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

Shamoon Malware Analysis

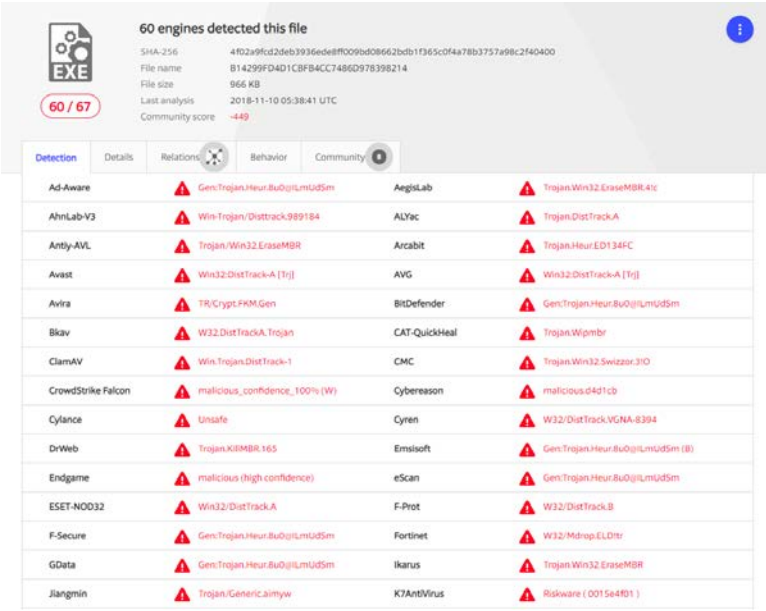
For the purpose of this project, I decided to analyze the “Shamoon” malware which was used to target national oil companies in Saudi Arabia. Essentially, this virus can spread to other machines on a network and it more or less erases all files from a machine, and overwrites the master boot record rendering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

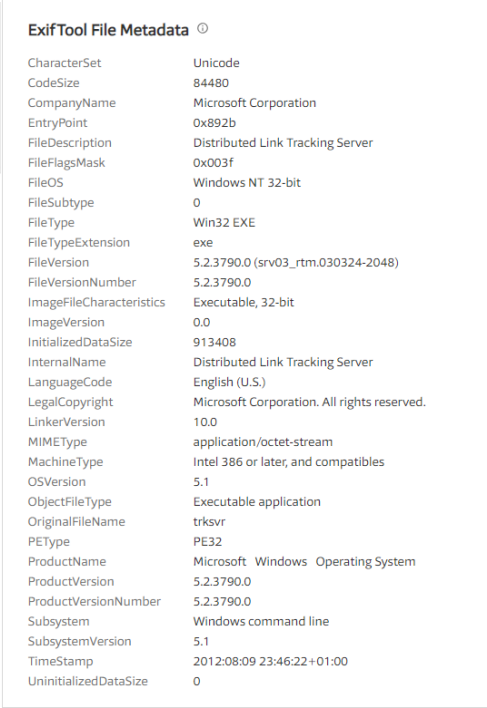
I performed the various levels of analysis covered in this class including basic static, basic dynamic, advanced static, and advanced dynamic. All of the various analyses highlighted important things in the malware which are discussed throughout the report and a summary is provided at the end of the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





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 8

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

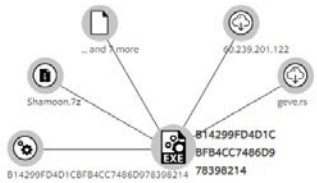
Creation Time	2012-08-09 22:46:22
First Seen In The Wild	2008-04-14 04:00:00
First Submission	2012-08-15 13:21:36
Last Submission	2018-11-10 05:38:41
Last Analysis	2018-11-10 05:38:41

File Names

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

Detection | Details | Relations | Behavior | Community 8

Graph Summary



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%\windowsshell.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 strerror.
- 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

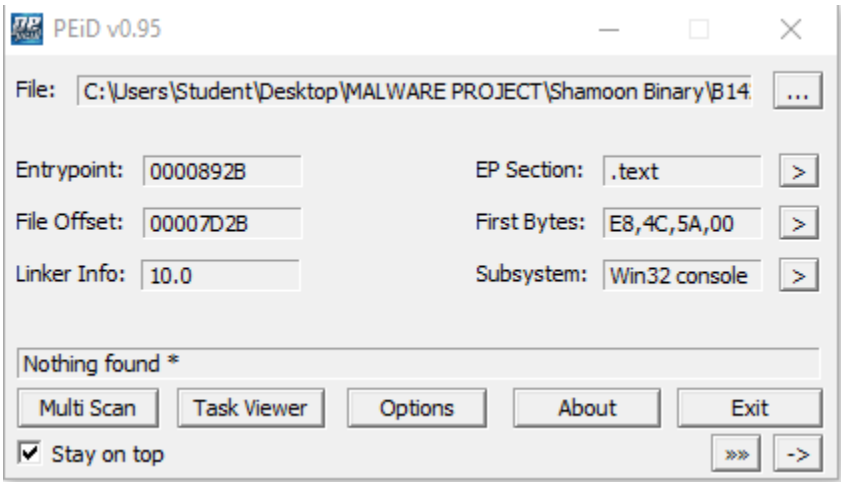
Just out of curiosity, I also ran FLOSS to see if there will be any additional interesting strings and also to see if there are any strings that can be decoded. As can be seen below, the highlighted strings are really important which are discussed later in the report.

```
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.

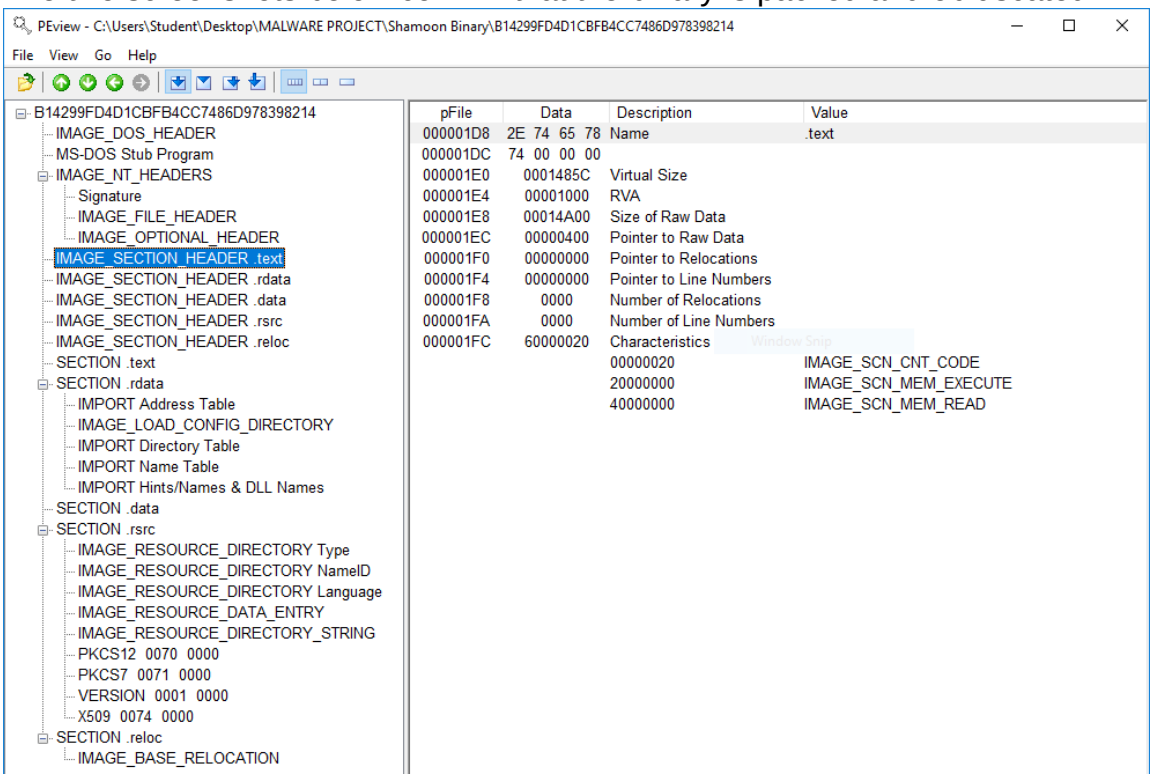
PEiD

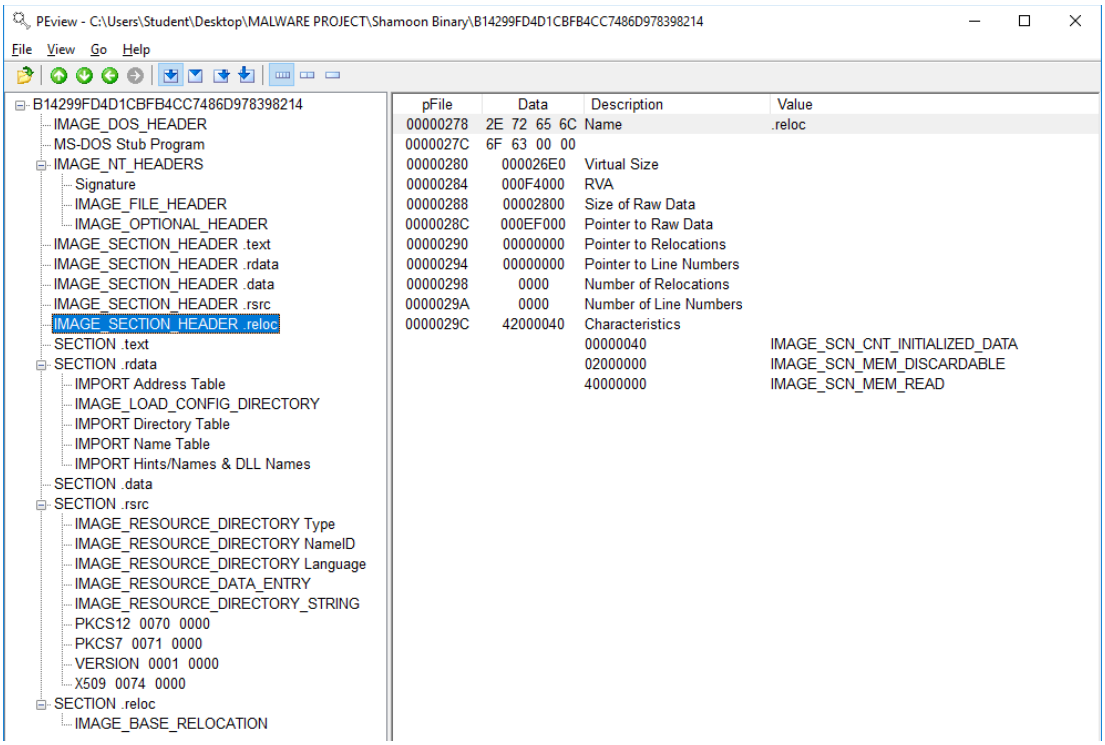
As can be seen below, the binary is indeed packed and obfuscated.



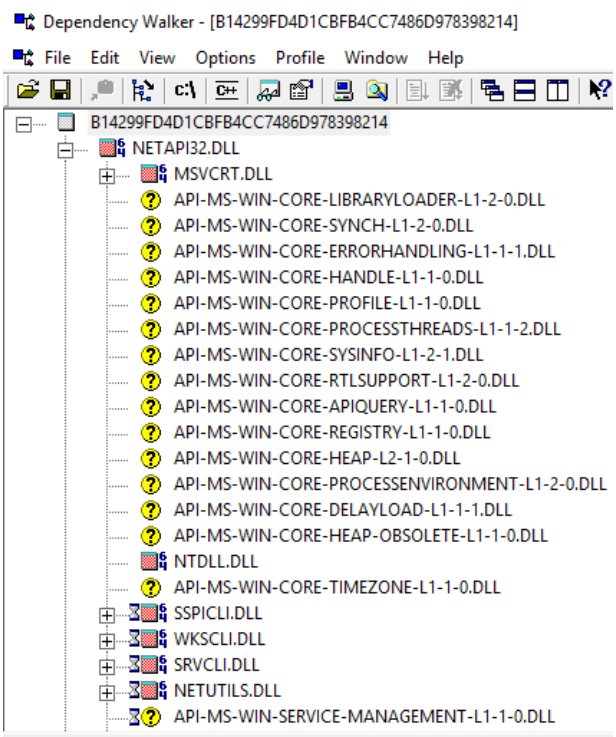
PEview

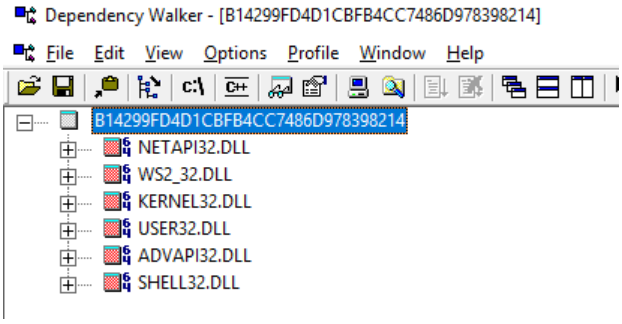
The two screenshots below confirm that the binary is packed and obfuscated.





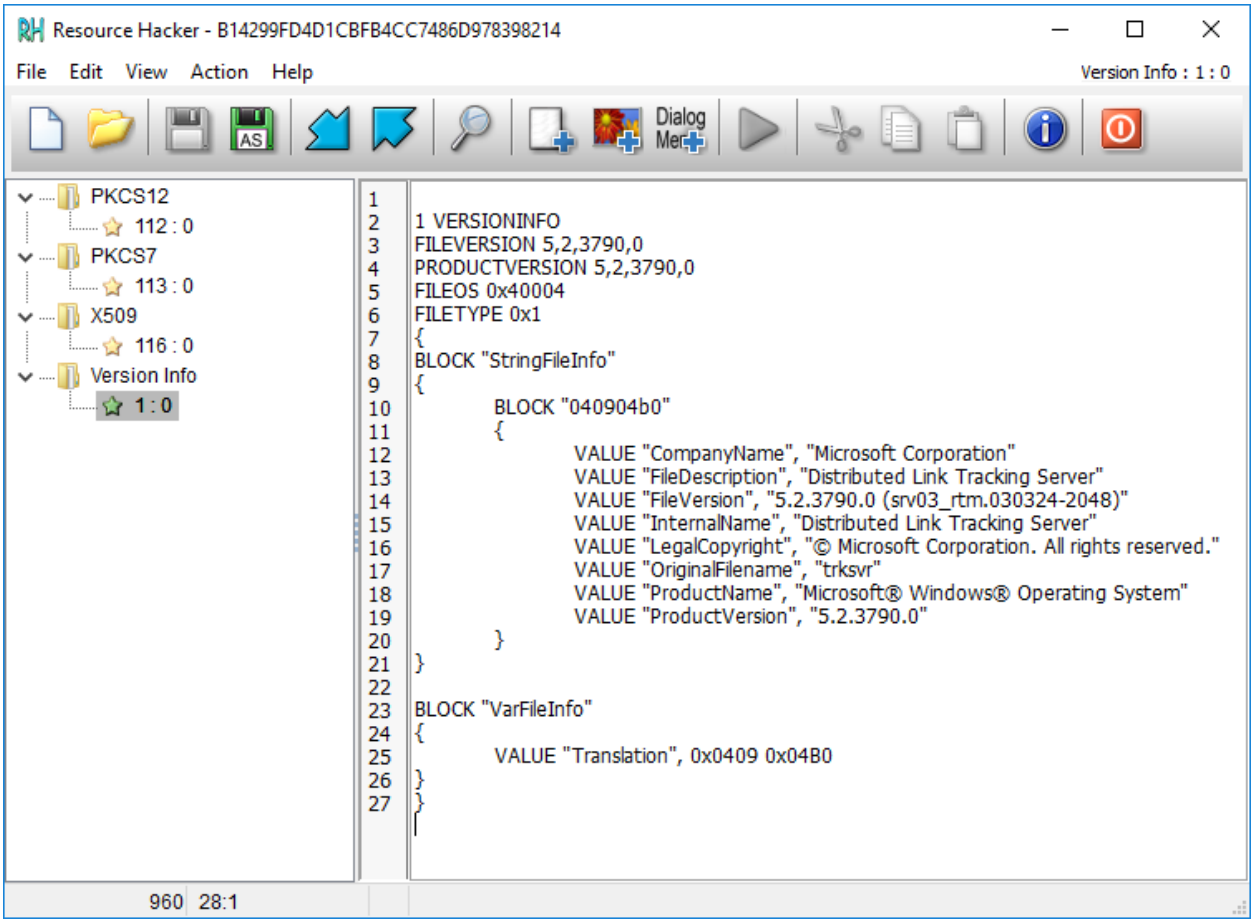
Dependency Walker:





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

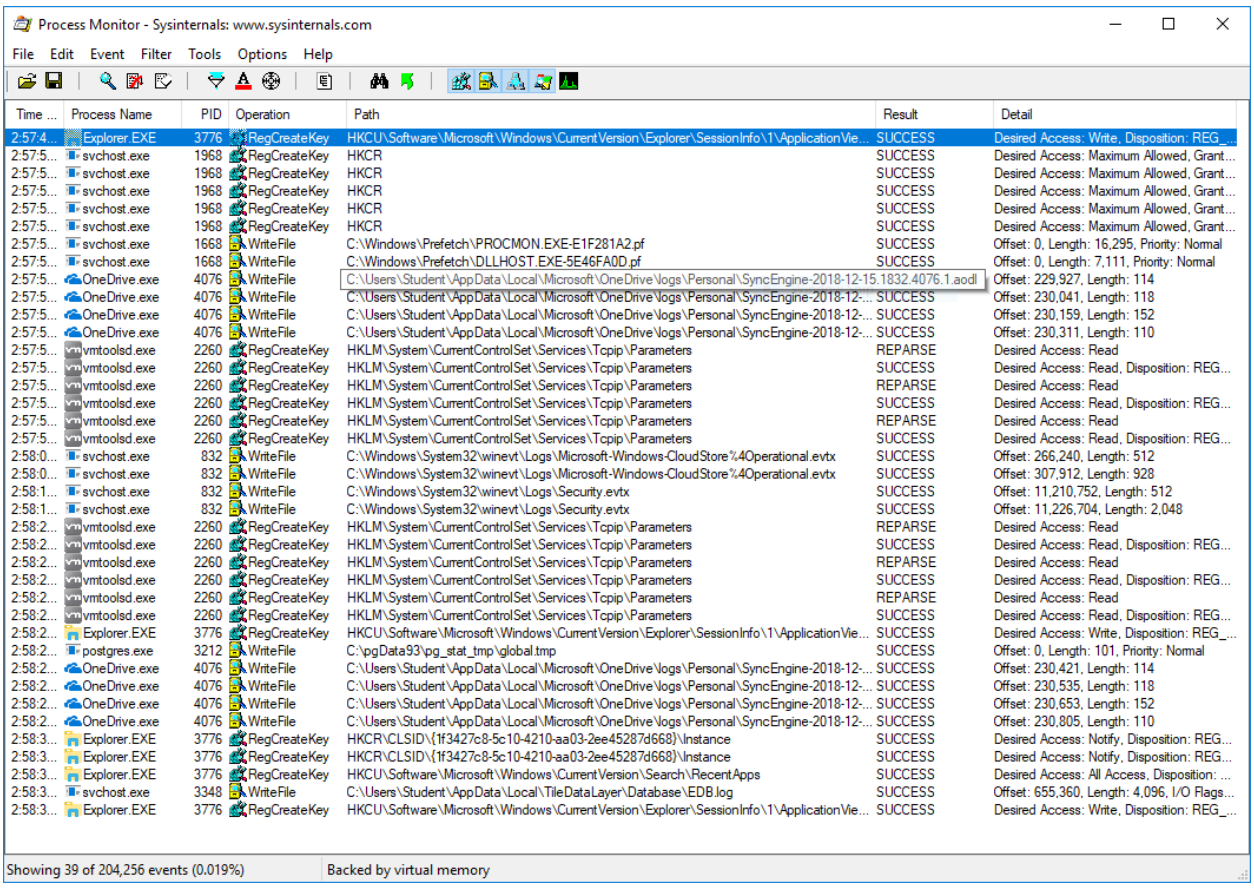


As can be seen above, there is a lot of info about the actual binary such as the file name and the original file name which shows that it was renamed to mask its true identity. We can also see internal file name and its description.

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		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%4Operational.evtx	SUCCESS	Offset: 266,240, Length: 512
2:58:0...	svchost.exe	832	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-CloudStore%4Operational.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

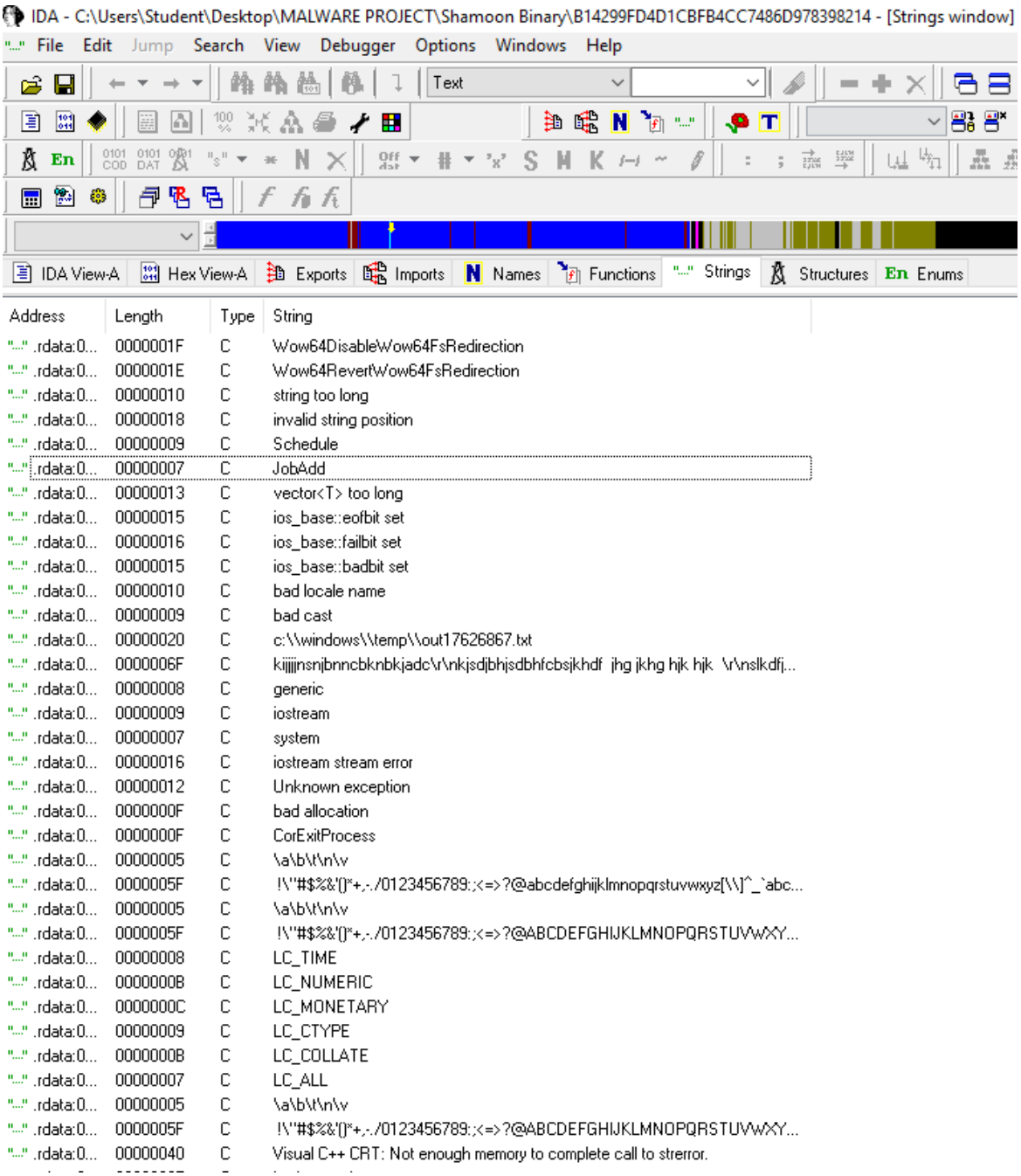
```
OllyDbg - B14299FD4D1CBFB4CC7486D978398214 - [CPU - main thread, module B14299FD4D1CBFB4CC7486D97839821]
C File View Debug Trace Plugins Options Windows Help

00D388E6  >  E8 7AFEFFFF   CALL 00D38765
00D388EB  .v EB 2E         JMP SHORT 00D3891B
00D388ED  .  8B45 EC       MOV EAX,DWORD PTR SS:[EBP-14]
00D388F0  .  8B08          MOV ECX,DWORD PTR DS:[EAX]
00D388F2  .  8B09          MOV ECX,DWORD PTR DS:[ECX]
00D388F4  .  894D DC       MOV DWORD PTR SS:[EBP-24],ECX
00D388F7  .  50            PUSH EAX
00D388F8  .  51            PUSH ECX
00D388F9  .  E8 FC550000   CALL 00D3DEFA
00D388FE  .  59            POP ECX
00D388FF  .  59            POP ECX
00D38900  .  C3            RETN
00D38901  .  8B65 E8       MOV ESP,DWORD PTR SS:[EBP-18]
00D38904  .  8B45 DC       MOV EAX,DWORD PTR SS:[EBP-24]
00D38907  .  8945 E0       MOV DWORD PTR SS:[EBP-20],EAX
00D3890A  .  837D E4 00    CMP DWORD PTR SS:[EBP-1C],0
00D3890E  .v 75 06         JNE SHORT 00D38916
00D38910  .  50            PUSH EAX
00D38911  .  E8 39FEFFFF   CALL 00D3874F
00D38916  >  E8 59FEFFFF   CALL 00D38774
00D3891B  >  C745 FC FEFF  MOV DWORD PTR SS:[EBP-4],-2
00D38922  .  8B45 E0       MOV EAX,DWORD PTR SS:[EBP-20]
00D38925  .  E8 DB380000   CALL 00D3C205
00D3892A  .  C3            RETN
00D3892B  .  E8 4C5A0000   CALL 00D3E37C
00D38930  .^ E9 95FEFFFF   JMP 00D387CA
00D38935  $  8BFF          MOV EDI,EDI
00D38937  .  55            PUSH EBP
00D38938  .  8BEC          MOV EBP,ESP
00D3893A  .  8B45 08       MOV EAX,DWORD PTR SS:[EBP+8]
00D3893D  .  85C0          TEST EAX,EAX
00D3893F  .v 74 12         JZ SHORT 00D38953
00D38941  .  83E8 08       SUB EAX,8
00D38944  .  8138 DDDD000  CMP DWORD PTR DS:[EAX],0DDDD
00D3894A  .v 75 07         JNE SHORT 00D38953
00D3894C  .  50            PUSH EAX                          Arg1
00D3894D  .  E8 7AEEFFFF   CALL 00D377CC                     B14299FD4D1CBFB4CC7486D97839821.00D377CC
00D38952  .  59            POP ECX
00D38953  >  5D            POP EBP
00D38954  .  C3            RETN
00D38955  $  8BFF          MOV EDI,EDI                       B14299FD4D1CBFB4CC7486D97839821.00D38955(guessed Arg1)
00D38957  .  55            PUSH EBP
00D38958  .  8BEC          MOV EBP,ESP
00D3895A  .  8B45 08       MOV EAX,DWORD PTR SS:[EBP+8]
00D3895D  .  56            PUSH ESI
00D3895E  .  8BF1          MOV ESI,ECX
00D38960  .  C646 0C 00    MOV BYTE PTR DS:[ESI+0C],0
00D38964  .  85C0          TEST EAX,EAX
00D38966  .v 75 63         JNZ SHORT 00D389CB
00D38968  .  E8 752C0000   CALL 00D3B5E2                     B14299FD4D1CBFB4CC7486D97839821.00D3B5E2
00D3896D  .  8946 08       MOV DWORD PTR DS:[ESI+8],EAX
00D38970  .  8B48 6C       MOV ECX,DWORD PTR DS:[EAX+6C]
00D38973  .  890E          MOV DWORD PTR DS:[ESI],ECX
00D38975  .  8B48 68       MOV ECX,DWORD PTR DS:[EAX+68]
00D38978  .  894E 04       MOV DWORD PTR DS:[ESI+4],ECX
00D3897B  .  8B0E          MOV ECX,DWORD PTR DS:[ESI]
00D3897D  .  3B0D 40DBD40  CMP ECX,DWORD PTR DS:[0D4DB40]
00D38983  .v 74 12         JE SHORT 00D38997

ECX=00D3892B (B14299FD4D1CBFB4CC7486D97839821.<ModuleEntryPoint>) (current registers)
Stack [0133FB98]=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
.rdata:0...	0000001F	C	Wow64DisableWow64FsRedirection
.rdata:0...	0000001E	C	Wow64RevertWow64FsRedirection
.rdata:0...	00000010	C	string too long
.rdata:0...	00000018	C	invalid string position
.rdata:0...	00000009	C	Schedule
.rdata:0...	00000007	C	JobAdd
.rdata:0...	00000013	C	vector<T> too long
.rdata:0...	00000015	C	ios_base::eofbit set
.rdata:0...	00000016	C	ios_base::failbit set
.rdata:0...	00000015	C	ios_base::badbit set
.rdata:0...	00000010	C	bad locale name
.rdata:0...	00000009	C	bad cast
.rdata:0...	00000020	C	c:\\windows\\temp\\out17626867.txt
.rdata:0...	0000006F	C	kijjjjnsnjbnncbknbkjadc\r\nkjsdjbhjsdbhfcbsjkhdf jhg jkhg hjk hjk \r\nslkdfj...
.rdata:0...	00000008	C	generic
.rdata:0...	00000009	C	iostream
.rdata:0...	00000007	C	system
.rdata:0...	00000016	C	iostream stream error
.rdata:0...	00000012	C	Unknown exception
.rdata:0...	0000000F	C	bad allocation
.rdata:0...	0000000F	C	CorExitProcess
.rdata:0...	00000005	C	\a\b\t\n\v
.rdata:0...	0000005F	C	!\"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\\]^_`abc...
.rdata:0...	00000005	C	\a\b\t\n\v
.rdata:0...	0000005F	C	!\"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXY...
.rdata:0...	00000008	C	LC_TIME
.rdata:0...	0000000B	C	LC_NUMERIC
.rdata:0...	0000000C	C	LC_MONETARY
.rdata:0...	00000009	C	LC_CTYPE
.rdata:0...	0000000B	C	LC_COLLATE
.rdata:0...	00000007	C	LC_ALL
.rdata:0...	00000005	C	\a\b\t\n\v
.rdata:0...	0000005F	C	!\"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXY...
.rdata:0...	00000040	C	Visual C++ CRT: Not enough memory to complete call to strerror.

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.

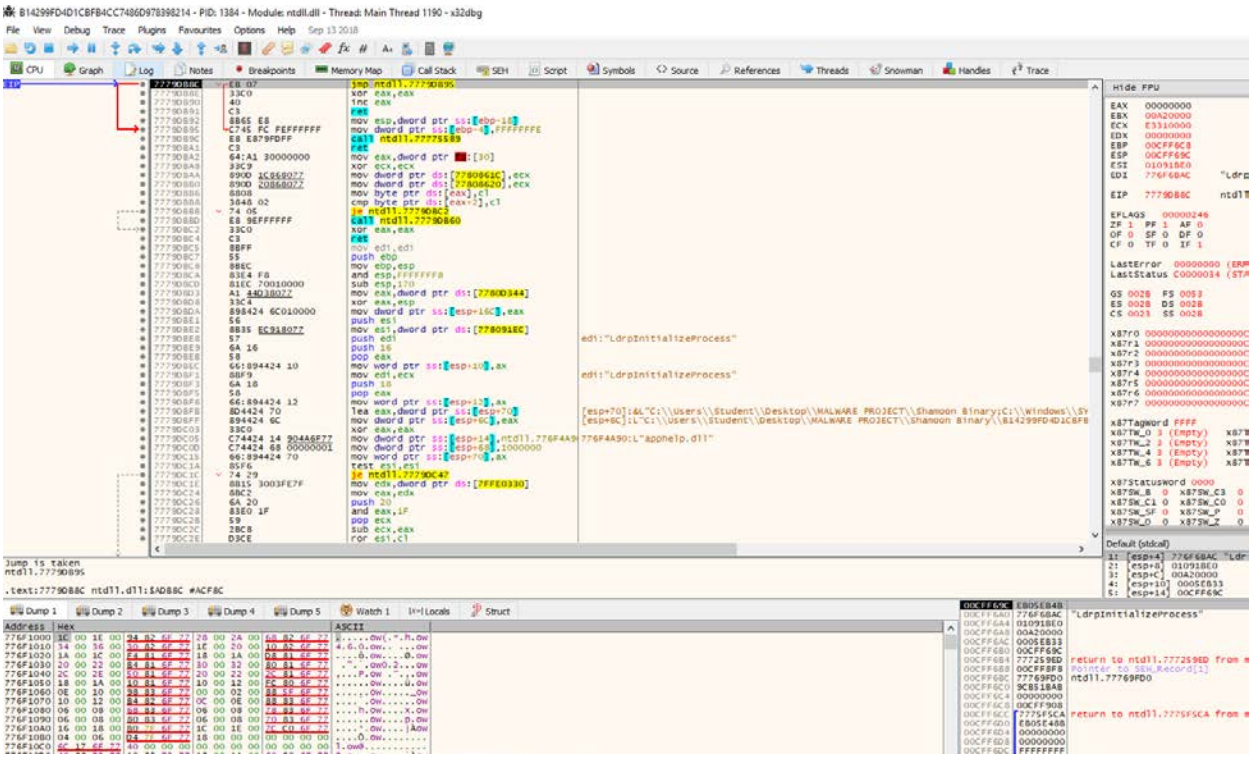
```
IDA View-A | Hex View-A | Exports | Imports | Names | Functions | Strings | Structures | Enums

.text:00408955 sub_408955      proc near               ; CODE XREF: sub_408BC3+E↓p
.text:00408955                                         ; sub_408C32+E↓p ...
.text:00408955
.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_40B5E2
.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_40EDBB
.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.

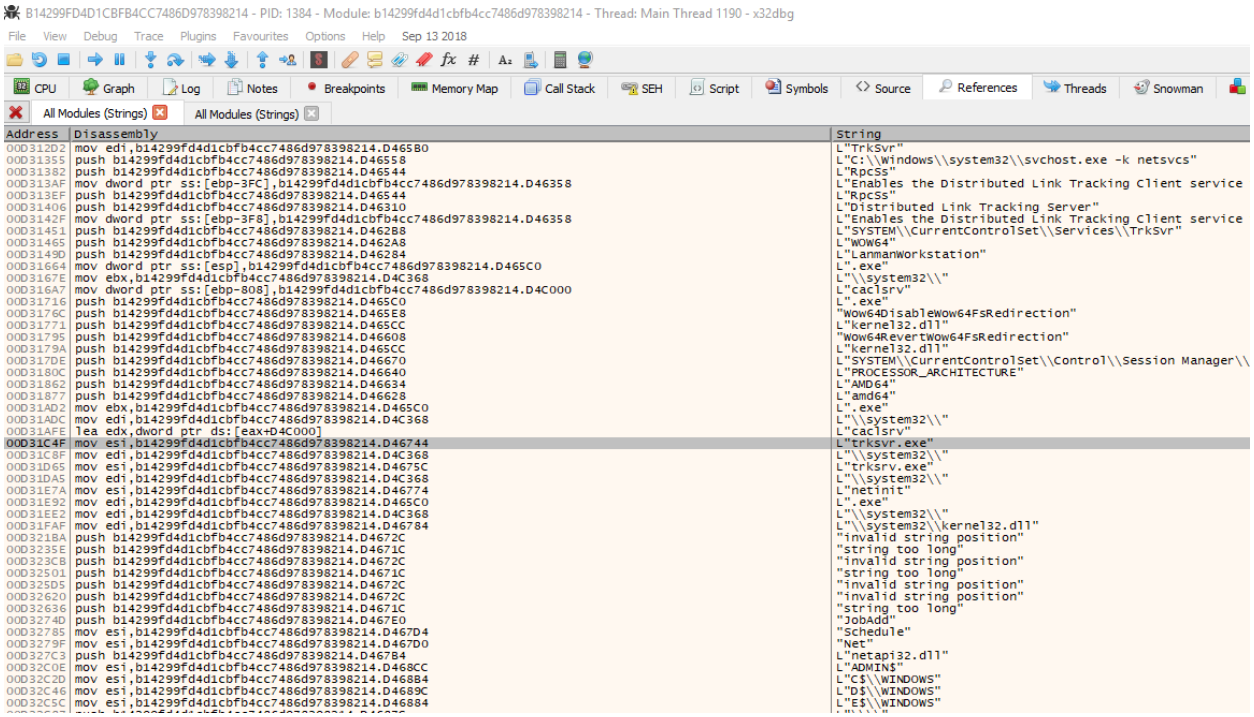
ADVANCED DYNAMIC

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

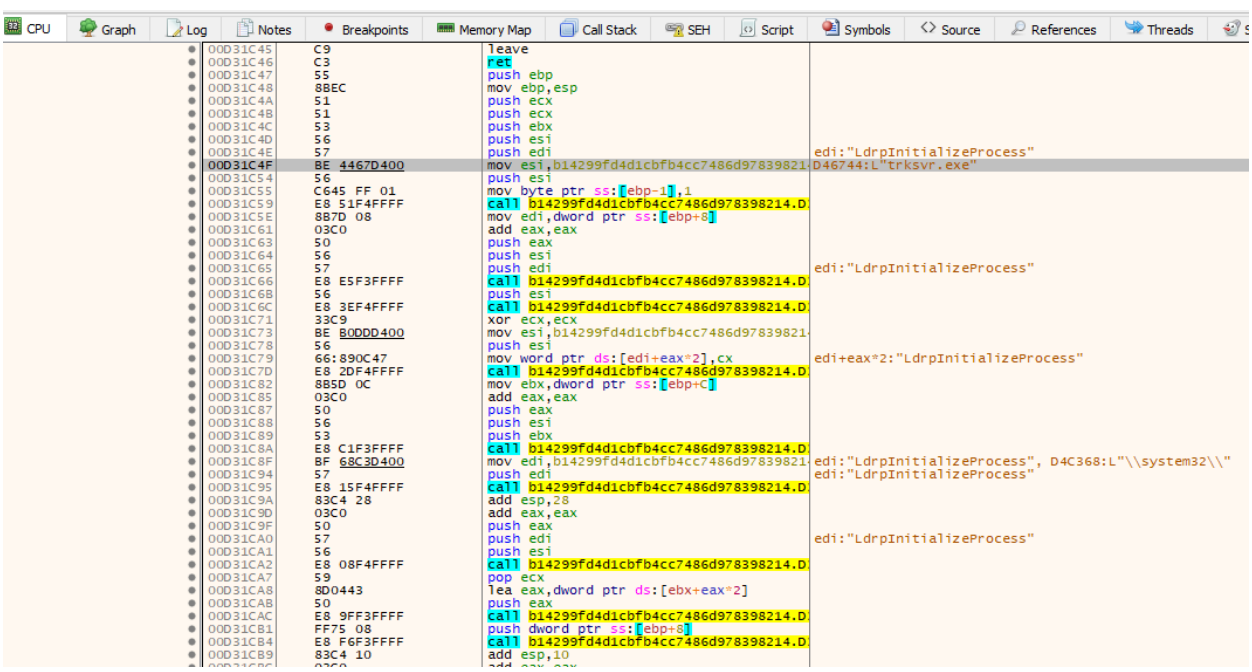
X64dbg



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



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.



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