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.

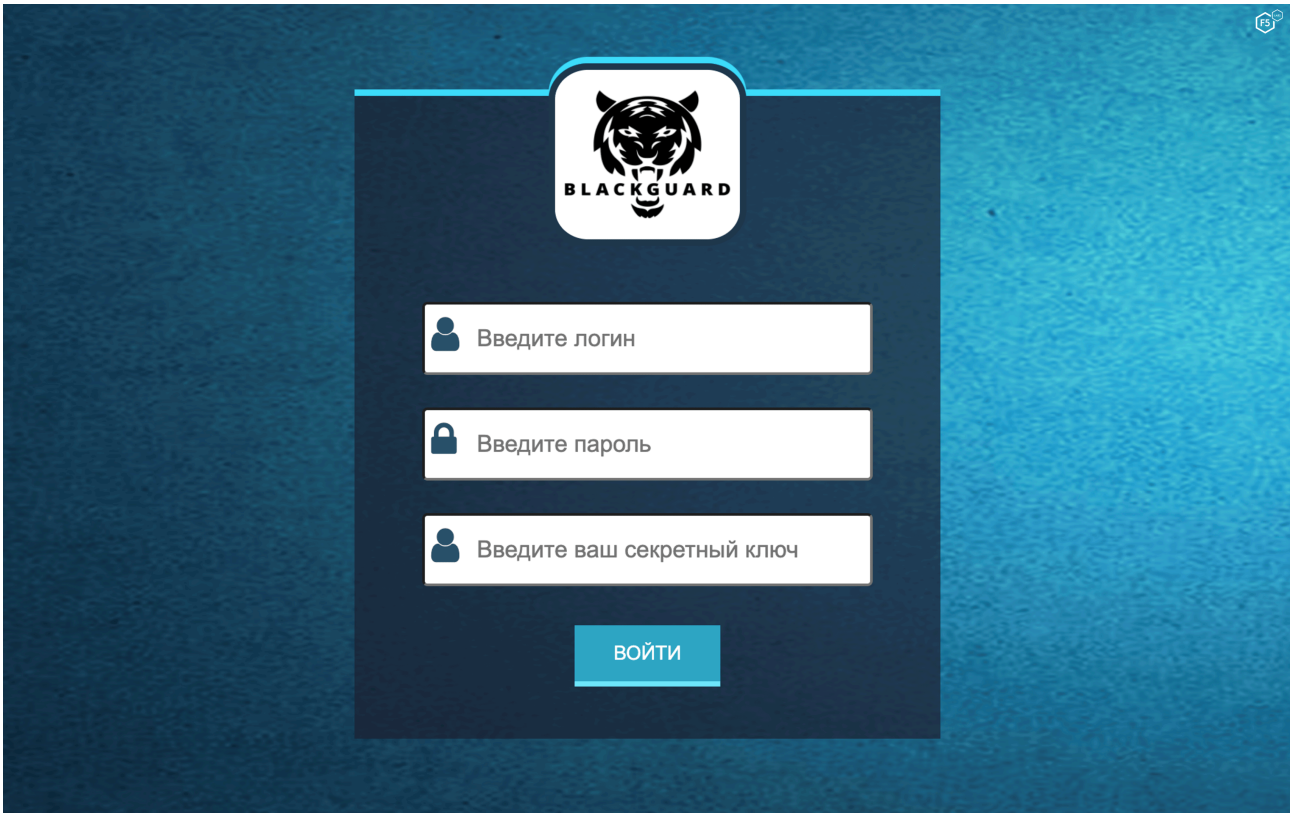

Figure 1. Blackguard malware administrative panel.

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 2highlights 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.

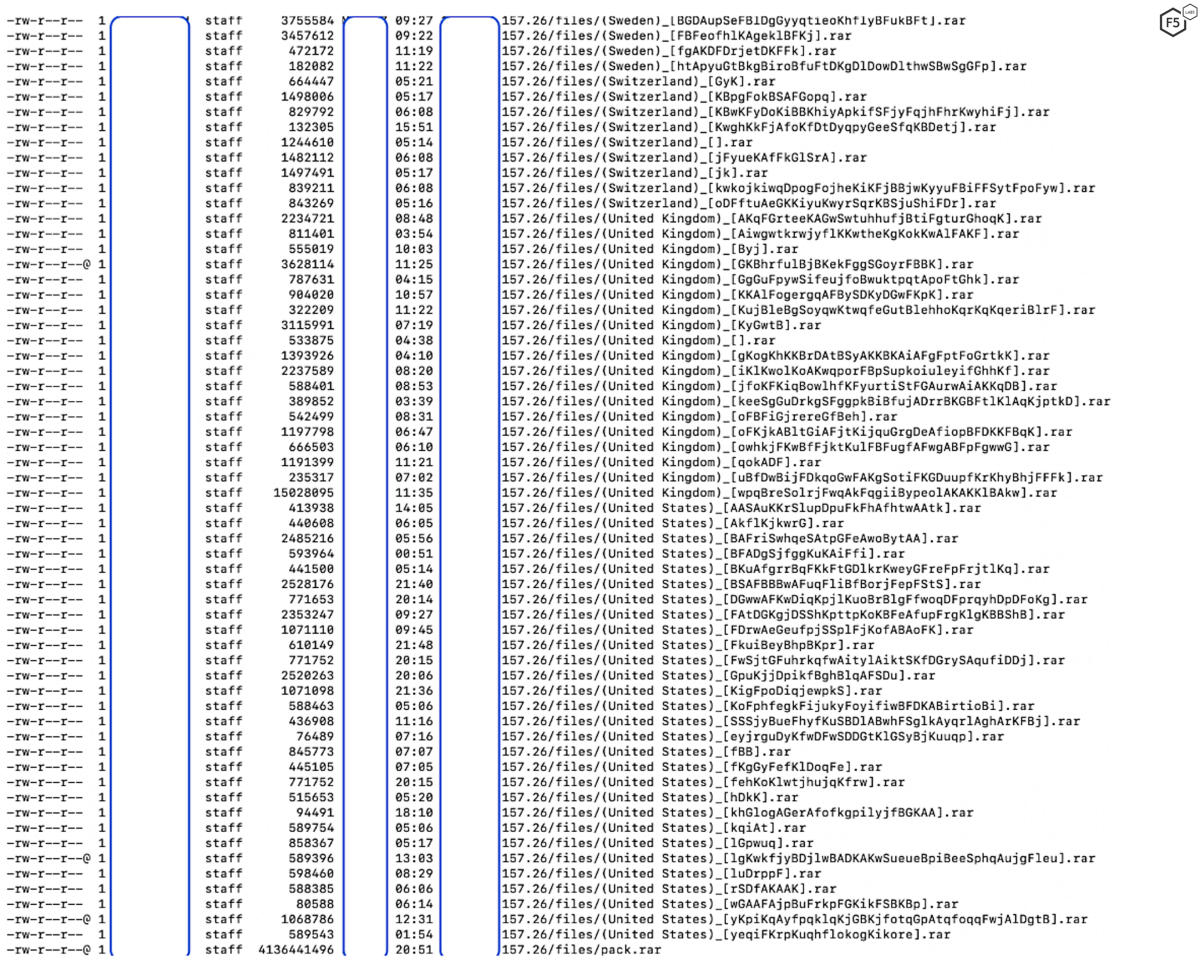

Figure 2. Data exfiltrated by blackguard and stored in a compressed format.

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.

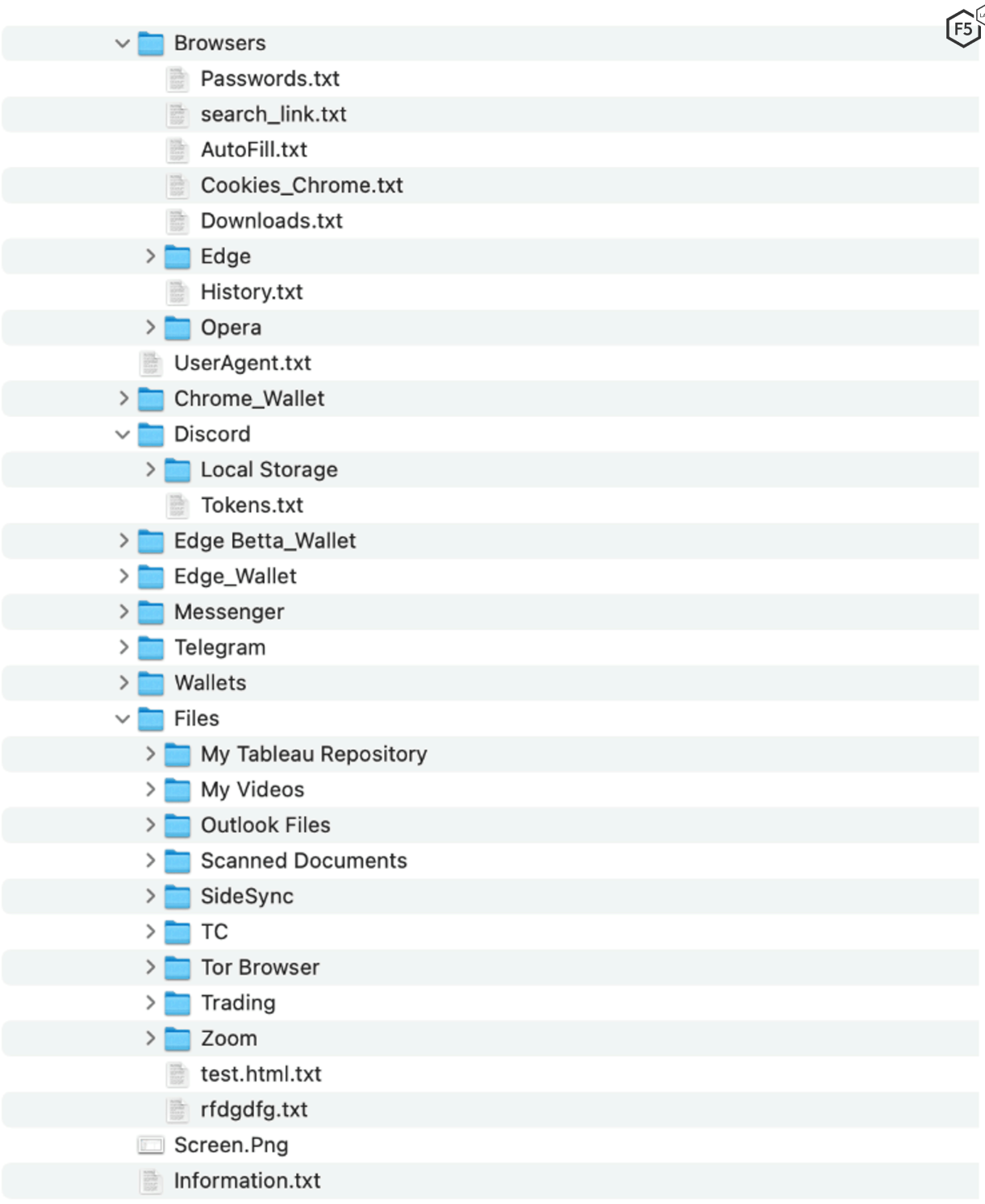

Figure 3. Directory structure used for storing stolen data.

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.

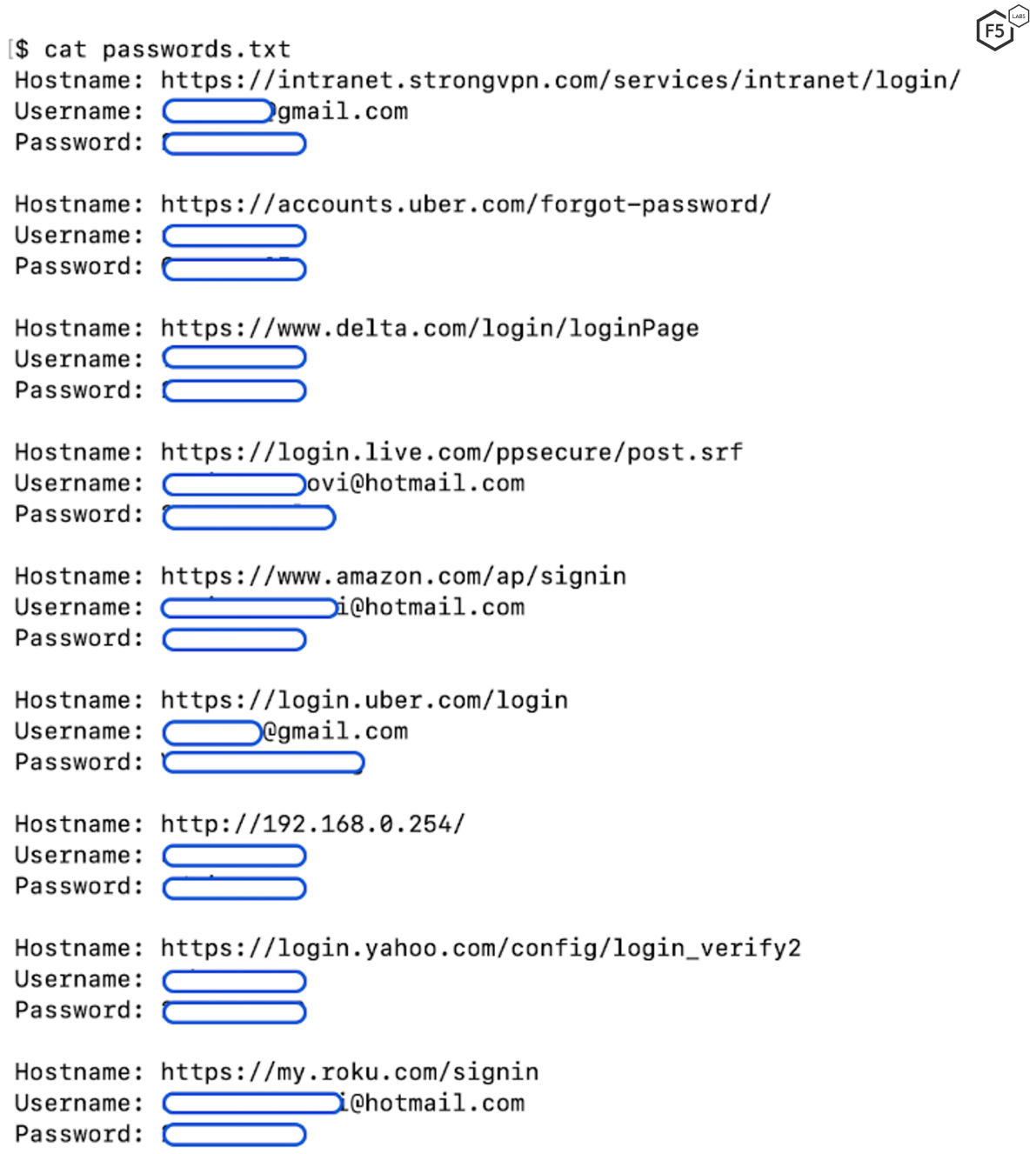

Figure 4. Stolen usernames and passwords from compromised system.

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 successful 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.

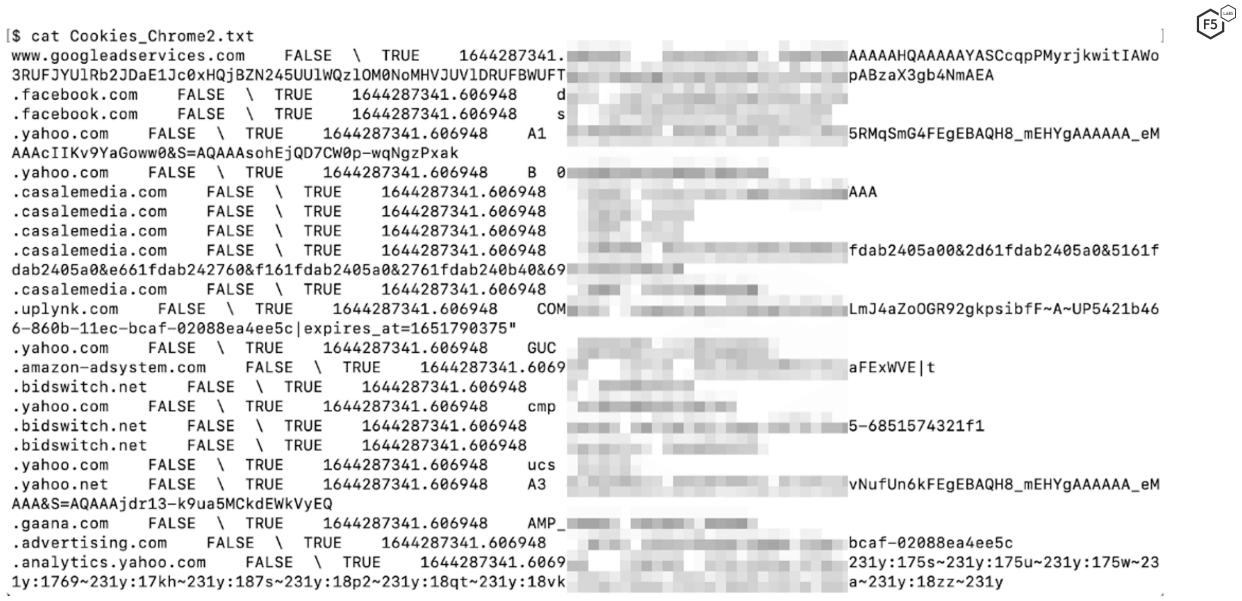

Figure 5 Stolen cookies and session data from a compromised system.

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.

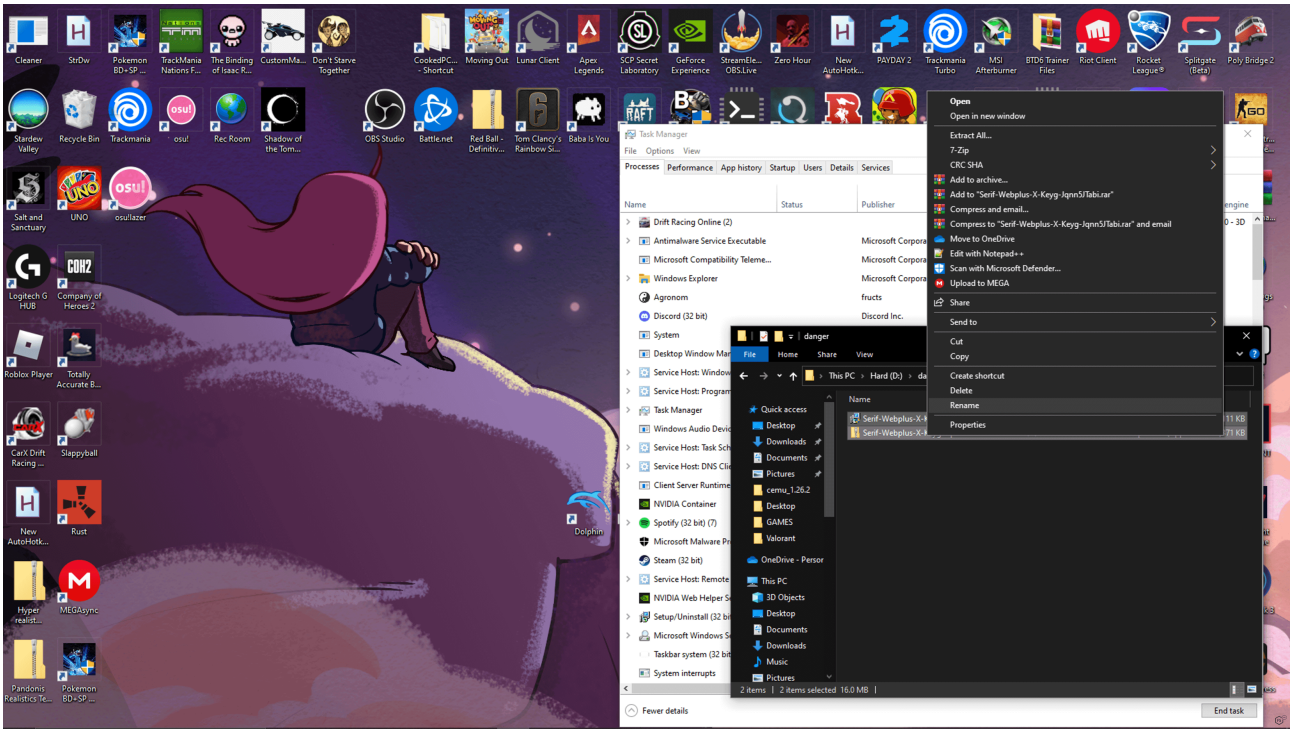

Figure 7. Screenshot of the desktop from the compromised systems.

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.

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.

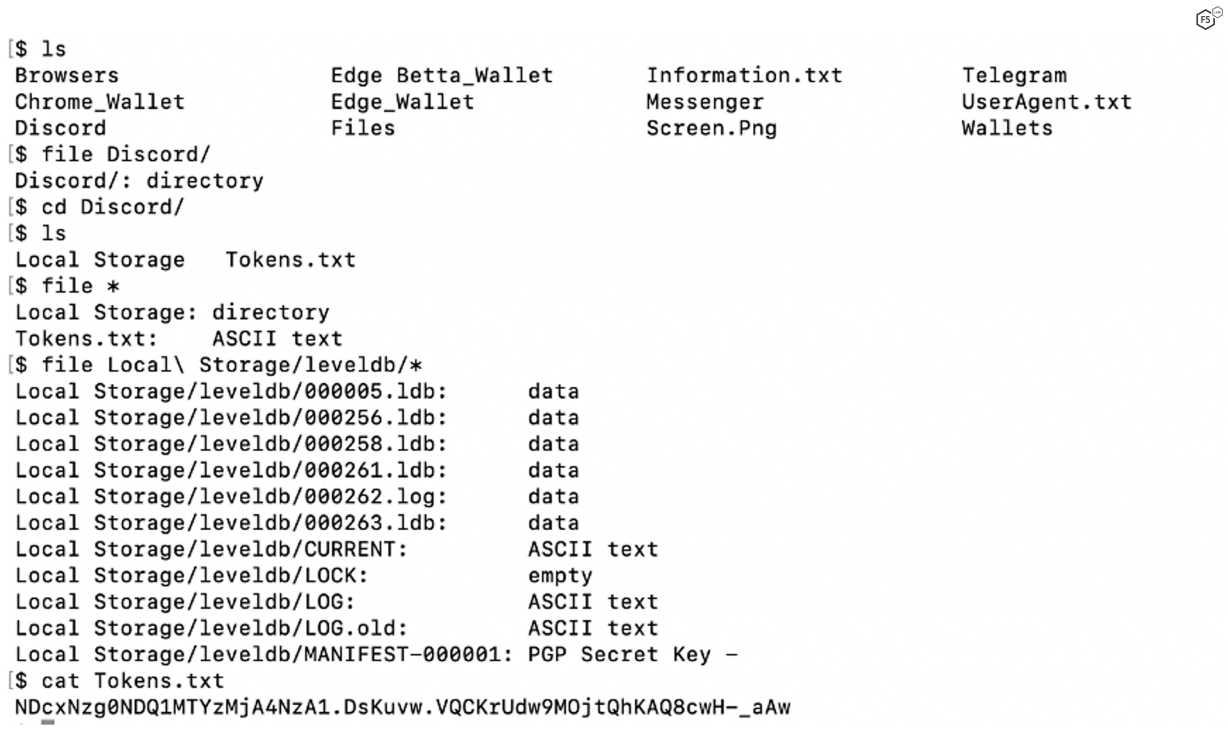

Figure 9. Stolen Discord data from a compromised system.

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.

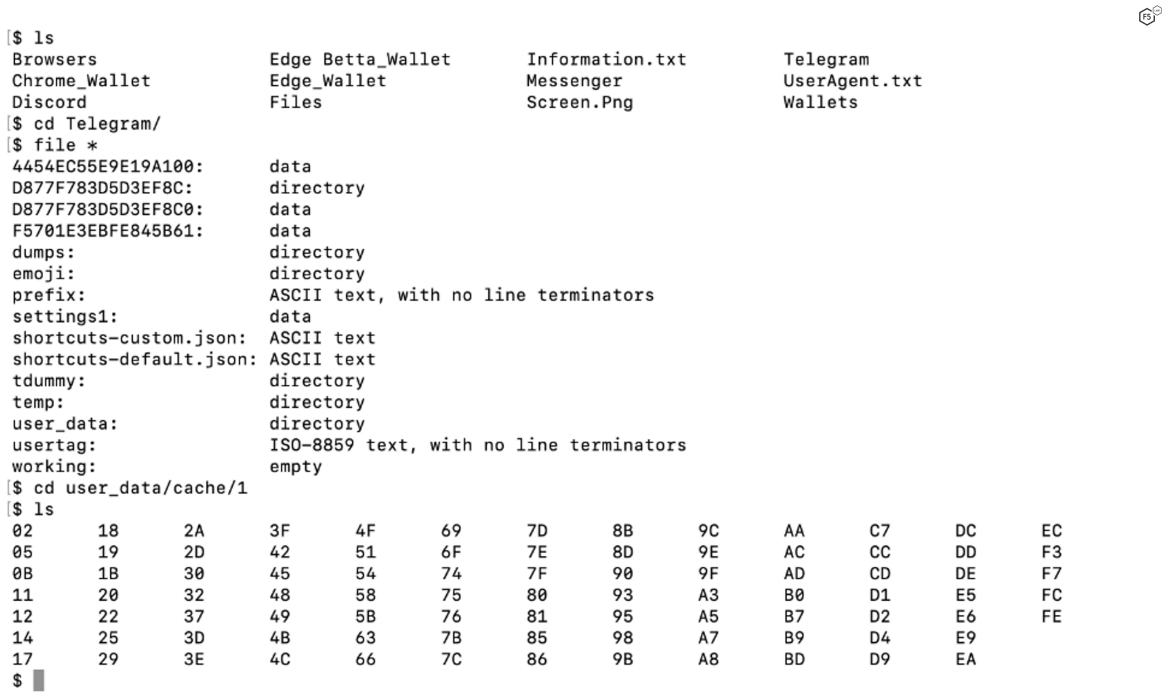

Figure 10. Stolen Telegram data from a compromised system.

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.
