Malware Reverse Engineering, Spring 2022

Practical 3

P0X03

Date: 10th April, 2022

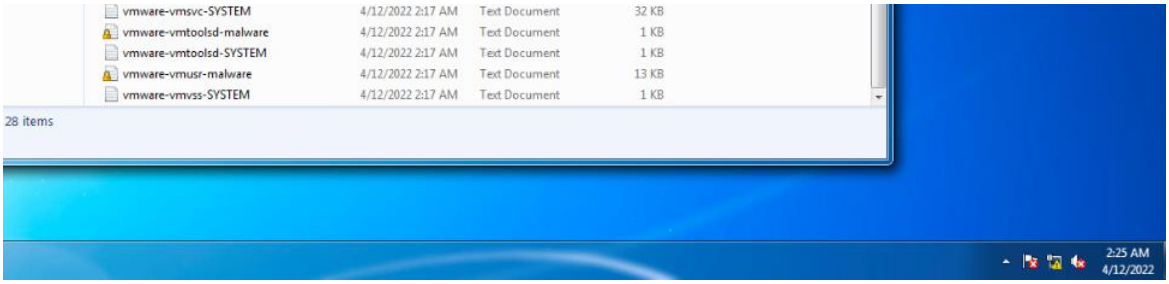
Prepared by:
Sudhanshu Tarale
starale@ufl.edu
UFID: 66177686

Executive Summary:

The malware with sha256 hash 94A84585432FB2AE6E9F836A92EFF960736416CB6E4E0D34B920E6DBC14F4246 is of Emotet family (a family of banking trojan malwares). When we run the malware we can see in the network activity that the malware is trying to contact C&C servers. This malware is essentially a credential stealer that can attack the host machine as a form of website, downloadable document, link etc.

Some key activities that the malware performs are:

- Creates files in the C:\Windows\Temp folder



vmware-vmsvc-SYSTEM	4/12/2022 2:17 AM	Text Document	32 KB
vmware-vmtoolsd-malware	4/12/2022 2:17 AM	Text Document	1 KB
vmware-vmtoolsd-SYSTEM	4/12/2022 2:17 AM	Text Document	1 KB
vmware-vmusr-malware	4/12/2022 2:17 AM	Text Document	13 KB
vmware-vmvss-SYSTEM	4/12/2022 2:17 AM	Text Document	1 KB

28 items

2:25 AM 4/12/2022

- Makes changes to registry keys

4:1...	rundll32.exe	3848	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	Desired Access: R...
4:1...	rundll32.exe	3848	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs	SUCCESS	Type: REG_DWO...
4:1...	rundll32.exe	3848	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	
4:1...	rundll32.exe	3848	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: R...
4:1...	rundll32.exe	3848	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS	Desired Access: R...
4:1...	rundll32.exe	3848	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap	NAME NOT FOUND	Length: 144

- Imports functions like TerminateProcess, SuspendThread, RegCreateKeyA, SetFileAttributesA etc. This shows that the malware works with processes, registry keys and the file system of the local machine.

- Network calls are made to external domains like sf.symcd.com where potentially the malware can have access to more malicious files.

Static Analysis:

a. Compilation date of the program:

Compilation date of the malware is March 4th, 2022 at 12:51:31

subsystem	GUI
compiler-stamp	0x62220B53 (Fri Mar 04 12:51:31 2022 | UTC)
debugger-stamp	n/a

b. Suspicious properties of program's Imports:

TerminateProcess: Terminates a process and all of it's threads. **GetEnvironmentVariable** let's the malware retrieve the environment variable for the current process. **GetTimeZoneInformation** gets the current time zone settings. **SetEnvironmentVariableA** can be used by the malware to some specific environment variable for a process. **SetFileAttributesA, FindFirstFileA, UnlockFile, WriteFile, LockFile, DeleteFileA, MoveFileA** shows that the malware is working with files. **GetVolumeInformationA** get's information about the file system and volume associated with the root directory. **GetCurrentProcessId,GetCurrentThreadId** gets the process/thread ID of a particular process/thread. Malware can use this to get a process, change it's environment variables etc. **RegisterClipboardFormatA** registers a new clipboard format. **SuspendThread** suspends a thread. **PostThreadMessageA** posts a message to a specified thread. This means that the malware is accessing a thread to send some message. **WinHelpA** launches Windows Help (malware starts winhelp.exe process). **GetCapture** receives mouse input in a particular windows meaning that the malware tracks mouse events. **SystemParametersInfoA** retrieves or sets the value of one of the system-wide parameters. This function can also update the user profile while setting a parameter. **RegCreateKeyA, RegDeleteValueA, RegSetValueExA, RegSetValueA, RegEnumKeyA, RegDeleteKeyA** shows us that the malware is working with registry keys.

c. Suspicious Strings:

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, Software\Microsoft\Windows\CurrentVersion\Policies\Network, Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32, Software\Classes, Software : These strings show that the malware is working with these registry keys. **Command failed.)Insufficient memory…Registry entries have been removed** also shows that the malware is working with Registry entries.

Destination disk drive is full.5Unable to read from %1, it is opened by someone else.AUnabl...
Enter a number.#Enter an integer between %1 and %2.!Enter a number between %1 and %2...
%1 contains an incorrect path.8Could not open %1 because there are too many open files.
Access to %1 was denied.0An incorrect file handle was associated with %1.8Could not rem...
Seek failed on %14Encountered a hardware I/O error while accessing %1.3Encountered a sh...
Disk full while accessing %1.$Attempted to access %1 past its end.
No error occurred.-An unknown error occurred while accessing %1.%Attempted to write to...
%1 has a bad format."%1 contained an unexpected object. %1 contains an incorrect schema.
%1: %2\r\nontinue running script?
t.Ht

Here we can see the error messages that the malware might be using while performing it's activity.

USER32.DLL, GDI32.DLL, COMDLG32.DLL,COMCTL32.dll,CustomMessageBox.dll are some of the dll's that are being used by the malware. **RecentFileList** shows that the malware is accessing files. **unsigned, long, int short, char**: Maybe the malware is working with different datatypes.

HH:mm:ss
dddd, MMMM dd, yyyy
MM/dd/yy
December
November
October
September
August
July
June
April
March
February
January
Saturday
Friday
Thursday
Wednesday
Tuesday
Monday
Sunday
am/pm
united-states
united-kingdom
trinidad & tobago

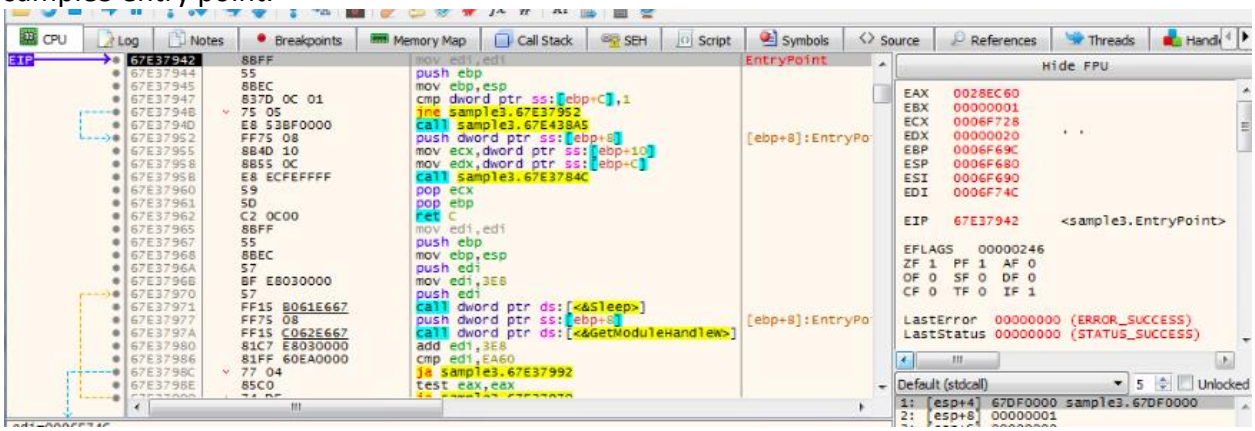
Here we can see the time and date formats along with name of months and countries suggesting that maybe the malware is using different timezones to it's benefit. **GetDateFormat** and **GetTimeFormat** also points to the same. **DllGetVersion** get's the version of cabinet.dll file.

d. Anti-Disassembly techniques

Nothing found as ghidra was able to disassemble the dll file without any errors.

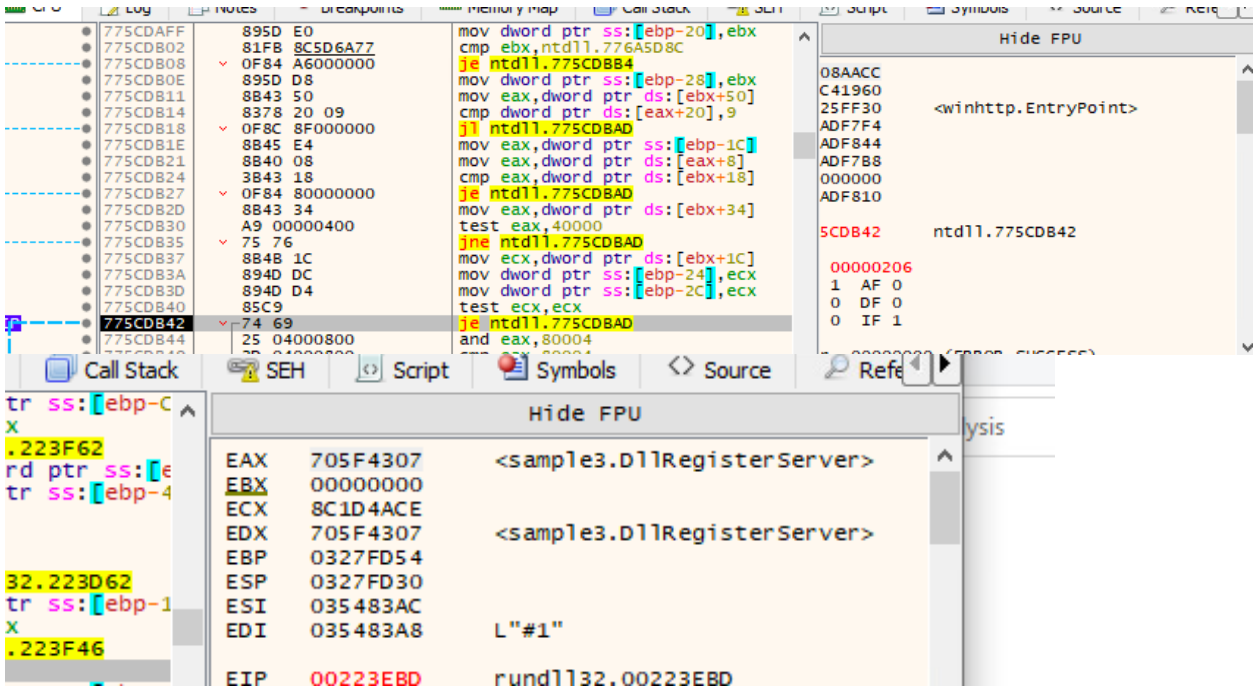
e. Is the program obfuscated?

Yes, the program is obfuscated. After loading the rundll32.dll file into x32dbg and changing the command line arguments to include sample3.dll file with #1 as the ordinal, we can run the debugger and we finally reach a point where we get the sample3 entry point.



Once we continue running from here we can see that in some of the functions being called some of the DLL's that are being imported by the malware.

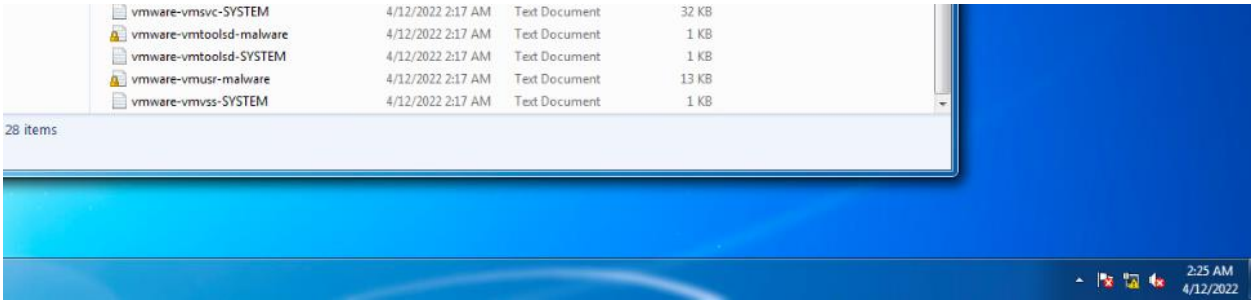
Here we can see that



Dynamic Analysis

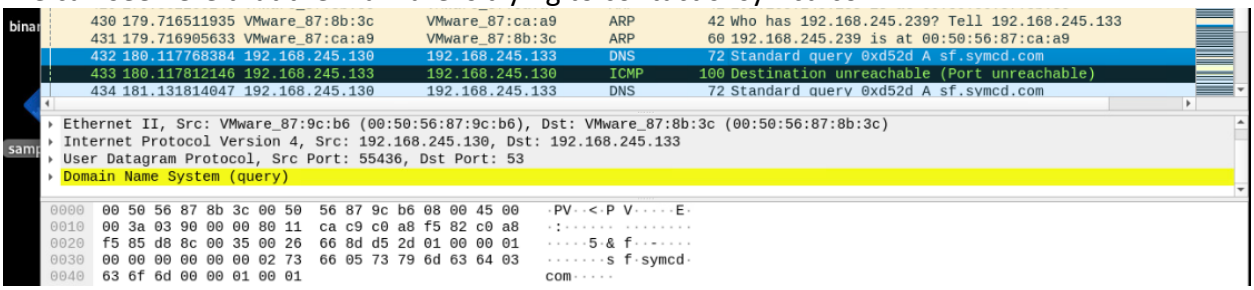
a. Interesting Behavior after malware execution

Once the malware is run, we can see in C:\Windows\Temp directory that some file are created. We can see the file creation time and the time on the local machine in the screenshot below.

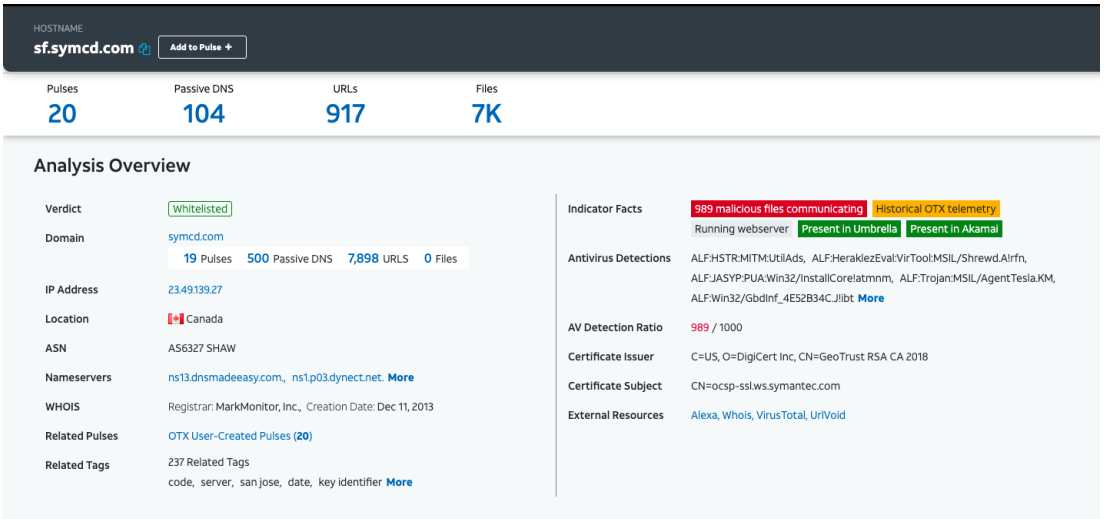


b. Network Calls:

We can see here that the malware is trying to contact sf.symcd.com.



A quick google search about sf.symcd.com shows us a domain with many malicious files hosted in it. Maybe the malware is trying to contact the domain to get access to these files.



HOSTNAME

sf.symcd.com Add to Pulse +

SHOWING 1 TO 10 OF 917 ENTRIES

1 2 3 4 5 ... 92 NEXT >

Associated Files

Show 10 entries

DATE	HASH	AVAST	AVG	CLAMAV	MSDEFENDER
Apr 10, 2022	a8a4bf2fa5e7481018da32150a60efb51643ce9afab54288b00c5f-da6c073a63			Win.Malware.Slimware-680448...	
Apr 9, 2022	cc93b64865955fc6a7c75bc779219cd3f3ca89fc355f24dcc1c98f128f1e9568			Win.Malware.Slimware-680448...	
Apr 9, 2022	9443c42a4e5dcc176f61b7c70708596b13d2019703d5dded3c3d-d024983f38c4				ALF:HSTR:MITM:UtilAds

Here we can see that the malware is making some DHCPv6 calls and we can see interesting things like “2022Malware7-2”.

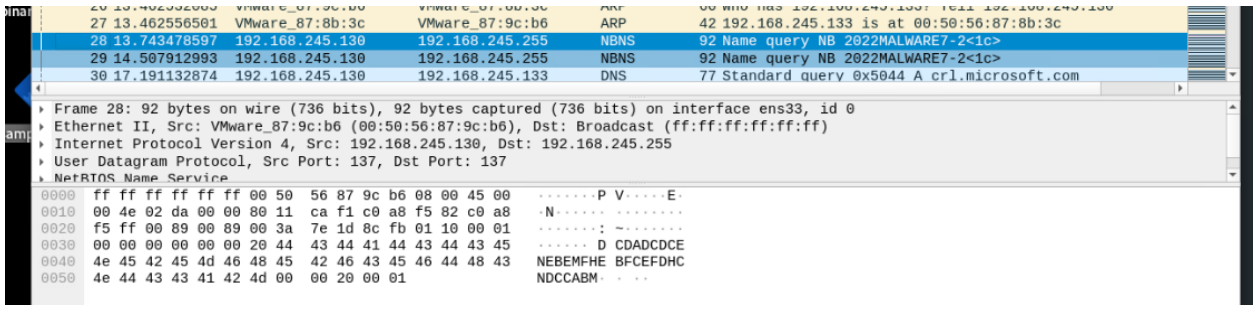
```
190.897453828 192.168.245.130   192.168.245.133   DNS     83 Standard query 0x90da A ctldl.windowsupdate.com
190.897470319 192.168.245.133   192.168.245.130   ICMP   111 Destination unreachable (Port unreachable)
191.162875164 192.168.245.130   192.168.245.255   NBNS    92 Name query NB SF.SYMCD.COM<00>
191.381140355 fe80::4112:80a3:e23… ff02::1:2      DHCPv6 156 Solicit XID: 0x40c859 CID: 0001000129e50c0a005056879cb6
191.927034435 192.168.245.130   192.168.245.255   NBNS    92 Name query NB SF.SYMCD.COM<00>
192.691420871 192.168.245.130   192.168.245.255   NBNS    92 Name query NB SF.SYMCD.COM<00>
193.643663449 192.168.245.130   192.168.245.255   NBNS    92 Name query NB SF.SYMCB.COM<00>

▸ Frame 475: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_87:9c:b6 (00:50:56:87:9c:b6), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
▸ Internet Protocol Version 6, Src: fe80::4112:80a3:e23b:13b4, Dst: ff02::1:2
▸ User Datagram Protocol, Src Port: 546, Dst Port: 547
▸ DHCPv6

0030  00 00 00 01 00 02 02 22  02 23 00 66 29 70 01 40   ······ " ·#·f)p·@
0040  c8 59 00 08 00 02 18 9c  00 01 00 0e 00 01 00 01   ·Y····· ····· ····
0050  29 e5 0c 0a 00 50 56 87  9c b6 00 03 00 0c 0e 00   )····PV· ·····
0060  0c 29 00 00 00 00 00 00  00 00 00 27 00 10 00 0e   ·)····· ···'····
0070  32 30 32 32 4d 61 6c 77  61 72 65 37 2d 32 00 10   2022Malw are7-2··
0080  00 0e 00 00 01 37 00 08  4d 53 46 54 20 35 2e 30   ·····7·· MSFT 5.0
```

```
.@.Y..............)..
.PV..........)........'....2022Malware7-2.......7..MSFT
5.0...........'.@.Y.....d........)..
.PV..........)........'....2022Malware7-2.......7..MSFT
5.0...........'.@.Y.....,........)..
.PV..........)........'....2022Malware7-2.......7..MSFT
5.0...........'.@.Y..............)..
.PV..........)........'....2022Malware7-2.......7..MSFT
5.0...........'.@.Y..............)..
.PV..........)........'....2022Malware7-2.......7..MSFT
5.0...........'.@.Y..............)..
.PV..........)........'....2022Malware7-2.......7..MSFT
5.0...........'.@.Y..............)..
.PV..........)........'....2022Malware7-2.......7..MSFT 5.0...........'
```

We can also se NBNS calls to 2022MALWARE7-2<1c>. Perhaps a device or network that malware is trying to contact.



27	13.462556501	VMware_87:8b:3c	VMware_87:9c:b6	ARP	42 192.168.245.133 is at 00:50:56:87:8b:3c
28	13.743478597	192.168.245.130	192.168.245.255	NBNS	92 Name query NB 2022MALWARE7-2<1c>
29	14.507912993	192.168.245.130	192.168.245.255	NBNS	92 Name query NB 2022MALWARE7-2<1c>
30	17.191132874	192.168.245.130	192.168.245.133	DNS	77 Standard query 0x5044 A crl.microsoft.com

```
Frame 28: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface ens33, id 0
Ethernet II, Src: VMware_87:9c:b6 (00:50:56:87:9c:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.245.130, Dst: 192.168.245.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
0000  ff ff ff ff ff ff 00 50  56 87 9c b6 08 00 45 00   ·******P V*****E·
0010  00 4e 02 da 00 00 80 11  ca f1 c0 a8 f5 82 c0 a8   ·N**************
0020  f5 ff 00 89 00 89 00 3a  7e 1d 8c fb 01 10 00 01   *******: ~*******
0030  00 00 00 00 00 00 20 44  43 44 41 44 43 44 43 45   ****** D CDADCDCE
0040  4e 45 42 45 4d 46 48 45  42 46 43 45 46 44 48 43   NEBEMFHE BFCEFDHC
0050  4e 44 43 43 41 42 4d 00  00 20 00 01               NDCCABM· · ··
```

c. Registry Keys created/modified:

Keys added:

```
----------------------------------
Keys added: 28
----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-39733034-3216902470-2998706464-1000\{13CEFC
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1044
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2748
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3984
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4920
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5200
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5740
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6436
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6960
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\7756
HKLM\SYSTEM\ControlSet001\Control\Power\Profile\BootCheck
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
HKLM\SYSTEM\CurrentControlSet\Control\Power\Profile\BootCheck
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\VssapiPublisher
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000020408
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000030392
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000704DE
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000008031A
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\4
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\84
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\84\Shell
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\84\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C
HKU\S-1-5-21-39733034-3216902470-2998706464-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\4
HKU\S-1-5-21-39733034-3216902470-2998706464-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\84
HKU\S-1-5-21-39733034-3216902470-2998706464-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\84\Shell
HKU\S-1-5-21-39733034-3216902470-2998706464-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\84\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

----------------------------------
```

Keys Deleted:

```
----------------------------------
Keys deleted: 10
----------------------------------
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{7C0C823A-9A56-4BA3-9492-AE2F1BF8D7BC}
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{9484C0DB-1604-4BF9-B815-48A99E83C2CF}
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{C959F880-A3CB-451E-83DB-E49BD9DFF788}
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{DE3F04D3-91C6-4382-B698-9E453E7D4D76}
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft
HKU\S-1-5-21-39733034-3216902470-2998706464-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft
HKU\S-1-5-21-39733034-3216902470-2998706464-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.
HKU\S-1-5-21-39733034-3216902470-2998706464-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.

----------------------------------
```

Keys modified:

```
----------------------------------
Values modified: 80
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\ConnectivityRestrictedNetworkTime: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\ConnectivityRestrictedNetworkTime: 0x00000709
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\HeartBeats\Default\LastHeartBeatTime:  DB AC 1A 2D FB 4D D8 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\HeartBeats\Default\LastHeartBeatTime:  9B FB 02 5E FF 4D D8 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\HeartBeats\Default\HeartBeatSequenceNumber: 0x0000001A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\HeartBeats\Default\HeartBeatSequenceNumber: 0x0000001B
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests\LastDownloadTime:  87 B4 87 45 FD 4D D8 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests\LastDownloadTime:  47 A2 38 65 FF 4D D8 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime:  72 0F 09 4C FE 4D D8 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime:  A3 7B 23 6A FF 4D D8 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75:  44 06 00 00 00 00 00 00 04 00 04 00 01 00 05 00 01 01 00 0
39 01 2A 68 A9 00 2A B7 22 01 2A C7 DE 00 2B 24 99 00 2C 3D 81 00 2C D8 42 01 2D 0A EE 01 2D D8 F4 00 2E 80 1D 01 2F 34 FB 00 2F 95 46 01 30 31 14
2 6B 79 FB 01 6C 52 0D 01 6D 3E 43 01 6E F8 41 01 6F B3 11 01 6F BD A9 00 6F E5 D6 01 71 05 28 01 71 40 A3 00 72 3C 12 00 72 6E 4A 00 72 9B 37 01 7
 05 06 00 A3 E7 15 01 A4 58 02 00 A4 BA 37 01 A4 C0 08 02 A5 6C FE 01 A5 AD CF 00 A6 44 A6 00 A6 82 44 01 A7 36 A8 00 A7 B8 AD 00 A8 A2 35 01 A9 54
1E 02 DF 1F 80 01 E0 3E E7 01 E1 7E 8C 00 E2 18 ED 01 E2 1B 56 00 E4 40 27 01 E4 69 C9 00 E5 76 F8 01 E6 3E 2B 0D E6 7D D7 01 E7 A4 D9 00 E8 9E FA
1 A3 00 2E 53 4C 01 2E 68 A9 00 32 55 1E 01 32 56 AE 00 32 D4 5F 01 34 BB EF 00 36 D8 41 01 37 22 C7 00 37 F8 1D 01 3D 5E 35 01 3F 1C EA 00 42 7F 7
 00 A3 C4 E2 00 A3 F7 6A 00 A5 04 03 01 A5 22 A4 00 A5 8F 60 00 A6 38 DA 00 A7 C2 33 01 A9 B2 DB 00 AB 78 3D 01 AC 84 0E 01 AF EF C9 00 B0 75 5E 06
A9 00 2A B7 22 01 C9 38 4F 01 CD AD 05 01 03 00 42 01 00 00 27 69 12 01 38 0E 67 01 72 ED 81 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75:  54 06 00 00 00 00 00 00 04 00 04 00 01 00 05 00 01 01 00 0
3B 01 29 45 01 01 29 CC 10 01 2A 0E 39 01 2A 68 A9 00 2A B7 22 01 2A B8 5E 01 2A C7 DE 00 2B 24 99 00 2C 3D 81 00 2C D8 42 01 2D 0A EE 01 2D D8 F4
0 63 E5 07 02 64 1C A3 01 64 D4 19 01 65 30 54 01 65 A6 9E 00 67 1E F9 01 68 13 EC 01 69 CC 4F 01 6A 13 17 02 6B 79 FB 01 6C 52 0D 01 6D 3E 43 01 6
 72 46 01 9B 2B DB 00 9B 4D 87 00 9C 23 05 02 9C 47 41 01 9C 62 3A 01 9C A4 EB 00 9C E0 A8 00 9D 9D 92 00 9D BD FB 01 9E BC E9 01 9F 91 92 01 A0 86
DA 00 CC 49 56 00 CC EF EF 00 CD AD 05 01 CD BD 8C 00 CF 86 E7 01 CF D9 35 00 D0 17 56 00 D1 9A 7B 00 D1 D2 A7 00 D2 A9 2B 01 D3 82 61 00 D6 F6 DE
5 80 00 12 8D 0E 02 13 19 83 00 13 2F D3 00 14 AA FD 00 15 40 28 01 15 9A DB 00 18 1F 1B 01 19 C3 98 00 1A 66 11 01 1A FA 99 00 21 DF 5E 01 22 D3 8
 00 82 E6 F4 00 84 68 0B 01 8C 3B D3 00 8D 05 47 01 8F 06 43 01 8F 3C F3 00 91 67 C8 00 91 96 22 01 92 82 71 00 92 83 51 01 92 C4 14 01 93 05 47 01
E9 D1 F5 00 F0 0E 4E 01 F0 3A DD 00 F1 9F 43 01 F3 89 40 01 F3 9E D3 00 F4 06 28 01 F4 79 3D 01 F4 AD 7A 00 F4 C8 2F 01 F6 D9 EC 00 F7 D4 5F 01 F8
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475:  A2 03 00 00 00 00 00 00 04 00 04 00 01 02 04 00 00 00 00 0
```

d. Files created/modified

Files added:

```
----------------------------------
Files added: 18
----------------------------------
C:\Windows\Logs\waasmedic\waasmedic.20220411_154418_082.etl
C:\Windows\Logs\waasmedic\waasmedic.20220411_164418_104.etl
C:\Windows\Logs\waasmedic\waasmedic.20220411_171858_968.etl
C:\Windows\Logs\waasmedic\waasmedic.20220411_173941_363.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20220411.111349.340.3.etl
C:\Windows\Performance\WinSAT\DataStore\2022-04-11 11.59.32.834.winsat.etl
C:\Windows\Performance\WinSAT\DataStore\2022-04-11 11.59.33.569 Cpu.Assessment (Recent).WinSAT.xml
C:\Windows\Performance\WinSAT\DataStore\2022-04-11 11.59.33.569 Graphics3D.Assessment (Recent).WinSAT.xml
C:\Windows\Performance\WinSAT\DataStore\2022-04-11 12.00.40.562 Formal.Assessment (Recent).WinSAT.xml
C:\Windows\Prefetch\AgG1UAD_P_S-1-5-21-39733034-3216902470-2998706464-1000.db
C:\Windows\Prefetch\AgG1UAD_S-1-5-21-39733034-3216902470-2998706464-1000.db
C:\Windows\Prefetch\RUNDLL32.EXE-F4F26DED.pf
C:\Windows\Prefetch\SVCHOST.EXE-473F5CDC.pf
C:\Windows\System32\SleepStudy\ScreenOn\ScreenOnPowerStudyTraceSession-2022-04-11-11-55-18.etl
C:\Windows\System32\SleepStudy\user-not-present-trace-2022-04-11-13-39-41.etl
C:\Windows\System32\sru\SRU000BC.log
C:\Windows\System32\sru\SRU000BD.log
C:\Windows\System32\sru\SRU000BE.log
```

Folders added:

```
------------------------------------
Folders added: 1
------------------------------------
C:\Windows\Logs\SystemRestore
```

Files deleted:

```
-----------------------------------
Files deleted: 12
-----------------------------------
C:\Windows\System32\SleepStudy\ScreenOn\ScreenOnPowerStudyTraceSession-2022-02-17-14-29-24.etl
C:\Windows\System32\SleepStudy\ScreenOn\ScreenOnPowerStudyTraceSession-2022-02-17-14-36-14.etl
C:\Windows\System32\SleepStudy\ScreenOn\ScreenOnPowerStudyTraceSession-2022-02-17-14-39-17.etl
C:\Windows\System32\SleepStudy\ScreenOn\ScreenOnPowerStudyTraceSession-2022-02-19-11-17-59.etl
C:\Windows\System32\sru\SRU0006C.log
C:\Windows\System32\sru\SRU0006D.log
C:\Windows\System32\sru\SRU0006E.log
C:\Windows\System32\sru\SRU0006F.log
C:\Windows\System32\sru\SRU00070.log
C:\Windows\System32\sru\SRU00071.log
C:\Windows\System32\sru\SRU00072.log
C:\Windows\System32\sru\SRU00073.log
```

e. Processes started by the malware:

The malware starts the rundll32.exe and slui.exe process. The slui process checks if the Windows OS on the system is genuine or not. This is a very important process for Windows as if this process is deleted or tampered with in a way that it does not work, the system will stop working altogether.

Time ...	Process Name	PID	Operation	Path	Result	Detail
7:19:4...	rundll32.exe	2472	Process Start		SUCCESS	Parent PID: 3824, ...
7:19:5...	slui.exe	2836	Process Start		SUCCESS	Parent PID: 620, C...

f. Persistence mechanism employed by Malware

No persistence mechanism was found.

g. Deobfuscation:

The obfuscation method is the same as described in static analysis.

Indicators of Compromise

When the malware runs, it tries to contact sf.symcd.com which is a domain which contains other malicious files (potentially malwares) that can affect the local system. On the local system we can see that about 4 files are created in the C:\Windows\Temp directory (for Win 7 machines).

Yara rule:

```
rule identify_emotet
{

meta:
        description="YARA Rule to detect a emotet malware"
strings:
        $a="Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
```

```
        $b="Software\Microsoft\Windows\CurrentVersion\Policies\Network"
        $c="Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32"
        $d="GetTimeZoneInformation"
        $d="VirtualProtect"
        $e="GetModuleFileName"


condition:
        ($a or $b or $c or $d or $e)
}
```

Note: We are not checking for file extension as this family of malware essentially attacks by making the user download some content. That content could be pdf, image, doc or any other file.