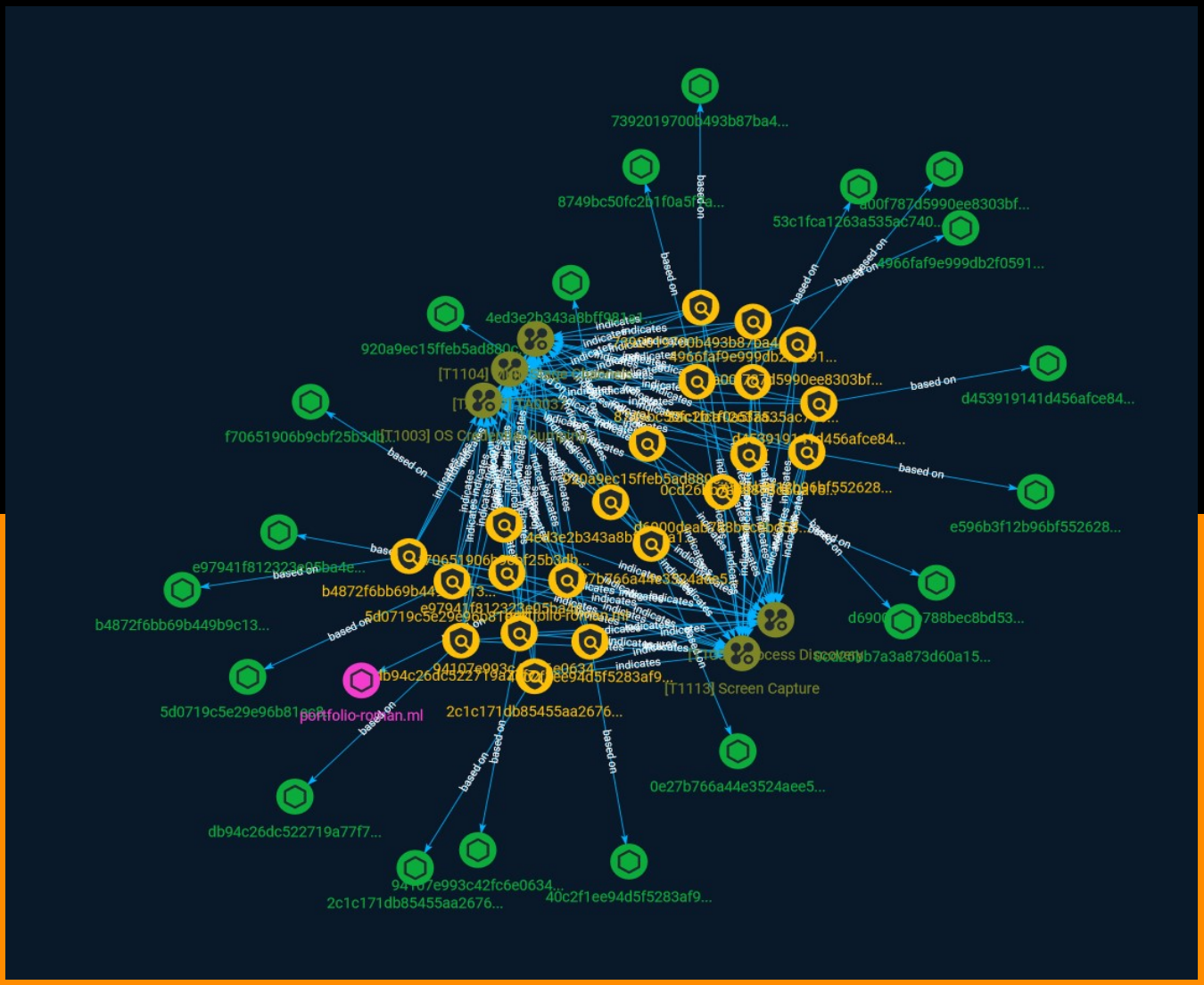
NETMANAGEIT

# Intelligence Report

# SapphireStealer: Open-source information stealer enables credential and data theft



# Table of contents

## Overview



## Entities



## Observables



## External References

# Overview

## Description

Information stealers have become increasingly popular across the threat landscape over the past several years. While these threats have been around for a very long time, Cisco Talos has recently observed an increase in the emergence of new stealers being offered for sale or rent on various underground forums and marketplaces. Stealers are often seen as an attractive option for financially motivated threat actors, as they provide a simple means to compromise and distribute sensitive information and account-related details to adversaries.

## Confidence

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

15 / 100

# Indicator

| Name |
| --- |
| d6900deab788bec8bd5343a64423ebea6b323603c10b3cca03c08ebe0774bb5a |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'd6900deab788bec8bd5343a64423ebea6b323603c10b3cca03c08ebe0774bb5a'] |
| **Name** |
| b4872f6bb69b449b9c13ac694a8e54a22dce012cba48a5e8bce0607690d08254 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'b4872f6bb69b449b9c13ac694a8e54a22dce012cba48a5e8bce0607690d08254'] |
| **Name** |

4966faf9e999db2f059162a8d1e17c44d8f77697ec268ff55f2f4efdb96797a8

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '4966faf9e999db2f059162a8d1e17c44d8f77697ec268ff55f2f4efdb96797a8']

**Name**

e596b3f12b96bf5526285df19dc9674aaaafeb8375eeac4face8eb4285c63e3b

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'e596b3f12b96bf5526285df19dc9674aaaafeb8375eeac4face8eb4285c63e3b']

**Name**

94107e993c42fc6e0634be29191410b50c076e129260d23351baa9f6dc7c883e

**Description**

Win32:PWSX-gen\ [Trj]

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '94107e993c42fc6e0634be29191410b50c076e129260d23351baa9f6dc7c883e']

**Name**

0cd26bb7a3a873d60a150ad2e776a37de07f1317639d75f3a0df4939982ac0bf

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '0cd26bb7a3a873d60a150ad2e776a37de07f1317639d75f3a0df4939982ac0bf']

**Name**

4ed3e2b343a8bff981a139af0f871bbe76e3e93ac0d6ad4c16acbb1ec0a74bff

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '4ed3e2b343a8bff981a139af0f871bbe76e3e93ac0d6ad4c16acbb1ec0a74bff']

**Name**

920a9ec15ffeb5ad880c9368238c3b1ab189d429bd3ef99ac9ab16615eeacedf

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '920a9ec15ffeb5ad880c9368238c3b1ab189d429bd3ef99ac9ab16615eeacedf']

**Name**

53c1fca1263a535ac740916a24b28807246a204c6fa22b7374dc17fe913375d4

**Description**

Win64:PWSX-gen\ [Trj]

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '53c1fca1263a535ac740916a24b28807246a204c6fa22b7374dc17fe913375d4']

**Name**

2c1c171db85455aa2676e02693c8a9b7d62055fee843a17097dba29915637acf

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '2c1c171db85455aa2676e02693c8a9b7d62055fee843a17097dba29915637acf']

**Name**

8749bc50fc2b1f0a5f7a1c3c1a3132c45c30ba7dc7a849523bb42cf617fc4a65

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '8749bc50fc2b1f0a5f7a1c3c1a3132c45c30ba7dc7a849523bb42cf617fc4a65']

**Name**

40c2f1ee94d5f5283af9b6f7c660aba3921138fc1fcc66dab2489fc9e421589a

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '40c2f1ee94d5f5283af9b6f7c660aba3921138fc1fcc66dab2489fc9e421589a']

**Name**

0e27b766a44e3524aee546e3279bcbca22255fa7171b8c6013efa7708e37c633

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '0e27b766a44e3524aee546e3279bcbca22255fa7171b8c6013efa7708e37c633']

**Name**

d453919141d456afce8476b4af9082b4af8d4c644e8468aa62259d704c22e074

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'd453919141d456afce8476b4af9082b4af8d4c644e8468aa62259d704c22e074']

**Name**

e97941f812323e05ba4e83b138e8bb794b88efcd56980d07313b5acc965b2661

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'e97941f812323e05ba4e83b138e8bb794b88efcd56980d07313b5acc965b2661']

**Name**

7392019700b493b87ba4a53cc25e7cc639ce58da390b1b3780eaf8ee0889dcf3

**Description**

ConventionEngine_Term_Desktop

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7392019700b493b87ba4a53cc25e7cc639ce58da390b1b3780eaf8ee0889dcf3']

**Name**

portfolio-roman.ml

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'portfolio-roman.ml']

**Name**

f70651906b9cbf25b3db874e969af7a14caac21bf1db328e4664db54566a15b0

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'f70651906b9cbf25b3db874e969af7a14caac21bf1db328e4664db54566a15b0']

**Name**

a00f787d5990ee8303bfd5cdc8eda650317434482e6f82cc53dfcf565006896d

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'a00f787d5990ee8303bfd5cdc8eda650317434482e6f82cc53dfcf565006896d']

**Name**

db94c26dc522719a77f7585bff8884400f389dab012a880734bd9dbc3e52d93c

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'db94c26dc522719a77f7585bff8884400f389dab012a880734bd9dbc3e52d93c']

**Name**

5d0719c5e29e96b81ec8198e8bba5d531a2dc433c3107be6263dee33b54d578a

| Pattern Type |
| --- |
| stix |

| Pattern |
| --- |
| [file:hashes.'SHA-256' = '5d0719c5e29e96b81ec8198e8bba5d531a2dc433c3107be6263dee33b54d578a'] |

# Attack-Pattern

| Name |
| --- |
| TA0037 |
| **ID** |
| TA0037 |
| **Name** |
| Process Discovery |
| **ID** |
| T1057 |
| **Description** |
| Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is |

accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

**Name**

OS Credential Dumping

**ID**

T1003

**Description**

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

**Name**

Multi-Stage Channels

**ID**

T1104

**Description**

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point

to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

**Name**

Screen Capture

**ID**

T1113

**Description**

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

# Domain-Name

| Value |
| --- |
| portfolio-roman.ml |

# StixFile

| Value |
| --- |
| d453919141d456afce8476b4af9082b4af8d4c644e8468aa62259d704c22e074 |
| 2c1c171db85455aa2676e02693c8a9b7d62055fee843a17097dba29915637acf |
| e97941f812323e05ba4e83b138e8bb794b88efcd56980d07313b5acc965b2661 |
| 0e27b766a44e3524aee546e3279bcbca22255fa7171b8c6013efa7708e37c633 |
| 53c1fca1263a535ac740916a24b28807246a204c6fa22b7374dc17fe913375d4 |
| 4966faf9e999db2f059162a8d1e17c44d8f77697ec268ff55f2f4efdb96797a8 |
| 94107e993c42fc6e0634be29191410b50c076e129260d23351baa9f6dc7c883e |
| 7392019700b493b87ba4a53cc25e7cc639ce58da390b1b3780eaf8ee0889dcf3 |
| 40c2f1ee94d5f5283af9b6f7c660aba3921138fc1fcc66dab2489fc9e421589a |
| db94c26dc522719a77f7585bff8884400f389dab012a880734bd9dbc3e52d93c |
| 4ed3e2b343a8bff981a139af0f871bbe76e3e93ac0d6ad4c16acbb1ec0a74bff |
| 5d0719c5e29e96b81ec8198e8bba5d531a2dc433c3107be6263dee33b54d578a |
| 920a9ec15ffeb5ad880c9368238c3b1ab189d429bd3ef99ac9ab16615eeacedf |

e596b3f12b96bf5526285df19dc9674aaaafeb8375eeac4face8eb4285c63e3b

8749bc50fc2b1f0a5f7a1c3c1a3132c45c30ba7dc7a849523bb42cf617fc4a65

a00f787d5990ee8303bfd5cdc8eda650317434482e6f82cc53dfcf565006896d

d6900deab788bec8bd5343a64423ebea6b323603c10b3cca03c08ebe0774bb5a

b4872f6bb69b449b9c13ac694a8e54a22dce012cba48a5e8bce0607690d08254

f70651906b9cbf25b3db874e969af7a14caac21bf1db328e4664db54566a15b0

0cd26bb7a3a873d60a150ad2e776a37de07f1317639d75f3a0df4939982ac0bf

# External References

- https://otx.alienvault.com/pulse/64f0afd80b14f8aad315c223
- https://blog.talosintelligence.com/sapphirestealer-goes-open-source/
- https://github.com/Cisco-Talos/IOCs/blob/main/2023/08/sapphirestealer-goes-open-source.txt