

# Raccoon Stealer Announce Return After Hiatus

Ci [cyberint.com/blog/financial-services/raccoon-stealer/](https://cyberint.com/blog/financial-services/raccoon-stealer/)

August 15, 2023



## Introduction to Raccoon Stealer

First observed in 2019 and advertised (Figure 1) as a 'Malware-as-a-Service' (MaaS) threat on various cybercriminal forums, Raccoon is an information stealer targeting victim credentials and cryptocurrency wallets.



Seemingly favored by some threat actors due to its simplicity, the malware element of Raccoon omits advanced features, such as those used to evade detection, and instead focuses on the 'stealer' task in hand.

Whilst this approach requires those deploying the threat to utilize third-party tools for evasion, such as cryptors or packers to thwart signature-based detection, the ongoing popularity and apparent success of Raccoon suggests that this has not been a problem for many.

Lacking their own distribution method, in the past Raccoon incidents appear to have begun with the delivery of malicious document attachments sent via an indiscriminate unsolicited email (malspam) campaign. It was also reported that Raccoon malware had dropped using third-party exploit kits and other malware families.

Raccoon samples have been seen to mimic other executables although, based on their filenames, these have likely been distributed via sites hosting copyright-infringing materials which, in themselves, should be considered high-risk and be avoided.

Further leading to Raccoon's continued prevalence and success, those behind this MaaS offering are lauded for their high levels of service, and their management dashboard, much like the malware element, is reportedly straightforward and easy to use.

In 2019 Raccoon advertised on various cybercriminal forums with subscriptions available for \$499 (US) for four months, \$200 for one month and \$75 for a 'trial' week. The minimal outlay combined with a positive reputation appealed to many less sophisticated threat actors, especially given the potential return on investment (ROI) following the resale or abuse of stolen credentials and cryptocurrency wallets.

**But yesterday, Raccoon Infostealer announced its return after a hiatus of 6 months.**

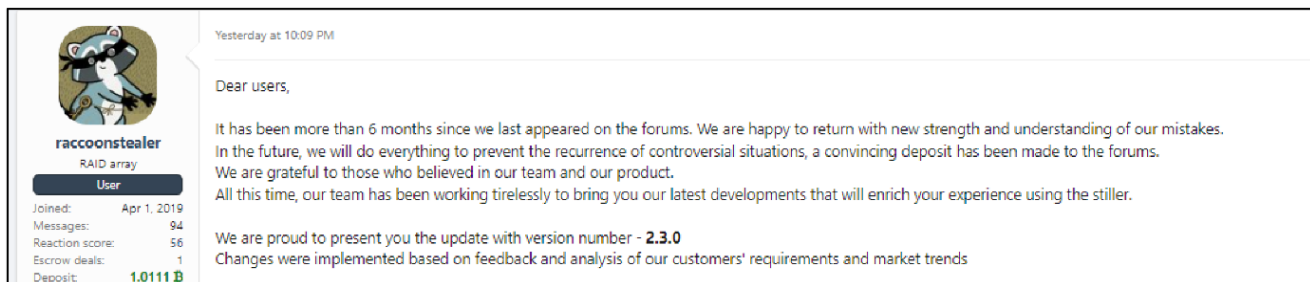


Figure 1: Raccoon Operator Post in a Hacking Forum

In October 2022, one of its main operators named, Mark Sokolovsky, responsible for the infrastructure of the Raccoon Infostealer, was arrested in the Netherlands with an extradition request from the United States due to its role in the operation of the Raccoon Infostealer's malware-as-a-service or "MaaS".

With his arrest, the FBI has collected data stolen from many computers that cybercriminals infected with Raccoon Infostealer. While an exact number has yet to be verified, FBI agents have identified more than 50 million unique credentials and forms of identification (email addresses, bank accounts, cryptocurrency addresses, credit card numbers, etc.) in the stolen data from what appears to be millions of potential victims around the world. The credentials appear to include over four million email addresses.

The arrest of Mark Sokolovsky caused the Raccoon Infostealer Operators to temporarily halt the operation for fear of being indicted. As mentioned above, the Raccoon Infostealer was one of the most famous and popular infostealer because of its relatively low price (USD\$75

weekly subscription and \$200 per month) and its promising features. Also known as “Racealer,” Raccoon Infostealer is used to steal sensitive and confidential information, including login credentials, credit card information, cryptocurrency wallets, and browser information (cookies, history, autofill) from almost 60 applications.

## New Features and Updates

---

1. **Quick search for cookies and passes** – The new Raccoon admin panel introduces a new way to search for URLs in the latest version. This means finding specific links in large datasets is now much faster, even when dealing with millions of documents and thousands of different links. The improvement is not just a minor upgrade – it’s a significant step forward and changes in how searches work for those who purchase Raccoon Malware, making them much quicker, even with huge amounts of data. This update aims to make it easier for Threat Actors to find the links they need, providing a new level of convenience.

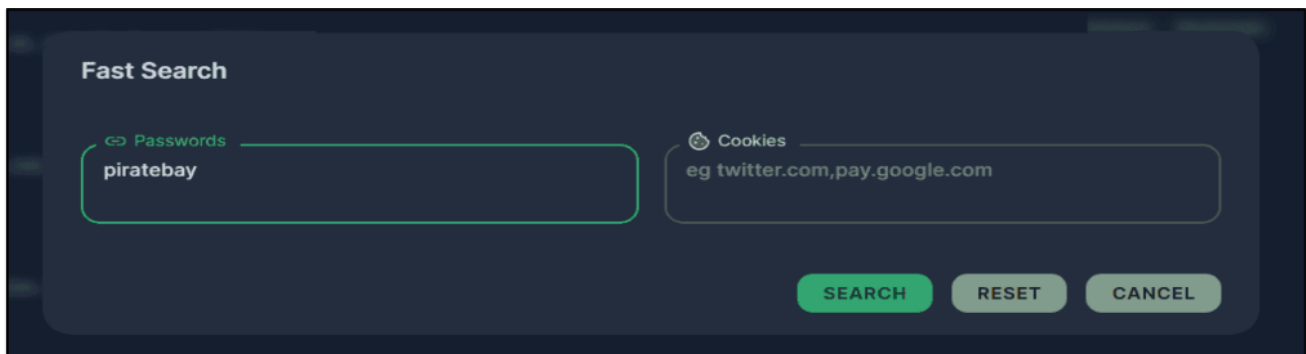


Figure 2: Raccoon Stealer Quick Search Module

2. **Automatic bot blocking and panel display** – A new system is now added to the infostealer to detect unusual activity patterns, such as multiple accesses from the same IP address or range. If this system identifies suspicious behavior, it automatically deletes records associated with those activities and updates the information on each client pad. This makes it harder for security tools that use automation and bots for the detection of malware.

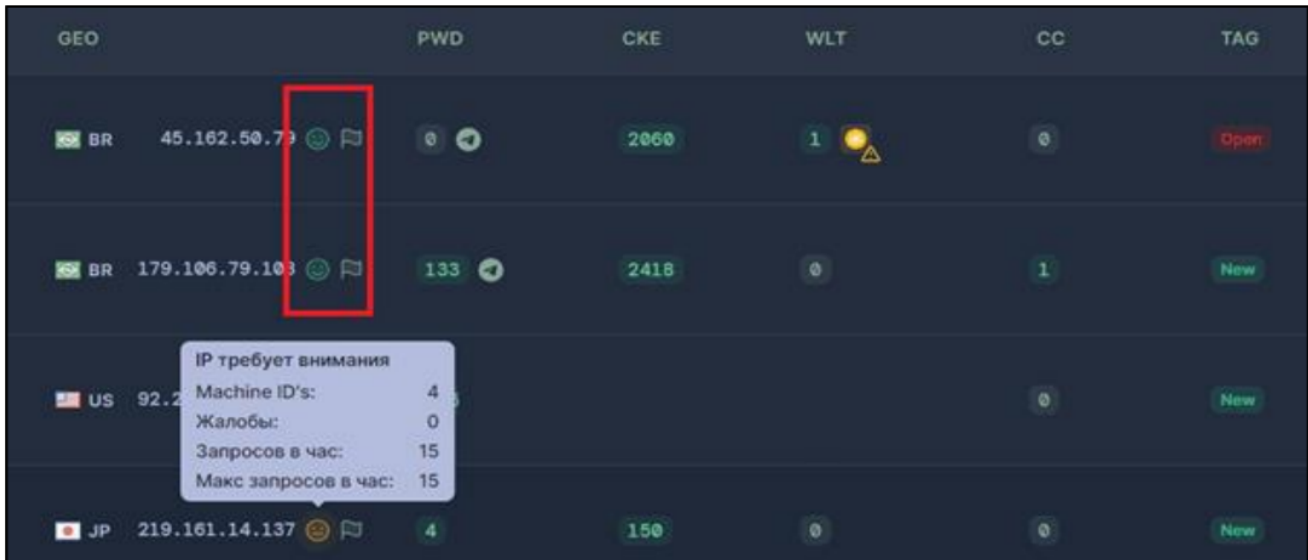


Figure 3: Raccoon Stealer Dashboard with Bot Blocking and Panel Display

Legend: Green Smiley = Activity of the IP is normal. Red Smiley = High probability that bots or other automated systems created or actively used the log.

**3. Reporting System** – This feature was added to block IP Addresses used by crawlers and bots often used by Security Practitioners to monitor Raccoon Traffic

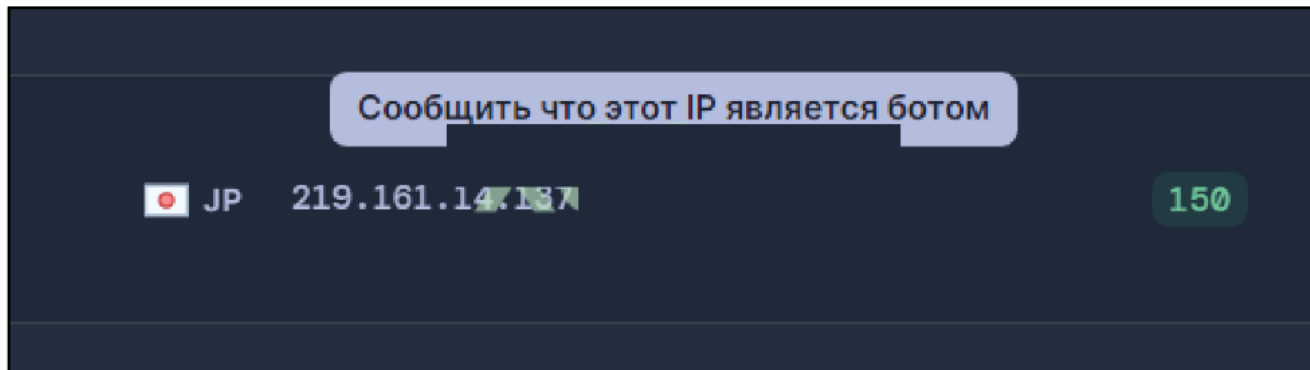


Figure 4: Raccoon Stealer Reporting System per IP Address

**4. Log Statistics** – With this, any Threat Actor who purchases the Raccoon Infostealer can see the top countries by the number of logs, as in the first versions of our stealer.



Figure 5: Raccoon Stealer Log Graph Feature

## Uncover your compromised credentials from the deep and dark web.

Fill in your business email to start.

### Raccoon Stealer Behavior and Capabilities

Raccoon targets a wide range of applications and uses specific techniques to extract and harvest data from those applications.

Additionally, it is observed that Raccoon performs the same procedure to extract data from its

targeted applications:

- Extract the application file that contains the sensitive data.
- Copy the file to a specific folder (%Temp%).
- Create and write a text file to the target application's folder with the stolen information.

To obtain and decrypt credentials from applications, Raccoon acquires and downloads the DLLs

associated with those applications.

## Raccoon Stealer Target Applications

### Browsers:

- 
- Google Chrome
  - Comodo Dragon
  - Amigo
  - Orbitum
  - Bromium
  - Nichrome
  - RockMelt
  - 360Browser
  - Vivaldi
  - Opera
  - Sputnik
  - Kometa
  - Uran
  - QIP Surf
  - Epic Privacy
  - CocCoc
  - CentBrowser
  - 7Star
  - Elements
  - TorBro
  - Suhba
  - Safer Browser
  - Mustang
  - Superbird
  - Chedot
  - Torch
  - Internet Explorer
  - Microsoft Edge
  - Firefox
  - WaterFox
  - SeaMonkey
  - PaleMoon

### **Email Clients:**

---

- ThunderBird
- Outlook
- Foxmail

### **Cryptocurrency:**

---

- Electrum
- Ethereum
- Exodus
- Jaxx
- Monero
- Bither

After successfully extracting data and information, Raccoon gathers all the files and collects it to a newly created folder by the malware itself called “Log.zip”. Afterward, the file is sent to its configured C&C server, removing all its infection traces.

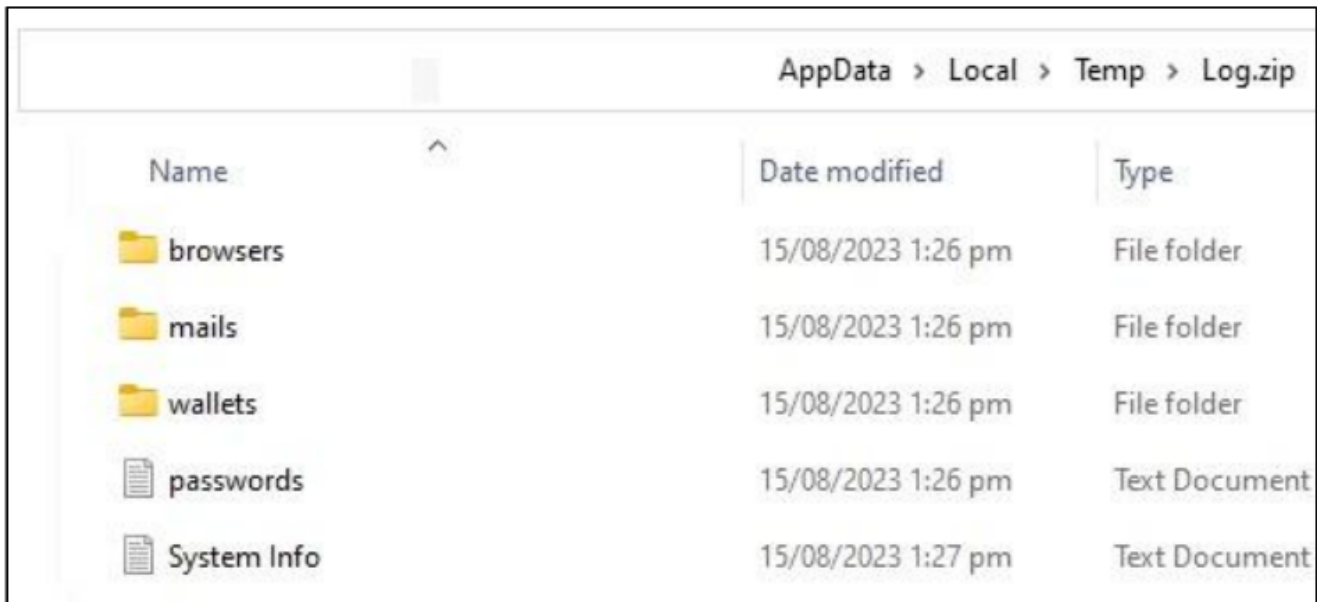


Figure 6: Log.zip Folder Created by Raccoon to Store Stolen Information

The resurgence of the well-known infostealer group “Raccoon” following a hiatus has triggered alarm

in the cyber security landscape, particularly within the financial sector. The return of Raccoon highlights the potential danger for industries like finance, which are prime targets for data breaches and financial fraud.

## Raccoon Stealer Control Panel

Hosted on a Tor onion service, Raccoon subscribers have access to a centralized control panel from which they can generate and/or manage campaign configurations, build Raccoon malware payloads, and view data stolen from victims.

Displayed in English by default, although also available in Russian, visitors to the control panel are prompted to log in using the username and password (Figure 2) they presumably received when subscribing.

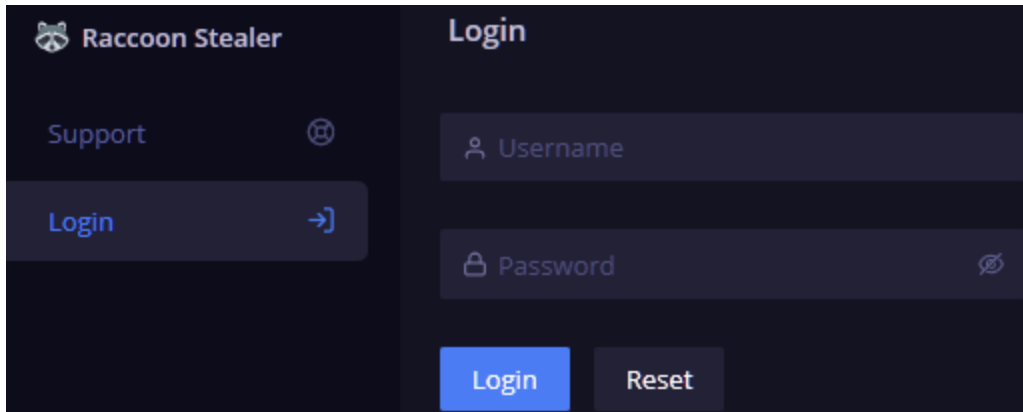


Figure 7 – Dashboard login

Visitors can also view the Support page, without authentication, that provides both Jabber and Telegram contact details for those who are behind this MaaS threat (Figure 8).

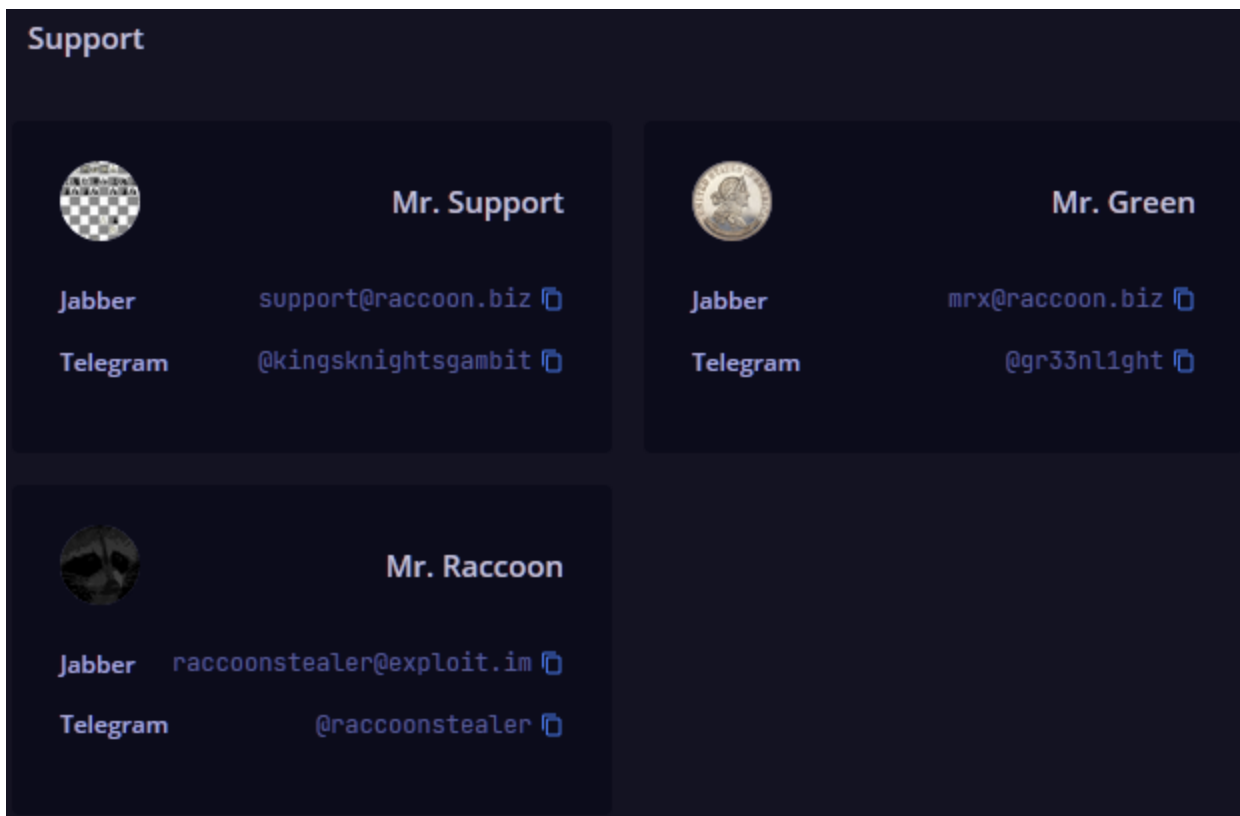


Figure 8 – Support contacts

Given the inability to purchase access through this official control panel, threat actors seeking access would presumably need to initiate contact with the Raccoon team, via their forum posts or using the contact details above to ‘subscribe’.

Although access to this control panel requires an active Raccoon subscription and credentials, screenshots previously shared by the threat actor provide an insight into its interface and functionality based on the available menu options (Figure 9)



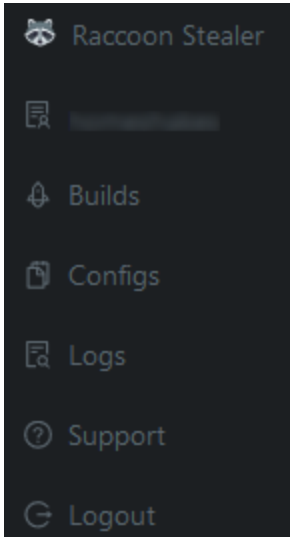


Figure 9 – Menu options

Notably, the control panel makes use of JavaScript resources (Figure 10) that can be accessed without authentication and allows some of the current functionality to be determined, including features that would likely require administrative access.

```
var l = this.webpackJsonpraccoon_frontend = this.webpackJsonpraccoon_frontend || [],
    a = l.push.bind(l);
l.push = r, l = l.slice();
for (var c = 0; c < l.length; c++) r(l[c]);
var i = a;
t()
}([])
</script>
<script src="/static/js/2.21d0e99c.chunk.js"></script>
<script src="/static/js/main.c06a8983.chunk.js"></script>
</body>
</html>
```

Figure 10 – Control panel HTML including the ‘revealing’ JavaScript resource

In addition to this, the JavaScript exposes text related to the user agreement and FAQ sections, both of which are provided within the appendices for reference.

## Administrative Options

---

Based on an analysis of the exposed JavaScript resource, the following additional menu options appear to be available to Raccoon’s administrators:

- All logs
- All statistics
- News

Proxies

Users

Potentially leaving a subscriber unaware of their malware deployment's success, code references related to the 'All logs' and 'All statistics' options appear to provide Raccoon administrators with the ability to access and/or delete data processed by the platform.

Theoretically allowing administrators to have their pick of any victim data, it would likely be naive to think that this would not be the case and may therefore be one cost of doing business with other cybercriminals, especially given the adage that there is no honor amongst thieves.

Commonly used for anonymization, even though the intent is not obvious from the JavaScript (Figure 11) and may be related to their gate infrastructure, the 'Proxy' option enables Raccoon administrators to add, remove and test proxies, including running checks against 'VT' (presumably VirusTotal) as well as assigning them to and from users.

```
s.r(u), s.d(u, "readProxies", (function () {
    return ic
})), s.d(u, "toggleProxyActive", (function () {
    return rc
})), s.d(u, "addProxyComment", (function () {
    return nc
})), s.d(u, "testProxy", (function () {
    return cc
})), s.d(u, "vtCheck", (function () {
    return lc
})), s.d(u, "addProxyToUser", (function () {
    return dc
})), s.d(u, "removeProxyFromUser", (function () {
    return uc
})), s.d(u, "generateUserHash", (function () {
    return pc
})), s.d(u, "testCloudGate", (function () {
    return hc
})), s.d(u, "updateCloudLink", (function () {
    return jc
})), s.d(u, "addProxy", (function () {
    return bc
})), s.d(u, "removeProxy", (function () {
    return mc
}));
```

Figure 11 – Proxy functionality available to control panel administrators

Given that the Raccoon malware component does not appear to upload stolen data directly to this Tor onion site, it is possible that the proxy configuration is used to mask the exfiltration process to intermediate infrastructure, although, without further analysis, this is currently speculation.

Finally, the remaining administrative options are likely more self-explanatory with the 'News' option facilitating the creation of news articles or notifications and the 'Users' option providing subscriber management.

## Statistics/Account

Likely displayed upon login and the default page for a subscriber visiting the control panel, the Statistics panel provides an at-a-glance overview of active campaigns (Figure 12).

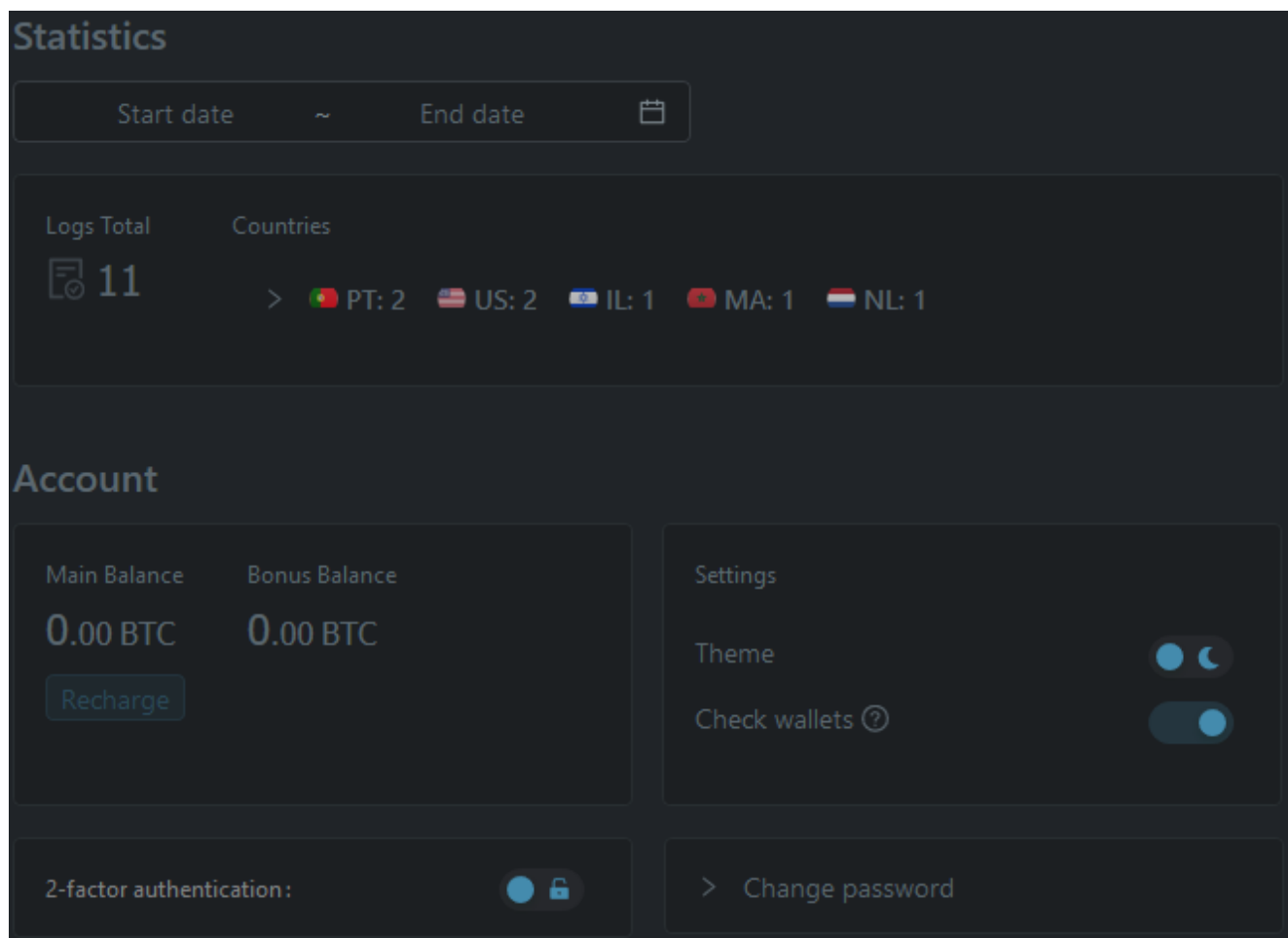


Figure 12 – Management control panel 'Statistics' and 'Account'

Additionally, the Account section displays the current Main and Bonus balances, likely related to subscription funds, alongside options that allow the control panel interface to be switched between light and dark modes, the configuration of two-factor authentication, and a password reset function.

Notably, the 'Check wallets' option visible in the screenshot does not appear to be referenced by the current JavaScript resource and may have been removed. Whilst vague, this option may have provided the ability to determine the value of stolen cryptocurrency wallets, such as via public blockchain services, although with an increase in targeted currencies it may no longer be relevant.

## Logs

Seemingly enhanced since Raccoon's initial release, victim data presented within a legacy screenshot (Figure 13) is consistent with the malware's current capabilities but lacks additional columns identified from an analysis of the currently deployed JavaScript resource.

	GEO	IP	PWD	CKE	WLT	STA	DAT	COM	GET	ACT
<input type="checkbox"/>	efi N/A	0.0.0.0	85	1491	0	Open	2019-04-07 12:40:25		1.4MB	
<input type="checkbox"/>	AE	94.██████████	82	3178	0	Open	2019-04-07 11:11:47		359.0KB	
<input checked="" type="checkbox"/>	VN	113.██████████	45	3173	0	New	2019-04-07 13:26:57		1018.2KB	
<input checked="" type="checkbox"/>	SA	5.██████████	35	1645	0	New	2019-04-07 12:58:03		189.9KB	

Figure 13 – Management control panel 'Logs'

Based on the current control panel, it appears that the 'Logs' table now shows the following headers:

GEO – Country code based on victim IP address geolocation.

IP – Victim IP address.

USR – Implies 'username' but may be another unique victim identifier (references 'bot\_id').

UTC – Victim system time.

UA – Victim browser user-agent strings.

PWD – Number of acquired victim passwords.

CKE – Number of acquired victim cookies.

CC – Number of acquired victim credit card details.

WLT – Number of acquired victim cryptocurrency wallets.

TAG – Likely a user-customizable tag feature.

DAT – Potentially identifies date/time the data was acquired (references 'create\_data\_unix').

USR – Seemingly duplicated header displaying the victim's username.

COM – Customizable comment field.

GET – Displays the exfiltrated file size and allows the Zip archive to be downloaded.

ACT – Additional 'actions' including the ability to delete the stolen data.

A comprehensive search capability is also provided within the Logs section (Figure 14) that, given the presence of an `elasticsearch_id` string within the JavaScript, may indicate that the control panel is using Elasticsearch to store stolen data.

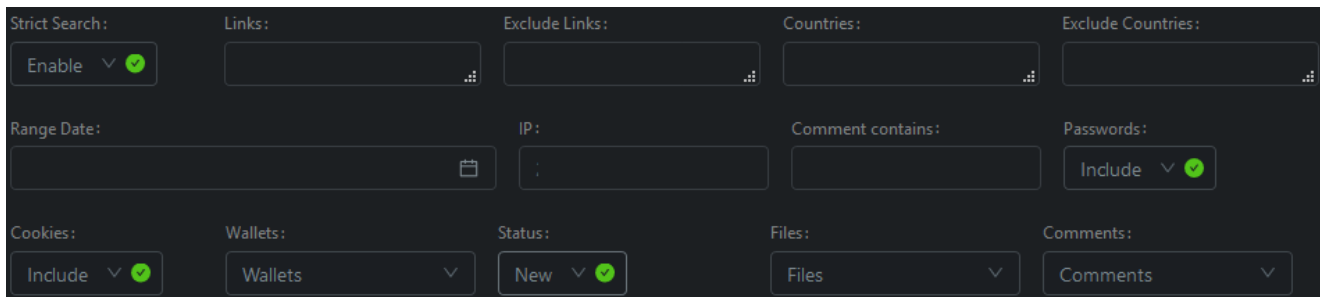


Figure 14- Log search capability

## Builds/Config

Undoubtedly used to configure and create Windows executables that contain the Raccoon stealer payload, the JavaScript resource provides an indication of the functionality present in the Builds and Configs sections of the control panel.

Based on the FAQ, subscribers have the ability to generate a single build, although multiple configurations are supported as these can be updated and downloaded from the C2 infrastructure mid-campaign. In addition to preventing subscriber abuse, such as account sharing or usage after license expiration, this eliminates the need for subscribers to rebuild their payload after making subtle configuration changes.

Having assigned a name to their configuration, the following options can be set:

Screenshots – Disabled by default; takes a screenshot of the victim desktop.

Browser history – Disabled by default; gathers 1,000 lines of recent web-browser history.

Self removal – Automatically removes Raccoon stealer after data exfiltration.

File loader URLs – Download and execute additional payloads on the victim host after data exfiltration.

Additionally, 'file grabber rules' can be configured to allow collection and exfiltration of files from victim hosts based on the following conditions:

Path – Starting directory on the victim host from which to start the 'file grabber'; for example: `C:\`.

Mask – Comma-delimited list of filename masks including wildcards; for example: `*.doc, *.xls`.

Size Limit – Maximum size per file (up-to 100mb), in kilobytes; for example 150kb would be: `150`.

Exceptions – Directories, within the specified path, to excluded from searches, for example: `\Windows\`.

Subfolders – Presumably enabling or disabling searches within subdirectories.

Shortcuts – Collect matching files referenced by shortcuts; for example, `file.doc.lnk` would download the corresponding `file.doc`.

After defining and selecting a configuration, the build process allows the creation of either a dynamic link library (DLL) or executable (EXE) that would enable the threat actor to deliver and launch the payload using their preferred method.

As a somewhat professional touch, and likely contributing toward the positive opinion of Raccoon, a test feature allows this newly built payload to be tested in a virtual machine maintained by the Raccoon team. Presumably used to check that the payload successfully executes and communicates with the C2 infrastructure, the conclusion of this test reportedly results in a notification being sent to the subscriber via the control panel.

Consistent with many other Russian-language cybercriminal threats, attention is drawn to the fact that Raccoon stealer will not function on victim hosts that are determined as being within the Commonwealth of Independent States (CIS) based on their system locale (language) or IP address. Subscribers are also reminded to 'crypt' their builds to evade detection and to 'keep in mind' that long-term use could increase the chances of detection (Figure 15).

```
buildAttentionTextMainPart2: "Note that Build will not work on systems related to CIS.",  
[...]  
updateBuildP2: "And you need to crypt updated build.",  
[...]  
keepInMindConfigForm: "Keep in mind that the more files you rob or download, the longer stealer  
runs, which can directly affect the detection in runtime.",
```

Figure 15 – Build/Config warnings

## Raccoon Stealer Payload

---

Having tested and secured their payload, the threat actor will need to deliver Raccoon to would-be victims.

Based on observations of recent activity, many appear to favor using malicious document attachments sent via unsolicited email (malspam) campaigns, potentially linked to the use of third-party exploit kits or other malware families, as well as Raccoon payloads being uploaded to file-sharing sites, such as those hosting copyright-infringing materials, and/or mimicking other executables.

## Command & Control

---

Based on the intelligence gathered from the Raccoon Stealer control panel, each payload will attempt to communicate with some seemingly benign or legitimate URL from which an encrypted string is gathered and processed to obtain the true command and control (C2) URL, typically comprised of an IP address and potentially a `/gate/log.php` resource.

As detailed in a February 2020 analysis, Raccoon previously hid this C2 server address in an encrypted string that posed as a filename hosted on Google Drive, even though this is seemingly no longer the case.

Based on analysis of recent payloads, Raccoon currently communicates with websites offering Telegram URL shortening services. Upon access, the profile overview of a threat actor-controlled Telegram user is displayed (Figure 16) with the 'description' field containing an encrypted C2 string.

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

**jiocacossa**

5 subscribers

e93dbWZ/aL2zyum33P+dw4kLEHlIkYgNdQ  
==da-v4d

VIEW IN TELEGRAM

Preview channel

Figure 16 – Example Telegram user details

Parsing this HTML response, Raccoon locates the encrypted C2 URL by locating the preceding string `description" dir="auto">` (Figure 17).

```
<div class="tgme_page_extra">5 subscribers</div>
<div class="tgme_page_description" dir="auto">e93dbWZ/aL2zyum33P+dw4kLEHlIkYgNdQ==da-v4d</div>
<div class="tgme_page_action">
  <a class="tgme_action_button_new" href="tg://resolve?domain=jiocacossa">View in Telegram</a>
</div>
```

Figure 17 – Telegram user details HTML (Yellow: element search; Red: encoded string)

While this feature allows the C2 servers to be easily updated, the use of third-party Telegram URL shortening services rather than the legitimate service (`https://t[.]me/<GROUP|USER>`) allows defenders to detect and block anomalous behavior, especially given the low-reputation domains that these are hosted on.

Having decrypted and decoded the encrypted C2 URL, using its own XOR cipher routines, Raccoon calls home via a HTTP POST containing three parameters hidden in a base64 encoded and RC4 encrypted string (Figure 18):

**b=** – Bot identifier, comprised of the victim ‘machine GUID’, as found in the Windows registry, an underscore and the victim username.

**c=** – Configuration identifier, a hexadecimal string or hash that refers to a specific threat actor’s configuration.

**f=** – Configuration file format, only observed as being set to ‘JSON’.



## Figure 18 – Example C2 HTTP POST

In response, the C2 server sends a JSON configuration, also base64 encoded and RC4 encrypted with the same passphrase, containing the following values (Figure 19):

`_id` – Identifier, potentially related to the threat actor or some combination of victim and/or configuration.

`au` – Previously known as `attachment_url`, specifies the C2 path containing supporting files used by the Raccoon payload such as `sqlite3.dll`.

`ls` – Previously known as `libraries`, supporting files for the Raccoon payload.

`ip` – Victim IP address.

`location` – Victim IP geolocation, contains `country`, `country_code`, `state`, `state_code`, `city`, `zip`, `latitude` and `longitude`.

`c` – Previously known as the `config` section, contains:

`m` – Previously known as `masks`, specifies any file search masks used for data theft.

`lu` – Previously known as `loader_urls`, specifies any additional payloads to be downloaded and executed after the conclusion of Raccoon's data exfiltration.

`lu` – Seemingly a second `loader_urls` value.

`rm` – Disables (0) or enables (1) the self-removal feature.

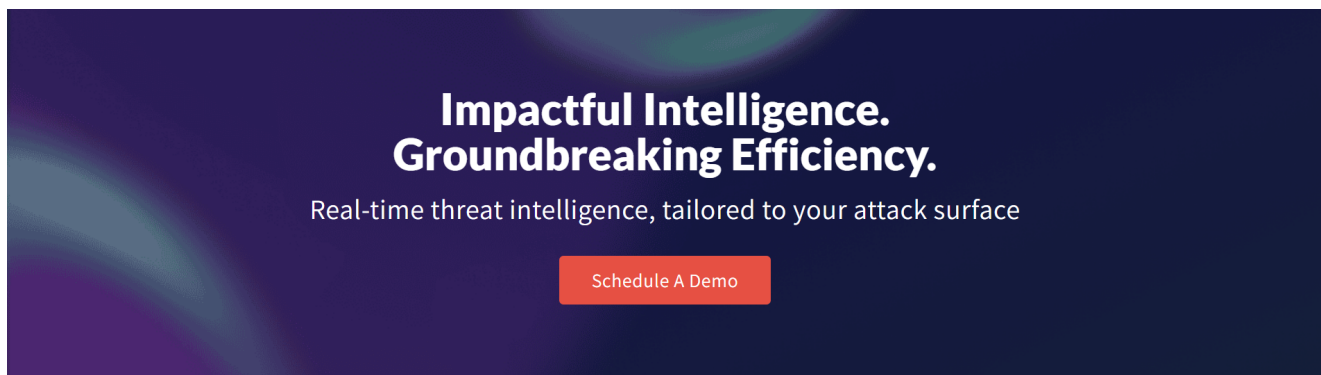
`is_screen_enabled` – Disables (0) or enables (1) the screenshot feature.

`is_history_enabled` – Disables (0) or enables (1) the browser history acquisition feature.

`depth` – Undetermined, potentially a path depth used to limit the file search mask feature.

```
{
  "_id": "fDzID3kBuI_ccNKoWUKn",
  "au": "/1/f/fDzID3kBuI_ccNKoWUKn/ca34e820510993f7ae8aad17dc28303b9efdb779",
  "ls": "/1/f/fDzID3kBuI_ccNKoWUKn/a6e8c6aec5447a4238f15ce1adf79b22d25bf002",
  "ip": "100.75.77.5",
  "location": {
    "country": "United Kingdom",
    "country_code": "GB",
    "state": null,
    "state_code": null,
    "city": null,
    "zip": null,
    "latitude": 51.5074,
    "longitude": -0.1278
  },
  "c": {
    "m": null,
    "lu": null
  },
  "lu": null,
  "rm": 1,
  "is_screen_enabled": 0,
  "is_history_enabled": 0,
  "depth": 3
}
```

Figure 19 – Example C2 response



**Impactful Intelligence.  
Groundbreaking Efficiency.**

Real-time threat intelligence, tailored to your attack surface

[Schedule A Demo](#)

## Data Theft

---

Raccoon stealer can extract credentials, cookies and payment card data from a number of applications including the following as identified from recently analyzed samples:

Browsers: Google Chrome, Mozilla Firefox, Opera and those that are Chromium-based including Microsoft Edge.

Cryptocurrency Wallets: Electron Cash, Electrum-LTC, Ethereum, Exodus, Guarda, Jaxx Liberty, MetaMask and MyMonero

Notably, to gather other cryptocurrency wallets, Raccoon also searches for the commonly used filename `wallet.dat`.

Utilizing dynamic link libraries (DLL) downloaded from C2 paths specified in the JSON configuration and saved to `%USERPROFILE%\AppData\LocalLow\`, supporting files allow access to data stored by the targeted applications. For example, recent campaigns have been observed as deploying the legitimate SQLite file `sqlite3.dll` allowing access to browser data stored within SQLite databases.

In addition to data theft, Raccoon gathers system information that is saved in a file named `machineinfo.txt` and includes details of the build version, operating system, hardware and installed applications (Figure 20).



Presumably confirming the upload, the server responds with a forty-character hexadecimal string, potentially some SHA1 hash or checksum, before allowing Raccoon to act on any final configuration such as self-removal or the download and execution of additional payloads.

## Additional Payloads

Given the file loader capability provided by Raccoon, it is possible for a threat actor to initiate the download and execution of additional payloads once the stealer has completed its data exfiltration.

While these payloads will undoubtedly change depending on each threat actor's requirements, recent observations include the deployment of additional malware, such as those used to gain and maintain remote access, as well as crypto-jacking payloads that abuse a compromised host's computational power to mine cryptocurrencies including 'Ether'.

In the latter case, crypto-jacking payloads typically join a shared pool and will likely generate significant cryptocurrency incomes for the threat actor given enough victims.

Furthermore, those behind Raccoon announced the beta release of a module on April 23, 2021 (Figure 21) named Raccoon Clipper that currently targets Bitcoin (BTC), Dogecoin (DOGE), Ethereum (ETH), Litecoin (LTC) and Monero (XMR) cryptocurrency wallets.

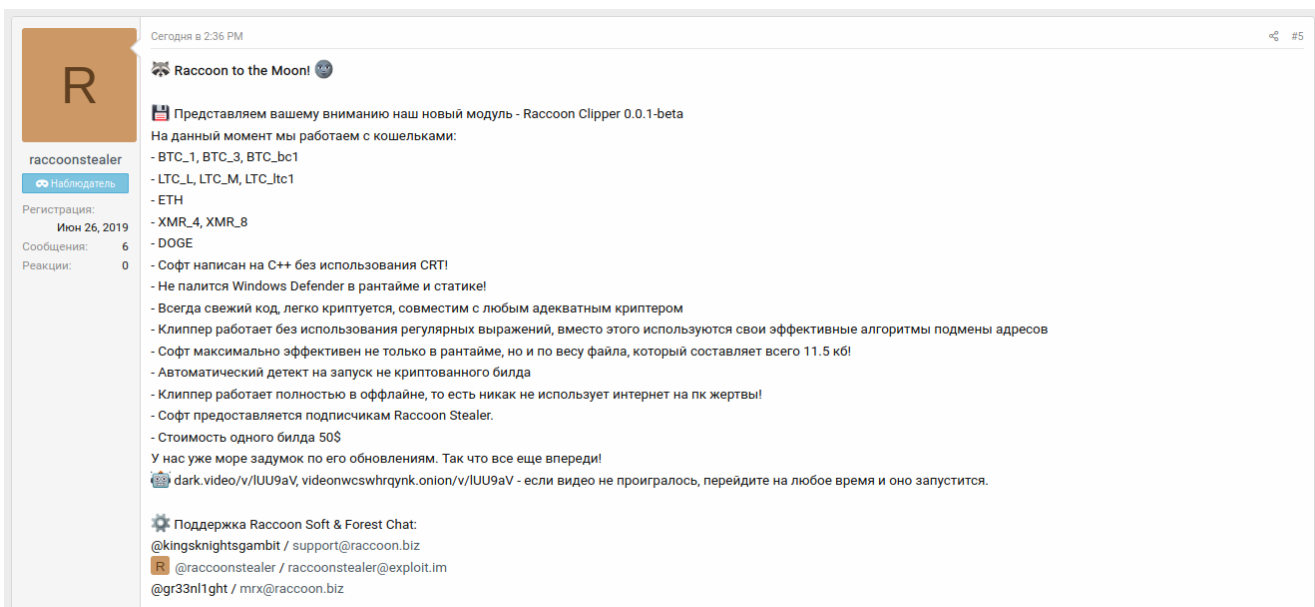


Figure 21 – 'Raccoon Clipper' forum announcement

Based on a promotional video released alongside this announcement (Figure 22), this module allows legitimate payment addresses within cryptocurrency applications to be replaced surreptitiously resulting in victims inadvertently making payments to a cryptocurrency address belonging to the threat actor.

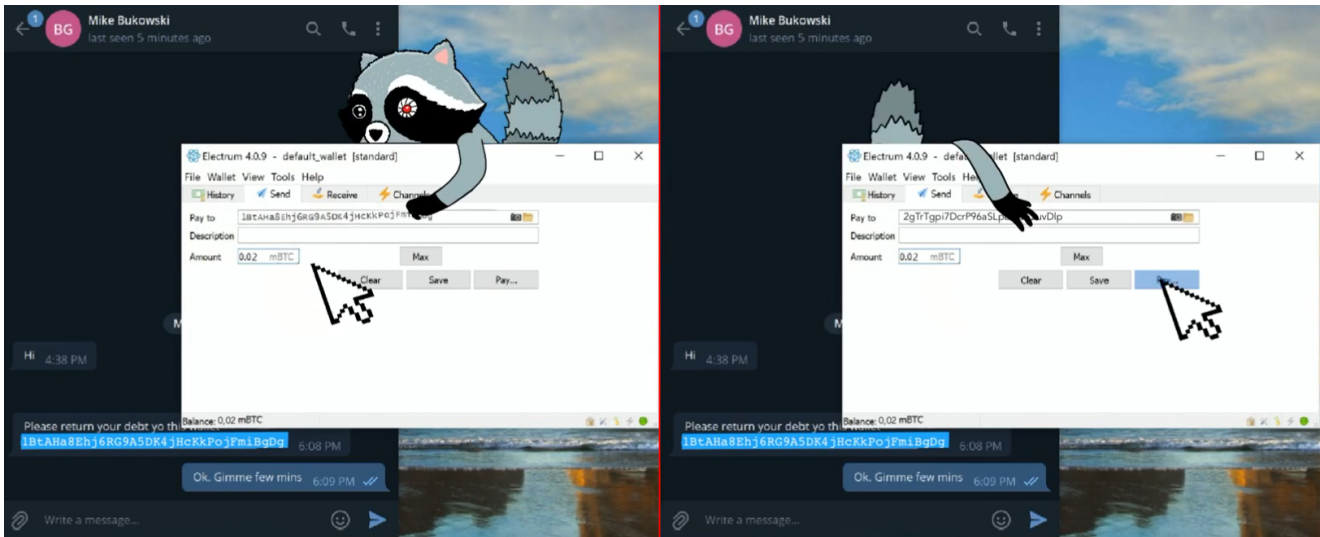


Figure 22 – Promotional video (Left: Legitimate address removed; Right: Threat Actor address inserted)

Information stealer malware constitutes a persistent and adaptive threat that demands an intricate response from cybersecurity. Several key strategies emerge as these malicious tools continuously refine their techniques to target sensitive data across individuals, businesses, and industries. Organizations must adopt an agile defense approach that combines advanced endpoint security, robust network monitoring, and proactive threat intelligence sharing to counter information stealer malware effectively.

Additionally, highlighting the importance of user awareness and adherence to data protection regulations is very crucial. By prioritizing comprehensive training, strengthening security measures, and practicing collaboration among security professionals, organizations can establish a more resilient defense against the evolving tactics of information stealer malware. This proactive stance and the integration of cutting-edge technologies will better equip the cybersecurity community to safeguard against these persistent threats and minimize potential breaches.

## Recommendations to Protect Against Raccoon Stealer

- Develop and enforce a comprehensive security policy that outlines best practices for employees, including guidelines on password management, email usage, and software updates.

- Provide regular security awareness training to employees to educate them about the risks of infostealer malware, phishing attacks, and safe online practices.
- Implement robust endpoint security solutions, including advanced antivirus and anti-malware software, to detect and prevent infostealer infections on devices used within the organization.
- Ensure that email security controls are applied to limit the delivery of potentially malicious attachments or links to end-users, as well as implementing protocols and security controls such as DKIM, DMARC and SPF.
- Enforce using MFA for accessing sensitive systems and applications, adding an extra layer of security even if credentials are compromised.
- Develop and regularly update an incident response plan that outlines the steps to take in case of an infostealer malware incident. This plan should include isolation, containment, eradication, and recovery procedures.
- Conduct regular security audits and assessments to ensure that your security practices align with industry standards and regulation.
- Those using cryptocurrencies should consider the use of hardware-based wallets and ensure that payment addresses are verified before submitting a transaction.

## Cyberint and the Dark Web

Cyberint excels in accessing high-tier sources that remain elusive to most companies. Our unique ability to penetrate these hidden corners enables us to collect and analyze invaluable data. We enrich our automated collection with a human approach, through research and analysis of our military-grade expert team.

Find new sources in deep and dark web marketplaces, forums, and sites, even if those sources are volatile and difficult to track. Get deep analysis and reports, that allow you to understand a specific threat actor and group profiling, including the places of operation, targeted countries or verticals, TTPs and more. [Get a demo and see what assets you have exposed on the deep & dark web.](#)

## Indicators of Compromise

---

### SHA256 Hashes

---

The following samples were observed in May 2021 and may be beneficial for those seeking to further understand the nature of this threat:

- 012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1
- 18c27b85f26566dd782171e00ea5b5872546b23526cca0ebb185caca35fdec93
- 24499fbfd8a2b2663899841f3cf424b60d60c26351b5d491fd475adf9e301256
- 3c5120a6e894b64924dc44f3cdc0da65f277b32870f73019cfeacf492663c0e
- 40175d0027919244b6b56fe5276c44aba846d532501e562da37831403c9ed44e

- 624b7ae8befcf91dbf768d9703147ac8f9bd46b08ffe14a75c77e88736bf07d0
- 75c3a83073d9b15d4f47308b5d688f1ec07422419e3bd54e78f6ef8683d42e5c
- 8815b21c44c22aec31f7fa6e69dcb83a60c572f8365ff02b5c6f12154e01a4c2
- 97e95e99fd499ec45a7c1d8683d5731ce5e7a8fb8b710622e578cd169a00d8d9
- a2420c7f0c7bf5d3c0893aff6b7440a09c0531632434d2bbb6f8ed98b04317b9
- bfb37c9adc809e880f56dd10898b5425242330d6e2fa69e014a98e6dc18ce416
- caf3eca514de58e215b5e9f568f748293be64a3c82e15c2f905903cd9bfacc1c
- de7ccff53ca27db1ed1e3e0d0df07f2e3364ec6b7e60622dc7726cba56831eb7

## Domains

---

- `telete[.]in` – Initial ‘call home’ to an unofficial Telegram service
- `telecut[.]in` – Suspicious domain related to `telete[.]in`
- `tgraph[.]io` – Suspicious domain related to `telete[.]in`
- `tttttt[.]me` – Initial ‘call home’ to an unofficial Telegram service
- `telegram[.]cat` – Suspicious domain related to `tttttt[.]me`
- `telegram[.]services` – Suspicious domain related to `tttttt[.]me`
- `tlgr[.]org` – Suspicious domain related to `tttttt[.]me`
- `xn--r1a[.]click` (`τ[.]click`) – Suspicious domain related to `tttttt[.]me`
- `xn--r1a[.]link` (`τ[.]link`) – Suspicious domain related to `tttttt[.]me`
- `xn--r1a[.]live` (`τ[.]live`) – Suspicious domain related to `tttttt[.]me`
- `xn--r1a[.]site` (`τ[.]site`) – Suspicious domain related to `tttttt[.]me`
- `xn--r1a[.]website` (`τ[.]website`) – Suspicious domain related to `tttttt[.]me`

## IP Addresses

---

- `195.201.225[.]248` – Resolves to `telete[.]in` and related domains
- `95.216.186[.]40` – Resolves to `tttttt[.]me` and related domains

## URLs

---

- `hxxps://telete[.]in/jiocacossa`
  - `hxxps://tttttt[.]me/kokajakprozak`
  - `hxxps://tttttt[.]me/antitantief3`
  - `hxxps://telete[.]in/baudemars`
  - `hxxps://telete[.]in/bpa1010100102`
  - `hxxps://tttttt[.]me/brikitiki`
  - `hxxps://tttttt[.]me/ch0koalpengold`
- [Contact us](#) to learn more about how threat intelligence can protect your business.

## Appendix A – Raccoon Stealer ‘User Agreement’

---



Extracted from the currently deployed Raccoon Stealer control panel, the following text is presented as the 'User Agreement' that subscribers must accept.

User agreement

By paying (by becoming a customer) Raccoon Stealer (hereinafter referred to as the service) you agree to the conditions described below.

This user agreement is final and non-negotiable.

Our service does not work and will never be in the CIS. Discussion of this in the chat will be punishable by ban.

We are only responsible for the correct operation of our service. No third-party services apply to this.

We are not responsible for the ratio, because a huge number of elements are involved in the process of log extraction. But we always want our customers to be satisfied. Just contact one of the support and we will try to solve your problem.

We are not responsible for logs stored in our panel for more than 2 months. Logs of inactive clients are deleted 2 days after the end of the subscription. We recommend that you always download your logs to avoid unpleasant situations.

## **Appendix B – Raccoon Stealer FAQ**

---

Extracted from the currently deployed control panel, the following text is presented as a frequently asked questions (FAQ) page for subscribers.

Q0. How long do you store logs if my account is inactive?

A0. We are not responsible for logs stored in our panel for more than 2 months. Logs of inactive clients are deleted 2 days after the end of the subscription. We recommend that you always download your logs to avoid unpleasant situations

Q1. Where can I find info about my account and set it up?

A1. Click on your nick on the sidebar. This is your profile. You can see your install statistics there. Also license time, balance (temporary n/a), theme setting, 2FA, etc.

Q2. How can I protect my account?

A2. You can change your password in your profile settings. Also you can set up 2FA for your account.

Q3. How do I know about your product updates?

A3. Click on News button on the sidebar. If you haven't read messages yet, you will see red circle sign. Important news and updated apper as banner on the top of any page.

Q4. How to test and download my build?

A4: Click on Build button on the sidebar. Click on the Add Build button on the top of the menu. Your build will appear on the bottom. Please read the sign in the orange box. Push the "Test" button. After that you must receive notification on the top of the page. And test log must appear in "Logs" menu. Test emulate full build work on our VM. If you receiving an error please contact our support team.

Q5. In what file formats is your build available?

A5. In \*.EXE and \*.DLL

Q6. Does your build work at Low Integrity Level?

A6. Yes!

Q7. Must I crypt your build?

A7. It's necessary. By using clean build you increase AV detects quantity. It will affect your results and results of each user of our service, especially your account. Users who check build on Virus Total and similar sites are blocked without money back.

Q8. Why must I test the build?

A8. We always ask our users to make these steps:

- 1) Test with 'test button' in panel
- 2) Test on virtual or real Windows machine
- 3) Check log archive from Windows machine if everything is stealed fine

Q9. Should I generate new build after gate change, update, etc.?

A9. No! This is our difference from other info-stealing software. You can keep working with same build and it will be active. Of course, exceptions are possible with global updates. In such cases we notify our users in News tabs and in clients chat.

Q10. Why can I generate only one build?

A10. This was made to avoid speculation and use of the account by several people. We

are planning to add multi-build function in the future for additional price.

Q11. How to create and use configs?

A11: On the top of the "Builds" you can see "Add config" button. You must add config name. After that you can choose and apply it in drop-down list on your build. You can turn on screenshots function and history grabbing, they are turned off by default. Also you can add loader urls, set them up with some required links and prepare file grabber settings.

Q12. Must I generate new build after config change?

A12. No. Raccoon loads configuration from the server. You can edit your config on the go with no rebuild required.

Q13. Does Raccoon work on CIS PC's?

A13. No for all. If you run Raccoon of PC with CIS language or IP, it will stop working. Don't be surprised with such behavior.

No! And don't even ask about it. Also notice if you will run our file on RU or CIS machine nothing will happen. This is normal. Our soft doesn't work in this countries.

Q14. How can I save my search parameters?

A14: Just fill "Mask name" box and make a search. Button with your search template will appear on the top of your log table. This options very useful and help increase speed of your daily routine work.

Q15. What do logs statuses mean?

A15: "NEW" - new log which has not been opened or downloaded yet.

"OPEN" - log which one was opened or downloaded (or you viewed passwords/links/cookies).

"DOUBLE" - someone in the panel has the same log. So it may mean your traffic was sold to many hands.

"TEST" - test log from our virtual machine. - Deprecated

"VM" - log from VM (this function in demo mode now). - Deprecated

Q16. I'm receiving so many EMPTY logs. Why?

A16: 1. Stealer knocks to the gate on the start of his work.

2. "EMPTY" log will appear in your panel.

3. Soft collects data and sends archive to the gate.

4. Panel parse data from log and give log status "NEW".

If after some time status has not changed, Raccoon died in the battle with antivirus. Or upload speed on the machine is too slow. If you are receiving many "EMPTY" logs you should check quality of your crypt / traffic.

Q17. Can you share contacts of crypt, traffic or install guys?

A17. We are working on support and updates only. We can not guarantee successful work of people who sell certain services. Please ask for advice in chat and don't forget to use escrow service of our Telegram chat!

Q18. I have a logs store and I need CSV table for it.

A18: On the top of the logs tab you can see "CSV" button. Feel free to use it.

Q19. I can't download all logs at once, what should I do?

A19. In case of high load, the multi-download process may fail. Please download less than 2000 logs per multi-download. If you have any problems downloading logs, feel free to contact our support and they will restart the process.

Q20. What if I have issues with particular log?

A20: Place your mouse arrow on the date of log, you "Bot ID" of this log. Send this information to one of our support and we'll do our best to fix the problem.

Q21. How do you monitor the status of your system?

A21. We have set up alarm system for all important nodes. We track AV detects and health of our gates and make decisions based on this info. Everything for least downtime! You will be notified about planned downtime.

Q22. What influences my ratio?

A22. There are a lot of factors that affect ratio. From crypt to methods of spreading your malware. Also your config may affect amount of AV detects in runtime. You should consult with admins if you are not sure that your config is set up fine.

Q23. What maximum file size can Raccoon grab?

A23. 100 Mb

Q24. Can I host your panel on my server?

A24. No for all.

Q25. What will happen with my logs if my license time is over?

A25. We are not responsible for logs stored in our panel for more than 2 months. Logs of inactive clients are deleted 2 days after the end of the subscription. We recommend that you always download your logs to avoid unpleasant situations.

Q26. Can I load multiple files with your loader option?

A26. Yes you can.

Q27. Where can I leave my wishes about work of your soft and panel?

A27. Please contact our support. We also give constant consideration to our customers' ideas.

Q28. I am receiving API Error.

A28. This is happen due to that back-end and front-end hosts on separate servers and your node doesn't receive or response to the request. Please restart Tor browser and try again. If you are still facing the problem, please contact support.

## References

---

[1] <https://www.cyberark.com/resources/threat-research-blog/raccoon-the-story-of-a-typical-infostealer>