SYNC 3.15.89

Date: September 21st, 2018.

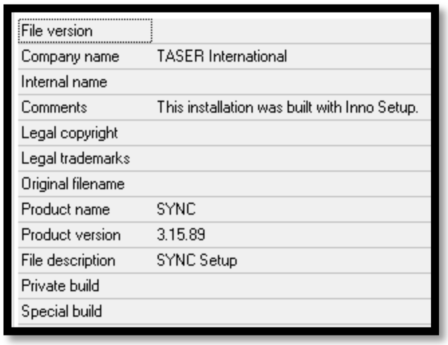
Description: This is an assessment of the software SYNC 3.15.89 (Evidence_SYNC_Setup.exe). Initially, was identified a few red flags regarding the timestamp and the size of the raw data. Further analysis revealed the presence of a TLS call back function and connections with suspicious files and websites.

The main components reviewed in the software included the sync.exe, taskkill.exe, imm32.dll, driver package installers and the msiexec.exe files.

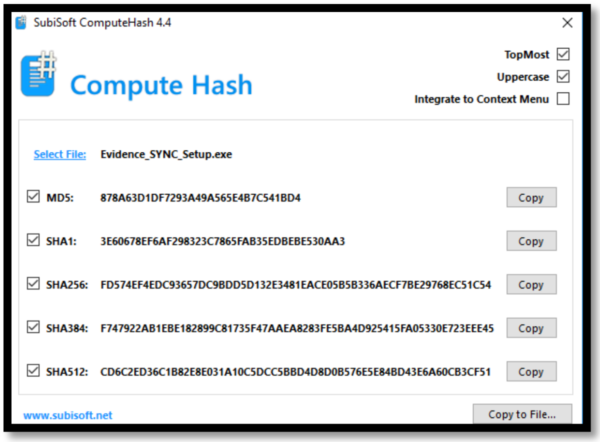
The software was considered malicious and vulnerable to documented attacks techniques such as process injection and query registry.

Table of Contents

File Identification



File version	
Company name	TASER International
Internal name	
Comments	This installation was built with Inno Setup.
Legal copyright	
Legal trademarks	
Original filename	
Product name	SYNC
Product version	3.15.89
File description	SYNC Setup
Private build	
Special build	



SubiSoft ComputeHash 4.4

Compute Hash

TopMost ☑

Uppercase ☑

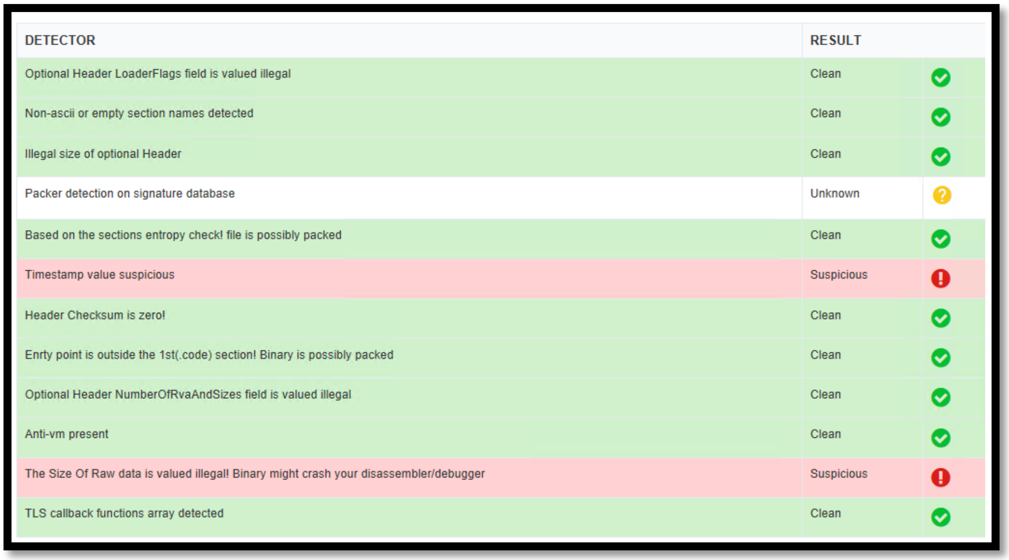
Integrate to Context Menu □

Select File: Evidence_SYNC_Setup.exe

☑ MD5:	878A63D1DF7293A49A565E4B7C541BD4	Copy
☑ SHA1:	3E60678EF6AF298323C7865FAB35EDBEBE530AA3	Copy
☑ SHA256:	FD574EF4EDC93657DC9BDD5D132E3481EACE05B5B336AECF7BE29768EC51C54	Copy
☑ SHA384:	F747922AB1EBE182899C81735F47AAEA8283FE5BA4D925415FA05330E723EEE45	Copy
☑ SHA512:	CD6C2ED36C1B82E8E031A10C5DCC5BBD4D8D0B576E5E84BD43E6A60CB3CF51	Copy

Initial Assessment

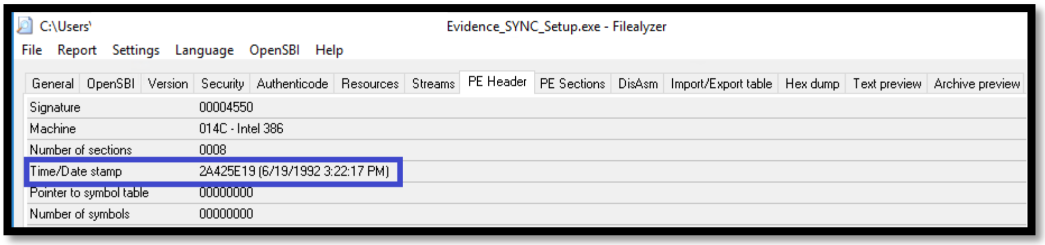
1. The size and timestamp were considered suspicious in the static analysis[1]:



DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✓
Timestamp value suspicious	Suspicious	!
Header Checksum is zero!	Clean	✓
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	✓
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	✓
Anti-vm present	Clean	✓
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Suspicious	!
TLS callback functions array detected	Clean	✓

[1] https://valkyrie.comodo.com/get_info?sha1=3E60678EF6AF298323C7865FAB35EDBEBE530AA3

This is the timestamp:

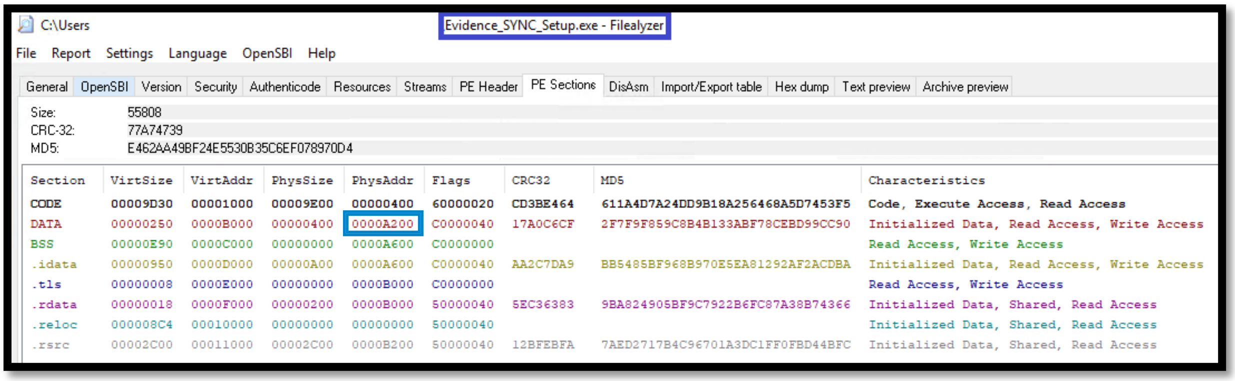


C:\Users\ Evidence_SYNC_Setup.exe - Filealyzer

File Report Settings Language OpenSBI Help
General OpenSBI Version Security Authenticode Resources Streams PE Header PE Sections DisAsm Import/Export table Hex dump Text preview Archive preview

Signature	00004550
Machine	014C - Intel 386
Number of sections	0008
Time/Date stamp	2A425E19 (6/19/1992 3:22:17 PM)
Pointer to symbol table	00000000
Number of symbols	00000000

The PE Sections, shows some relevant information such as the size of the raw data and confirm the possibility of processing errors.

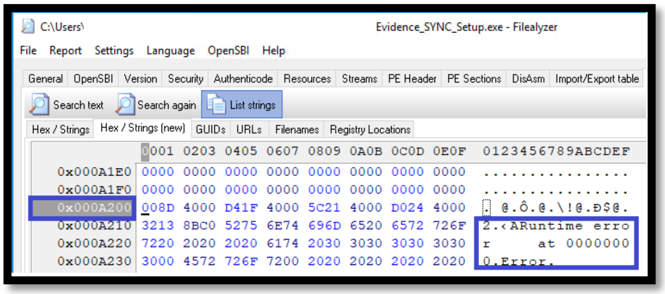


C:\Users Evidence_SYNC_Setup.exe - Filealyzer

File Report Settings Language OpenSBI Help
General OpenSBI Version Security Authenticode Resources Streams PE Header PE Sections DisAsm Import/Export table Hex dump Text preview Archive preview

Size: 55808
CRC-32: 77A74739
MD5: E462AA49BF24E5530B35C6EF078970D4

Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	CRC32	MD5	Characteristics
CODE	00009D30	00001000	00009E00	00000400	60000020	CD3BE464	611A4D7A24DD9B18A256468A5D7453F5	Code, Execute Access, Read Access
DATA	00000250	0000B000	00000400	0000A200	C0000040	17A0C6CF	2F7F9F859C8B4B133ABF78CEBD99CC90	Initialized Data, Read Access, Write Access
BSS	00000E90	0000C000	00000000	0000A600	C0000000			Read Access, Write Access
.idata	00000950	0000D000	00000A00	0000A600	C0000040	AA2C7DA9	BB5485BF968B970E5EA81292AF2ACDBA	Initialized Data, Read Access, Write Access
.tls	00000008	0000E000	00000000	0000B000	C0000000			Read Access, Write Access
.rdata	00000018	0000F000	00000200	0000B000	50000040	5EC36383	9BA824905BF9C7922B6FC87A38B74366	Initialized Data, Shared, Read Access
.reloc	000008C4	00010000	00000000	00000000	50000040			Initialized Data, Shared, Read Access
.rsrc	00002C00	00011000	00002C00	0000B200	50000040	12BFEBFA	7AED2717B4C96701A3DC1FF0FBD44BFC	Initialized Data, Shared, Read Access

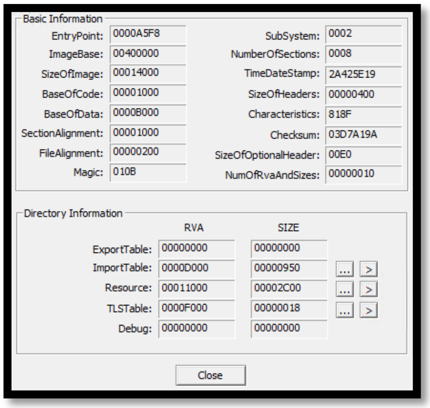


C:\Users\ Evidence_SYNC_Setup.exe - Filealyzer

File Report Settings Language OpenSBI Help
General OpenSBI Version Security Authenticode Resources Streams PE Header PE Sections DisAsm Import/Export table
Search text
Search again
List strings
Hex / Strings Hex / Strings (new) GUIDs URLs Filenames Registry Locations

```
            0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x000A1E0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x000A1F0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x000A200  008D 4000 D41F 4000 5C21 4000 D024 4000  . @.Ô.@.\!@.Ð$@.
0x000A210  3213 8BC0 5275 6E74 696D 6520 6572 726F  2.‹ARuntime erro
0x000A220  7220 2020 2020 6174 2030 3030 3030 3030  r      at 0000000
0x000A230  3000 4572 726F 7200 2020 2020 2020 2020  0.Error.
```

2. The PE section on the previous item, also shows the BSS section with a zero value and the identification of the TLS section referencing to a callback table.

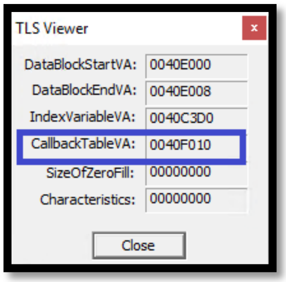


Basic Information

EntryPoint:	0000A5F8	SubSystem:	0002
ImageBase:	00400000	NumberOfSections:	0008
SizeOfImage:	00014000	TimeDateStamp:	2A425E19
BaseOfCode:	00001000	SizeOfHeaders:	00000400
BaseOfData:	0000B000	Characteristics:	818F
SectionAlignment:	00001000	Checksum:	03D7A19A
FileAlignment:	00000200	SizeOfOptionalHeader:	00E0
Magic:	010B	NumOfRvaAndSizes:	00000010

Directory Information

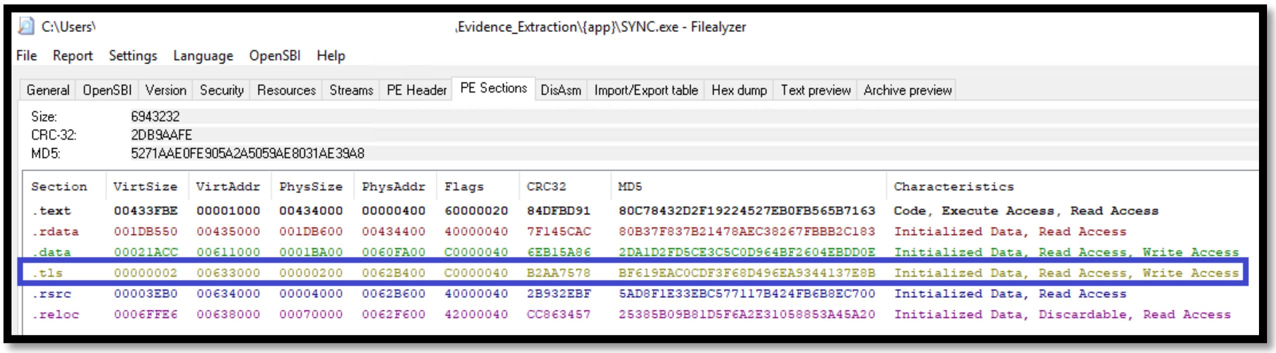
	RVA	SIZE
ExportTable:	00000000	00000000
ImportTable:	0000D000	00000950
Resource:	00011000	00002C00
TLSTable:	0000F000	00000018
Debug:	00000000	00000000



TLS Viewer

DataBlockStartVA:	0040E000
DataBlockEndVA:	0040E008
IndexVariableVA:	0040C3D0
CallbackTableVA:	0040F010
SizeOfZeroFill:	00000000
Characteristics:	00000000

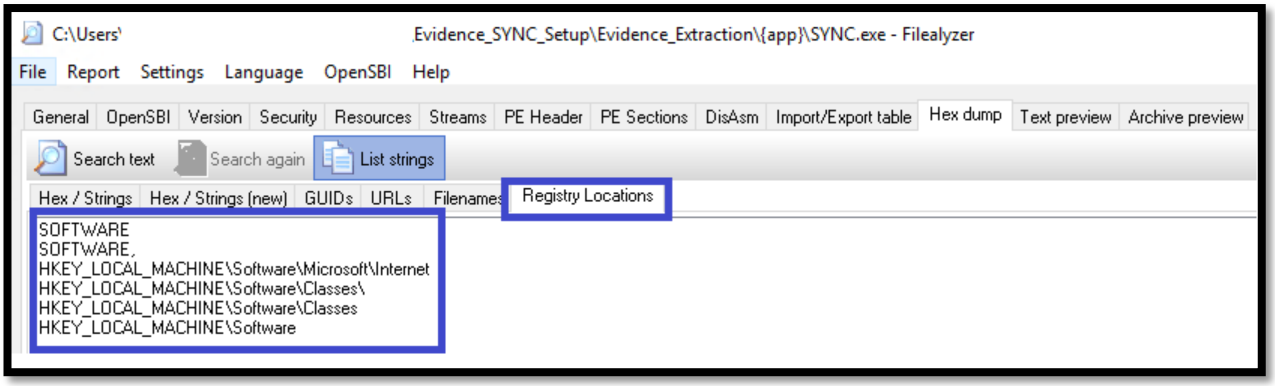
TLS section[2] is further identified when the file is decompressed. This could be later referred to the SYNC.exe[3] file in the aspects of a TLS call back[4] function and importation of suspicious application programming interface (API).


C:\Users\ .Evidence_Extraction\{app}\SYNC.exe - Filealyzer
File Report Settings Language OpenSBI Help
General OpenSBI Version Security Resources Streams PE Header PE Sections DisAsm Import/Export table Hex dump Text preview Archive preview

Size: 6943232
CRC-32: 2DB9AAFE
MD5: 5271AAE0FE905A2A5059AE8031AE39A8

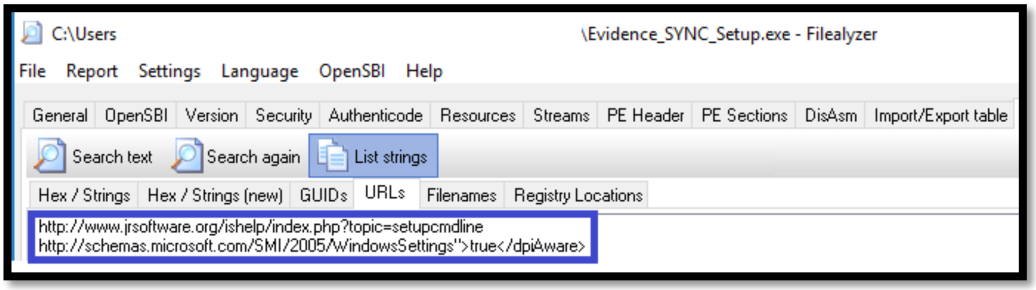
Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	CRC32	MD5	Characteristics
.text	00433FBE	00001000	00434000	00000400	60000020	84DFBD91	80C78432D2F19224527EB0FB565B7163	Code, Execute Access, Read Access
.rdata	001DB550	00435000	001DB600	00434400	40000040	7F145CAC	80B37F837B21478AEC38267FBBB2C183	Initialized Data, Read Access
.data	00021ACC	00611000	0001BA00	0060FA00	C0000040	6EB15A86	2DA1D2FD5CE3C5C0D964BF2604EBDD0E	Initialized Data, Read Access, Write Access
.tls	00000002	00633000	00000200	0062B400	C0000040	B2AA7578	BF619EAC0CDF3F68D496EA9344137E8B	Initialized Data, Read Access, Write Access
.rsrc	00003EB0	00634000	00004000	0062B600	40000040	2B932EBF	5AD8F1E33EBC577117B424FB6B8EC700	Initialized Data, Read Access
.reloc	0006FFE6	00638000	00070000	0062F600	42000040	CC863457	25385B09B81D5F6A2E31058853A45A20	Initialized Data, Discardable, Read Access

The SYNC.exe make changes in the registry locations when decompressed.


C:\Users\ Evidence_SYNC_Setup\Evidence_Extraction\{app}\SYNC.exe - Filealyzer
File Report Settings Language OpenSBI Help
General OpenSBI Version Security Resources Streams PE Header PE Sections DisAsm Import/Export table Hex dump Text preview Archive preview
Search text Search again List strings
Hex / Strings Hex / Strings (new) GUIDs URLs Filenames Registry Locations

```
SOFTWARE
SOFTWARE,
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
HKEY_LOCAL_MACHINE\Software\Classes\
HKEY_LOCAL_MACHINE\Software\Classes
HKEY_LOCAL_MACHINE\Software
```

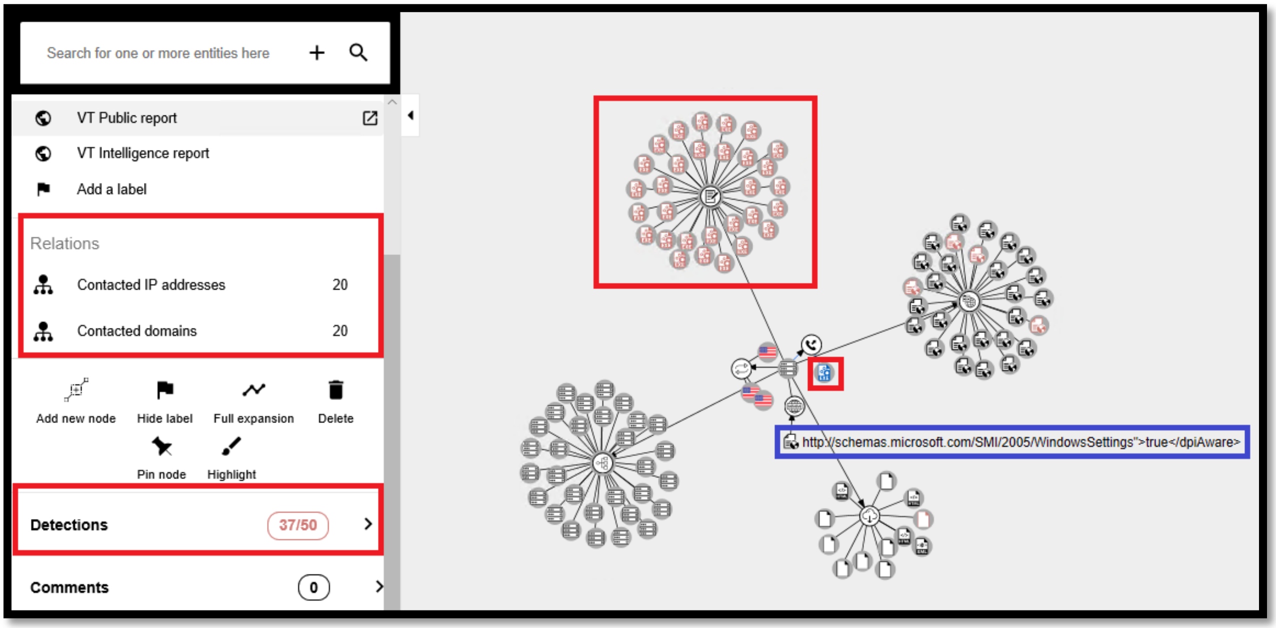
3. Some network security risks were identified, mainly related to two websites:


C:\Users \Evidence_SYNC_Setup.exe - Filealyzer
File Report Settings Language OpenSBI Help
General OpenSBI Version Security Authenticode Resources Streams PE Header PE Sections DisAsm Import/Export table
Search text Search again List strings
Hex / Strings Hex / Strings (new) GUIDs URLs Filenames Registry Locations

```
http://www.jrsoftware.org/ishelp/index.php?topic=setupcmdline
http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
```

[2] https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html
[3] https://www.hybrid-analysis.com/sample/c7d3e5cd27afa2d7f613ddeb4f3898ae295eca20b343591d710a8fd4903d0432/5ba103287ca3e147ff34f9c6
[4] https://isc.sans.edu/diary/How+Malware+Defends+Itself+Using+TLS+Callback+Functions/6655

Which could download or reference to other websites and suspicious files.

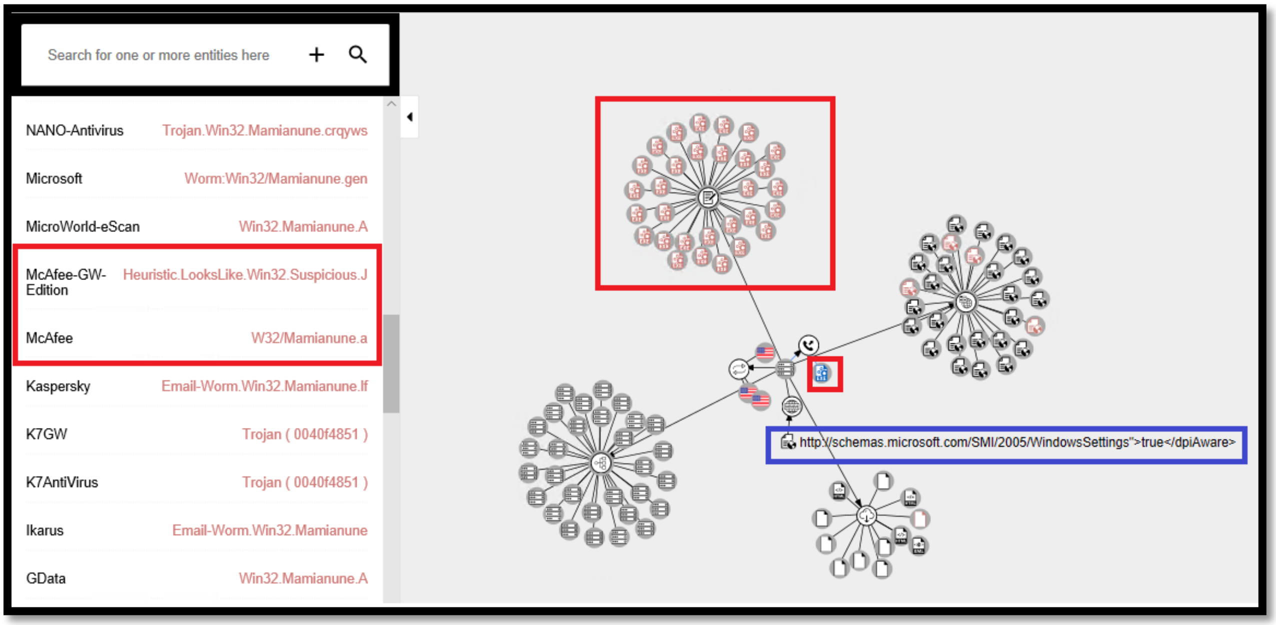


Relations

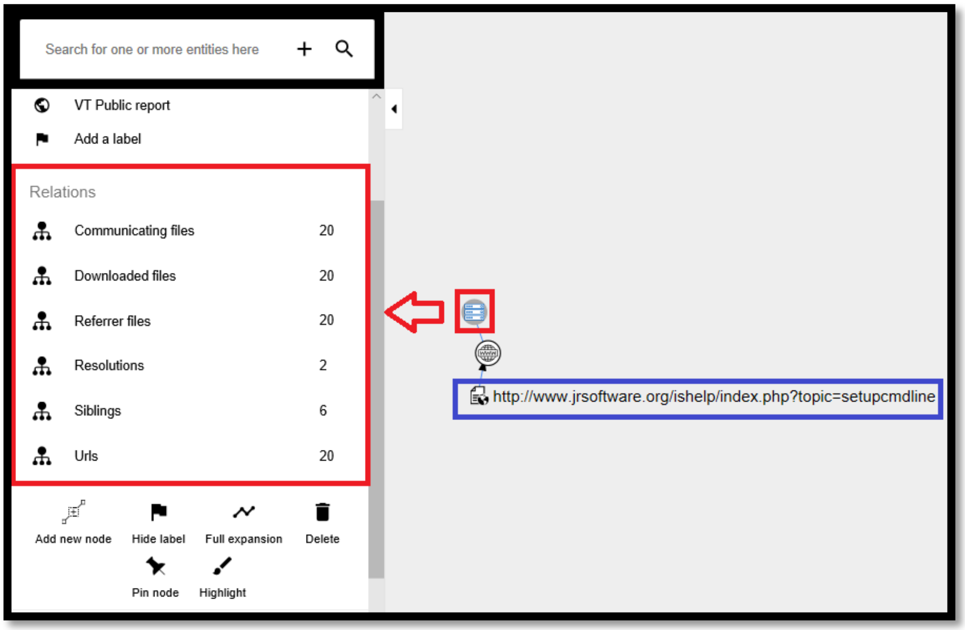
Contacted IP addresses	20
Contacted domains	20

Detections 37/50

Comments 0


Search for one or more entities here
http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>

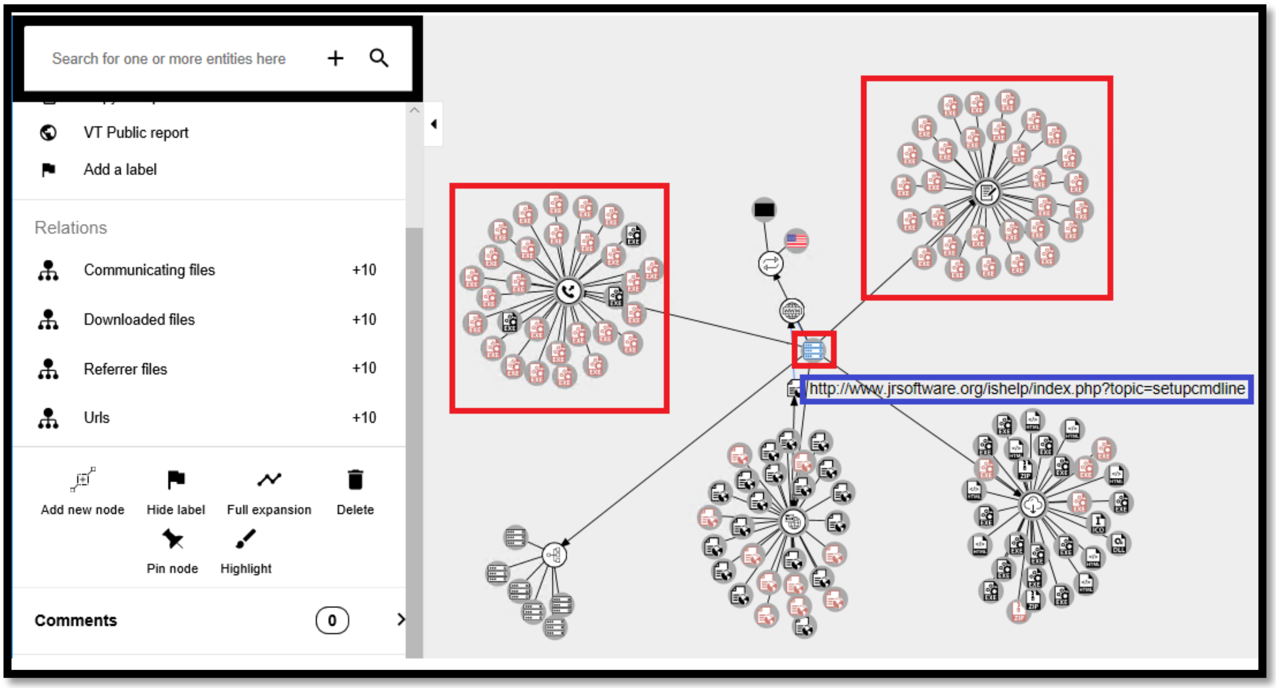
NANO-Antivirus	Trojan.Win32.Mamianune.crqyws
Microsoft	Worm:Win32/Mamianune.gen
MicroWorld-eScan	Win32.Mamianune.A
McAfee-GW-Edition	Heuristic.LooksLike.Win32.Suspicious.J
McAfee	W32/Mamianune.a
Kaspersky	Email-Worm.Win32.Mamianune.lf
K7GW	Trojan (0040f4851)
K7AntiVirus	Trojan (0040f4851)
Ikarus	Email-Worm.Win32.Mamianune
GData	Win32.Mamianune.A



Relations

Communicating files	20
Downloaded files	20
Referrer files	20
Resolutions	2
Siblings	6
Urls	20

http://www.jrsoftware.org/ishelp/index.php?topic=setupcmdline



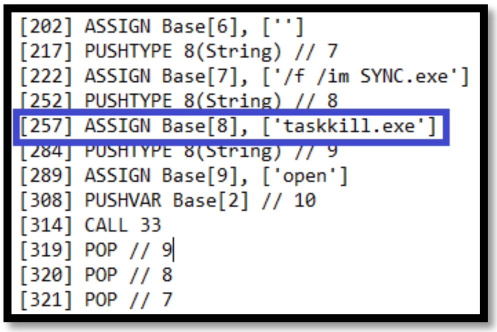
Relations

Communicating files	+10
Downloaded files	+10
Referrer files	+10
Urls	+10

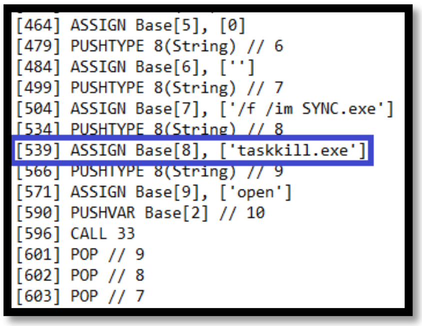
http://www.jrsoftware.org/ishelp/index.php?topic=setupcmdline

Analysis

1. The software has some anti-detection files like taskkill.exe[5]

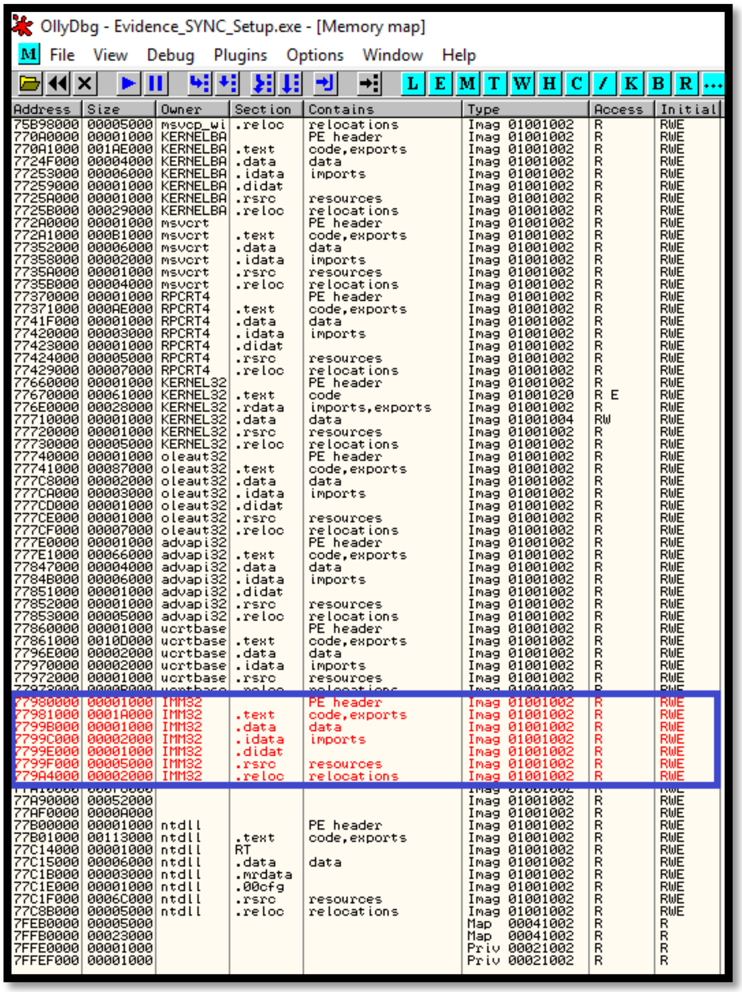


```
[202] ASSIGN Base[6], ['']
[217] PUSHTYPE 8(String) // 7
[222] ASSIGN Base[7], ['/f /im SYNC.exe']
[252] PUSHTYPE 8(String) // 8
[257] ASSIGN Base[8], ['taskkill.exe']
[284] PUSHTYPE 8(String) // 9
[289] ASSIGN Base[9], ['open']
[308] PUSHVAR Base[2] // 10
[314] CALL 33
[319] POP // 9
[320] POP // 8
[321] POP // 7
```



```
[464] ASSIGN Base[5], [0]
[479] PUSHTYPE 8(String) // 6
[484] ASSIGN Base[6], ['']
[499] PUSHTYPE 8(String) // 7
[504] ASSIGN Base[7], ['/f /im SYNC.exe']
[534] PUSHTYPE 8(String) // 8
[539] ASSIGN Base[8], ['taskkill.exe']
[566] PUSHTYPE 8(String) // 9
[571] ASSIGN Base[9], ['open']
[590] PUSHVAR Base[2] // 10
[596] CALL 33
[601] POP // 9
[602] POP // 8
[603] POP // 7
```

2. The file IMM32.dll[6] shows a process error and this could adversely impact the computer system:



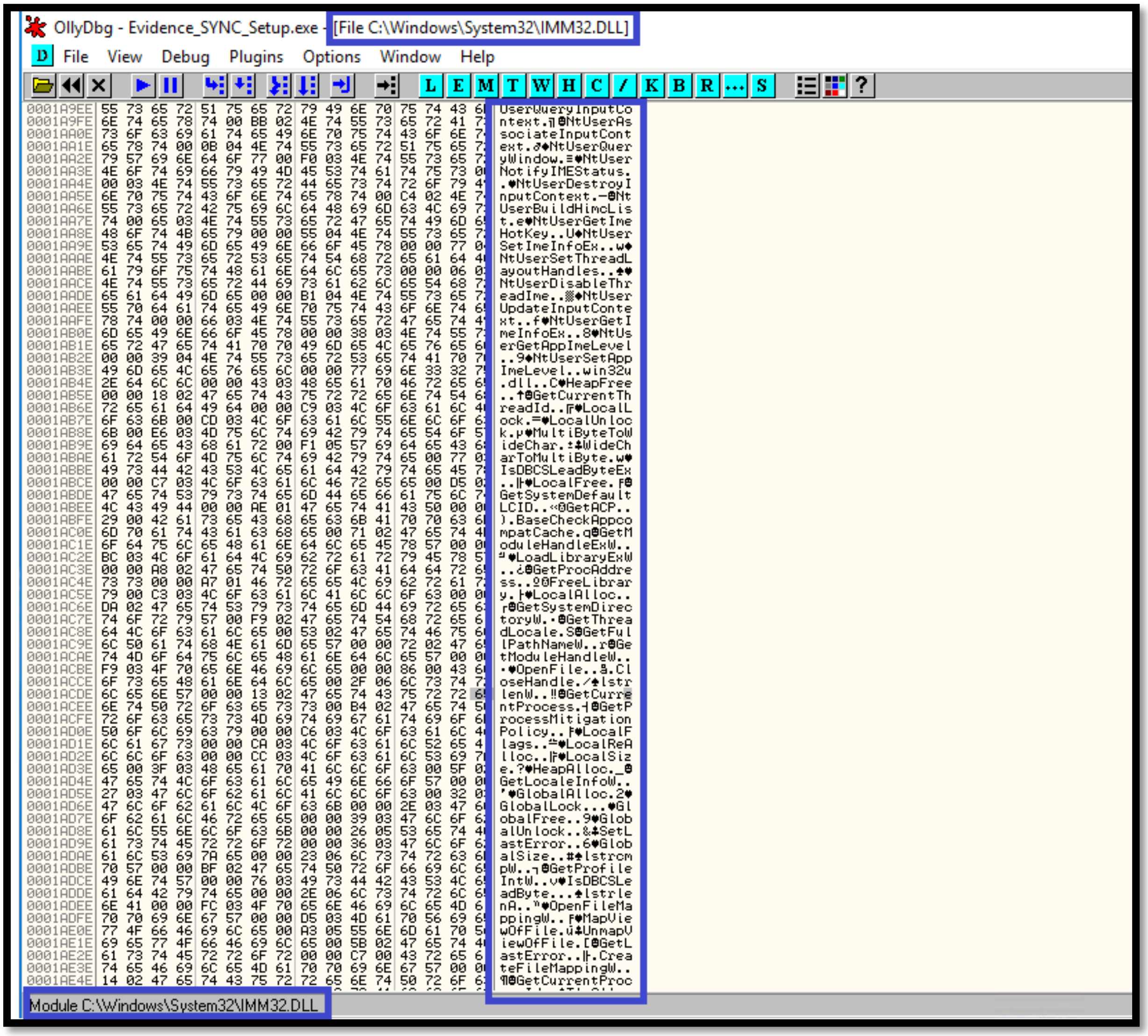
OllyDbg - Evidence_SYNC_Setup.exe - [Memory map]

M File View Debug Plugins Options Window Help
L E M T W H C / K B R ...

```
Address  Size     Owner     Section  Contains          Type          Access  Initial
75B98000 00005000 msvcp_wi  .reloc   relocations       Imag 01001002 R       RWE
770A0000 00001000 KERNELBA           PE header         Imag 01001002 R       RWE
770A1000 001AE000 KERNELBA  .text    code,exports      Imag 01001002 R       RWE
7724F000 00004000 KERNELBA  .data    data              Imag 01001002 R       RWE
77253000 00006000 KERNELBA  .idata   imports           Imag 01001002 R       RWE
77259000 00001000 KERNELBA  .didat                     Imag 01001002 R       RWE
7725A000 00001000 KERNELBA  .rsrc    resources         Imag 01001002 R       RWE
7725B000 00029000 KERNELBA  .reloc   relocations       Imag 01001002 R       RWE
772A0000 00001000 msvcrt             PE header         Imag 01001002 R       RWE
772A1000 000B1000 msvcrt    .text    code,exports      Imag 01001002 R       RWE
77352000 00006000 msvcrt    .data    data              Imag 01001002 R       RWE
77358000 00002000 msvcrt    .idata   imports           Imag 01001002 R       RWE
7735A000 00001000 msvcrt    .rsrc    resources         Imag 01001002 R       RWE
7735B000 00004000 msvcrt    .reloc   relocations       Imag 01001002 R       RWE
77370000 00001000 RPCRT4             PE header         Imag 01001002 R       RWE
77371000 000AE000 RPCRT4    .text    code,exports      Imag 01001002 R       RWE
7741F000 00001000 RPCRT4    .data    data              Imag 01001002 R       RWE
77420000 00003000 RPCRT4    .idata   imports           Imag 01001002 R       RWE
77423000 00001000 RPCRT4    .didat                     Imag 01001002 R       RWE
77424000 00005000 RPCRT4    .rsrc    resources         Imag 01001002 R       RWE
77429000 00007000 RPCRT4    .reloc   relocations       Imag 01001002 R       RWE
77660000 00001000 KERNEL32           PE header         Imag 01001002 R       RWE
77670000 00061000 KERNEL32  .text    code              Imag 01001020 R E     RWE
776E0000 00028000 KERNEL32  .rdata   imports,exports   Imag 01001002 R       RWE
77710000 00001000 KERNEL32  .data    data              Imag 01001004 RW      RWE
77720000 00001000 KERNEL32  .rsrc    resources         Imag 01001002 R       RWE
77730000 00005000 KERNEL32  .reloc   relocations       Imag 01001002 R       RWE
77740000 00001000 oleaut32           PE header         Imag 01001002 R       RWE
77741000 00087000 oleaut32  .text    code,exports      Imag 01001002 R       RWE
777C8000 00002000 oleaut32  .data    data              Imag 01001002 R       RWE
777CA000 00003000 oleaut32  .idata   imports           Imag 01001002 R       RWE
777CD000 00001000 oleaut32  .didat                     Imag 01001002 R       RWE
777CE000 00001000 oleaut32  .rsrc    resources         Imag 01001002 R       RWE
777CF000 00007000 oleaut32  .reloc   relocations       Imag 01001002 R       RWE
777E0000 00001000 advapi32           PE header         Imag 01001002 R       RWE
777E1000 00066000 advapi32  .text    code,exports      Imag 01001002 R       RWE
77847000 00004000 advapi32  .data    data              Imag 01001002 R       RWE
7784B000 00006000 advapi32  .idata   imports           Imag 01001002 R       RWE
77851000 00001000 advapi32  .didat                     Imag 01001002 R       RWE
77852000 00001000 advapi32  .rsrc    resources         Imag 01001002 R       RWE
77853000 00005000 advapi32  .reloc   relocations       Imag 01001002 R       RWE
77860000 00001000 ucrtbase           PE header         Imag 01001002 R       RWE
77861000 0010D000 ucrtbase  .text    code,exports      Imag 01001002 R       RWE
7796E000 00002000 ucrtbase  .data    data              Imag 01001002 R       RWE
77970000 00002000 ucrtbase  .idata   imports           Imag 01001002 R       RWE
77972000 00001000 ucrtbase  .rsrc    resources         Imag 01001002 R       RWE
77973000 0000D000 ucrtbase  .reloc   relocations       Imag 01001002 R       RWE
77980000 00001000 IMM32              PE header         Imag 01001002 R       RWE
77981000 0001A000 IMM32     .text    code,exports      Imag 01001002 R       RWE
7799B000 00001000 IMM32     .data    data              Imag 01001002 R       RWE
7799C000 00002000 IMM32     .idata   imports           Imag 01001002 R       RWE
7799E000 00001000 IMM32     .didat                     Imag 01001002 R       RWE
7799F000 00005000 IMM32     .rsrc    resources         Imag 01001002 R       RWE
779A4000 00002000 IMM32     .reloc   relocations       Imag 01001002 R       RWE
77A10000 [illegible]                                   Imag 01001002 R       RWE
77A90000 00052000                                      Imag 01001002 R       RWE
77AF0000 0000A000                                      Imag 01001002 R       RWE
77B00000 00001000 ntdll              PE header         Imag 01001002 R       RWE
77B01000 00113000 ntdll     .text    code,exports      Imag 01001002 R       RWE
77C14000 00001000 ntdll     RT                         Imag 01001002 R       RWE
77C15000 00006000 ntdll     .data    data              Imag 01001002 R       RWE
77C1B000 00003000 ntdll     .mrdata                    Imag 01001002 R       RWE
77C1E000 00001000 ntdll     .00cfg                     Imag 01001002 R       RWE
77C1F000 0006C000 ntdll     .rsrc    resources         Imag 01001002 R       RWE
77C8B000 00005000 ntdll     .reloc   relocations       Imag 01001002 R       RWE
7FEB0000 00005000                                      Map  00041002 R       R
7FFB0000 00023000                                      Map  00041002 R       R
7FFE0000 00001000                                      Priv 00021002 R       R
7FFEF000 00001000                                      Priv 00021002 R       R
```

[5] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb491009(v=technet.10)

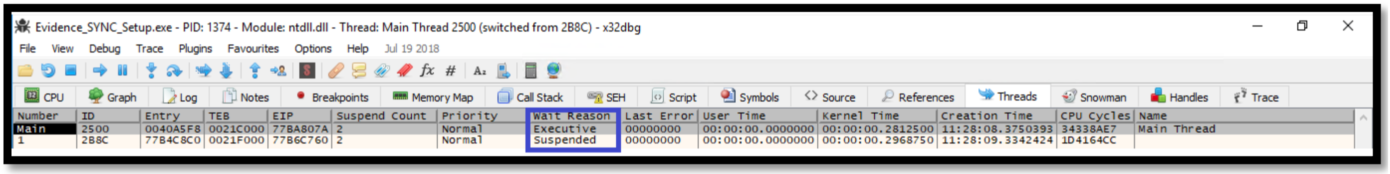
[6] https://www.processlibrary.com/en/directory/files/imm32/22508/


OllyDbg - Evidence_SYNC_Setup.exe - [File C:\Windows\System32\IMM32.DLL]
D File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

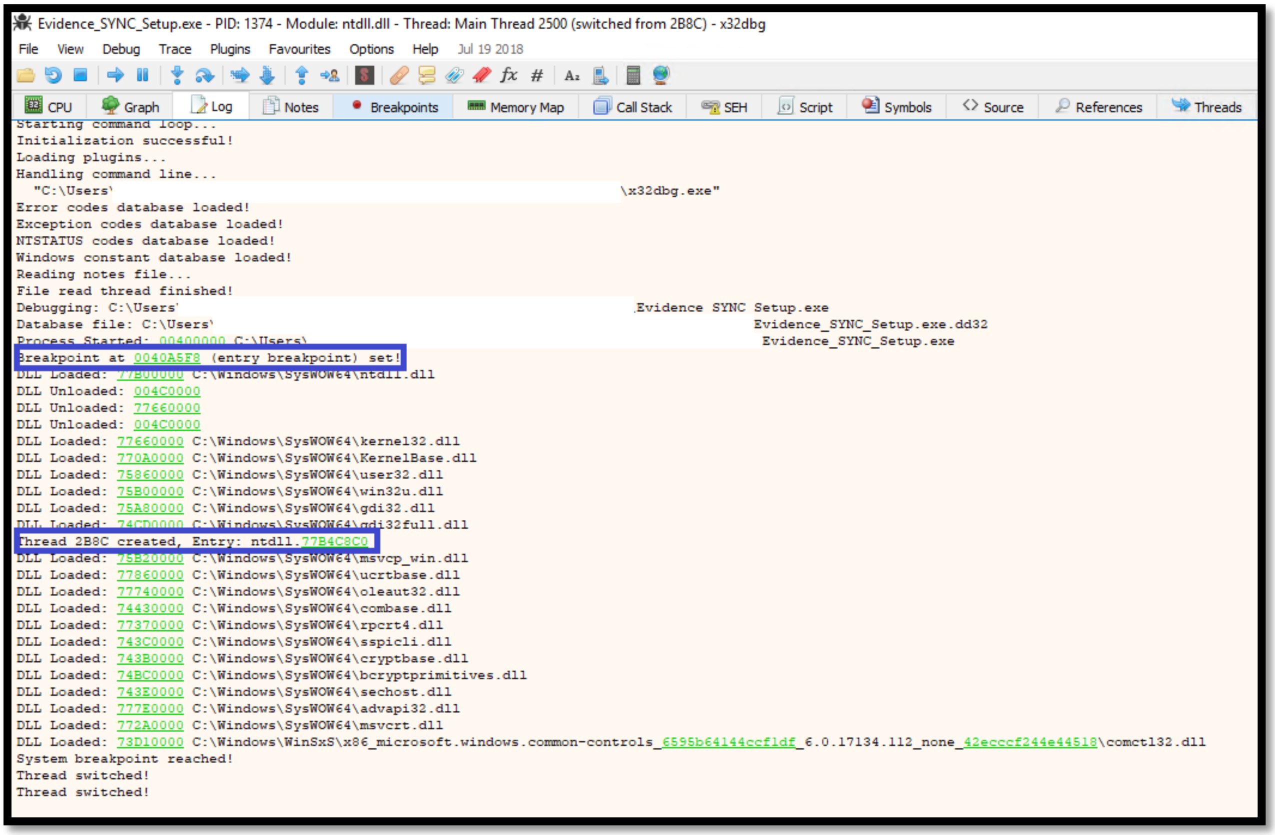
```
0001A9EE 55 73 65 72 51 75 65 72 79 49 6E 70 75 74 43   UserQueryInputCo
0001A9FE 6E 74 65 78 74 00 BB 02 4E 74 55 73 65 72 41   ntext.╗☻NtUserAs
0001AA0E 73 6F 63 69 61 74 65 49 6E 70 75 74 43 6F 6E   sociateInputCont
0001AA1E 65 78 74 00 0B 04 4E 74 55 73 65 72 51 75 65   ext.♂♦NtUserQuer
0001AA2E 79 57 69 6E 64 6F 77 00 F0 03 4E 74 55 73 65   yWindow.≡♥NtUser
0001AA3E 4E 6F 74 69 66 79 49 4D 45 53 74 61 74 75 73   NotifyIMEStatus.
0001AA4E 00 03 4E 74 55 73 65 72 44 65 73 74 72 6F 79   .♥NtUserDestroyI
0001AA5E 6E 70 75 74 43 6F 6E 74 65 78 74 00 C4 02 4E   nputContext.─☻Nt
0001AA6E 55 73 65 72 42 75 69 6C 64 48 69 6D 63 4C 69   UserBuildHimcLis
0001AA7E 74 00 65 03 4E 74 55 73 65 72 47 65 74 49 6D   t.e♥NtUserGetIme
0001AA8E 48 6F 74 4B 65 79 00 00 55 04 4E 74 55 73 65   HotKey..U♦NtUser
0001AA9E 53 65 74 49 6D 65 49 6E 66 6F 45 78 00 00 77   SetImeInfoEx..w♦
0001AAAE 4E 74 55 73 65 72 53 65 74 54 68 72 65 61 64   NtUserSetThreadL
0001AABE 61 79 6F 75 74 48 61 6E 64 6C 65 73 00 00 06   ayoutHandles..♠♥
0001AACE 4E 74 55 73 65 72 44 69 73 61 62 6C 65 54 68   NtUserDisableThr
0001AADE 65 61 64 49 6D 65 00 00 B1 04 4E 74 55 73 65   eadIme..▒♦NtUser
0001AAEE 55 70 64 61 74 65 49 6E 70 75 74 43 6F 6E 74   UpdateInputConte
0001AAFE 78 74 00 00 66 03 4E 74 55 73 65 72 47 65 74   xt..f♥NtUserGetI
0001AB0E 6D 65 49 6E 66 6F 45 78 00 00 38 03 4E 74 55   meInfoEx..8♥NtUs
0001AB1E 65 72 47 65 74 41 70 70 49 6D 65 4C 65 76 65   erGetAppImeLevel
0001AB2E 00 00 39 04 4E 74 55 73 65 72 53 65 74 41 70   ..9♦NtUserSetApp
0001AB3E 49 6D 65 4C 65 76 65 6C 00 00 77 69 6E 33 32   ImeLevel..win32u
0001AB4E 2E 64 6C 6C 00 00 43 03 48 65 61 70 46 72 65   .dll..C♥HeapFree
0001AB5E 00 00 18 02 47 65 74 43 75 72 72 65 6E 74 54   ..↑☻GetCurrentTh
0001AB6E 72 65 61 64 49 64 00 00 C9 03 4C 6F 63 61 6C   readId..╔♥LocalL
0001AB7E 6F 63 6B 00 CD 03 4C 6F 63 61 6C 55 6E 6C 6F   ock.═♥LocalUnloc
0001AB8E 6B 00 E6 03 4D 75 6C 74 69 42 79 74 65 54 6F   k.µ♥MultiByteToW
0001AB9E 69 64 65 43 68 61 72 00 F1 05 57 69 64 65 43   ideChar.±♣WideCh
0001ABAE 61 72 54 6F 4D 75 6C 74 69 42 79 74 65 00 77   arToMultiByte.w♥
0001ABBE 49 73 44 42 43 53 4C 65 61 64 42 79 74 65 45   IsDBCSLeadByteEx
0001ABCE 00 00 C7 03 4C 6F 63 61 6C 46 72 65 65 00 D5   ..╟♥LocalFree.╒☻
0001ABDE 47 65 74 53 79 73 74 65 6D 44 65 66 61 75 6C   GetSystemDefault
0001ABEE 4C 43 49 44 00 00 AE 01 47 65 74 41 43 50 00   LCID..«☺GetACP..
0001ABFE 29 00 42 61 73 65 43 68 65 63 6B 41 70 70 63   ).BaseCheckAppco
0001AC0E 6D 70 61 74 43 61 63 68 65 00 71 02 47 65 74   mpatCache.q☻GetM
0001AC1E 6F 64 75 6C 65 48 61 6E 64 6C 65 45 78 57 00   oduleHandleExW..
0001AC2E BC 03 4C 6F 61 64 4C 69 62 72 61 72 79 45 78   ╝♥LoadLibraryExW
0001AC3E 00 00 A8 02 47 65 74 50 72 6F 63 41 64 64 72   ..¿☻GetProcAddre
0001AC4E 73 73 00 00 A7 01 46 72 65 65 4C 69 62 72 61   ss..º☺FreeLibrar
0001AC5E 79 00 C3 03 4C 6F 63 61 6C 41 6C 6C 6F 63 00   y.├♥LocalAlloc..
0001AC6E DA 02 47 65 74 53 79 73 74 65 6D 44 69 72 65   ┌☻GetSystemDirec
0001AC7E 74 6F 72 79 57 00 F9 02 47 65 74 54 68 72 65   toryW.·☻GetThrea
0001AC8E 64 4C 6F 63 61 6C 65 00 53 02 47 65 74 46 75   dLocale.S☻GetFul
0001AC9E 6C 50 61 74 68 4E 61 6D 65 57 00 00 72 02 47   lPathNameW..r☻Ge
0001ACAE 74 4D 6F 64 75 6C 65 48 61 6E 64 6C 65 57 00   tModuleHandleW..
0001ACBE F9 03 4F 70 65 6E 46 69 6C 65 00 00 86 00 43   ·♥OpenFile..å.Cl
0001ACCE 6F 73 65 48 61 6E 64 6C 65 00 2F 06 6C 73 74   oseHandle./♠lstr
0001ACDE 6C 65 6E 57 00 00 13 02 47 65 74 43 75 72 72   lenW..‼☻GetCurre
0001ACEE 6E 74 50 72 6F 63 65 73 73 00 B4 02 47 65 74   ntProcess.┤☻GetP
0001ACFE 72 6F 63 65 73 73 4D 69 74 69 67 61 74 69 6F   rocessMitigation
0001AD0E 50 6F 6C 69 63 79 00 00 C6 03 4C 6F 63 61 6C   Policy..╞♥LocalF
0001AD1E 6C 61 67 73 00 00 CA 03 4C 6F 63 61 6C 52 65   lags..╩♥LocalReA
0001AD2E 6C 6C 6F 63 00 00 CC 03 4C 6F 63 61 6C 53 69   lloc..╠♥LocalSiz
0001AD3E 65 00 3F 03 48 65 61 70 41 6C 6C 6F 63 00 5F   e.?♥HeapAlloc._☻
0001AD4E 47 65 74 4C 6F 63 61 6C 65 49 6E 66 6F 57 00   GetLocaleInfoW..
0001AD5E 27 03 47 6C 6F 62 61 6C 41 6C 6C 6F 63 00 32   '♥GlobalAlloc.2♥
0001AD6E 47 6C 6F 62 61 6C 4C 6F 63 6B 00 00 2E 03 47   GlobalLock...♥Gl
0001AD7E 6F 62 61 6C 46 72 65 65 00 00 39 03 47 6C 6F   obalFree..9♥Glob
0001AD8E 61 6C 55 6E 6C 6F 63 6B 00 00 26 05 53 65 74   alUnlock..&♣SetL
0001AD9E 61 73 74 45 72 72 6F 72 00 00 36 03 47 6C 6F   astError..6♥Glob
0001ADAE 61 6C 53 69 7A 65 00 00 23 06 6C 73 74 72 63   alSize..#♠lstrcm
0001ADBE 70 57 00 00 BF 02 47 65 74 50 72 6F 66 69 6C   pW..┐☻GetProfile
0001ADCE 49 6E 74 57 00 00 76 03 49 73 44 42 43 53 4C   IntW..v♥IsDBCSLe
0001ADDE 61 64 42 79 74 65 00 00 2E 06 6C 73 74 72 6C   adByte...♠lstrle
0001ADEE 6E 41 00 00 FC 03 4F 70 65 6E 46 69 6C 65 4D   nA..ⁿ♥OpenFileMa
0001ADFE 70 70 69 6E 67 57 00 00 D5 03 4D 61 70 56 69   ppingW..╒♥MapVie
0001AE0E 77 4F 66 46 69 6C 65 00 A3 05 55 6E 6D 61 70   wOfFile.ú♣UnmapV
0001AE1E 69 65 77 4F 66 46 69 6C 65 00 5B 02 47 65 74   iewOfFile.[☻GetL
0001AE2E 61 73 74 45 72 72 6F 72 00 00 C7 00 43 72 65   astError..╟.Crea
0001AE3E 74 65 46 69 6C 65 4D 61 70 70 69 6E 67 57 00   teFileMappingW..
0001AE4E 14 02 47 65 74 43 75 72 72 65 6E 74 50 72 6F   ¶☻GetCurrentProc
```

Module C:\Windows\System32\IMM32.DLL

Then we see that the software shows the presence of two threads that allows to import additional *.dll files.

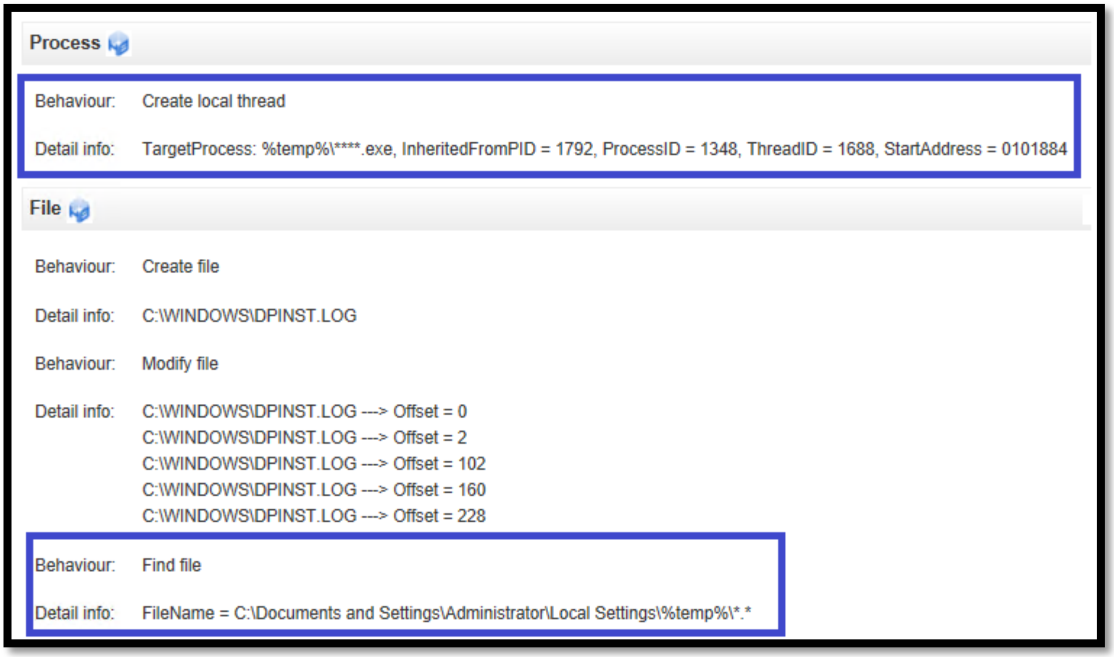

Evidence_SYNC_Setup.exe - PID: 1374 - Module: ntdll.dll - Thread: Main Thread 2500 (switched from 2B8C) - x32dbg
File View Debug Trace Plugins Favourites Options Help Jul 19 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

Number	ID	Entry	TEB	EIP	Suspend Count	Priority	Wait Reason	Last Error	User Time	Kernel Time	Creation Time	CPU Cycles	Name
Main	2500	0040A5F8	0021C000	77BA807A	2	Normal	Executive	00000000	00:00:00.0000000	00:00:00.2812500	11:28:08.3750393	34338AE7	Main Thread
1	2B8C	77B4C8C0	0021F000	77B6C760	2	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.2968750	11:28:09.3342424	1D4164CC	


Evidence_SYNC_Setup.exe - PID: 1374 - Module: ntdll.dll - Thread: Main Thread 2500 (switched from 2B8C) - x32dbg
File View Debug Trace Plugins Favourites Options Help Jul 19 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads

```
Starting command loop...
Initialization successful!
Loading plugins...
Handling command line...
  "C:\Users\[redacted]\x32dbg.exe"
Error codes database loaded!
Exception codes database loaded!
NTSTATUS codes database loaded!
Windows constant database loaded!
Reading notes file...
File read thread finished!
Debugging: C:\Users\[redacted].Evidence SYNC Setup.exe
Database file: C:\Users\[redacted]Evidence_SYNC_Setup.exe.dd32
Process Started: 00400000 C:\Users\[redacted]Evidence_SYNC_Setup.exe
Breakpoint at 0040A5F8 (entry breakpoint) set!
DLL Loaded: 77B00000 C:\Windows\SysWOW64\ntdll.dll
DLL Unloaded: 004C0000
DLL Unloaded: 77660000
DLL Unloaded: 004C0000
DLL Loaded: 77660000 C:\Windows\SysWOW64\kernel32.dll
DLL Loaded: 770A0000 C:\Windows\SysWOW64\KernelBase.dll
DLL Loaded: 75860000 C:\Windows\SysWOW64\user32.dll
DLL Loaded: 75B00000 C:\Windows\SysWOW64\win32u.dll
DLL Loaded: 75A80000 C:\Windows\SysWOW64\gdi32.dll
DLL Loaded: 74CD0000 C:\Windows\SysWOW64\gdi32full.dll
Thread 2B8C created, Entry: ntdll.77B4C8C0
DLL Loaded: 75B20000 C:\Windows\SysWOW64\msvcp_win.dll
DLL Loaded: 77860000 C:\Windows\SysWOW64\ucrtbase.dll
DLL Loaded: 77740000 C:\Windows\SysWOW64\oleaut32.dll
DLL Loaded: 74430000 C:\Windows\SysWOW64\combase.dll
DLL Loaded: 77370000 C:\Windows\SysWOW64\rpcrt4.dll
DLL Loaded: 743C0000 C:\Windows\SysWOW64\sspicli.dll
DLL Loaded: 743B0000 C:\Windows\SysWOW64\cryptbase.dll
DLL Loaded: 74BC0000 C:\Windows\SysWOW64\bcryptprimitives.dll
DLL Loaded: 743E0000 C:\Windows\SysWOW64\sechost.dll
DLL Loaded: 777E0000 C:\Windows\SysWOW64\advapi32.dll
DLL Loaded: 772A0000 C:\Windows\SysWOW64\msvcrt.dll
DLL Loaded: 73D10000 C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.112_none_42ecccf244e44518\comctl32.dll
System breakpoint reached!
Thread switched!
Thread switched!
```

This second thread could be related to the driver installation (dpinst,2) which also execute a search on administrator settings:



Process

Behaviour: Create local thread

Detail info: TargetProcess: %temp%****.exe, InheritedFromPID = 1792, ProcessID = 1348, ThreadID = 1688, StartAddress = 0101884

File

Behaviour: Create file

Detail info: C:\WINDOWS\DPINST.LOG

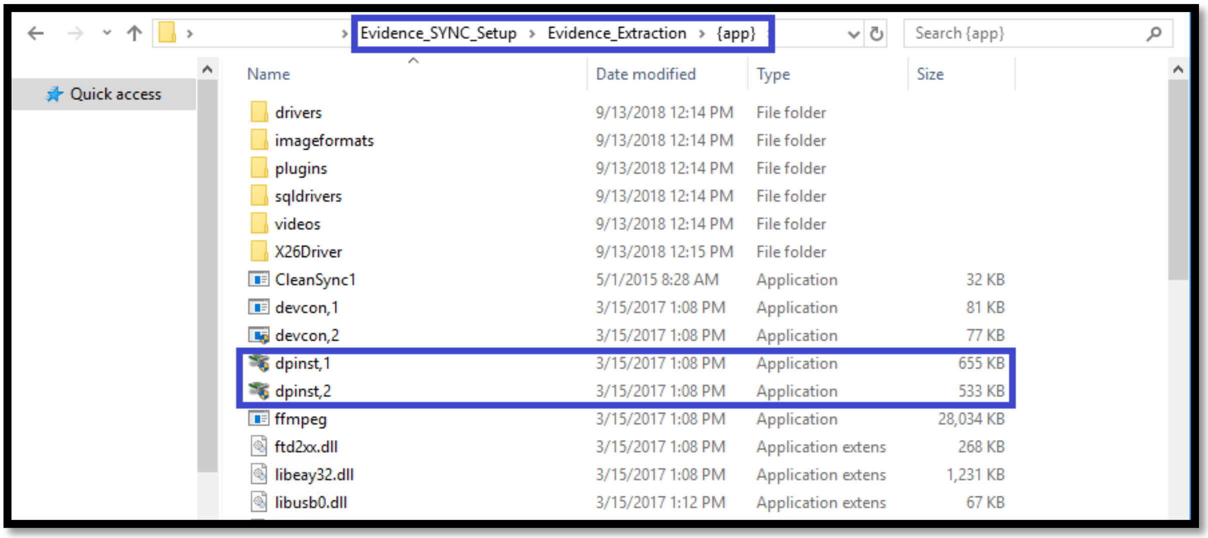
Behaviour: Modify file

Detail info: C:\WINDOWS\DPINST.LOG ---> Offset = 0
C:\WINDOWS\DPINST.LOG ---> Offset = 2
C:\WINDOWS\DPINST.LOG ---> Offset = 102
C:\WINDOWS\DPINST.LOG ---> Offset = 160
C:\WINDOWS\DPINST.LOG ---> Offset = 228

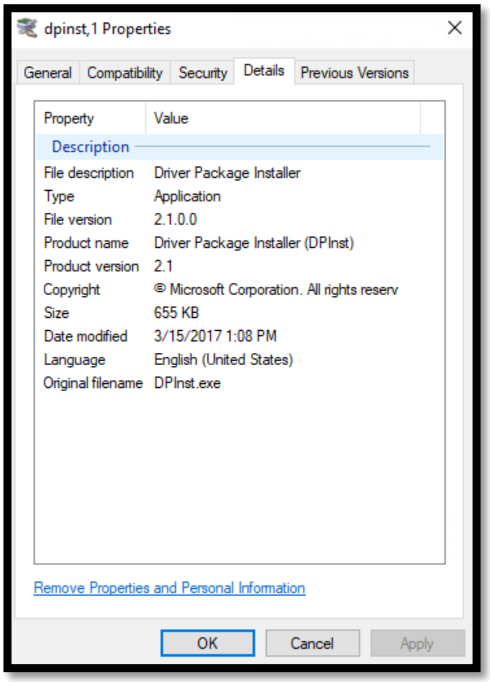
Behaviour: Find file

Detail info: FileName = C:\Documents and Settings\Administrator\Local Settings\%temp%*.*

3. The driver package installer “dpinst,1” (after decompression) could represent some security risks[7], despite the fact of being whitelisted[8]:



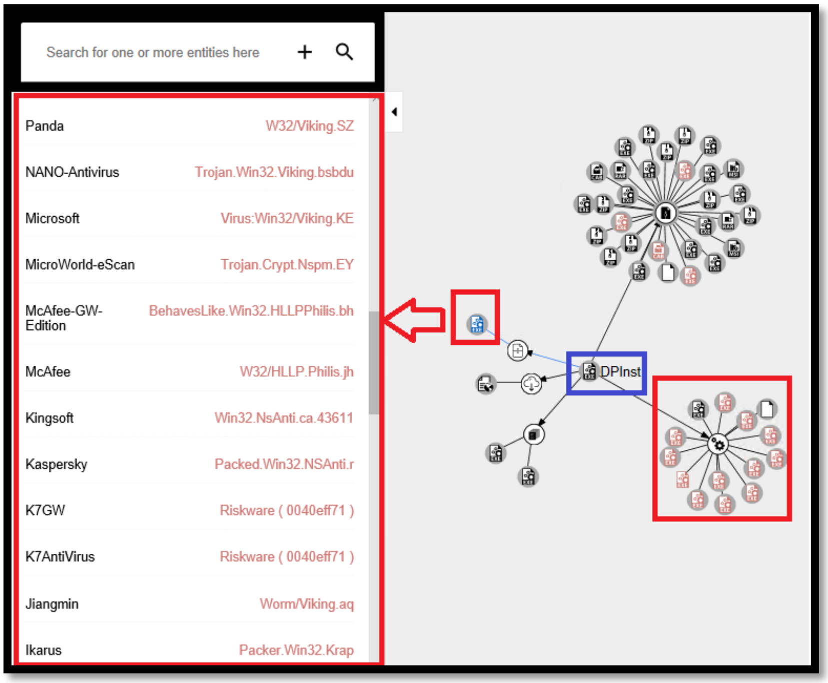
Name	Date modified	Type	Size
drivers	9/13/2018 12:14 PM	File folder	
imageformats	9/13/2018 12:14 PM	File folder	
plugins	9/13/2018 12:14 PM	File folder	
sqldrivers	9/13/2018 12:14 PM	File folder	
videos	9/13/2018 12:14 PM	File folder	
X26Driver	9/13/2018 12:15 PM	File folder	
CleanSync1	5/1/2015 8:28 AM	Application	32 KB
devcon,1	3/15/2017 1:08 PM	Application	81 KB
devcon,2	3/15/2017 1:08 PM	Application	77 KB
dpinst,1	3/15/2017 1:08 PM	Application	655 KB
dpinst,2	3/15/2017 1:08 PM	Application	533 KB
ffmpeg	3/15/2017 1:08 PM	Application	28,034 KB
ftd2xx.dll	3/15/2017 1:08 PM	Application extens	268 KB
libeay32.dll	3/15/2017 1:08 PM	Application extens	1,231 KB
libusb0.dll	3/15/2017 1:12 PM	Application extens	67 KB



Property	Value
Description	
File description	Driver Package Installer
Type	Application
File version	2.1.0.0
Product name	Driver Package Installer (DPInst)
Product version	2.1
Copyright	© Microsoft Corporation. All rights reserv
Size	655 KB
Date modified	3/15/2017 1:08 PM
Language	English (United States)
Original filename	DPInst.exe

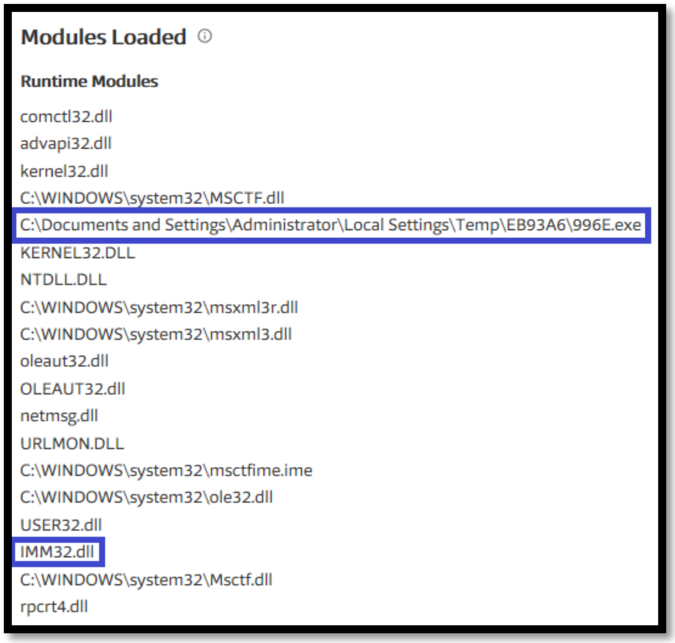
[7] https://www.virustotal.com/#/file/cdd0b13eefadc1ad1fd815d188c377671c46a6822ee95590aca19f83b112c5f5/relations

[8] https://www.hybrid-analysis.com/sample/cdd0b13eefadc1ad1fd815d188c377671c46a6822ee95590aca19f83b112c5f5/5ba14f497ca3e111c36bf665



Panda	W32/Viking.SZ
NANO-Antivirus	Trojan.Win32.Viking.bsbdu
Microsoft	Virus:Win32/Viking.KE
MicroWorld-eScan	Trojan.Crypt.Nspm.EY
McAfee-GW-Edition	BehavesLike.Win32.HLLPPhilis.bh
McAfee	W32/HLLP.Philis.jh
Kingsoft	Win32.NsAnti.ca.43611
Kaspersky	Packed.Win32.NSAnti.r
K7GW	Riskware (0040eff71)
K7AntiVirus	Riskware (0040eff71)
Jiangmin	Worm/Viking.aq
Ikarus	Packer.Win32.Krap

While the driver package installer[9] “dpinst,2” shows some ambiguous[10] behavior, which could be associated with the file 996E.exe[11]:



Modules Loaded

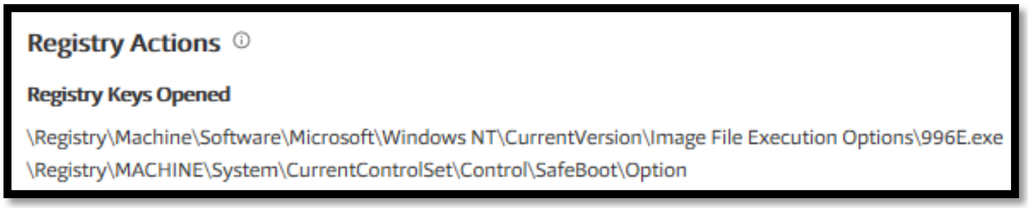
Runtime Modules

```
comctl32.dll
advapi32.dll
kernel32.dll
C:\WINDOWS\system32\MSCTF.dll
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
KERNEL32.DLL
NTDLL.DLL
C:\WINDOWS\system32\msxml3r.dll
C:\WINDOWS\system32\msxml3.dll
oleaut32.dll
OLEAUT32.dll
netmsg.dll
URLMON.DLL
C:\WINDOWS\system32\msctfime.ime
C:\WINDOWS\system32\ole32.dll
USER32.dll
IMM32.dll
C:\WINDOWS\system32\Msctf.dll
rpcrt4.dll
```

[9] https://www.virustotal.com/#/file/cf2910e87e064c5b1beec56c6603750bbb579548bafe8b30095920de2f9b4a30/behavior

[10] https://www.hybrid-analysis.com/sample/cf2910e87e064c5b1beec56c6603750bbb579548bafe8b30095920de2f9b4a30/57d22b4daac2ed54468e6e2d

[11] http://www.exefilesupport.com/easy-guide-to-remove-996e-exe-from-pc

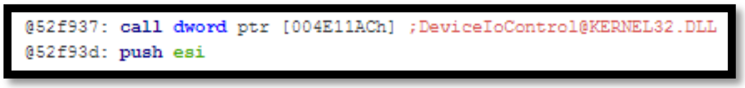


Registry Actions

Registry Keys Opened

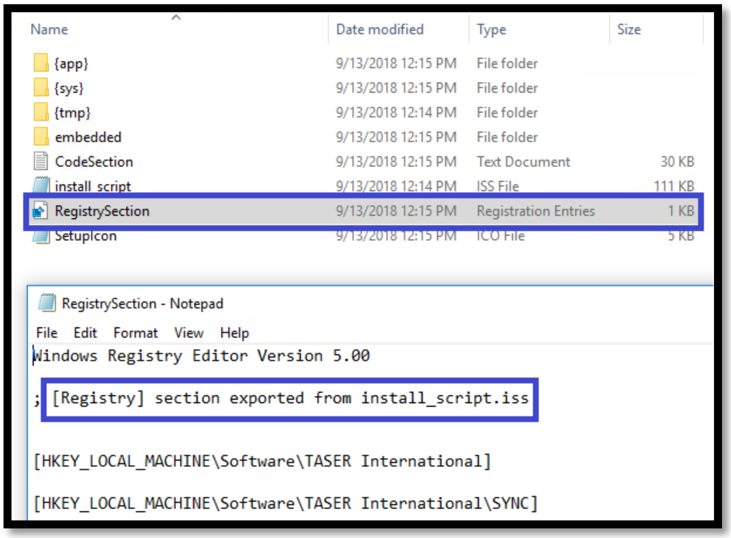
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option

And the Kernel32 function DeviceIoControl [12]:



```
@52f937: call dword ptr [004E11ACh] ;DeviceIoControl@KERNEL32.DLL
@52f93d: push esi
```

4. Finally, changes in the registry are possibly due to the file install_script.iss observed after decompressing the executable file.



Name	Date modified	Type	Size
{app}	9/13/2018 12:15 PM	File folder	
{sys}	9/13/2018 12:15 PM	File folder	
{tmp}	9/13/2018 12:14 PM	File folder	
embedded	9/13/2018 12:15 PM	File folder	
CodeSection	9/13/2018 12:15 PM	Text Document	30 KB
install_script	9/13/2018 12:14 PM	ISS File	111 KB
RegistrySection	9/13/2018 12:15 PM	Registration Entries	1 KB
SetupIcon	9/13/2018 12:15 PM	ICO File	5 KB

RegistrySection - Notepad

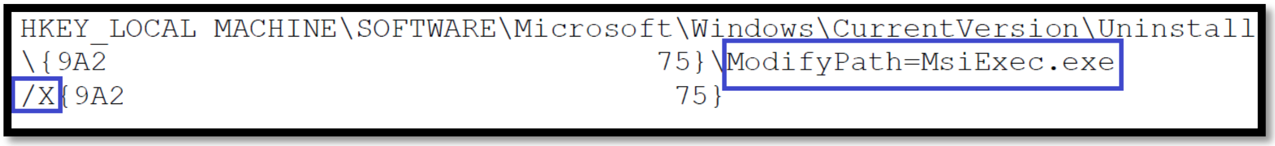
```
Windows Registry Editor Version 5.00

; [Registry] section exported from install_script.iss

[HKEY_LOCAL_MACHINE\Software\TASER International]

[HKEY_LOCAL_MACHINE\Software\TASER International\SYNC]
```

For instance, there was a change related to the file msiexec.exe[13] which gives full control over the installation process:



```
HKEY_LOCAL MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\{9A2                                   75}\ModifyPath=MsiExec.exe
/X{9A2                                  75}
```

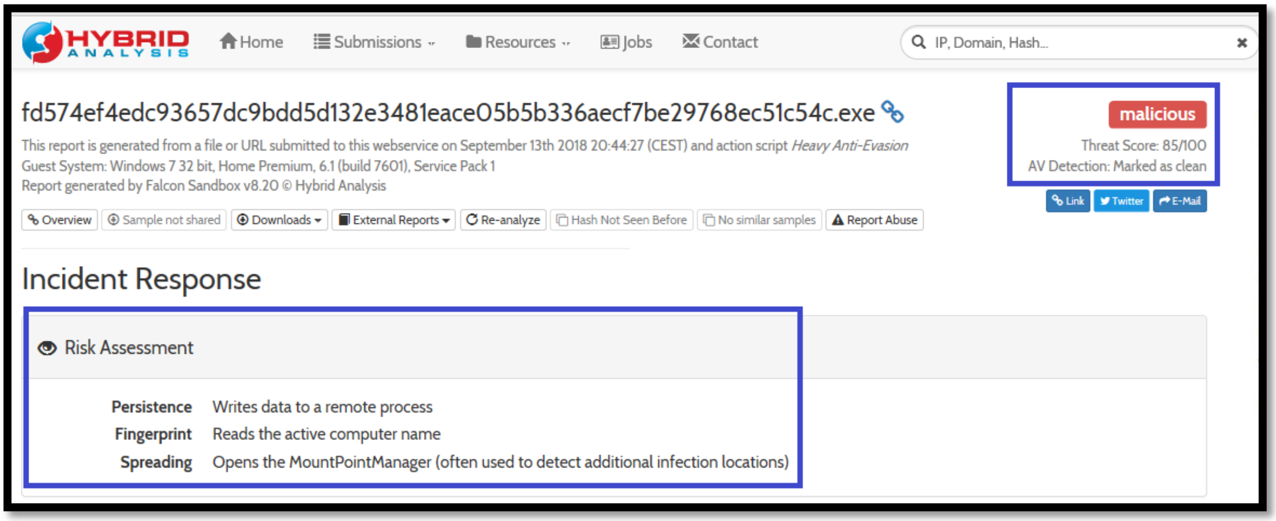
Further analysis is also recommended for the other registries such as Current User, Classes Root, and Users.

[12] https://msdn.microsoft.com/en-us/library/windows/desktop/aa363216(v=vs.85).aspx

[13] https://www.advancedinstaller.com/user-guide/msiexec.html

Attack

These were the identified risks[14]:



fd574ef4edc93657dc9bdd5d132e3481eace05b5b336aecf7be29768ec51c54c.exe

This report is generated from a file or URL submitted to this webservice on September 13th 2018 20:44:27 (CEST) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.20 © Hybrid Analysis

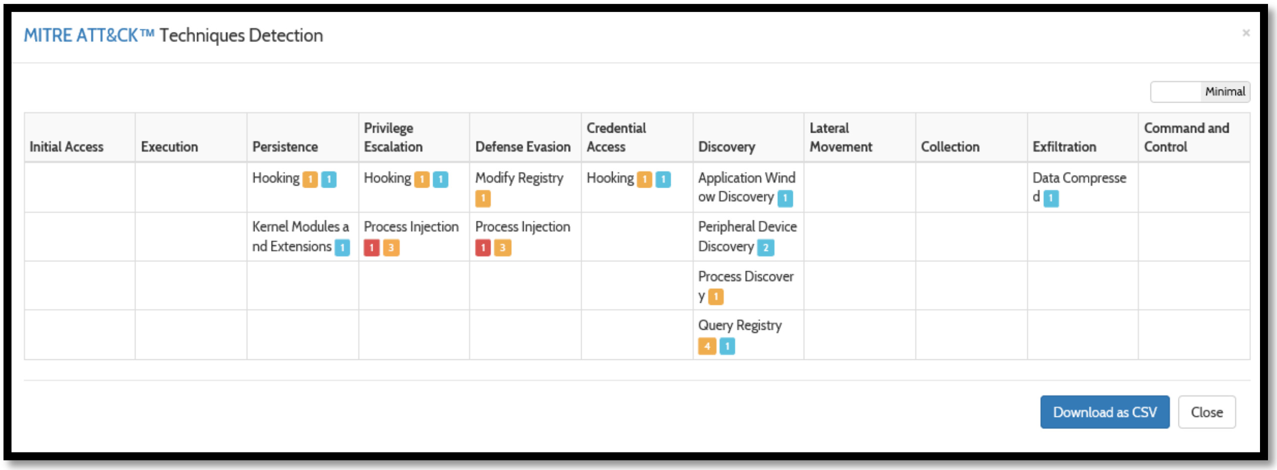
malicious
Threat Score: 85/100
AV Detection: Marked as clean

Incident Response

Risk Assessment

Persistence	Writes data to a remote process
Fingerprint	Reads the active computer name
Spreading	Opens the MountPointManager (often used to detect additional infection locations)

These are the documented attack techniques identified:



MITRE ATT&CK™ Techniques Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Hooking 1 1	Hooking 1 1	Modify Registry 1	Hooking 1 1	Application Window Discovery 1			Data Compressed 1	
		Kernel Modules and Extensions 1	Process Injection 1 3	Process Injection 1 3		Peripheral Device Discovery 2				
						Process Discovery 1				
						Query Registry 4 1				

[14] https://www.hybrid-analysis.com/sample/fd574ef4edc93657dc9bdd5d132e3481eace05b5b336aecf7be29768ec51c54c/5b05353d7ca3e159605736d9