

Name: Smayan Daruka
Date: 12/15/18
CSEC-466: Introduction to Malware

Shamoon Malware Analysis


For the purpose of this project, I decided to analyze the “Shamoon” malware which was used to target national oil companies in Saudi Arabia. Essentially, this virus can spread to other machines on a network and it more or less erases all files from a machine, and overwrites the master boot record rendering the machine unusable.

I performed the various levels of analysis covered in this class including basic static, basic dynamic, advanced static, and advanced dynamic. All of the various analyses highlighted important things in the malware which are discussed throughout the report and a summary is provided at the end of the report as well.

BASIC STATIC

I used a variety of tools to perform basic static analysis which included Virus Total, Strings, FLOSS, PEiD, PEview, Dependency Walker, and Resource Hacker.

Virus Total



60 engines detected this file

SHA-256: 4f02a9fcd2deb3936ede8f009bd08662bdb1f365c0f4a78b3757a98c2f40400

File name: B14299FD4D1CBF84CC7486D978398214

File size: 966 KB

Last analysis: 2018-11-10 05:38:41 UTC

Community score: -449

Detection

Details

Relations

Behavior

Community

Ad-Aware	Gen:Trojan.Heur.BuOjILmJdSm	AegisLab	Trojan.Win32.EraseMBR.41c
AhnLab-V3	Win-Trojan/DistTrack.989184	ALYac	Trojan.DistTrack.A
Antiy-AVL	Trojan.Win32.EraseMBR	Arcabit	Trojan.Heur.ED134FC
Avast	Win32:DistTrack-A [Trj]	AVG	Win32:DistTrack-A [Trj]
Avira	TR/Crypt.FKM.Gen	BitDefender	Gen:Trojan.Heur.BuOjILmJdSm
Bkav	W32/DistTrackA.Trojan	CAT-QuickHeal	Trojan.Wipmbr
ClamAV	Win.Trojan.DistTrack-1	CMC	Trojan.Win32.Swizzor.310
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.d4d1cb
Cylance	Unsafe	Cyren	W32/DistTrack.VG.NA.8394
DrWeb	Trojan.XORMBR.165	Emsisoft	Gen:Trojan.Heur.BuOjILmJdSm (B)
Endgame	malicious (high confidence)	eScan	Gen:Trojan.Heur.BuOjILmJdSm
ESET-NOD32	Win32/DistTrack.A	F-Prot	W32/DistTrack.B
F-Secure	Gen:Trojan.Heur.BuOjILmJdSm	Fortinet	W32/Midrop.EL0tr
GData	Gen:Trojan.Heur.BuOjILmJdSm	Ikarus	Trojan.Win32.EraseMBR
Jiangmin	Trojan/Generica.aimye	K7AntiVirus	Riskware (OO15e4f01)

ExifTool File Metadata

CharacterSet	Unicode
CodeSize	84480
CompanyName	Microsoft Corporation
EntryPoint	0x892b
FileDescription	Distributed Link Tracking Server
FileFlagsMask	0x003f
FileOS	Windows NT 32-bit
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	5.2.3790.0 (srv03_rtm.030324-2048)
FileVersionNumber	5.2.3790.0
ImageFileCharacteristics	Executable, 32-bit
ImageVersion	0.0
InitializedDataSize	913408
InternalName	Distributed Link Tracking Server
LanguageCode	English (U.S.)
LegalCopyright	Microsoft Corporation. All rights reserved.
LinkerVersion	10.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	5.1
ObjectFileType	Executable application
OriginalFileName	trksvr
PEType	PE32
ProductName	Microsoft Windows Operating System
ProductVersion	5.2.3790.0
ProductVersionNumber	5.2.3790.0
Subsystem	Windows command line
SubsystemVersion	5.1
TimeStamp	2012:08:09 23:46:22 +01:00
UninitializedDataSize	0

As can be seen in the above two images, this binary is detected to contain trojan or other malicious characteristics by around 60 out of 67 engines. The one on the right highlights that the file uses a Unicode character set and is a distributed link tracking server file. It is also shown that the binary is a PE32 executable.

Detection

Details

Relations

Behavior

Community

Basic Properties

MD5	b14299fd4d1cbfb4cc7486d978398214
SHA-1	7c0dc6a8f4d2d762a07a523f19b7acd2258f7ecc
Authentihash	6196a1f3d12f6dfd33332e4833f0d2ba9a6559520cb87ca28a4e471ab069315b
Imphash	da9452a2aec343eaa7f76987d3524568
File Type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
SSDeep	12288:Xfz3ZXNPcwmGWdCCg98gJWGG2EbZxHlk3qBUb7Ub:XfzZdE5Ng98gJWb2Ebzm3q
TRiD	Win32 Executable MS Visual C++ (generic) (41%) Win64 Executable (generic) (36.3%) Win32 Dynamic Link Library (generic) (8.6%) Win32 Executable (generic) (5.9%) OS/2 Executable (generic) (2.6%)
File Size	966 KB

Tags

peexe via-tor

History

Creation Time	2012-08-09 22:46:22
First Seen In The Wild	2008-04-14 04:00:00
First Submission	2012-08-15 13:21:36
Last Submission	2018-11-10 05:38:41
Last Analysis	2018-11-10 05:38:41

File Names

B14299FD4D1CBFB4CC7486D978398214
Distributed Link Tracking Server
trksvr
trksvr.exe
VirusShare_b14299fd4d1cbfb4cc7486d978398214
B14299FD4D1CBFB4CC7486D978398214.exe
Shamoon.exe



As can be seen above, the various hashes of the file are given, and also the common names this binary has been seen to use. The graph summary also shows us the various IP addresses in use and the dependencies.

Signature Info ⓘ

Signature Verification

⚠ This file is not signed

File Version Information

Copyright © Microsoft Corporation. All rights reserved.
Product Microsoft® Windows® Operating System
Description Distributed Link Tracking Server
Original Name trksvr
Internal Name Distributed Link Tracking Server
File Version 5.2.3790.0 (srv03_rtm.030324-2048)

Portable Executable Info ⓘ

Header

Target Machine Intel 386 or later processors and compatible processors
Compilation Timestamp 2012-08-09 22:46:22
Entry Point 35115
Contained Sections 5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	84060	84480	6.56	9b7dd2814196d4e8ff374a5c35f460b1
.rdata	90112	23866	24064	4.88	808604e81d696da976c86743e6385dc7
.data	114688	17060	7680	2.78	1a0c07eac1759c283f180b21c724e391
.rsrc	135168	861472	861696	7.64	a7f1881e3af06feac03dd3a2298f5a69
.reloc	999424	9952	10240	4.34	b5a6fa4a6300ae0fd06ec445e50ec9e5

Imports

+ ADVAPI32.dll
+ KERNEL32.dll
+ NETAPI32.dll
+ SHELL32.dll



Registry Keys Deleted

<HKLM>\SYSTEM\CurrentControlSet\Services\TrkSvr\WOW64

Process And Service Actions ⓘ

Processes Created

<PATH_SAMPLE.EXE>
<SYSTEM32>\trksvr.exe

Processes Terminated

<PATH_SAMPLE.EXE>


Services Created


TrkSvr

Services Started

TrkSvr

The screenshot above shows the headers of the executable and the various imports that this binary uses. This information is really helpful since it tells us the behavior of the binary by analyzing the commonly used imports. The sizes of the various sections also tell us that this binary is most certainly packed and obfuscated. The screenshot on the left shows us the registry keys that are modified by this binary and also the processes created.

Detection	Details	Relations 	Behavior	Community 8
-----------	---------	---	-----------------	--------------------------

 Dr.Web vxCube

File System Actions ?

Files Opened

%WINDIR%\windowshell.manifest
 <SYSTEM32>\trksvr.exe
 <SYSTEM32>\ntdll.dll


Files Written

<SYSTEM32>\trksvr.exe

Files With Modified Attributes

<SYSTEM32>\trksvr.exe

Files Dropped

 <SYSTEM32>\trksvr.exe


Registry Actions ?

Registry Keys Opened

<HKLM>\System\CurrentControlSet\Control\Terminal Server
 <HKLM>\System\CurrentControlSet\Control\SafeBoot\Option
 <HKLM>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
 <HKLM>\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics
 <HKLM>\System\CurrentControlSet\Control\Error Message Instrument\
 <HKLM>\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
 <HKLM>\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32
 <HKLM>\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility
 <HKLM>\Software\Microsoft\Windows NT\CurrentVersion\Windows
 <HKLM>\Software\Microsoft\Windows\CurrentVersion\Explorer\Performance

▼

Registry Keys Set

 <HKLM>\System\CurrentControlSet\Services\TrkSvr\Type

The above screenshot tells us the registry keys that are accessed by this binary and also what registry keys are set and modified.

Strings

I ran strings on the binary and found the following to interesting in nature:

- t6f90t1f94Pu
- <at,<rt"<wt
- @LanmanWorkstation
- SYSTEM\CurrentControlSet\Services\TrkSvr
- Distributed Link Tracking Server
- Enables the Distributed Link Tracking Client service within the same domain to provide more reliable and efficient maintenance of links within the domain. If this service is disabled, any services that explicitly depend on it will fail to start.
- C:\Windows\system32\svchost.exe -k netsvcs
- kernel32.dll
- Wow64DisableWow64FsRedirection
- Wow64RevertWow64FsRedirection
- PROCESSOR_ARCHITECTURE
- SYSTEM\CurrentControlSet\Control\Session Manager\Environment
- trksrv.exe
- E\$\WINDOWS
- D\$\WINDOWS
- C\$\WINDOWS
- \inf\netft429.pnf
- \System32\cmd.exe /c "ping -n 30 127.0.0.1 >nul && sc config TrkSvr binpath= system32\trksrv.exe && ping -n 10 127.0.0.1 >nul && sc start TrkSvr "
- myimage12767
- c:\windows\temp\out17626867.txt
- Visual C++ CRT: Not enough memory to complete call to sterror.
- bad exception
- AKERNEL32.DLL
- spanish-argentina
- portuguese-brazilian
- norwegian-bokmal
- italian-swiss
- irish-english
- german-swiss
- french-swiss
- english-usa
- dutch-belgian
- chinese-hongkong
- GetCurrentProcessId
- GetSystemTimeAsFileTime
- IsValidCodePage
- IsValidLocale
- WriteConsoleW
- \system32\
- Copyright (c) 1992-2004 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED.
- StringFileInfo
- CompanyName
- Microsoft Corporation
- FileDescription
- Distributed Link Tracking Server
- FileVersion
- 5.2.3790.0 (srv03_rtm.030324-2048)

As can be seen above, there is a string that shows a system command being executed and there are a lot of country and locale strings which shows the widespread nature of this malware.

FLOSS

Just out of curiosity, I also ran FLOSS to see if there will be any additional interesting strings and also to see if there are any strings that can be decoded. As can be seen below, the highlighted strings are really important which are discussed later in the report.

```
PKCS12
PKCS7
X509
VS_VERSION_INFO
StringFileInfo
040904b0
CompanyName
Microsoft Corporation
FileDescription
Distributed Link Tracking Server
FileVersion
5.2.3790.0 (srv03_rtm.030324-2048)
InternalName
Distributed Link Tracking Server
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
trksvr
ProductName
Microsoft
Windows
Operating System
ProductVersion
5.2.3790.0
VarFileInfo
Translation
```

FLOSS decoded 0 strings

FLOSS extracted 4 stackstrings

D\$\WINDOWS

ADMIN\$

C\$\WINDOWS

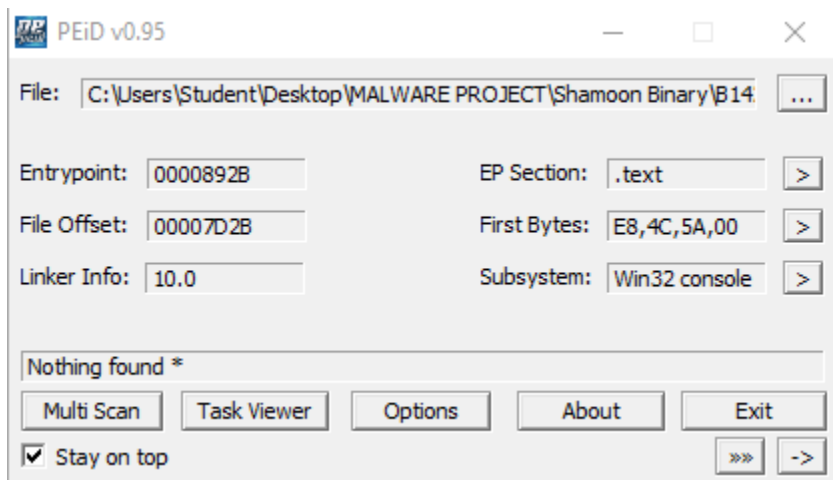
E\$\WINDOWS

Finished execution after 78.473000 seconds

There weren't any strings that were decoded by FLOSS but at least, this was a confirmation that there are a lot of interesting strings.

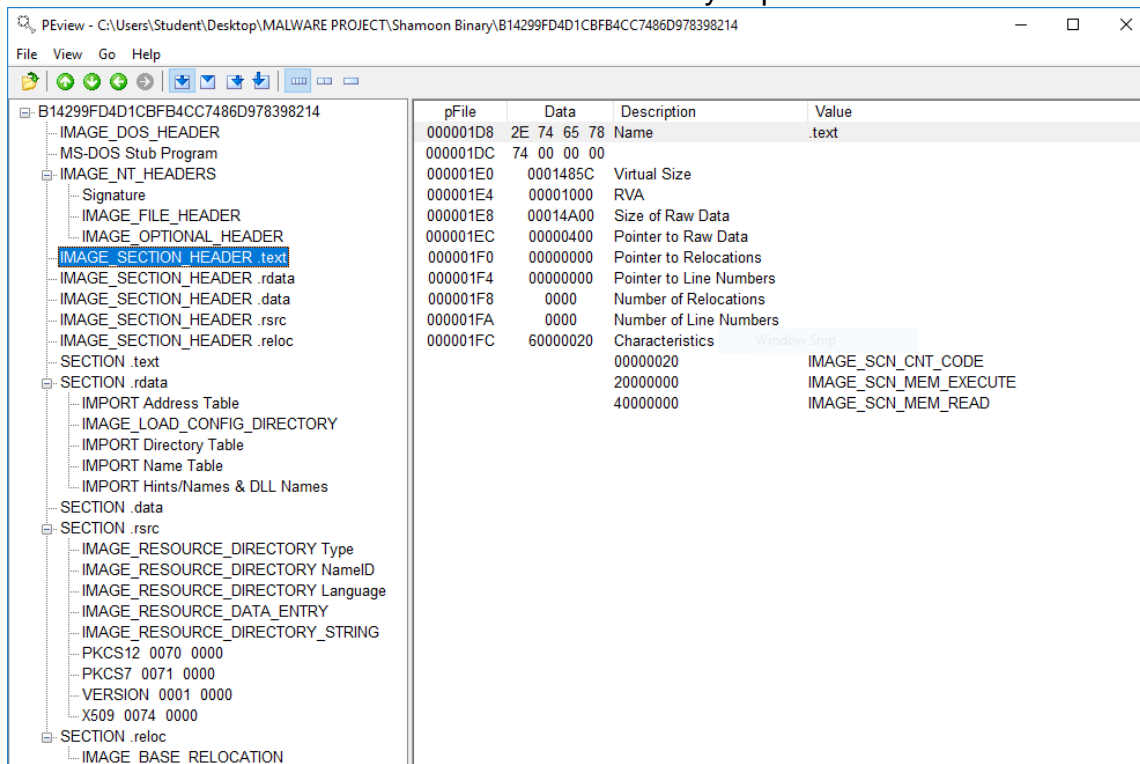
PEiD

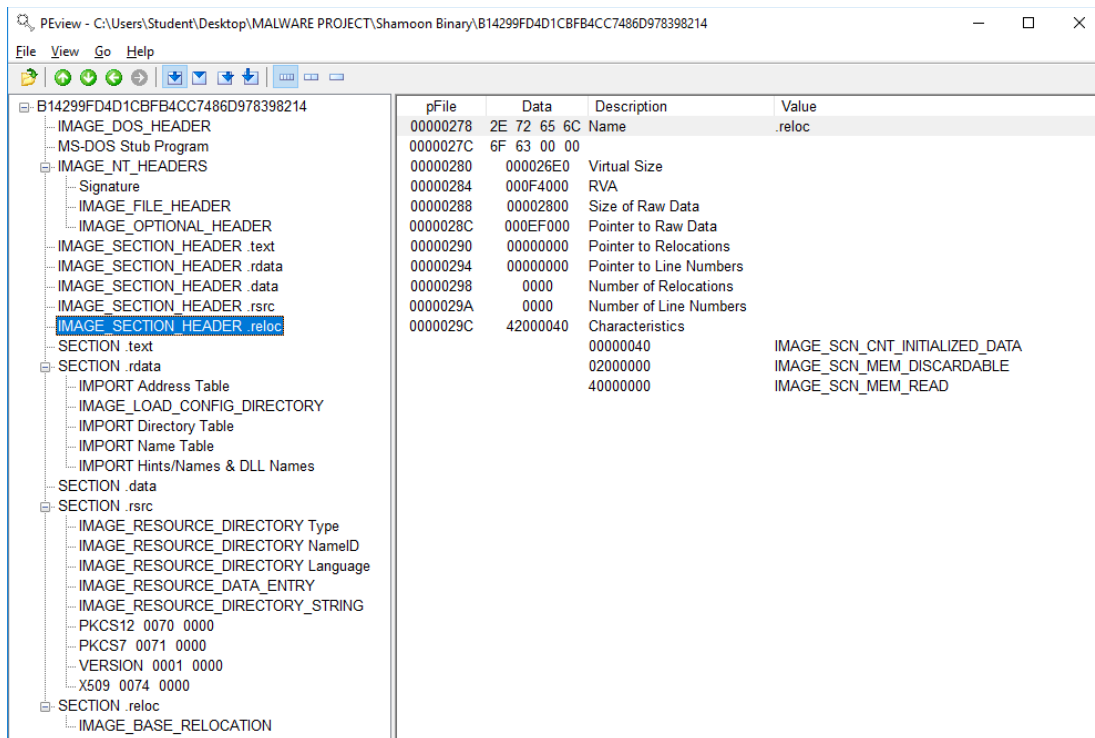
As can be seen below, the binary is indeed packed and obfuscated.



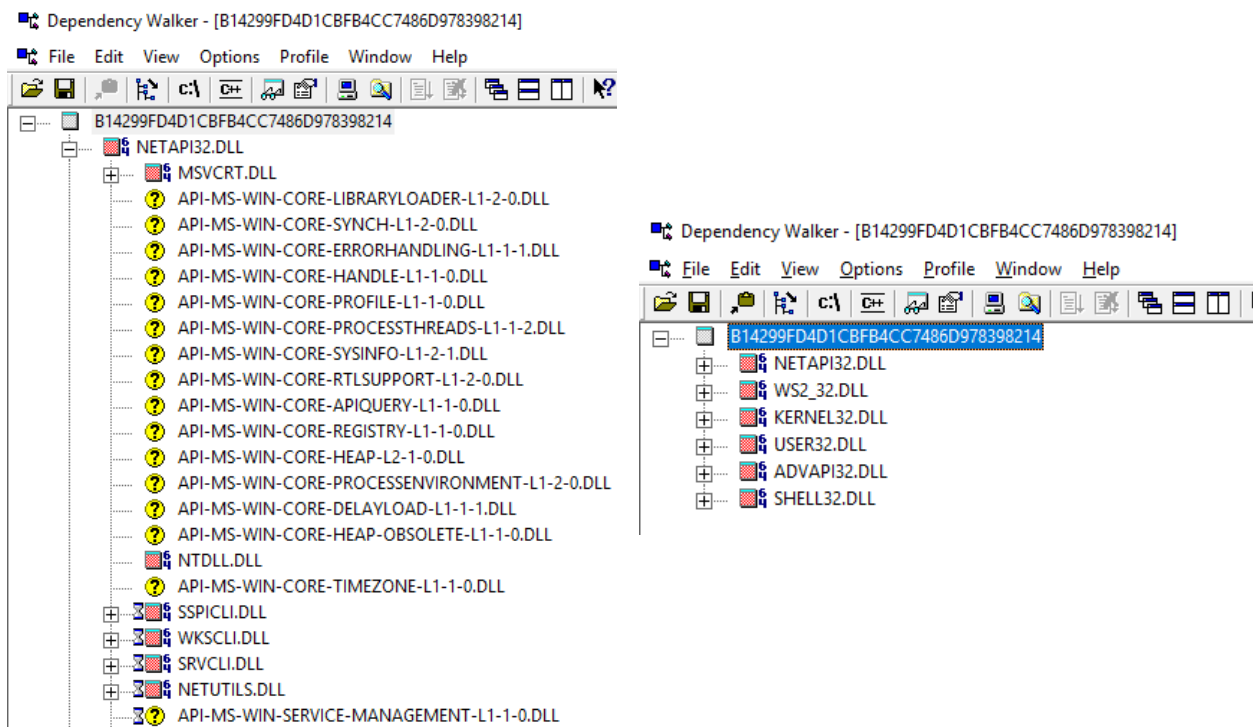
PEview

The two screenshots below confirm that the binary is packed and obfuscated.



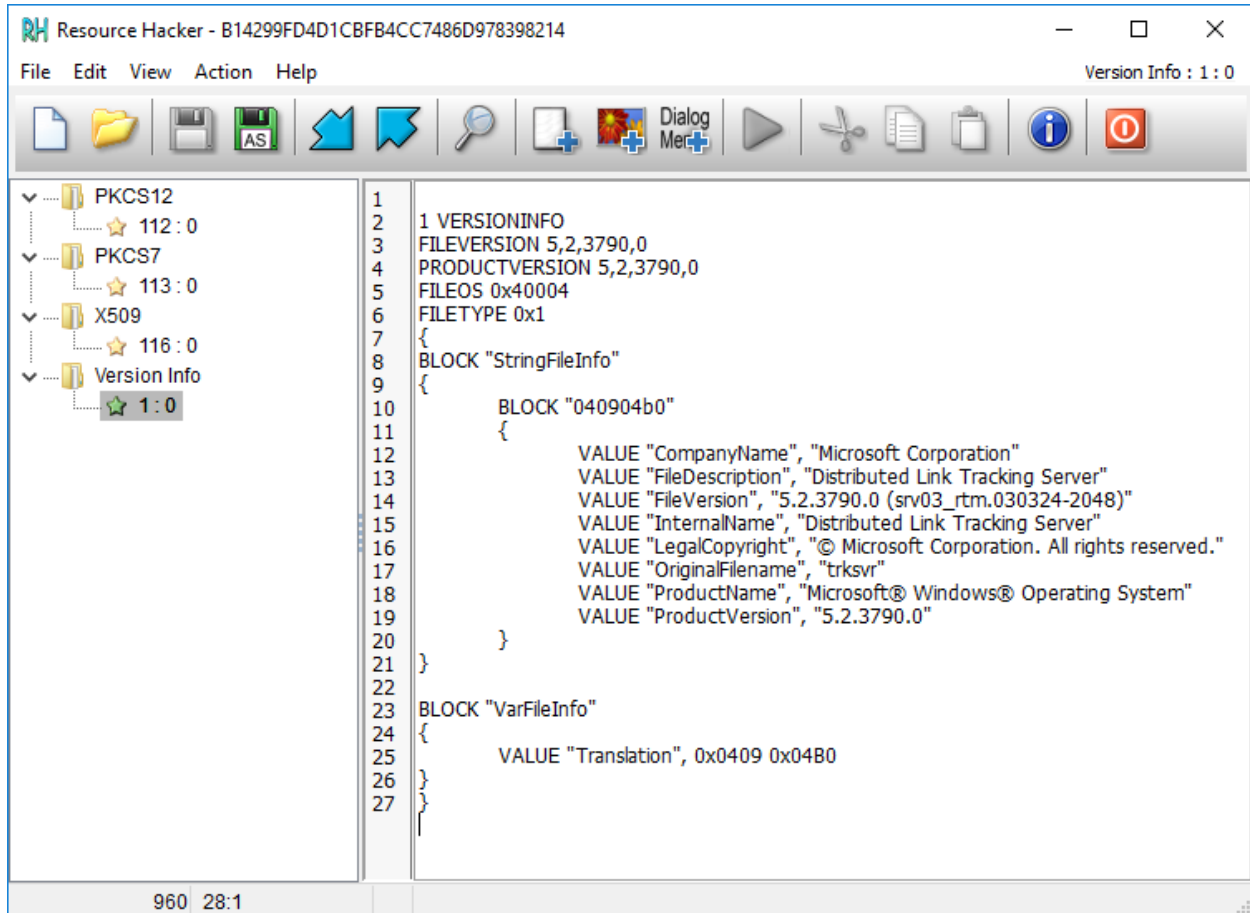


Dependency Walker:



As can be seen in the above images, there are a lot of dependencies used by this binary which are helpful in determining that nature of this binary.

Resource Hacker

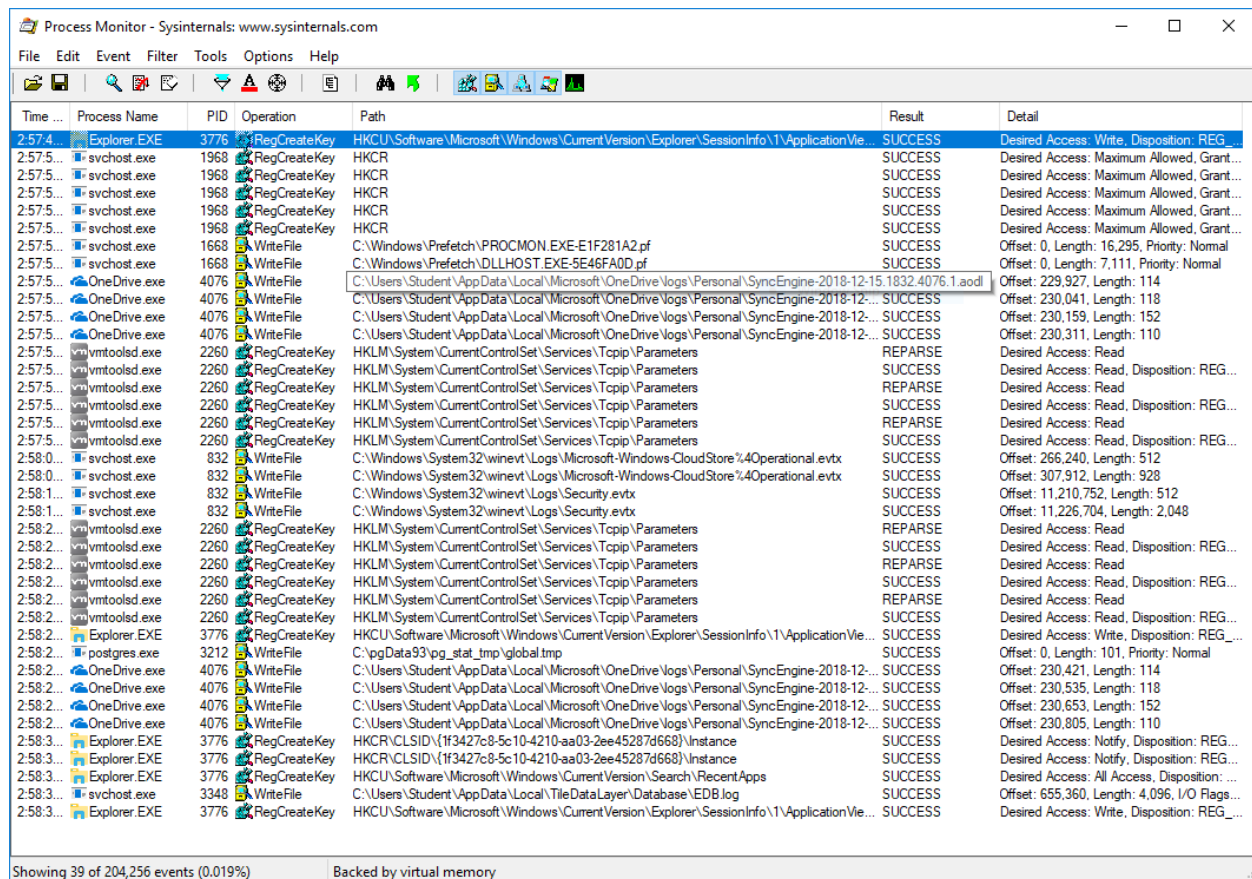


As can be seen above, there is a lot of info about the actual binary such as the file name and the original file name which shows that it was renamed to mask its true identity. We can also see internal file name and its description.

BASIC DYNAMIC

I was unable to use most of the tools in this section with the exception of ProcMon and OllyDebug as the computer kept crashing as soon as the binary was actually run.

ProcMon



Time ...	Process Name	PID	Operation	Path	Result	Detail
2:57.4...	Explorer.EXE	3776	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationVie...	SUCCESS	Desired Access: Write, Disposition: REG...
2:57.5...	svchost.exe	1968	RegCreateKey	HKCR	SUCCESS	Desired Access: Maximum Allowed, Grant...
2:57.5...	svchost.exe	1968	RegCreateKey	HKCR	SUCCESS	Desired Access: Maximum Allowed, Grant...
2:57.5...	svchost.exe	1968	RegCreateKey	HKCR	SUCCESS	Desired Access: Maximum Allowed, Grant...
2:57.5...	svchost.exe	1968	RegCreateKey	HKCR	SUCCESS	Desired Access: Maximum Allowed, Grant...
2:57.5...	svchost.exe	1968	RegCreateKey	HKCR	SUCCESS	Desired Access: Maximum Allowed, Grant...
2:57.5...	svchost.exe	1668	WriteFile	C:\Windows\Prefetch\PROCMON.EXE-E1F281A2.pf	SUCCESS	Offset: 0, Length: 16,295, Priority: Normal
2:57.5...	svchost.exe	1668	WriteFile	C:\Windows\Prefetch\DLLHOST.EXE-5E46FA0D.pf	SUCCESS	Offset: 0, Length: 7,111, Priority: Normal
2:57.5...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-15.1832.4076.1.aodl	SUCCESS	Offset: 229,927, Length: 114
2:57.5...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,041, Length: 118
2:57.5...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,159, Length: 152
2:57.5...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,311, Length: 110
2:57.5...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
2:57.5...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read, Disposition: REG...
2:57.5...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
2:57.5...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read, Disposition: REG...
2:57.5...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
2:57.5...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read, Disposition: REG...
2:58.0...	svchost.exe	832	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-CloudStore%40Operational.evtx	SUCCESS	Offset: 266,240, Length: 512
2:58.0...	svchost.exe	832	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-CloudStore%40Operational.evtx	SUCCESS	Offset: 307,912, Length: 928
2:58.1...	svchost.exe	832	WriteFile	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 11,210,752, Length: 512
2:58.1...	svchost.exe	832	WriteFile	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 11,226,704, Length: 2,048
2:58.2...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
2:58.2...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read, Disposition: REG...
2:58.2...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
2:58.2...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read, Disposition: REG...
2:58.2...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
2:58.2...	vmtoolsd.exe	2260	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read, Disposition: REG...
2:58.2...	Explorer.EXE	3776	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationVie...	SUCCESS	Desired Access: Write, Disposition: REG...
2:58.2...	postgres.exe	3212	WriteFile	C:\pgData93\pg_stat_tmp\global.tmp	SUCCESS	Offset: 0, Length: 101, Priority: Normal
2:58.2...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,421, Length: 114
2:58.2...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,535, Length: 118
2:58.2...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,653, Length: 152
2:58.2...	OneDrive.exe	4076	WriteFile	C:\Users\Student\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2018-12-...	SUCCESS	Offset: 230,805, Length: 110
2:58.3...	Explorer.EXE	3776	RegCreateKey	HKCR\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: Notify, Disposition: REG...
2:58.3...	Explorer.EXE	3776	RegCreateKey	HKCR\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance	SUCCESS	Desired Access: Notify, Disposition: REG...
2:58.3...	Explorer.EXE	3776	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps	SUCCESS	Desired Access: All Access, Disposition: ...
2:58.3...	svchost.exe	3348	WriteFile	C:\Users\Student\AppData\Local\TileDataLayer\Database\EDB.log	SUCCESS	Offset: 655,360, Length: 4,096, I/O Flags...
2:58.3...	Explorer.EXE	3776	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationVie...	SUCCESS	Desired Access: Write, Disposition: REG...

Showing 39 of 204,256 events (0.019%) Backed by virtual memory

There isn't a whole lot of useful information in here except the fact that a lot of registry keys are being consistently modified on the system.

OllyDebug

OllyDbg - B14299FD4D1CBFB4CC7486D978398214 - [CPU - main thread, module B14299FD4D1CBFB4CC7486D97839821]

Address	Disassembly	Comment
000388E6	> E8 7AFEFFFF CALL 00038765	
000388E8	EB 2E JMP SHORT 0003891B	
000388ED	8B45 EC MOV EAX, DWORD PTR SS:[EBP-14]	
000388F0	8B08 MOV ECX, DWORD PTR DS:[EAX]	
000388F2	8B09 MOV ECX, DWORD PTR DS:[ECX]	
000388F4	894D DC MOV DWORD PTR SS:[EBP-24], ECX	
000388F7	50 PUSH EAX	
000388F8	51 PUSH ECX	
000388F9	E8 FC550000 CALL 0003DEFA	
000388FF	59 POP ECX	
00038900	59 POP ECX	
00038900	C3 RETN	
00038901	8B65 E8 MOV ESP, DWORD PTR SS:[EBP-18]	
00038904	8B45 DC MOV EAX, DWORD PTR SS:[EBP-24]	
00038907	8945 E0 MOV DWORD PTR SS:[EBP-20], EAX	
0003890A	837D E4 00 CMP DWORD PTR SS:[EBP-1C], 0	
0003890E	75 06 JNE SHORT 00038916	
00038910	50 PUSH EAX	
00038911	E8 39FEFFFF CALL 0003874F	
00038916	> E8 59FEFFFF CALL 00038774	
0003891B	> C745 FC FEFF MOV DWORD PTR SS:[EBP-4], -2	
00038922	8B45 E0 MOV EAX, DWORD PTR SS:[EBP-20]	
00038925	E8 DB380000 CALL 0003C205	
00038928	C3 RETN	
0003892B	E8 4C5A0000 CALL 0003E37C	
00038930	E9 95FEFFFF JMP 000387CA	
00038935	8BFF MOV EDI, EDI	
00038937	55 PUSH EBP	
00038938	8BEC MOV EBP, ESP	
0003893A	8B45 08 MOV EAX, DWORD PTR SS:[EBP+8]	
0003893D	85C0 TEST EAX, EAX	
0003893F	74 12 JZ SHORT 00038953	
00038941	83E8 08 SUB EAX, 8	
00038944	8138 D0D00000 CMP DWORD PTR DS:[EAX], 0D0D0000	
0003894A	75 07 JNE SHORT 00038953	
0003894C	50 PUSH EAX	
0003894D	E8 7AEFFFFF CALL 000377CC	
00038952	59 POP ECX	
00038953	59 POP EBP	
00038954	C3 RETN	
00038955	8BFF MOV EDI, EDI	
00038957	55 PUSH EBP	
00038958	8BEC MOV EBP, ESP	
0003895A	8B45 08 MOV EAX, DWORD PTR SS:[EBP+8]	
0003895D	56 PUSH ESI	
0003895E	8BF1 MOV ESI, ECX	
00038960	C646 0C 00 MOV BYTE PTR DS:[ESI+0C], 0	
00038964	85C0 TEST EAX, EAX	
00038966	75 63 JNZ SHORT 000389CB	
00038968	E8 752C0000 CALL 0003B5E2	
0003896D	8946 08 MOV DWORD PTR DS:[ESI+8], EAX	
00038970	8B48 6C MOV ECX, DWORD PTR DS:[EAX+6C]	
00038973	890E MOV DWORD PTR DS:[ESI], ECX	
00038975	8B48 68 MOV ECX, DWORD PTR DS:[EAX+68]	
00038978	894E 04 MOV DWORD PTR DS:[ESI+4], ECX	
0003897B	8B0E MOV ECX, DWORD PTR DS:[ESI]	
0003897D	3B0D 40D0D401 CMP ECX, DWORD PTR DS:[0D40D401]	
00038983	74 12 JF SHORT 00038997	

ECX=0003892B (B14299FD4D1CBFB4CC7486D97839821.<ModuleEntryPoint>) (current registers)
Stack [013FB981]=0 (current registers)

As can be seen above, this binary has a lot of call instructions indicating there are many conditions and even pathways for this binary to take.

ADVANCED STATIC

I was only able to use IDA Pro to perform advanced static analysis of this binary.

IDA Pro

Address	Length	Type	String
0000001F	00000001	C	Wow64DisableWow64FsRedirection
0000001E	00000001	C	Wow64RevertWow64FsRedirection
00000010	00000001	C	string too long
00000018	00000001	C	invalid string position
00000009	00000001	C	Schedule
00000007	00000007	C	JobAdd
00000013	00000001	C	vector<T> too long
00000015	00000001	C	ios_base::eofbit set
00000016	00000001	C	ios_base::failbit set
00000015	00000001	C	ios_base::badbit set
00000010	00000001	C	bad locale name
00000009	00000001	C	bad cast
00000020	00000001	C	c:\windows\temp\out17626867.txt
0000000F	00000001	C	kijijnsjbnncbknbkjadc\r\nkjdsjbjhsdbhfcbjskhdj jhg jkhg hjk hjk \r\nslkdj...
00000008	00000001	C	generic
00000009	00000001	C	iostream
00000007	00000001	C	system
00000016	00000001	C	iostream stream error
00000012	00000001	C	Unknown exception
0000000F	00000001	C	bad allocation
0000000F	00000001	C	CorExitProcess
00000005	00000001	C	\a\b\n\v
0000005F	00000001	C	!\'#\$%&()*+,-./0123456789;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abc...
00000005	00000001	C	\a\b\n\v
0000005F	00000001	C	!\'#\$%&()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZUVWXY...
00000008	00000001	C	LC_TIME
00000008	00000001	C	LC_NUMERIC
0000000C	00000001	C	LC_MONETARY
00000009	00000001	C	LC_CTYPE
00000008	00000001	C	LC_COLLATE
00000007	00000001	C	LC_ALL
00000005	00000001	C	\a\b\n\v
0000005F	00000001	C	!\'#\$%&()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZUVWXY...
00000040	00000001	C	Visual C++ CRT: Not enough memory to complete call to sterror.

As can be seen above, there are a lot of strings in this program which correlate to the strings in the basic static analysis stage.

```

.text:00408955 sub_408955 proc near                                     ; CODE XREF: sub_408BC3+E↓p
.text:00408955                                     ; sub_408C32+E↓p ...
.text:00408955 arg_0 = dword ptr 8
.text:00408955
* .text:00408955 mov edi, edi
* .text:00408957 push ebp
* .text:00408958 mov ebp, esp
* .text:0040895A mov eax, [ebp+arg_0]
* .text:0040895D push esi
* .text:0040895E mov esi, ecx
* .text:00408960 mov byte ptr [esi+0Ch], 0
* .text:00408964 test eax, eax
* .text:00408966 jnz short loc_4089CB
* .text:00408968 call sub_4085E2
* .text:0040896D mov [esi+8], eax
* .text:00408970 mov ecx, [eax+6Ch]
* .text:00408973 mov [esi], ecx
* .text:00408975 mov ecx, [eax+68h]
* .text:00408978 mov [esi+4], ecx
* .text:0040897B mov ecx, [esi]
* .text:0040897D cmp ecx, off_41DB40
* .text:00408983 jz short loc_408997
* .text:00408985 mov ecx, dword_41D8F8
* .text:0040898B test [eax+70h], ecx
* .text:0040898E jnz short loc_408997
* .text:00408990 call sub_40E0BB
* .text:00408995 mov [esi], eax
* .text:00408997
* .text:00408997 loc_408997:                                     ; CODE XREF: sub_408955+2E↑j
* .text:00408997                                     ; sub_408955+39↑j
* .text:00408997 mov eax, [esi+4]
* .text:0040899A cmp eax, lpAddend
* .text:004089A0 jz short loc_4089B8
* .text:004089A2 mov eax, [esi+8]
* .text:004089A5 mov ecx, dword_41D8F8
* .text:004089AB test [eax+70h], ecx
* .text:004089AE jnz short loc_4089B8
* .text:004089B0 call sub_40E63A
* .text:004089B5 mov [esi+4], eax
* .text:004089B8
* .text:004089B8 loc_4089B8:                                     ; CODE XREF: sub_408955+4B↑j
* .text:004089B8                                     ; sub_408955+59↑j

```

The screenshot above shows a part of the binary's executable statements that correlate to the initial workings of this malware. This malware overwrites all files on the infected machine and spreads itself throughout the network rendering everything unusable.

ADVANCED DYNAMIC

In this section, I only used X64dbg to perform advanced dynamic analysis. I ran this binary inside a VM which had no internet connection.

X64dbg

The screenshot displays the X64dbg debugger interface. The top menu bar includes File, View, Debug, Trace, Plugins, Favourites, Options, Help, and Sep 13 2018. The toolbar contains icons for CPU, Graph, Log, Notes, Breakpoints, Memory Map, Call Stack, SEH, Script, Symbols, Source, References, Threads, Snowman, Handles, and Trace.

The main window is divided into several panes:

- Disassembly:** Shows assembly instructions with their addresses and hex values. The instruction at address 77F0B880 is highlighted: `EB 00`. The instruction at address 77F0B881 is `33C0`. The instruction at address 77F0B882 is `40`. The instruction at address 77F0B883 is `8B45 E8`. The instruction at address 77F0B884 is `C7 45 FC FFFFFFFF`. The instruction at address 77F0B885 is `E8 E879DFFF`. The instruction at address 77F0B886 is `C3`. The instruction at address 77F0B887 is `64:A1 30000000`. The instruction at address 77F0B888 is `33C9`. The instruction at address 77F0B889 is `9900 3C858077`. The instruction at address 77F0B88A is `9900 3C858077`. The instruction at address 77F0B88B is `8B08`. The instruction at address 77F0B88C is `3648 02`. The instruction at address 77F0B88D is `74 05`. The instruction at address 77F0B88E is `E8 9EFFFFFF`. The instruction at address 77F0B88F is `33C0`. The instruction at address 77F0B890 is `C3`. The instruction at address 77F0B891 is `8BFF`. The instruction at address 77F0B892 is `95`. The instruction at address 77F0B893 is `8BEC`. The instruction at address 77F0B894 is `8B45 FB`. The instruction at address 77F0B895 is `81EC 70010000`. The instruction at address 77F0B896 is `33C0`. The instruction at address 77F0B897 is `8B45 6C010000`. The instruction at address 77F0B898 is `56`. The instruction at address 77F0B899 is `8B45 EC3A0077`. The instruction at address 77F0B89A is `56`. The instruction at address 77F0B89B is `6A 16`. The instruction at address 77F0B89C is `56`. The instruction at address 77F0B89D is `66:894424 10`. The instruction at address 77F0B89E is `8BFF`. The instruction at address 77F0B89F is `6A 16`. The instruction at address 77F0B8A0 is `56`. The instruction at address 77F0B8A1 is `66:894424 12`. The instruction at address 77F0B8A2 is `8D4424 70`. The instruction at address 77F0B8A3 is `894424 6C`. The instruction at address 77F0B8A4 is `33C9`. The instruction at address 77F0B8A5 is `C74424 14 804A8F77`. The instruction at address 77F0B8A6 is `C74424 68 00000001`. The instruction at address 77F0B8A7 is `66:894424 70`. The instruction at address 77F0B8A8 is `0516`. The instruction at address 77F0B8A9 is `74 29`. The instruction at address 77F0B8AA is `8B45 3003FE7F`. The instruction at address 77F0B8AB is `8B45`. The instruction at address 77F0B8AC is `6A 20`. The instruction at address 77F0B8AD is `8B45 1F`. The instruction at address 77F0B8AE is `59`. The instruction at address 77F0B8AF is `7BCB`. The instruction at address 77F0B8B0 is `D3CE`.
- Registers:** Shows the state of the CPU registers. The EAX register is highlighted, showing its value as 00000000.
- Memory Dump:** Shows a dump of memory at address 77F0B880. The dump is organized into columns for Address, Hex, ASCII, and Comment. The comment for the first row is "Jump is taken".
- Registers:** Shows the state of the CPU registers. The EAX register is highlighted, showing its value as 00000000.
- Registers:** Shows the state of the CPU registers. The EAX register is highlighted, showing its value as 00000000.

As can be seen above, this binary initializes processes and runs scheduled tasks to persist on the machine and also be able to spread.

B14299FD4D1CBFB4CC7486D978398214 - PID: 1384 - Module: b14299fd4d1cbfb4cc7486d978398214 - Thread: Main Thread 1190 - x32dbg

File View Debug Trace Plugins Favourites Options Help Sep 13 2018

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman

All Modules (Strings) All Modules (Strings)

Address	Disassembly	String
00D312D2	mov edi, b14299fd4d1cbfb4cc7486d978398214.D46580	"L\"Trksvr"
00D31355	push b14299fd4d1cbfb4cc7486d978398214.D46558	"L\"C:\\windows\\system32\\svchost.exe -k netsvcs"
00D31382	push b14299fd4d1cbfb4cc7486d978398214.D46544	"L\"RpcSs"
00D313AF	mov dword ptr ss:[ebp-3FC], b14299fd4d1cbfb4cc7486d978398214.D46358	"L\"Enables the Distributed Link Tracking Client service"
00D313EF	push b14299fd4d1cbfb4cc7486d978398214.D46544	"L\"RpcSs"
00D31406	push b14299fd4d1cbfb4cc7486d978398214.D46310	"L\"Distributed Link Tracking Server"
00D3142F	mov dword ptr ss:[ebp-3F8], b14299fd4d1cbfb4cc7486d978398214.D46358	"L\"Enables the Distributed Link Tracking Client service"
00D31451	push b14299fd4d1cbfb4cc7486d978398214.D46288	"L\"SYSTEM\\CurrentControlSet\\Services\\Trksvr"
00D31465	push b14299fd4d1cbfb4cc7486d978398214.D462A8	"L\"Wow64"
00D31490	push b14299fd4d1cbfb4cc7486d978398214.D46284	"L\"LanmanWorkstation"
00D31664	mov dword ptr ss:[esp], b14299fd4d1cbfb4cc7486d978398214.D465C0	"L\".exe"
00D3167E	mov ebx, b14299fd4d1cbfb4cc7486d978398214.D4C368	"L\"\\system32\\\\"
00D316A7	mov dword ptr ss:[ebp-808], b14299fd4d1cbfb4cc7486d978398214.D4C000	"L\"cac1srv"
00D31716	push b14299fd4d1cbfb4cc7486d978398214.D465C0	"L\".exe"
00D3176C	push b14299fd4d1cbfb4cc7486d978398214.D465E8	"L\"Wow64Disab1ewow64FsRedirection"
00D31771	push b14299fd4d1cbfb4cc7486d978398214.D465CC	"L\"kernel32.dll"
00D31795	push b14299fd4d1cbfb4cc7486d978398214.D46608	"L\"Wow64RevertWow64FsRedirection"
00D3179A	push b14299fd4d1cbfb4cc7486d978398214.D465C0	"L\"kernel32.dll"
00D317DE	push b14299fd4d1cbfb4cc7486d978398214.D46670	"L\"SYSTEM\\CurrentControlSet\\Control\\Session Manager\\"
00D3180C	push b14299fd4d1cbfb4cc7486d978398214.D46640	"L\"PROCESSOR_ARCHITECTURE"
00D31862	push b14299fd4d1cbfb4cc7486d978398214.D46634	"L\"AMD64"
00D31877	push b14299fd4d1cbfb4cc7486d978398214.D46628	"L\"amd64"
00D31AD2	mov ebx, b14299fd4d1cbfb4cc7486d978398214.D465C0	"L\".exe"
00D31AD0	mov edi, b14299fd4d1cbfb4cc7486d978398214.D4C368	"L\"\\system32\\\\"
00D31AFE	lea edx, dword ptr ds:[eax+D4C000]	"L\"cac1srv"
00D31C4F	mov esi, b14299fd4d1cbfb4cc7486d978398214.D46744	"L\"trksvr.exe"
00D31C8F	mov edi, b14299fd4d1cbfb4cc7486d978398214.D4C368	"L\"\\system32\\\\"
00D31D65	mov esi, b14299fd4d1cbfb4cc7486d978398214.D4675C	"L\"trksrv.exe"
00D31DA5	mov edi, b14299fd4d1cbfb4cc7486d978398214.D4C368	"L\"\\system32\\\\"
00D31E7A	mov esi, b14299fd4d1cbfb4cc7486d978398214.D46774	"L\"netinit"
00D31E92	mov edi, b14299fd4d1cbfb4cc7486d978398214.D465C0	"L\"\\system32\\\\"
00D31EE2	mov edi, b14299fd4d1cbfb4cc7486d978398214.D46784	"L\"\\system32\\kernel32.dll"
00D31FAF	push b14299fd4d1cbfb4cc7486d978398214.D4672C	"L\"invalid string position"
00D3235E	push b14299fd4d1cbfb4cc7486d978398214.D4671C	"L\"string too long"
00D323CB	push b14299fd4d1cbfb4cc7486d978398214.D4672C	"L\"invalid string position"
00D32501	push b14299fd4d1cbfb4cc7486d978398214.D4671C	"L\"string too long"
00D325D5	push b14299fd4d1cbfb4cc7486d978398214.D4672C	"L\"invalid string position"
00D32620	push b14299fd4d1cbfb4cc7486d978398214.D4672C	"L\"invalid string position"
00D32636	push b14299fd4d1cbfb4cc7486d978398214.D4671C	"L\"string too long"
00D3274D	push b14299fd4d1cbfb4cc7486d978398214.D467E0	"L\"Jobadd"
00D327B5	mov esi, b14299fd4d1cbfb4cc7486d978398214.D467D4	"L\"Schedule"
00D3279F	mov esi, b14299fd4d1cbfb4cc7486d978398214.D467D0	"L\"Net"
00D327C3	push b14299fd4d1cbfb4cc7486d978398214.D467B4	"L\"netapi32.dll"
00D32C0E	mov esi, b14299fd4d1cbfb4cc7486d978398214.D468CC	"L\"ADMIN\$"
00D32C2D	mov esi, b14299fd4d1cbfb4cc7486d978398214.D46884	"L\"C:\\WINDOWS"
00D32C46	mov esi, b14299fd4d1cbfb4cc7486d978398214.D4689C	"L\"D:\\WINDOWS"
00D32C5C	mov esi, b14299fd4d1cbfb4cc7486d978398214.D46884	"L\"E\$\\WINDOWS"

The above screenshot and the highlighted row shows one of the most important strings in this binary. The executable highlighted is central to the workings of this malware which are discussed at the end of this report.

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads

Address	Disassembly	Comment
00D31C45	C9	leave
00D31C46	C3	ret
00D31C47	55	push ebp
00D31C48	8BEC	mov ebp, esp
00D31C4A	51	push ecx
00D31C4B	51	push ecx
00D31C4C	53	push ebx
00D31C4D	56	push esi
00D31C4E	57	push edi
00D31C4F	BE 4467D400	mov esi, b14299fd4d1cbfb4cc7486d978398214.D46744
00D31C54	56	push esi
00D31C55	C645 FF 01	mov byte ptr ss:[ebp-1], 1
00D31C59	E8 51F4FFFF	call b14299fd4d1cbfb4cc7486d978398214.D4675C
00D31C5E	8B7D 08	mov edi, dword ptr ss:[ebp+8]
00D31C61	03C0	add eax, eax
00D31C63	50	push eax
00D31C64	56	push esi
00D31C65	57	push edi
00D31C66	E8 5F3FFFFF	call b14299fd4d1cbfb4cc7486d978398214.D46774
00D31C68	56	push esi
00D31C6C	E8 3EF4FFFF	call b14299fd4d1cbfb4cc7486d978398214.D46784
00D31C71	33C9	xor ecx, ecx
00D31C73	BE 80DD400	mov esi, b14299fd4d1cbfb4cc7486d978398214.D467D0
00D31C78	56	push esi
00D31C79	66: 890C47	mov word ptr ds:[edi+eax*2], cx
00D31C7D	E8 20F4FFFF	call b14299fd4d1cbfb4cc7486d978398214.D467D4
00D31C82	8B5D 0C	mov ebx, dword ptr ss:[ebp+C]
00D31C85	03C0	add eax, eax
00D31C87	50	push eax
00D31C88	56	push esi
00D31C89	53	push ebx
00D31C8A	E8 C1F3FFFF	call b14299fd4d1cbfb4cc7486d978398214.D467E0
00D31C8F	BF 68C3D400	mov edi, b14299fd4d1cbfb4cc7486d978398214.D467E0
00D31C9A	83C4 28	add esp, 28
00D31C9D	03C0	add eax, eax
00D31C9F	50	push eax
00D31CA0	57	push edi
00D31CA1	56	push esi
00D31CA2	E8 08F4FFFF	call b14299fd4d1cbfb4cc7486d978398214.D467E0
00D31CA7	59	pop ecx
00D31CA8	8D0443	lea eax, dword ptr ds:[ebx+eax*2]
00D31CAB	50	push eax
00D31CAC	E8 9FF3FFFF	call b14299fd4d1cbfb4cc7486d978398214.D467E0
00D31CB1	F75 08	push dword ptr ss:[ebp+8]
00D31CB4	E8 F6F3FFFF	call b14299fd4d1cbfb4cc7486d978398214.D467E0
00D31CB9	83C4 10	add esp, 10

The above screenshot shows the code fragment highlighting said executable and also shows that there is process initialization soon after.

FINDINGS

My analysis above and further research into this malware indicates that this binary attempts to spread to other machines via the network and wipes files on the infected machine which include hardcoded directories as well as other files. This malware destroys the data which essentially renders the machine inoperable. Overall, I was able to find hardcoded domains and strings that closely resembled passwords and hardcoded directories as well as command execution instructions.

There are a lot of variants of this malware and the common thing amongst them all is that they create a service called "NtsSrv" or some variation of that name, which is the original installation of the malware. There are scheduled tasks run by this malware which drop a payload of a wiper component that deletes all system files rendering it inoperable. The "PKCS7", "PKCS12", and "x509" are all embedded resources in the malware that mask the actual binary and behave like a logic bomb used to install and spread the malware while also corrupting the master boot record of the machines.

There are a couple different methods to prevent this malware from causing any harm and some of them include:

- Make sure that all machines are up-to-date and are thoroughly patched.
- Use LAPS (Local Administrator Password Solution) since it heavily restricts lateral movement of the malware.
- Disable Remote Registry service on all machines in the network since that would prevent this malware from being able to install as it relies on this system to disable UAC (User Account Control).

I was able to obtain this malware from the following GitHub repo:

<https://github.com/ytisf/theZoo>

<https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Shamoon>