ThreatMon

ARKEI STEALER

@threatmon

@MonThreat

ThreatMon Arkei Stealer Malware Analysis

Executive Summary

What Is Malware?

Malware, short for "Malicious Software", is software developed by cybercriminals to steal information and damage devices connected to the Internet. Common examples of malware are traditionally viruses, worms, trojans, and ransomware. However, stealer pests have also come to the fore in recent years.

What is Stealer Malware?

Stealer, as a term, completes itself as an information thief. This type of malware infects the device and then collects data from the device to send the information to the attacker. Typical targets are credentials used in online banking services, emails, or FTP accounts.

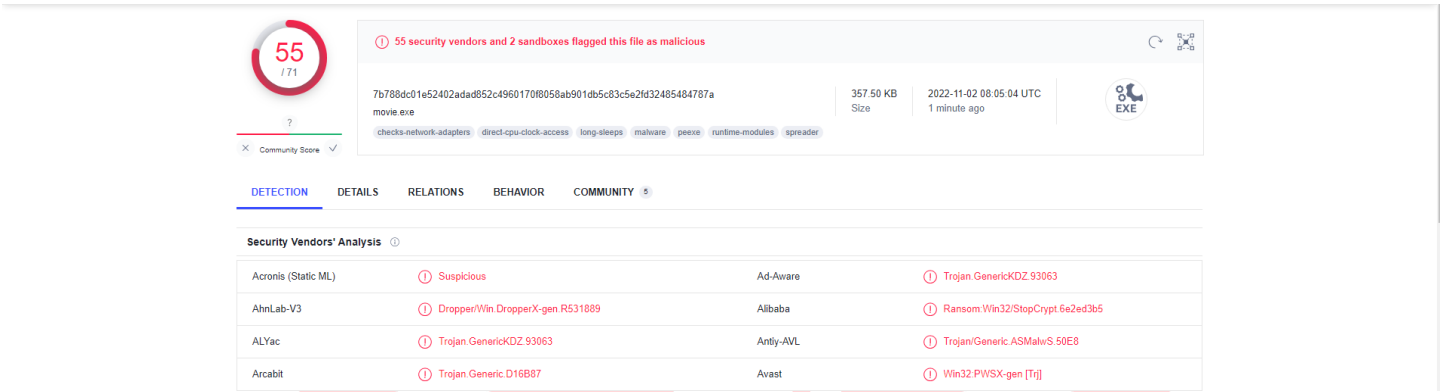
What is Arkei Stealer?

Arkei is a stealer family, mostly written in C++. It was first seen in the wild around May 2018. It collects data about local computer, browser cookies, messengers, cryptocurrency wallets. Then it zips the collected data and upload to Hacker’s C&C Channel.

Static Analysis

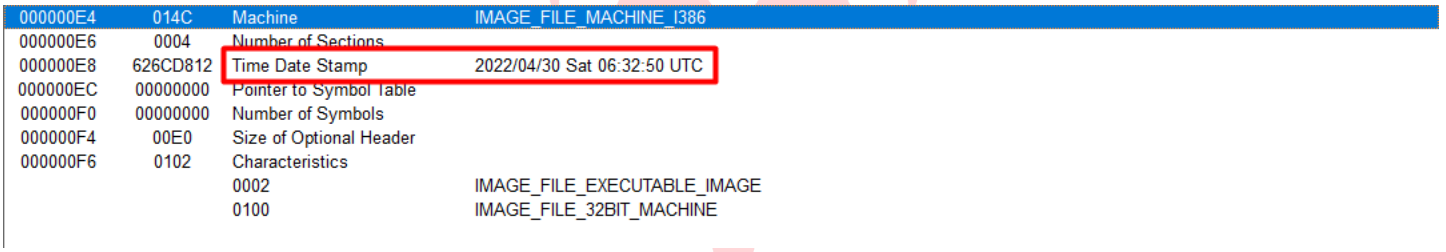
Virustotal Check

"55 Security vendors and 2 sandboxes flagged this file as malicious." So we understood that this Malware doesn't do much to bypass Anti-Viruses.

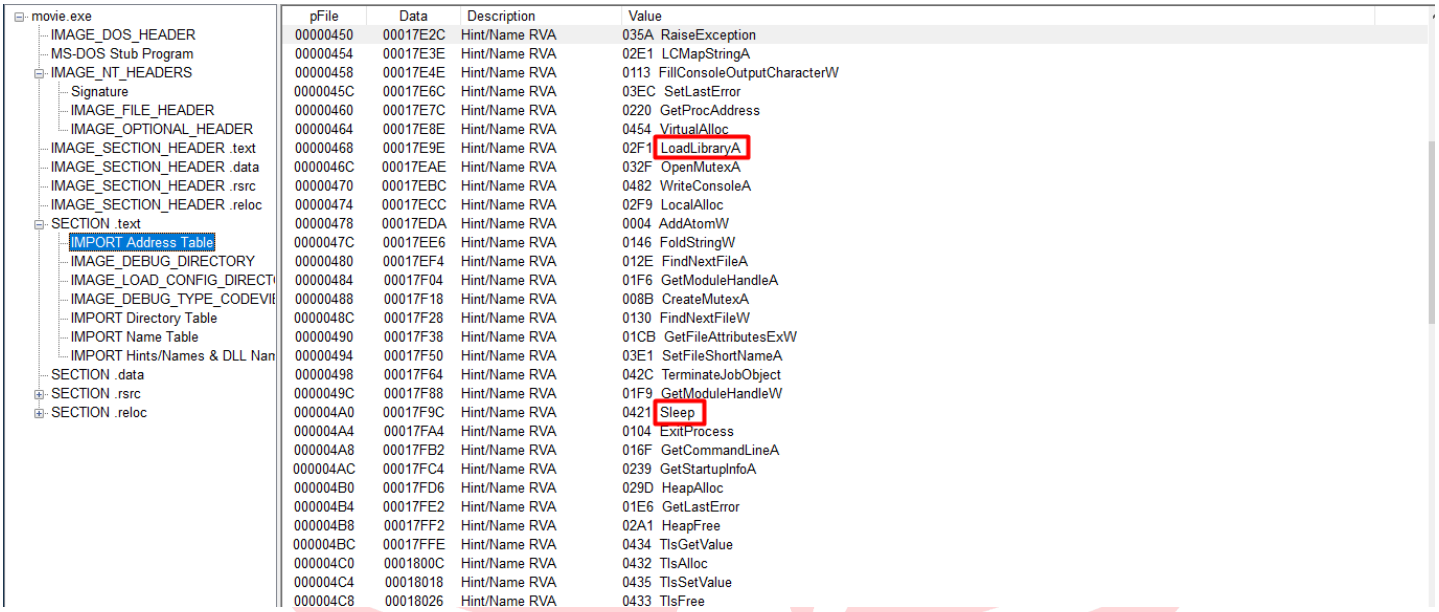


Examining PE File Header

Malware's compilation date is 30/04/2022, it has been with us for 6 months.



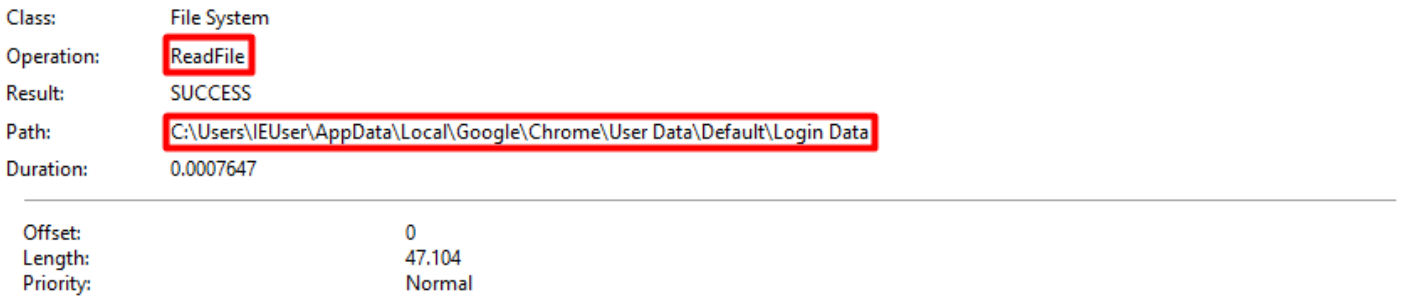
In the Import Address Table, we found **LoadLibrary** and **Sleep** API Calls which are used to bypass AV's. Malware sleeps for a while after starting so AV thinks that this file does nothing then loads other libraries dynamically.

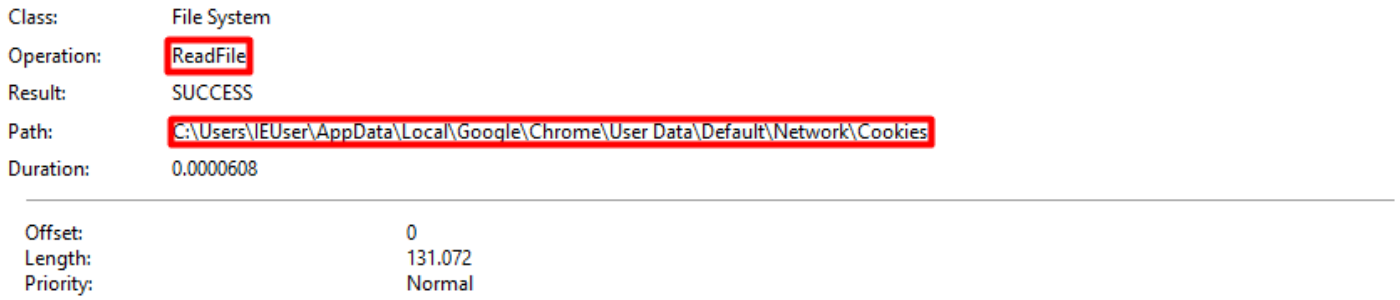


Strings of file are heavily obfuscated so it makes our job harder, we will keep further with Dynamic Analysis.

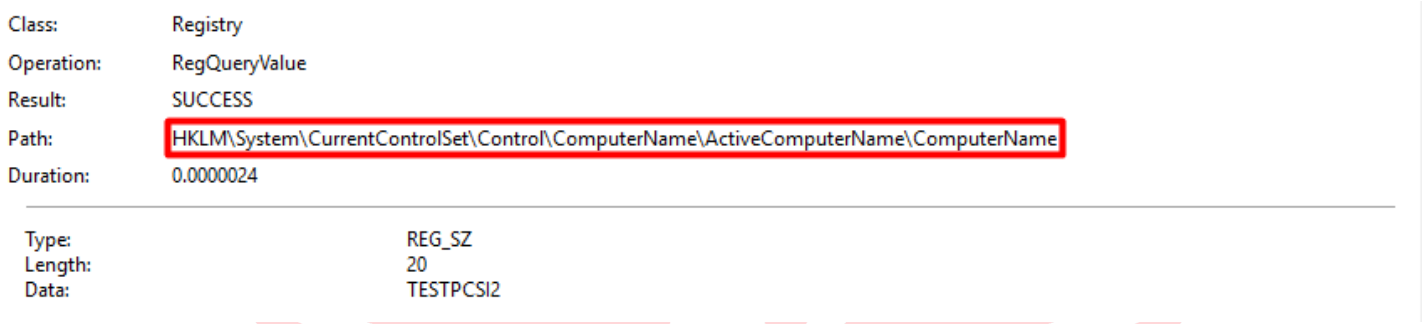
Dynamic Analysis

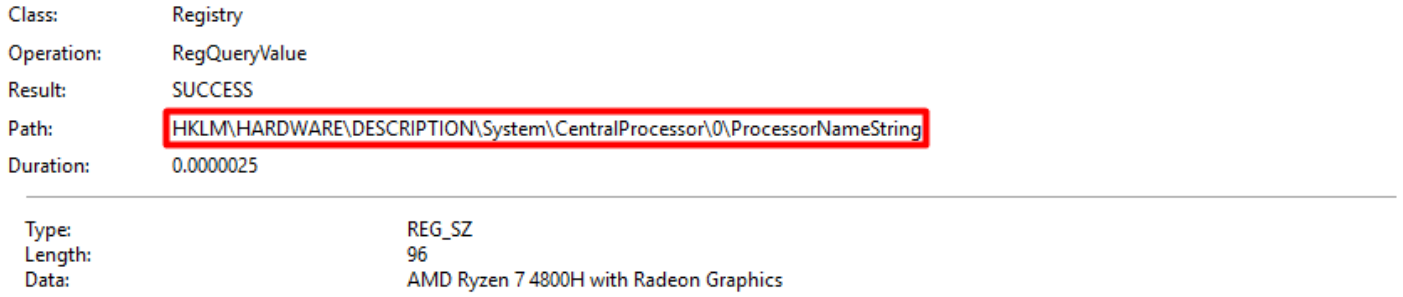
After execution of the file, it read Browser Credential Data, Cookies and some System Information.



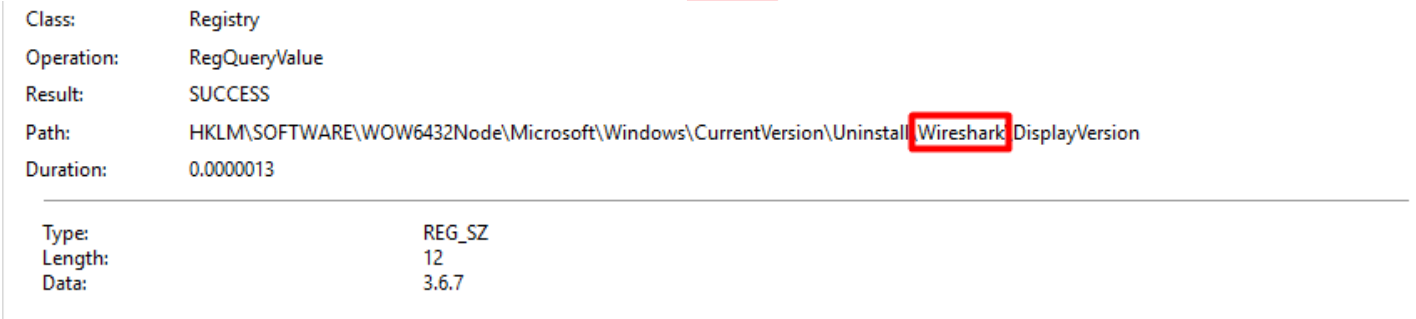


Read Computer name, CPU Information.

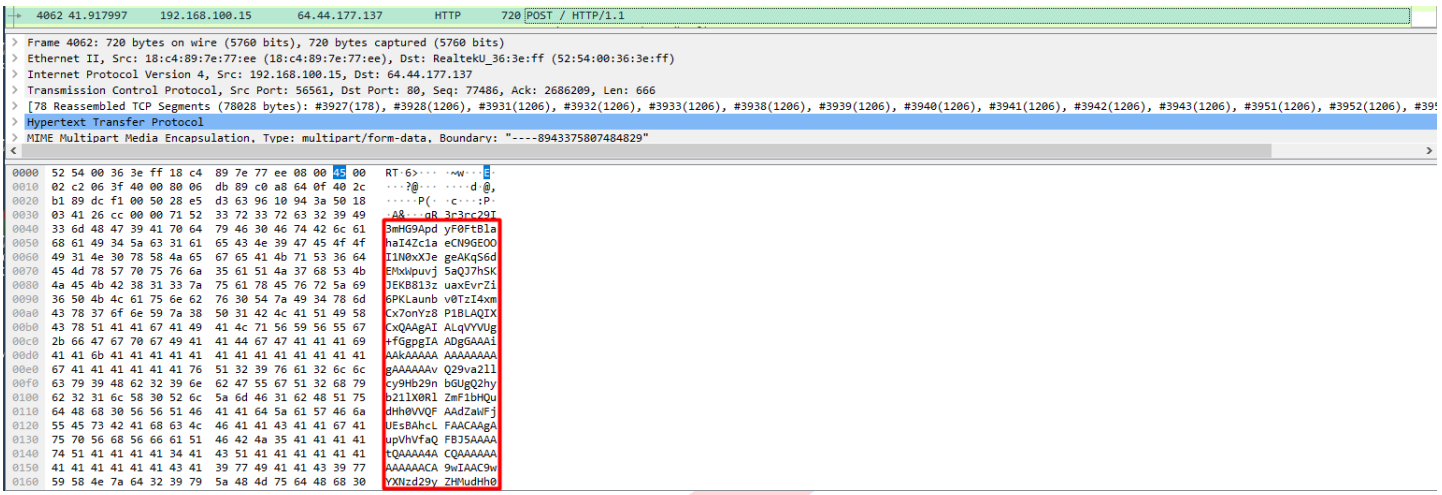




Searches for installed softwares.



After these operations, Malware sent the encrypted data to Hacker's C&C Channel over HTTP Protocol.



We have seen a little bit of the behavior of the Malware. We will continue with Code Analysis to dig deeper and understand inner workings.

Code Analysis

In addition to file reading operations, we see that wallets and some messenger data are read here. We also see Multi-Factor Authenticators are targeted.

Wallet List:

- EQUAL Wallet
- BitApp Wallet
- iWallet
- Guild Wallet
- Ronin Wallet

- Clover Wallet
- Liquality Wallet
- Auro Wallet
- Polymesh Wallet
- EVER Wallet
- Brave Wallet
- Xdefi Wallet
- Nami Wallet
- Ethereum
- Coinbase
- Coinomi
- Coin98

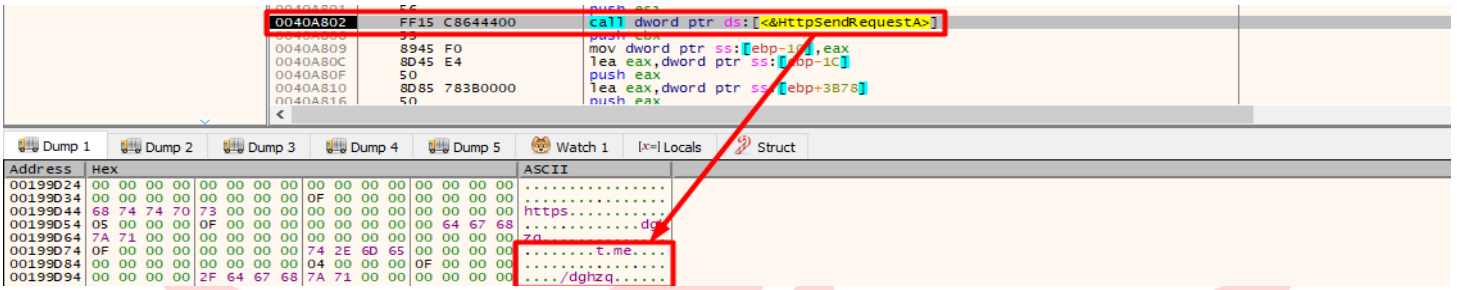
Messenger and Authenticator softwares are also targeted.

```
6A 16          push 16
59             pop ecx
A3 D05C4400    mov dword ptr ds:[445CD0],eax     00445CD0:&"Brave"
E8 24070000    call movie.403E9C
68 B0B24300    push movie.43B2B0                 43B2B0:"IFNGL5GURGW"
68 BCB24300    push movie.43B2BC
8BCF           mov ecx,edi
A3 C05E4400    mov dword ptr ds:[445EC0],eax     00445EC0:&"\\Thunderbird\\Profiles\\"
E8 0E070000    call movie.403E9C
68 C8B24300    push movie.43B2C8                 43B2C8:"9XRGLTASU689J0887V"
68 DCB24300    push movie.43B2DC
6A 12          push 12
59             pop ecx
A3 4C5C4400    mov dword ptr ds:[445C4C],eax     00445C4C:&"Thunderbird"
E8 F7060000    call movie.403E9C
68 F0B24300    push movie.43B2F0                 43B2F0:"IGEXO777U"
68 FCB24300    push movie.43B2FC
6A 09          push 9
59             pop ecx
A3 F05C4400    mov dword ptr ds:[445CF0],eax     00445CF0:&"\\Telegram Desktop\\"
E8 E0060000    call movie.403E9C
68 08B34300    push movie.43B308                 43B308:"MCSA"
68 10B34300    push movie.43B310                 43B310:" \"#k"
6A 04          push 4
59             pop ecx
A3 20624400    mov dword ptr ds:[446220],eax     00446220:&"key_datas"
E8 C9060000    call movie.403E9C
68 18B34300    push movie.43B318                 43B318:"R4G5D852I53X1KFEP"
68 2CB34300    push movie.43B32C
6A 11          push 11
59             pop ecx
A3 1C5F4400    mov dword ptr ds:[445F1C],eax     00445F1C:&"map*"
E8 B2060000    call movie.403E9C
68 40B34300    push movie.43B340                 43B340:"N6J8IARL7TJN9YPB6"
68 54B34300    push movie.43B354
6A 11          push 11
59             pop ecx
```

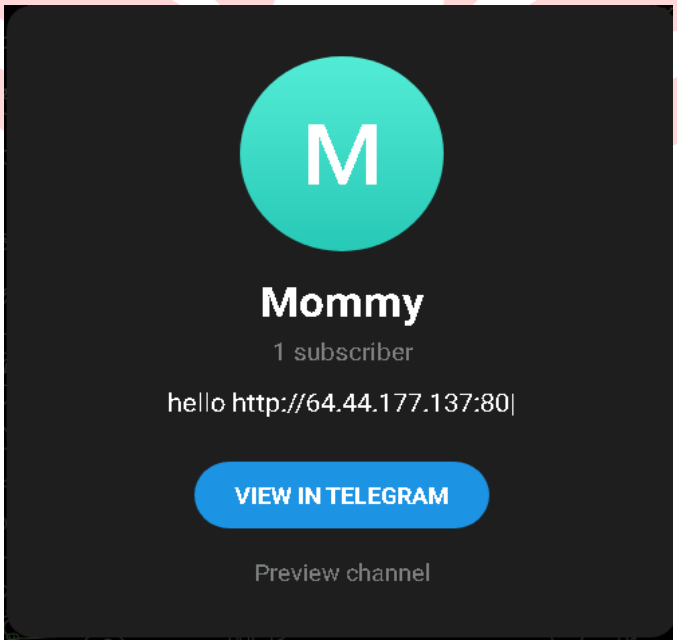
```
A3 BC5A4400    mov dword ptr ds:[445ABC],eax     00445ABC:&"Authy"
E8 C0120000    call movie.403E9C
68 D89F4300    push movie.439FD8                 439FD8:"UTH46Q9OJ6P2VL2OX"
68 EC9F4300    push movie.439FEC
6A 11          push 11
59             pop ecx                           ecx:"/1636"
A3 245D4400    mov dword ptr ds:[445D24],eax     00445D24:&"oeljdldpnmdbchonielidgobddfffla1"
E8 A9120000    call movie.403E9C
68 00A04300    push movie.43A000                 43A000:"7UBS3ZC9JK353TFLTO8BPNKCWV2QASMD"
68 24A04300    push movie.43A024                 43A024:"^9%0]2&U:([[P1#%$YH+:/')<4^3\"</("
8BCE           mov ecx,esi                       ecx:"/1636"
A3 505B4400    mov dword ptr ds:[445B50],eax     00445B50:&"EOS Authenticator"
E8 93120000    call movie.403E9C
68 48A04300    push movie.43A048                 43A048:"54FTKH14F5XFGTQNKRC"
68 5CA04300    push movie.43A05C                 43A05C:"ru3 #hpA2]=(3=2/?=1"
6A 13          push 13
59             pop ecx                           ecx:"/1636"
A3 D85E4400    mov dword ptr ds:[445ED8],eax     00445ED8:&"ilgcnhelpchnceeipipijaljkblbcobl"
E8 7C120000    call movie.403E9C
68 70A04300    push movie.43A070                 43A070:"V3NHTJ96I6V8O8OA8OWBL9E6TOE6CEPGSQOJRWWJKLS7T6O"
68 A8A04300    push movie.43A0A8
6A 36          push 36
59             pop ecx                           ecx:"/1636"
A3 A8614400    mov dword ptr ds:[4461A8],eax     004461A8:&"GAuth Authenticator"
E8 65120000    call movie.403E9C
68 E0A04300    push movie.43A0E0                 43A0E0:"OWYQX2ED3DRP"
68 F0A04300    push movie.43A0F0
6A 0C          push C
59             pop ecx                           ecx:"/1636"
A3 84614400    mov dword ptr ds:[446184],eax     00446184:&"\\com.liberty.jaxx\\IndexedDB\\file__0.indexe
E8 4E120000    call movie.403E9C
68 00A14300    push movie.43A100                 43A100:"QKHQSL2MOAQHNW47QTXQSCOEUB"
68 1CA14300    push movie.43A11C
6A 1A          push 1A
```

Connecting to C&C Server

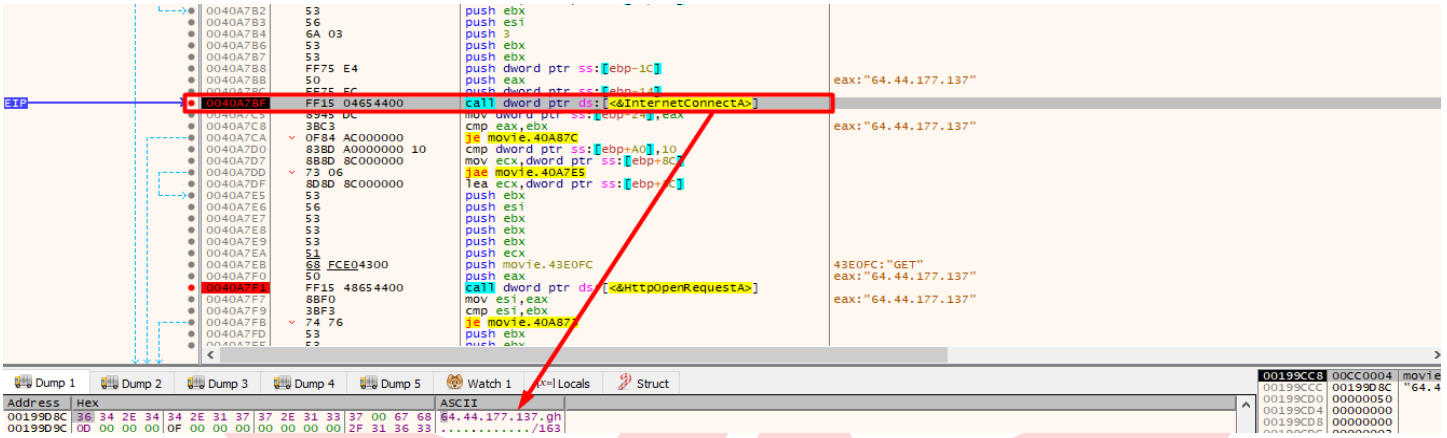
Malware follows a different and interesting way while connecting to C&C Server. It first sends a GET Request to a Telegram address. It fetches the actual C2 Server IP from the description of Telegram Channel.



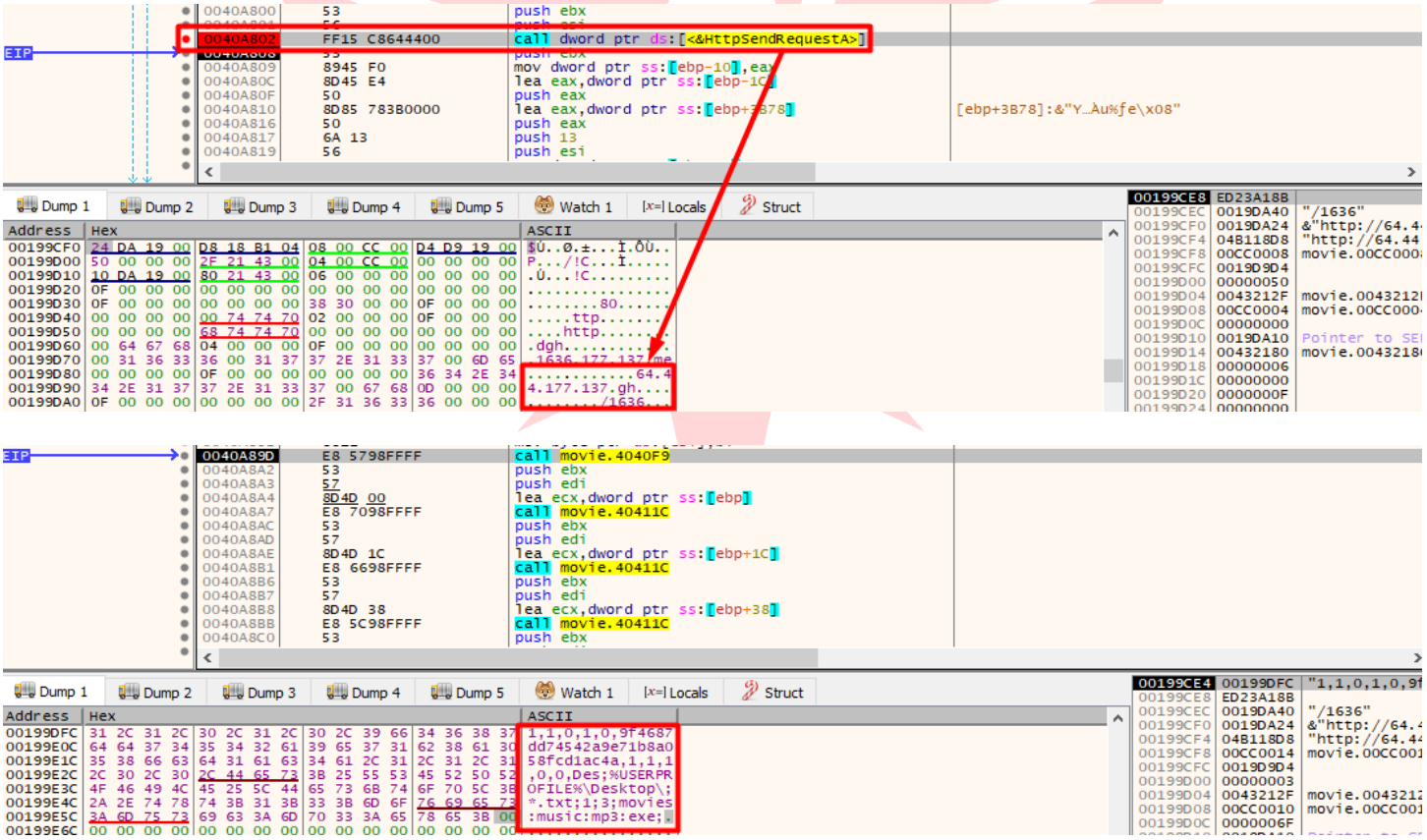
As you see, the *"hello hxxp://64[.]44[.]177[.]137:80"* string is located in the description of the Channel.



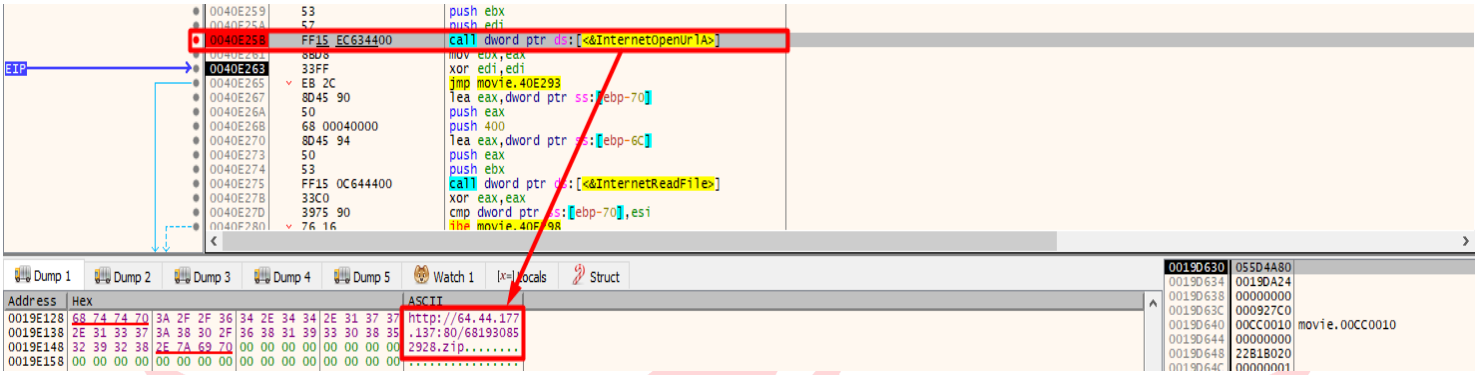
What is exactly the purpose of this behavior ? Hacker wants to make sure the malware works correctly. The IP address of C&C Channel may be blacklisted or Hacker may want to change it, that's enough to change the description of Telegram Channel, so he/she won't have to make a new binary.



After connecting to C2 Channel Malware first fetches a Config file. This file determines the pattern of the operations.



So how do we read this config ? First 1 is for Saved Passwords, second 1 is for Cookies / Autofill etc. Last part is obvious “*.txt;1;3;movies:music:mp3;exe;”. Then in addition to the Config file, Malware fetches a Zip file.

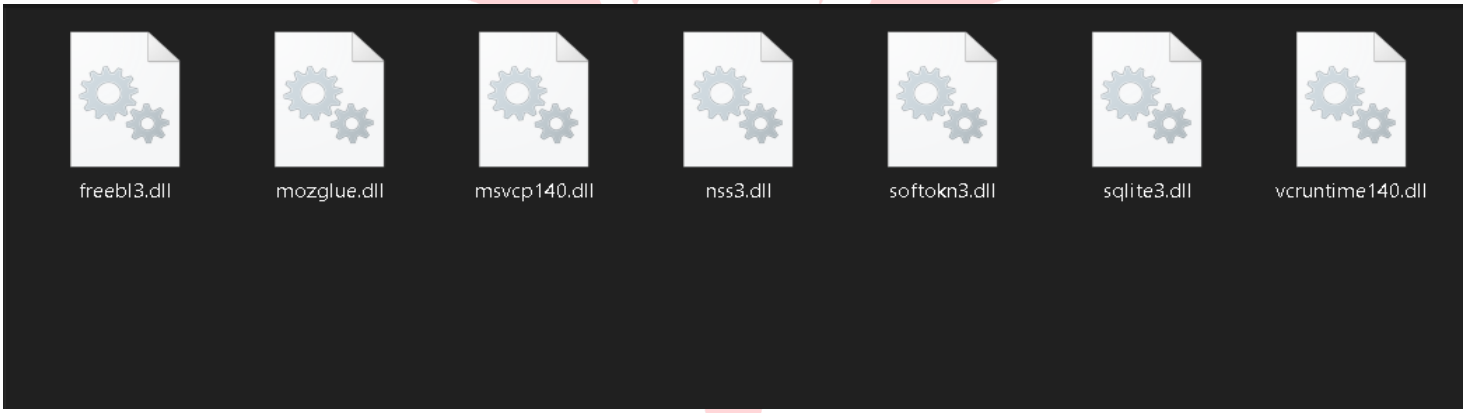


There are some libraries in zip file. These libraries are necessary to grab some kind of data. For instance :

Freebl3.dll : Freebl Library of Mozilla Firefox

Mozglue.dll : Library for Firefox

Vcruntime140.dll : Library for Visual Runtime

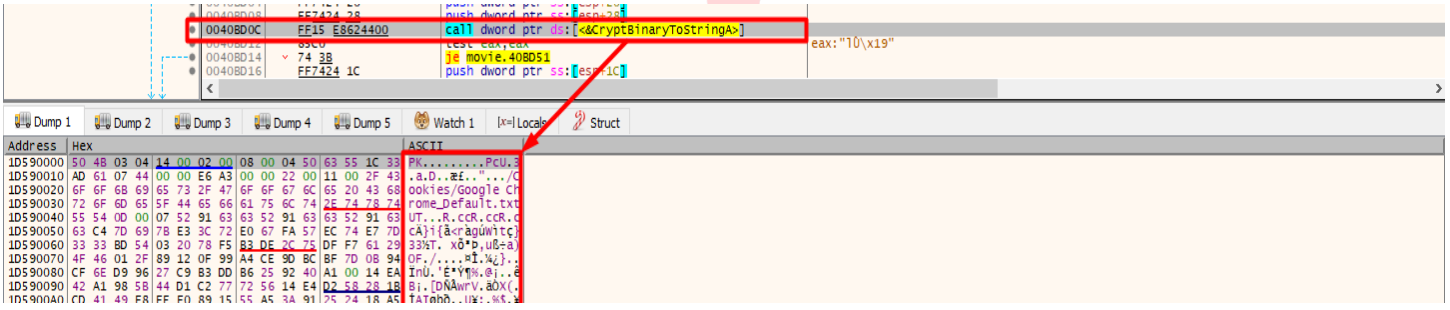


Taking Screenshot

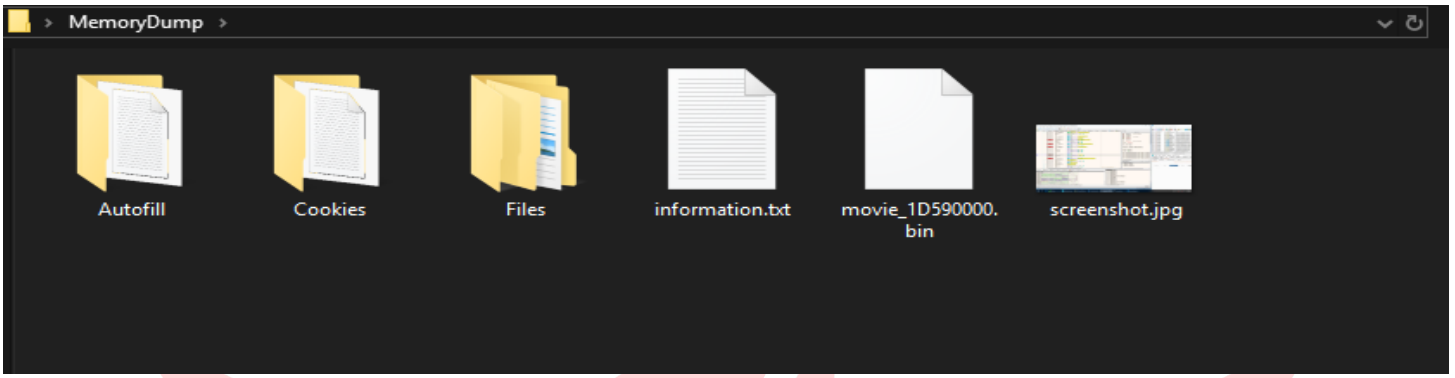
It has been detected that the Malware has taken a screenshot with help of **gdip** library.

Encrypting and Uploading the Collected Data

After all of these operations Malware zips the data that are collected. Then it encrypts the zip file to make it ready to be uploaded. We generated a **memory dump** before Malware encrypts the data.

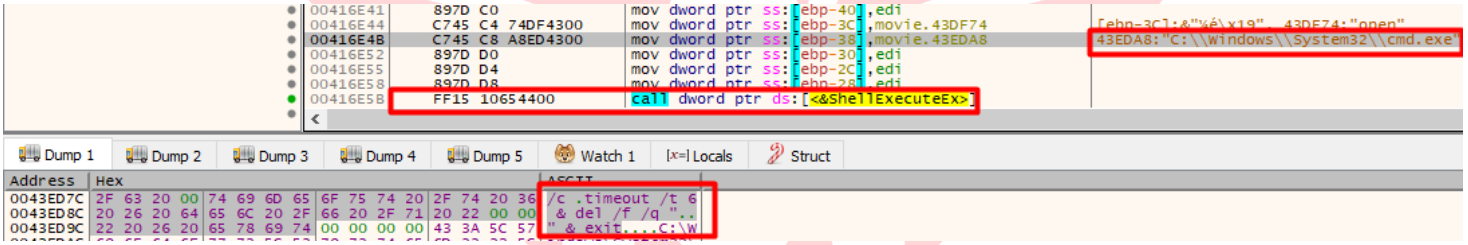


In the zip file there are data that are taken from Browsers, some information about our local Computer and there is a screenshot when we were debugging the Malware.



Finally, Malware is getting ready to destroy itself.

"C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "movie.exe" & exit



INDICATOR OF COMPROMISE (IOC)

SHA-256 HASH
7b788dc01e52402adad852c4960170f8058ab901db5c83c5e2fd32485484787a

IP/URL
t.me/dghzq
http://64[.]44[.]177[.]137:80
http://64[.]44[.]177[.]137/1636
http://64[.]44[.]177[.]137/090459701475.zip

MITRE ATT&CK

TECHNIC	ID
Steal Web Session Cookie	T1539
Credentials From Password Stores	T1555
Unsecured Credentials	T1552
Query Registry	T1012
Software Discovery	T1518
System Information Discovery	T1082
Ingress Tool Transfer	T1105
Exfiltration Over Alternative Protocol	T1048