Nov 26 2023

NETMANAGEIT

Intelligence Report

MetaStealer - Redline's Doppelgänger

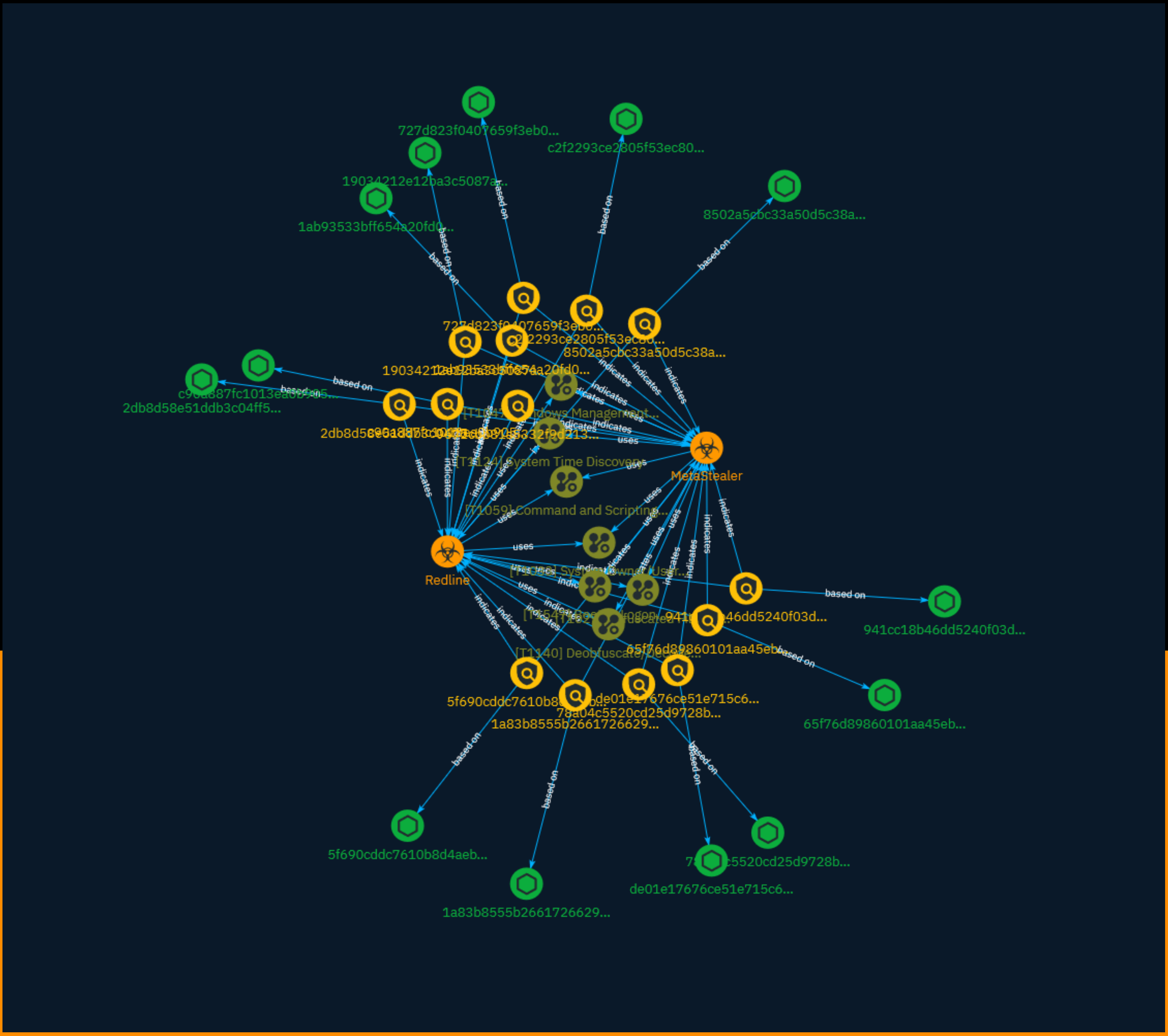

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Indicator 12
- Malware 18

Observables

- StixFile 19

External References

● External References 20

Overview

Description

MetaStealer made its debut on Russian hacking forums on March 7, 2022. The stealer is said to incorporate the functionality, code, and panel of Redline Stealer. The developer claims to have improved the stub of the payload. It is priced at $150 per month, mirroring the price of Redline Stealer.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Windows Management Instrumentation
ID
T1047
Description
Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015) An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)
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

System Time Discovery

ID

T1124

Description

An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network.(Citation: MSDN System Time)(Citation: Technet Windows Time Service) System time information may be gathered in a number of ways, such as with [Net](https://attack.mitre.org/software/S0039) on Windows by performing `net time \\hostname` to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using `w32tm /tz`.(Citation: Technet Windows Time Service) On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show clock detail` can be used to see the current time configuration.(Citation: show_clock_detail_cisco_cmd) This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)(Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://attack.mitre.org/techniques/T1614)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

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

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

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Indicator

Name

9672cbb81a5332f9d2135377e197c3ed854f0c96

Pattern Type

yara

Pattern

import "pe" rule MetaStealer { meta: author = "RussianPanda" decription = "Detects MetaStealer" date = "11/16/2023" strings: $s1 = "FileScannerRule" $s2 = "MSObject" $s3 = "MSValue" $s4 = "GetBrowsers" $s5 = "Biohazard" condition: 4 of ($s*) and pe.imports("mscoree.dll") }

Name

941cc18b46dd5240f03d438ff17f19d946a8037fbe765ae4bc35ffea280df976

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '941cc18b46dd5240f03d438ff17f19d946a8037fbe765ae4bc35ffea280df976']

Name

65f76d89860101aa45eb3913044bd6c36c0639829f863a85f79b3294c1f4d7bb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'65f76d89860101aa45eb3913044bd6c36c0639829f863a85f79b3294c1f4d7bb']

Name

c90a887fc1013ea0b90522fa1f146b0b33d116763afb69ef260eb51b93cf8f46

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c90a887fc1013ea0b90522fa1f146b0b33d116763afb69ef260eb51b93cf8f46']

Name

5f690cddc7610b8d4aeb85b82979f326373674f9f4032ee214a65758f4e479be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f690cddc7610b8d4aeb85b82979f326373674f9f4032ee214a65758f4e479be']

Name

19034212e12ba3c5087a21641121a70f9067a5621e5d03761e91aca63d20d993

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19034212e12ba3c5087a21641121a70f9067a5621e5d03761e91aca63d20d993']

Name

8502a5cbc33a50d5c38aaa5d82cd2dbf69deb80d4da6c73b2eee7a8cb26c2f71

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8502a5cbc33a50d5c38aaa5d82cd2dbf69deb80d4da6c73b2eee7a8cb26c2f71']

Name

78a04c5520cd25d9728becca1f032348b2432a3a803c6fed8b68a8ed8cca426f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'78a04c5520cd25d9728becca1f032348b2432a3a803c6fed8b68a8ed8cca426f']

Name

1ab93533bff654a20fd069d327ac4185620beb243135640c2213571c8902e325

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1ab93533bff654a20fd069d327ac4185620beb243135640c2213571c8902e325']

Name

de01e17676ce51e715c6fc116440c405ca4950392946a3aa3e19e28346239abb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'de01e17676ce51e715c6fc116440c405ca4950392946a3aa3e19e28346239abb']

Name

2db8d58e51ddb3c04ff552ecc015de1297dc03a17ec7c2aed079ed476691c4aa

Description

Win.Trojan.Redline-9938775-1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'2db8d58e51ddb3c04ff552ecc015de1297dc03a17ec7c2aed079ed476691c4aa']

Name

c2f2293ce2805f53ec80a5f9477dbb44af1bd403132450f8ea421a742e948494

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c2f2293ce2805f53ec80a5f9477dbb44af1bd403132450f8ea421a742e948494']

Name

1a83b8555b2661726629b797758861727300d2ce95fe20279dec098011de1fff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1a83b8555b2661726629b797758861727300d2ce95fe20279dec098011de1fff']

Name

727d823f0407659f3eb0c017e25023784a249d76c9e95a288b923abb4b2fe0dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'727d823f0407659f3eb0c017e25023784a249d76c9e95a288b923abb4b2fe0dd']

Malware

Name
MetaStealer

Name
Redline

StixFile

Value
5f690cddc7610b8d4aeb85b82979f326373674f9f4032ee214a65758f4e479be
78a04c5520cd25d9728becca1f032348b2432a3a803c6fed8b68a8ed8cca426f
1a83b8555b2661726629b797758861727300d2ce95fe20279dec098011de1fff
c2f2293ce2805f53ec80a5f9477dbb44af1bd403132450f8ea421a742e948494
8502a5cbc33a50d5c38aaa5d82cd2dbf69deb80d4da6c73b2eee7a8cb26c2f71
1ab93533bff654a20fd069d327ac4185620beb243135640c2213571c8902e325
19034212e12ba3c5087a21641121a70f9067a5621e5d03761e91aca63d20d993
2db8d58e51ddb3c04ff552ecc015de1297dc03a17ec7c2aed079ed476691c4aa
941cc18b46dd5240f03d438ff17f19d946a8037fbe765ae4bc35ffea280df976
65f76d89860101aa45eb3913044bd6c36c0639829f863a85f79b3294c1f4d7bb
de01e17676ce51e715c6fc116440c405ca4950392946a3aa3e19e28346239abb
727d823f0407659f3eb0c017e25023784a249d76c9e95a288b923abb4b2fe0dd
c90a887fc1013ea0b90522fa1f146b0b33d116763afb69ef260eb51b93cf8f46

External References

- https://otx.alienvault.com/pulse/656081565b87ed05ff3c7d55
- https://russianpanda.com/2023/11/20/MetaStealer-Redline%27s-Doppelganger/