

Cybereason vs. NetWalker Ransomware

 cybereason.com/blog/cybereason-vs.-netwalker-ransomware

Cybereason vs. NetWalker Ransomware



Cybereason vs. NetWalker Ransomware



Written By
Cybereason Nocturnus

February 16, 2021 | 4 minute read

The NetWalker ransomware has been one of the most notorious ransomware families over the course of the past year, targeting organizations in the US and Europe including several healthcare organizations, despite several known threat actors publicly claiming to abstain from targeting such organizations due to COVID-19.

Key Findings

Worldwide Threat: NetWalker was employed in attacks across a variety of industries around the world, which caused great damage to many organizations.

Encrypting Mapped Drives: NetWalker encrypts shared network drives of adjacent machines on the network.

Double Extortion Operations: The threat actor behind NetWalker threatens to publicly reveal stolen data if payments are not made.

High Severity: The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.

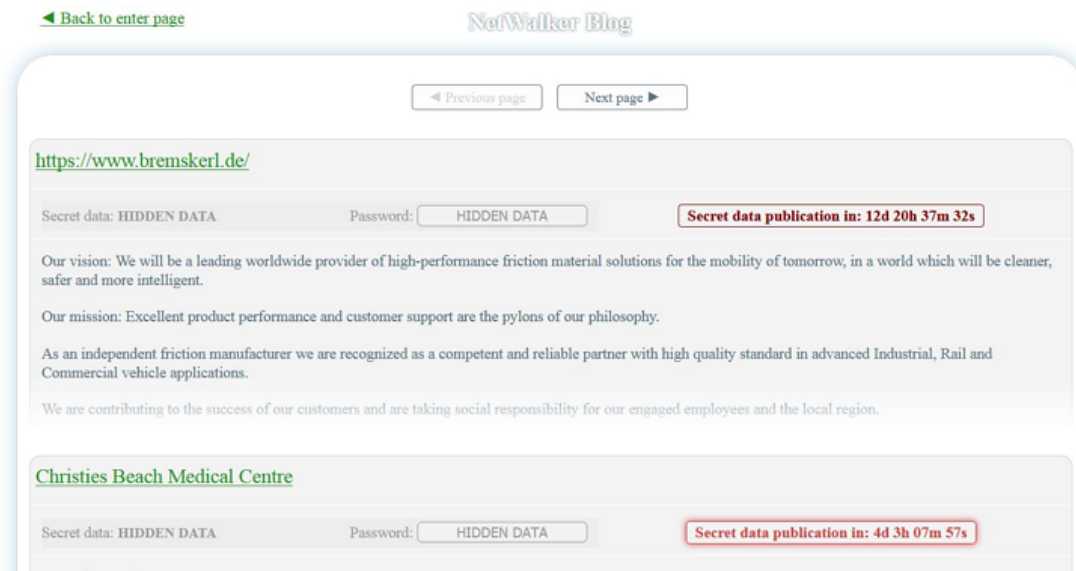
Detected and Prevented: The Cybereason Defense Platform fully detects and prevents the NetWalker ransomware.

Cybereason Blocks NetWalker Ransomware

NetWalker ransomware first surfaced in August of 2019 (first dubbed Mailto). The group behind NetWalker operates a Ransomware-as-a-Service (RaaS) business model, which means they provide their infrastructure, tools and support in exchange for affiliate payment.

NetWalker operators have adopted the recent popular trend among ransomware purveyors: double extortion. In addition to demanding a ransom for the encrypted files, the group behind NetWalker steals sensitive data and files from its victims. The group extorts the victims by threatening to leak the stolen data unless ransom is paid. This technique renders the practice of data backups all but moot in combating the impact from ransomware attacks. Other known ransomware groups that leverage the double extortion paradigm are Maze, REvil, and DoppelPaymer.

The group behind NetWalker also maintains a blog on the Darknet where the group publishes information about its new victims alongside a countdown to the deadline for the ransom to be paid. If the time limit has expired and no ransom has been paid, the stolen data is published to this blog:



Netwalker Blog

The targets of NetWalker belong to various sectors, among them educational facilities, local government, healthcare providers, and private companies. In June of 2020, three US universities were targeted with the ransomware: the University of California San Francisco, Michigan State University, and Columbia College of Chicago.

Different government facilities were victims of NetWalker in Austria and Argentina in the past year as well. The attackers behind NetWalker do not pass on healthcare facilities as well - it has been reported that NetWalker has attacked Wilmington Surgical Associates and 13GB of data was stolen. Other healthcare facilities have been targeted as well, among them Crozer-Keystone Health System.

Other companies that fell victim include NameSouth, a US-based auto parts distributor, K-Electric, an electricity provider in Pakistan, and Toll Group Deliveries, an Australian transportation and logistics company.

Infection

The NetWalker ransomware has operators have been observed to using several different methods to infect an organization, these including the abuse of COVID-19 topics for phishing mails, weak credentials for Remote Desktop Protocol (RDP), exposed web applications and unpatched VPNs. According to a Federal Bureau of Investigation (FBI) Flash Alert, “two of the most common vulnerabilities exploited by actors using NetWalker are Pulse Secure VPN (CVE-2019-11510) and Telerik UI (CVE-2019-18935).”

For example, Cybereason observed an attack that started with a VBS file was attached to a phishing email with a COVID-19 lure content:

As a means of evasion, NetWalker does not directly declare its Windows API imported function in the import table. Instead, the ransomware dynamically resolves all of its API as a technique used to make static analysis harder. NetWalker compares a CRC32 hashed value of an API name to the exports of specific modules, then it builds a struct that holds the address of NetWalker's API:

```
api_struct->RtlAllocateHeap = search_api(v1, 0xA1D45974);
api_struct->RtlFreeHeap = search_api(v1, 0xAF11BC24);
api_struct->RtlReAllocateHeap = search_api(v1, 0xB973B8DC);
api_struct->memset = search_api(v1, 0x8463960A);
api_struct->memcpy = search_api(v1, 0xD141AFD3);
api_struct->memcmp = search_api(v1, 0x57F17B6B);
api_struct->sprintf = search_api(v1, 0x23398D9A);
api_struct->strcpy = search_api(v1, 0xBD6735C3);
api_struct->strcat = search_api(v1, 0x900F6A6E);
api_struct->strchr = search_api(v1, 0xA8AE7412);
api_struct->strtol = search_api(v1, 0x4896A43);
api_struct->wcscpy = search_api(v1, 0x4C8A5B22);
api_struct->wcscat = search_api(v1, 0x61E2048F);
api_struct->strstr = search_api(v1, 0x52FF8A3F);
api_struct->wcsstr = search_api(v1, 0xA312E4DE);
api_struct->wcsncmp = search_api(v1, 0xCA3A8F9A);
api_struct->wcsncpy = search_api(v1, 0x958F47AF);
api_struct->RtlRandomEx = search_api(v1, 0x9AB4737E);
api_struct->RtlRandom = search_api(v1, 0x7EF4BAE5);
api_struct->RtlInitAnsiString = search_api(v1, 0x4A5A980C);
api_struct->RtlInitUnicodeString = search_api(v1, 0x7AA7B69B);
api_struct->RtlAnsiStringToUnicodeString = search_api(v1, 0x4491B126);
api_struct->RtlUnicodeStringToAnsiString = search_api(v1, 0x27AE6B27);
api_struct->RtlFreeUnicodeString = search_api(v1, 0x43681CE6);
```

NetWalker dynamically loads API

After resolving the needed API, NetWalker loads the ransomware configuration. The configuration is saved in the ransomware resources and is RC4 encrypted:

```

"mpk": "/fqCb2TTvBeb3VoL4lXa1fgDDn+sE04+
"mode": 0,
"spsz": 15360,
"thr": 1000,
"namesz": 8,
"idsz": 6,
"lfile": "{id}-Readme.txt",
"onion": "rnfdsgm6wb6j6su5txkek4u4y47kp
"lend": "SGkhDQpZb3VyIGZpbGVzIGFyZSB1bmN
"white": {
  "path": [
    "*system volume information",
    "*windows.old",
    "*:\\users\\*\\*temp",
    "*msocache",
    "*:\\winnt",
    "*$windows.~ws",
    "*perflogs",
    "*boot",
    "*:\\windows",
    "*:\\program file*\\vmware",
    "\\*\\users\\*\\*temp",

```

NetWalker configuration file

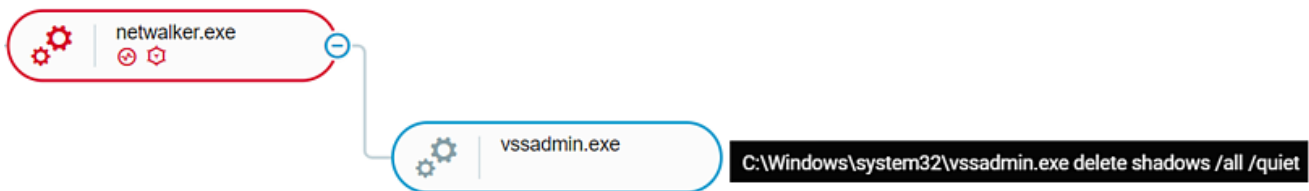
The configuration file holds the following information:

Parameter	Description
mpk	Public key

mode	Encryption mode
spsz	Encryption chunk size
thr	Threading limit
namesz	Length of generated named of persistence executable
idsz	Length of generated id
lfile	Template for the ransom file name
onion	TOR site
lend	Base64 encoded template of the ransom note
white	Whitelist of directories, files, and extensions
kill	Processes and Services to terminate, as well as a task to do after encryption.
net	Flags for network resources encryption
unlocker	Exclusion during encryption

NetWalker Configuration Data

Before encrypting the victim's files, NetWalker deletes the Windows' Shadow Copies using the `vssadmin.exe delete shadows /all /quiet` command. On some variants, the command is spawned by the executable of the ransomware; on others, it is spawned by the PowerShell script which executes NetWalker:



NetWalker deleted shadow copies

Next, the ransomware will start the encryption stage. NetWalker ransomware checks for valid drives in the system using *GetLogicalDriveStringsW*. For network drives, the ransomware uses *ImpersonateLoggedOnUser* in an attempt to impersonate the context of the current user in order to access the remote drive. NetWalker then encrypts the files on the network and local drive using Salsa20 encryption. After the files are encrypted, the ransom note is placed.

On some variants, NetWalker also creates persistence via the run registry key and drops a copy of the ransomware to *C:\Program Files\random_generated_name\random_generated_name.exe* or *'C:\Program Files (x86)\random_generated_name\random_generated_name.exe'*.

```

Hi!
Your files are encrypted.
All files for this computer has extension: .21ee3e

Your filenames can be changed too, except extensions for free decrypt.

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--
Our encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

--
For us this is just business and to prove to you our seriousness, we will decrypt you few files for free.
Just open our website, upload the encrypted files and get the decrypted files for free.

Additionally, you must know that your sensitive data has been stolen by our analyst experts and if you choose to no cooperate with us, you
are exposing yourself
to huge penalties with lawsuits and government if we both don't find an agreement. We have seen it before; cases with multi million costs in
fines and lawsuits,
not to mention the company reputation and losing clients trust and the medias calling non-stop for answers. Come chat with us and you could
be surprised on how
fast we both can find an agreement without getting this incident public.




--
***
IF YOU ARE AN EMPLOYER OF A COMPANY THEN YOU SHOULD KNOW THAT SPREADING SENSITIVE INFORMATION ABOUT YOUR COMPANY BEING COMPROMISED IS A
VIOLATION OF CONFIDENTIALITY.
YOUR COMPANY'S REPUTATION WILL SUFFER AND SANCTIONS WILL BE TAKEN AGAINST YOU.

```

NetWalker ransom note




CYBEREASON DETECTION AND PREVENTION

The Cybereason Defense Platform is able to prevent the execution of NetWalker Ransomware using multi-layer prevention that detects and blocks malware with threat intelligence, machine learning, and Next-Gen AV (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a MalopTM:

Type	Root cause	Affected machines	Detected activity
	Ransomware explorer.exe Ransomware behavior	 [REDACTED]	 Ransomware

Malop triggered due to the malicious activity

Additionally, using Cybereason's PowerShell protection feature, Cybereason is able to detect and prevent the initial PowerShell infection stage of NetWalker:

 Malicious command Fileless malware	Prevented		
Description PowerShell used to execute malicious command	Detection name Injection (240)	Module Injection (240)	Process name powershell.exe

PowerShell protection blocks script which injects NetWalker

MITRE ATT&CK TECHNIQUES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Impact
<u>Phishing</u>	<u>PowerShell</u>	<u>Registry Run Keys / Startup Folder</u>	Access Token Manipulation	<u>Dynamic-link Library Injection</u>	<u>Taint Shared Content</u>	<u>Data Encrypted for Impact</u>

JavaScript/JScript

Tom Fakterman



Tom Fakterman, Cyber Security Analyst with the Cybereason Nocturnus Research Team, specializes in protecting critical networks and incident response. Tom has experience in researching malware, computer forensics and developing scripts and tools for automated cyber investigations.

Netwalker Ransomware | Indicator's of Compromise

VBS | SHA-256

9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967
ad8d379a4431cabd079a1c34add903451e11f06652fe28d3f3edb6c469c43893

SHA-1

c880daabaca11dde198b6340e4430401d0bfef10
f26323676b7ed39590ddfedd344b0cf605393598

PowerShell | SHA-256

2357e1db66083920745ec85382c3bfc7d3e0a5ef6a7abd43e600c73705cb7198
f17974630cf05792a15a194a29ddae5aab8f88537cb4d12677498c21ad176cf4
7aa142995da4f813829d3cf46a0b359e26c60372abd44b15256a604543c4ca22
d481ca6cd079ff703d09fc4677c1e2c12dc2f4c4af51efc9ca43db873e0acd12
b1b7bf1bb54b3da1b1febbf1aab3878a28e4c5b4fc73532559771ee09541a18f
3053e044114b498d58a2cd2becb25d4efc1c701b6bf82658f1198f5dd03dd5c1
063aef7b4bb6479e9e7e8db36ae08d1b85f9b3502d8312e61dae6c3a80f6c88e
eaa0557cc769e333db8ae06ec97f19fa93082ae8f2964094794d7135b67b1e0b
7c3050a411edb10aaa9fd0c4e7ea793cfca85dc11c1aba3180e5c965f140725f
7e1f41c8fa1077d5f56ef070275d206aea7f05921a5bb866375eb752a22d2eb1
2bdd9326568cec881a39d11a6aef4be6a2d1d08573ba8d865eaa8a9621151259
9737bbe8af662f8d1e3956f2f7e31c0df3835994f52dbc7d6347151323c6de6f
fbadda96e8b96c78f38b76b883b65b83de7c27aa2fc12032b878f379c61b3544
1a387a66d0ae9f0aabeb33f46856fcd8d7621d210d87494f696b831f94537f1b
c98c0a52b328e834ea331f3d674d138c317443a2a0db2d13e15efd451cb1ad5c
d48e2f32bfc0fe23f8543fba5c5cd75ac59261c973e0f9596ae2c0881f9c5b48

SHA-1

0d75e9a2fbed9cdb31c4e46184d3a8dfcf2a6735
1b2d111cbfcdb1c42be9c704d4ae9a10a5af6f7e
01399a2d09aee2a0cadccd3d470bf0046d222bd8
b0e65b8376ac99c9af4b4817a15a8f7ac9af28e1
651d443a187bb38a5a552dff1f0e0a87ff7972f4
d02559afe68776836f3792a9d3becc7f3e92a88d
f3f08144aa146c38bd80acef687404cbe73a9511
681146f3b1e84f56e6e6c7516cd210784ceca8f1
a0d0b0f0ccd09e5b83c8ed7df9222366b819d4b9
eebf51b7b4e4c3108d455289de8db416bb185be4
53c52a1111fec1fa829f88ca081c0f3d682a33d5
75aa6ecf7694c73aed2d2670957e39e2703740c7
8bd97ba2060a90b7e08c8f1631c7eea92a807cca
c440ab6e70fc6d2dff7f7b3478b03a99672d062f
64176f72b05cf96e3a3dad206b488bdd82c5ef69
6f88450f9eaa8710497477ec36f9d8b65f5cdb99

SHA-256

57cf4470348e3b5da0fa3152be84a81a5e2ce5d794976387be290f528fa419fd
7a19f45ab150fd544872941be5c4a2919252e3af7ede1c3981ab35a1f92bee92
853fa18adc3f9263a0f98a9a257dd70d7e1aee0545ab47a114f44506482bd188
8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160
b6456d9f3af3bda0223cf7aafed13026e7c2e8f0c5a0b540b095d900ffbcddaa
d1d31e72a617a54648142bacc987ad860fce9b60f9813842877f2295e3a95ef4
b7dc59261a6a5a94c6a2350be1507ffabc8737c990ac0cac84c8b2ba001add21
bd3fdf1b50911d537a97cb93db13f2b4026f109ed23a393f262621faed81dae1
0ec55df6c5dd2f6e5b8ce35f546e6789a61bd8906952873e174d51ee3484f6de
1635be7dcf50c126665eaaaf8737d279b4f4039123bbdb64f1e928722052e0fb5
48924e3a42973944c65ce56842397bfce50189a9eb90cba08d23fba17d385e91
28f3d14de7356631cc6526b9df9f1539c71f6e3d7fcb1a5382f50bd1aecb0faf
4d38e23d5847465b21de7e99bd209ba113b47d5370f8118297d641d33db3cfc2
72174353e04e2544f88b3b23aa228c088470e568066afabc5aac40bfe3ad1e
6764c4f08019a120e1636891e05481cd226b7baa29c9b00c839161e443814d7e
c21cc94e3b9f3999b183f12a075ab662dd12662b11dd4f9274152979bf68d4db
e825159d11f047e54150d9e5819c6302acf151ccc9cec9e2f5fb01e030e82bf2
8e0589b59866389754b78dd818f7b6727f532ef8834d99c0636cb7e0a5b3bdf5
db664e01160a2a353a2f2387b3ff03e8e5e3c29166939860cd2efb888ca479aa
de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d
c414bbb789af8e3fb93b33344b31f1991582ec0f06558b29a3178d2b02465c72
4c9a1e6a8114e2482efb00398dc2817bb5fa1a0d52328be2ce7e16e215f8fee0
946a922d8693249525f60ddafaf3d982e32d3ed10cea73438eb353c97ab7d6bc
58e923ff158fb5aec293b7a0e0d305296110b83c6e270786edcc4fea1c8404c
c6f4e1f9aa954cfd4d2e36c9b2d3e46ea0f8ad963860831211d5d3984fb6467d

SHA-1

3a233709f22db2e63f41c9f095bc1bc3e1e6932d
789d07687e27e9dc245fb0c754dbc48d482df7f8
8e7a5500007c1552e1231bd1157433f7ef638672
a3bc2a30318f9bd2b51cb57e2022996e7f15c69e
1156df56a6659457129a33543f46a278a49fd701
51a413a1ebf50357c5377c3a3ed49a5f80977758
c3acd818beaf88f75fbc3cbf44708b58aa7aced8
03023d7e3a54d915cca82429dfeedb1bebd5c182
aced3880b62721cd2cd1d8d425086394a4e39fbc
df062e7482c73a19c69288970e90628e9dd57111
ccd52c78ee9843bb40df148c04b98fb63b564a76
05d6978485745fe73ef3b624e39219bbcfa8c4c8
3d094461dcdbb3d5c50ff368e36c73e94f702334
3a34b13bd0545231aa68344412130d296e17835a
156fc33f237c6d92aa56386e1f72360a46b6331a
b6e43e43f3ea5d008e08126d4d172a0e2a437a08

5d67c7b45c4c0f7ee324caa369404079803dea1b
89dbeae64eaf6e9ed6bde9b7cb927b58962dde59
63d72bc6c5b43959b25ecd091ccd20fb4edd2955
6fd314af34409e945504e166eb8cd88127c1070e
3abeddbbbd29310290955cc7c1a895550c92ab96
bc0ff76bce27a22ab41038e057fd5687bf2eff1d
D4c2fc3f782d4d2e3d64e17d6ca3ed8e6495cd01
e393a9ecf0d0a8babaa5efcc34f10577aff1cad1
43493ae4e94f9db1335d1e1395634d7768c7732c



About the Author

Cybereason Nocturnus



The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

[All Posts by Cybereason Nocturnus](#)