Mphasis
The Next Applied

Bandit Stealer Advisory

Severity: High

Date: xx xx 2023

Description

A newly emerged information-stealing malware named Bandit Stealer is gaining traction as it targets numerous browsers and cryptocurrency wallets while evading detection. Currently, there is a growing interest and promotional activity within the malware community to increase awareness and use of the malware. While the focus of targeting is limited to the Windows platform as of this writing, it has the potential to expand to other platforms as Bandit Stealer was developed using the Go programming language, possibly allowing cross-platform compatibility.

Name	**Bandit information stealer**
Threat Type	Information stealer
Detection Names	Avast (Win64:Malware-gen), Combo Cleaner (Trojan.GenericKD.50686234), ESET-NOD32 (A Variant Of Generik.HAYHJZO), Kaspersky (Trojan-PSW.Win64.Coins.no), Microsoft (Trojan:Win32/Casdet!rfn)
Symptoms	Trojans are designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are clearly visible on an infected machine.
Distribution methods	Infected email attachments, malicious online advertisements, social engineering, software 'cracks', fake (malicious) installers.
Damage	Stolen passwords and banking information, identity theft, the victim's computer added to a botnet.

Escalation

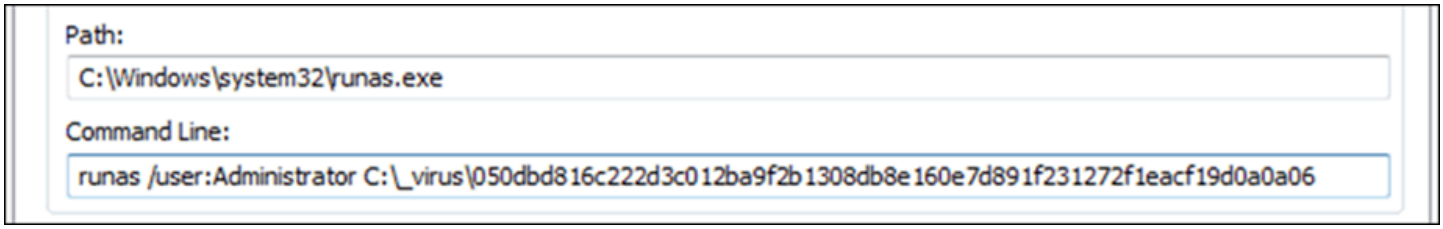
The malware is currently focused on targeting Windows by using a legitimate command-line tool called runas.exe that allows users to run programs as another user with different permissions, the goal is to escalate privileges and execute itself with administrative access, thereby effectively bypassing security measures to harvest wide swathes of data.

The malware uses runas.exe command where it can run programs as an administrator or any other user account with appropriate privileges.

The malware downloads the content of the Pastebin link hxxps[:]//pastebin[.]com/raw/3fS0MSjN and saves it to a file named “blacklist.txt” in the AppData folder. This list contains hardware IDs, IP addresses, MAC addresses, usernames, hostnames, and process names typically used to detect whether the malware is running in a sandbox or testing environment.

Microsoft has implemented various measures to prevent the unauthorized use of the runas.exe function, including the implementation of security restrictions. This limits the privileges and actions that can be performed using runas.exe. Microsoft has also strengthened user access controls, ensuring that only authorized individuals with the necessary permissions can execute privileged operations, but the malware is trying to run itself as an administrator using the runas.exe with administrator rights which requires a password.

Runas.exe executes the binary itself as an administrator.



Evasion

Bandit Stealer checks for the following to determine if it's running in a sandbox environment and alters its behavior accordingly to avoid detection or analysis:

- container
- jail
- KVM
- QEMU
- sandbox
- Virtual Machine
- VirtualBox
- VMware
- Xen

Affected Versions

Windows Server 2003, Windows Vista, Windows XP, Windows HPC Server 2008 R2, Windows Server 2008, Windows 7, Windows Server 2003 R2, Windows Server 2000, Windows Server 2012, Windows Server 2003 with SP1, Windows 8

Recommendation

- Initiate a full Scan on the malware infected systems.
- Block the below IOCs.

Recommendation

SHA 256 Hash Values

- 050dbd816c222d3c012ba9f2b1308db8e160e7d891f231272f1eacf19d0a0a06
- 782ec01fa989886571a72b77dc662640a9df7a5fbdc8a863a256820c7faf8e3b
- 050dbd816c222d3c012ba9f2b1308db8e160e7d891f231272f1eacf19d0a0a06
- c4776e3d50d53cb0cad3f6b4e685bbb8e0b6efe0b3e761db2b64a4232f21996e
- ecc311fcf3884ead2e5614baedfe412e6d797d044df005dff2fae86f9c80d63a
- 191ce844c2381564bfc289789e364d1330ddc05bd97c9a8c13139e5f240c2527
- 70a577151ba8b726808ad4bda7a4caf31eb2f4ab7e70045247b145d5feda5440
- da3c3df0712fffd047e3b7326852d96def7584f5070c3c7803e47593899b4d0a
- 1cd60650fa3e560d8f7c80d4d059e669e64486bd3ca6daed52d8fdce14d0455b
- d934a1bde6bb75936d223426e64497e92526b8bc75a4f8a59a87f1d25ed1a0d2
- 106a184d39858af7b0264f26fe0fc657a84ccfd87df3a4f55e7060b3c3c1d92d
- 064338e9b9075b48890d9db21fec27a3c7ce10e80abc954ba3777b660eceeacb
- 64fe4148c74e0603c198459fd46b3ed3bece8066498f91782b6d98d5c3fc2d01
- 69088f95523d2199e5a277a67a2f70a42e653bf58fb0f3790aa1436bd101eeb1
- 191ce844c2381564bfc289789e364d1330ddc05bd97c9a8c13139e5f240c2527
- ecc311fcf3884ead2e5614baedfe412e6d797d044df005dff2fae86f9c80d63a

URLs

- https[:]//api[.]telegram[.]org/bot5943289606:AAGNEW2B3zDRhGDxY7E1tg7_m2BJcVkUJDw/sendDocument
  URL where the malware sends data
- https[:]//pastebin[.]com/raw/3fS0MSjN
  URL where the malware downloads the blacklist.txt file

Reference Links

New Info Stealer Bandit Stealer Targets Browsers, Wallets (trendmicro.com)

New Stealthy Bandit Stealer Targeting Web Browsers and Cryptocurrency Wallets (thehackernews.com)