Agniane Stealer | ThreatLabz

By Mallikarjun Piddannavar

Published: 2023-08-22 · Archived: 2026-04-05 16:29:25 UTC

Stealer Capabilities

Agniane Stealer possesses several form-grabbing capabilities. Let’s dive into those.

Sidesteps dependencies

Upon execution, Agniane Stealer, with a compact sample size, adeptly operates on both 32 and 64-bit systems, sidestepping any reliance on pre-existing dependencies.

Intriguingly, it dynamically retrieves a set of 5 DLLs from its C&C servers, leveraging legitimate third-party DLLs to enhance its functionalities and capabilities. It employs the following:

- SQLite.dll
- SQLite.EF6.dll
- SQLite.Linq.dll
- SQLite.Interop.dll(x86 & x64bit)

Steals from the following areas:

AREAS	DETAILS
Telegram and Steam Sessions	• Steals user tokens for logged-in Discord and Steam sessions, and OpenVPN profiles; sends data to threat actors. • Tries to search Telegram software under the “\\AppData\\Roaming\\Telegram” directory. If found, Agniane Stealer steals Telegram Sessions and archives it. • Tries to locate the Telegram process. If found, the malware kills the process and grabs all the Telegram files except emojis and user_data. Then, Agniane Stealer archives all remaining directories.
Browser cookies	Agniane Stealer targets login data, history, and web data from the following browsers: • OperaGX • Chrome • Opera • FireFox • Vivaldi • Brave • Edge • Yandex • Chromium
Domains	Agniane Stealer tries to harvest login credentials and cookies from following domains: • VK.com • facebook.com • instagram.com • mail.ru If any passwords are found in the domains listed above, then Agniane Stealer places them into the Important Detects.txt file and archives them.
SSH File Transfer Protocol	Agniane Stealer pilfers WinSCP to collect Hostname, username, and password from all sessions by traversing through Software\\Martin Prikryl\\WinSCP 2\\Sessions registry entry.
Filezilla FTP Software	Agniane Stealer reads FileZilla\\recentservers.xml and searches for the tag. If available, then Agniane Stealer grabs Hostname, username, and password. If the XML path was not found, then Agniane Stealer logs that it was unable to find the FileZilla session.

AREAS	DETAILS
Computer System	Agniane Stealer gets the external IP address of the victim's machine using https://ipwho.is/?output=xml. In addition, Agniane Stealer collects victims Windows version using SELECT * FROM win32_operatingsystem. Then, it obtains the bit version of the machine using Windows Registry and checks the value. If the value matches, then it is x86 but if it doesn't then that indicates a x64bit machine.

Uses WMI to collect

- **Installed Antiviruses:** Collects all installed antivirus software with the WMI query Select * from AntivirusProduct.
- **GPUName:** Using WMI query SELECT * FROM Win32_VideoController and GetEnumerator() method Compares with "VMware SVGA 3D"
- **CPU name:** Using WMI query SELECT * FROM Win32_Processor tries to access the CPU name of the victim's machine.

Captures a screenshot

Agniane Stealer captures a screenshot of the victim's desktop using Bitmap.

Checks RAM

By querying WMI to Select * From Win32_ComputerSystem, Agniane Stealer calculates RAM allocated to the victim's machine.

Exfiltrates data

Agniane Stealer enumerates the users Desktop and the Documents folder for the files with .txt,.doc,.mafile,.rdp, and .db extension. The discovered files are then copied to the previously created subfolder under the %TEMP% location.

Finds installed applications

Agniane Stealer collects all applications installed on the victim's machine by querying the Registry Key SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall. Then, it stores that information in the Installed Apps.txt file, as you can see in the image below.

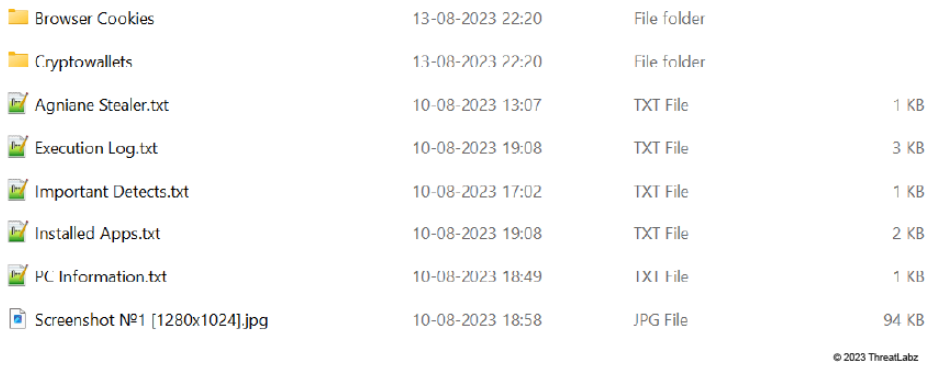

Figure 9: Example information collected by Agniane Stealer

Agniane Stealer keeps a record of its actions in a file named execution log.txt, which documents all the operations executed and associated information.

Exfiltrates crypto data

In addition to form-grabbing, Agniane Stealer also utilizes clipper qualities to exfiltrate cryptocurrency data.

Agniane Stealer is a prolific cryptocurrency data exfiltrator with extensive support for nearly 70+ crypto extensions and 10+ crypto wallets. See the **Crypto Extension & Wallet** table at the bottom of this blog for a complete list.

How it works

Agniane Stealer uploads all the exfiltrated data to:

hxxps[:]//central-cee-doja.ru/TEST.php?ownerid=REPLACEUSER1D&buildid=spriteuser&countp=2&countc=29&username=saturn&country=IN&ipaddr=XX.XX.XX.XX&BSSID=XXXXXX

After uploading the stolen data to a remote server, the Agniane Stealer removes its traces from the victim's system by deleting the sub-folder.

We observed that the latest version of the Agniane Stealer uses ConfuserEx Protector. Also, the recent variant employs more obfuscation techniques when compared to the earlier version, which makes it harder for security modules to detect.

In the images below, Figure 10 is from the earlier version of Agniane Stealer where the code is human-readable, and Figure 11 is from the latest version of Agniane Stealer where the same code is obfuscated through ConfuserEx Protector. The Figure 12 is showing the de-obfuscated code.

Human-readable code

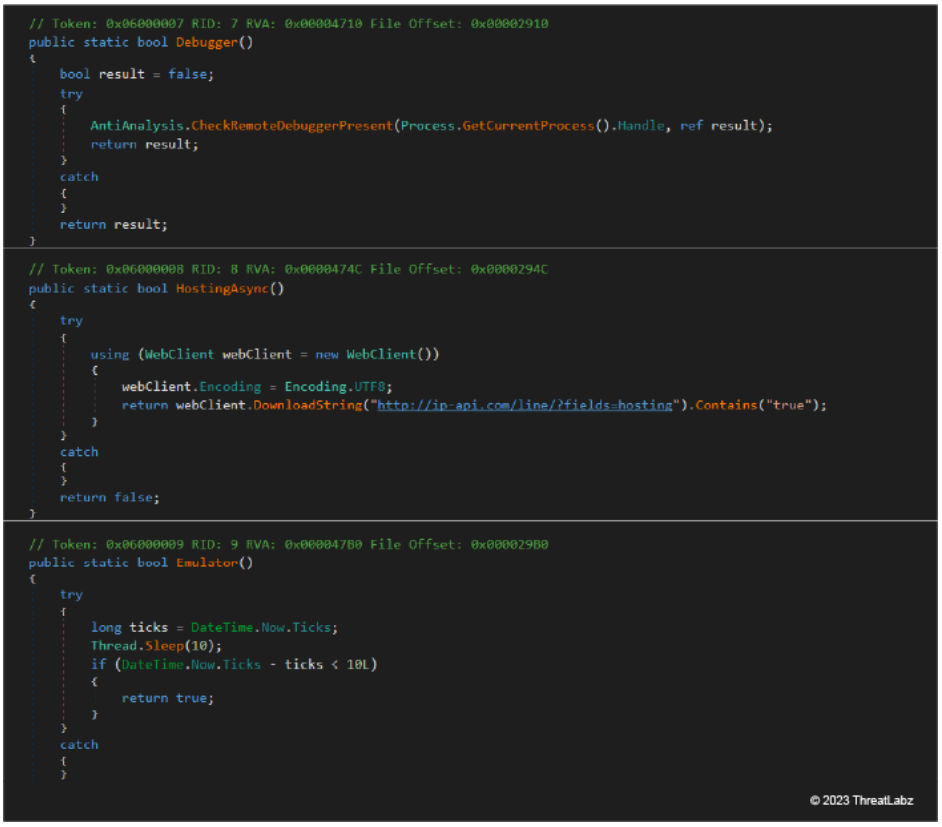

Figure 10: Human-readable Agniane Stealer sample code

Obfuscated code

Figure 11: Obfuscated Agniane Stealer code sample

Deobfuscated code

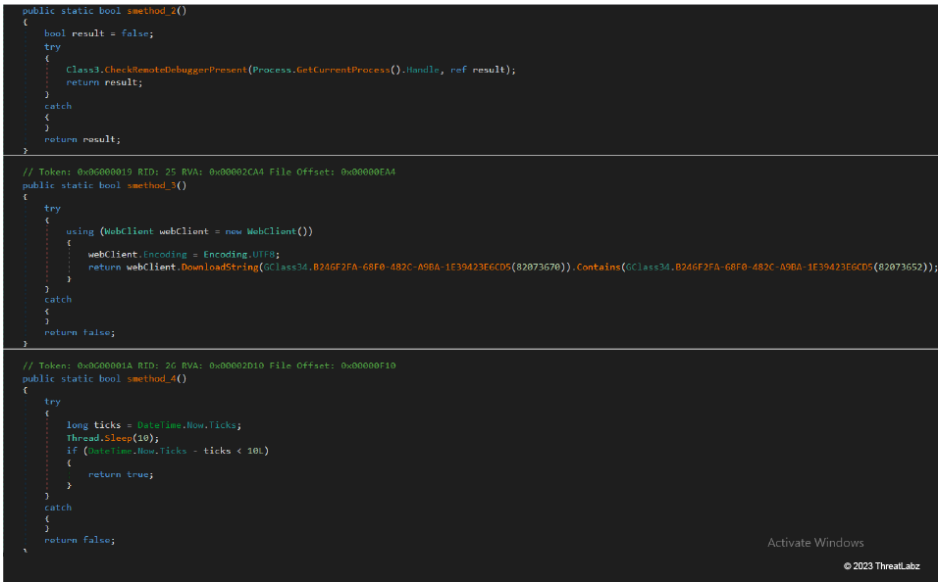

Figure 12: Deobfuscated Agniane Stealer code sample

Explore more Zscaler blogs

Source: https://www.zscaler.com/blogs/security-research/agniane-stealer-dark-webs-crypto-threat