

BlackGuard Infostealer Malware: Dissecting the State of Exfiltrated Data

By Authors & Contributors

Archived: 2026-04-06 00:13:40 UTC

Overview

Blackguard Infostealer is a malware strain that was first discovered infecting Windows devices at the start of 2022. Other security researchers have already documented how the malware operates and its dissemination via underground Russian crimeware forums.¹ This article aims to expand on existing research by exploring its data exfiltration capabilities in greater detail. Blackguard is designed to steal a wide range of personal data, including credentials, cookies, messaging history, browsing history, cryptocurrency wallet information, and screenshots from the infected machine. By understanding what types of data attackers want, we can better understand the value Blackguard offers its authors and writers, and therefore how malware fits into the broader cybercrime ecosystem.

Attackers distribute Blackguard using a variety of techniques, including drive-by downloads and phishing emails containing malicious attachments. Once Blackguard Infostealer has infected a victim's device, it initiates techniques such as system Application Programming Interface (API) hooking, Dynamic Link Library (DLL) injection and resource hijacking to steal credentials from browsers, messenger clients, and other client-side software. The stolen data is compressed and exfiltrated in the same HTTP-based communication channel that the attackers use for command and control (C&C). The exfiltrated credentials are stored on the C&C server and then used to conduct additional attacks such as credential stuffing, account creation, and online fraud.

Analysis

In our research of BlackGuard Infostealer we identified an exposed command and control (C&C) administrator panel (Figure 1) and analyzed the stolen data stored within.

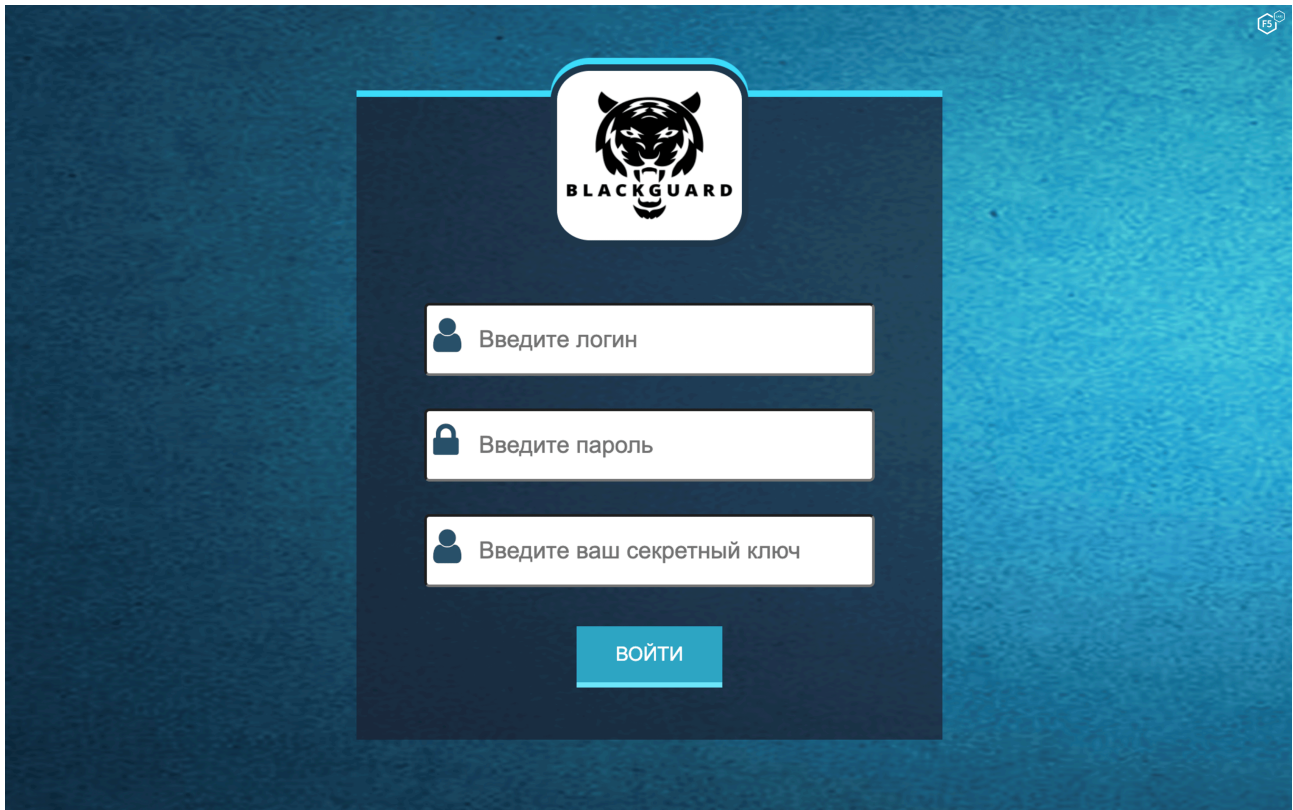


Figure 1. Blackguard malware administrative panel.

During active and passive analysis of the BlackGuard C&C panel, we found that the malware records geographical information from the compromised systems, indicating that BlackGuard is used to target victims all around the world. Figure 2 highlights a snippet of exposed zipped files containing stolen data from compromised systems showing data stolen from users in Sweden, Switzerland, the UK, and the United States.



-IW-I--I--	1	staff	3755584	09:27	157.26/files/(Sweden)_[BGDAupSeFBIdGgyqtieoKhtlyBFuKBft].rar
-IW-I--I--	1	staff	3457612	09:22	157.26/files/(Sweden)_[FBFeofh1KAgeklBFKj].rar
-IW-I--I--	1	staff	472172	11:19	157.26/files/(Sweden)_[fgAKDFrjetDKFFk].rar
-IW-I--I--	1	staff	182082	11:22	157.26/files/(Sweden)_[tApyuDtBkgBiroBfuFDKgdDlDowDlthwSBwSgGfP].rar
-IW-I--I--	1	staff	664447	05:21	157.26/files/(Switzerland)_[GyK].rar
-IW-I--I--	1	staff	1498006	05:17	157.26/files/(Switzerland)_[KBpgFokBSAFGopq].rar
-IW-I--I--	1	staff	829792	06:08	157.26/files/(Switzerland)_[KBwFyDoKiBBKhyApkifSFjyFqjhFhrKwyhiFj].rar
-IW-I--I--	1	staff	132305	15:51	157.26/files/(Switzerland)_[KwghKkfjAfoKfDtdYqyGeeSfqKBDetj].rar
-IW-I--I--	1	staff	1244610	05:14	157.26/files/(Switzerland)_[].rar
-IW-I--I--	1	staff	1482112	06:08	157.26/files/(Switzerland)_[fjyueKaffG1SrA].rar
-IW-I--I--	1	staff	1497491	05:17	157.26/files/(Switzerland)_[jK].rar
-IW-I--I--	1	staff	839211	06:08	157.26/files/(Switzerland)_[kwojkiwqDpogFojheKiKFjBBwKyyuFBiFFSyfPfoFyw].rar
-IW-I--I--	1	staff	843269	05:16	157.26/files/(Switzerland)_[oDFftuAeGKKiyKwyrSqrKBSjUshIFDr].rar
-IW-I--I--	1	staff	2234721	08:48	157.26/files/(United Kingdom)_[AKqFGrteeKAGwSwtuhhfjBtiFgturGhoqK].rar
-IW-I--I--	1	staff	811401	03:54	157.26/files/(United Kingdom)_[Aiwgwtkrwjf1KwtheKqKokKwAlFAKF].rar
-IW-I--I--	1	staff	555819	10:03	157.26/files/(United Kingdom)_[Byj].rar
-IW-I--I--@	1	staff	3628114	11:25	157.26/files/(United Kingdom)_[GKBhrfUlBjBkekFggSGoyrFBBK].rar
-IW-I--I--	1	staff	787631	04:15	157.26/files/(United Kingdom)_[GgGuFpywSifeujfoBwuktqtApoFtGhk].rar
-IW-I--I--	1	staff	984020	10:57	157.26/files/(United Kingdom)_[KKAIFogergqAFBySDKyDgWfKpK].rar
-IW-I--I--	1	staff	322209	11:22	157.26/files/(United Kingdom)_[KujBleBgSoyqKtwqfeGutBlehoKqrKqQeriBlrF].rar
-IW-I--I--	1	staff	3115991	07:19	157.26/files/(United Kingdom)_[KyGwtB].rar
-IW-I--I--	1	staff	533875	04:38	157.26/files/(United Kingdom)_[].rar
-IW-I--I--	1	staff	193926	04:10	157.26/files/(United Kingdom)_[gKqKkKkBrDatBSyAKKBAiAfgFptFoGrtkK].rar
-IW-I--I--	1	staff	2237589	08:20	157.26/files/(United Kingdom)_[k1KwolkAKwqoxrFBpSupkoiluyifghhkf].rar
-IW-I--I--	1	staff	588401	08:53	157.26/files/(United Kingdom)_[jfoKfkiqBowlhfKfYurtistFGaurwAiAKKqD8].rar
-IW-I--I--	1	staff	389852	03:39	157.26/files/(United Kingdom)_[keeSgUdrkgSfggkBiBfujAdrBKGBFt1K1AqjktKD].rar
-IW-I--I--	1	staff	542499	08:31	157.26/files/(United Kingdom)_[oFBiGjreGfBeh].rar
-IW-I--I--	1	staff	1197798	06:47	157.26/files/(United Kingdom)_[oFKjABlTGiAFjtkijquGrGdeFioBFDKFBqK].rar
-IW-I--I--	1	staff	666503	06:10	157.26/files/(United Kingdom)_[owhKfKwBFfjktKulFBFugfAFwqABFpGwG].rar
-IW-I--I--	1	staff	1191399	11:21	157.26/files/(United Kingdom)_[qqoADf].rar
-IW-I--I--	1	staff	235317	07:02	157.26/files/(United Kingdom)_[uBfDwBijFDkqoGwFAKqSotiFKGDuupfKrhYBhjFFFK].rar
-IW-I--I--	1	staff	15028095	11:35	157.26/files/(United Kingdom)_[wpqBreSolrjFwqAkFqgiBypealAKAKK1BAkw].rar
-IW-I--I--	1	staff	413938	14:05	157.26/files/(United States)_[AASauKkrSlupDpuKfHfhtwAAtk].rar
-IW-I--I--	1	staff	440608	06:05	157.26/files/(United States)_[AKf1Kjkwrg].rar
-IW-I--I--	1	staff	2485216	05:56	157.26/files/(United States)_[BAFrIswhqeSAtpGFeAwoByTAA].rar
-IW-I--I--	1	staff	593964	00:51	157.26/files/(United States)_[BFADgSjfqgKukAifFi].rar
-IW-I--I--	1	staff	441500	05:14	157.26/files/(United States)_[BKuAfgrrBqFKkFtGD1krKweyGFrFpFrjtlKq].rar
-IW-I--I--	1	staff	2528176	21:40	157.26/files/(United States)_[BSAFBBwAFuqFlifBorjFepFStS].rar
-IW-I--I--	1	staff	771653	20:14	157.26/files/(United States)_[DGwAFKwDiqKp1kUoBrB1glFwogDFprqyhDpDfoKqg].rar
-IW-I--I--	1	staff	2353247	09:27	157.26/files/(United States)_[FADGkgjDSShKpttpKokBFeAfupFrgKlgKBSSH].rar
-IW-I--I--	1	staff	1071110	09:45	157.26/files/(United States)_[FDwAeGeufjSSp1FjKofABAOFK].rar
-IW-I--I--	1	staff	618149	21:48	157.26/files/(United States)_[FkuibeyBhpBkor].rar
-IW-I--I--	1	staff	771752	20:15	157.26/files/(United States)_[FwSjGfuhRkfwaiy1AiktSKfGrySAqufIDdj].rar
-IW-I--I--	1	staff	2520263	20:06	157.26/files/(United States)_[GpuKjDpikfBghBlqAFSDu].rar
-IW-I--I--	1	staff	1071098	21:36	157.26/files/(United States)_[KigFopDijewpKS].rar
-IW-I--I--	1	staff	588463	05:06	157.26/files/(United States)_[KofPhfegKfijukyFoyifwBFDKABirtioBi].rar
-IW-I--I--	1	staff	436908	11:16	157.26/files/(United States)_[SSSjyBueFhyKusBD1ABwhFSq1kAyqr1AghArKFbj].rar
-IW-I--I--	1	staff	76489	07:16	157.26/files/(United States)_[eyjrguDyKfWfWSDDGK1G5yBjkuuqpl].rar
-IW-I--I--	1	staff	845773	07:07	157.26/files/(United States)_[fBB].rar
-IW-I--I--	1	staff	445105	07:05	157.26/files/(United States)_[fKgyFefK1DooFe].rar
-IW-I--I--	1	staff	771752	20:15	157.26/files/(United States)_[fehKoklwtjhujqKfW].rar
-IW-I--I--	1	staff	515653	05:20	157.26/files/(United States)_[hdKk].rar
-IW-I--I--	1	staff	94491	18:10	157.26/files/(United States)_[khGlogAgerAfokgpi1yfgBKAA].rar
-IW-I--I--	1	staff	589754	05:06	157.26/files/(United States)_[kqiAt].rar
-IW-I--I--	1	staff	858367	05:17	157.26/files/(United States)_[1Gpwuq].rar
-IW-I--I--@	1	staff	589396	13:03	157.26/files/(United States)_[1gKwKfjyBDj1wBADKAKwSueeBpiBeeSphqAujGfleu].rar
-IW-I--I--	1	staff	598460	08:29	157.26/files/(United States)_[1uDppf].rar
-IW-I--I--	1	staff	588385	06:06	157.26/files/(United States)_[rSdFAKAAK].rar
-IW-I--I--	1	staff	80588	06:14	157.26/files/(United States)_[wGAAPAjpbuFrkpFGK1fSBKbp].rar
-IW-I--I--@	1	staff	1068786	12:31	157.26/files/(United States)_[yKpiKqAyfpq1kqjGBKjfoTqGpAtqfoqqFw1AlDgtB].rar
-IW-I--I--	1	staff	589543	01:54	157.26/files/(United States)_[yeq1FKrpKuqh1okogKikore].rar
-IW-I--I--@	1	staff	413644196	20:51	157.26/files/pack.rar

Figure 2. Data exfiltrated by blackguard and stored in a compressed format.

We analyzed these compressed files to understand the potential storage constructs used. Since there was a risk that these compressed files could contain malware as well, the files were decompressed into ephemeral virtual machines and subsequently destroyed. BlackGuard Infostealer stores the stolen data in a specific layout, as highlighted in Figure 3.



Figure 3. Directory structure used for storing stolen data.

The rest of the article will detail each of the major types of stolen data to examine what is stolen, how it is collected, and the impact of the theft.

Exfiltrating Credentials

Stolen credentials, obtained by malware infections or website hacks, are often used by attackers for a number of purposes. These may include:

1. Being sold in the underground community as part of crimeware services to earn money and enable additional adversaries to use the exfiltrated data.
2. Using the stolen credentials to target applications using credential stuffing attacks to gain access as the compromised users.
3. Conducting online fraud by impersonating victims and purchasing gift cards or performing financial transfers.
4. Launching malware distribution attacks from the compromised accounts.

Figure 4 shows the variety of credentials stolen by BlackGuard, including usernames and passwords from online ecommerce sites, email services, and even internal/intranet sites.



```
[$ cat passwords.txt
Hostname: https://intranet.strongvpn.com/services/intranet/login/
Username: [redacted]gmail.com
Password: [redacted]

Hostname: https://accounts.uber.com/forgot-password/
Username: [redacted]
Password: [redacted]

Hostname: https://www.delta.com/login/loginPage
Username: [redacted]
Password: [redacted]

Hostname: https://login.live.com/ppsecure/post.srf
Username: [redacted]ovi@hotmail.com
Password: [redacted]

Hostname: https://www.amazon.com/ap/signin
Username: [redacted]i@hotmail.com
Password: [redacted]

Hostname: https://login.uber.com/login
Username: [redacted]@gmail.com
Password: [redacted]

Hostname: http://192.168.0.254/
Username: [redacted]
Password: [redacted]

Hostname: https://login.yahoo.com/config/login_verify2
Username: [redacted]
Password: [redacted]

Hostname: https://my.roku.com/signin
Username: [redacted]i@hotmail.com
Password: [redacted]
```

Figure 4. Stolen usernames and passwords from compromised system.

The stolen credentials are stored in a “password.txt” file on the C&C server which contains the usernames, passwords, and associated URLs.

Session Cookies

Web servers often use cookies to store session state; that is to say, they signal to the server that a user has already successfully authenticated to the system. Stealing session cookies allows attackers to conduct session hijacking, allowing them to interact with the web server as the victim without ever having to provide credentials. Once that is accomplished, the attackers can inject malicious code into various web resources specific to the user account

and injected code can be distributed to large sets of users by sharing tampered resources. BlackGuard Infostealer exfiltrates web session cookies from browsers such as Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple’s Safari. Figure 5, shows how Blackguard Infostealer stores stolen cookies from the Chrome browser. The log file “*Cookies_Chrome2.txt*” contains the session cookie details along with the session key and the associated website.

```
[S cat Cookies_Chrome2.txt
www.googleadservices.com FALSE \ TRUE 1644287341.606948 AAAAAHQAAAAAYASCcqpMyrjkwitIAWo
3RUFJYU1Rb2JDaE1Jc0xHQjBZN245UULWQZlOM0NoMHVJUVIDRUFBWUFT pABzaX3gb4NmAEA
.facebook.com FALSE \ TRUE 1644287341.606948 d
.facebook.com FALSE \ TRUE 1644287341.606948 s
.yahoo.com FALSE \ TRUE 1644287341.606948 A1 5RMqSmG4FEgEBAQH8_mEHYgAAAAAA_eM
AAAcIiKv9YaGoww0&S=AQAAAsohEjQD7CW0p-wqNgzPxak
.yahoo.com FALSE \ TRUE 1644287341.606948 B 0
.casalemedia.com FALSE \ TRUE 1644287341.606948 AAA
.casalemedia.com FALSE \ TRUE 1644287341.606948
.casalemedia.com FALSE \ TRUE 1644287341.606948
.casalemedia.com FALSE \ TRUE 1644287341.606948 fdab2405a00&2d61fdab2405a0&5161f
dab2405a0&e661fdab242760&f161fdab2405a0&2761fdab240b40&69
.casalemedia.com FALSE \ TRUE 1644287341.606948
.uplynk.com FALSE \ TRUE 1644287341.606948 COM LmJ4aZo0GR92gkpsibFF~A~UP5421b46
6~860b~11ec~bcaf~02088ea4ee5c|expires_at=1651790375"
.yahoo.com FALSE \ TRUE 1644287341.606948 GUC
.amazon-adsystem.com FALSE \ TRUE 1644287341.6069 aFExWWE|t
.bidswitch.net FALSE \ TRUE 1644287341.606948
.yahoo.com FALSE \ TRUE 1644287341.606948 cmp
.bidswitch.net FALSE \ TRUE 1644287341.606948 5~6851574321f1
.bidswitch.net FALSE \ TRUE 1644287341.606948
.yahoo.com FALSE \ TRUE 1644287341.606948 ucs
.yahoo.net FALSE \ TRUE 1644287341.606948 A3 vNufUn6kFEgEBAQH8_mEHYgAAAAAA_eM
AAA&S=AQAAAjdr13~k9ua5MCKdEWkVyeQ
.gaana.com FALSE \ TRUE 1644287341.606948 AMP_
.advertising.com FALSE \ TRUE 1644287341.606948 bcaf~02088ea4ee5c
.analytics.yahoo.com FALSE \ TRUE 1644287341.6069 231y:175s~231y:175u~231y:175w~23
1y:1769~231y:17kh~231y:187s~231y:18p2~231y:18qt~231y:18vk
```



Figure 5 Stolen cookies and session data from a compromised system.

Browsing History

A user’s web browsing history provides useful information to attackers by showing the websites a victim will visit and their browsing preferences.² This information enables attackers to build a profile of the victim based on their behavior which allows them to conduct additional attacks, such as spear phishing emails based on the victim’s favorite sites. For this reason, BlackGuard steals and scrapes browser history from compromised systems. Figure 6 shows one such real-world example.



```

$ cat History.txt
### https://online.citibank.com/US/JPS/portal/Index.do ### (Banking with Citi | Citi.com) 1
### https://www.junglescout.com/ ### (0) 1
### http://www.administradoraintegralmargarita.com.ve/ ### (! Administradora Integral Margarita) 1
### http://www.di.fm/ ### (DI.FM - addictive electronic music) 1
### https://www.amazon.es/ ### (0) 66
### http://www.vrbo.com/ ### (VRBO) 1
### 0 ### (htt) 1
### http://ipims.com/ ### (ipims) 1
### 0 ### (0) 1
### http://www.cinema.bh/ ### (VIVA Cinema) 1
### http://www.eiu.com/ ### (EIU) 1
### http://wtffunfact.com/ ### (WTF Facts : funny, interesting & weird facts) 1
### 0 ### (https) 1
### http://www.franquiciator.es/page/2/?s=cafe ### (Buscó por el término cafe - Página 2 de 4 -) 1
### http://w20.bcn.cat/cartobcn/default.aspx?lang=en ### (CartoBCN) 1
### http://www.millennial-revolution.com/ ### (Millennial Revolution - Stop Working. Start Living.) 1
### http://www.mrmoneymustache.com/ ### (Mr. Money Mustache - Early Retirement through Badassity) 1
### 0 ### (http://scree) 1
### 0 ### (http://editor.wix.) 1
### http://www.openculture.com/freeonlinecourses ### (0) 1
### https://scrapconnection.com/features ### (Scrap Connection - features) 1
### http://www.hsbc.com.eg/1/2/eg/personal ### (HSBC Egypt) 1
### http://www.microchip.com/wwwproducts/en/ATSENSE101 ### (ATSENSE101 - Smart Energy SOC) 1
### 0 ### (http://www.splashlaundry.es/empresa-lavanderia-autoser) 1
### http://www.yahoo.com/ ### (Yahoo ahora forma parte de Verizon Media) 1
### 0 ### (https://secu) 1
### 0 ### (https://) 1

```

Figure 6. Stolen history details from the compromised system.

As you can see in Figure 6, the browsing history reveals a lot about the user's preferences. Blackguard Infostealer logs the history data from the browser and stores the collected data in the “*History.txt*” file. The file also contains a counter highlighting the number of times the user has visited a specific website.

Capturing Screenshots

BlackGuard Infostealer also captures screenshots from compromised systems at regular intervals. Screenshots of a user interacting with the system is common tactic used by attackers since they can reveal sensitive information about the user and present state of the system. This can result in personal information leakage, including addresses, credit card numbers, passwords, and more. One such example is presented in Figure 7 highlighting the user's actions and their installed applications.

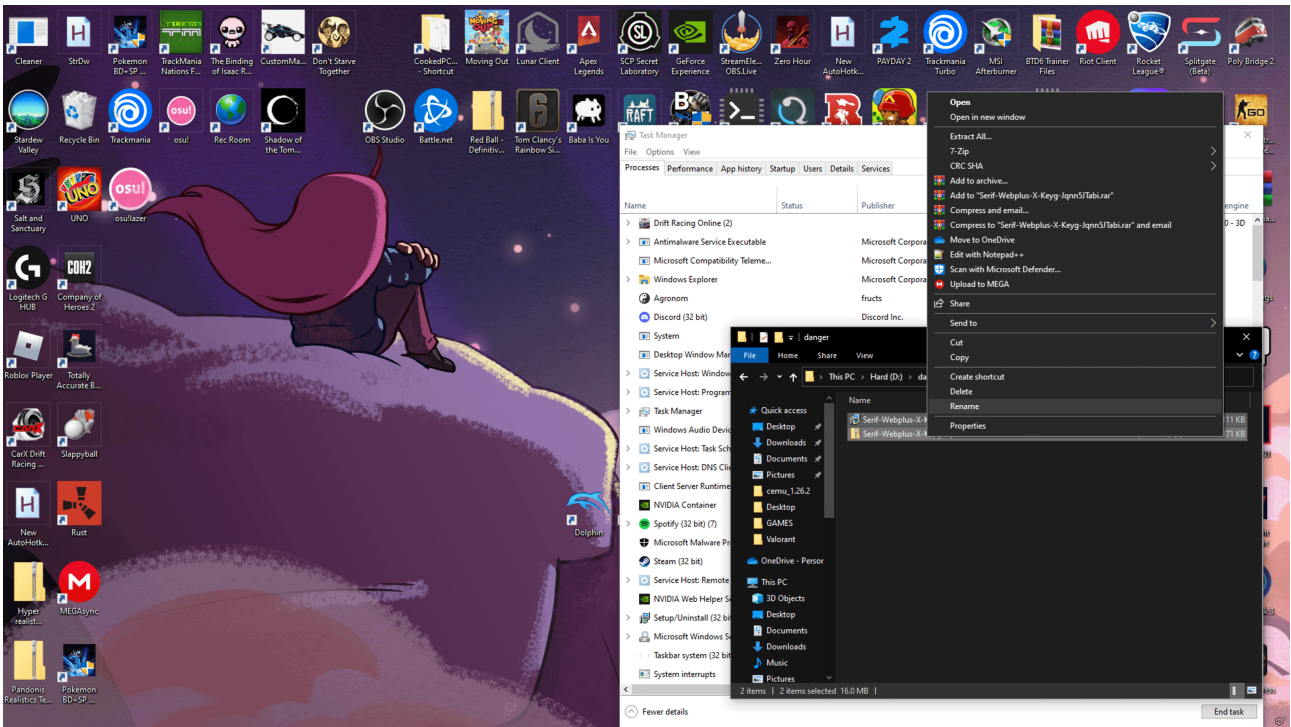


Figure 7. Screenshot of the desktop from the compromised systems.

Crypto Wallets

Perhaps Blackguard Infostealer’s most immediately impactful functionality is the ability to steal information from crypto wallets on infected systems. The malware scans the compromised system looking for crypto wallets for BitcoinCore, DashCore, Electrum, Ethereum, LitecoinCore, Exodus, and others. Before exfiltration, BlackGuard Infostealer creates a folder named “Wallets” to store the wallet information, and the complete “Wallets” folder is then compressed into a single zip file. Figure 8 shows an example of a stolen crypto wallet account (authentication tokens) from a compromised system.



```

$ ls
Browsers           Edge_Wallet       Messenger          UserAgent.txt
Chrome_Wallet     Files            Screen.Png        Wallets
Edge_Betta_Wallet Information.txt    Telegram
$ cd Wallets/Exodus/
[$ ls
info.seco          seed.seco         twofactor.seco
passphrase.json   twofactor-secret.seco
$ cat passphrase.json
[{"
  "passphrase": "Aayavi[REDACTED]2FCgxqg=",
  "system": true
}]
$ cd ../../Chrome_Wallet/
[$ ls
Chrome_Equal      Chrome_Metamask
$ cd Chrome_Metamask/
[$ ls
000005.ldb       000007.ldb       LOCK              LOG.old
000006.log       CURRENT          LOG               MANIFEST-000001
$ cd ../Chrome_Equal/
[$ ls
000005.ldb       000007.ldb       LOCK              LOG.old
000006.log       CURRENT          LOG               MANIFEST-000001
$ cay 000006.log
[-bash: cay: command not found
$ cat 000006.log
[;???
U'??Udata?{"AlertController":{"alertEnabledness":{"unconnectedAccount":true,"web3ShimUsage":true},"unconnectedAccountAlertShownOrigins":{},"web3ShimUsageOrigins":{},"AppStateController":{"browserEnvironment":{"t
rowser":"chrome","os":"win"},"collectiblesDetectionNoticeDismissed":false,"connectedStatusPopoverHasBeenShown":true,"defaultHomeActiveTabName":null,"fullScreenGasPollTokens":[],"notificationGasPollTokens":[],"popupGasF
ollTokens":[],"qrHardware":{},"recoveryPhraseReminderHasBeenShown":false,"recoveryPhraseReminderLastShown":1.644531094587e+12,"showTestnetMessageInDropdown":true,"trezorModel":null},"CachedBalancesController":{"cachedE
alances":{"0x1":{"0x2f58c156[REDACTED]ea244a870":"0x0"}}},"CurrencyController":{"conversionDate"

```

Figure 8. Stolen wallets data from a compromised system.

In Figure 8, we can see that BlackGuard Infostealer stole information about an Exodus crypto wallet and a Google Chrome wallet from the compromised system. Exodus provides desktop, mobile, and hardware-specific wallets that secure and manage cryptocurrency for the user.³ BlackGuard Infostealer steals crypto information from all the active wallets on the compromised system. In the example, the “*passphrase.json*” file was extracted from the compromised system which reveals the passphrase that can be used to recover the Exodus wallet. In addition, the associated log files contain configuration-related information and other files containing transaction-specific details.

Messaging Application Tokens and Logs

Blackguard can also steal information from various messaging applications on the compromised system. Targeted applications include Telegram and Discord. The malware creates associated directories with the same name as the messaging application to hold the stolen data and then exfiltrates this data. Figure 9 highlights a directory structure of the stolen Discord data.



```
[ $ ls
Browsers           Edge Betta_Wallet  Information.txt    Telegram
Chrome_Wallet     Edge_Wallet       Messenger         UserAgent.txt
Discord           Files             Screen.Png       Wallets
[ $ file Discord/
Discord/: directory
[ $ cd Discord/
[ $ ls
Local Storage     Tokens.txt
[ $ file *
Local Storage: directory
Tokens.txt:      ASCII text
[ $ file Local\ Storage\ leveldb/*
Local Storage/leveldb/000005.ldb:      data
Local Storage/leveldb/000256.ldb:      data
Local Storage/leveldb/000258.ldb:      data
Local Storage/leveldb/000261.ldb:      data
Local Storage/leveldb/000262.log:      data
Local Storage/leveldb/000263.ldb:      data
Local Storage/leveldb/CURRENT:        ASCII text
Local Storage/leveldb/LOCK:           empty
Local Storage/leveldb/LOG:            ASCII text
Local Storage/leveldb/LOG.old:        ASCII text
Local Storage/leveldb/MANIFEST-000001: PGP Secret Key -
[ $ cat Tokens.txt
NDcxNzg0NDQ1MTYzMjA4NzA1.DsKuvw.VQCKrUdw9MOjtQhKAQ8cwH-_aAw
```

Figure 9. Stolen Discord data from a compromised system.

Note that the “Tokens.txt” file contains a long string of alphanumeric characters. Discord generates this token when the user logs into the Discord server and uses it as an authorization code which is passed by the Discord client application to the server. BlackGuard Infostealer steals the authorization token which is then used to log into the victim’s Discord account. In addition, the malware acquires all many other Discord files from the system, including logs, and local application database entries. Similarly, Figure 10 shows how the Telegram messaging application data is exfiltrated and stored on the C&C server.



```

[$ ls
Browsers                Edge Betta_Wallet      Information.txt        Telegram
Chrome_Wallet           Edge_Wallet            Messenger              UserAgent.txt
Discord                  Files                  Screen.Png            Wallets
[$ cd Telegram/
[$ file *
4454EC55E9E19A100:      data
D877F783D5D3EF8C:      directory
D877F783D5D3EF8C0:     data
F5701E3EBFE845B61:     data
dumps:                  directory
emoji:                  directory
prefix:                 ASCII text, with no line terminators
settings1:              data
shortcuts-custom.json:  ASCII text
shortcuts-default.json: ASCII text
tdummy:                 directory
temp:                   directory
user_data:              directory
usertag:                ISO-8859 text, with no line terminators
working:                 empty
[$ cd user_data/cache/1
[$ ls
02    18    2A    3F    4F    69    7D    8B    9C    AA    C7    DC    EC
05    19    2D    42    51    6F    7E    8D    9E    AC    CC    DD    F3
0B    1B    30    45    54    74    7F    90    9F    AD    CD    DE    F7
11    20    32    48    58    75    80    93    A3    B0    D1    E5    FC
12    22    37    49    5B    76    81    95    A5    B7    D2    E6    FE
14    25    3D    4B    63    7B    85    98    A7    B9    D4    E9
17    29    3E    4C    66    7C    86    9B    A8    BD    D9    EA
$ █

```

Figure 10. Stolen Telegram data from a compromised system.

Conclusion

BlackGuard Infostealer is a powerful crimeware tool designed to steal the widest possible variety of personal data from a victim's device. The combination of stolen account credentials, cryptocurrency wallet information, session cookies, screenshots and messaging history indicates that the authors probably want to keep their options open in terms of monetizing the stolen data. In mid-June F5 Labs published Dor Nizar's analysis of the [Malibot Android malware](#), which also had the capability to exfiltrate a wide range of options and data types.

These new malware strains stand in contrast to more specific forms of malware such as [banking trojans](#), which tend to focus not just on a specific type of data, but on a specific set of banks (see, for example, the [list of targets for Qbot](#)). This raises questions about changing dynamics in the market for stolen data and monetization options for attackers. In the meantime, however, there can be no question that Blackguard Infostealer is not just a potent tool for cybercriminals, but also a quite versatile one. The implication is that defenders of all types need to understand its capabilities and how to detect it in order to manage the risk it presents.

Source: <https://www.f5.com/labs/articles/threat-intelligence/blackguard-infostealer-malware-dissecting-the-state-of-exfiltrated-data>