

Analysis of Raccoonstealer

By

|  |  |
| --- | --- |
| Aisha | MT20ACS490 |
| Aswin Vijay | MT20ACS500 |
| Gnani Chintapalli | MT20ACS510 |
| Sumedha Gandhi | MT20ACS540 |
| Vijayabharathi | MT20ACS545 |

**MALWARE FAMILY** – Raccoonstealer

**FILETYPE** – EXE

# **INTRODUCTION**

An info-stealer is a type of malware that is focused on gathering sensitive and conditional information from the compromised system. While this information is often related to the user’s credentials, they have also been known to seek out financial data and personal information.

Raccoonstealer is an info-stealer malware and is written in C++. It checks for the existence of various types of applications such as browsers, email clients, coin wallets and attempts to steal their data by reading their configuration files or databases. The execution of the malware is closely related with the configuration that the CnC server will send, thus there is an obstacle during the dynamic analysis if the CnC domain is down.

Raccoon stealer is not the most sophisticated malware that’s available to cyber attackers, but it proves to be quite effective. This reaffirms that attackers do not require anything overly advanced when these less-sophisticated techniques are still very much effective in carrying out an attack.

# **PROCESS**

Raccoonstealer targets a wide range of applications and uses known techniques in order to extract sensitive data from those applications. It uses the same procedure for each of the targeted applications:

1. It gets application files that contains the sensitive data.
2. It downloads all the files it needs (DLLs, zip file, and dropped malware) to temp folder and writes all the stolen data to text files in this directory
3. After fulfilling all its stealing capabilities, it gathers all the files that it wrote to the temp folder into one zip file named Log.zip (Perform the specific routines for the application in order to extract and decrypt the related data)
4. To send the file back to C&C, it creates a POST request that contains that zip file. Like most of the strings in Raccoon’s binary, the strings for sending the file back to the C&C are encrypted. So, Raccoon decrypts them.
5. Once Raccoon has sent the file, it will delete its trace from the machine. It creates a cmd.exe process that creates a ping.exe process and runs a delete command for the stealer file.

# **TARGETED APPLICATIONS**

**1. BROWSERS -**

* Raccoon targets **29 chromium-based browsers including**Google Chrome, Opera, etc. (full list below) that have the same folder structure and share a similar codebase, which leads to a similar way of handling sensitive data.

It performs SQL queries in order to get the user autologin passwords, credit card information, cookies and browser history.

* The stealer targets **four Mozilla-based browsers** including Firefox and SeaMonkey, (full list below) and one Mozilla-based email client, ThunderBird. Here, the stealer extracts and decrypts sensitive data like username and password, cookies and history. In order to do so, Raccoon downloads a zip file containing a lot of DLLs for decrypting protected data. By using functions from nss3.dll, the malware is able to decrypt and extract the data from the SQLite databases and the JSON login file.

#### **2. EMAIL CLIENTS-**

* ThunderBird, Outlook, Foxmail

**3. CRYPTOCURRENCY WALLETS**

* When looking for **cryptocurrency wallets,** Racoon targets popular applications like Exodus, Jaxx and more. Like most stealers, Raccoon is looking for those wallet files in the default application locations, but it also has a wallet scanning feature that allows it to grab any wallet.dat file.

# **Samples**: 8 samples have been chosen from Malware Bazaar

0d8501287af1bdb73891772549bf9f60e1119327a5c3e7ff3bd75b36dc22a93d

2ef903462ba81fd5419d88ed6f5771554859f16068267227116601bde1ca5ba6

f584f1003f8cc6767461c6e67a6b96f9d8779cc27212712185fb7aaf8f569ce6

9f900d8fa07652fef51b583c5422ce011ce0940c59de8487d90ee0cabaeba530

336b73345346ecc0c06d050402fba00e1301be6c4989b448e7cc11c967722d7c

9775f4ba684a002d68c8cdf8b6790775db9ce17e2a604073c5ee1e47f4e544c0

11adb6fd4fbcb8fe68033ff2bc3b8cc45b980c573f7c58be291383d5b95d6e41

e4c826244f01a7c81d9fa83e0aed1e783714abd0556b663777bc5d8760f42c99

# **STATIC ANALYSIS-**

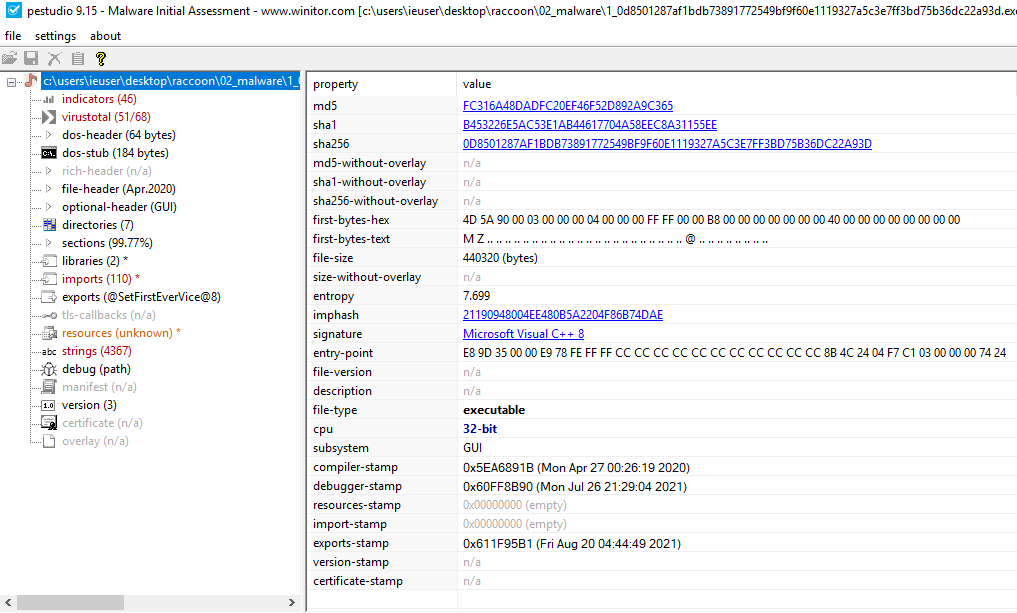
**TOOLS USED** - PE Studio, Detect it Easy, BinText

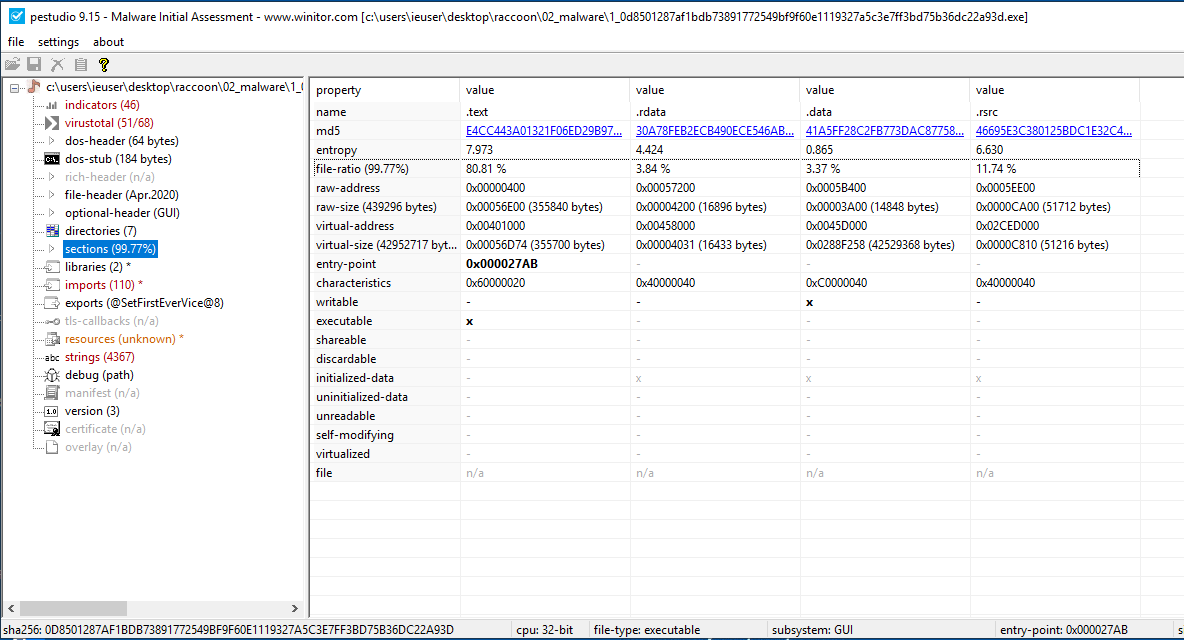
We started our analysis by investigating malware strings. Most of the strings that Raccoon uses are encrypted, therefore it decrypts them in runtime.

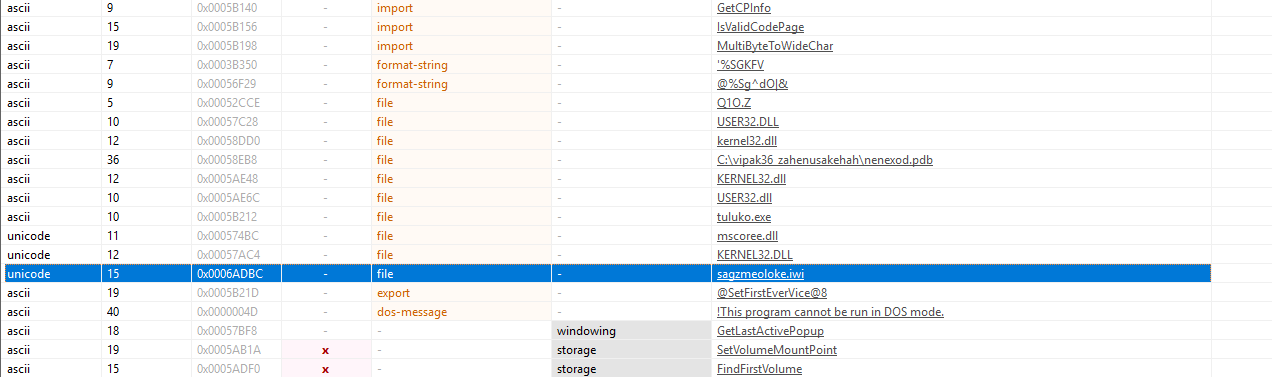
Firstly, Raccoon gets its C&C server and after querying C&C server it gets the configuration file in JSON format. Client can customize its configuration file too, which can be saved in the binary built by the malware or in the C&C server and sent back to the malware when executed.

Let’s begin with Static Analysis-

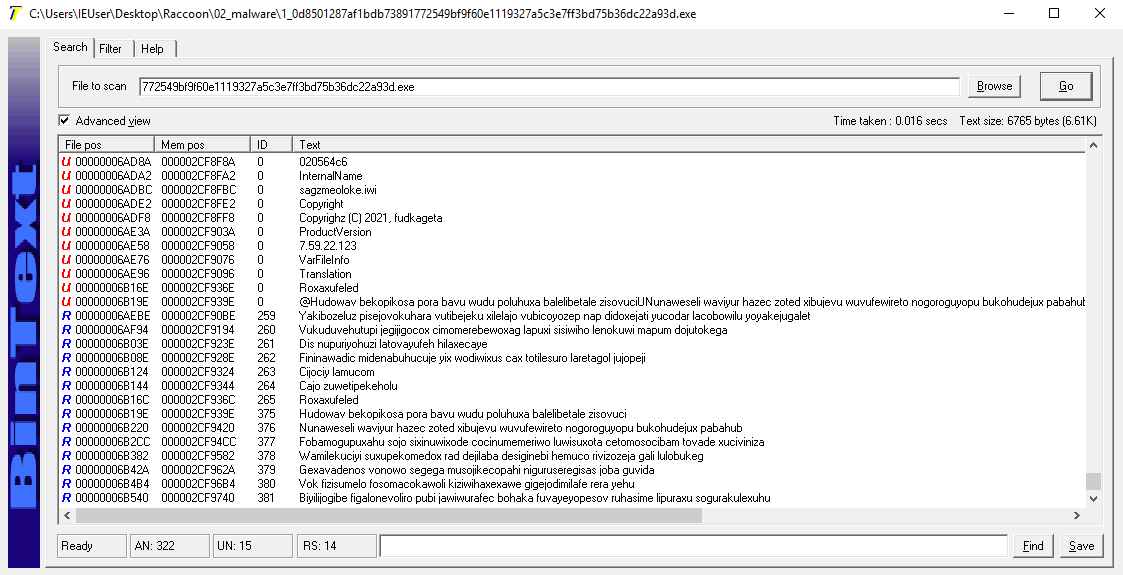
1. Initial Assessment Details of EXE files using PEStudio.







1. BinText tool is used for strings extraction



1. Below Mitre ATT&CK matrix is showing, what steps are performed by the Raccoonstealer.



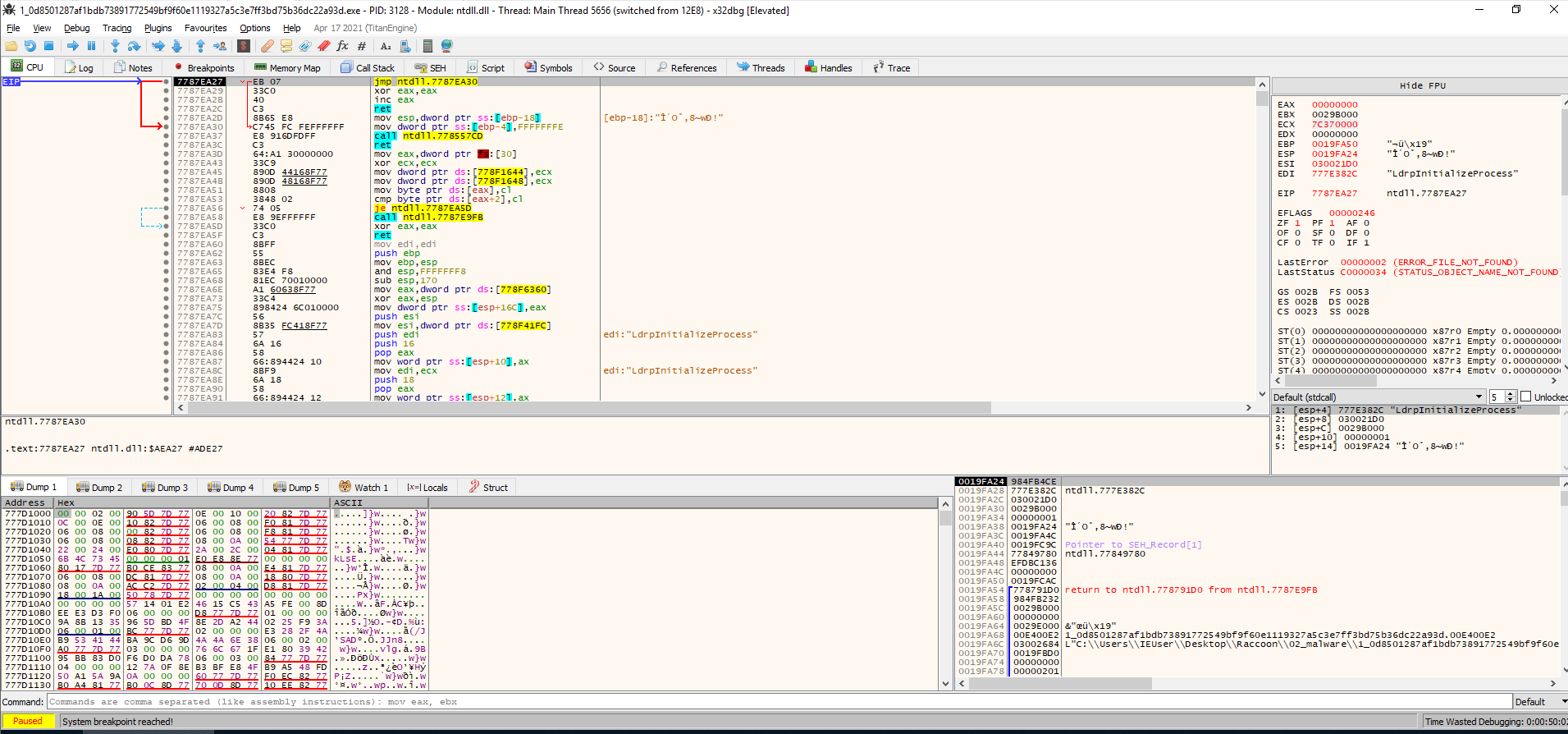
Ref: <https://app.any.run/tasks/1a9215f0-2c65-4fa1-a683-7126ee506b1a/>

# **DYNAMIC ANALYSIS-**

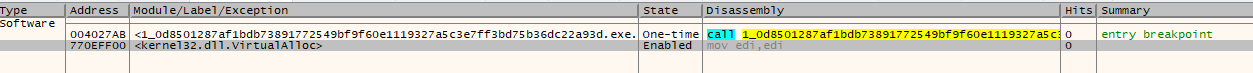
**TOOLS USED -** x32dbg, app.any.run

Let’s see the Dynamic Analysis now-

1. x32dbg



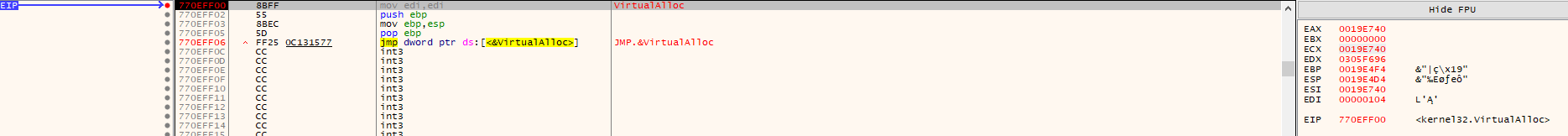
Breakpoint at VirtualAlloc



Pointer moved to user code

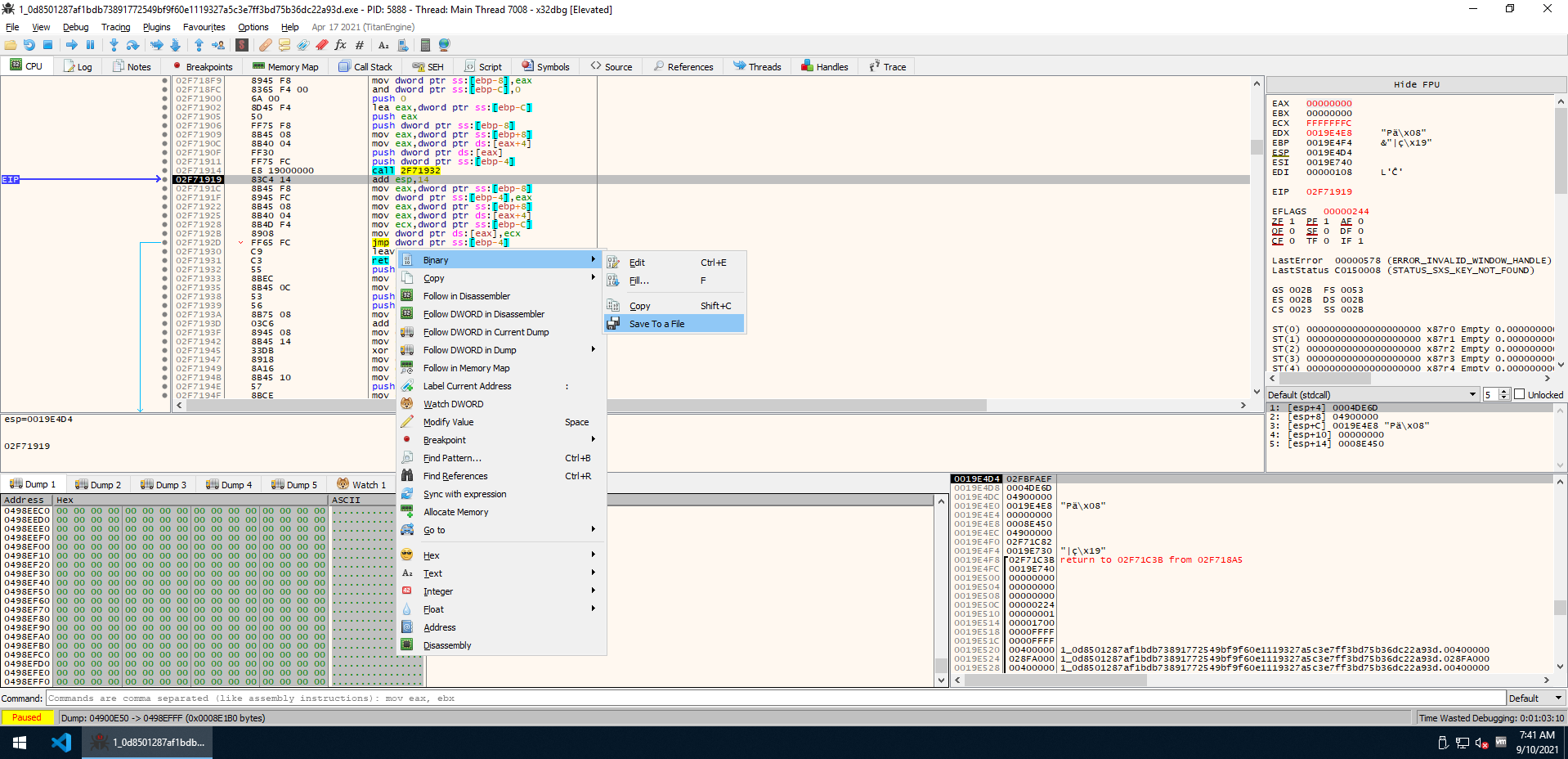


Code execution stopped at breakpoint

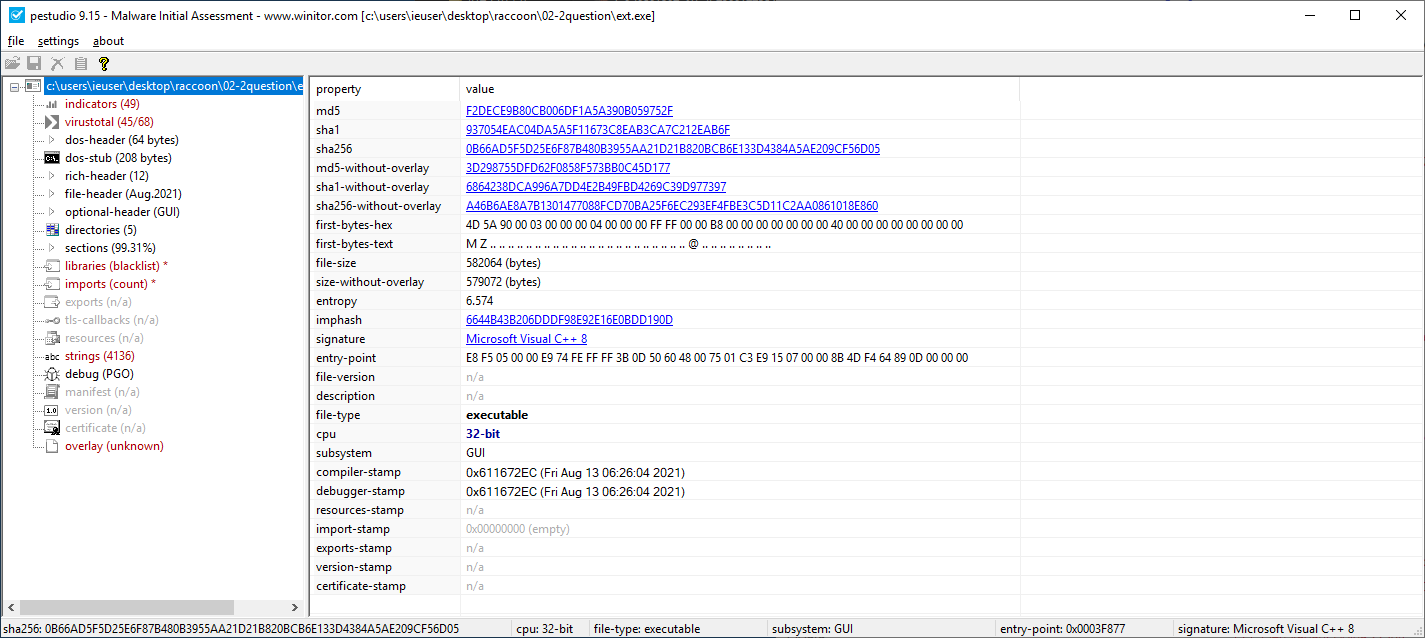


Execute till return and follow the mem allocation in dump

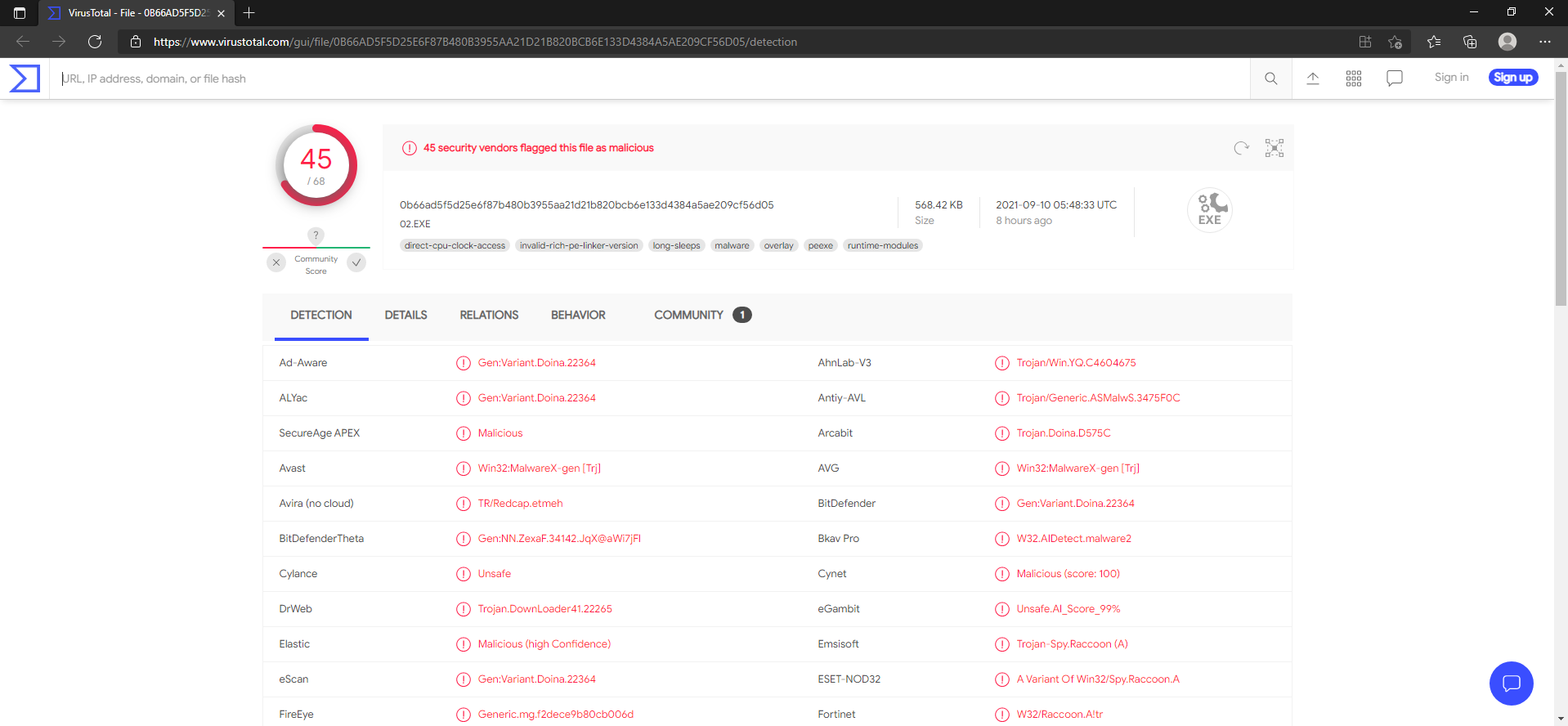




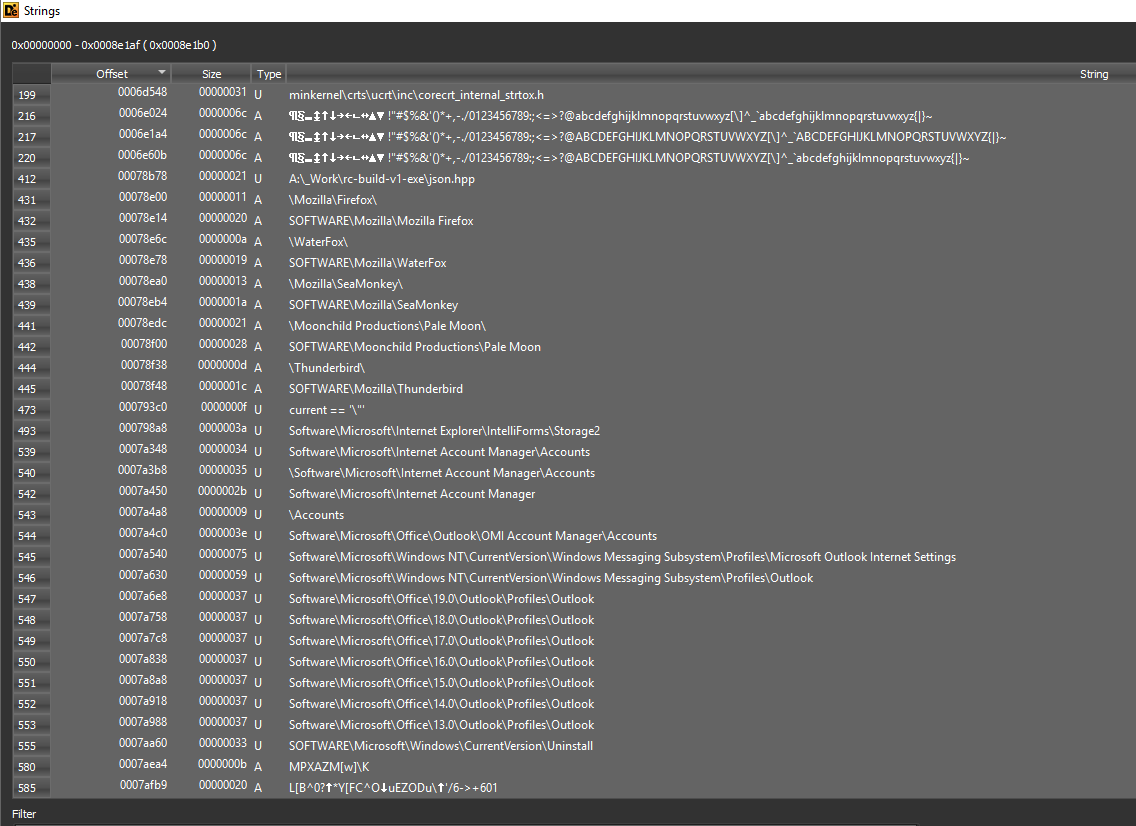
Extracted exe file

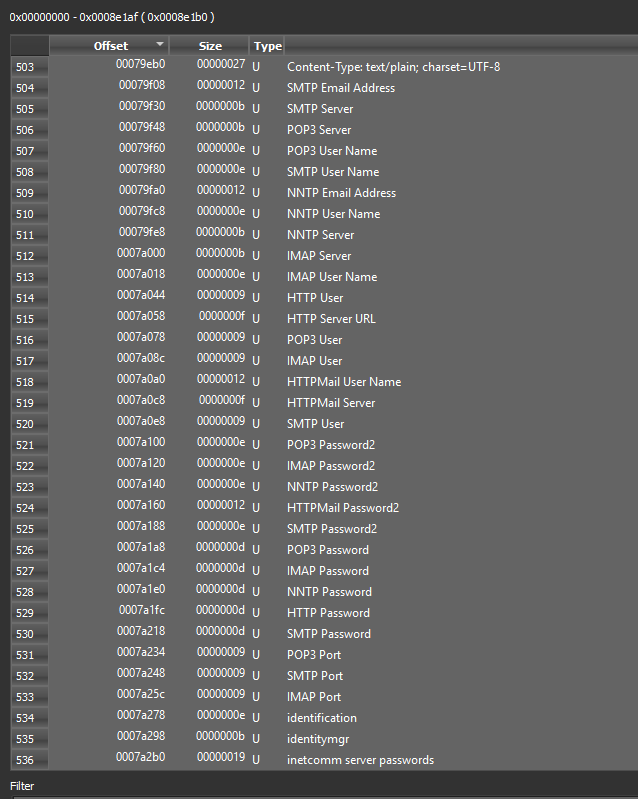


VirusTotal was able to detect the malware.

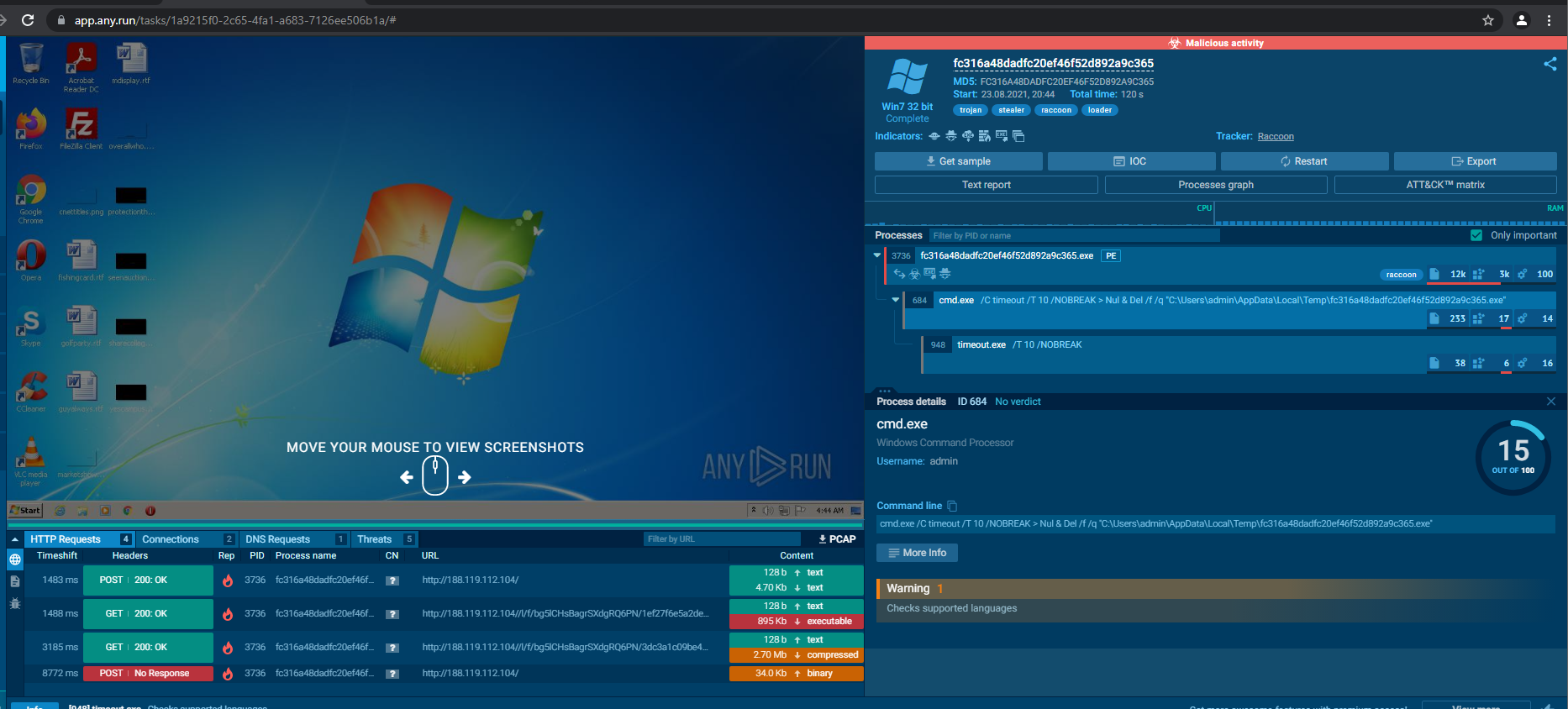


Through x32dbg, we decrypted the malware and found below malware strings.

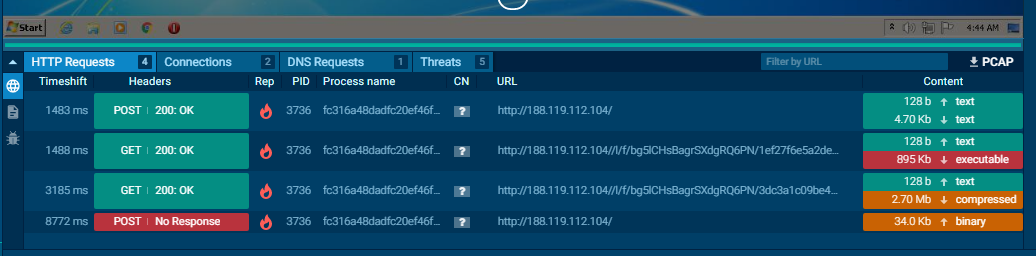




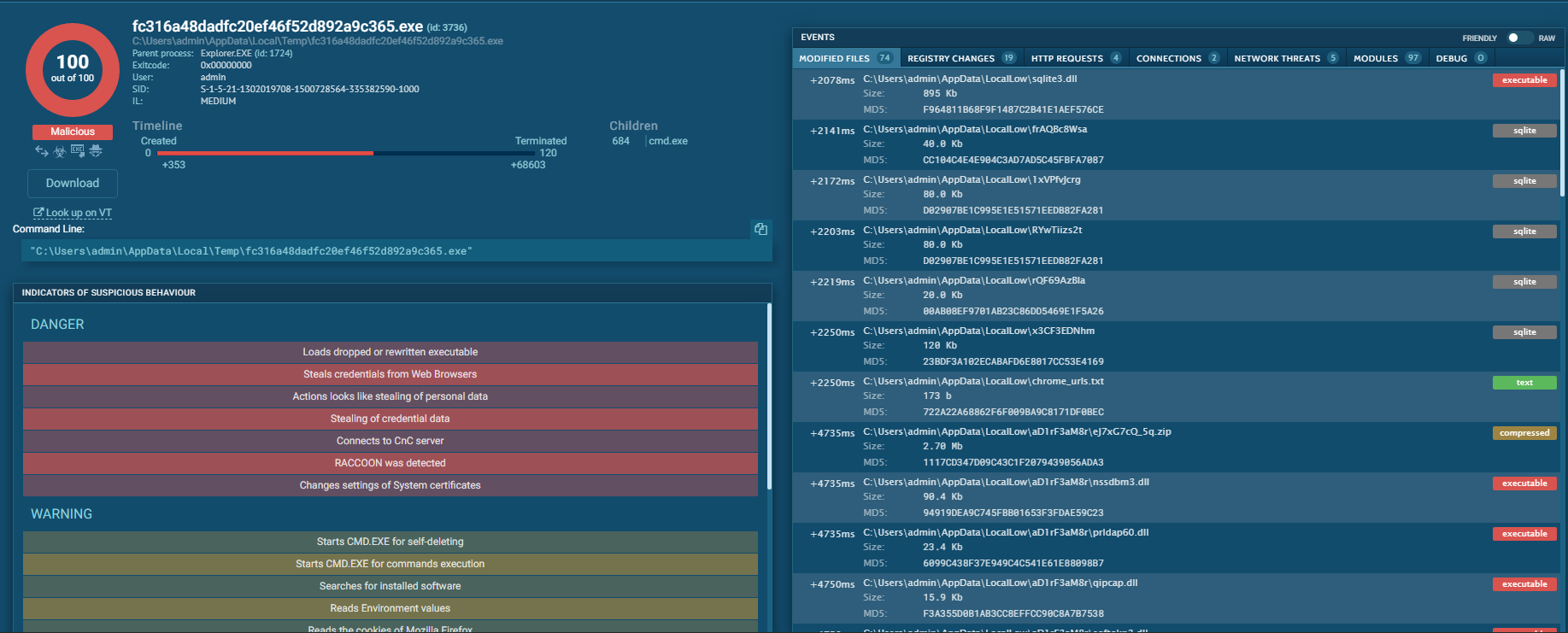
1. Running malware on app.any.run



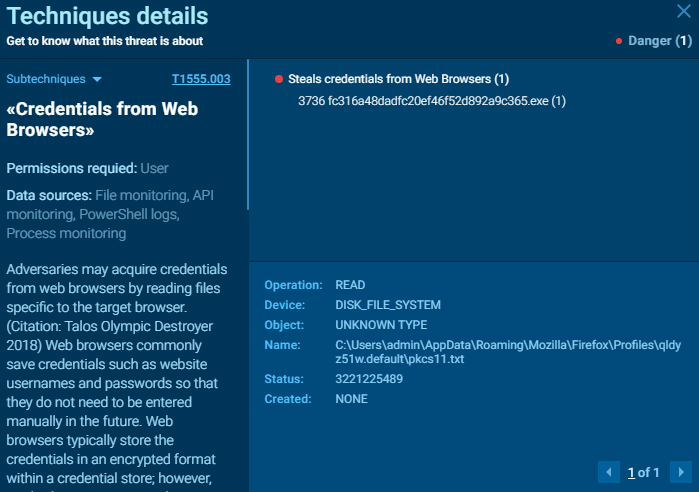
Here, POST request is sending the binary file to C&C server which contains all the stolen data.

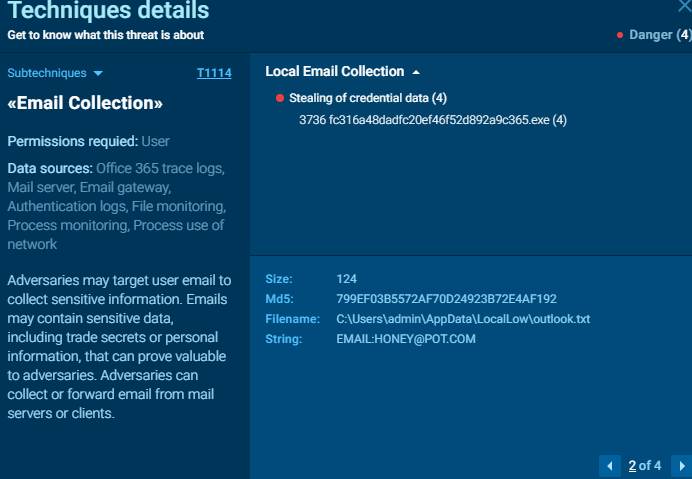


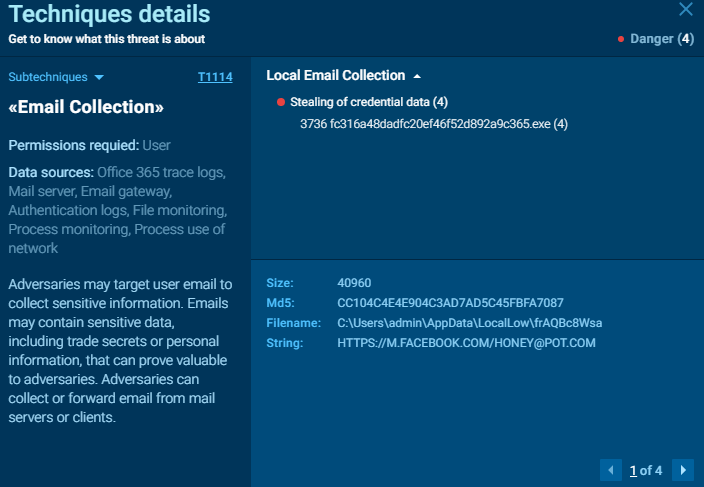
During runtime, Raccoon downloads all the files it needs (DLLs, zip file, and dropped malware) to temp folder and writes all the stolen data to text files in temp directory

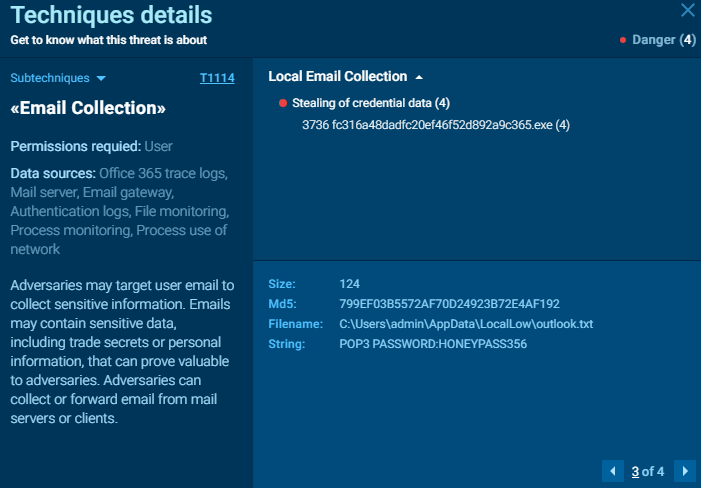


Through app.any.run, we can see the technical details too of what is being done by malware like stealing credentials from web browsers and email clients.





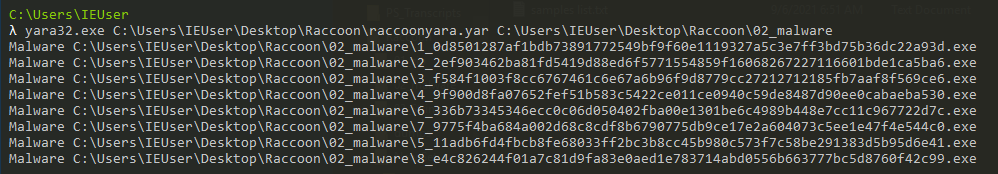




# **YARA RULE-**

To identify the malwares of Raccoonstealer family, below YARA rule has been created.





O/P of YARA rule

# **CONCLUSION-**

While Raccoon malware is not a very technically advanced malicious program it sure made a lot of noise in the underground community in 2019, when it was first released. Available as a service for $200 per month, it came equipped with everything necessary to start a malware attack. And if a customer couldn’t do it on their own, they could always get support from the team behind this malware.

In fact, underground forums are filled with raving feedback about the excellent work of Raccoon support staff. Some even say that they were treated like real VIPs.

Developers have also shown that they are capable of rolling out updates very quietly and promise to upgrade the malware with Keylogger functionality in the near future.

While technical simplicity makes this threat relatively easy to defend against at the moment, growing popularity, extreme ease of use, and potential future improvement certainly suggest that this malware can become a big phenomenon.

# **References-**

1. <https://www.cyberark.com/resources/threat-research-blog/raccoon-the-story-of-a-typical-infostealer>
2. <https://any.run/malware-trends/raccoon>
3. <https://bazaar.abuse.ch/sample/0d8501287af1bdb73891772549bf9f60e1119327a5c3e7ff3bd75b36dc22a93d>