

New BlackGuard password-stealing malware sold on hacker forums

bleepingcomputer.com/news/security/new-blackguard-password-stealing-malware-sold-on-hacker-forums/

Bill Toulas

By

[Bill Toulas](#)

- March 31, 2022
- 03:30 PM
- 2



A new information-stealing malware named BlackGuard is winning the attention of the cybercrime community, now sold on numerous darknet markets and forums for a lifetime price of \$700 or a subscription of \$200 per month.

The stealer can snatch sensitive information from a broad range of applications, pack everything in a ZIP archive and send it to the C2 of the malware-as-a-service (MaaS) operation.

Threat actors who purchased the subscription can then access the BlackGuard web panel to retrieve the stolen data logs, either exploiting them themselves or selling them to others.

BlackGuard's user panel (Zscaler)

BlackGuard was spotted and analyzed by researchers at [Zscaler](#), who have noticed a sudden spike in the popularity of the malware, especially after the abrupt [shutdown of Raccoon Stealer](#).

Bleeping Computer was able to find that BlackGuard first appeared on Russian-speaking forums in January 2022, circulated privately for testing purposes.

Stealer BlackGuard


BlackGUARD07 · 11 Янв 2022 · 2К · blackguard stealer web

Форумы > Рынок > Приватное ПО > **Официальное**

Назад 1 2

Перейти к новому Отслеживать

24 Фев 2022 Новое #16



hyipblock2
Пользователь
Регистрация: 19 Янв ...
Сообщения: 11
Реакции: 3
Баллы: 45

Взял данный стиллак, очень доволен отступком и как он собирает файлы, а он тащит блин реально все что можно.

Для меня самое главное было чтоб он тащил все... особенно меты, кто работает с криптой меня поймет, более половины стилаков не дают эту возможность, а тут все ровно собирает..

Вот вид лога, все ровно и красиво.

Папка с файлами						
Wallets	641	641	Папка с файлами	22.02.2022	6:50	
Telegram	12 806 831	12 806 831	Папка с файлами	22.02.2022	6:50	
Messenger	0	0	Папка с файлами	22.02.2022	6:50	
Files	310 746	310 746	Папка с файлами	22.02.2022	6:50	
Edge_Wallet	240	240	Папка с файлами	22.02.2022	6:50	
Edge Betta_Wallet	0	0	Папка с файлами	22.02.2022	6:50	
Chrome_Wallet	16 299 604	16 299 604	Папка с файлами	22.02.2022	6:50	
Browsers	885 722	885 722	Папка с файлами	22.02.2022	6:53	
UserAgent.txt	103	103	Текстовый докуме...	22.02.2022	6:53	7C4B26B1
Screen.Png	1 280 282	1 280 282	Файл "PNG"	22.02.2022	6:50	BA8BA673
Information.txt	569	569	Текстовый докуме...	22.02.2022	6:45	1533F361

A February 2022 forum post showcasing BlackGuard's loot (KELA)

Extensive stealing abilities

As with all modern information-stealers, there aren't many apps storing or handling sensitive user data that are not in BlackGuard's targeting scope, and the focus is heavy on cryptocurrency assets.

BlackGuard will seek the presence of the following software and attempt to steal user data from them:

- **Web browsers:** Passwords, cookies, autofill, and history from Chrome, Opera, Firefox, MapleStudio, Iridium, 7Star, CentBrowser, Chedot, Vivaldi, Kometa, Elements Browser, Epic Privacy Browser, uCozMedia, Coowon, liebao, QIP Surf, Orbitum, Comodo, Amigo, Torch, Comodo, 360Browser, Maxthon3, K-Melon, Sputnik, Nichrome, CocCoc, Uran, Chromodo, Edge, BraveSoftware

- **Wallet browser extensions:** Binance, coin98, Phantom, Mobox, XinPay, Math10, Metamask, BitApp, Guildwallet, iconx, Sollet, Slope Wallet, Starcoin, Swash, Finnie, KEPLR, Crocobit, OXYGEN, Nifty, Liquidity, Auvitas wallet, Math wallet, MTV wallet, Rabet wallet, Ronin wallet, Yoroi wallet, ZilPay wallet, Exodus, Terra Station, Jaxx
- **Cryptocurrency wallets:** AtomicWallet, BitcoinCore, DashCore, Electrum, Ethereum, Exodus, LitecoinCore, Monero, Jaxx, Zcash, Solar, Zap, AtomicDEX, Binance, Frame, TokenPocket, Wassabi
- **Email:** Outlook
- **Messengers:** Telegram, Signal, Tox, Element, Pidgin, Discord
- **Other:** NordVPN, OpenVPN, ProtonVpn, Totalcommander, Filezilla, WinSCP, Steam

The collected information is bundled in a ZIP file, also known as logs, and sent to the C2 server via a POST request, along with a system profiling report that sets a unique hardware ID for the victim and determines their location.

```
public static string[] f000015 = new string[]
{
    "Temp\\dotnetbrowser-chromium\\64.0.3282.24.1.19.0.0.642\\32bit",
    "Chromium\\User Data",
    "Google\\Chrome\\User Data",
    "Google(x86)\\Chrome\\User Data",
    "Opera Software",
    "Opera Software\\Opera GX Stable\\Login Data",
    "Opera Software\\Opera GX Stable",
    "Mozilla\\Firefox",
    "MapleStudio\\ChromePlus\\User Data",
    "Iridium\\User Data",
    "7Star\\User Data",
    "CentBrowser\\User Data",
    "Chedot\\User Data",
    "Vivaldi\\User Data",
    "Kometa\\User Data",
    "Elements Browser\\User Data",
    "Epic Privacy Browser\\User Data",
    "uCozMedia\\Uran\\User Data",
    "Fenrir Inc\\Sleipnir5\\setting\\modules\\ChromiumViewer",
    "CatalinaGroup\\Citrio\\User Data",
    "Coowon\\Coowon\\User Data",
    "liebao\\User Data",
    "QIP Surf\\User Data",
    "Orbitum\\User Data",
    "Comodo\\Dragon\\User Data",
    "Amigo\\User\\User Data",
    "Torch\\User Data",
    "Comodo\\User Data",
    "360Browser\\Browser\\User Data",

```

Stealing information from a range of web browsers (Zscaler)

Anti-detection features

BlackGuard's evasion capabilities are still under heavy development, but some systems are already in place to help the malware escape detection and analysis.

First, it is packed with a crypter, and all its strings are base64 obfuscated, so many anti-virus tools relying on static detection will miss it.

Any AVs running on the system will be detected by the malware, which will then attempt to kill their processes and terminate their operation.

The malware also checks the victim's IP address, and if it's running on a system in Russia or any other CIS country, it will stop and exit. This is yet another indication of the origin of the malware.

```
List<string> list = new List<string>();
list.Add(Class56.Armenia());
list.Add(Class56.Azerbaijan());
list.Add(Class56.Belarus());
list.Add(Class56.Kazakhstan());
list.Add(Class56.Kyrgyzstan());
list.Add(Class56.Moldova());
list.Add(Class56.Tajikistan());
list.Add(Class56.Uzbekistan());
list.Add(Class56.Ukraine());
list.Add(Class56.Russia());
list.Sort();
foreach (string value in list)
{
    if (Class26.smethod_7().Contains(value))
    {
        return true;
    }
}
return false;
```

List of countries excluded from attacks (Zscaler)

Finally, an anti-debug feature blocks the operation of the mouse and keyboard inputs, making it further difficult for researchers to analyze the malware.

Outlook

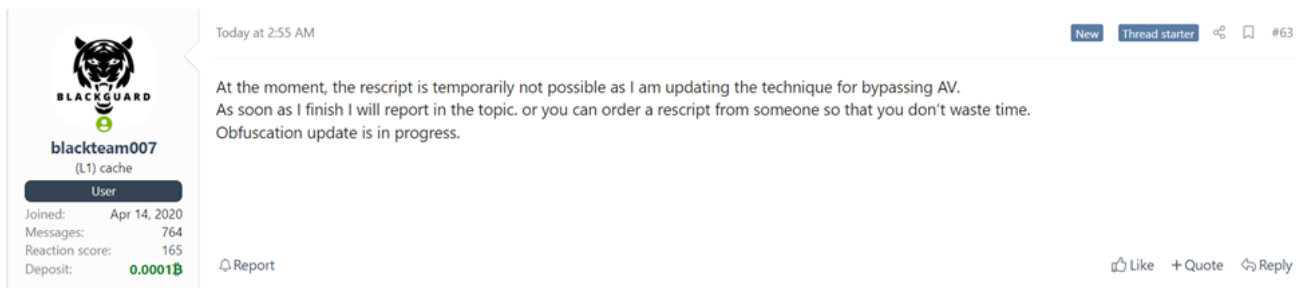
Info-stealers are on the rise, with [Redline](#), [MarsStealer](#), [Vidar Stealer](#), and [AZORult](#) currently dominating the space.

The exit of Raccoon Stealer, which was one of the biggest players, has left a gap in the cybercrime market, so other MaaS operators will try to take advantage of this development.

Daria Romana Pop, a threat analyst at [KELA](#), has shared the following insights with Bleeping Computer on the status of the info-stealers landscape:

"Given the increase in usage and exploitation of compromised accounts and data obtained by information stealers as a vector for initial access to a target, KELA has recently observed new variants being advertised on cybercrime forums, as threat actors aim at improving the malware capabilities to better avoid detection and to advance the data collection and exfiltration processes."

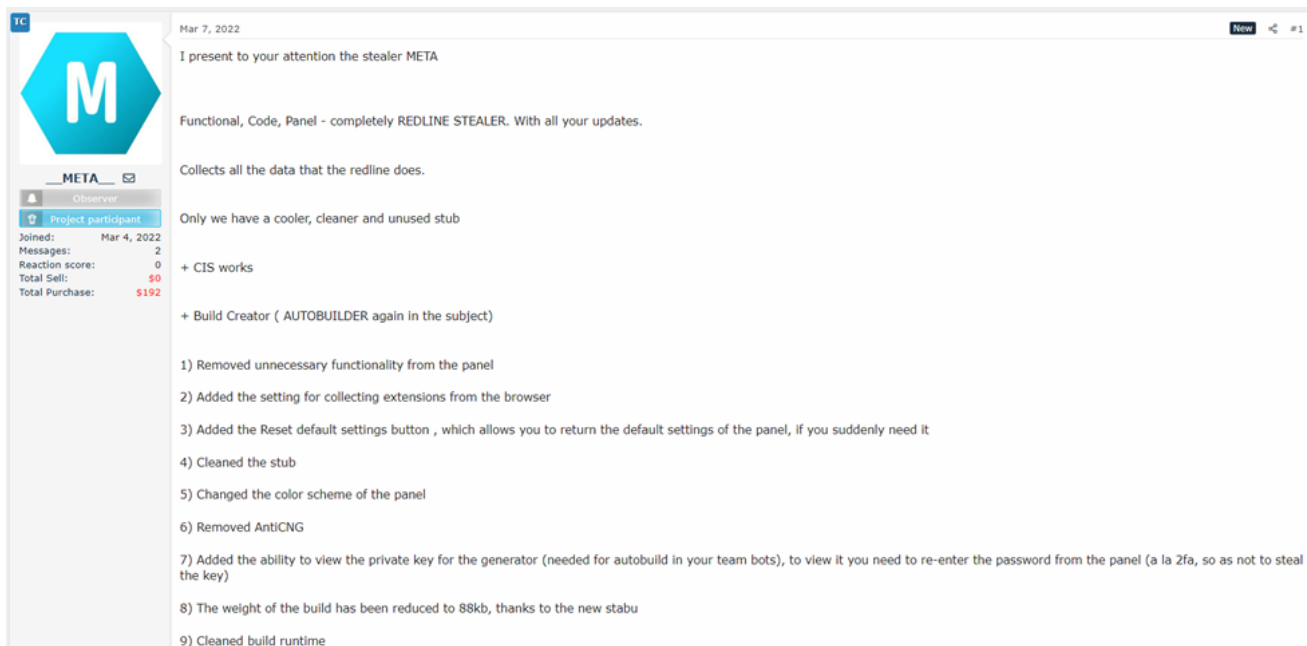
"BlackGuard stealer launched in early 2021. As cybercriminals are constantly testing the capabilities of such malicious tools, they do not shy away from demanding more quality and improvements. KELA came across several recent discussions in which users were complaining about BlackGuard not being able to properly avoid detection. As in any business, the operators promised to provide an updated version in no time."



The screenshot shows a forum post from a user named 'blackteam007' (L1 cache). The user's profile includes a tiger logo, a 'BLACKGUARD' tag, and statistics: Joined: Apr 14, 2020; Messages: 764; Reaction score: 165; Deposit: 0.0001B. The post content, dated 'Today at 2:55 AM', reads: 'At the moment, the rescript is temporarily not possible as I am updating the technique for bypassing AV. As soon as I finish I will report in the topic. or you can order a rescript from someone so that you don't waste time. Obfuscation update is in progress.' The post has 63 replies and includes interaction buttons for 'Like', 'Quote', and 'Reply'.

Author of BlackGuard promising to improve anti-detection scheme (KELA)

"In a different scenario, KELA identified META - a new information stealer very similar in appearance to RedLine, whose collected data is being sold on the TwoEasy botnet marketplace. The stealer was launched at the beginning of March, now sold for USD125 per month or USD1000 for unlimited use, and the operators claim that it is an improved version of RedLine."



The screenshot shows a forum post from a user named 'META' (Observer). The user's profile includes a blue hexagonal logo with a white 'M' and statistics: Joined: Mar 4, 2022; Messages: 2; Reaction score: 0; Total Sell: \$0; Total Purchase: \$192. The post content, dated 'Mar 7, 2022', reads: 'I present to your attention the stealer META. Functional, Code, Panel - completely REDLINE STEALER. With all your updates. Collects all the data that the redline does. Only we have a cooler, cleaner and unused stub. + CIS works. + Build Creator (AUTOBUILDER again in the subject). 1) Removed unnecessary functionality from the panel. 2) Added the setting for collecting extensions from the browser. 3) Added the Reset default settings button , which allows you to return the default settings of the panel, if you suddenly need it. 4) Cleaned the stub. 5) Changed the color scheme of the panel. 6) Removed AntiCNG. 7) Added the ability to view the private key for the generator (needed for autobuild in your team bots), to view it you need to re-enter the password from the panel (a la 2fa, so as not to steal the key). 8) The weight of the build has been reduced to 88kb, thanks to the new stub. 9) Cleaned build runtime.'

META info-stealer promoted on hacking forums (KELA)

To protect yourself from all of the circulating info-stealing malware, avoid visiting shady websites and downloading files from untrustworthy or dubious sources.

Finally, use two-factor authentication, keep your OS and applications up to date, and use strong and unique passwords for all your online accounts.

Related Articles:

[New powerful Prynt Stealer malware sells for just \\$100 per month](#)

[Fake Binance NFT Mystery Box bots steal victim's crypto wallets](#)

[Fake Pixelmon NFT site infects you with password-stealing malware](#)

[Eternity malware kit offers stealer, miner, worm, ransomware tools](#)

[German automakers targeted in year-long malware campaign](#)

- [BlackGuard](#)
- [Credential Theft](#)
- [Credentials](#)
- [Info Stealer](#)
- [Information Stealer](#)
- [Password Stealing Trojan](#)

[Bill Toulas](#)

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- [Previous Article](#)
- [Next Article](#)

Comments



Elko_NV - 1 month ago

- o
- o

Another fine article Bill ~!

Unless Blackguard somehow ships with own ZIP capability, guess it uses Windows itself to package those .ZIP files before being sent ? Other concerns too, vulnerability like sending LNK malware via ZIP had been an issue. Luckily we can disable reading that extension entirely with Windows, with no default program set. Also, can lower CPU usage when disabled on some PC, otherwise always indexing ZIPs in background.

Windows Registry Editor Version 5.00

; Open Notepad, copy and paste all the text of this comment and save it as:
DisableZipFolders.reg

; Disable ZIP folders in Windows 7/8/10/11

; Apply & Relog/Reboot

[-HKEY_CLASSES_ROOT\SystemFileAssociations\.zip\CLSID]

[-HKEY_CLASSES_ROOT\CompressedFolder\ShellEx\StorageHandler]

[-HKEY_CLASSES_ROOT\CompressedFolder\CLSID]

[-HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.zip\CLSID]

[-
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CompressedFolder\ShellEx\StorageHandler]

[-HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CompressedFolder\CLSID]



• [JohnnyJammer](#) - 1 month ago

-
-

LOL, that wont do anything mate.
Ever heard of compress-archive in Powershell?

By the way most stealers like this will set the registry values before execution anyway to ensure it works, that is IF the user has elevated privs.

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
