Feb 18 2024

NETMANAGEIT

Intelligence Report

Alpha Ransomware Emerges From NetWalker Ashes

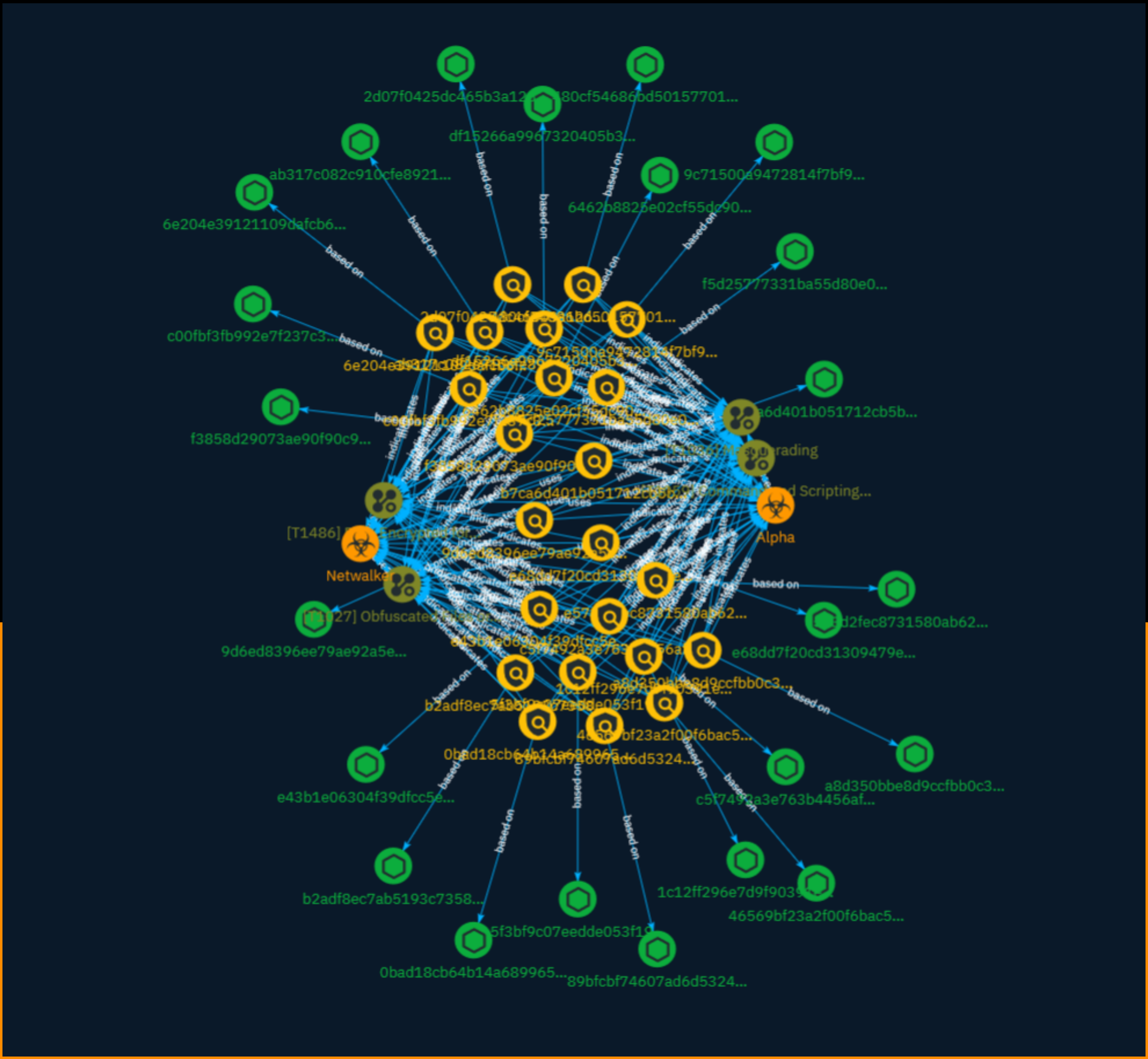

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Alpha ransomware first appeared in February 2023 and has strong similarities to the now-defunct NetWalker ransomware. Analysis shows code overlap between Alpha and NetWalker payloads. Both use a PowerShell-based loader and have similar execution flows, process/service killing logic, and configuration details. After initially maintaining a low profile, Alpha recently began scaling up attacks and launching a data leak site.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name

f5d25777331ba55d80e064dea72240c1524ffcd3870555a8c34ff5377def3729

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f5d25777331ba55d80e064dea72240c1524ffcd3870555a8c34ff5377def3729']

Name

f3858d29073ae90f90c9bb284913752533fe1a6437edd6536e4b1775fc8f6db4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f3858d29073ae90f90c9bb284913752533fe1a6437edd6536e4b1775fc8f6db4']

Name

e68dd7f20cd31309479ece3f1c8578c9f93c0a7154dcf21abce30e75b25da96b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e68dd7f20cd31309479ece3f1c8578c9f93c0a7154dcf21abce30e75b25da96b']

Name

e573d2fec8731580ab620430f55081ceb7153d0344f2094e28785950fb17f499

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e573d2fec8731580ab620430f55081ceb7153d0344f2094e28785950fb17f499']

Name

e43b1e06304f39dfcc5e59cf42f7a17f3818439f435ceba9445c56fe607d59ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e43b1e06304f39dfcc5e59cf42f7a17f3818439f435ceba9445c56fe607d59ea']

Name

df15266a9967320405b3771d0b7353dc5a4fb1cbf935010bc3c8c0e2fe17fb94

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df15266a9967320405b3771d0b7353dc5a4fb1cbf935010bc3c8c0e2fe17fb94']

Name

c5f7492a3e763b4456afbb181248fdb8e652575cea286db7861e97ffcd1b72e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c5f7492a3e763b4456afbb181248fdb8e652575cea286db7861e97ffcd1b72e4']

Name

c00fbf3fb992e7f237c396d69081246570cbd60d6c7a2262c01ae4d8e6f17ddd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c00fbf3fb992e7f237c396d69081246570cbd60d6c7a2262c01ae4d8e6f17ddd']

Name

b7ca6d401b051712cb5b1a388a2135921a4420db8fe41842d51d2ec27380b479

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b7ca6d401b051712cb5b1a388a2135921a4420db8fe41842d51d2ec27380b479']

Name

b2adf8ec7ab5193c7358f6acb30b003493466daee33ea416e3f703e744f73b7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b2adf8ec7ab5193c7358f6acb30b003493466daee33ea416e3f703e744f73b7d']

Name

ab317c082c910cfe89214b31a0933eaab6c766158984f7aafb9943aef7ec6cbb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'ab317c082c910cfe89214b31a0933eaab6c766158984f7aafb9943aef7ec6cbb']

Name

a8d350bbe8d9ccfbb0c3e9c2dd9251c957d18ce13ae405ceb2f2d087c115db15

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a8d350bbe8d9ccfbb0c3e9c2dd9251c957d18ce13ae405ceb2f2d087c115db15']

Name

9d6ed8396ee79ae92a5e6cef718add321226def3461711cf585e0fd302c961ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9d6ed8396ee79ae92a5e6cef718add321226def3461711cf585e0fd302c961ae']

Name

9c71500a9472814f7bf97a462fe9822cf93dc41e2e34cc068734586d5e5146ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9c71500a9472814f7bf97a462fe9822cf93dc41e2e34cc068734586d5e5146ef']

Name

89bfcbf74607ad6d532495de081a1353fc3cf4cd4a00df7b1ba06c10c2de3972

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'89bfcbf74607ad6d532495de081a1353fc3cf4cd4a00df7b1ba06c10c2de3972']

Name

6e204e39121109dafcb618b33191f8e977a433470a0c43af7f39724395f1343e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e204e39121109dafcb618b33191f8e977a433470a0c43af7f39724395f1343e']

Name

5f3bf9c07eedde053f19ce134caa7587f8fb6c466e33256e1253f3a9450b7110

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f3bf9c07eedde053f19ce134caa7587f8fb6c466e33256e1253f3a9450b7110']

Name

6462b8825e02cf55dc905dd42f0b4777dfd5aa4ff777e3e8fe71d57b7d9934e7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6462b8825e02cf55dc905dd42f0b4777dfd5aa4ff777e3e8fe71d57b7d9934e7']

Name

480cf54686bd50157701d93cc729ecf70c14cd1acd2cb622b38fc25e23dfbc26

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'480cf54686bd50157701d93cc729ecf70c14cd1acd2cb622b38fc25e23dfbc26']

Name

46569bf23a2f00f6bac5de6101b8f771feb972d104633f84e13d9bc98b844520

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'46569bf23a2f00f6bac5de6101b8f771feb972d104633f84e13d9bc98b844520']

Name

2d07f0425dc465b3a1267a672c1293f9a3d0cd23106b7be490807fea490978ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d07f0425dc465b3a1267a672c1293f9a3d0cd23106b7be490807fea490978ea']

Name

1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d']

Name

0bad18cb64b14a689965540126e0adbc952f090f1fb7b6447fe897a073860cdb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0bad18cb64b14a689965540126e0adbc952f090f1fb7b6447fe897a073860cdb']

Malware

Name
Alpha
Name
Netwalker
Description
[Netwalker](https://attack.mitre.org/software/S0457) is fileless ransomware written in PowerShell and executed directly in memory.(Citation: TrendMicro Netwalker May 2020)

Attack-Pattern

Name
Data Encrypted for Impact

ID
T1486

Description
Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal

Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

StixFile

Value
f5d25777331ba55d80e064dea72240c1524ffcd3870555a8c34ff5377def3729
e68dd7f20cd31309479ece3f1c8578c9f93c0a7154dcf21abce30e75b25da96b
f3858d29073ae90f90c9bb284913752533fe1a6437edd6536e4b1775fc8f6db4
e573d2fec8731580ab620430f55081ceb7153d0344f2094e28785950fb17f499
e43b1e06304f39dfcc5e59cf42f7a17f3818439f435ceba9445c56fe607d59ea
df15266a9967320405b3771d0b7353dc5a4fb1cbf935010bc3c8c0e2fe17fb94
c5f7492a3e763b4456afbb181248fdb8e652575cea286db7861e97ffcd1b72e4
c00fbf3fb992e7f237c396d69081246570cbd60d6c7a2262c01ae4d8e6f17ddd
b7ca6d401b051712cb5b1a388a2135921a4420db8fe41842d51d2ec27380b479
b2adf8ec7ab5193c7358f6acb30b003493466daee33ea416e3f703e744f73b7d
ab317c082c910cfe89214b31a0933eaab6c766158984f7aafb9943aef7ec6cbb
a8d350bbe8d9ccfbb0c3e9c2dd9251c957d18ce13ae405ceb2f2d087c115db15
9d6ed8396ee79ae92a5e6cef718add321226def3461711cf585e0fd302c961ae

9c71500a9472814f7bf97a462fe9822cf93dc41e2e34cc068734586d5e5146ef
89bfcbf74607ad6d532495de081a1353fc3cf4cd4a00df7b1ba06c10c2de3972
6e204e39121109dafcb618b33191f8e977a433470a0c43af7f39724395f1343e
6462b8825e02cf55dc905dd42f0b4777dfd5aa4ff777e3e8fe71d57b7d9934e7
5f3bf9c07eedde053f19ce134caa7587f8fb6c466e33256e1253f3a9450b7110
480cf54686bd50157701d93cc729ecf70c14cd1acd2cb622b38fc25e23dfbc26
46569bf23a2f00f6bac5de6101b8f771feb972d104633f84e13d9bc98b844520
1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d
2d07f0425dc465b3a1267a672c1293f9a3d0cd23106b7be490807fea490978ea
0bad18cb64b14a689965540126e0adbc952f090f1fb7b6447fe897a073860cdb

External References

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/alpha-netwalker-ransomware
- https://otx.alienvault.com/pulse/65cf7368d63e3fb9b3d302d9