ManageEngine
Log360

RANSOMWARE DEMYSTIFIED

What security analysts need to know

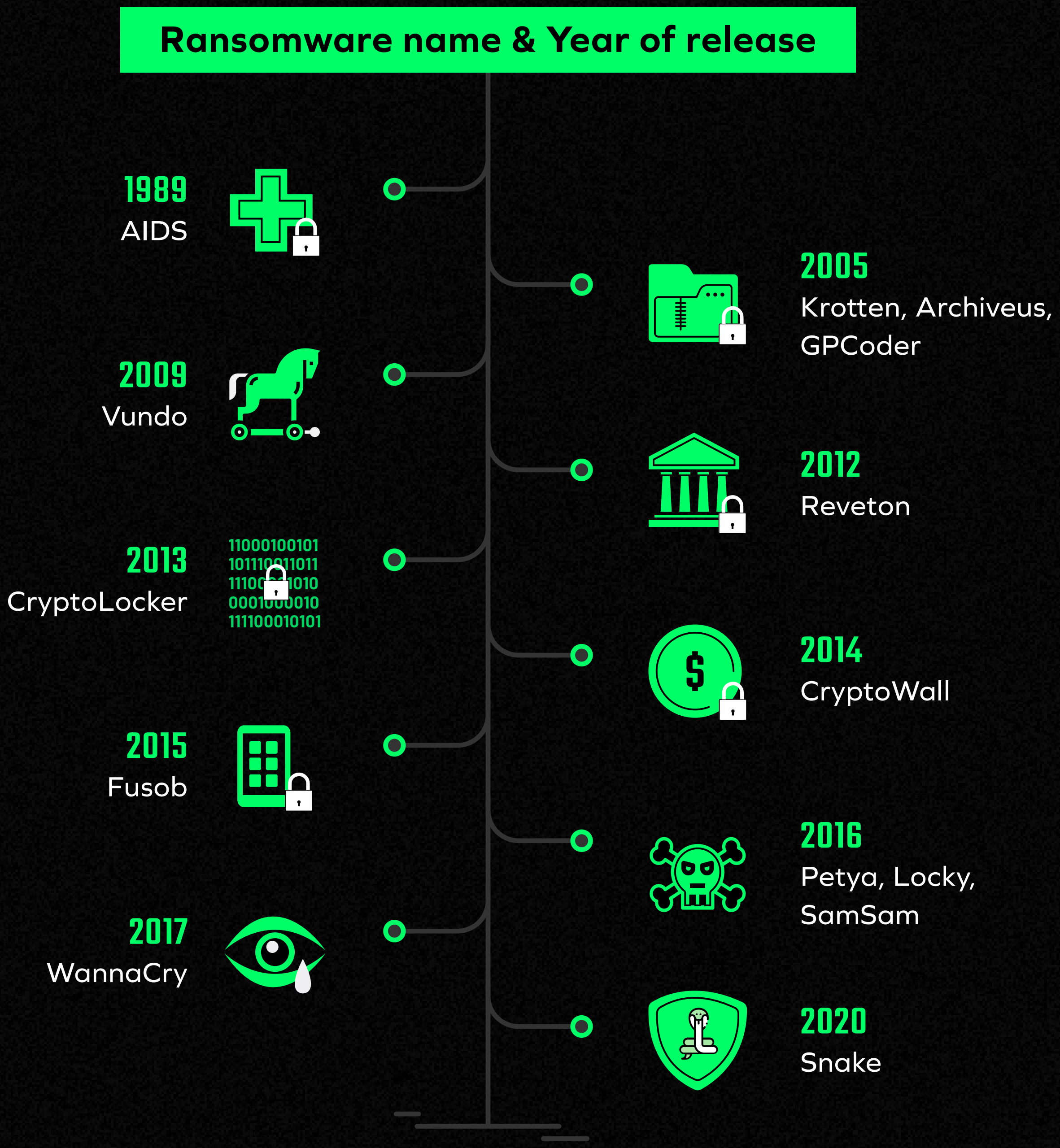
Includes details on the newest ransomware strain, Snake

Table of Contents

Ransomware: An introduction and history lesson

The year was 1989, and the world's first ransomware—AIDS—was introduced by Joseph Popp, an evolutionary biologist. Popp mailed 20,000 infected floppy disks to attendees of the World Health Organization's AIDS conference. The malware would stay benign on the victim's system until the computer was rebooted 90 times. It would then hide all directories and encrypt files on the victim's C:\ drive. Victims were asked to send $189 to a post office box in Panama to get their files back. Since basic symmetric key cryptography was used to encrypt the files, this ransomware was soon defeated.

Ransomware then laid low until 2005, when attackers started using sophisticated encryption methodologies to release new strains. In the ensuing years, we have seen ransomware become a huge threat for organizations around the world. Figure 1 shows a timeline of some of the most popular ransomware.



Ransomware name & Year of release

1989
AIDS

2005
Krotten, Archiveus, GPCoder

2009
Vundo

2012
Reveton

2013
CryptoLocker

2014
CryptoWall

2015
Fusob

2016
Petya, Locky, SamSam

2017
WannaCry

2020
Snake

Figure 1: A timeline of ransomware: 1989 to 2020 (To be changed into an infographic/diagram)

A ransomware attack can be extremely expensive for victims and can cost them over $700,000 to recover.[1] Research suggests that in 2020, a new organization will be hit by ransomware every 14 seconds.[2] In the future, ransomware as a service is expected to rise quickly as well, making ransomware an even bigger threat. Given these realities, security analysts should continuously educate themselves on the latest ransomware strains, how they work, and how they can be prevented. Security analysts should also be aware of defense techniques so that they can take the right action in case ransomware strikes.

Anatomy of a ransomware attack

There are five stages of any ransomware attack. It starts with initial exploitation and ends with a ransom demand, blackmail or extortion. Figure 2 shows the different stages of an attack.

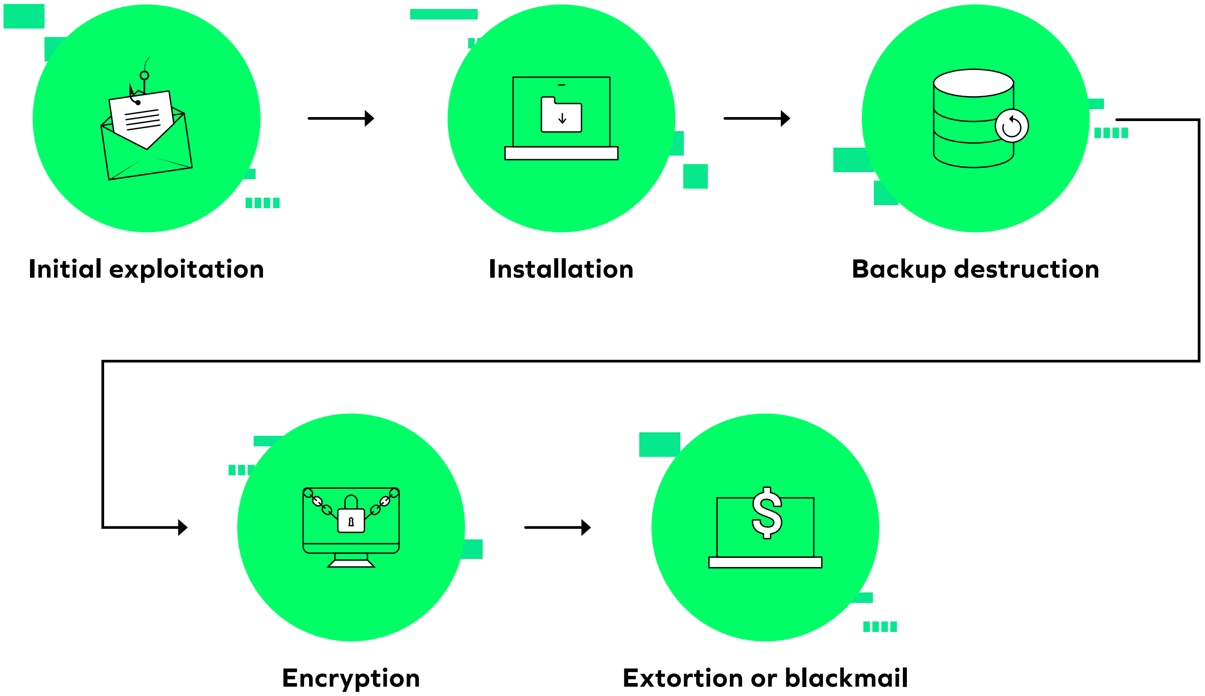


Figure 2: The five stages of a ransomware attack (Diagram to be enhanced)

Initial exploitation:

Initial exploitation is required for ransomware to gain a foothold in a network. This is achieved by any of these methods: a phishing or spam email, redirection to a malicious website, compromise of a Remote Desktop Connection (RDP), etc.

Installation:

Through the initial exploitation, ransomware is installed on the victim's machine. Every time the machine boots up, the ransomware code is executed. At this stage, a lot of sophisticated ransomware variants actually check if the machine is worth infecting. If it is, the attack goes forward. If it determines that it is not a machine worth infecting (e.g., the machine is a sandbox or a virtual machine), the ransomware will quietly exit.

Backup destruction:

To raise the effectiveness of the attack and increase the chance that a victim will pay the ransom, ransomware will usually search for and destroy backup files.

Encryption:

The ransomware now starts to encrypt the victim's files. To accomplish this, the installed ransomware establishes a connection with a command-and-control (C&C) server, which gives instructions for the encryption. Here, it may also take instructions about what file formats to target for encryption.

Extortion or blackmail:

A ransom message appears on the victim's screen informing them that they have been compromised and their important files have been encrypted. Victims are given a specific time by which they should pay a ransom amount (usually in Bitcoin) to get their files back.

How does encryption take place?

There are four major methods by which encryption of files can take place, and different types of ransomware use different methods to encrypt files. These are:

- Symmetric encryption.
- Asymmetric encryption from the client side.
- Asymmetric encryption from the server side.
- A combination of asymmetric encryption—from both the client and server side—and symmetric encryption.

Symmetric encryption

In this method, all the files on the infected device will be encrypted using symmetric encryption algorithms, such as the Advanced Encryption Standard (AES) or the Data Encryption Standard (DES). The keys that are used to encrypt the files will be stored on the victim's disk. When the victim pays the ransom, the same key will be used to decrypt the files.

The advantage of using this method is the speed at which encryption takes place, and the simplicity of deployment. However, the disadvantage is that the key is easy to find for ransomware researchers, and the threat can be defeated quickly.

Asymmetric encryption from the client side

Two keys are generated using the RSA algorithm on the infected device: a public key and a private key. This is known as a key pair. The public key is used to encrypt the files, and the private key is sent to the C&C server where it is stored. When the victim pays the ransom, the corresponding private key is retrieved from the server, and the files are decrypted.

The advantage of asymmetric encryption from the client side is that the ransomware uses distinct key pairs for encryption and decryption, and hence it is hard to defeat. However, this method takes a long time to execute. Moreover, an internet connection is required to send the private key to the C&C server.

Asymmetric encryption from the server side

In this method, a key pair is generated using the RSA algorithm on the C&C server. The public key is then hardcoded into the ransomware. When the ransomware gets executed on the victim's device, it will encrypt all the files using the public key. When the demanded ransom is paid by the victim, the private key is retrieved from the server, and the files are decrypted.

The advantage of this method is that it is quick to execute on the infected device, and an internet connection is required only during the decryption of the files once the ransom is paid. However, the disadvantage is that there is only one private key that is used to decrypt all the files. Therefore, only one victim needs to pay the ransom to get the common decryption key.

Combination of asymmetric encryption—from both the client and server side—and symmetric encryption

In this hybrid method, a key pair is generated both at the infected device by the ransomware and at the C&C server. Let us denote the client public key as PubC and the client private key as PriC. Similarly, we'll denote the server public key as PubS and the server private key as PriS. When the ransomware reaches the client, it will already have PubS hardcoded within it.

Each infection will have its own unique PubC and PriC. The PriC will be encrypted by the PubS.

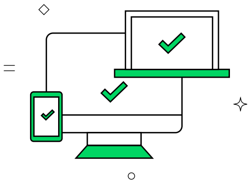
Then the file encryption routine starts, and files will get encrypted using symmetric key cryptography. When this is completed, all the symmetric keys will be encrypted with PubC.

After the victim pays the ransom, they would need the symmetric key to decrypt the files. Since the symmetric key has been encrypted with PubC, they would need PriC. However, since PriC has been encrypted by PubS, they would first need PriS. And PriS is only available at the C&C server.

Snake ransomware

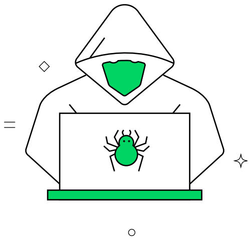
Ransomware can be classified into different families or strains according to its code signature, which contains the sequence of commands and instructions responsible for carrying out the attack.[3] One of the most recent ransomware families to hit organizations is Snake ransomware, which was first noticed in January 2020. In this chapter, we will go over how Snake operates and wreaks havoc.

Snake is written in Go, or Golang. This programming language, first designed at Google, has become very popular among the malware and ransomware development community. There are two main reasons for attackers' fast adoption of Go:



Uniform codebase for different operating systems:

With Go, an attacker can use a single codebase to perpetrate a ransomware attack on different devices across different operating systems.



Difficult for anti-virus to pick up:

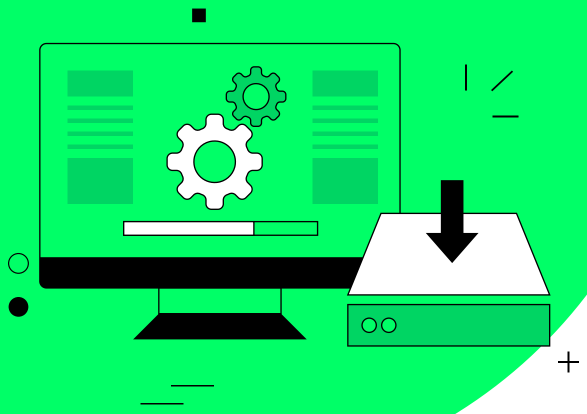
Ransomware written in Go is more stealthy than other ransomware. This is because malware written in this language is very large, so many anti-virus programs cannot pick it up.

The initial exploitation: How Snake slithers in

The initial point of entry for Snake ransomware can be any of the following:

- A malicious attachment in a phishing email
- A malicious link in a phishing email that leads the victim to an exploit kit
- Malvertising
- A watering hole attack

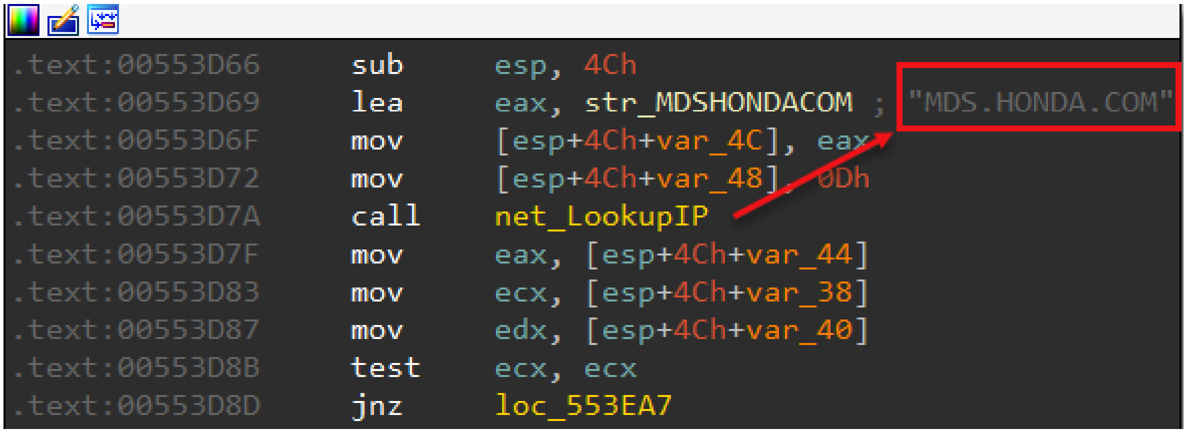
However, **insecure RDP** has been found to be the main reason attackers gain an initial foothold. As of the time of writing this e-book, most victims of Snake had machines with RDP access enabled, and this was known to attackers. It's well-known that RDP uses port 3389 to communicate. Attackers could then use tactics such as a brute-force attack to acquire the RDP login credentials.



Installation: How Snake bites

After gaining an initial foothold into a machine, Snake ransomware executes. It first registers a mutual exclusion object (mutex) marker called "EKANS" (just "snake" spelled backwards) to the machine. This mutex marker stops Snake from infecting an already infected machine multiple times.

Once Snake confirms that the machine is not already infected, it proceeds further. Unlike other ransomware strains, Snake is highly targeted—the victim's domain name and IP address are written into the ransomware code before the attack begins. Figure 3 shows how this is done within the malcode that executes.[4]



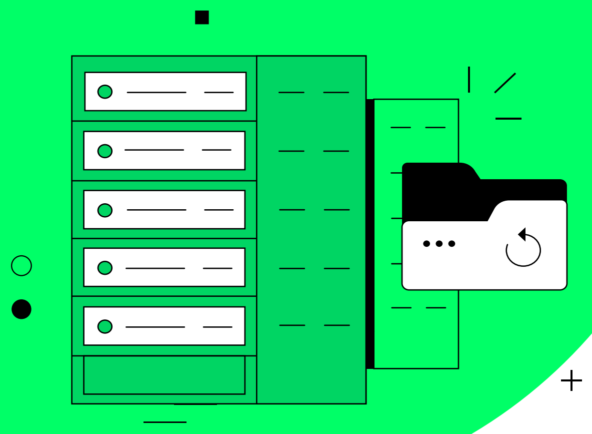
```
.text:00553D66      sub     esp, 4Ch
.text:00553D69      lea     eax, str_MDSHONDACOM ; "MDS.HONDA.COM"
.text:00553D6F      mov     [esp+4Ch+var_4C], eax
.text:00553D72      mov     [esp+4Ch+var_48], 0Dh
.text:00553D7A      call    net_LookupIP
.text:00553D7F      mov     eax, [esp+4Ch+var_44]
.text:00553D83      mov     ecx, [esp+4Ch+var_38]
.text:00553D87      mov     edx, [esp+4Ch+var_40]
.text:00553D8B      test    ecx, ecx
.text:00553D8D      jnz     loc_553EA7
```

Figure 3: Resolving the internal domain name to validate the target

This means that attackers have specific organizations that they want to target, and they would have already done a number of reconnaissance activities to get this information. The domain name and IP address combination that is embedded into the malcode is unique for each attack and applicable for the entire internal network of the organization under attack.

On the machine where the ransomware is executed, the domain name hardcoded into the malcode is resolved to its IP address. The malcode then checks if the resolved IP address is equal to the hardcoded IP address. If it is equal, the attack continues. If it is not equal, the attack terminates.

After verifying that the victim's machine is the right target, Snake makes changes to the Windows firewall settings so that all incoming and outgoing connections that are not configured already are blocked. Furthermore, all communication that does not match the firewall's existing rules are also blocked. This is done so that the system gets isolated from the outside world before the file encryption process starts.



Backup destruction: Venom goes deep

The ransomware then goes on to delete shadow copy backups so that recovery options are not available to the victim. Shadow copies are snapshots of files or volumes, even when they are in use. A versioning method is followed so that only changes in a file are backed up rather than the entire file. Shadow copies are extremely useful for recovering deleted files, but by deleting the shadow copies, Snake takes this option away from the victim.

After deleting the shadow copies, Snake kills numerous processes related to supervisory control and data acquisition, (SCADA) and industrial control systems (ICS), virtual machines, remote management tools, network management software, and more. This list of processes to be killed is actually hardcoded into the ransomware. These processes are especially critical for the smooth operation of manufacturing units and factories that rely on machine automation. By killing these processes, Snake halts production, increases downtime, and causes increased financial losses for the victim. The victim will therefore face immense pressure to pay the ransom.

Appendix A shows the list of processes that are killed, along with a short description of each one.[5] Many of the killed processes are associated with General Electric's Proficy Historian (e.g., prcalculationmgr.exe), which is used for industrial data collection. Some other processes killed are associated with databases (e.g., msmdsrv.exe) and data backup solutions (e.g., dsmcsvc.exe). It must be noted that attackers may easily modify the type of processes to be killed by changing the malcode.

Encryption: Changes occur in the victim

It's only after all of the above groundwork is complete that Snake begins its actual work. The process of encryption ignores system files, and files that are located in Windows system folders such as windir, :\Program Files, :\Local Settings, :\Boot, :\System Volume Information, :\$Recycle Bin, and :\Local Settings. This ensures that the victim is still able to log on to their system. The list of files and folders to be skipped is hard-coded into the ransomware. Appendix B shows a partial list of files and folders that are ignored.[6]

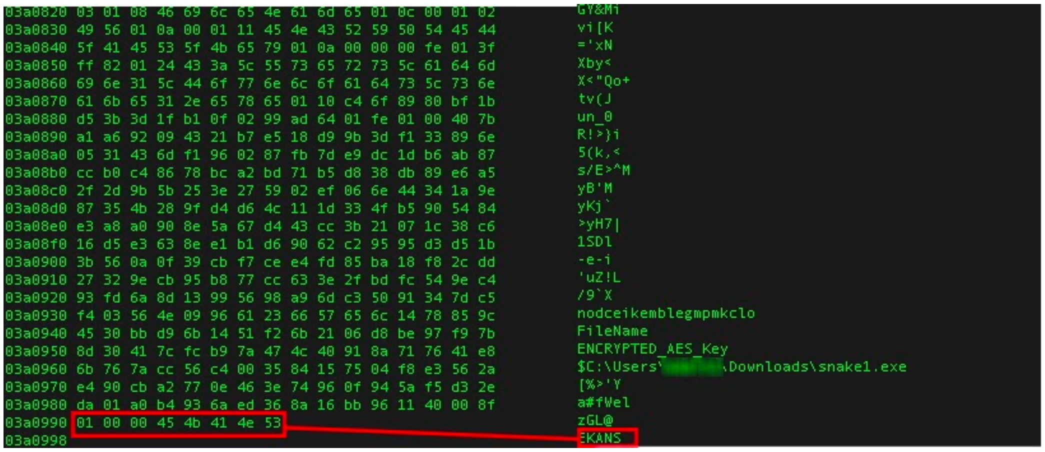
Encryption then begins, and all files with extensions that are part of a hardcoded list are targeted. This list includes Word documents (.doc and .docx), Excel files (.xls and .xlsx), and PowerPoint presentations (.ppt and .pptx). Table 1 below gives a more complete, but not exhaustive, list of file extensions that are targeted for encryption.[7] Even though these file extensions are available in the malcode, Snake doesn't just encrypt these files; it encrypts all files in a system that are not included in the folders it skips.

File extension	Description
.docx	Microsoft Word document
.doc	Microsoft Word document
.asp	Active Server Pages of Microsoft.Net
.aspx	ActiveX Server Pages of Microsoft.Net
.xls	Microsoft Excel file
.xlsx	Microsoft Excel file
.zip	Compress and archive
.rar	Compress and archive
.sql	Structured Query Language
.py	Python script file
.ppt	Microsoft PowerPoint file
.pptx	Microsoft PowerPoint file
.java	Java source code file
.csv	Comma Separated Values text file
.html	Hypertext Markup Language

Table 1: Some of the file extensions and types targeted by Snake for encryption

During the encryption process, Snake uses a combination of symmetric and asymmetric cryptography. This process was described earlier in this e-book under the "How does encryption take place?" section. While symmetric encryption is achieved through the AES-256 algorithm, asymmetric encryption is achieved through the RSA-2048 algorithm. A symmetric key will be used to first encrypt the files, after which it will in turn be encrypted with the attacker's public key. Decryption of the encrypted symmetric key can only be done with the attacker's private key, which will be sent to the victim upon payment of the ransom. Finally, the decryption of the victim’s files will be done with the symmetric key.

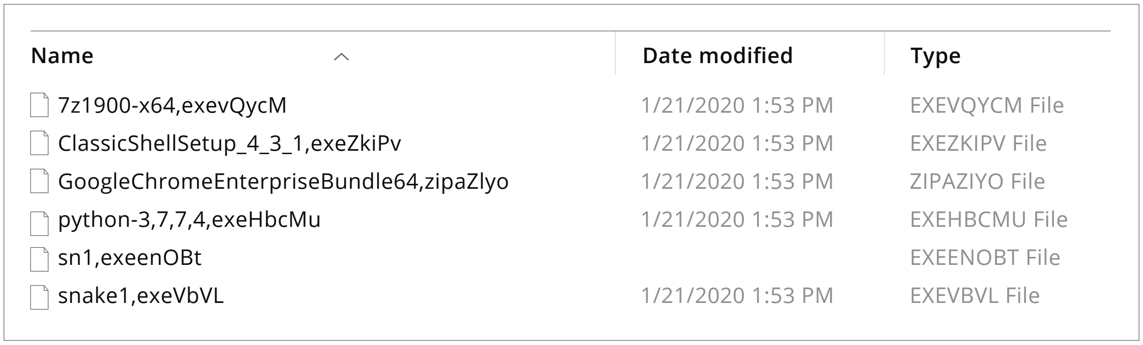
Upon infection, targeted files are overwritten with encrypted data. The encrypted data includes the original name of the file as well as the symmetric decryption key. Snake appends the "EKANS" file marker at the end of each file that is encrypted. This is shown in Figure 4.[8] The encryption itself is done via a single process called nmon.exe. This is a malicious trojan that can alter settings and disable or add features, files, or programs.



```
03a0820 03 01 08 46 69 6c 65 4e 61 6d 65 01 0c 00 01 02     GY&Mi
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     1SDl
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     nodceikemblegmpmkclo
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\[redacted]\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
```

Figure 4: The "EKANS" marker at the end of an encrypted file

After encrypting all the target files, Snake renames the files. It appends a random five-character string to the file extension. For example, a file named "design.doc" may be renamed "design.dochGDxc", and a file named "trees.py" may be renamed "trees.pyDQvlKh". Figure 5 shows how files could be renamed with random file extensions.7

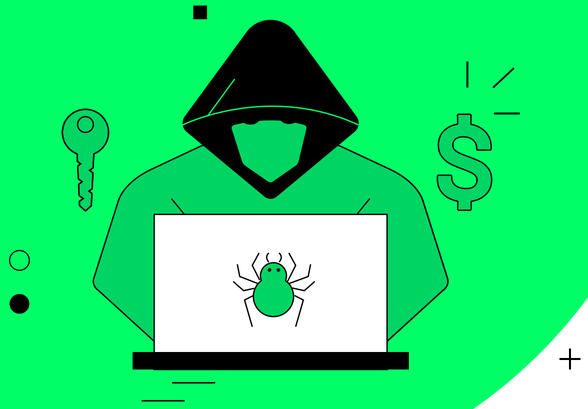


Name	Date modified	Type
7z1900-x64,exevQycM	1/21/2020 1:53 PM	EXEVQYCM File
ClassicShellSetup_4_3_1,exeZkiPv	1/21/2020 1:53 PM	EXEZKIPV File
GoogleChromeEnterpriseBundle64,zipaZlyo	1/21/2020 1:53 PM	ZIPAZIYO File
python-3,7,7,4,exeHbcMu	1/21/2020 1:53 PM	EXEHBCMU File
sn1,exeenOBt		EXEENOBT File
snake1,exeVbVL	1/21/2020 1:53 PM	EXEVBVL File

Figure 5: Filenames are modified with random five-character extensions

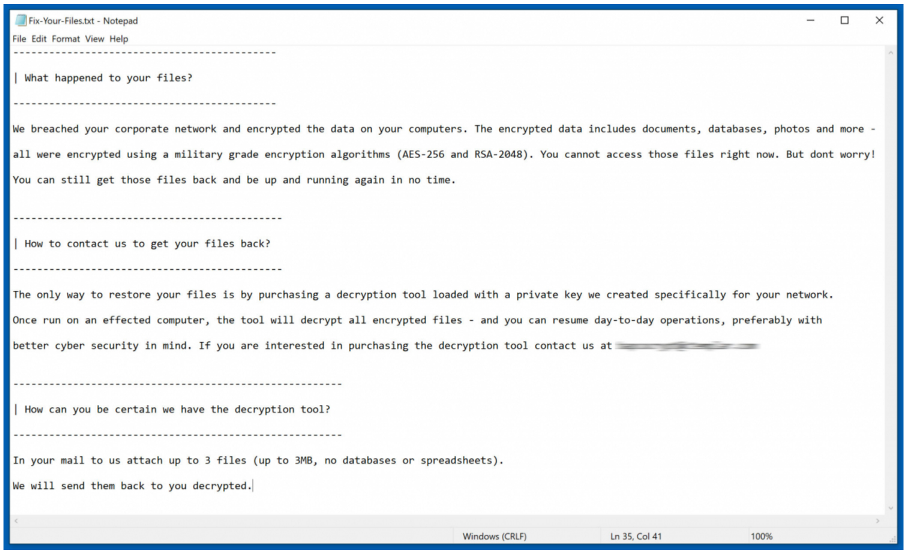
While traditional ransomware may append the same character string to the file extension of encrypted files, Snake is different. By appending random five-character strings to the file extensions, this ransomware attempts to hide itself from signature-based ransomware detection systems.

Another big distinction in the way Snake works is that it does not encrypt and rename each file one by one. Instead, it first encrypts all the target files and once that's completed, starts to rename them. This makes sure that the victim is not alerted to what is going on until the entire attack is complete.



Extortion: Pay for the antivenom

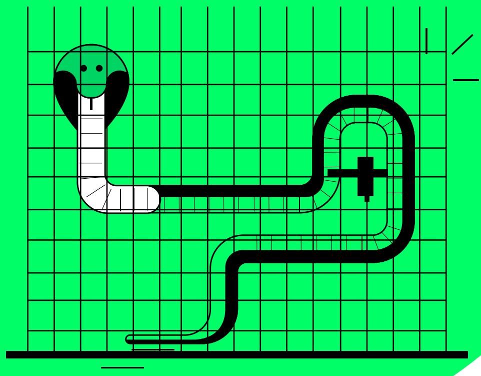
Once the files are encrypted and renamed, Snake leaves a ransom note on the victim's desktop. This message is a text file named "Fix-Your-Files.txt", found at C:\users\public\desktop. Figure 6 shows a typical Snake ransom message. Since this step involves writing to the public folder, it requires the ransomware to have run with administrator privileges. If Snake runs without administrative privileges, the ransom message will be written to \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 [redacted]


-------------------------------------------------------

| 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.
```

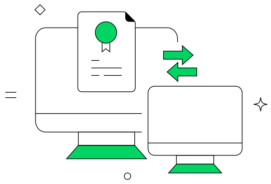
Figure 6: Snake's ransom message

The contact email address shared with the victim could be different under different attacks. As proof of how decryption works, the attacker may offer free decryption of any three encrypted files.



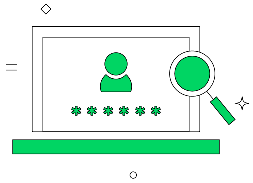
How to defend against Snake

There are several steps that organizations can take to defend against this ransomware strain:



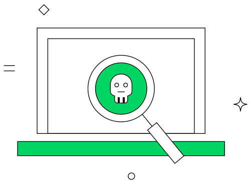
Detect changes to GPOs in real time:

One of the most common ways for Snake to gain entry into a network is through an insecure RDP connection. Organizations should therefore constantly monitor changes to users' remote access rights in Group Policy. Alerts can be configured so that IT administrators get notified when specific users' remote desktop access rights change. It might be best for the organization to follow a policy of not allowing remote access for users unless absolutely required to perform their job.



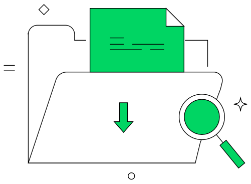
Monitor user logons:

Users can log on using RDP, RADIUS, and VPNs. Organizations should monitor each of these logon types and analyze both the source computer name and the source IP address. Any unusual activity needs to be detected immediately. Furthermore, action should be taken if tell-tale signs of malicious activity, such as a brute-force attack, are noticed.



Analyze if an attacker is attempting to hide their tracks:

One of the first things attackers do after gaining an initial foothold is attempt to hide their tracks by deleting event logs. After doing this, they may try to change audit policies so that further actions are not logged. Organizations should be able to detect both of these malicious activities.

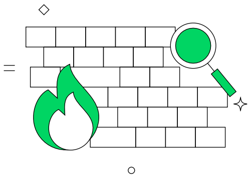


Look for unusual software installations:

An organization should be able to detect unusual software being installed anywhere in its network. In case unusual services or processes are started, these should again be detected in real time. It's even better if the organization is able to kill unusual processes through an automated incident response mechanism.

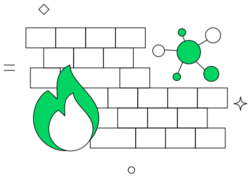
Look for killed processes:

Before encrypting files, Snake ransomware force-stops several important processes that are valuable for the smooth operations of a business. In case important processes are killed in quick succession, organizations should be in a position to put an end to this before things get worse.



Monitor firewall configuration rules:

Several ransomware variants, including Snake, make changes to firewall rules before encryption in an attempt to isolate the infected system. Unusual configuration changes must be detected and stopped.



Monitor firewall connections:

Apart from monitoring firewall configuration rules, organizations must also keep tabs on the traffic allowed through their firewalls and VPNs. This should be done to become aware of the source IP of any connection. Threat intelligence capabilities can be used stop communication with known malicious sources.

Detect deletions of shadow copies:

Shadow copies are stored locally on a machine at the root of the Windows volume in the System Volume Information folder. File integrity monitoring can help detect any change in or deletions from this folder.

Look for unusual file activity:

Ransomware, including Snake, perform several file activities such as file access, file modification, and file rename. These activities are usually performed in a very short period across different files. Organizations should be alerted in case this happens.

Implement multi-factor authentication (MFA):

MFA should be used at as many user touchpoints as possible. Even two-factor authentication can go a long way in deterring attackers.

Summary

Ransomware is one of the biggest challenges that organizations face today. This menace started way back in 1988 with the AIDS ransomware. After this initial foray, it kept a low profile until the mid-2000s when organizations were hit by Krotten. Recent years have seen more sophisticated ransomware, such as WannaCry and NotPetya. Snake ransomware made its entry in 2020. Unlike other ransomware, Snake focuses on hitting SCADA systems and ICSs. It is also a lot stealthier by virtue of being scripted in the Go language.

Snake usually gains an initial foothold due to an insecure RDP connection. The malware is then installed after making sure that the system is not already infected. The ransomware then goes on to delete shadow copy backups so that recovery options are not available to the victim. Encryption then begins, and all files with extensions that are part of a hardcoded list are targeted.

This list includes Word documents (.doc and .docx), Excel files (.xls and .xlsx), and PowerPoint presentations (.ppt and .pptx). After encrypting all the target files, Snake renames the files by appending a random five-character string to the file extension. Finally, once the files are encrypted and renamed, Snake leaves a ransom note on the victim's desktop.

To defend against Snake and other types of ransomware, organizations need to deploy the right security solutions and adopt cybersecurity best practices.

About Log360

Log360 is a comprehensive security analytics solution for all your log management and network security challenges. It brings together SIEM, UEBA, and SOAR capabilities. Perform audits, generate reports, and configure alerts for all changes in Active Directory, servers, file servers, NAS devices, workstations, endpoints, applications, and network devices. You can view your organization's security posture and meet the demands of security, privacy, and compliance from a single console. The automated incident response module enables you to configure workflows to mitigate risk even further. To learn more, visit http://www.manageengine.com/log-management.

About ManageEngine

ManageEngine is the IT management division of Zoho Corporation. It crafts comprehensive IT management software with a focus on making IT admins' jobs easier. Its 90+ products and free tools cover everything that IT needs, all at affordable prices. From network and device management to security and service desk software, ManageEngine is bringing IT together for an integrated, overarching approach to optimizing IT.

Appendix A

List of processes killed by Snake ransomware

These are some of the processes that Snake kills while executing an attack. This may not be an exhaustive list.

Process	Description
bluestripecollector.exe	BlueStripe Data Collector
ccflic0.exe	Proficy Licensing
ccflic4.exe	Proficy Licensing
cdm.exe	Nimsoft Related
certificateprovider.exe	Ambiguous
client.exe	Ambiguous
client64.exe	Ambiguous
collwrap.exe	BlueStripe Data Collector
config_api_service.exe	ThingWorx Industrial Connectivity Suite, Ambiguous
dsmcsvc.exe	Tivoli Storage Manager Client
epmd.exe	RabbitMQ Server (SolarWinds)
erlsrv.exe	Erlang
fnplicensingservice.exe	FLEXNet Licensing Service
hasplmv.exe	Sentinel Hasp License Manager
hdb.exe	Honeywell HMIWeb
healthservice.exe	Microsoft SCCM
ilicensesvc.exe	GE Fanuc Licensing
inet_gethost.exe	Erlang
keysvc.exe	Ambiguous
managementagenthost.exe	VMWare CAF Management Agent Service
monitoringhost.exe	Microsoft SCCM
msdtssrvr.exe	Microsoft SQL Server Integration Service
msmdsrv.exe	Microsoft SQL Server Analysis Services
musnotificationux.exe	Microsoft Update Notification Service
n.exe	Ambiguous
nimbus.exe	Broadcom Nimbus
npmdagent.exe	Microsoft OMS Agent

ntevl.exe	Nimsoft Monitor
ntservices.exe	Ambiguous
pralarmmgr.exe	Proficy Related
prcalculationmgr.exe	Proficy Historian Data Calculation Service
prconfigmgr.exe	Proficy Related
prdatabasemgr.exe	Proficy Related
premailengine.exe	Proficy Related
preventmgr.exe	Proficy Related
prftpengine.exe	Proficy Related
prgateway.exe	Proficy Secure Gateway
prlicensemgr.exe	Proficy License Server Manager
proficy administrator.exe	Proficy Related
proficyclient.exe	Proficy Related
proficypublisherservice.exe	Proficy Related
proficyserver.exe	Proficy Server
proficysts.exe	Proficy Related
prprintserver.exe	Proficy Related
prproficymgr.exe	Proficy Plant Applications
prrds.exe	Proficy Remote Data Service
prreader.exe	Proficy Historian Data Calculation Service
prrouter.exe	Proficy Related
prschedulemgr.exe	Proficy Related
prstubber.exe	Proficy Related
prsummarymgr.exe	Proficy Related
prwriter.exe	Proficy Historian Data Calculation Service
reportingservicesservice.exe	Microsoft SQL Server Reporting Service
server_eventlog.exe	Proficy Event Log Service, Ambiguous
server_runtime.exe	Proficy Related, Ambiguous
spooler.exe	Ambiguous
sqlservr.exe	Microsoft SQL Server
taskhostw.exe	Windows OS
vgauthservice.exe	VMWare Guest Authentication Service
vmacthlp.exe	VMWare Activation Helper
vmtoolsd.exe	VMWare Tools Service
win32sysinfo.exe	RabbitMQ
winvnc4.exe	WinVNC Client
workflowresttest.exe	Ambiguous

Appendix B

List of folders ignored by Snake during encryption

This is a partial list of files and folders that are ignored by Snake during the encryption process. The instruction to skip these files can be easily hardcoded into ransomware.

- Windir
- SystemDrive
- :\Recycle.Bin
- :\ProgramData
- :\Users\All Users
- :\Program Files
- :\Local Settings
- :\Boot
- :\System Volume Information
- :\Recovery
- \AppData\

Endnotes

1. Luke Graham, "Ransomware can cost firms over $700,000; cloud computing may provide the protection they need," CNBC, August 4, 2020, https://www.cnbc.com/2017/08/04/cloud-computing-cybersecurity-defend-against-ransomware-hacks.html.

2. Joel Witts, "How to stop ransomware attacks," Expert Insights, January 2, 2020, https://www.expertinsights.com/insights/how-to-stop-ransomware-attacks/.

3. Nihad Hassan, Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks, (New York: Apress, 2019), 47.

4. milkream (@milkr3am), "#Honda and #Enelint became next victims of #Ekans #Ransomware, " Twitter, June 8, 2020, 3:30 p.m., https://twitter.com/milkr3am/status/1269932348860030979?s=20.

5. Steve Dodson, "Snake ransomware sinks teeth into Honda and Enel," Admin By Request, https://www.adminbyrequest.com/Blogs/Snake-Ransomware-Sinks-Teeth-into-Honda-and-Enel.

6. Milena Dimitrova, "Remove Snake ransomware virus - What you should know about it," Sensors Tech Forum, January 29, 2020, https://sensorstechforum.com/remove-snake-ransomware/.

7. Takashi Yoshikawa and Kei Sugawara, "Understanding internal structure of the SNAKE (EKANS) ransomware," MBSD Blog, June 23, 2020, https://www.mbsd.jp/blog/20200623.html.

8. Jim Walter, "New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware," Sentinel Labs, January 23, 2020, https://labs.sentinelone.com/new-snake-ransomware-adds-itself-to-the-increasing-collection-of-golang-crimeware/.

$ Get Quote   ⤓ Download