

Hunting Raccoon: The New Masked Bandit on the Block

cybereason.com/blog/hunting-raccoon-stealer-the-new-masked-bandit-on-the-block

TC 13 Apr 2019 #1



raccoonstealer


Участник проекта

Регистрация: 12 Apr 2019
Сообщения: 49
Реакции: 28

Raccoon Stealer. We steal, You deal!

Наша команда с гордостью представляет вам результат своей многомесячной работы. Еще никогда процесс добычи логов не был так легкий 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.

TC 13 Apr 2019 #1



raccoonstealer

Участник проекта

Регистрация: 12 Apr 2019
Сообщения: 49
Реакции: 28

Raccoon Stealer. We steal, You deal!

Наша команда с гордостью представляет вам результат своей многомесячной работы. Еще никогда процесс добычи логов не был так легкий 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.

Written By
Cybereason Nocturnus

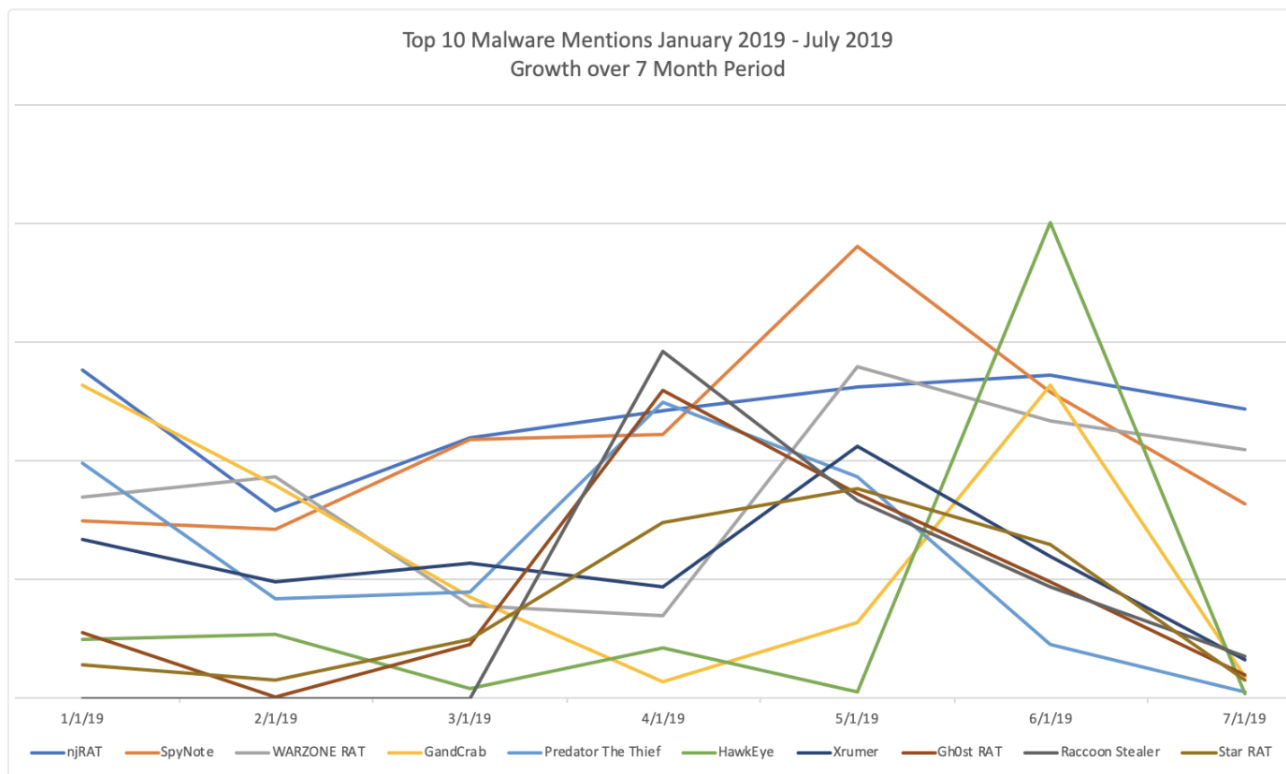
October 24, 2019 | 14 minute read

Research by: Assaf Dahan & Lior Rochberger

Introduction

Since April 2019, the Cybereason Nocturnus team has investigated multiple infections of the Raccoon stealer in the wild across organizations and individuals. In this research, we focus on two key aspects:

- **A Glimpse Into the Underground:** A survey of Raccoon's origin, team members, business model, and marketing efforts, as well as Raccoon's reception by the underground cybercrime community and the existing feuds between Raccoon's team and their direct competitors.
- **A Technical Breakdown:** A comprehensive technical overview of Raccoon's current capabilities and delivery methods, with a look into their future plans for the malware.



Most referenced malware mentions. (January 2019 to July 2019)

The top 10 malware mentions over seven months in 2019 from [Recorded Future](#).

The Raccoon stealer is one of the [2019 top 10 most-mentioned malware in the underground economy](#), and is widely known to have infected hundreds of thousands of devices around the world, despite it not being overly sophisticated or innovative. This strain of malware first emerged as recently as 2019, and has already established a strong following among cybercriminals. Its popularity, even with a limited feature set, signals the continuation of a growing trend of the commoditization of malware as they follow a MaaS (Malware-as-a-Service) model and evolve their efforts.

Build an iterative defense that addresses threats like these. [Read our white paper on how to use MITRE ATT&CK to create a closed-loop security process.](#)

Key Points

- **The Raccoon Infostealer:** The Cybereason Nocturnus team has been investigating multiple incidents involving the Raccoon infostealer since April 2019, and is now able to give a thorough analysis of the technical aspects of the malware alongside a look into the likely Russian team behind it.
- **Steals a Wide Range of Data:** Raccoon lacks sophistication, but leverages several potential delivery methods and is able to steal a large swath of important data, including credit card information, cryptocurrency wallets, browser data, and email credentials.
- **Is Quickly Gaining Traction:** Despite being released earlier this year, the Raccoon stealer is exploding in popularity in the underground community to become one of the top 10 most-referenced malware on the market in 2019, infecting hundreds of thousands of endpoints globally across organizations and individuals in North America, Europe, and Asia.
- **Enables Any Individual to Easily Commit Cybercrime:** Raccoon follows a malware-as-a-service model, allowing individuals a quick-and-easy way to make money stealing sensitive data without a huge personal investment or technical know-how.
- **Has a Strong Following Underground:** The team behind Raccoon is lauded in the underground community for their level of service, support, and user experience, but has faced several bouts of public feuds and internal disputes.

TABLE OF CONTENTS

Raccoon, also known as “[Mohazo](#)” or “[Racemailer](#)”, is at its core a simple information stealer often seen delivered by the [Fallout](#) and [RIG](#) Exploit Kits. It is used to steal data like credit card information, cryptocurrency wallets, browser-related data, and mail clients. Although it is not an advanced malware, it is estimated to have infected hundreds of thousands of devices around the world and is in the [top 10 mentioned in the underground communities](#) for 2019.

Raccoon is written in C++ and works on both 32-bit and 64-bit operating systems. Though it was originally classified as a password stealer by many AV companies, we and others in the community see it leverage broader capabilities and categorize it as an information stealer.

Raccoon searches system files for a range of confidential data which it saves and sends to its operator. It is able to collect the following data:

- Credit Card Data
- Cryptocurrency Wallets
- Passwords
- Emails
- Data from All Popular Browsers Including Credit Card Info, URLs, Usernames, Passwords
- Cookies
- System Information

Threat Actor Overview

The Raccoon stealer is developed by a team that appears to originate in Russia and be Russian-speaking. The team initially promoted the stealer in exclusively Russian-speaking hacking forums, but now actively promotes it in English-speaking communities as well. It is aggressively marketed in the cybercrime underground and has been since April 2019.



13 Apr 2019 #1

Raccoon Stealer. We steal, You deal!

raccoonstealer
Участник проекта
Регистрация: 12 Apr 2019
Сообщения: 49
Реакции: 28

Наша команда с гордостью представляет вам результат своей многомесячной работы. Еще никогда процесс добычи логов не был так легкий 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.

Raccoon stealer marketed in a Russian underground forum.

Raccoon is sold as a MaaS with features like an easy-to-use automated backend panel, bulletproof hosting, and 24/7 customer support in both Russian and English. As of this writing, it costs \$200 per month to use.

Contacts

- support@raccoon.biz
- Telegram: [@darkgr33n](#)

Best regards,
Raccoon Stealer Team

From Russia with love!

How to contact the Raccoon Team.

Much like any other software-as-a-service, the Raccoon stealer appears to be in active development. The development team seems to be quick, responsive, and dedicated, using short development cycles to release updates, bug fixes, and new features within days. They are also highly active in underground communities under the username *raccoonstealer*. They post daily and reply to community questions and comments within hours in underground forums and on Telegram.

Who is behind the Raccoon Stealer?

While the identity of the team behind Raccoon remains unknown, some members in the underground community attribute the project to another well-known member, *glad0ff*. *Alexuiop1337*, the [author of predator stealer](#) and one of the strongest critics of Raccoon, [was one of the first to make this allegation](#). Of course, the accusations made by direct competitors should be taken with a grain of salt. However, the leads *Alexuiop1337* provided in his blog can potentially tie *glad0ff* to Raccoon.

An analysis of the Raccoon stealer's [hacked panel](#) and [leaked customer base](#) could imply the admin of Raccoon is a user with the online handle *glad0ff*. The user *glad0ff* was created in the Raccoon stealers database in February of 2019, roughly two months before the team began aggressively marketing Raccoon to the underground community.

```
"create_date":"2019-02-27 17:22:25",  
  "is_google_auth_enabled":0,  
  "google_auth_secret":null,  
  "is_email_confirmed":0,  
  "ulogin_uid":null,  
  "ban_id":null,  
  "is_banned":0,  
  "telegram":"@glad0ff",  
  "jabber":null,  
  "user_type":"master",  
  "login":"glad0ff",
```

glad0ff user creation date in Raccoon's database.



The image shows a forum profile for a user named 'raccoonstealer'. The profile includes a blue 'TC' tag, a profile picture of a cartoon raccoon with a key, and a blue 'Project participant' badge. Below the badge, the profile statistics are listed: registration on Apr 12, 2019, 51 messages, and 28 reactions.

TC

raccoonstealer

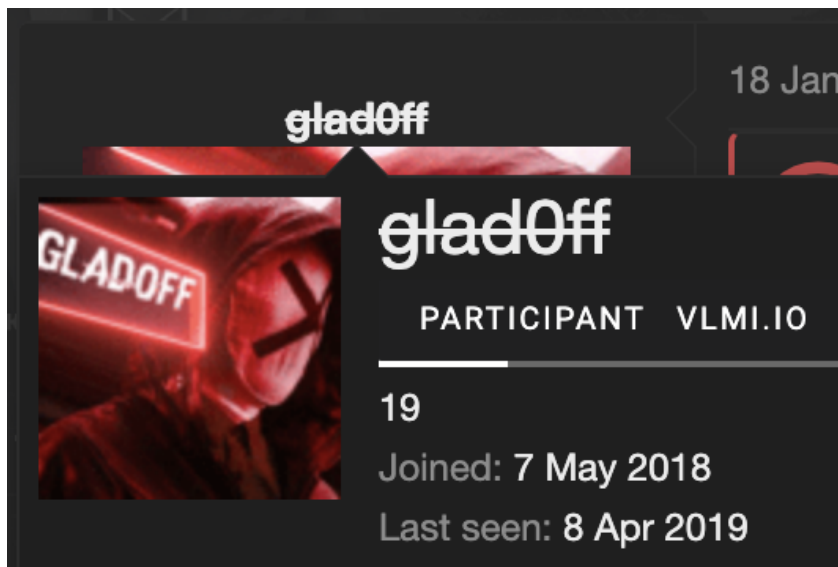
registration: Apr 12, 2019
Messages: 51
Reactions: 28

One of the first mentions of Raccoon in underground forums.

Who is glad0ff?

gladOff is a long-time threat actor responsible for developing malware like the Decrux and Acrux cryptominers, the Mimosa RAT and the ProtonBot loader. *gladOff* caters to less sophisticated cyber criminals looking for easy-to-use, end-to-end solutions. Similar to customers of Raccoon, customers from many of *gladOff*'s previous projects praise the quality of service, dedication, and responsiveness when fixing issues. It was previously believed that gladOff operated alone, however, there are indications that the Raccoon stealer involved other members, as we discuss later on.

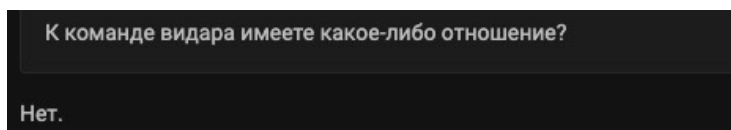
It's also interesting to note that *gladOff* stopped posting in many underground forums in April of 2019, which aligns with the launch of the Raccoon stealer.



Last seen date for the gladOff user.

Is Raccoon Tied to Malware from Other Threat Actors?

Other members in the underground community have questioned whether Raccoon is linked to other stealers like Vidar and Baldr, as they noticed great similarities between the aforementioned infostealers. Raccoon team members consistently deny any ties to other stealers.



"Do you have any relation to the Vidar team?" Reply: "No."

Raccoon's Reception in the Underground Community

It is interesting to note that many individuals choose to write reviews for Raccoon. As malware authors turn to MaaS, they follow many of the same paths as a legitimate SaaS business: marketing efforts, relying on positive reviews, responsive customer support, and regularly improving features in their product.

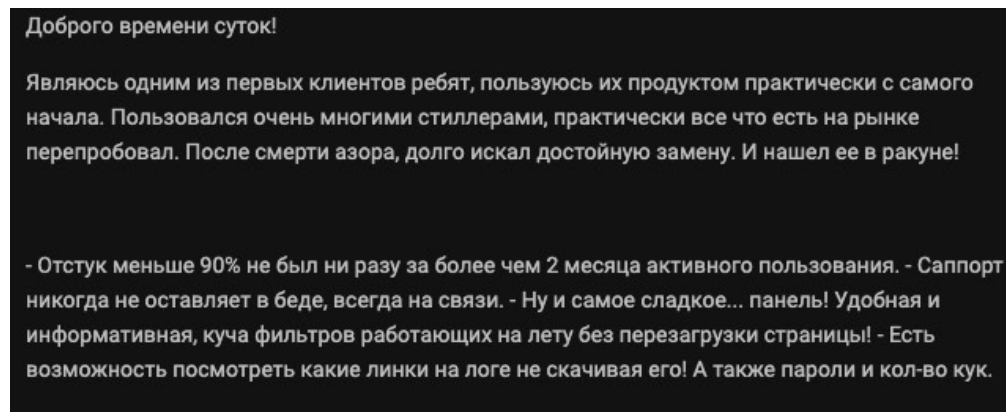
Positive Feedbacks and Endorsements

Generally, feedback around Raccoon in the underground community is positive. Many in the community praise and endorse Raccoon's malware capabilities and the services the team provides. Some voices in the community even endorse it as a worthy replacement for the famous Azorult stealer. However, it is important to note that there are some dissenting opinions. Advanced members in the community find Raccoon to be simple and lacking in features when compared to other information stealers. With that said, many in the community believe that while the malware may lack in features, sophistication, or innovation, it largely makes up for it with consistency and an impressive level of service, support, and quality user experience.

Raccoon's popularity combined with its limited feature set yet high adoption speaks to a growing trend of the commoditization of malware, as malware authors shoot to create platforms for crime instead of committing the crimes directly.

Example #1: Early Adopter Replaces Azorult

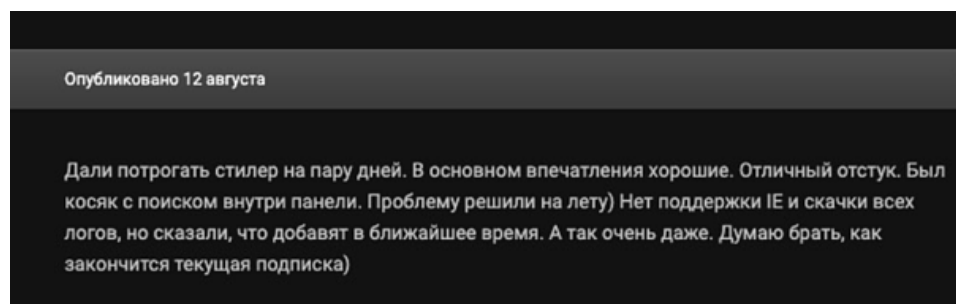
This early adopter of Raccoon claims he has been using it since the initial launch. After Azorult was shut down at the end of 2018, he tried almost every stealer on the market before settling on Raccoon.



"I am among the first clients of these guys, practically using their product since the initial launch. I have used many other stealers before, essentially i tried all there is in this market to offer. After the "death" of "azora" (Azorult malware), I searched for a long time for a decent replacement and finally, found it in Raccoon!

Example #2: Praise for Excellent Service

This user leveraged a free trial of Raccoon, and deemed it an excellent product they were interested in switching to. They specifically reference one instance where there was a bug in the panel's search engine that was fixed immediately on the fly.



"They let me try the stealer for a few days. In general, first impressions were good. The rate of successful infection is very good. Had an issue with the control panel's search engine. Problem was solved immediately, on the fly) There is no support for IE, and the download of all logs, but i have been told that these features will be added in the near future. Not bad at all. Thinking of getting it as soon as my current lease is over)"

Example #3: User Testimonial - A Worthy Replacement for Azorult

This user switched from Azorult to Raccoon because of how easy the control panel was to use. In addition, the user experiences a very high success rate and is a big supporter of the quality of service.

Перешел с азора на ракуна и получил огромное удовольствие от удобства админки, Там нету ничего лишнего как в видаре но есть те все мелочи которые необходимы человеку который отработывает огромное количество логов. По билду могу сказать все хорошо, с азором у меня всегда был отстук 60%+ ну а тут же я нашел хорошего криптора и 90% отстук есть. Так же радует что не надо париться и устанавливать хост по 150\$, не дрочиться с ним и не переживать если можно за 200\$ в месяц пользоваться хорошим продуктом. Что меня удивило это саппорты, которые относятся к тебе как клиенту вип класса, все что просишь делают добавляют выражают благодарность и т.д. это очень приятно и я нигде такого еще не встречал.

“I switched from azor (Azorult) to raccoon and got a great joy of how convenient the admin control panel is, there are no extra, unnecessary details such as in vidar (Vidar malware) but there are these small, little details that are helpful and mandatory for people who process a large amount of logs. If judging the build, that everything is alright, with azor i always had around 60%+ of successful infection rate and here i found a good crypter and have 90% of rate... [snipped] What surprised me is the support that treats you as a VIP class client, they will do whatever you demand and with expressing gratitude, etc. it is very nice and I have never seen experienced it anywhere else.”

Criticism of Raccoon by Members of the Underground Community

Since day one, some members of the underground community have criticized Raccoon, specifically targeting it's lack of capabilities, poor coding, and several security issues in the infrastructure and admin panel code.

Perhaps one of the most negative reviews comes from [Alexuiop1337](#). *Alexuiop1337* wrote a [very detailed blog](#) dissecting and criticizing the malware and its infrastructure. According to *Alexuiop1337*, Raccoon has vulnerabilities that let attackers DDoS their servers and dump sensitive data. In his review, *Alexuiop1337* also tries to expose the identity of one of the developers behind Raccoon by claiming it is *gladOff/wankfbi*, another member of the underground community

Other negative reviews voiced by customers or testers complain that Raccoon has:

1. A low success rate for infection at about 45%.
2. Some bugs that make it difficult to access logs and delete logs from the control panel.
3. Some missing information or version compatibility issues in its stealing modules.

- долго скачиваются логи, при интернете в 200 мбит/с приходится качать 5-10 мегабайт несколько минут
- стиллер довольно часто не ворует все софты и их версии, для меня это было важно
- куки с этого стиллера часто заливаются в сферу не полностью, не понимаю с чем это связано но на прошлом стиллере таких проблем не было
- отстук супер, панель очень удобная

“- The stealer often doesn't still software or its version, and for me it was important

The cookies from the stealer are often transferred incomplete,

I don't understand why it does it, but in the previous stealer there were no such problems ”

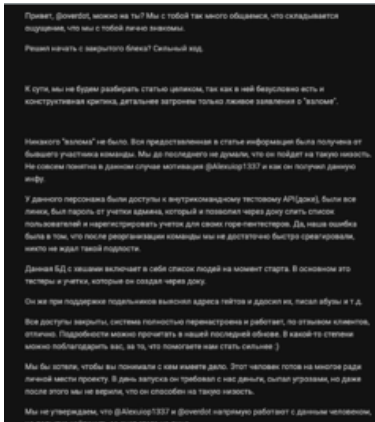
Public Disputes and Controversies with the Raccoon Team

Within the underground community, the Raccoon team is also facing some public disputes and controversies. These disputes offer an important glimpse into the inner workings of the team and give a broader sense of just how competitive the commodity malware market is.

In addition, these conflicts validate **our hypothesis that Raccoon is not operated by a single user, but by a team**. It gives insight into the types of relationships the team members have and how fragile and opportunistic those ties can be.

Internal Disputes Shed Light on the Raccoon Team Dynamics

The first public signs of tension between Raccoon team members began shortly after their launch in April. Following a [leak of their customer database](#), the team released a statement claiming their servers were not hacked, but that the leak was caused by a disgruntled team member using the database as blackmail for more money. When the team member demands were not met, they released the database to embarrass the Raccoon team. Though the team explicitly states the blackmailer was not working directly with their competitors, they did accuse *Alexuiop1337* and *overdot* of hyping the situation in order to capitalize on it.

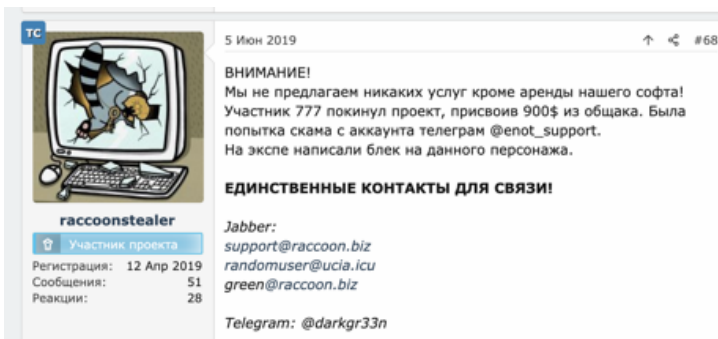


“The aforementioned user had access to the intra-team test API (dock), had all the links, had a password from the admin account, which allowed us to document the list of users and register accounts for their unfortunate pentesters. Yes, our mistake was that after the reorganization of the team, we did not react quickly enough, no one expected such meanness.”

“This person will do what it takes, for personal revenge against the project. On the launch day, he demanded money from us, threatened us, but even after that we couldn’t believe that he was capable of such baseness.”

“We do not claim that @Alexuiop1337 and @overdot work directly with this person, but an attempt to hype this situation on behalf (of the aforementioned person)”

Additionally, in June of 2019 *raccoonstealer* published an unusual post that revealed an internal feud with former team members. Allegedly, *Participant 777 (777@raccoon.biz)* stole \$900 from the community balance and left the project.



“Attention!

We do not offer any services except the rental of our software! Participant 777 left the project, taking \$900 from the shared common fund. There was scam attempt from the telegram account @enot_support.

In the “expe” (a Russian slang for the infamous “exploit[.jin]” underground hacking community), they blacklisted the aforementioned account.

THE ONLY CONTACTS FOR CONTACTING US!

Jabber: support@raccoon.biz randomuser@ucia.icu green@raccoon.biz Telegram: @ darkgr33n“

These two incidents make it clear that Raccoon is developed by several individuals that work together, but are not necessarily a tight-knit team.

Raccoon Stealer Overview

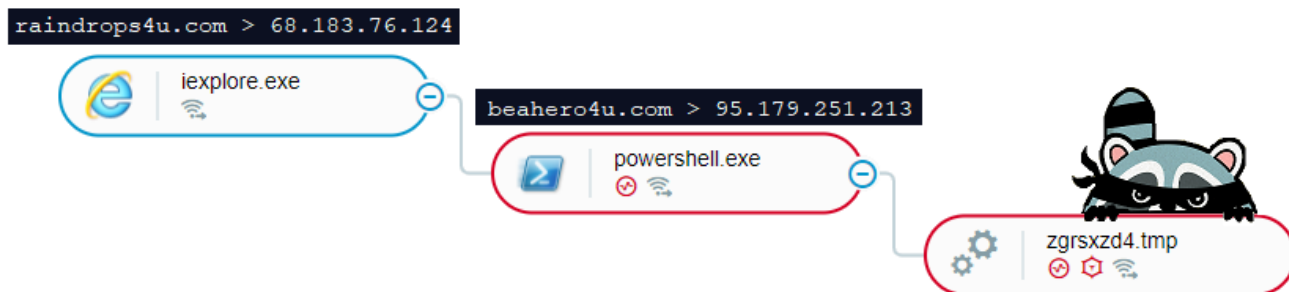
How is Raccoon Delivered?

Raccoon is delivered in multiple ways, though we see Raccoon delivered most often through exploit kits, phishing attacks, and through bundled malware.

Delivery by Exploit Kit

Exploit kits automatically exploit vulnerabilities on a victim's machine while they are browsing the web. In browsing the web, the user visits a malicious page that redirects to a landing page containing exploit code, often executed without the users consent or interaction.

In order to deliver Raccoon, the attackers leverage the Fallout exploit kit to spawn a PowerShell instance from Internet Explorer and subsequently download the main payload of the infostealer.



The Fallout exploit kit delivers Raccoon, as seen in the Cybereason platform.

Delivery by Phishing

Phishing is a social engineering attack where a user is tricked into executing malicious content. Most commonly, the user receives an email with an attached Office document. This document contains embedded malicious macro code that, when opened, executes.

In order to deliver Raccoon, the attackers use an email with an attached Word document. Upon opening the Word document and enabling macros, the macro code creates a connection to a malicious domain and downloads the main payload of the infostealer.



The malicious Word document downloading the Raccoon stealer payload, as seen in the Cybereason platform.

Delivery by Bundled Malware

Bundled malware is malware that is bundled with legitimate software downloaded from “shady” websites. The bundled malware is often hidden from the user during installation or makes use of social engineering techniques to enable installation.

In order to deliver Raccoon, the attackers use legitimate software bundled with the main payload of the infostealer to infect unsuspecting users. Raccoon installs itself behind-the-scenes, hidden from the user.

Exploring Raccoon’s Code and Core Functionality

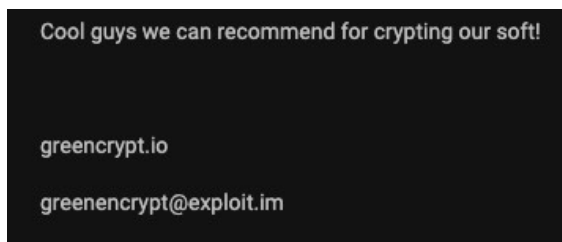
```

; DATA XREF: sub_414649+4↑o
; sub_4147E2+3E↑o ...
'g:\stealer\stealler\json.hpp',0

```

The internal path from malware compilation on the attackers machine.

As mentioned above, the Raccoon team appears to be of Russian origin. A typo found in the internal path also suggests they are not native English speakers.

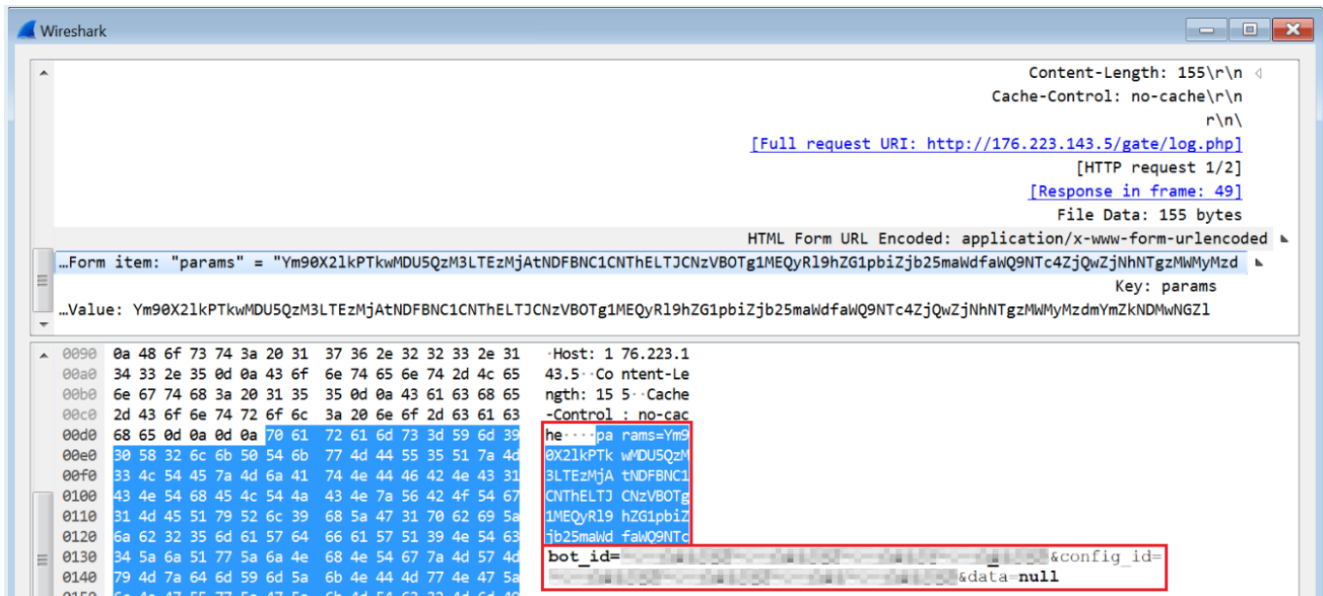


The Raccoon team issuing a recommendation for a third-party crypter.

The main payload of Raccoon is not packed and does not include built-in anti-debug or anti-VM protections. It is sold *as-is* without any protection from analysts or detection. However, the Raccoon team does recommend a third-party crypter call GreenCrypt to evade antivirus products and protect against detection and analysis.

Raccoon's Communication with its C2 Server

Once the loader executes on the target machine, it unpacks itself in memory and connects to its C2 server. Raccoon sends a POST request with Base64-encoded parameters *bot_id* and *config_id*.



Raccoon sending a POST request with two parameters.

Upon successful connection and verification of Raccoon's Bot ID, it downloads a compressed zip file with multiple different DLLs. These DLLs are not necessarily malicious on their own, but Raccoon depends on them to successfully collect and steal data on the target machine.

Gathering Local Settings on the Target Machine

```
if ( sub_430B34() )
    sub_430BD9();
memset(&LCDData, 0, 0xFFu);
v4 = GetUserDefaultLCID();
GetLocaleInfoA(v4, 0x1001u, &LCDData, 255);
v5 = 55;
*( _DWORD *)Str2 = -1145202121;
v1062 = -1498832453;
```

The Raccoon stealer code checks the target machine's local settings.

However, the Raccoon stealer does check the target machine's local settings and compare it against a list of languages, including Russian, Ukrainian, Belarussian, Kazakh, Kyrgyz, Armenian, Tajik, and Uzbek. If the target machine's local settings match one of these languages, the malware immediately aborts. This is common practice by malware originating from CIS countries.

Collecting Sensitive Data

After initial infection, the Raccoon stealer uses several methods to collect sensitive information. It stores any sensitive information it finds in the *Temp* folder.

Capturing Screenshots from Infected Machine

```
mov     [ebp-2Ch], ebx
mov     [ebp-28h], ebx
call    ds:GdiplusStartup
call    ds:GetDesktopWindow
mov     esi, eax
lea     eax, [ebp-44h]
```

The Raccoon stealer code takes a screen capture of the target machine.

Firefox

WaterFox

SeaMonkey

Pale Moon

GO!

```

; "Web Data"
dd offset aGoogleChrome ; "Google Chrome"
db 1Ch
db 0
db 0
db 0
dd offset off_46DF34
dd offset aLoginData ; "Login Data"
dd offset aCookies ; "Cookies"
dd offset aWebData ; "Web Data"
dd offset aChromium ; "Chromium"
db 1Ch
db 0
db 0
db 0
dd offset aChromiumUserDa ; "\\Chromium\\User Data"
dd offset aLoginData ; "Login Data"
dd offset aCookies ; "Cookies"
dd offset aWebData ; "Web Data"
```

Example of Raccoon's browser stealing configuration code

Raccoon copies targeted browser data files to the *Temp* folder with random names. It uses a DLL, *SQLite3.dll*, downloaded from its C2 server to parse the files and extract sensitive data. The stolen information is divided into several text files named after their associated browser and saved under *Temp/browsers*.

Raccoon also creates one master file with the name *passwords.txt* that contains any and all passwords stolen from the victim's machine.

```
SOFT: Google Chrome
HOST: https://m.facebook.com/
USER: Cybereason_Facebook_user.com
PASS: Aa123456!
```

```
SOFT: Internet Explorer
HOST: https://linkedin.com/
USER: Cybereason_Linkedin_user.com
PASS: Aa123456!
```

Example of the format of passwords.txt, containing passwords stolen by Raccoon.

Stealing Outlook Accounts

```

call sub_42DA29
lea ecx, [ebp+var_4]
mov [esp+0Ch+1pSubKey], offset aSoftwareMicros_0 ; "Software\\Microsoft\\Internet Account M".
call sub_42DE84
mov [esp+0Ch+1pSubKey], offset String ; "\\Software\\Microsoft\\Internet Account"...
lea ecx, [ebp+var_4]
; const WCHAR String ; DATA XREF: sub_42E275+2D70
String:
    text "UTF-16LE", "\\Software\\Microsoft\\Internet Account Manager\\Account"
    text "UTF-16LE", 'ts',0
```

Raccoon's code to extract information about Microsoft Outlook accounts.

Raccoon extracts information about Microsoft Outlook accounts from registry keys on the target machine.

- HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook

In addition, Raccoon searches the Windows Registry for sensitive information stored in Mail clients, such as usernames and passwords, then saves it to a text file under *Temp/mails*.

```
esi, offset ValueName ; "SMTP Email Address"
[ebp+var_94], offset aSmtplibServer ; "SMTP Server"
edi
edi, ecx
[ebp+var_98], esi
[ebp+var_90], offset aPop3Server ; "POP3 Server"
ebx, [ebp+var_98]
[ebp+var_8C], offset aPop3UserName ; "POP3 User Name"
[ebp+var_88], offset aSmtplibUserName ; "SMTP User Name"
[ebp+var_84], offset aNntplibEmailAddre ; "NNTP Email Address"
[ebp+var_80], offset aNntplibUserName ; "NNTP User Name"
[ebp+var_7C], offset aNntplibServer ; "NNTP Server"
[ebp+var_78], offset aImapServer ; "IMAP Server"
[ebp+var_74], offset aImapUserName ; "IMAP User Name"
[ebp+var_70], offset aEmail ; "Email"
[ebp+var_6C], offset aHttpUser ; "HTTP User"
[ebp+var_68], offset aHttpServerUrl ; "HTTP Server URL"
```

Raccoon gathering information from Mail client accounts on the target machine.

Stealing Cryptocurrency Wallets

Raccoon searches for multiple cryptocurrency wallets on the machine, including:

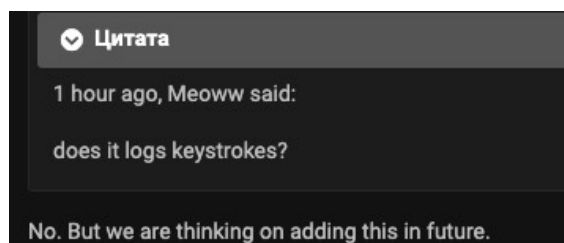
- C:\Users\\AppData\Roaming\Electrum\wallets
- C:\Users\\AppData\Roaming\Jaxx\Local Storage
- C:\Users\\AppData\Roaming\Exodus\exodus.wallet
- C:\Users\\AppData\Roaming\Ethereum Wallet

If any cryptocurrency wallets are found, they are saved under *Temp*.

For the convenience of the client, Raccoon has a service that automatically processes all cryptocurrency wallets without needing to search for specific logs among all the stolen data.

New features to come?

Current versions of Raccoon do not have keylogging functionality. Several users in the underground community are asking for this feature, and the Raccoon team has suggested it may be available in the future.



Screenshot from the underground community of the Raccoon team considering adding support for keylogging.

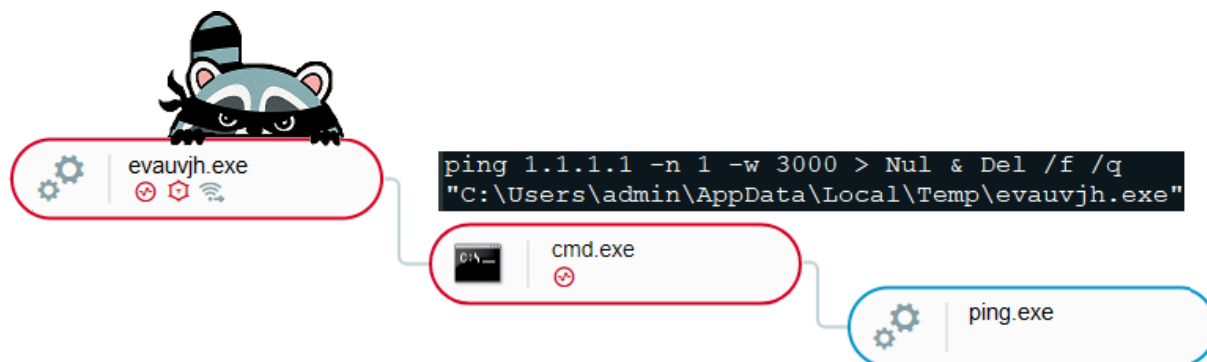
Data Exfiltration & Self Deletion

Raccoon saves all stolen data to a zip file *gate.zip* and sends the information to its C2 server.

browsers	File folder
mails	File folder
passwords.txt	Text Document
screen.jpeg	JPEG image
System Info.txt	Text Document

All stolen data Raccoon has collected on the target machine.

After it successfully exfiltrates all sensitive data, Raccoon deletes its binary from the victim's machine, as can be seen in the following screenshot of Raccoon's process spawning cmd.exe with ping.exe and executing the deletion command.



The malicious process Raccoon creates to delete any trace on the machine.

How is Raccoon Affecting Businesses and Individuals?

Based on the logs for sale in the underground community, Raccoon is estimated to have infected over 100,000 endpoints worldwide within a few months. It is easy to operate for technical and nontechnical individuals alike, lending it mass appeal. Moreover, the team behind Raccoon is constantly working to improve it and provide responsive service. It gives individuals a quick-and-easy way to make money stealing sensitive data without investing a lot of funds or having a deep technical background.

Raccoon collects a wide swath of information, including credit card information, cryptocurrency wallets, usernames and passwords, and browsing data, which is used to steal corporate data, money, and other sensitive information. This data is used against victims as blackmail or monetized by cybercriminals selling it in underground communities.

Cybereason Vs. Raccoon?

In addition to our anomalous behavior detection and investigation capabilities, Cybereason's NGAV technology can detect and prevent Raccoon infections.

BitDefender	! Gen:Heur.Titirez.1.15
Comodo	! Malware@#1ye1nfi10d8h6
Cybereason	! Malicious.a10914
Cyren	! W32/Trojan.JUDX-6735
Emsisoft	! Gen:Heur.Titirez.1.15 (B)

Screenshot from VirusTotal, Cybereason NGAV detects Raccoon's executable as malicious.



evauvjh.exe
App Control

Prevented

Investigate

Exclude

Cybereason platform prevents the malicious executable.

Conclusion

Though the Raccoon stealer may not be the most innovative infostealer on the market, it is still gaining significant traction in the underground community. Based on testimonials from the underground community, The Raccoon team provides reliable customer service to give cybercriminals a quick-and-easy way to commit cybercrime without a huge personal investment.

This has not come without strife. The team has faced several public disputes in underground forums, and has received some criticism from competitors. Despite this, Raccoon has quickly become one of the top ten mentioned malware in the underground community, despite being launched in early 2019. Overall, sentiment around Raccoon is positive, with some calling it the best replacement available for the now defunct Azorult infostealer.

Raccoon's popularity combined with its limited feature set yet high adoption speaks to a growing trend of the commoditization of malware, as malware authors shoot to create platforms for crime instead of committing the crimes directly. As malware authors choose to develop MaaS, they must partake in many of the same activities as a legitimate SaaS business: marketing efforts, relying on positive reviews, responsive customer support, and regularly improving features in their product. We only expect this trend to continue into 2020 and push the evolution of MaaS forward.

Endpoint protection is key to defending against techniques like these. [Learn more during our webinar on Endpoint Protection Platforms.](#)

APPENDIX

INDICATORS OF COMPROMISE

[Review the Indicators of Compromise for the Raccoon Stealer here.](#)

MITRE ATT&CK TECHNIQUES BREAKDOWN

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Command and Control
<u>Spear Phishing Attachment</u>	<u>Execution through API</u>	<u>Software Packing</u>	<u>Credential Dumping</u>	<u>System Time Discovery</u>	<u>Data from Local System</u>	<u>Data Encrypted</u>	<u>Remote File Copy</u>
<u>Drive-by Compromise</u>	<u>Command-Line Interface</u>	<u>Deobfuscate / Decode Files or Information</u>	<u>Credentials in Files</u>	<u>Account Discovery</u>	<u>Screen Capture</u>		<u>Standard Cryptographic Protocol</u>
<u>Exploitation for Client Execution</u>		<u>Obfuscated Files or Information</u>	<u>Input Capture</u>	<u>File and Directory Discovery</u>			<u>Standard Non-Application Layer Protocol</u>

System
Information
Discovery.

Standard
Application
Layer
Protocol

Query
Registry.

Process
Discovery.

System
Owner/User
Discovery.

Remote
System
Discovery.

System
Network
Configuration
Discovery.



About the Author

Cybereason Nocturnus



The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

[All Posts by Cybereason Nocturnus](#)