Cybereason vs. NetWalker Ransomware

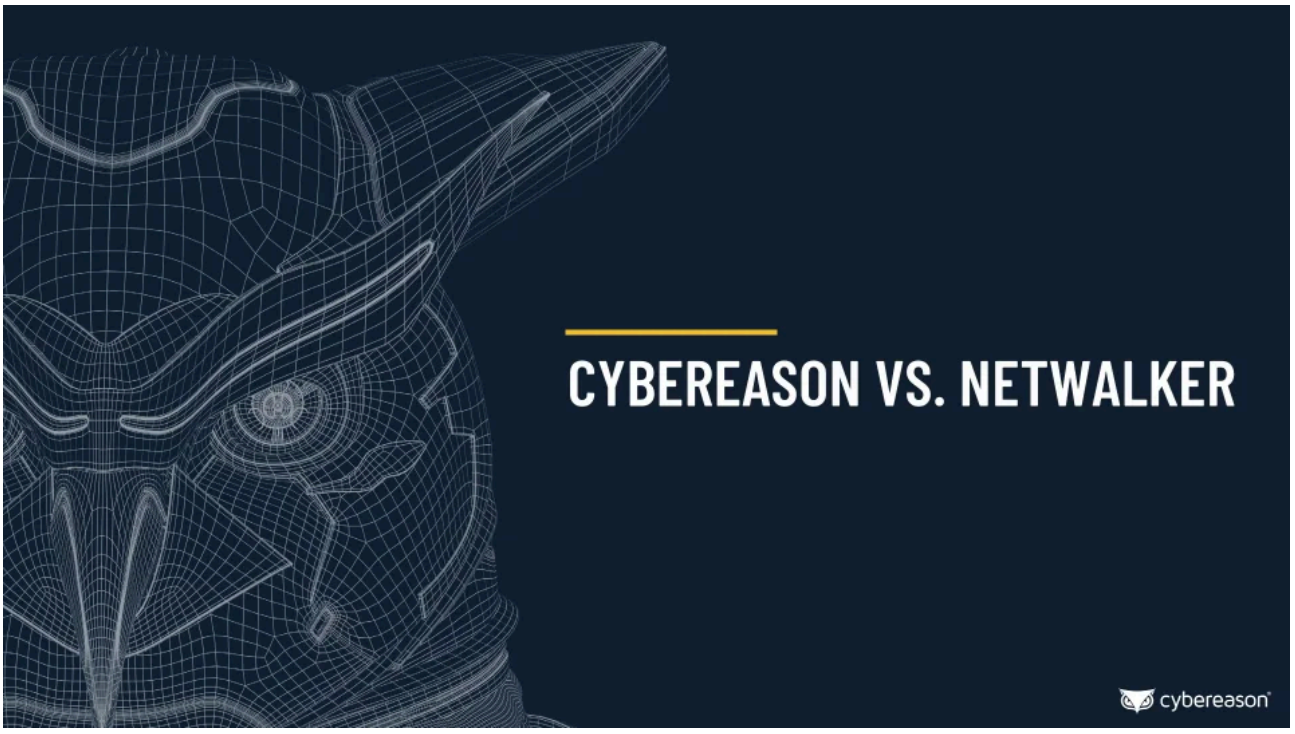
By Cybereason Nocturnus

Archived: 2026-04-05 19:21:53 UTC

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.

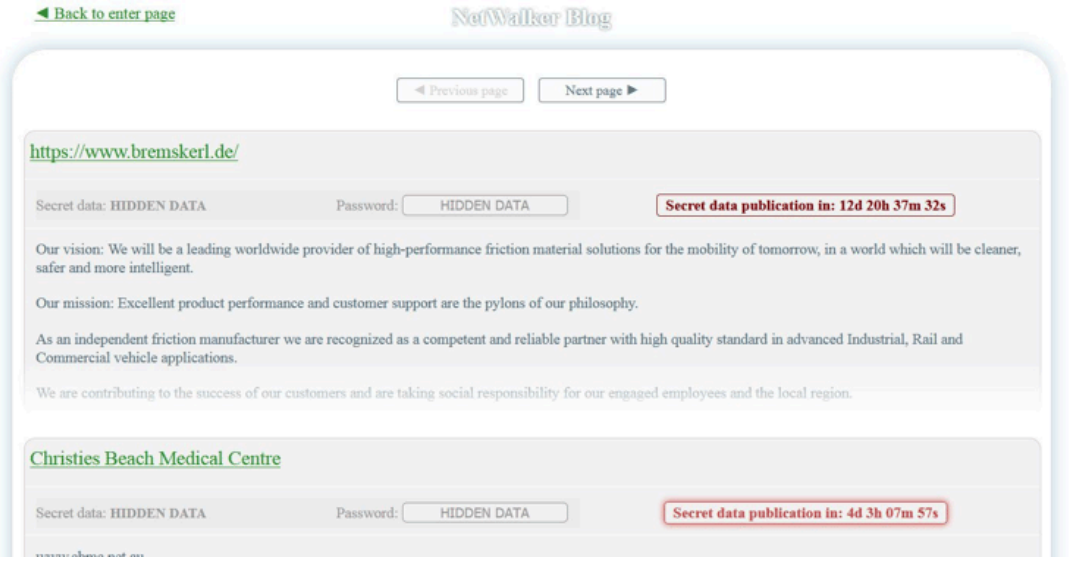


Cybereason Blocks NetWalker Ransomware

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:

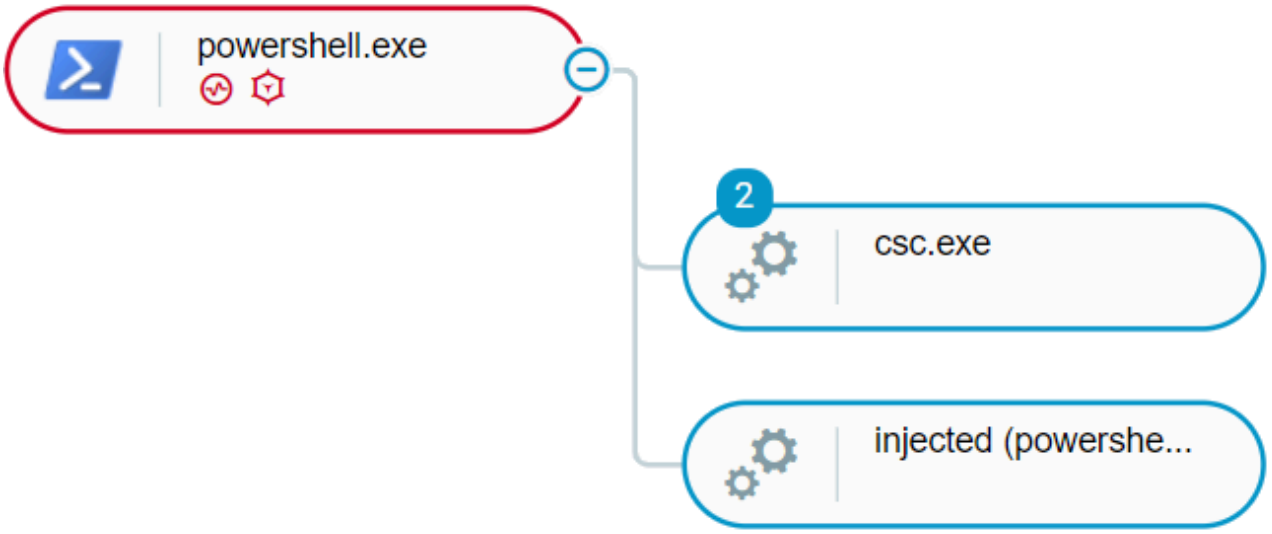
```
code = "==A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,A#>,i0es@Ls@IfoE.MbgDxT*B2dWyaG+VteLPCE.pmOx9oIbLiv?J<
    A#>,wZGrzh!PE.uDPb1jdtjh!J<HA#>,qJ<h!Bs@aC3ICA#>,*d+rabmaSn4cZ3uYSmg61Xh!nDTE.J<
    gel8$r9SgjVs@XwLxdr77F%KySoBPw1UdeR4mTCpfs@5h!VA#>,cOgOx8$M0c0eWMtke3h!LCWqHS8$*jxJ<
    F%VclYYdddLT7eVRBULN4WJ<Z9z9h!deo5dxMq5CbzA#>,v?Os@yaLQy+h!QE.T4F%BZfZ13TP8$8$F%eBaLBeJ<
    IyInoVps@1s@xqF%v?R*6OIt5iUOkzRpS776w33u9MKVr8$MMf7KUqKXRQrVHXj3XUWql9peK8$51l+wJ<
    MotH49HTjKXbR7g1BQA#>,CSA#>,A#>,F%E.QA#>,B0w9Gikh!qkgBNA#>,Tmv?SGWYMxs@SJ<WwxO3fGB23eh!p4TQBBWE.DBJ<
    E.QD3bISGqSCGMCMaNTMxUTMycTMzA#>,DMy0wF%PE.TBJ<E.QD3bISGqSCGwBMBcQA#>,Ncv?h!IZoKJ<
```

CORONAVIRUS_COVID-19.vbs script

Upon execution, the script will drop the ransomware to "%temp%" and execute NetWalker:

CORONAVIRUS_COVID-19.vbs script deploys NetWalker as seen in Cybereason

In other cases, the ransomware was deployed following an interactive hacking operation using a ported-version of the ransomware payload that was injected to explorer.exe by a PowerShell script:



PowerShell payload injects NetWalker as seen in Cybereason

Ransomware Analysis

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->wcscmp = search_api(v1, 0xCA3A8F9A);
api_struct->wcsncmp = 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:

NetWalker configuration file

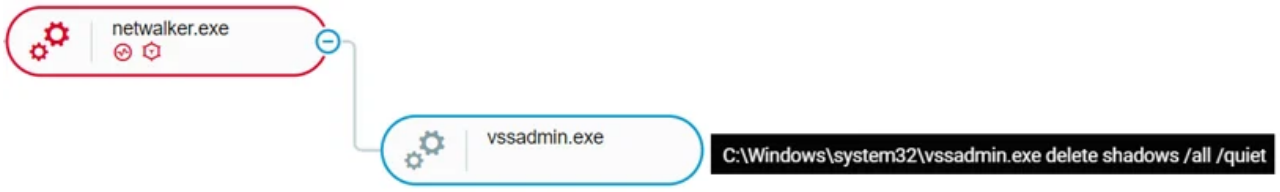
The configuration file holds the following information:

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.

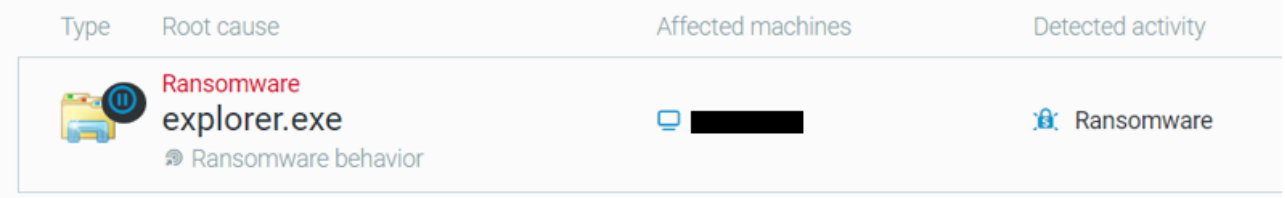
On some variants, NetWalker also creates persistence via the run registry key and drops a copy of the ransomware to *C:\Program Files\random_generated_name\random_generated_name.exe'* or *'C:\Program Files (x86)\random_generated_name\random_generated_name.exe'*.

```
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

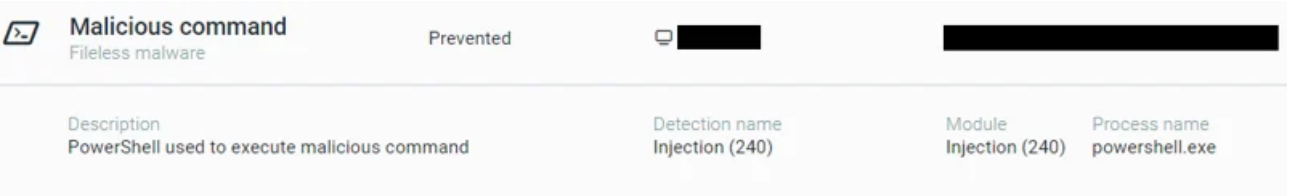
CYBEREASON DETECTION AND PREVENTION

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 Malop™:



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:

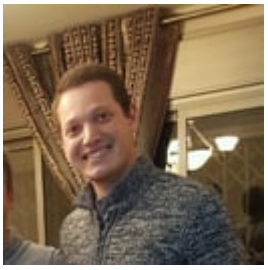


PowerShell protection blocks script which injects NetWalker

MITRE ATT&CK TECHNIQUES

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

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
