Sep 05 2023

NETMANAGEIT

Intelligence Report

Chae$ 4: New Chaes Malware Variant Targeting Financial and Logistics Customers

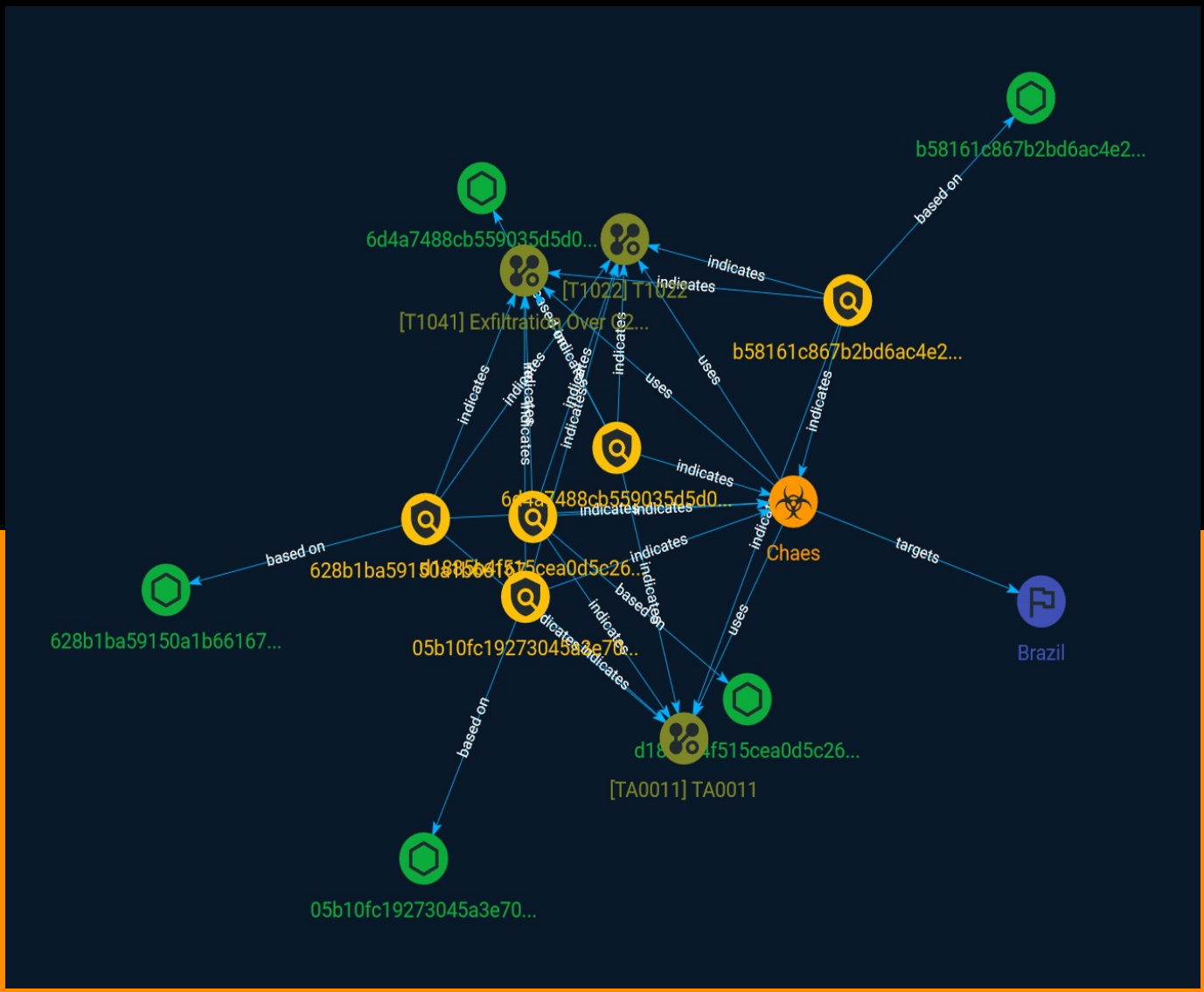

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Morphisec identified an alarming trend where numerous clients, primarily within the logistics and financial sectors, were under the onslaught of a new and advanced variant of Chaes malware. The sophistication of the threat was observed to increase over multiple iterations from April to June 2023.

Confidence

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

15 / 100

Indicator

Name
b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a']
Name
d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6']
Name

6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c']

Name

05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd']

Name

628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57']
```

Malware

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)

Attack-Pattern

Name
T1022
ID
T1022
Name
TA0011
ID
TA0011
Name
Exfiltration Over C2 Channel
ID
T1041
Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Country

Name
Brazil

StixFile

Value
b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a
05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd
6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c
d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6
628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57

External References

- https://otx.alienvault.com/pulse/64f77c1ea1ca19fd5bc11e14
- https://blog.morphisec.com/chaes4-new-chaes-malware-variant-targeting-financial-and-logistics-customers