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

labs.sentinelone.com/new-snake-ransomware-adds-itself-to-the-increasing-collection-of-golang-crimeware/

Jim Walter

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).

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.zipaZIyo	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:

bluestripecollector.exe	msmdsrv.exe	prproficymgr.exe
ccflic0.exe	musnotificationux.exe	prrds.exe
ccflic4.exe	n.exe	prreader.exe
cdm.exe	nimbus.exe	prrouter.exe
certificateprovider.exe	npmdagent.exe	prschedulemgr.exe
client.exe	ntevl.exe	prstubber.exe
client64.exe	ntservices.exe	prsummarymgr.exe
collwrap.exe	pralarmmgr.exe	prwriter.exe
config_api_service.exe	prcalculationmgr.exe	reportingservicesservice.exe
dsmcsvc.exe	prconfigmgr.exe	server_eventlog.exe
epmd.exe	prdatabasemgr.exe	server_runtime.exe
erlsrv.exe	premailengine.exe	spooler.exe
fnplicensingservice.exe	preventmgr.exe	sqlservr.exe
hasplmv.exe	prftpengine.exe	taskhostw.exe
hdb.exe	prgateway.exe	vgauthservice.exe
healthservice.exe	prlicensemgr.exe	vmacthlp.exe
ilicensesvc.exe	proficy administrator.exe	vmtoolsd.exe
inet_gethost.exe	proficyclient.exe	win32sysinfo.exe
keysvc.exe	proficypublisherservice.exe	winvnc4.exe
managementagenthost.exe	proficyserver.exe	workflowresttest.exe
monitoringhost.exe	proficysts.exe	
msdtssrvr.exe	prprintserver.exe	

If the threat is executed with administrative privileges, the ransom note will be written to `c:userspublicdesktopFix-Your-Files.txt`. In the event that administrative privileges are not present, the ransom note will be written to an alternative location: `c:usersAppDataLocalVirtualStore`

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 “bapcocrypt @ 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
```