x64.exevQycM	1/21/2020 1:53 PM	EXEVQYCM File
ClassicShellSetup_4_3_1.exeZkiPv	1/21/2020 1:53 PM	EXEZKIPV File
GoogleChromeEnterpriseBundle64.zipaZlyo	1/21/2020 1:53 PM	ZIPAZIYO File
python-3.7.4.exeHbcMu	1/21/2020 1:53 PM	EXEHBCMU File
sn1.exeenOBt		EXEENOBT File
snake1.exeVbJVL	1/21/2020 1:53 PM	EXEVBJVL File

The actual encryption process is achieved via a mix of symmetric and asymmetric cryptography (across AES-256 and RSA-2048). A symmetric key is required for encrypting and decrypting of files. Said symmetric key is encrypted with the attacker’s public key. Decryption is only possible with possession of the attacker’s private key. This mixture, along with the key lengths (AES-256, RSA-2048), aims to make 3rd party decryption difficult or impossible.

The malware excludes critical system files and folders from encryption. In parallel, it attempts to encrypt data on adjacent and available network resources. Current analysis indicates that any decryption purchased from the attacker covers the scope of the targeted network rather than individual files.

As with most modern ransomware, Snake attempts to remove Volume Shadow Copies that the OS uses for backup. The ransomware also attempts to terminate various processes. It appears to be targeting those associated with SCADA platforms, enterprise management tools, system utilities and the like. Some specifically targeted applications include VMware Tools, Microsoft System Center Operations Manager, Nimbus, Honeywell HMIWeb, FLEXnet, and more. A full list of the terminated processes is as follows:

<code>bluestripecollector.exe</code> <code>ccflc0.exe</code> <code>ccflc4.exe</code> <code>cdm.exe</code> <code>certificateprovider.exe</code> <code>client.exe</code> <code>client64.exe</code> <code>collwrap.exe</code> <code>config_api_service.exe</code> <code>dsmcsvc.exe</code> <code>epmd.exe</code> <code>erlsrv.exe</code> <code>fnplicensing-service.exe</code> <code>hasplmv.exe</code> <code>hdb.exe</code> <code>healthservice.exe</code> <code>ilicensesvc.exe</code> <code>inet_gethost.exe</code> <code>keysvc.exe</code> <code>managementagenthost.exe</code> <code>monitoringhost.exe</code> <code>msdtssrvr.exe</code>	<code>msmdsrv.exe</code> <code>musnotificationux.exe</code> <code>n.exe</code> <code>nimbus.exe</code> <code>npmdagent.exe</code> <code>ntrl.exe</code> <code>ntservices.exe</code> <code>pralarmmgr.exe</code> <code>prcalculationmgr.exe</code> <code>prconfigmgr.exe</code> <code>prdatasemgr.exe</code> <code>premailengine.exe</code> <code>preventmgr.exe</code> <code>prftengine.exe</code> <code>prgateway.exe</code> <code>prlicensemgr.exe</code> <code>proficy administrator.exe</code> <code>proficyclient.exe</code> <code>proficypublisherservice.exe</code> <code>proficyserver.exe</code> <code>proficysts.exe</code> <code>prprintserver.exe</code>	<code>prproficymgr.exe</code> <code>prrds.exe</code> <code>prreader.exe</code> <code>prrouter.exe</code> <code>prschedulemgr.exe</code> <code>prstubber.exe</code> <code>prsummarymgr.exe</code> <code>prwriter.exe</code> <code>reportingservices-service.exe</code> <code>server_eventlog.exe</code> <code>server_runtime.exe</code> <code>spooler.exe</code> <code>sqlservr.exe</code> <code>taskhostw.exe</code> <code>vgauthservice.exe</code> <code>vmacthlp.exe</code> <code>vmtoolsd.exe</code> <code>win32sysinfo.exe</code> <code>winvnc4.exe</code> <code>workflowresttest.exe</code>
--	---	---

If the threat is executed with administrative privileges, the ransom note will be written to `c:\users\publicdesktop\Fix-Your-Files.txt` . In the event that administrative privileges are not present, the ransom note will be written to an alternative location: `c:\users\AppData\Local\VirtualStore`

| 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 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.

The ransom note provides fairly straightforward details on how the victim should proceed (according to the attacker). Rather than providing a web address to obtain a payment address and further details, victims are instructed to initiate direct contact via email. Note the email address in the ransom note is “bapccrypt@ctemplar.com”  BAPCO (The Bahrain Petroleum Company) was the target of the recent ‘Dustman’ campaign. There may very well be a relationship between the Snake and ‘Dustman’ attacks.

Conclusion

Snake, like other targeted ransomware campaigns, has the potential to do serious and critical damage to an infected environment. As always we should stay aware and vigilant, and aggressively defend environments against this type of attack. Part of this strategy comes down to properly choosing, deploying, and maintaining a modern endpoint protection technology. It is also critical to have functional and well-tested backup procedures in place as part of your greater business continuity and disaster recovery planning.

References

Thanks to [@VK_Intel](#) and [sysopfb](#) for their insights about this ransomware.

Indicators of Compromise (IOCs):

SHA-256: e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60

MITRE ATT&CK: [T1486](#) Data Encrypted for Impact

Source: <https://labs.sentinelone.com/new-snake-ransomware-adds-itself-to-the-increasing-collection-of-golang-crimeware/>