Rising Stealer in Q1 2022: BlackGuard Stealer

medium.com/s2wblog/rising-stealer-in-q1-2022-blackguard-stealer-f516d9f85ee5

S2W May 24, 2022

S2
W

S2W

Apr 1

.

8 min read

Author: Jiho Kim | S2W TALON

> *: 2022.04.01.*

Photo by on

Executive Summary

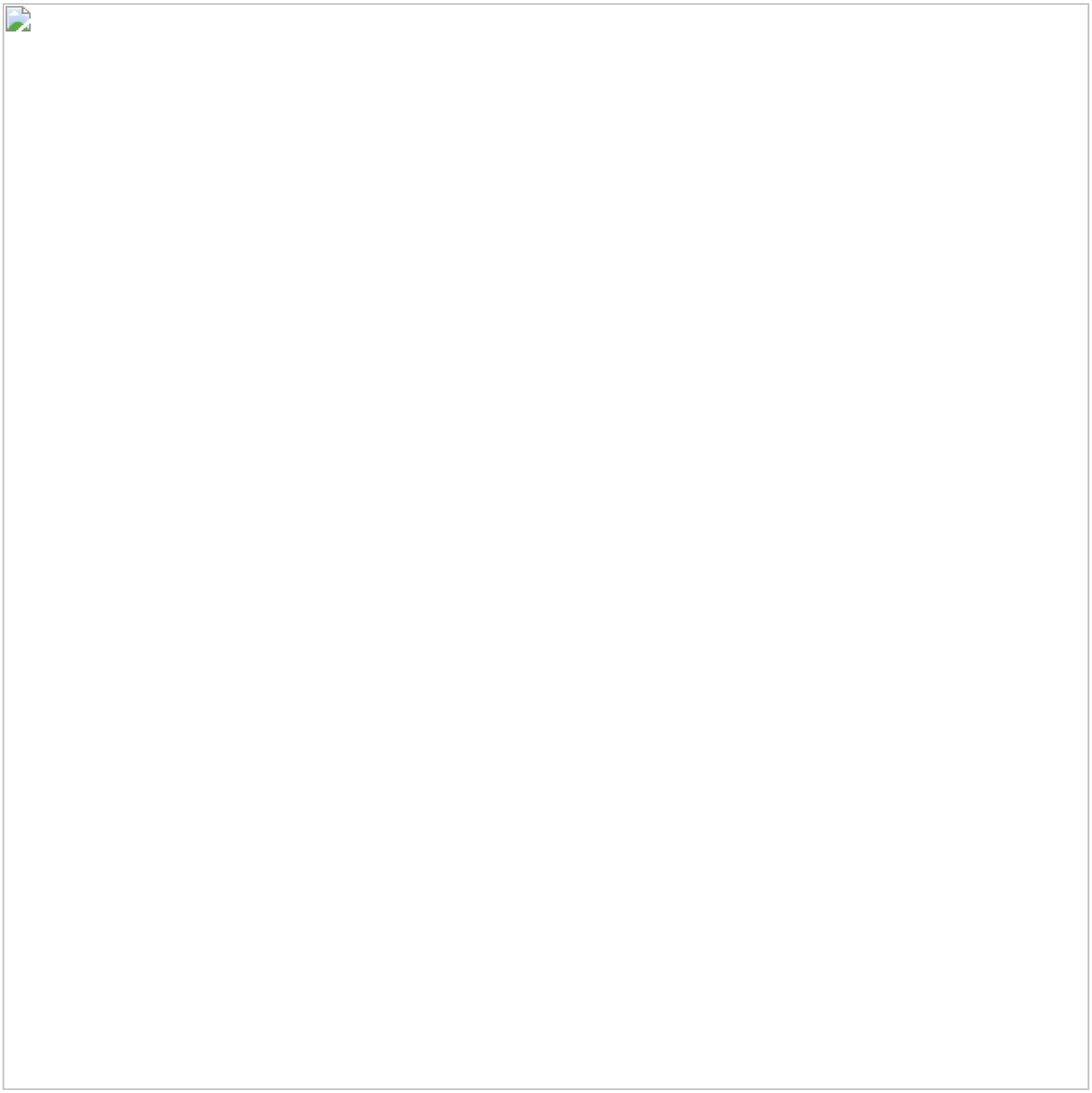
- BlackGuard Stealer, which collects and exfiltrates credentials and device information from infected PC, first appeared when the official seller posted a promotion article on the dark web forum in January 2022
- BlackGuard Stealer collects and exfiltrates not only credentials such as Browser user data, Local files, Crypto wallets, VPN accounts, Steam accounts, Discord tokens, FileZilla data, and Telegram session data, but also device information such as OS version, System information, IPv4, country, and screenshot from infected PC

- The collected information is stored in a temporarily created folder. After collecting information, the folder is compressed to a *.zip file and exfiltrated through Telegram API.

Introduction of BlackGuard Stealer

BlackGuard is one of the info stealers written in C#. It is mostly distributed through malicious software disguised as Windows Update file, Fake MS Office Installer, Computer cleaner software, etc.

Recently, the info stealer abused the description of a YouTube video by attaching the download link that contains the info stealer. In March 2022, a link to download a game hack program was posted in the YouTube video description, but when users downloaded and ran the software, 44Caliber Stealer was executed on the users' PC.

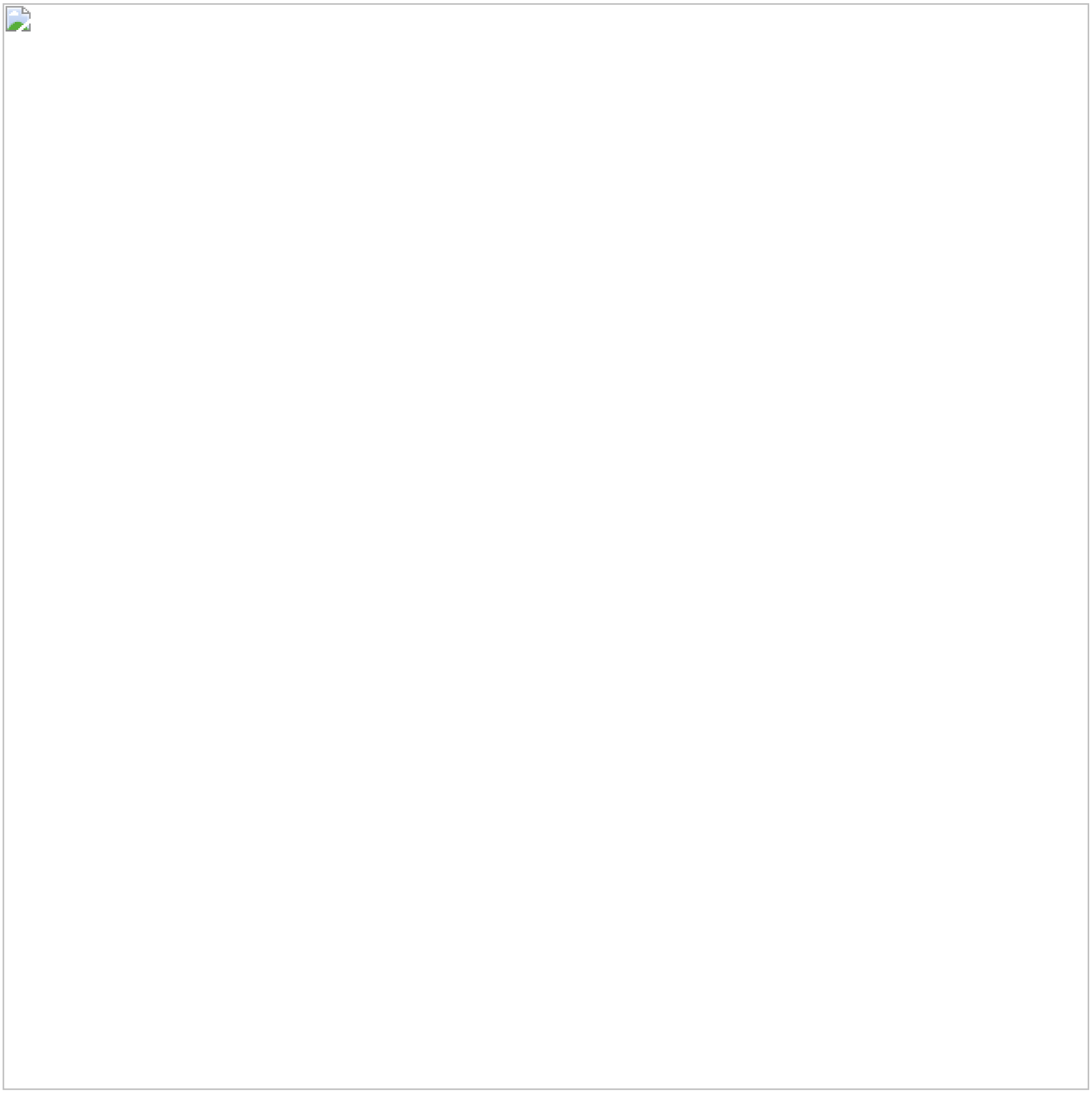


- Reference:
- YouTube link: https[:]//www[.]youtube[.]com/watch?v=YI8rJhQLsfg
- Malware download page: https[:]//anonfiles[.]com/J0b03cKexf

BlackGuard Stealer, which is currently being distributed, is forked from 44Caliber Stealer. Both BlackGuard and 44Caliber use the same method to collect credentials and device information. In addition, they store them in a temporarily created folder and compress them to the *.zip file. But while BlackGuard uses Telegram’s **sendDocument** API, 44Caliber uses Discord Webhook API to exfiltrate.

Timeline of BlackGuard Stealer

Since it first appeared on the dark web forum in January 2022, BlackGuard Stealer has been updated its builder and web panel. In particular, considering that the proportion of samples discovered from March 2022 is increasing, it can be seen that BlackGuard Stealer is currently active.



The most recent major update was on February 9, 2022. At that time, Wallet extensions of Chrome and Edge, Edge Beta were added, and the types of collected information became more diverse.

BlackGuard Stealer on DDW

The user with the nicknames “BlackGUARD07” and “blackteam007” posted a Stealer promotion article in Russian-based forums, XSS and BHF, in January 2022. BlackGuard Stealer has different prices and additional services depending on the period of use.

BlackGuard Stealer’s Pricing Policy

$200 (for a month)

— Build cleaning for an additional payment of $50

$700 (forever)

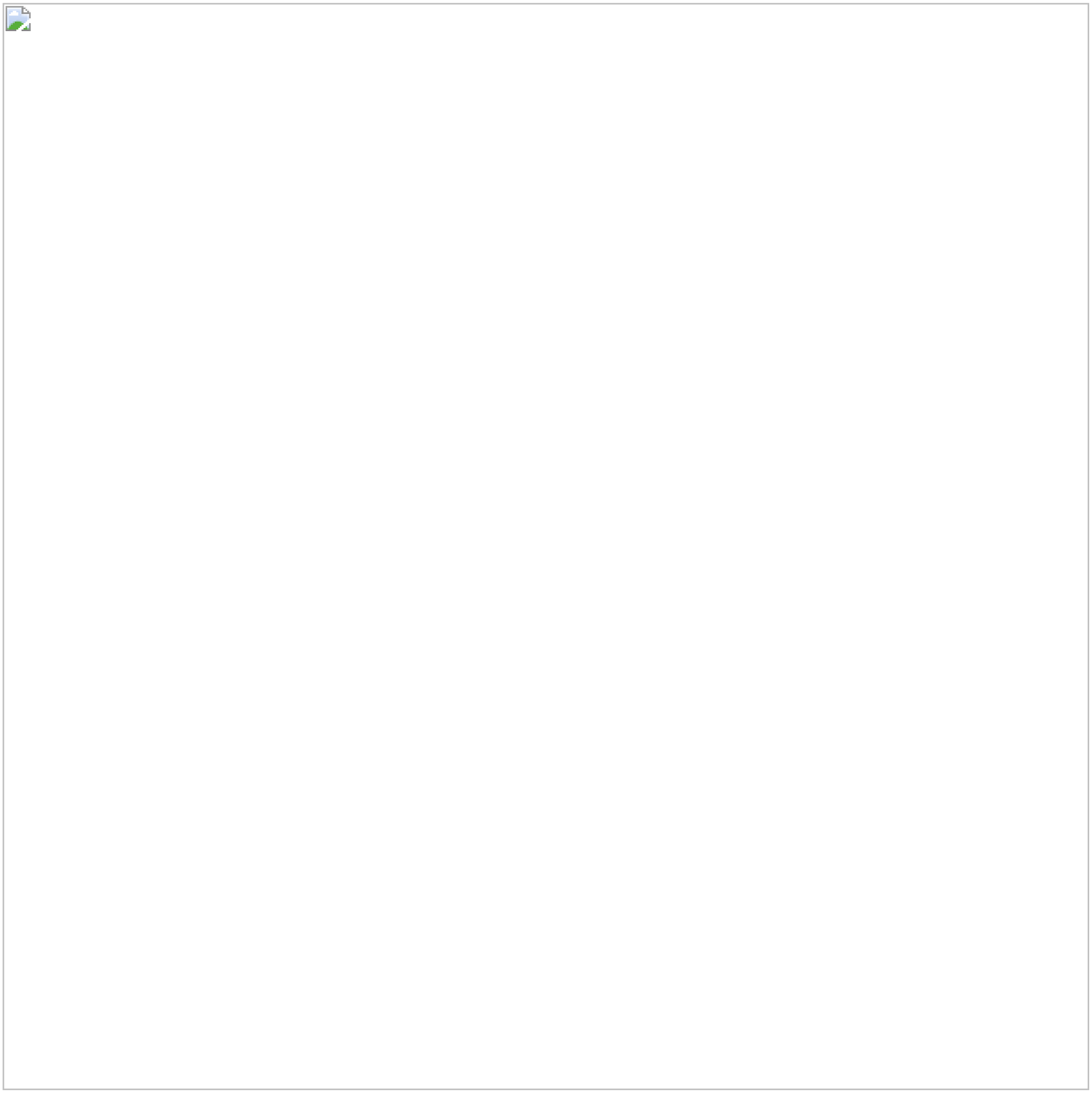
— All updates for free

— Build cleaning for free

The official seller contacts buyers through Telegram Channel and Jabber. Both are only used for sales and inquiries, and announcements and updated information are posted on the forums.

BlackGuard Stealer Official Seller’s Contact

- Telegram: @blackwalter
- Jabber: blackwalter1@01337.io



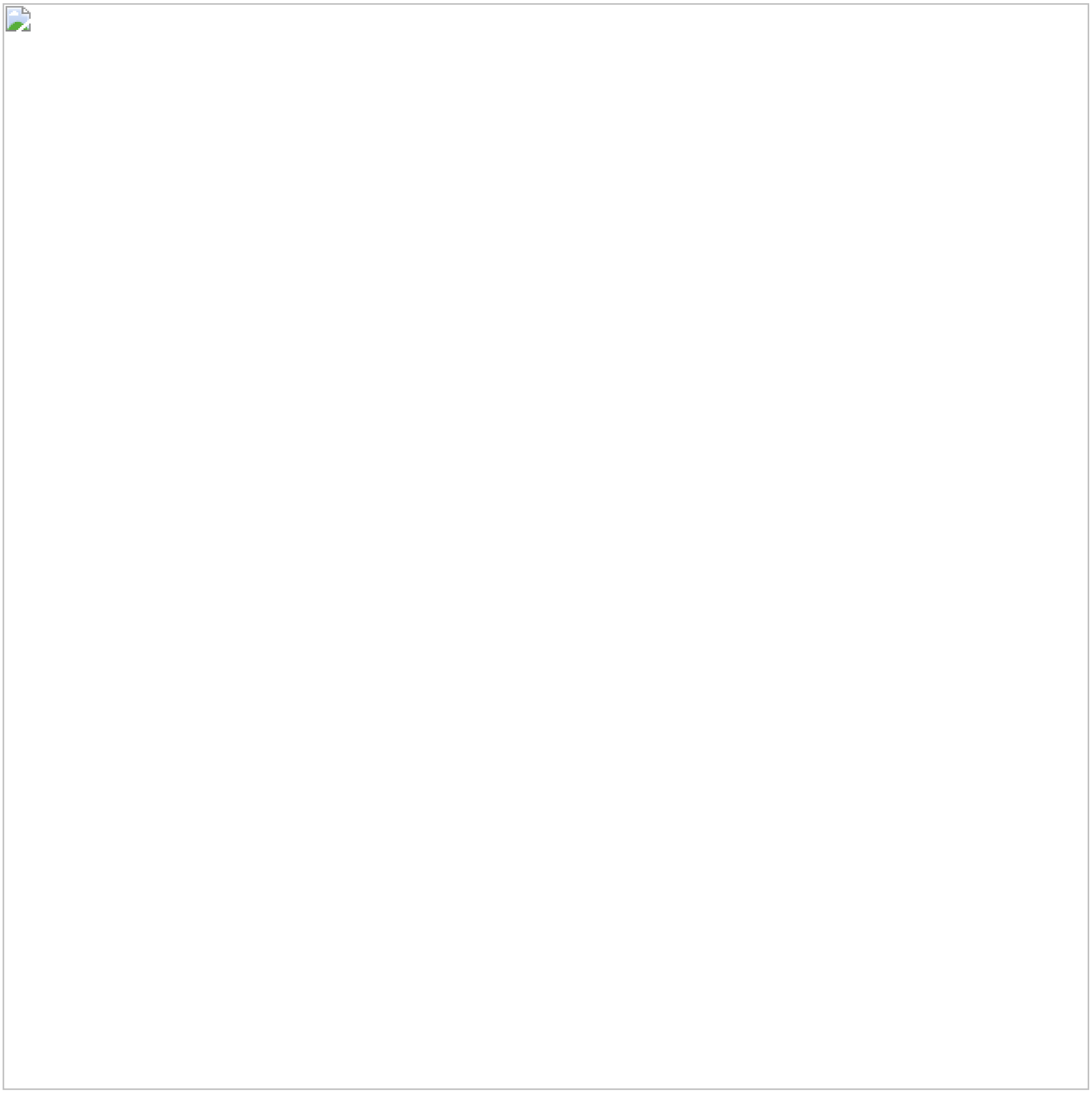
Malware analysis

1. Sample Information

- File Name: Soft.exe
- File Type: PE32 executable .NET assembly
- File Size: 1.18 MB
- Compiled Date: 2055–07–22 09:06:25
- MD5: eb6c563af372d1af92ac2b60438d076d
- SHA256: 67843d45ba538eca29c63c3259d697f7e2ba84a3da941295b9207cdb01c85b71

2. BlackGuard Stealer Execution Flow

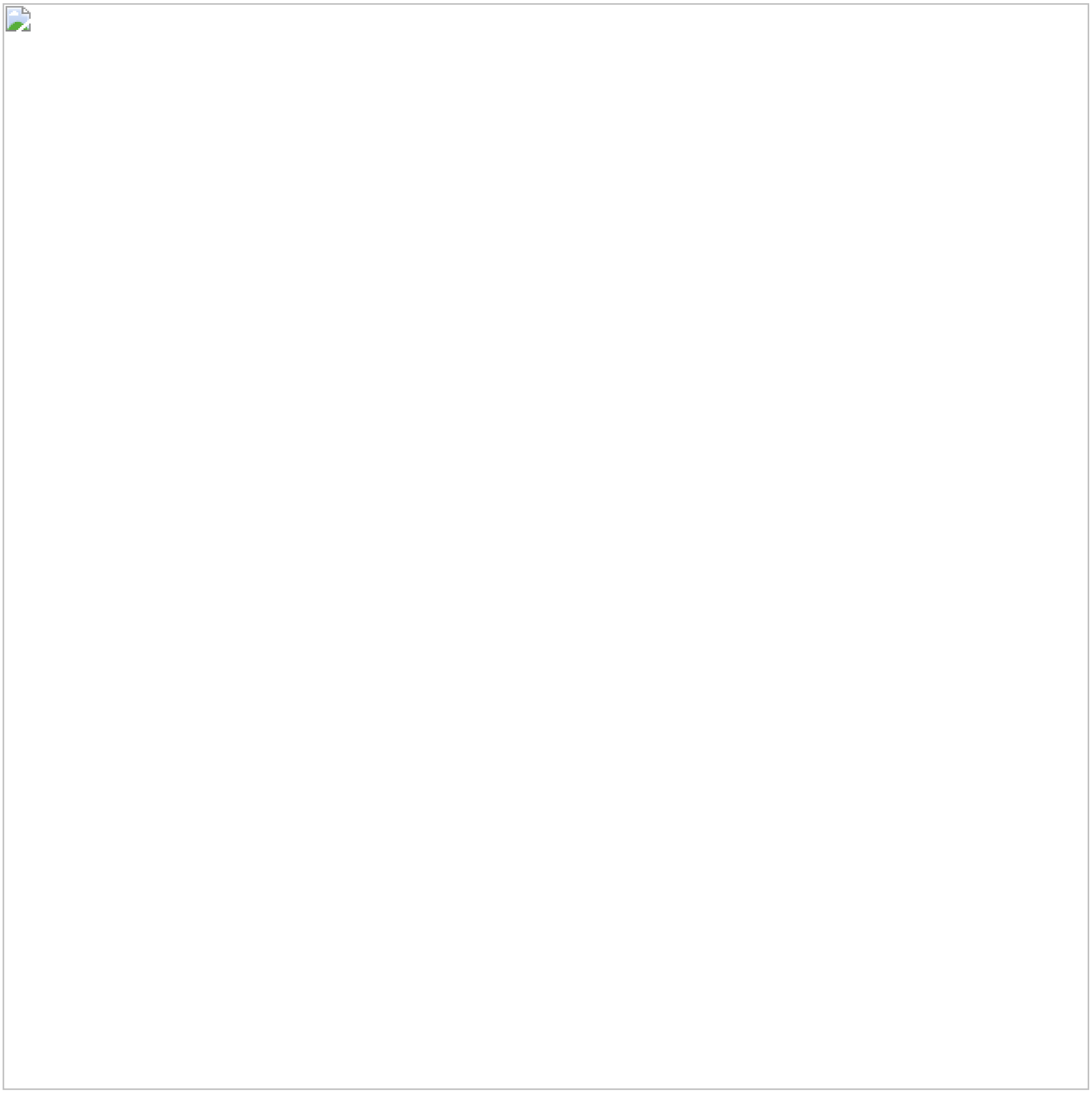
1. When the loader is executed, BlackGuard Stealer is dropped and executed.
2. are decoded and then used for collecting and exfiltrating credentials and device information.
3. Anti Debugging: Checks the existence of DnSpy, a tool used for decompiling .NET assembly, and whether it is currently being debugged.
4. Collects credentials and device information from infected PC and stores them in the folder specified in
5. Compresses to the zip file.
6. Exfiltrates the zip file through Telegram API.



3. Decode Help & Config Data

In the BlackGuard Stealer, the data used for collecting and exfiltrating credentials and device information are hard-coded. **Help Data** is used to collect and includes system directory paths, the **ChikenDir** folder path, and device information. Config data is mainly used to exfiltrate collected information through Telegram API and includes Telegram Bot Token, Chat ID, and keywords for collecting files. Most of the data inside these classes are base64-encoded and gzip-compressed.

(***Help Data** and **Config Data** are described in Appendix.A.)



4. Anti Debugging

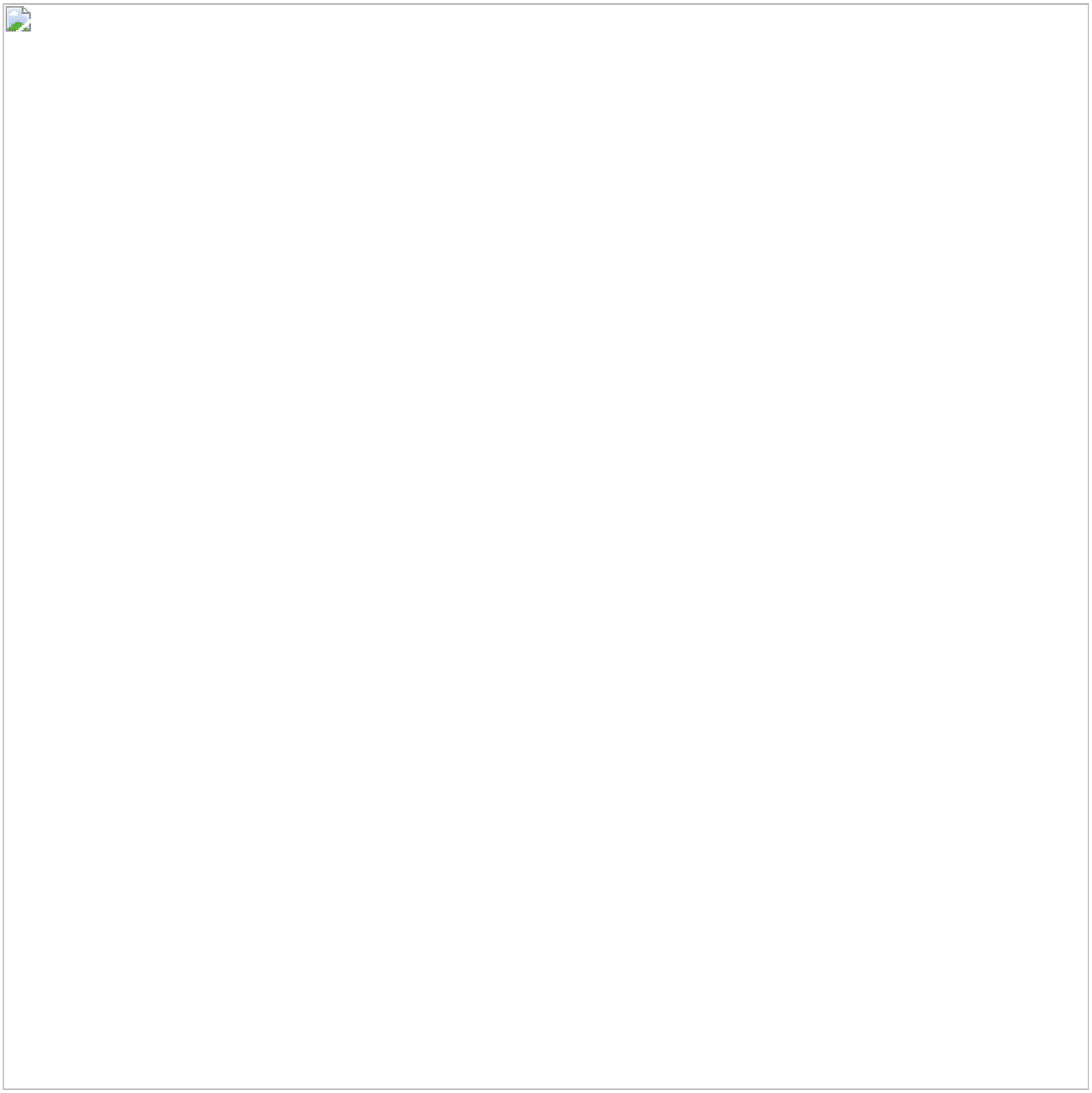
Before BlackGuard collects credentials and device information, it uses Anti Debugging methods. It detects the decompiler by checking if the “dnSpy.xml” file exists, and uses “Sleep()” and “DateTime.Now.Ticks” to determine whether it is being debugged.

5. Collect Credentials and Device Information

BlackGuard Stealer collects Browser user data, Local files, Crypto wallets, VPN, Steam, Discord, FileZilla, Telegram, system information, and screenshot. Every time each piece of information is collected, the number of information is counted and stored separately. The collected data stored in the **ChikenDir** folder is shown in the figure below.

Browsers Folder

In the *Browsers* folder, each browsers' user data is stored. A subfolder is created for each type of browser, and the collected user data is saved as *.txt files in each folder. While Chrome and Edge browsers' user data includes CC, Password, Cookie, History, Downloads, and AutoFill, and Gecko-based browsers additionally collect logins.json, which contains login information, key3.db, and key4.db.



After storing the collected user data in each browser’s folder, BlackGuard checks and transfers whether a specific domain is included among the *.txt files.

[Domain Check List]

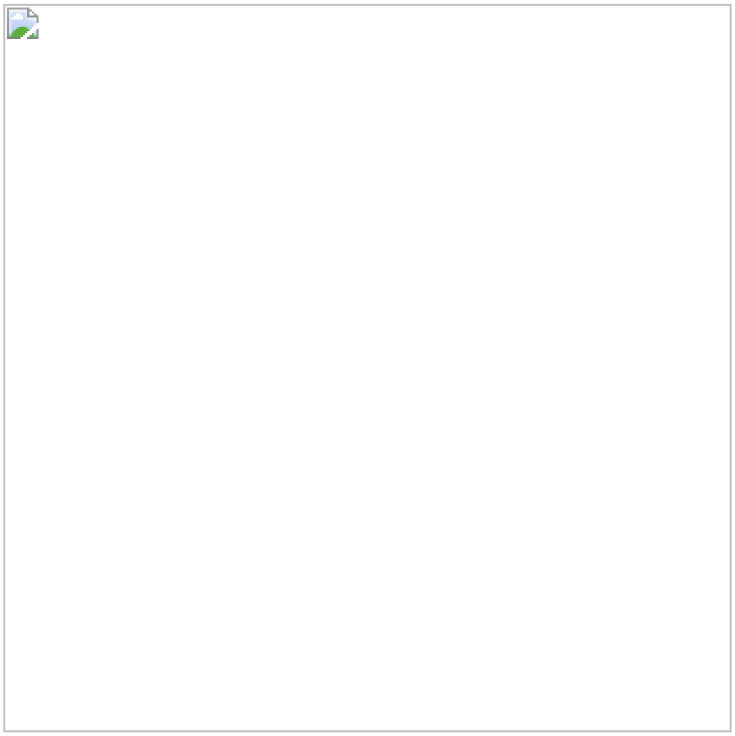
- btc.com
- bitpapa.com
- block.io
- blockchain.com
- www.chase.com
- www.wellsfargo.com
- www.capitalone.com

- www.bankofamerica.com
- gmail.com
- pay.google.com
- facebook.com
- navyfederal.org
- paypal.com

(*Target browser list is described in Appendix.A.)

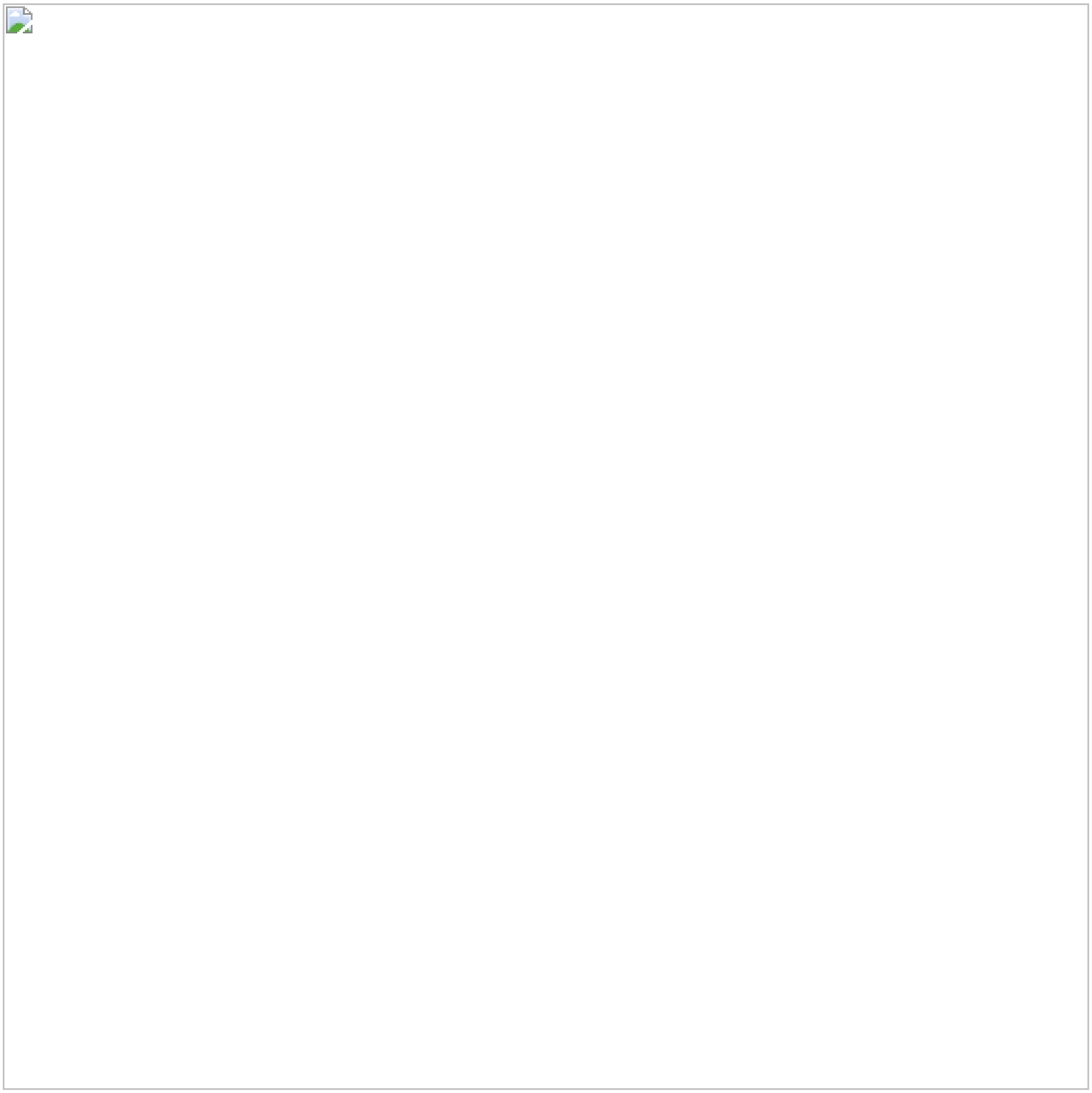
Files Folder

BlackGuard browses Desktop, MyDocuments, and USERPROFILE\source path to steal specific files. It copies files with a file size of less than 2.5MB and has an extension such as ***.txt, *.config, and *.rdp** to the *Files* folder.



Wallets Folder

In the *Wallets* folder, BlackGuard creates a subfolder for each wallet type and copies the wallet.dat file.



[Crypto Wallet List]

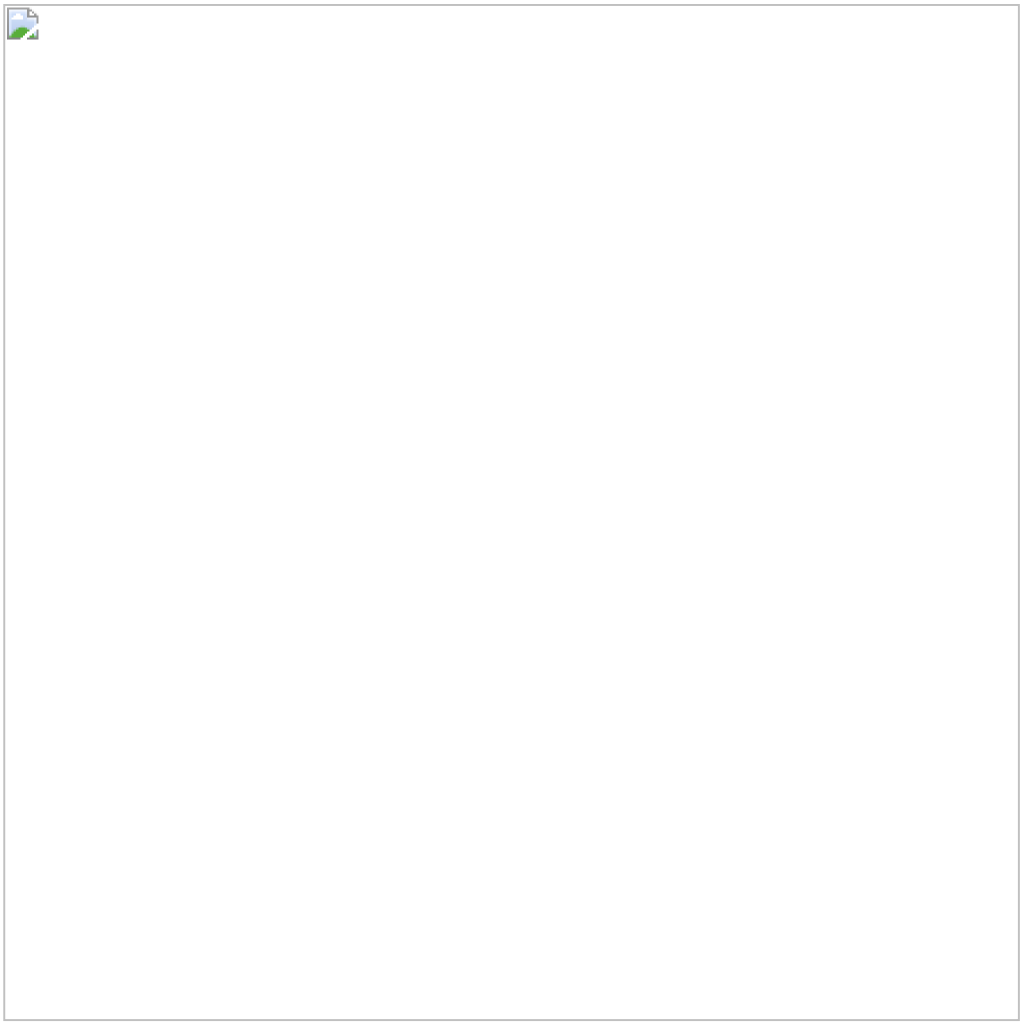
- Armory
- AtomicWallet
- BitcoinCore
- DashCore
- Electrum
- Ethereum
- LitecoinCore
- XMRcoin (Monero)
- Exodus
- Zcash
- Jaxx

VPN Folder

BlackGuard collects three types of VPN: software ProtonVPN, OpenVPN, and NordVPN. The files mainly collected by BlackGuard are **user.config** and **ovpn** file, which contains the private keys. In the case of NordVPN, only the username and password in the **ovpn** file are copied and stored in **accounts.txt.**

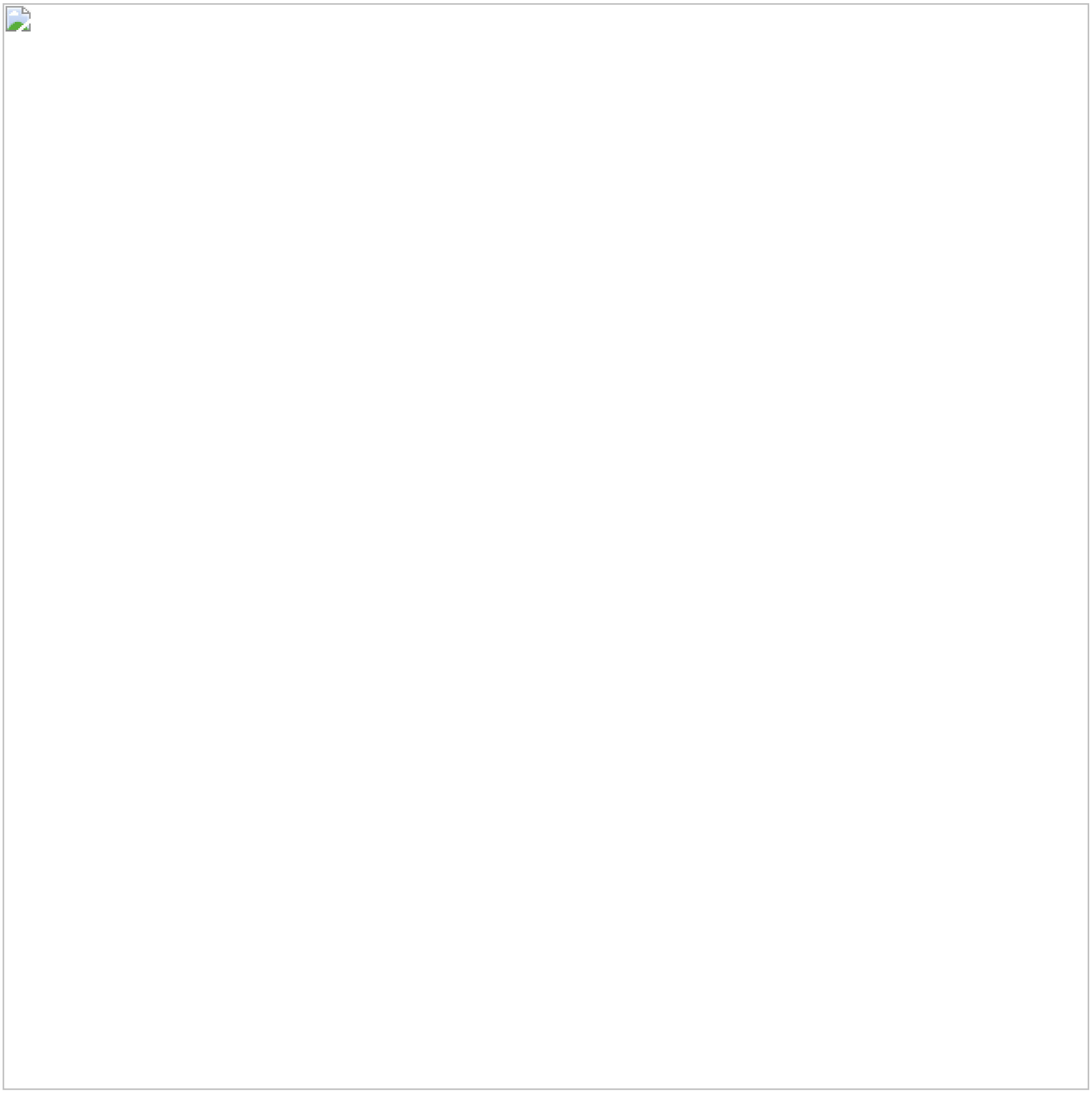
Steam Folder

First, check if Steam is installed on the infected PC. If Steam is installed, BlackGuard copies Steam-related information such as the name and metadata list of installed games, user account data, configuration data, **ssnf** files containing authorization information, and ***.vdf** file which includes resource data.



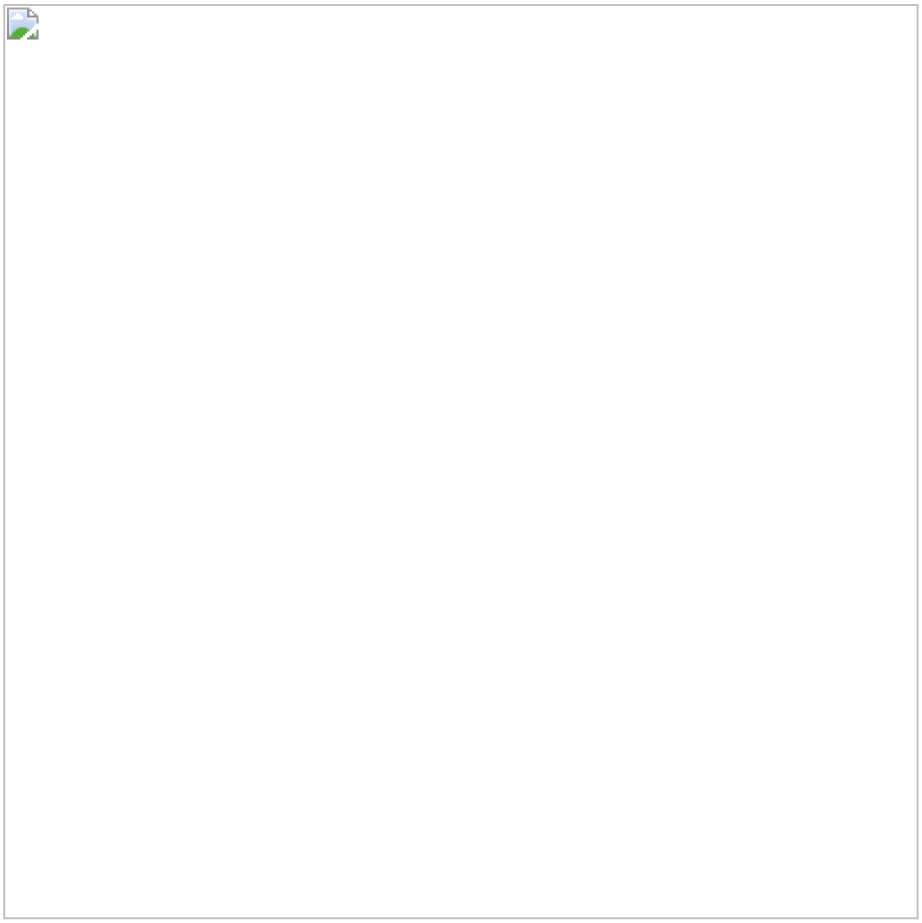
Discord Folder

BlackGuard checks if *.log and *.ldb files are included in the directory list related to Discord. And if so, it copies Discord Token data in the files and Discord Storage folder, then stored in the *Discord* folder.



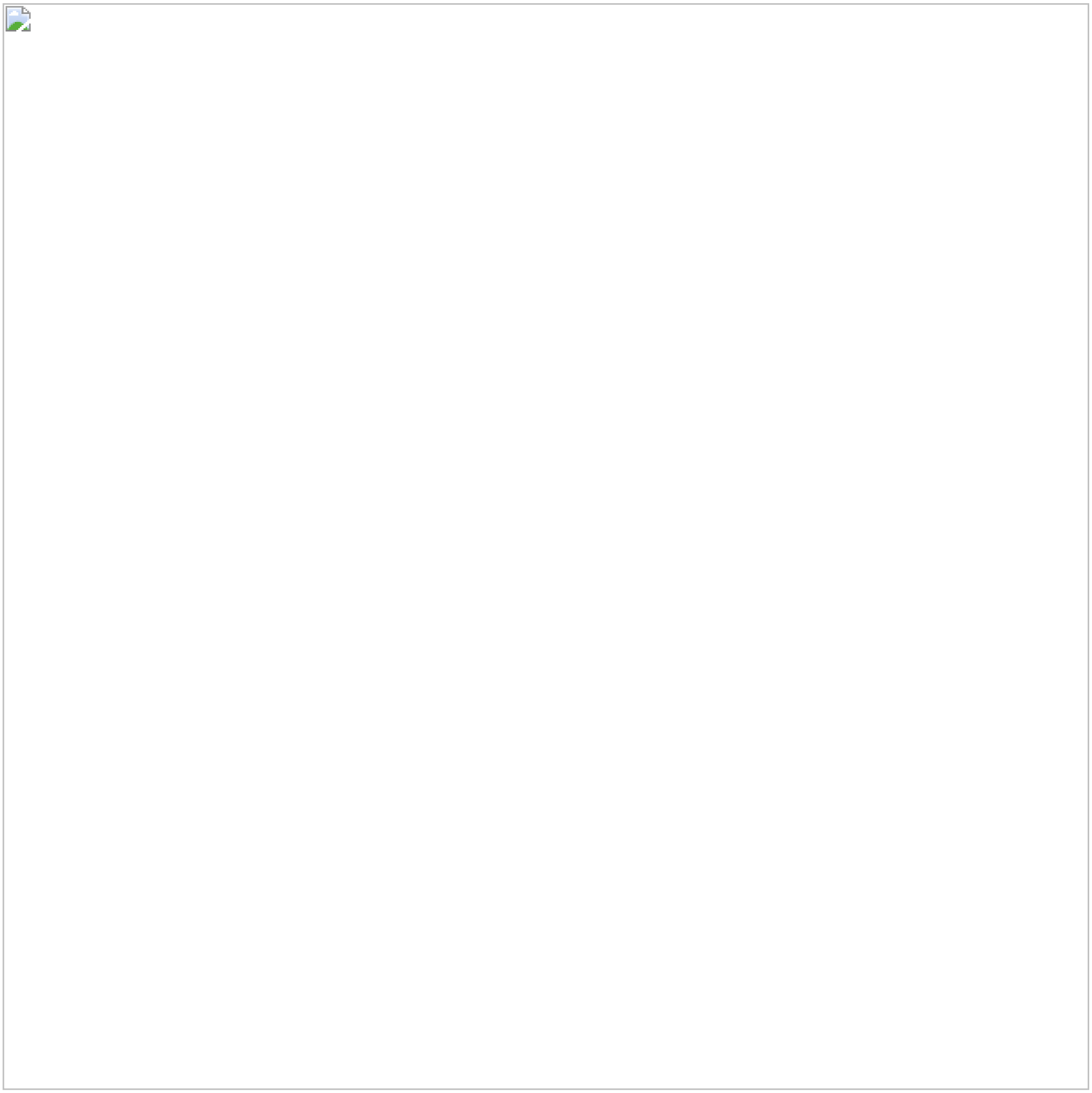
FileZilla Folder

To collect FTP information, BlackGuard browses the FileZilla installation path and copies the host, port number, username, password from recentservers.xml.



Telegram Folder

BlackGuard searches the installed path of the process containing “Telegram” to collect Telegram Session information. If it finds the path where Telegram cache, user data, and the files named “usertag”, “settings” and “key_data” are stored, copies and stores them in the *Telegram* folder.



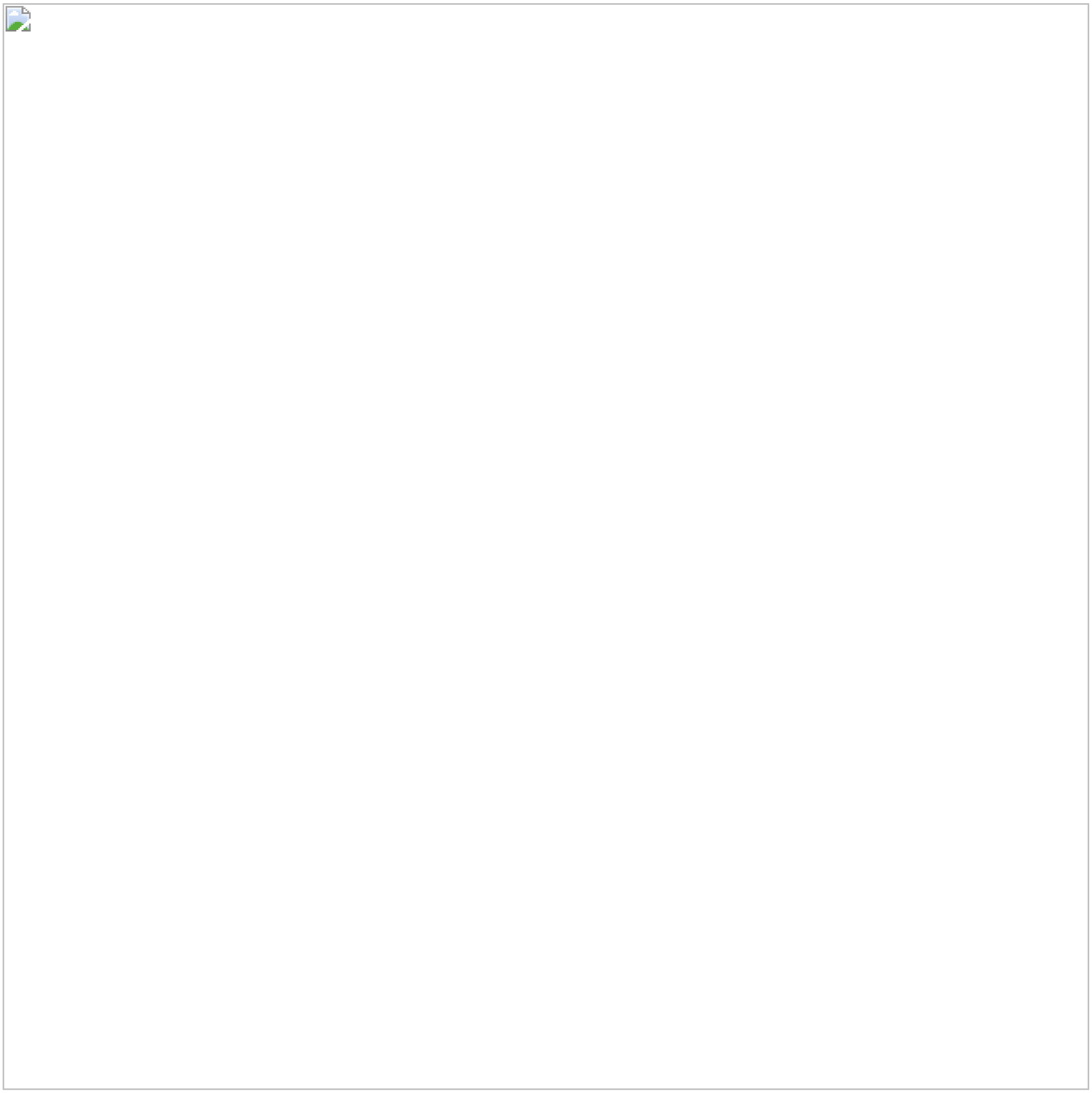
Information.txt

Device information is stored in information.txt. It includes OS Version, CPU architecture, malware file location, screen size, current date and time, HWID, IPv4, country, and malware execution time.

Screenshot.png

BlackGuard takes a screen capture of the current monitor according to the screen size and saves it as *Screenshot.png.*

Categorizing the collected information by type



6. Exfiltrate Information

Compress the folder to the *.zip file

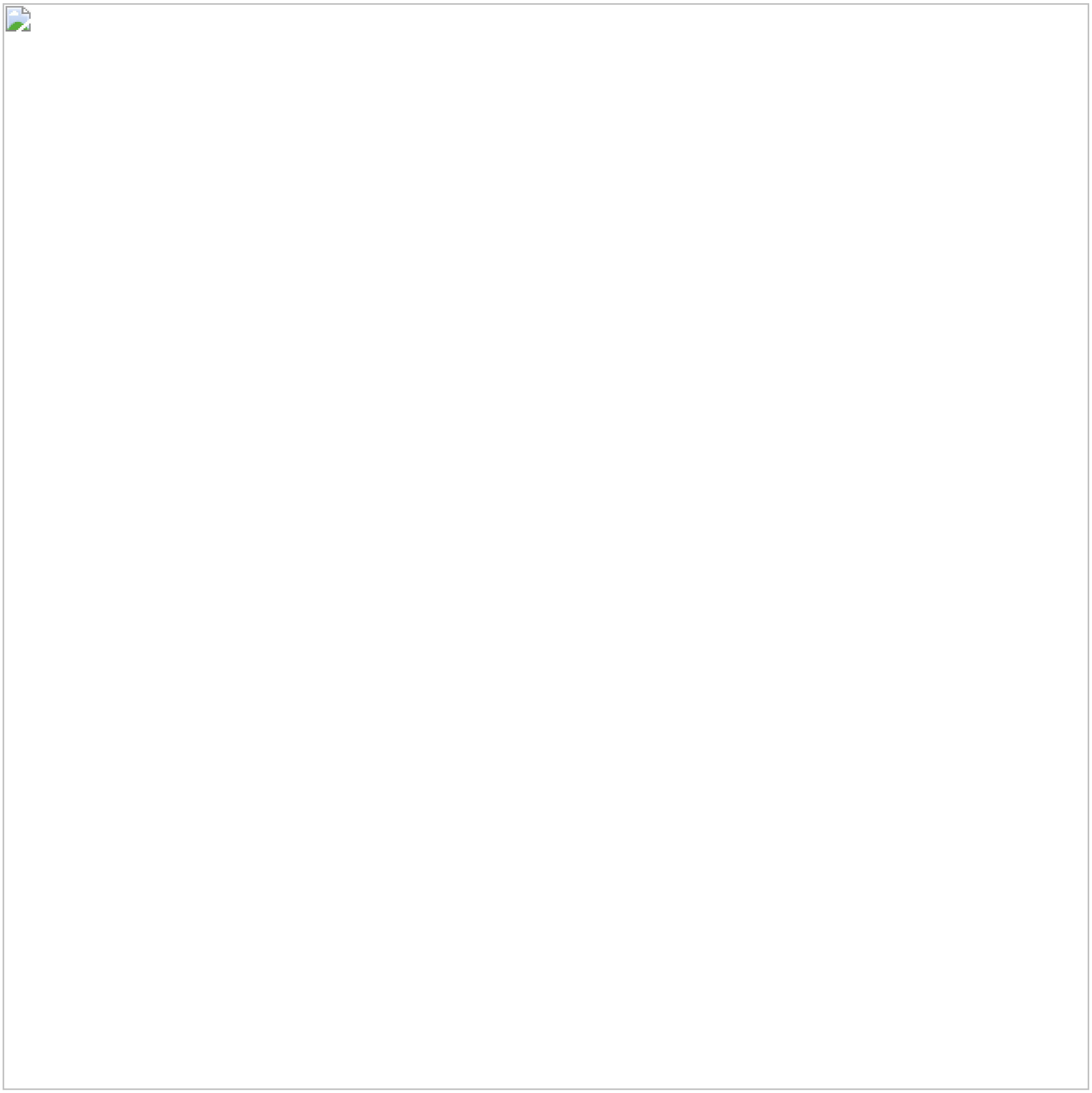
BlackGuard compresses the ChikenDir folder that contains collected information to the zip file and exfiltrates it to the Telegram C2 Server. The name format of zip file is **[HWID]([Current Date]).zip**

Telegram Bot API

BlackGuard sets up Telegram Bot URL to exfiltrate the zip file and send it using **sendDocument** API with POST method. The data sent together includes the number of collected information for each type, the collected target software list, and the list of detected target domains. The message body sent to the Telegram Bot is as shown below.

Telegram Bot information used in this sample is as follows.

- username: @Zeusdarknet_bot
- Chat ID: 1068601339
- Token: 1068601339:AAGUm6n8fS0wwbMhDzm8XXbjUYb6Vb9–64Q



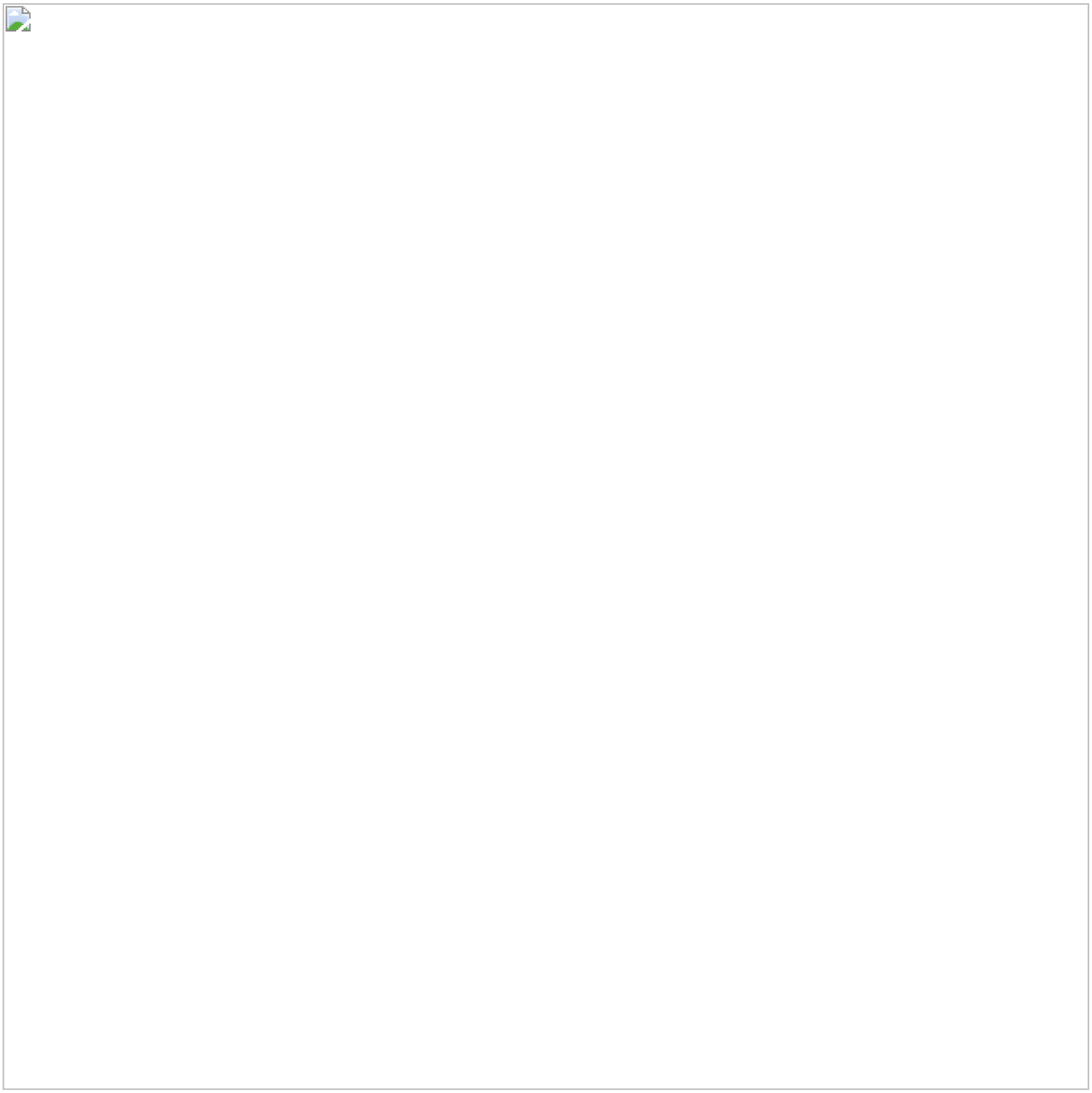
Conclusion

- BlackGuard Stealer has been active on the dark web forums since it appeared in January 2022.
- Considering the type of information collected by BlackGuard and the recent status of distribution, there is a possibility that it will develop into high-impact info stealers such as Redline, Vidal, Raccoon, and Ficker.

Appendix. A: Configuration Data & Browser List

[Help Data]

[Config Data]



Browser List

```
dotnetbrowser-chromium, Chrome, Opera Software, Opera Software GX Stable, Firefox,
ChromePlus, Iridium, 7Star, CentBrowser, Chedot, Vivaldi, Kometa, Elements Browser, Epic
Privacy Browser, uCozMedia, Sleipnir5, Citrio, Coowon, liebao, QIP Surf, Orbitum,
Comodo, Amigo, Torch, 360Browser, Maxthon3, K-Meleon, Sputnik, Nichrome, CooCoc, Uran,
Chromodo, Brave-Browser
```

Appendix. B: MITRE ATT&CK MATRIX

Appendix. C: IoCs

Sample Hash

- 5293c26f29b4af6bc2f3f74ae1ed93537e6c311a695cc0a6920a635c57383617
- 67843d45ba538eca29c63c3259d697f7e2ba84a3da941295b9207cdb01c85b71
- 3c5a8e9820b549a70a353997bbce4fe16956dbab22dedde2f358f0f10930cf44
- 216c960ac6ef399e7ff33b18c03777237ced76d59ce0f8bb4d5f9a22e85b3bd8
- 352c936eaf45ffd2f99ba2a9e726eaa39af29d4c37a6ad5106849f07aa35896c
- 3d3de136d6a22e6064a306452dab72dc70493b02f8f4a505f00bf3dc59e971d3
- 52bd68ea60e7171ed2413cd5292b74ac9872928a1a723405fb73ad57419c5bc6

- 7976a7aa5618c833edfebdbc29853c2f433ce1095a752a177deb76d7f68188be
- 30023cfbcb45d75e461333e376fde3b053c33de84b88c64ef816c9f77e45b21f
- 4f4d29507bafc223646d98f5fed78d52dd96caeee2072ff17b15718b45a1811f
- ba2bc430c4661aab84cf7e8fedf2684e5fc106f7797af4553aef7490193b00a6
- d888dafb1f2ae06311d507e5d3dfa41c851df2175e8441255e2095c09a058d0a
- 7f2542ed2768a8bd5f6054eaf3c5f75cb4f77c0c8e887e58b613cb43d9dd9c13
- a00ef641b6163d787f2210d75eaf631ba1cb3a6f2d4a072226a885a056ee1c4d
- bbc8ac47d3051fbab328d4a8a4c1c8819707ac045ab6ac94b1997dac59be2ece
- b287dcb70b7a9ed7025171572a96f1447efa6adf88cd30aba591270052acfe8b
- 0fc2a7d0dc1a3b0ec547deae8dc296a0b139f94f7f8609c91a8f04a8f939a3e9
- 5b8d0e358948f885ad1e6fa854f637c1e30036bc217f2c7f2579a8782d472cda
- 18db274624914ee6388bda20233db28307be4873bc053e05ad8f6761b217136f
- 76b90299713b5d4ffd3c92b2cd66b3de68148c3133f927dfa385b075fd00d5b1
- 62416ed5c114e347643b51879ee8a75e8a871ab7c02679402f99aaf697e9f9e8
- da5fdea2780ff2e36a3594283a24846c19953daf03063a875073deecc183c3ff
- c5c1a48c0062e113389988d4c70dbcc1a594da3b516dfe14185e622b9050b649
- 918af1137f069eccc04220c280e13ed440a380aa0446cfa1d80b4e0ade6c3528
- 15fc2939e2e67f1317f2e549b8214e83b8e1c493d94eeff2cf4a1cf58b94274f
- 3f36af60743bfb923246e36bb860ff9021986c9e88c5a4176b67a4d0923125b8
- c1237d0e517abc7cd15bb55110196247b1f6ec397c28b8b2bdfba86dc5c8805f
- 5ce632f1f10c96a7524bf384015c25681ef4771f09a6b86883a4da309d85452a
- 26ebf8a0830652c9ea0de64dc0dca6d62caffc0aaa34abf43e7c410095c502ce
- d3b27ba36d01a6ed5492d662c20b38569b0019c29fe065e8f810b369fba76531
- 4d66b5a09f4e500e7df0794552829c925a5728ad0acd9e68ec020e138abe80ac
- f2d25cb96d3411e4696f8f5401cb8f1af0d83bf3c6b69f511f1a694b1a86b74d
- 31c4edabd35f8a9d0695c96f21acd8787eec68b8028973470d64c4956d9f1cd1
- f47db48129530cf19f3c42f0c9f38ce1915f403469483661999dc2b19e12650b
- c98e24c174130bba4836e08d24170866aa7128d62d3e2b25f3bc8562fdc74a66
- 3335f6aff82ff30e3aa29e0cb487be0252ab7b6cf7fcbb074c5642c1f0d7d0c0
- 9fff9895c476bee0cba9d3e209e841873f1756d18c40afa1b364bd2d8446997c

C2s

- https://api.telegram.org/bot1068601339:AAGUm6n8fS0wwbMhDzm8XXbjUYb6Vb9-64Q
- https://api.telegram.org/bot1840568117:AAGlvKQeSfXkObSE7__yYc5jM9o8qSrkFUw
- https://api.telegram.org/bot1822617155:AAF5DW4sJVsYGItkXWeX3elycmmu-6nOK8g
- https://api.telegram.org/bot1625195044:AAHK-2Z52Nk0cJXJ-G7Ad1kKnmzwMberIVU
- https://api.telegram.org/bot2113738307:AAEFFkU5zCHejtwoMag2cI5zpW4JKy8A5jI
- https://greenblguard.shop/
-