Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report

By Unit 42

Published: 2021-03-17 · Archived: 2026-04-02 12:30:25 UTC

Threat Assessment: NetWalker Ransomware

Executive Summary

NetWalker ransomware was first observed in August 2019 and was originally called Mailto by the security community because the encrypted files were changed to a .mailto extension. After analysis of a decryption tool, provided by developers after payment, the true name given by its developers was found to be NetWalker. At the time, it was a commodity threat, meaning it would be distributed via mass spam campaigns not taking into consideration who their victims would be.

A cybercrime group called Circus Spider, which is believed to be of Russian origin, created this ransomware.

NetWalker has become a considerable threat to corporate victims in particular due to not only encrypting data but threatening to publicly release sensitive data stolen during encryption.

NetWalker Ransomware Overview

In March 2020, NetWalker shifted to a ransomware-as-a-service (RaaS) model, and the Circus Spider group began looking for affiliates to propagate their malware. Affiliate attackers would be responsible for propagating the

malware and would receive a percentage of the ransom collected in return. Circus Spider sought affiliates who met the following requirements:

- Speak Russian.
- Experience with Red Team skills.
- Proof of experience.

Circus Spider wanted their affiliates to take a more targeted approach toward larger and higher paying victims with their malware. Victims have been reported to include hospitals, educational institutions and local governments. NetWalker often capitalizes on current events as part of their decoys. Since early 2020, several groups leveraging NetWalker have used COVID-19 themed phishing emails to target and compromise a number of hospitals, as well as a university that specializes in medical research.

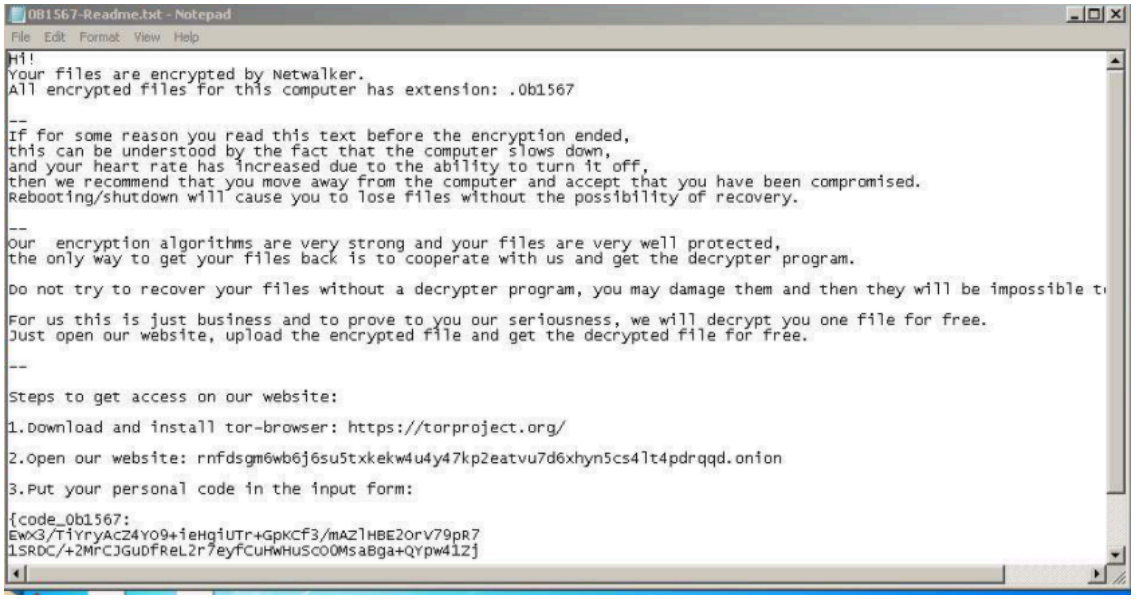

Figure 1. NetWalker ransom note (source: Any.Run).

As part of RaaS, affiliates would target victims in one of several different methods. The following methods are the most commonly observed:

- Phishing emails with attached malicious files, like VBScript or PowerShell.
- Exposed or vulnerable Remote Desktop Protocol (RDP) services.
- EXE files.

Once in victims' networks, affiliates often target and gather high-value data such as personally identifiable information (PII) or company-specific data. This data is then copied and exfiltrated before encrypting. Figure 1 shows a sample NetWalker ransom note. Actors behind NetWalker often also attempt to dump credentials and laterally move to other hosts, with the aim of compromising additional victims.

The exfiltrated data will be posted to a specific leak site that the NetWalker operators manage – similar to the approach used by many ransomware operators. Victims would then be on a countdown to pay ransom, with the price demanded increasing as the countdown decreases.

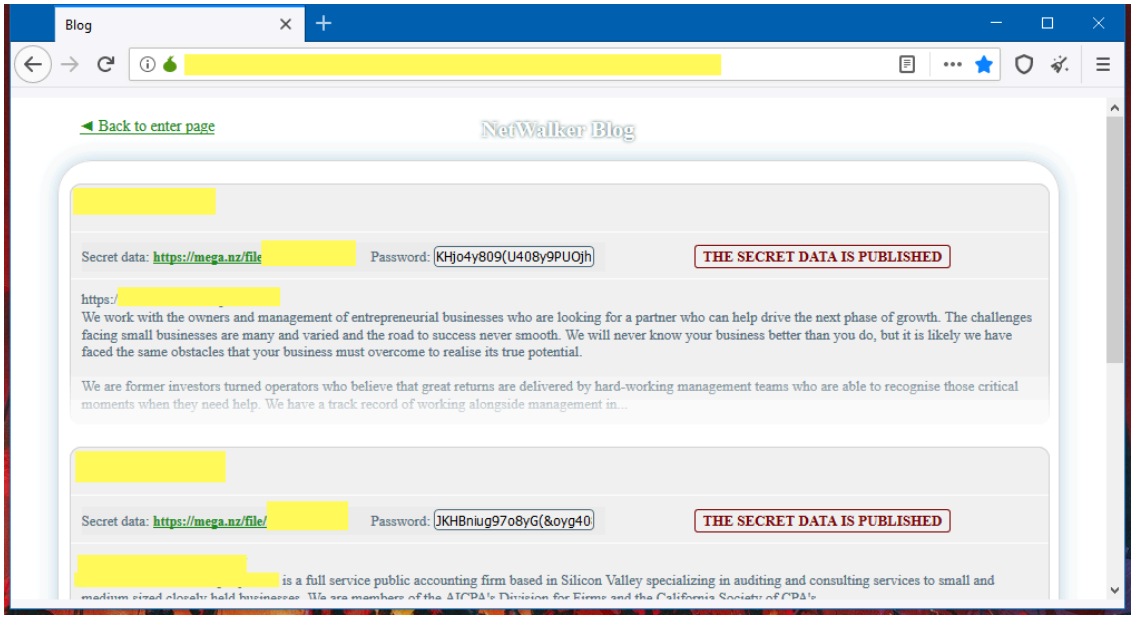

Figure 2. NetWalker leak site (source: ZDNet).

In 2020, Palo Alto Networks observed Netwalker victims in the government, healthcare, manufacturing, transportation and logistics, and energy sectors. Victim locations span nearly every continent, with countries including US, Canada, Saudi Arabia, France, Germany, Australia, New Zealand, Sweden, Pakistan, India, Thailand, UK, United Arab Emirates, Colombia, and South Africa.

In early 2021, authorities attempted a takedown of the NetWalker ransomware. This included an arrest, confiscation of funds and seizure of the leak website, seen in the NetWalker leak site image above, where victims' data is uploaded pending full release. It remains to be seen how effective these law enforcement actions will be in stopping Circus Spider developers, but it is a hopeful step in the direction of stopping and possibly prosecuting these actors.

More information on NetWalker victimology can be found in the 2021 Unit 42 Ransomware Threat Report.

Courses of Action

This section documents relevant tactics, techniques and procedures (TTPs) used with NetWalker and maps them directly to Palo Alto Networks product(s) and service(s). It also further instructs customers on how to ensure their devices are configured correctly.

Product / Service	Course of Action
Initial Access, Execution, Command and Control, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Credential Access, Collection, Discovery	
The below courses of action mitigate the following techniques: **Exploit Public-Facing Application [T1190], Windows Management Instrumentation [T1047], Ingress Tool Transfer [T1105], Spearphishing Attachment [T1566.001], Valid Accounts [T1078], Lateral Tool Transfer [T1570], PowerShell [T1059.001], Visual Basic [T1059.005], Obfuscated Files or Information [T1027], Deobfuscate/Decode Files or Information [T1140], Service Execution [T1569.002], Windows**	

Command Shell [T1059.003], Registry Run Keys / Startup Folder [T1547.001], Dynamic-link Library Injection [T1055.001], OS Credential Dumping [T1003], Data from Local System [T1005], Modify Registry [T1112], File and Directory Discovery [T1083]	
NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources exists
	Set up File Blocking
	Ensure that User-ID is only enabled for internal trusted interfaces
	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled
	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
	Ensure that the User-ID service account does not have interactive logon rights
	Ensure remote access capabilities for the User-ID service account are forbidden
	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones
	Ensure 'SSL Forward Proxy Policy' for traffic destined to the internet is configured
	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS
	Ensure that the certificate used for Decryption is trusted
Threat Prevention†	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low and informational vulnerabilities
	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic
	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
	Ensure a secure antivirus profile is applied to all relevant security policies
	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories and threats
	Ensure DNS sinkholing is configured on all anti-spyware profiles in use

	Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use
	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the internet
	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned and set to appropriate actions
URL Filtering†	Ensure that PAN-DB URL Filtering is used
	Ensure that URL Filtering uses the action of ‘block’ or ‘override’ on the <enterprise approved value> URL categories
	Ensure that access to every URL is logged
	Ensure all HTTP Header Logging options are enabled
	Ensure secure URL filtering is enabled for all security policies allowing traffic to the internet
WildFire†	Ensure that WildFire file size upload limits are maximized
	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
Cortex XSOAR	Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint
	Deploy XSOAR Playbook - Block IP
	Deploy XSOAR Playbook - Block URL
	Deploy XSOAR Playbook - Hunting and Threat Detection Playbook
	Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators
	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
	Deploy XSOAR Playbook - Endpoint Malware Investigation
	Deploy XSOAR Playbook - Access Investigation Playbook

	Deploy XSOAR Playbook - Impossible Traveler
Cortex XDR	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection
	Configure Behavioral Threat Protection under the Malware Security Profile
	Configure Restrictions Security Profile
	Configure Malware Security Profile
Credential Access	
The below courses of action mitigate the following techniques: **Brute Force [T1110]**	
NGFW	Customize the action and trigger conditions for a Brute Force Signature
Cortex XSOAR	Deploy XSOAR Playbook - Brute Force Investigation Playbook
Impact	
The below courses of action mitigate the following techniques: **Data Encrypted for Impact [T1486], Inhibit System Recovery [T1490]**	
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response
	Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation

Table 1. Courses of Action for Netwalker ransomware.

†These capabilities are part of the NGFW security subscriptions service.

Conclusion

While the concept of an attacker leveraging ransomware affiliate programs is not new, the actors behind NetWalker performed a certain level of vetting prior to the acceptance of new affiliates, which illustrates a higher level of effort than has been observed from other groups and actors. Their specific requirements – Russian-speaking candidates with demonstrated Red Team skills to attack and successfully compromise victims – allude to the relative sophistication of the actors. By recruiting skilled individuals as affiliates, the actors appear to be looking for larger payouts in more targeted campaigns against victim organizations.

The actors behind NetWalker aren’t the only group to move toward finding more skilled affiliates with an eye toward targeting larger organizations with higher potential for ransom payouts. In light of this, it’s important for enterprises to employ both robust defensive technologies and capable cybersecurity expertise in their environments.

Palo Alto Networks detects and prevents NetWalker in the following ways:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
    - Indicators for NetWalker.
    - Anti-Ransomware Module to detect NetWalker encryption behaviors.
    - Local Analysis detection for NetWalker binaries.
- Next-Generation Firewalls: DNS Signatures detect the known NetWalker command and control (C2) domains, which are also categorized as malware in URL Filtering.
- AutoFocus: Tracking related activity using the NetWalker tag, originally known as Mailto.

Additionally, Indicators of Compromise (IoCs) associated with NetWalker are available on GitHub, and have been published to the Unit 42 TAXII feed.

Additional Resources

- Department of Justice Launches Global Action Against NetWalker Ransomware
- Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay
- NetWalker Ransomware Group Enters Advanced Targeting “Game”
- Netwalker Ransomware Explained: What You Need to Know [Updated]
- Take a “NetWalk” on the Wild Side

Continue Reading: Zeppelin

Back to Top
