New BlackGuard password-stealing malware sold on hacker forums

By Bill Toulas

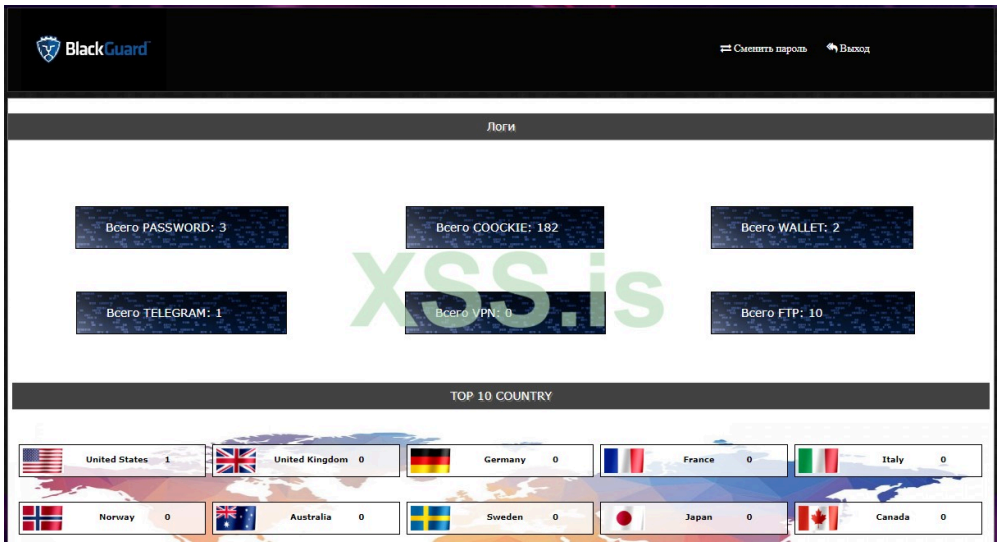
Published: 2022-03-31 · Archived: 2026-04-02 11:21:36 UTC

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.

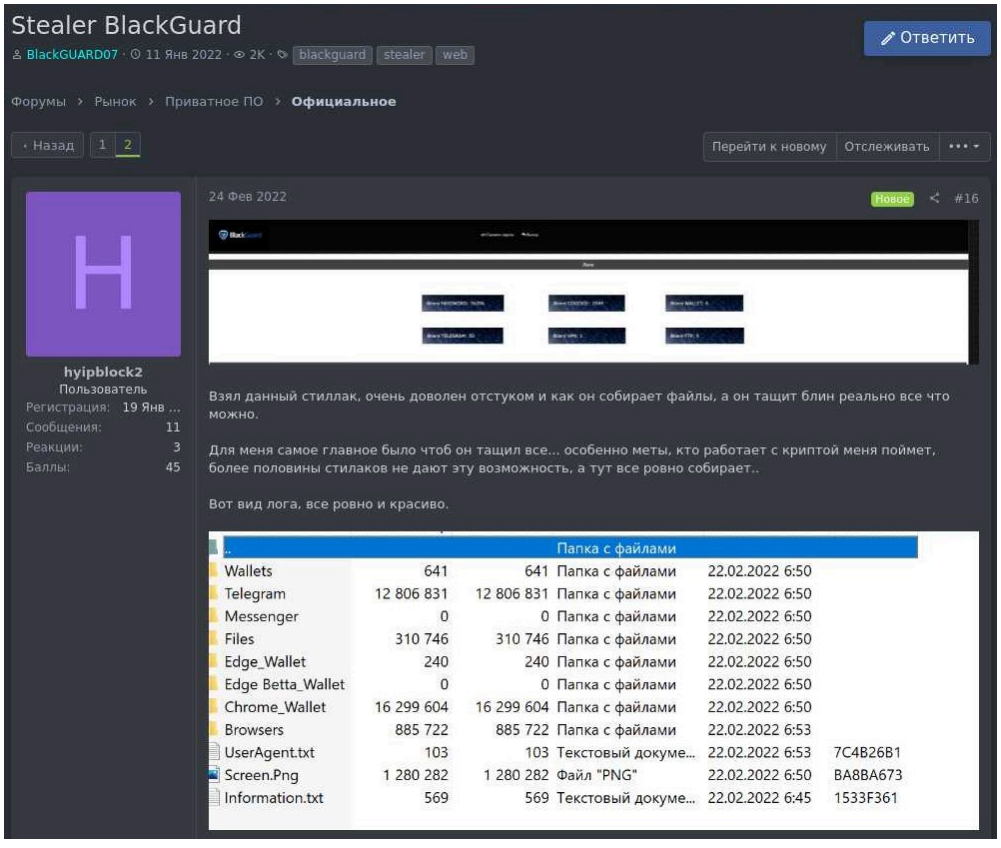

f5
Outlook
cisco
cisco



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.



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, Liquality, 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

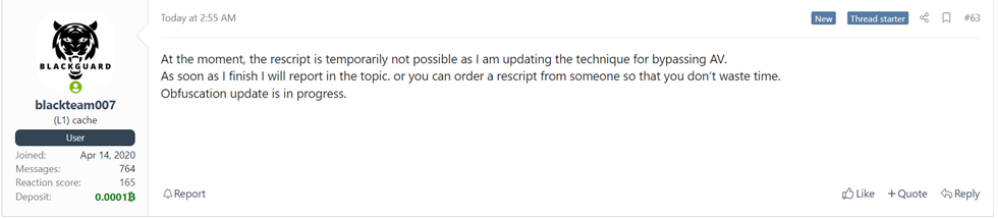
Info-stealers are on the rise, with Redline, MarsStealer, Vidar Stealer, and AZORult currently dominating the space.

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:

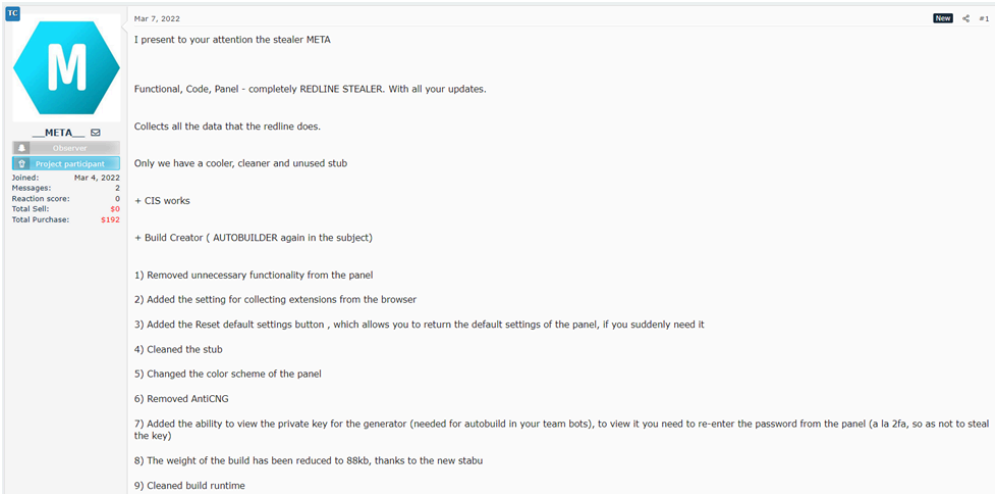
"Given the increase in usage and exploitation of compromised accounts and data obtained by information stealers as a vector for initial access to a target, KELA has recently observed new variants being advertised on cybercrime forums, as threat actors aim at improving the malware capabilities to better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



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."



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.

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