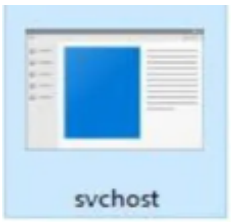
Name: Nguyễn Lê Đình Vũ

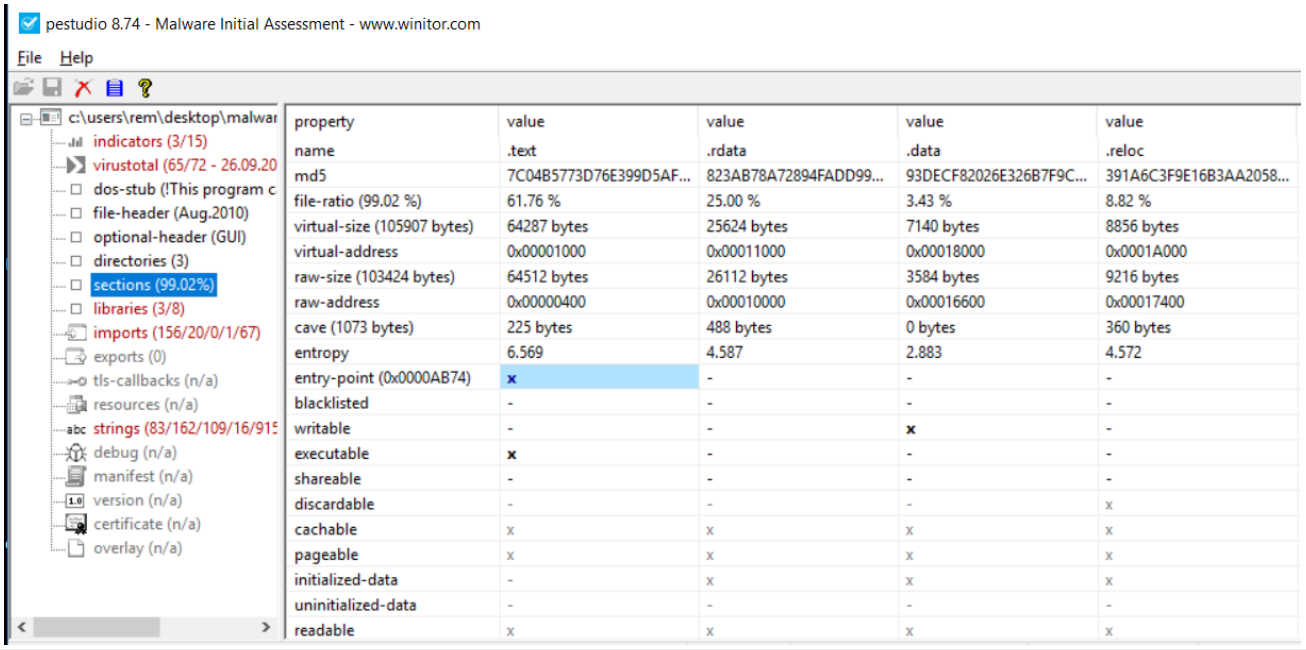
ID: BI11-291

Report for labwork svchost.exe

Date:	**23/10/2022**
Workstation:	**REM Vmware**
File Name:	**svchost.exe**
File Location:	**C:\Users\REM\Desktop\Malware\Day2\svchost.exe**
File Timestamps:	**Sat Aug 21 10:36:59 2010**
Notification Vector:	

File Size (bytes):	**104448 bytes**
Icon Graphic:	
Signed?:	
File Hash:	**Svchost.exe** **md5: C63A537090D34F29DAADBEF221637435** **sha1:BA17638BAC43E6E3B2FAF4BF3A22197B99D8A390** **sha256:28046C14EA3325885EE1E731CD0BCF9F38445DF02675836B851CB2AE94C050EB**
Imp Hash:	**31553623C43827D554AD9E1B7DFA6A5A**
PE Section Hashes:	

We can see by click on ‘sections” part



property	value	value	value	value
name	.text	.rdata	.data	.reloc
md5	7C04B5773D76E399D5AF...	823AB78A72894FADD99...	93DECF82026E326B7F9C...	391A6C3F9E16B3AA2058...
file-ratio (99.02 %)	61.76 %	25.00 %	3.43 %	8.82 %
virtual-size (105907 bytes)	64287 bytes	25624 bytes	7140 bytes	8856 bytes
virtual-address	0x00001000	0x00011000	0x00018000	0x0001A000
raw-size (103424 bytes)	64512 bytes	26112 bytes	3584 bytes	9216 bytes
raw-address	0x00000400	0x00010000	0x00016600	0x00017400
cave (1073 bytes)	225 bytes	488 bytes	0 bytes	360 bytes
entropy	6.569	4.587	2.883	4.572
entry-point (0x0000AB74)	x	-	-	-
blacklisted	-	-	-	-
writable	-	-	x	-
executable	x	-	-	-
shareable	-	-	-	-
discardable	-	-	-	x
cachable	x	x	x	x
pageable	x	x	x	x
initialized-data	-	x	x	x
uninitialized-data	-	-	-	-
readable	x	x	x	x

Compile Time (pescanner, PEView)**:**

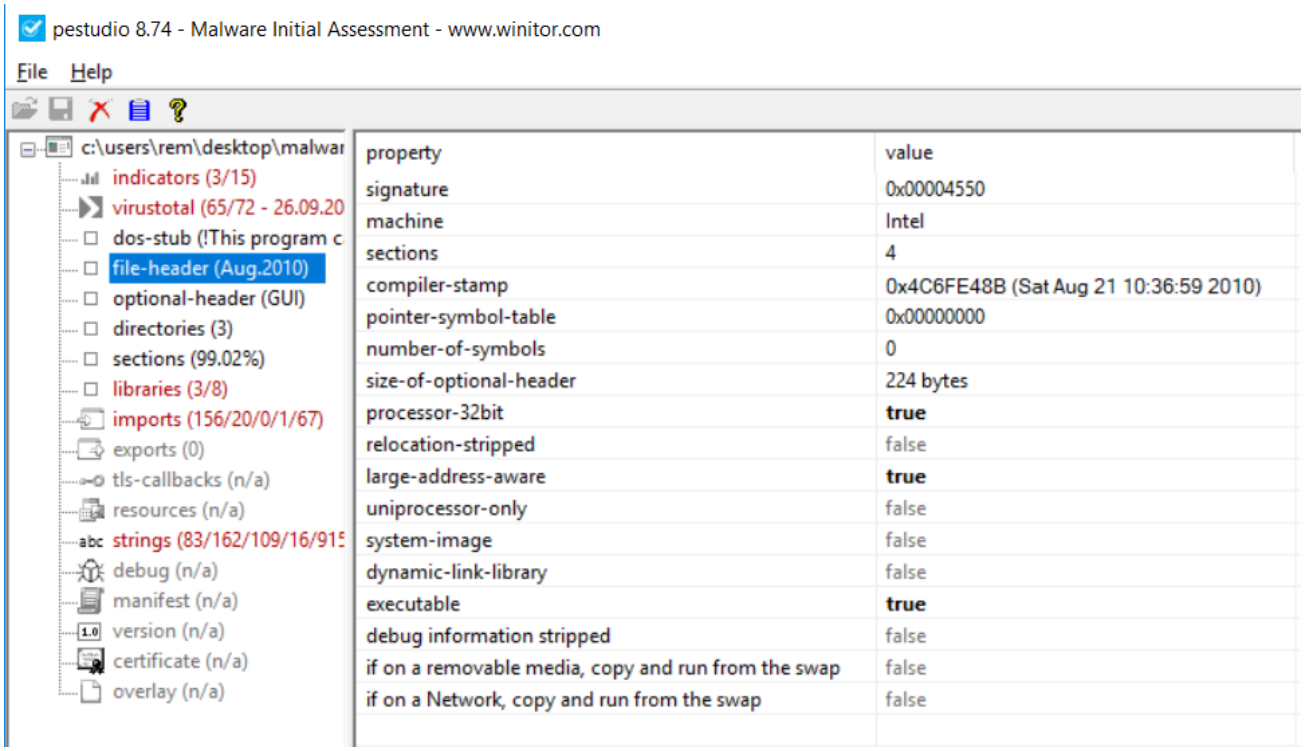
The compile time is Sat Aug 21 10:36:59 in the year 2010

subsystem	GUI
compiler-stamp	Sat Aug 21 10:36:59 2010
debugger-stamp	n/a

File Properties (PEStudio, PeView)**:** Description, version, file header characteristics

Version: Aug.2010

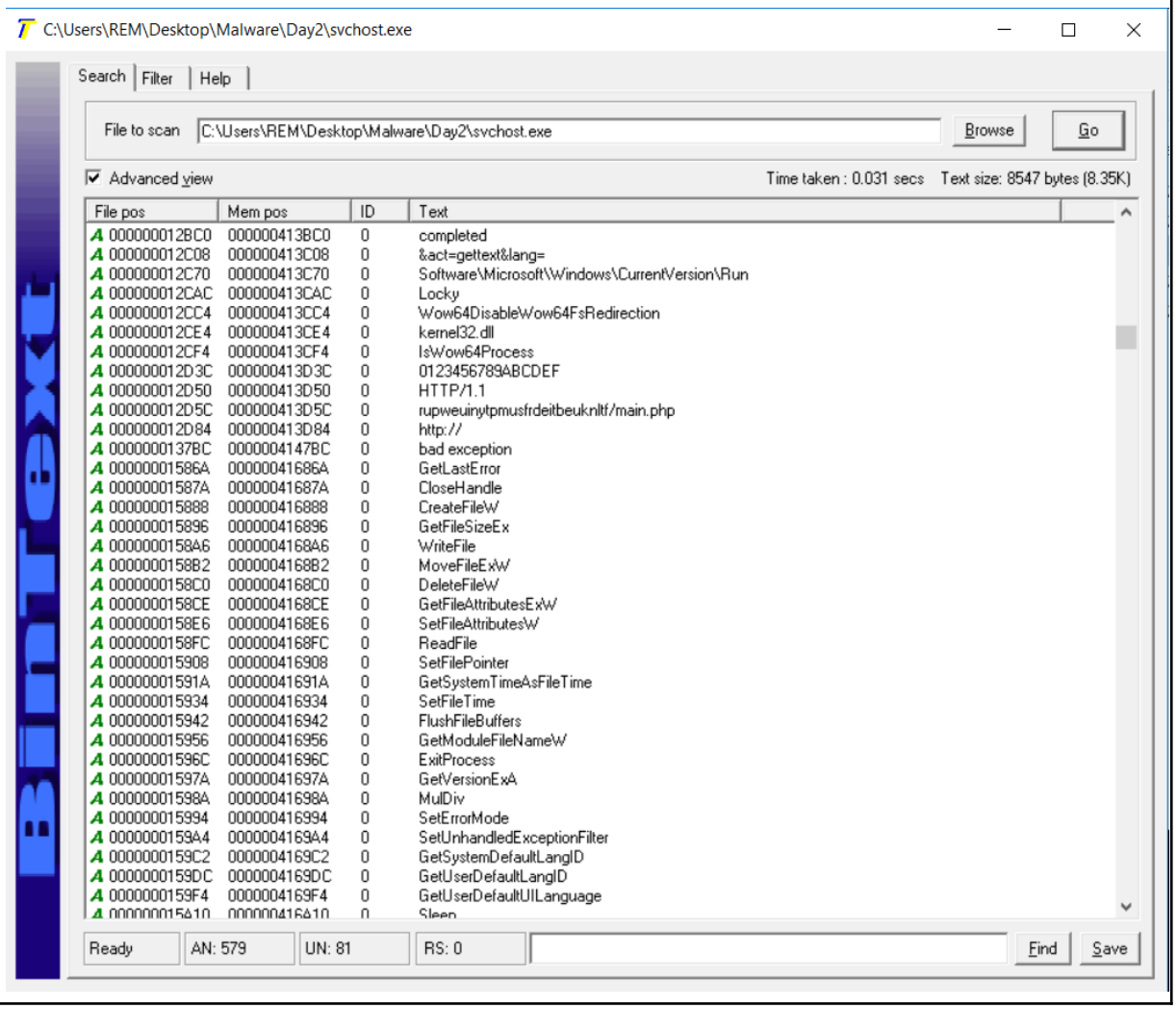
File header characteristics:

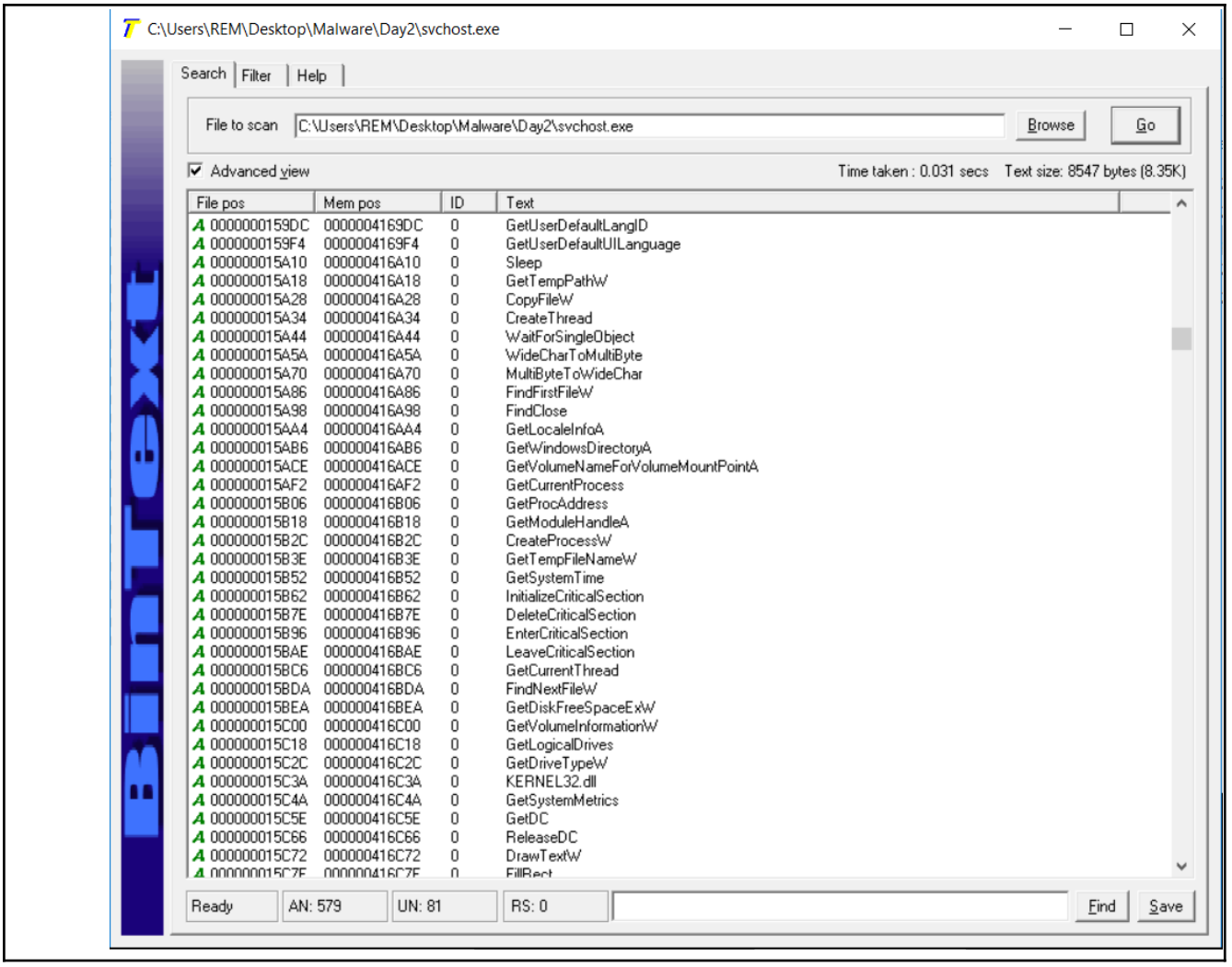


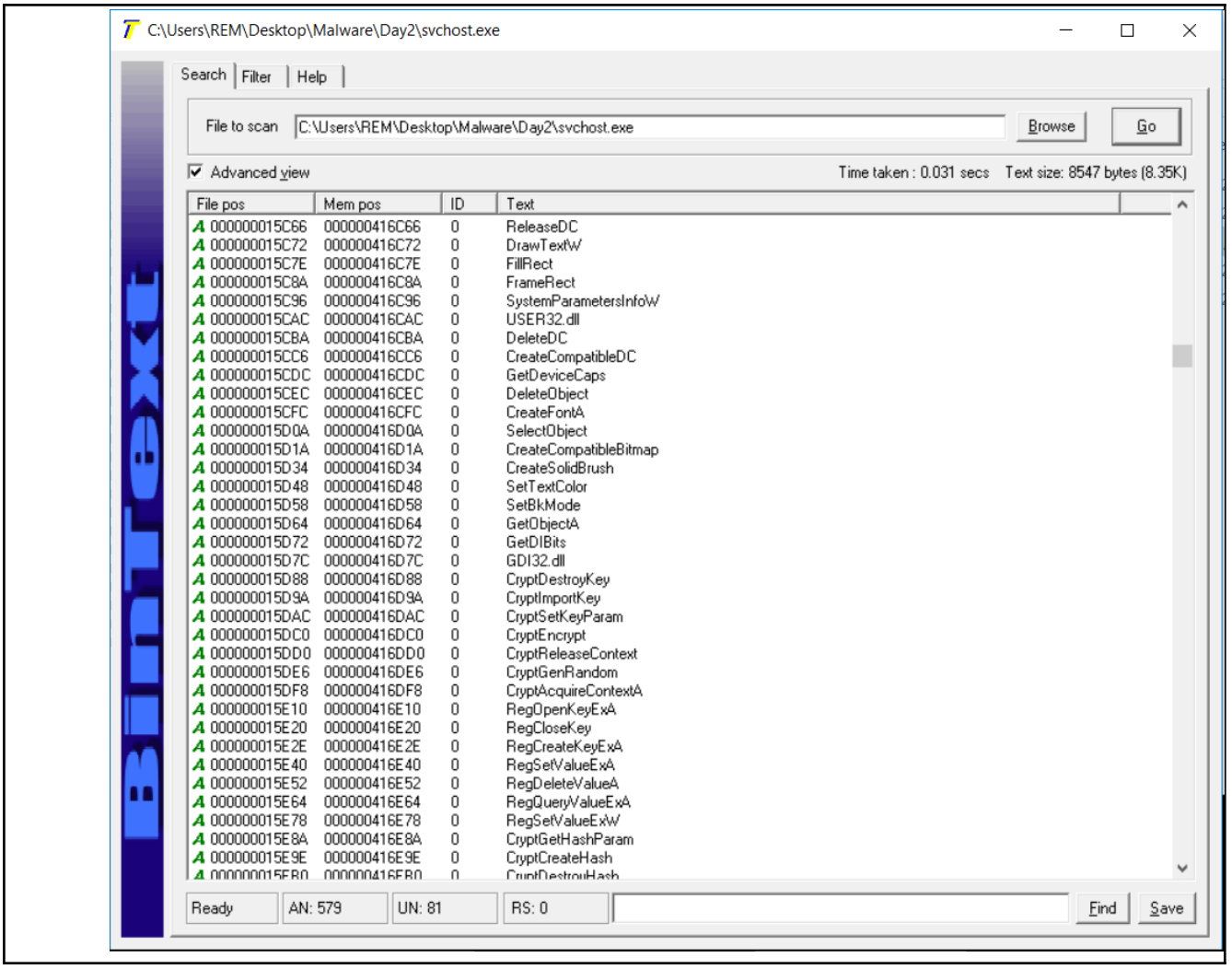
property	value
signature	0x00004550
machine	Intel
sections	4
compiler-stamp	0x4C6FE48B (Sat Aug 21 10:36:59 2010)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 bytes
processor-32bit	**true**
relocation-stripped	false
large-address-aware	**true**
uniprocessor-only	false
system-image	false
dynamic-link-library	false
executable	**true**
debug information stripped	false
if on a removable media, copy and run from the swap	false
if on a Network, copy and run from the swap	false

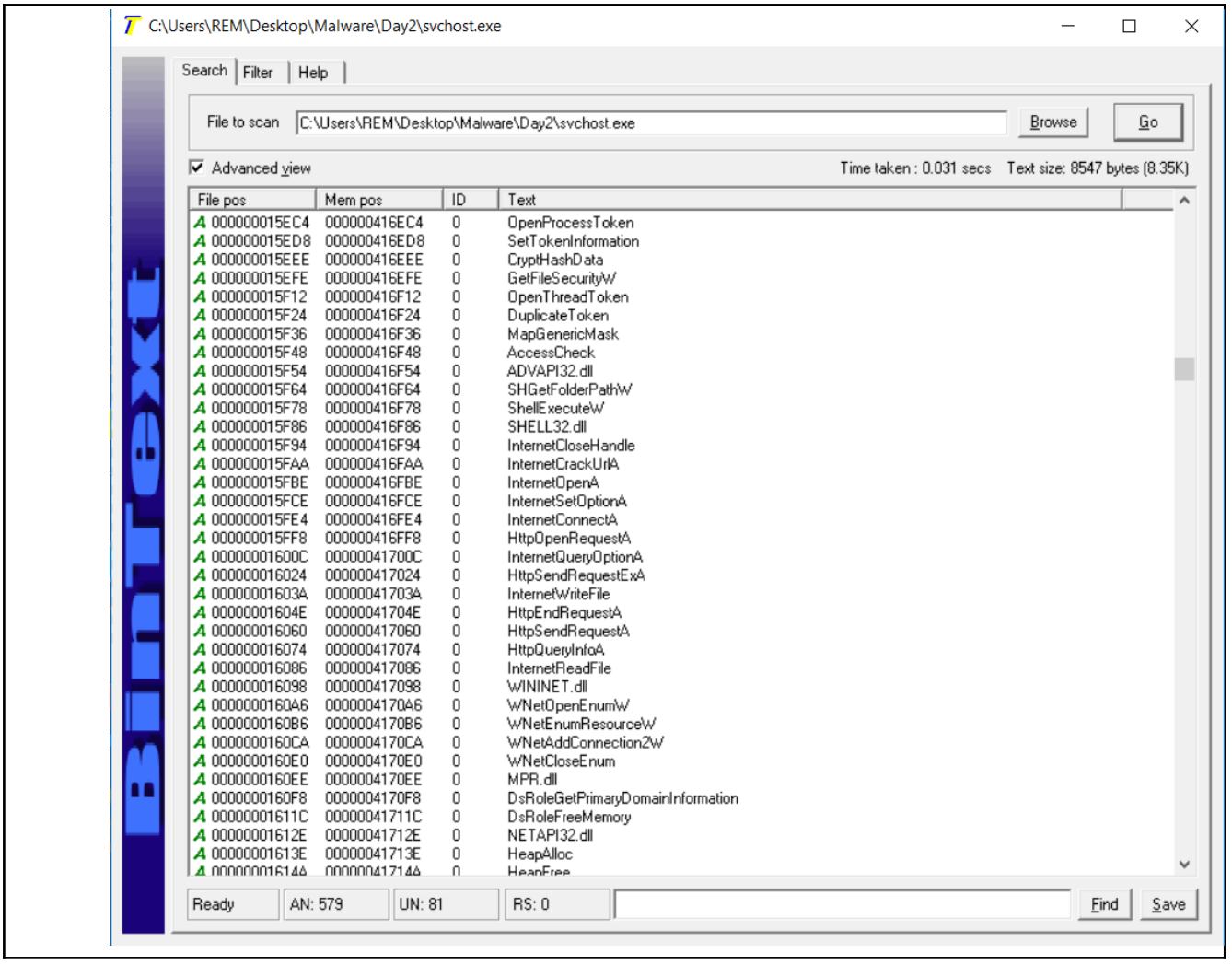
Strings (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs

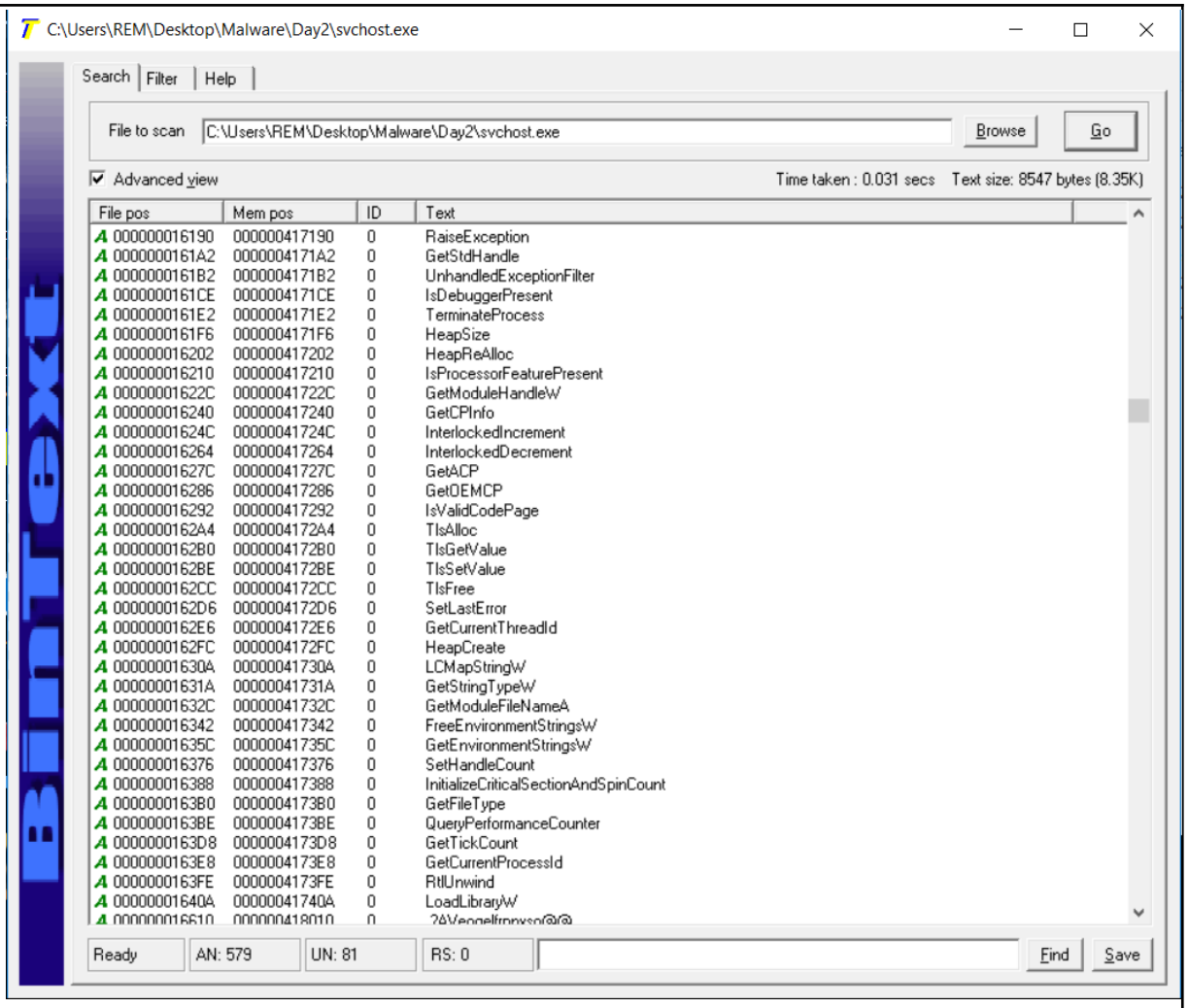
- **We can see some functions:**



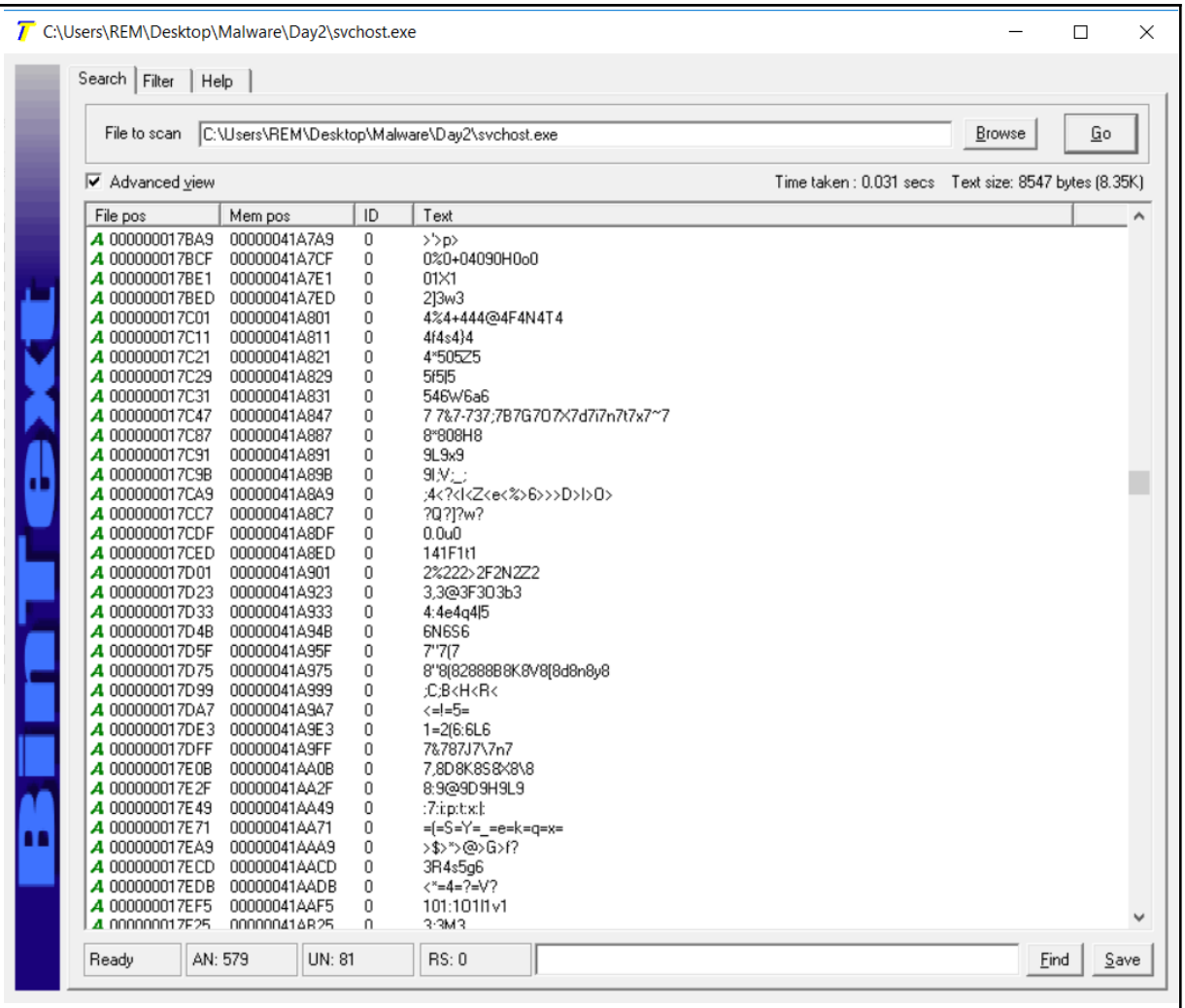

C:\Users\REM\Desktop\Malware\Day2\svchost.exe
Search
Filter
Help
File to scan
C:\Users\REM\Desktop\Malware\Day2\svchost.exe
Browse
Go
Advanced view
Time taken : 0.031 secs
Text size: 8547 bytes (8.35K)
File pos
Mem pos
ID
Text
A 0000000159DC 000000416 9DC 0 GetUserDefaultLangID
A 0000000159F4 000000416 9F4 0 GetUserDefaultUILanguage
A 000000015A10 000000416A10 0 Sleep
A 000000015A18 000000416A18 0 GetTempPathW
A 000000015A28 000000416A28 0 CopyFileW
A 000000015A34 000000416A34 0 CreateThread
A 000000015A44 000000416A44 0 WaitForSingleObject
A 000000015A5A 000000416A5A 0 WideCharToMultiByte
A 000000015A70 000000416A70 0 MultiByteToWideChar
A 000000015A86 000000416A86 0 FindFirstFileW
A 000000015A98 000000416A98 0 FindClose
A 000000015AA4 000000416AA4 0 GetLocaleInfoA
A 000000015AB6 000000416AB6 0 GetWindowsDirectoryA
A 000000015ACE 000000416ACE 0 GetVolumeNameForVolumeMountPointA
A 000000015AF2 000000416AF2 0 GetCurrentProcess
A 000000015B06 000000416B06 0 GetProcAddress
A 000000015B18 000000416B18 0 GetModuleHandleA
A 000000015B2C 000000416B2C 0 CreateProcessW
A 000000015B3E 000000416B3E 0 GetTempFileNameW
A 000000015B52 000000416B52 0 GetSystemTime
A 000000015B62 000000416B62 0 InitializeCriticalSection
A 000000015B7E 000000416B7E 0 DeleteCriticalSection
A 000000015B96 000000416B96 0 EnterCriticalSection
A 000000015BAE 000000416BAE 0 LeaveCriticalSection
A 000000015BC6 000000416BC6 0 GetCurrentThread
A 000000015BDA 000000416BDA 0 FindNextFileW
A 000000015BEA 000000416BEA 0 GetDiskFreeSpaceExW
A 000000015C00 000000416C00 0 GetVolumeInformationW
A 000000015C18 000000416C18 0 GetLogicalDrives
A 000000015C2C 000000416C2C 0 GetDriveTypeW
A 000000015C3A 000000416C3A 0 KERNEL32.dll
A 000000015C4A 000000416C4A 0 GetSystemMetrics
A 000000015C5E 000000416C5E 0 GetDC
A 000000015C66 000000416C66 0 ReleaseDC
A 000000015C72 000000416C72 0 DrawTextW
Ready
AN: 579
UN: 81
RS: 0
Find
Save


C:\Users\REM\Desktop\Malware\Day2\svchost.exe
Search
Filter
Help
File to scan
C:\Users\REM\Desktop\Malware\Day2\svchost.exe
Browse
Go
Advanced view
Time taken : 0.031 secs
Text size: 8547 bytes (8.35K)
File pos
Mem pos
ID
Text
000000015C66 000000416C66 0 ReleaseDC
000000015C72 000000416C72 0 DrawTextW
000000015C7E 000000416C7E 0 FillRect
000000015C8A 000000416C8A 0 FrameRect
000000015C96 000000416C96 0 SystemParametersInfoW
000000015CAC 000000416CAC 0 USER32.dll
000000015CBA 000000416CBA 0 DeleteDC
000000015CC6 000000416CC6 0 CreateCompatibleDC
000000015CDC 000000416CDC 0 GetDeviceCaps
000000015CEC 000000416CEC 0 DeleteObject
000000015CFC 000000416CFC 0 CreateFontA
000000015D0A 000000416D0A 0 SelectObject
000000015D1A 000000416D1A 0 CreateCompatibleBitmap
000000015D34 000000416D34 0 CreateSolidBrush
000000015D48 000000416D48 0 SetTextColor
000000015D58 000000416D58 0 SetBkMode
000000015D64 000000416D64 0 GetObjectA
000000015D72 000000416D72 0 GetDIBits
000000015D7C 000000416D7C 0 GDI32.dll
000000015D88 000000416D88 0 CryptDestroyKey
000000015D9A 000000416D9A 0 CryptImportKey
000000015DAC 000000416DAC 0 CryptSetKeyParam
000000015DC0 000000416DC0 0 CryptEncrypt
000000015DD0 000000416DD0 0 CryptReleaseContext
000000015DE6 000000416DE6 0 CryptGenRandom
000000015DF8 000000416DF8 0 CryptAcquireContextA
000000015E10 000000416E10 0 RegOpenKeyExA
000000015E20 000000416E20 0 RegCloseKey
000000015E2E 000000416E2E 0 RegCreateKeyExA
000000015E40 000000416E40 0 RegSetValueExA
000000015E52 000000416E52 0 RegDeleteValueA
000000015E64 000000416E64 0 RegQueryValueExA
000000015E78 000000416E78 0 RegSetValueExW
000000015E8A 000000416E8A 0 CryptGetHashParam
000000015E9E 000000416E9E 0 CryptCreateHash
Ready
AN: 579
UN: 81
RS: 0
Find
Save

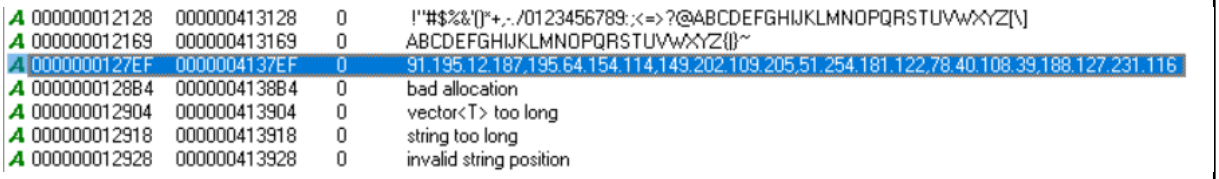

C:\Users\REM\Desktop\Malware\Day2\svchost.exe
Search
Filter
Help
File to scan
C:\Users\REM\Desktop\Malware\Day2\svchost.exe
Browse
Go
Advanced view
Time taken : 0.031 secs
Text size: 8547 bytes (8.35K)
File pos
Mem pos
ID
Text
000000015EC4 000000416EC4 0 OpenProcessToken
000000015ED8 000000416ED8 0 SetTokenInformation
000000015EEE 000000416EEE 0 CryptHashData
000000015EFE 000000416EFE 0 GetFileSecurityW
000000015F12 000000416F12 0 OpenThreadToken
000000015F24 000000416F24 0 DuplicateToken
000000015F36 000000416F36 0 MapGenericMask
000000015F48 000000416F48 0 AccessCheck
000000015F54 000000416F54 0 ADVAPI32.dll
000000015F64 000000416F64 0 SHGetFolderPathW
000000015F78 000000416F78 0 ShellExecuteW
000000015F86 000000416F86 0 SHELL32.dll
000000015F94 000000416F94 0 InternetCloseHandle
000000015FAA 000000416FAA 0 InternetCrackUrlA
000000015FBE 000000416FBE 0 InternetOpenA
000000015FCE 000000416FCE 0 InternetSetOptionA
000000015FE4 000000416FE4 0 InternetConnectA
000000015FF8 000000416FF8 0 HttpOpenRequestA
00000001600C 00000041700C 0 InternetQueryOptionA
000000016024 000000417024 0 HttpSendRequestExA
00000001603A 00000041703A 0 InternetWriteFile
00000001604E 00000041704E 0 HttpEndRequestA
000000016060 000000417060 0 HttpSendRequestA
000000016074 000000417074 0 HttpQueryInfoA
000000016086 000000417086 0 InternetReadFile
000000016098 000000417098 0 WININET.dll
0000000160A6 0000004170A6 0 WNetOpenEnumW
0000000160B6 0000004170B6 0 WNetEnumResourceW
0000000160CA 0000004170CA 0 WNetAddConnection2W
0000000160E0 0000004170E0 0 WNetCloseEnum
0000000160EE 0000004170EE 0 MPR.dll
0000000160F8 0000004170F8 0 DsRoleGetPrimaryDomainInformation
00000001611C 00000041711C 0 DsRoleFreeMemory
00000001612E 00000041712E 0 NETAPI32.dll
00000001613E 00000041713E 0 HeapAlloc
Ready
AN: 579
UN: 81
RS: 0
Find
Save



- **Some messages:**



- **Some IP addresses:**



- **We can see a list of IP addresses here:**

  + 91.195.12.187

  + 195.64.154.114

  + 149.202.109.205

  + 51.254.181.122

  + 78.40.108.39

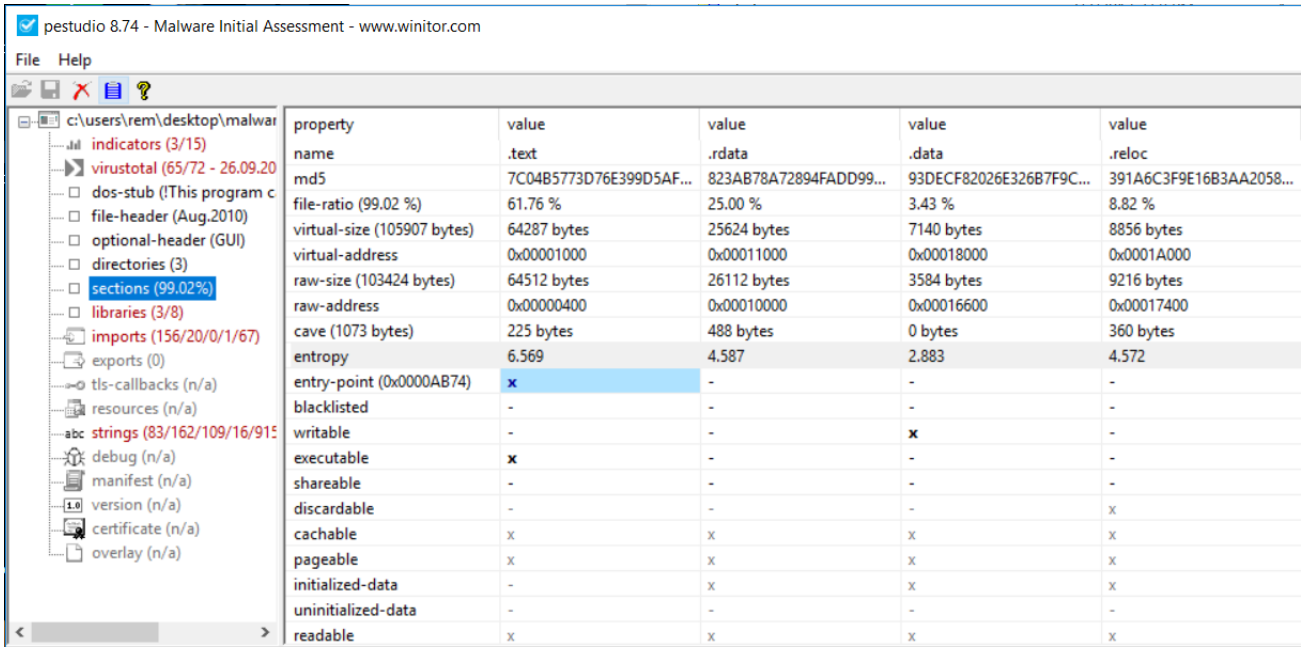
  + 188.127.231.116

Packed (pescanner, PEiD, ExeInfo)**:**

Not Packed

Testing using “ExeInfo”

Entropy (ByteHist, pescanner)**:** File, sections

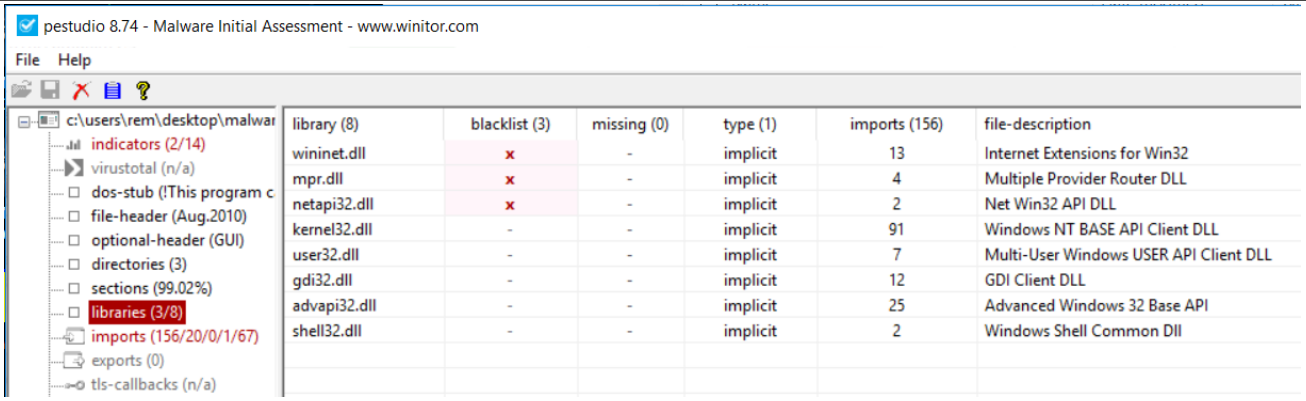


property	value	value	value	value
name	.text	.rdata	.data	.reloc
md5	7C04B5773D76E399D5AF...	823AB78A72894FADD99...	93DECF82026E326B7F9C...	391A6C3F9E16B3AA2058...
file-ratio (99.02 %)	61.76 %	25.00 %	3.43 %	8.82 %
virtual-size (105907 bytes)	64287 bytes	25624 bytes	7140 bytes	8856 bytes
virtual-address	0x00001000	0x00011000	0x00018000	0x0001A000
raw-size (103424 bytes)	64512 bytes	26112 bytes	3584 bytes	9216 bytes
raw-address	0x00000400	0x00010000	0x00016600	0x00017400
cave (1073 bytes)	225 bytes	488 bytes	0 bytes	360 bytes
entropy	6.569	4.587	2.883	4.572
entry-point (0x0000AB74)	x	-	-	-
blacklisted	-	-	-	-
writable	-	-	x	-
executable	x	-	-	-
shareable	-	-	-	-
discardable	-	-	-	x
cachable	x	x	x	x
pageable	x	x	x	x
initialized-data	-	x	x	x
uninitialized-data	-	-	-	-
readable	x	x	x	x

In Sections, we can see the entropy of each section:
+ .text: 6569
+ .rdata: 4587
+ .data: 2883
+ .reloc: 4572

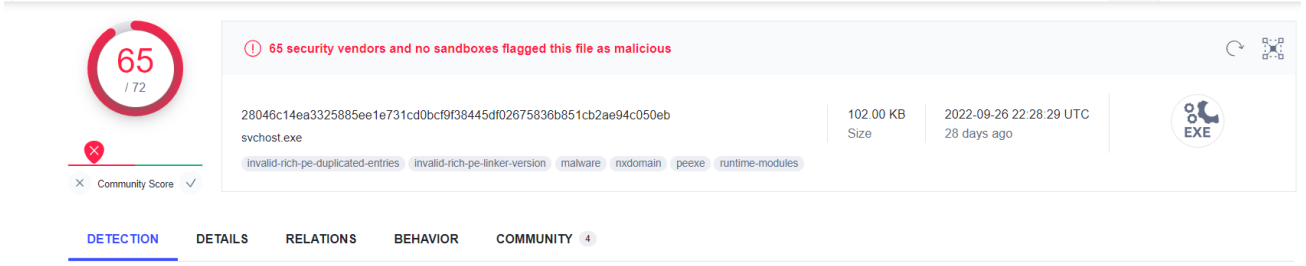
Imported/Exported Functions (PEStudio, Dependency Walker)**:**

Imported functions: wininet.dll, mpr.dll, netapi32.dll, kernel32.dll, user32.dll, gdi32.dll, advapi32.dll, shell32.dll



Open Source Research (VirusTotal, search engines, malware repositories)**:**

Searching on VirusTotal, the “svchost.exe” is flagged as a malicious file with the score 65/72



File System Artifacts (Regshot, CaptureBAT, Process Monitor, Cuckoo)**:**

Triggers: Browser, mail client, specific web pages (google, bank), time, reboot, user/admin privs

Dependencies: DNS, HTTP, IRC, ARP

- **Regshot:**
- **On m machine, after comparing 2 shots, I got the result like this. “Svchost.exe” and other processes did a lot of changes (maybe because I let it run for a longtime)**

svchost.txt

```
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2022/10/30 08:12:10  ,  2022/10/30 08:16:42
Computer: DESKTOP-2C3IQHO , DESKTOP-2C3IQHO
Username: REM , REM

----------------------------------
Keys deleted: 38468
----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\AppXwv0gcxhfzclwz3q9j596bfk9ths12een
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\windows.protocol\pandora\AppXwv0gcxhfzclwz3q9j596bfk9ths12een
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe
HKLM\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint
HKLM\SOFTWARE\Classes\Local
```

- **Added 610 keys:**

```
----------------------------------
Keys added: 610
----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\AppXzjrm2jd058qcnbeqk55rzmemp770dxzn
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\windows.protocol\pandora\AppXzjrm2jd058qcnbeqk55rzmemp770dxzn
HKLM\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\D5EA27B7.Duolingo-LearnLanguagesforFree_2017.112.1.0_neutral_split.scale-125_yx6k7tf7xvsea
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_2022.2203.1037.0_neutral_~_8wekyb3d8bbwe
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_6.2203.1037.0_x64__8wekyb3d8bbwe
HKLM\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_6.2203.1037.0_x64__8wekyb3d8bbwe\Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint
HKLM\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_6.2203.1037.0_x64__8wekyb3d8bbwe\Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint\windows.fileTypeAssociation
HKLM\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_6.2203.1037.0_x64__8wekyb3d8bbwe\Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint\windows.fileTypeAssociation\.3mf
HKLM\SOFTWARE\Classes\Local
```

- **Added 407 folders:**

```
----------------------------------
Folders added: 407
----------------------------------
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe6a88b651-bccc-4d1c-b49c-0073f4790dfd
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe6a88b651-bccc-4d1c-b49c-0073f4790dfd\AppxMetadata
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe6a88b651-bccc-4d1c-b49c-0073f4790dfd\microsoft.system.package.metadata
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\AppxMetadata
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Dial
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Fonts
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Images
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Images\HelpAndFeedback
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Images\SmartSelect
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Images\Stickers
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Images\Stickers\Thumbnails
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Logos
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Logos\contrast-high
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Logos\contrast-standard
C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe2485ebfd-43cc-48fa-b6a7-a5b935a03e54\Assets\Logos\contrast-white
```

- **Deleted 119 folders:**

```
Folders deleted: 119
----------------------------------
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\AppxMetadata
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\microsoft.system.package.metadata
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\AppxMetadata
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Dial
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Fonts
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Images
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Images\HelpAndFeedback
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Images\SmartSelect
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Images\Stickers
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Images\Stickers\Thumbnails
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Logos
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Logos\contrast-high
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Logos\contrast-standard
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Logos\contrast-white
C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64__8wekyb3d8bbwe\Assets\Logos\FileAssociation
```

- **Total changes 154876:**

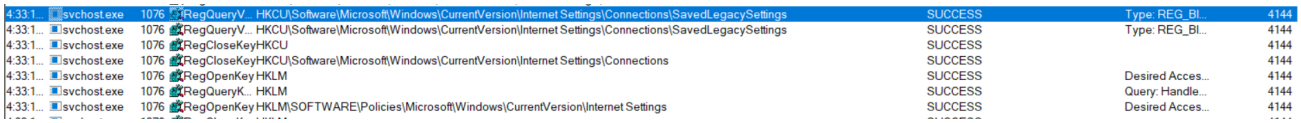
```
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.NET.Native.Framework.1.6_1.6.24903.0_x86__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.Services.Store.Engagement_10.0.1610.0_x64__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.Services.Store.Engagement_10.0.1610.0_x86__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.VCLibs.140.00_14.0.24605.0_x64__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.VCLibs.140.00_14.0.24605.0_x86__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.VCLibs.140.00_14.0.25426.0_x64__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.VCLibs.140.00_14.0.25426.0_x86__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.XboxGameOverlay_1.24.5001.0_neutral_split.scale-100_8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.XboxGameOverlay_1.24.5001.0_neutral_~_8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\Microsoft.XboxGameOverlay_1.24.5001.0_x64__8wekyb3d8bbwe
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_neutral_split.scale-100_n619g4d5j0fnw
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_neutral_~_n619g4d5j0fnw
C:\Users\All Users\Microsoft\Windows\AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_x64__n619g4d5j0fnw
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{3ac98f2e-d8dd-464e-84e5-ac09fa8e458a}
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{5b2b3d12-e945-4eaa-9874-db47189b5fbd}

----------------------------------
Total changes: 154876
----------------------------------
```

- **Looking at the processes by using “Process Monitor”:**
- **Some registry actions:**

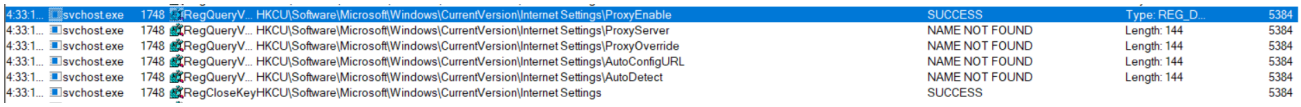
4:33:1...	svchost.exe	1748	RegCreateK...	HKCU\Software\Locky	SUCCESS	Desired Acces...	5360
4:33:1...	svchost.exe	1748	RegSetInfoK...	HKCU\Software\Locky	SUCCESS	KeySetInformat...	5360
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Locky\id	NAME NOT FOUND	Length: 144	5360
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Locky\pubkey	NAME NOT FOUND	Length: 144	5360
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Locky\paytext	NAME NOT FOUND	Length: 144	5360

→ A new registry key named “Locky”



4:33:1...	svchost.exe	1076	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS	Type: REG_Bl...	4144
4:33:1...	svchost.exe	1076	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS	Type: REG_Bl...	4144
4:33:1...	svchost.exe	1076	RegCloseKey	HKCU	SUCCESS		4144
4:33:1...	svchost.exe	1076	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS		4144
4:33:1...	svchost.exe	1076	RegOpenKey	HKLM	SUCCESS	Desired Acces...	4144
4:33:1...	svchost.exe	1076	RegQueryK...	HKLM	SUCCESS	Query: Handle...	4144
4:33:1...	svchost.exe	1076	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	Desired Acces...	4144

→Registry key named “SavedLegacySettings”, type: REG_BINARY

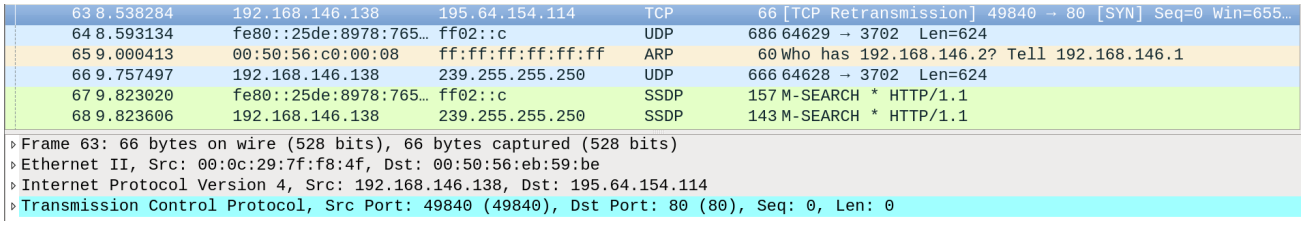


4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	SUCCESS	Type: REG_D...	5384
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer	NAME NOT FOUND	Length: 144	5384
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride	NAME NOT FOUND	Length: 144	5384
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL	NAME NOT FOUND	Length: 144	5384
4:33:1...	svchost.exe	1748	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect	NAME NOT FOUND	Length: 144	5384
4:33:1...	svchost.exe	1748	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS		5384

→Registry key named “ProxyEnable”, type: REG_DWORD

Network Artifacts (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark)**:** C2 domains/IP addresses, protocols, user-agent

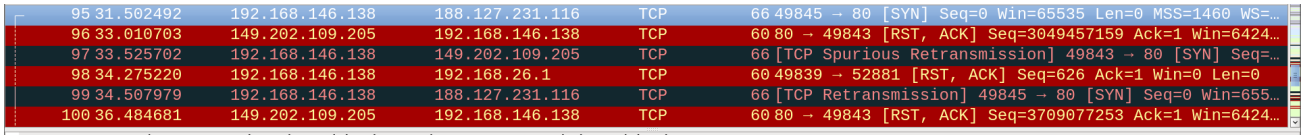
Using Wireshark:



63	8.538284	192.168.146.138	195.64.154.114	TCP	66 [TCP Retransmission] 49840 → 80 [SYN] Seq=0 Win=655…
64	8.593134	fe80::25de:8978:765…	ff02::c	UDP	686 64629 → 3702 Len=624
65	9.000413	00:50:56:c0:00:08	ff:ff:ff:ff:ff:ff	ARP	60 Who has 192.168.146.2? Tell 192.168.146.1
66	9.757497	192.168.146.138	239.255.255.250	UDP	666 64628 → 3702 Len=624
67	9.823020	fe80::25de:8978:765…	ff02::c	SSDP	157 M-SEARCH * HTTP/1.1
68	9.823606	192.168.146.138	239.255.255.250	SSDP	143 M-SEARCH * HTTP/1.1

```
▹ Frame 63: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▹ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be
▹ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 195.64.154.114
▹ Transmission Control Protocol, Src Port: 49840 (49840), Dst Port: 80 (80), Seq: 0, Len: 0
```

→ IP address 195.64.154.114, TCP protocol, Src port 49840, Dst port 80.

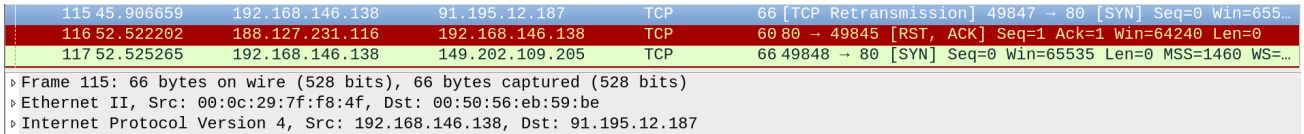


95	31.502492	192.168.146.138	188.127.231.116	TCP	66 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=…
96	33.010703	149.202.109.205	192.168.146.138	TCP	60 80 → 49843 [RST, ACK] Seq=3049457159 Ack=1 Win=6424…
97	33.525702	192.168.146.138	149.202.109.205	TCP	66 [TCP Spurious Retransmission] 49843 → 80 [SYN] Seq=…
98	34.275220	192.168.146.138	192.168.26.1	TCP	60 49839 → 52881 [RST, ACK] Seq=626 Ack=1 Win=0 Len=0
99	34.507979	192.168.146.138	188.127.231.116	TCP	66 [TCP Retransmission] 49845 → 80 [SYN] Seq=0 Win=655…
100	36.484681	149.202.109.205	192.168.146.138	TCP	60 80 → 49843 [RST, ACK] Seq=3709077253 Ack=1 Win=6424…

```
▹ Frame 95: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▹ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be
▹ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 188.127.231.116
▹ Transmission Control Protocol, Src Port: 49845 (49845), Dst Port: 80 (80), Seq: 0, Len: 0
```

→ IP address 188.127.231.116, TCP protocol, Src port 49845, Dst Port 80

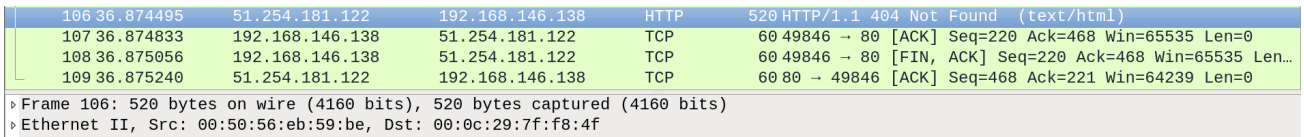
→ and IP address 149.202.109.205, TCP protocol, port 49843 (Dst) and port 80 (Src)



115	45.906659	192.168.146.138	91.195.12.187	TCP	66 [TCP Retransmission] 49847 → 80 [SYN] Seq=0 Win=655…
116	52.522202	188.127.231.116	192.168.146.138	TCP	60 80 → 49845 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
117	52.525265	192.168.146.138	149.202.109.205	TCP	66 49848 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=…

```
▹ Frame 115: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▹ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be
▹ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 91.195.12.187
▹ Transmission Control Protocol, Src Port: 49847 (49847), Dst Port: 80 (80), Seq: 0, Len: 0
```

→ I got the same with IP address 91.195.12.187



106	36.874495	51.254.181.122	192.168.146.138	HTTP	520 HTTP/1.1 404 Not Found (text/html)
107	36.874833	192.168.146.138	51.254.181.122	TCP	60 49846 → 80 [ACK] Seq=220 Ack=468 Win=65535 Len=0
108	36.875056	192.168.146.138	51.254.181.122	TCP	60 49846 → 80 [FIN, ACK] Seq=220 Ack=468 Win=65535 Len…
109	36.875240	51.254.181.122	192.168.146.138	TCP	60 80 → 49846 [ACK] Seq=468 Ack=221 Win=64239 Len=0

```
▹ Frame 106: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits)
▹ Ethernet II, Src: 00:50:56:eb:59:be, Dst: 00:0c:29:7f:f8:4f
▹ Internet Protocol Version 4, Src: 51.254.181.122, Dst: 192.168.146.138
▹ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49846 (49846), Seq: 1, Ack: 220, Len: 466
▹ Hypertext Transfer Protocol
```

→ IP address 51.254.181.122, HTTP protocol and TCP protocol, port 80 (Src), port 49846 (Dst).

We have an exciting file named “main.php”. Using follow TCP stream, I got this:

```
POST /main.php HTTP/1.1
Host: 51.254.181.122
Content-Length: 100
Connection: Keep-Alive
Cache-Control: no-cache

.T...4Kh.......r^..._....K.D......}...L..MS...-G.x..G...{.e.....+.ct.OJd.p.cd'.em.
3....Vbwz.9.LS.oa.pHTTP/1.1 404 Not Found
Date: Tue, 25 Oct 2022 10:41:43 GMT
Server: Apache/2.2.15 (CentOS)
Content-Length: 286
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /main.php was not found on this server.</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at 51.254.181.122 Port 80</address>
</body></html>
```

```
128 64.098705    192.168.146.138    78.40.108.39    TCP    60 49849 → 80 [RST, ACK] Seq=218 Ack=1 Win=0 Len=0
▸ Frame 128: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be
▸ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 78.40.108.39
▸ Transmission Control Protocol, Src Port: 49849 (49849), Dst Port: 80 (80), Seq: 218, Ack: 1, Len: 0
```

→ **IP address 78.40.108.39, we follow TCP stream and got this**

```
POST /main.php HTTP/1.1
Host: 78.40.108.39
Content-Length: 100
Connection: Keep-Alive
Cache-Control: no-cache

.T...4Kh.......r^..._....K.D......}...L..MS...-G.x..G...{.e.....+.ct.OJd.p.cd'.em.
3....Vbwz.9.LS.oa.p
```

Memory Analysis (Volatility, Rekall, Redline, Process Hacker)**:** rogue processes, code injection, rootkits, network artifacts

Open Source Research (centralops, robtex, urlvoid, ipvoid, TrustedSource)**:**

Static Analysis (IDA Pro)**:** Strings, CALLs, program flow, loops

- **Using IDA pro:**
- **We disassemble svchost.exe using IDA, click on Imports, we observe numerous APIs associated with registry access, such as RegOpenKeyExA**

xrefs to RegOpenKeyExA

Direction	Type	Address	Text	
Up	r	sub_403D8A+F5	call	ds:RegOpenKeyExA
Up	p	sub_403D8A+F5	call	ds:RegOpenKeyExA
Up	r	WinMain(x,x,x,x)+7AC	call	ds:RegOpenKeyExA
Up	p	WinMain(x,x,x,x)+7AC	call	ds:RegOpenKeyExA

- **We press Alt+ T to search String RegOpenKeyExA, This will take you to address 004047F0, where you will see a CALL to RegOpenKeyExA**
- **At address 004047E2, we can see the link "Software\Microsoft\Windows\CurrentVersion\Run". This is the path to the Run key and also the way this malware uses to keep the persistence.**

```
.text:004047CA                 mov     byte ptr [ebp+var_4], 15h
.text:004047CE                 mov     al, ds:byte_4137ED
.text:004047D3                 test    al, al
.text:004047D5                 jz      short loc_404833
.text:004047D7                 lea     eax, [ebp+var_50]
.text:004047DA                 push    eax             ; phkResult
.text:004047DB                 push    2000000h        ; samDesired
.text:004047E0                 push    0               ; ulOptions
.text:004047E2                 push    offset aSoftwareMicros ; "Software\\Microsoft\\Windows\\CurrentVe"...
.text:004047E7                 push    80000001h       ; hKey
.text:004047E7 ;   } // starts at 4047CA
.text:004047EC ;   try {
.text:004047EC                 mov     byte ptr [ebp+var_4], 16h
.text:004047F0                 call    ds:RegOpenKeyExA
.text:004047F6                 test    eax, eax
.text:004047F8                 jz      short loc_404817
.text:004047FA                 mov     [ebp+var_80], eax
.text:004047FD                 mov     [ebp+var_84], offset ??_7livsx@@6B@ ; const livsx::`vftable'
.text:00404807                 push    offset __TI1?AVlivsx@@ ; throw info for 'class livsx'
.text:0040480C                 lea     eax, [ebp+var_84]
.text:00404812                 jmp     loc_404209
.text:00404817 ; ---------------------------------------------------------------------------

; const CHAR aSoftwareMicros[]
aSoftwareMicros db 'Software\Microsoft\Windows\CurrentVersion\Run',0
                                        ; DATA XREF: WinMain(x,x,x,x)+79E↑o
```

- **At address 004047E7, there is a push "80000001h; hKey". We can search this on the internet:**

Syntax

C++ Copy

```
LSTATUS RegOpenKeyExA(
  [in]           HKEY   hKey,
  [in, optional] LPCSTR lpSubKey,
  [in]           DWORD  ulOptions,
  [in]           REGSAM samDesired,
  [out]          PHKEY  phkResult
);
```

Parameters

`[in] hKey`

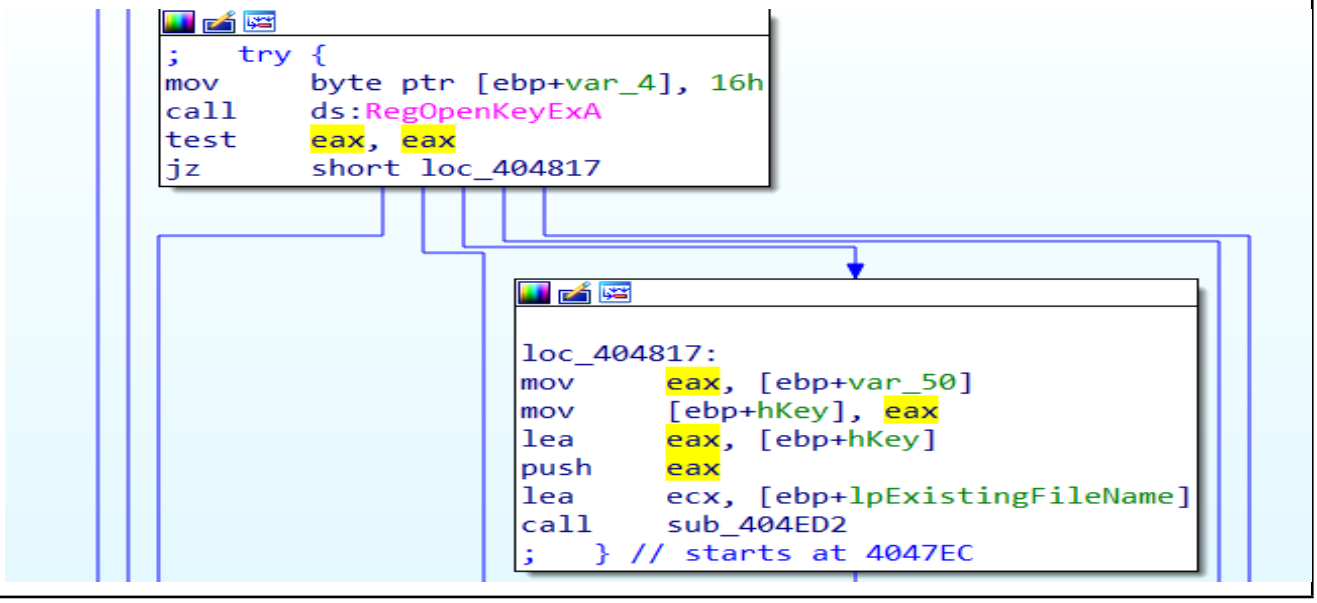
A handle to an open registry key. This handle is returned by the RegCreateKeyEx or **RegOpenKeyEx** function, or it can be one of the following predefined keys:

HKEY_CLASSES_ROOT HKEY_CURRENT_CONFIG HKEY_CURRENT_USER HKEY_LOCAL_MACHINE HKEY_USERS

- **We right-click on 80000001h and select Use Standard Symbolic Constant. We know that RegOpenKeyExA involves the registry. Reviewing the list of options, we see multiple references to HKEY_CURRENT_USER**

GDICOMMENT_WINDOWS_METAFILE	FFFFFFFF80000001	MS SDK (Windows 7)
HKEY_CURRENT_USER	FFFFFFFF80000001	MS SDK (Windows 7)
KERB_WRAP_NO_ENCRYPT	FFFFFFFF80000001	MS SDK (Windows 7)
LINEERR_ALLOCATED	FFFFFFFF80000001	MS SDK (Windows 7)
MQCONN_PING_FAILURE	FFFFFFFF80000001	MS SDK (Windows 7)

- **The call to RegOpenKeyExA happens right before the “test” and “jz” instructions. If the test return 0 (success) -> jump to the address loc_404817.**



- **If the call is not successful, execution will continue at 4047FA and then jump to loc_404209.**

```
.text:00404867                  mov     byte ptr [ebp+var_4], 18h
.text:0040486B                  push    offset ValueName ; "completed"
.text:00404870                  push    [ebp+phkResult] ; hKey
.text:00404873                  mov     dword ptr [ebp+var_5C], 1
.text:0040487A                  call    ds:RegSetValueExA
.text:00404880                  test    eax, eax
.text:00404882                  jz      short loc_4048A4
.text:00404884                  mov     [ebp+var_88], eax
.text:0040488A                  mov     [ebp+var_8C], offset ??_7livsx@@6B@ ; const livsx::`vftable'
.text:00404894                  push    offset __TI1?AVlivsx@@ ; throw info for 'class livsx'
.text:00404899                  lea     eax, [ebp+var_8C]
.text:0040489F                  jmp     loc_404209
```

- **<u>HTTP C2 Analysis</u>:**
- **The address of the CALL to HttpSendRequestA is 406B80. The CALL to HttpSendRequestA occurs immediately before the "test" and "jnz" instructions, these instructions likely serve to evaluate the result. If "eax" is not 0, jump to loc_406BAA otherwise jump to loc_406B8A.**

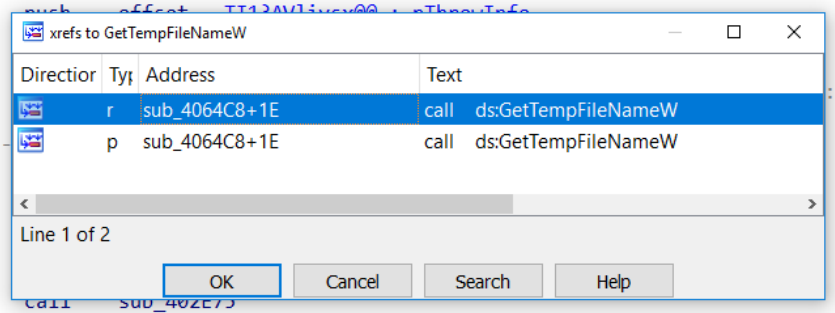
- **The CALL to InternetOpenA occurs at 4068D0, at 4068D6 we can see MOV that places EAX into EBX and CMP that places EDI into EBX. We have CMP and JNZ, the CMP is comparing EBX with 0, if EBX = 0 => the result = 0, and If EBX≠ 0 => the result ≠ 0. JNZ at 4068DA, If EBX≠ 0 then jump to loc_4068F9, the jump will occur if the call to InternetOpenA is successful. If the CALL to InternetOpenA is unsuccessful, execution will proceed linearly to 4068DC, where GetLastError will be called, and the JMP at 4068B2 will eventually be executed**

```
.text:004068CF                  push    edi             ; lpszAgent
.text:004068D0                  call    ds:InternetOpenA
.text:004068D6                  mov     ebx, eax
.text:004068D8                  cmp     ebx, edi
.text:004068DA                  jnz     short loc_4068F9
.text:004068DC                  call    ds:GetLastError
.text:004068E2                  mov     [esp+0AC8h+var_AA8], eax
.text:004068E6                  mov     [esp+0AC8h+pExceptionObject], offset ??_7cuovxnupr@@6B@ ; const cuovxnupr::`vftable'
.text:004068EE                  push    offset __TI2?AVcuovxnupr@@ ; throw info for 'class cuovxnupr'
.text:004068F3                  lea     eax, [esp+0ACCh+pExceptionObject]
.text:004068F7                  jmp     short loc_4068B2
.text:004068F9 ; ---------------------------------------------------------------------------
```

- **In sub_40684C, we can find the references to both InternetOpenA and HttpSendRequestA**

- **<u>Function components:</u>**
- **The address 4064E6 is the address of the CALL to GetTempFileNameW. the CALL to GetTempFileNameW is located in function sub_4064C8**

```
.text:004064DB                push    eax             ; lpTempFileName
.text:004064DC                push    0               ; uUnique
.text:004064DE                push    offset PrefixString ; "sys"
.text:004064E3                push    [ebp+lpPathName] ; lpPathName
.text:004064E6                call    ds:GetTempFileNameW
.text:004064EC                test    eax, eax
.text:004064EE                jnz     short loc_40650E
.text:004064F0                call    ds:GetLastError
.text:004064F6                mov     [ebp+var_4], eax
.text:004064F9
.text:004064FE
.text:00406501
.text:00406502                                                          :`vftable'
.text:00406509
.text:0040650E ; ------------
.text:0040650E
.text:0040650E loc_40650E:
.text:0040650E
.text:00406514
.text:00406515
.text:00406518
```



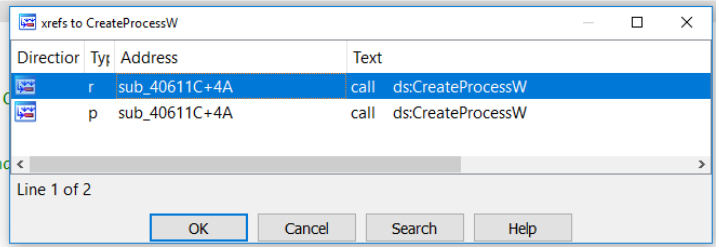

```
.text:004064C8
.text:004064C8 ; =============== S U B R O U T I N E =======================================
.text:004064C8
.text:004064C8 ; Attributes: bp-based frame
.text:004064C8
.text:004064C8 ; int __cdecl sub_4064C8(int, LPCWSTR lpPathName)
.text:004064C8 sub_4064C8      proc near               ; CODE XREF: sub_406196+67↑p
.text:004064C8
.text:004064C8 TempFileName    = word ptr -210h
.text:004064C8 pExceptionObject= dword ptr -8
.text:004064C8 var_4           = dword ptr -4
.text:004064C8 arg_0           = dword ptr  8
.text:004064C8 lpPathName      = dword ptr  0Ch
.text:004064C8
.text:004064C8                 push    ebp
.text:004064C9                 mov     ebp, esp
.text:004064CB                 sub     esp, 210h
.text:004064D1                 and     [ebp+var_4], 0
.text:004064D5                 lea     eax, [ebp+TempFileName]
.text:004064DB                 push    eax             ; lpTempFileName
.text:004064DC                 push    0               ; uUnique
.text:004064DE                 push    offset PrefixString ; "sys"
.text:004064E3                 push    [ebp+lpPathName] ; lpPathName
```

→ Sub_4064C8 has 2 arguments: lpPathName and arg_0. We have some other variables named TempFileName, var_8, and var_4. In this function, the prologue includes addresses 4064C8-4064CB and the epilogue includes addresses 406520-406521. In this case, it includes the typical LEAVE and RETN instructions as well as POP instructions to restore registers that were saved in the prologue.

```
.text:00406520                 leave
.text:00406521                 retn
.text:00406521 sub_4064C8      endp
```

- **We consider the call to CreateProcessW at the address 406166. This CALL is located in function sub_40611C**

```
.text:00406158                 push    ecx             ; lpProcessInformation
.text:00406159                 lea     ecx, [ebp+StartupInfo]
.text:0040615C                 push    ecx             ; lpStartupInfo
.text:0040615D                 push    ebx             ; lpCurrentDirectory
.text:0040615E                 push    ebx             ; lpEnvironment
.text:0040615F                 push    50h ; 'P'       ; dwCreationFlags
.text:00406161                 push    ebx             ; bInheritHandles
.text:00406162                 push    ebx             ; lpThreadAttributes
.text:00406163                 push    ebx             ; lpProcessAttributes
.text:00406164                 push    eax             ; lpCommandLine
.text:00406165                 push    ebx             ; lpApplicationName
.text:00406166                 call    ds:CreateProcessW
.text:0040616C                 test    eax, eax
.text:0040616E                 jnz     short loc_406182
.text:00406170
.text:00406170 loc_406170:                             ;
.text:00406170                 push    edi
.text:00406171                 xor     edi, edi
.text:00406173                 lea     esi, [ebp+lpCommand
.text:00406176                 call    sub_402D33
.text:0040617B                 pop     edi
.text:0040617C                 pop     esi
```




```
.text:0040611C ; int __cdecl sub_40611C(LPWSTR lpCommandLine, int, int, int, int, int)
.text:0040611C sub_40611C      proc near               ; CODE XREF: TopLevelExceptionFilter+12↑p
.text:0040611C                                         ; WinMain(x,x,x,x)+4EA↑p ...
.text:0040611C
.text:0040611C StartupInfo     = _STARTUPINFOW ptr -54h
.text:0040611C ProcessInformation= _PROCESS_INFORMATION ptr -10h
.text:0040611C lpCommandLine   = dword ptr  8
.text:0040611C arg_14          = dword ptr  1Ch
```

→ The sub_40611C has 2 arguments: lpCommandLine and arg_14. There are 2 variables named StartupInfo and hObject. Being the same as the previous function, in this one, the prologue includes addresses 40611C-406124 and the epilogue includes addresses 40617B-406181.

```
.text:0040617D                 mov     al, bl
.text:0040617F                 pop     ebx
.text:00406180                 leave
.text:00406181                 retn
```

- **<u>Loop components:</u>**
- **A group of strings is located at 418CD8, we press G to jump to 418CD8, click on off_418CD8, and press x to show the xrefs table, double click on the reference it leads to the address 407D84**

```
.text:00407D82 loc_407D82:                             ; CODE XREF: sub_407CA7+D0↑j
.text:00407D82                 xor     esi, esi
.text:00407D84
.text:00407D84 loc_407D84:                             ; CODE XREF: sub_407CA7+FF↓j
.text:00407D84                 push    off_418CD8[esi] ; String2
.text:00407D8A                 lea     eax, [ebp+FindFileData.cFileName]
.text:00407D90                 push    eax             ; String1
.text:00407D91                 call    __wcsicmp
.text:00407D96                 pop     ecx
.text:00407D97                 pop     ecx
.text:00407D98                 test    eax, eax
.text:00407D9A                 jz      loc_407F22
.text:00407DA0                 add     esi, 4
.text:00407DA3                 cmp     esi, 38h ; '8'
.text:00407DA6                 jb      short loc_407D84
.text:00407DA8                 test    byte ptr [ebp+FindFileData.dwFileAttributes], 10h
.text:00407DAF                 jz      short loc_407DF6
.text:00407DB1                 mov     edi, [ebp+arg_4]
.text:00407DB4                 lea     eax, [ebp+var_78]
```

- **The loop is presented by the dotted line and the arrow. Before the loop, we have the instruction "xor esi, esi", this zeroes esi and serves at the loop initiation. The CMP and JB instructions at 407DA3 and 407DA6, respectively, comprise the stopping condition. And our stopping condition is that check if "esi < 38h", and we increase esi by 4 each loop run (add esi 4 at 407DA0).**

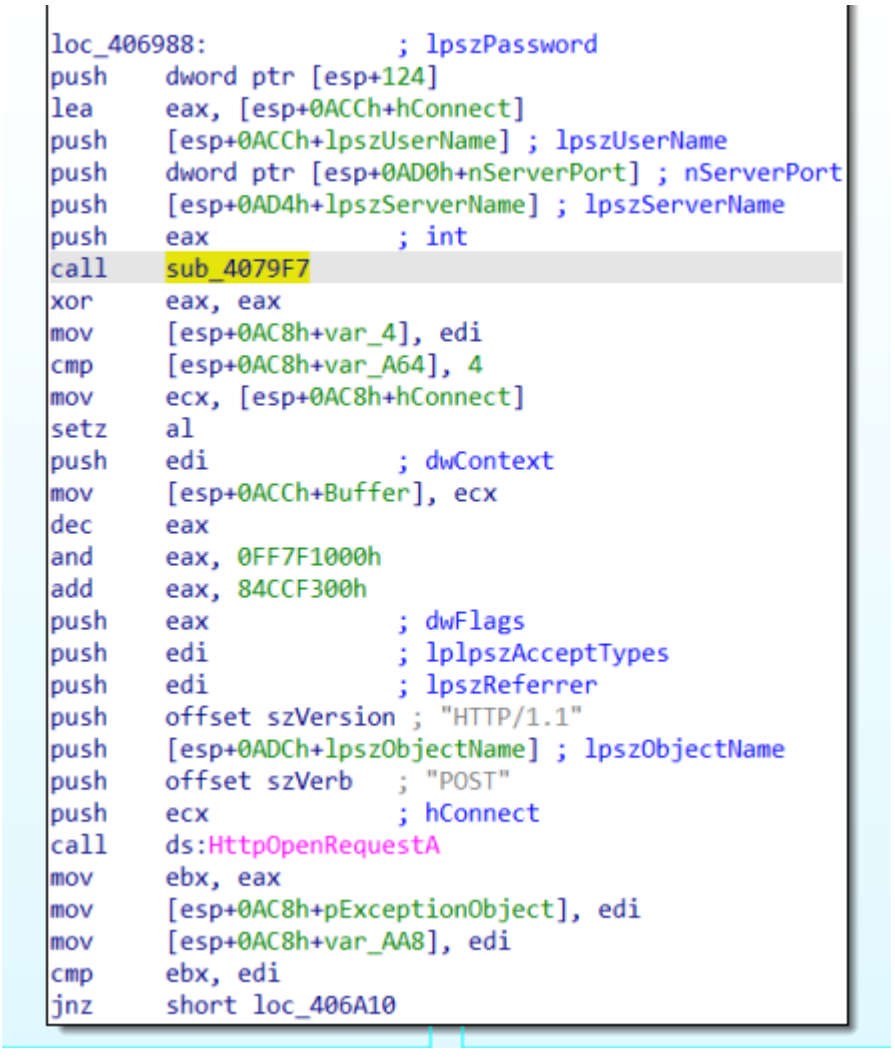
- **<u>Compound Expressions:</u>**
- **We consider the call to GetTempPathW at address 40526D**

```
.text:00405267                 mov     edi, 208h
.text:0040526C                 push    edi             ; nBufferLength
.text:0040526D                 call    ds:GetTempPathW
.text:00405273                 test    eax, eax
.text:00405275                 jz      short loc_4052A7
.text:00405277                 cmp     eax, edi
.text:00405279                 pop     edi
.text:0040527A                 jnb     short loc_4052A7
.text:0040527C                 push    [ebp+var_4]
.text:0040527F                 and     dword ptr [esi+10h], 0
.text:00405283                 xor     ecx, ecx
.text:00405285                 lea     eax, [ebp+eax*2+Buffer]
.text:0040528C                 mov     dword ptr [esi+14h], 7
.text:00405293                 push    eax
.text:00405294                 mov     [esi], cx
.text:00405297                 push    esi
.text:00405298                 lea     ecx, [ebp+Buffer]
.text:0040529E                 call    sub_405904
.text:004052A3                 mov     eax, esi
.text:004052A5                 leave
.text:004052A6                 retn
.text:004052A7 ; ---------------------------------------------------------------------------
```

- **We have the test and jz instruction, which means jump to 4052A7 if eax is zero. We know that eax stored the value returned by the function CALL to GetTempPathW. Now, we can understand the checking condition is "jump to 4052A7 if the GetTempPathW fails".**

- **Consider the jnb instruction at 405277, here we compare eax and edi. That means we "jump to 4052A7 if eax is not below edi".**
- **In conclusion, this sub-function has the ability to check if the CALL to GetTempPath returns correctly and check if the buffer has enough space for the temporary path (compare eax and edi - edi is considered as the specific size).**

- **At the address 406988, we can see a Call to HttpOpenRequestA, basically, we can get the version of the HTTP request is HTTP/1.1. And in this case, the HTTP verb is POST.**



```
loc_406988:             ; lpszPassword
push    dword ptr [esp+124]
lea     eax, [esp+0ACCh+hConnect]
push    [esp+0ACCh+lpszUserName] ; lpszUserName
push    dword ptr [esp+0AD0h+nServerPort] ; nServerPort
push    [esp+0AD4h+lpszServerName] ; lpszServerName
push    eax             ; int
call    sub_4079F7
xor     eax, eax
mov     [esp+0AC8h+var_4], edi
cmp     [esp+0AC8h+var_A64], 4
mov     ecx, [esp+0AC8h+hConnect]
setz    al
push    edi             ; dwContext
mov     [esp+0ACCh+Buffer], ecx
dec     eax
and     eax, 0FF7F1000h
add     eax, 84CCF300h
push    eax             ; dwFlags
push    edi             ; lplpszAcceptTypes
push    edi             ; lpszReferrer
push    offset szVersion ; "HTTP/1.1"
push    [esp+0ADCh+lpszObjectName] ; lpszObjectName
push    offset szVerb   ; "POST"
push    ecx             ; hConnect
call    ds:HttpOpenRequestA
mov     ebx, eax
mov     [esp+0AC8h+pExceptionObject], edi
mov     [esp+0AC8h+var_AA8], edi
cmp     ebx, edi
jnz     short loc_406A10
```

Debugging (OllyDbg)**:** Function breakpoints, monitor stack, memory map, plugins for unpacking, find OEP

ANALYSIS SUMMARY

Key Host and Network Indicators of Compromise (IOCs):

- **These strange IP addresses:**
  + 91.195.12.187
  + 195.64.154.114
  + 149.202.109.205

+ 51.254.181.122 **+ 78.40.108.39** **+ 188.127.231.116** - **HKCU\Software\Locky** - **HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Connections\SavedLegacySettings** - **HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable**
Key Functionality:
+RegOpenKeyExA, RegSetValueExA **+ InternetOpenA, InternetConnectA, HttpOpenRequestA, HttpSendRequestA, InternetReadFile.** **+ GetTempFileNameW** **+ CreateProcessW** **+ GetTempPathW**
Purpose:
Persistence:
Creates the persistence registry key in the path - **Software\Microsoft\Windows\CurrentVersion\Run**
Environment-specific Impact:
Root Cause:
Attribution: