Jun 14 2023

NETMANAGEIT

Intelligence Report

Pirated Windows builds with crypto stealer that penetrates EFI partition

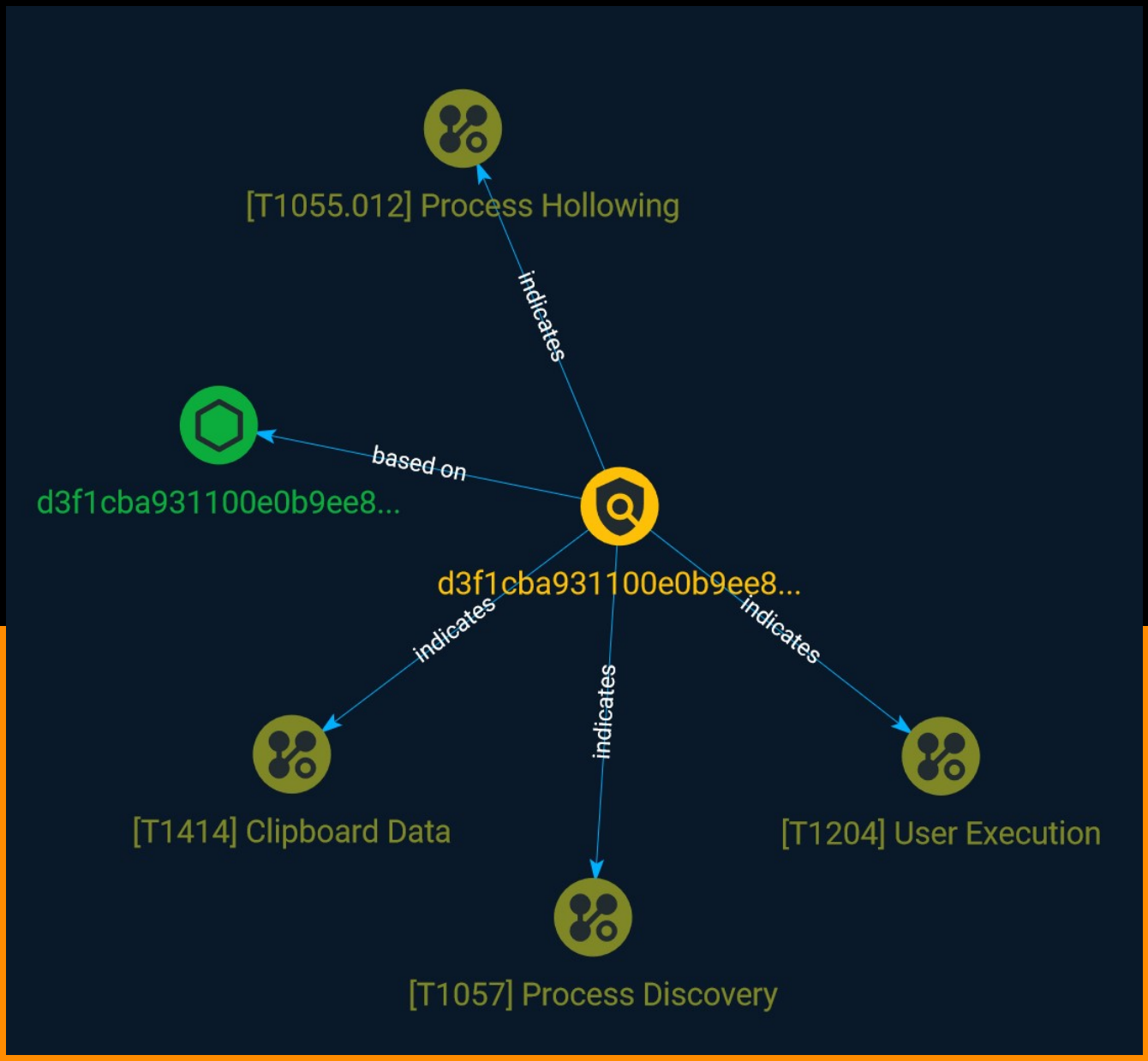

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Doctor Web has discovered a malicious clipper program in a number of unofficial Windows 10 builds that cybercriminals have been distributing via a torrent tracker. Dubbed Trojan.Clipper.231, this trojan app substitutes crypto wallet addresses in the clipboard with addresses provided by attackers. As of this moment, malicious actors have managed to steal cryptocurrency in an amount equivalent to about $19,000 US.

Confidence

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

15 / 100

Attack-Pattern

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

Clipboard Data

ID

T1414

Description

Adversaries may abuse clipboard manager APIs to obtain sensitive information copied to the device clipboard. For example, passwords being copied and pasted from a password manager application could be captured by a malicious application installed on the device. (Citation: Fahl-Clipboard) On Android, applications can use the `ClipboardManager.OnPrimaryClipChangedListener()` API to register as a listener and monitor the clipboard for changes. However, starting in Android 10, this can only be used if the application is in the foreground, or is set as the device's default input method editor (IME).(Citation: Github Capture Clipboard 2019)(Citation: Android 10 Privacy Changes) On iOS, this can be accomplished by accessing the `UIPasteboard.general.string` field. However, starting in iOS 14, upon accessing the clipboard, the user will be shown a system notification if the accessed text originated in a different application. For example, if the user copies the text of an iMessage from the Messages application, the notification will read "application_name has pasted from Messages" when the text was pasted in a different application.(Citation: UIPPasteboard)

Name

Process Hollowing

ID

T1055.012

Description

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process. Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as `CreateProcess`, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as `ZwUnmapViewOfSection` or `NtUnmapViewOfSection` before being written to, realigned to

the injected code, and resumed via `VirtualAllocEx`, `WriteProcessMemory`, `SetThreadContext`, then `ResumeThread` respectively.(Citation: Leitch Hollowing)(Citation: Elastic Process Injection July 2017) This is very similar to [Thread Local Storage](https://attack.mitre.org/techniques/T1055/005) but creates a new process rather than targeting an existing process. This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process hollowing may also evade detection from security products since the execution is masked under a legitimate process.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Indicator

Name
d3f1cba931100e0b9ee8cc92f0ef0fd1bdcbb7b53b06b6a7f8501608d4cd54f5
Description
#LowFiCreateRemoteThread SHA256 of a3adba5c8d41b4c5f63e209317740daf6330dfc6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd3f1cba931100e0b9ee8cc92f0ef0fd1bdcbb7b53b06b6a7f8501608d4cd54f5']

StixFile

Value
d3f1cba931100e0b9ee8cc92f0ef0fd1bdcbb7b53b06b6a7f8501608d4cd54f5

External References

- https://otx.alienvault.com/pulse/648a0d612bc78c61f9b3baa4
- https://github.com/DoctorWebLtd/malware-iocs/blob/master/Trojan.Clipper.231/README.adoc
- https://news.drweb.com/show/?i=14712&lng=en