Jan 22 2024

NETMANAGEIT

Intelligence Report

An update on Chaes malware Infostealer

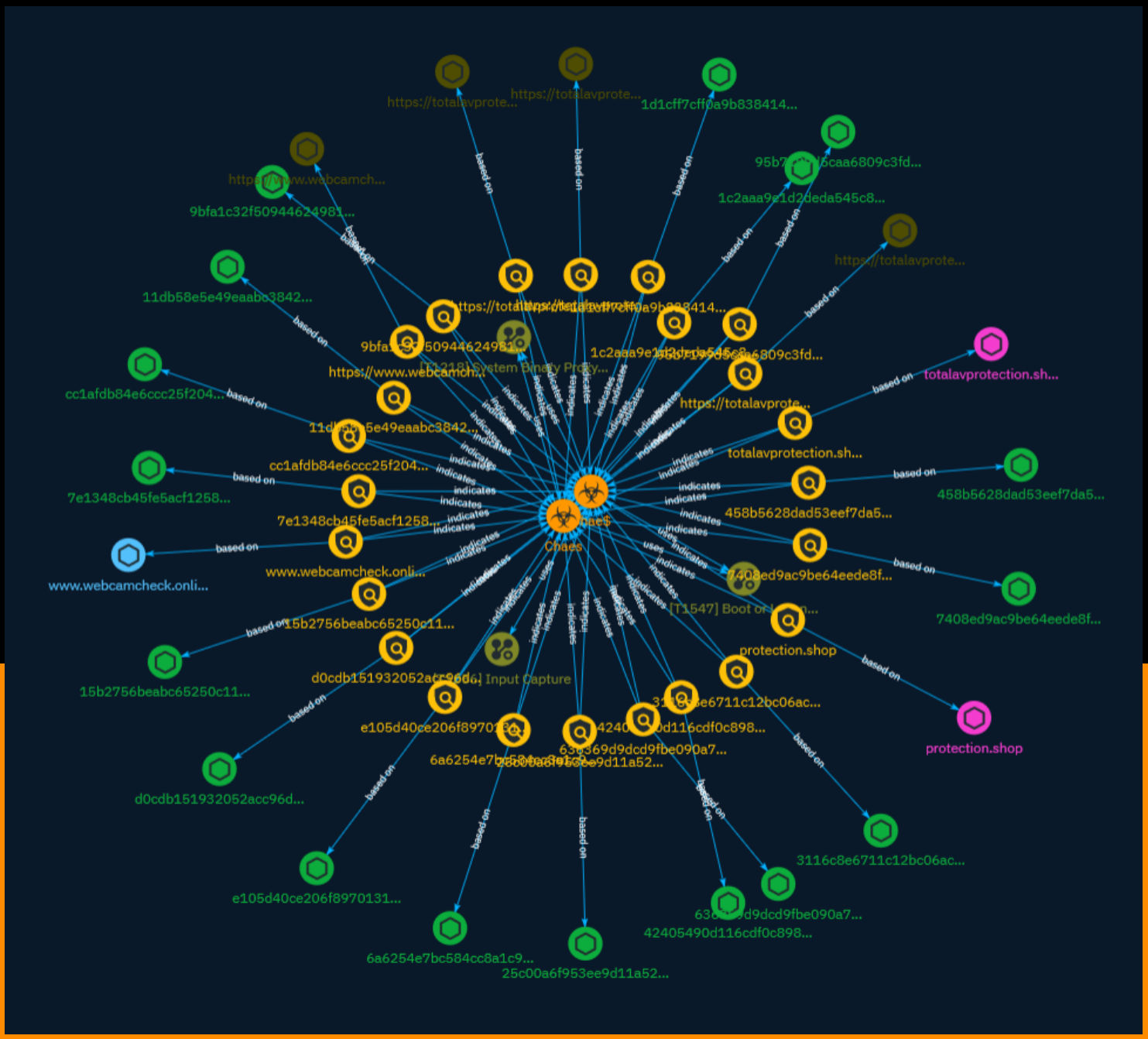

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An analysis of Chae$ 4.1, an update to the Chaes Infostealer malware.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
Name
Input Capture
ID
T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Indicator

Name
7e1348cb45fe5acf125895b1c3cb869c18a571a48f83ec188594a91a4b5d03c0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7e1348cb45fe5acf125895b1c3cb869c18a571a48f83ec188594a91a4b5d03c0']
Name
42405490d116cdf0c898b7b7f2e355084338b53505ac1ac7102f1a3f48139360
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '42405490d116cdf0c898b7b7f2e355084338b53505ac1ac7102f1a3f48139360']
Name

cc1afdb84e6ccc25f2041fb047caa5d577078441b206b72167020bba0b6156dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cc1afdb84e6ccc25f2041fb047caa5d577078441b206b72167020bba0b6156dd']

Name

https://totalavprotection.shop

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9 months ago', 'timestamp': 1681761099, 'iso': '2023-04-17T15:51:39-04:00'} - **IPQS: Domain:** totalavprotection.shop - **IPQS: IP Address:** 89.116.224.31

Pattern Type

stix

Pattern

[url:value = 'https://totalavprotection.shop']

Name

25c00a6f953ee9d11a52b1f8aa0535af426cdb79e8210b6d45bf6ae16b888967

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '25c00a6f953ee9d11a52b1f8aa0535af426cdb79e8210b6d45bf6ae16b888967']
Name
1c2aaa9e1d2deda545c8f246b933fa91b13ce682dcacbe7cd1611497ea84baf0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1c2aaa9e1d2deda545c8f246b933fa91b13ce682dcacbe7cd1611497ea84baf0']
Name
95b7199d5caa6809c3fd70fdca3e9eab3c3d4b4d86a56f88e2092fe0f86f0ccb
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '95b7199d5caa6809c3fd70fdca3e9eab3c3d4b4d86a56f88e2092fe0f86f0ccb']

Name

636369d9dcd9fbe090a7e7ac300faf1721da7559841546031543dd5f85e0a50e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '636369d9dcd9fbe090a7e7ac300faf1721da7559841546031543dd5f85e0a50e']

Name

https://totalavprotection.shop/abrirProcesso.php?email=

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9 months ago', 'timestamp': 1681761099, 'iso': '2023-04-17T15:51:39-04:00'} - **IPQS: Domain:** totalavprotection.shop - **IPQS: IP Address:** 89.116.224.31

Pattern Type

stix

Pattern

[url:value = 'https://totalavprotection.shop/abrirProcesso.php?email=']

Name

6a6254e7bc584cc8a1c9c590bf9288ed94cd6f95494cf39232693fe5101d5b07

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a6254e7bc584cc8a1c9c590bf9288ed94cd6f95494cf39232693fe5101d5b07']

Name

d0cdb151932052acc96db00f7442edbbefedfc7aea748e51d0240e1436a4b733

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0cdb151932052acc96db00f7442edbbefedfc7aea748e51d0240e1436a4b733']

Name

https://totalavprotection.shop/

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9 months ago', 'timestamp': 1681761099, 'iso': '2023-04-17T15:51:39-04:00'} - **IPQS: Domain:** totalavprotection.shop - **IPQS: IP Address:** 89.116.224.31

Pattern Type

stix

Pattern

[url:value = 'https://totalavprotection.shop/']

Name

totalavprotection.shop

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9 months ago', 'timestamp': 1681761099, 'iso': '2023-04-17T15:51:39-04:00'} - **IPQS: Domain:** totalavprotection.shop - **IPQS: IP Address:** 89.116.224.31

Pattern Type

stix

Pattern

[domain-name:value = 'totalavprotection.shop']

Name

https://www.webcamcheck.online/

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7 months ago', 'timestamp': 1687796449, 'iso': '2023-06-26T12:20:49-04:00'} - **IPQS: Domain:** webcamcheck.online - **IPQS: IP Address:** 89.116.224.31

Pattern Type

stix

Pattern

[url:value = 'https://www.webcamcheck.online/']

Name

protection.shop

Description

- **Unsafe:** False - **Server:** ope - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7 years ago', 'timestamp': 1474902011, 'iso': '2016-09-26T11:00:11-04:00'} - **IPQS: Domain:** protection.shop - **IPQS: IP Address:** 3.33.130.190

Pattern Type

stix

Pattern

[domain-name:value = 'protection.shop']

Name

11db58e5e49eaabc38425f8e3f3f989537aee2895b7dd01c765fce7a778116e2

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '11db58e5e49eaabc38425f8e3f3f989537aee2895b7dd01c765fce7a778116e2']
Name
1d1cff7cff0a9b838414143191562b27f97a61478d346c782932cb5a47d953c8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1d1cff7cff0a9b838414143191562b27f97a61478d346c782932cb5a47d953c8']
Name
7408ed9ac9be64eede8fd21ded0e546192766984bf2d90384c1c0259ef3d2481
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7408ed9ac9be64eede8fd21ded0e546192766984bf2d90384c1c0259ef3d2481']

Name

15b2756beabc65250c119921ede423eed0b83d1f436b9fabf3c07d71b2497590

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15b2756beabc65250c119921ede423eed0b83d1f436b9fabf3c07d71b2497590']

Name

458b5628dad53eef7da5339191796a636b6bd2433101e3cb6cbc43e7566cbdfe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '458b5628dad53eef7da5339191796a636b6bd2433101e3cb6cbc43e7566cbdfe']

Name

e105d40ce206f89701310c476c7a38c82ea69e1a41b32f23fe6babf7397d6c7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e105d40ce206f89701310c476c7a38c82ea69e1a41b32f23fe6babf7397d6c7b']

Name

9bfa1c32f509446249818ab67e27a4584c944a664fae20f85377ac59caa4bf5f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9bfa1c32f509446249818ab67e27a4584c944a664fae20f85377ac59caa4bf5f']

Name

3116c8e6711c12bc06ac26e0dbcc6870bd8207477363e49532a72ceb8d4f2543

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3116c8e6711c12bc06ac26e0dbcc6870bd8207477363e49532a72ceb8d4f2543']

Name

www.webcamcheck.online

Pattern Type

stix
Pattern
[hostname:value = 'www.webcamcheck.online']

Malware

Name
Chae$
Name
Chaes
Description
[Chaes](https://attack.mitre.org/software/S0631) is a multistage information stealer written in several programming languages that collects login credentials, credit card numbers, and other financial information. [Chaes](https://attack.mitre.org/software/S0631) was first observed in 2020, and appears to primarily target victims in Brazil as well as other e-commerce customers in Latin America.(Citation: Cybereason Chaes Nov 2020)

Domain-Name

Value
totalavprotection.shop
protection.shop

StixFile

Value
7e1348cb45fe5acf125895b1c3cb869c18a571a48f83ec188594a91a4b5d03c0
42405490d116cdf0c898b7b7f2e355084338b53505ac1ac7102f1a3f48139360
636369d9dcd9fbe090a7e7ac300faf1721da7559841546031543dd5f85e0a50e
15b2756beabc65250c119921ede423eed0b83d1f436b9fabf3c07d71b2497590
cc1afdb84e6ccc25f2041fb047caa5d577078441b206b72167020bba0b6156dd
1c2aaa9e1d2deda545c8f246b933fa91b13ce682dcacbe7cd1611497ea84baf0
3116c8e6711c12bc06ac26e0dbcc6870bd8207477363e49532a72ceb8d4f2543
95b7199d5caa6809c3fd70fdca3e9eab3c3d4b4d86a56f88e2092fe0f86f0ccb
25c00a6f953ee9d11a52b1f8aa0535af426cdb79e8210b6d45bf6ae16b888967
6a6254e7bc584cc8a1c9c590bf9288ed94cd6f95494cf39232693fe5101d5b07
458b5628dad53eef7da5339191796a636b6bd2433101e3cb6cbc43e7566cbdfe
d0cdb151932052acc96db00f7442edbbefedfc7aea748e51d0240e1436a4b733
7408ed9ac9be64eede8fd21ded0e546192766984bf2d90384c1c0259ef3d2481

1d1cff7cff0a9b838414143191562b27f97a61478d346c782932cb5a47d953c8

9bfa1c32f509446249818ab67e27a4584c944a664fae20f85377ac59caa4bf5f

11db58e5e49eaabc38425f8e3f3f989537aee2895b7dd01c765fce7a778116e2

e105d40ce206f89701310c476c7a38c82ea69e1a41b32f23fe6babf7397d6c7b

Hostname

Value
www.webcamcheck.online

Url

Value
https://totalavprotection.shop
https://totalavprotection.shop/
https://totalavprotection.shop/abrirProcesso.php?email=
https://www.webcamcheck.online/

External References

- https://otx.alienvault.com/pulse/65aa793c91404980f88ffc61
- https://www.morphisec.com/hubfs/Chae$_Chronicles_Chaes4.1.pdf
- https://blog.morphisec.com/chaes-chronicles