**Table of Contents:**

Part 1. → Basic Static Analysis:

- Strings
- Peview

Part 2 → Basic Dynamic Analysis:

- RegShot
- Procex
- ProcMon
- apateDNS
- NetCat

## PART 1:
## Basic Static Analysis

Analyzing malware **without looking at any instructions in the binary**
This should always be **the first step**

**Positives →**
Basic static analysis can help determine...

| |
|---|
| ● If a file is malicious or not |
| ● What the malware does |
| ● Where its communications go |

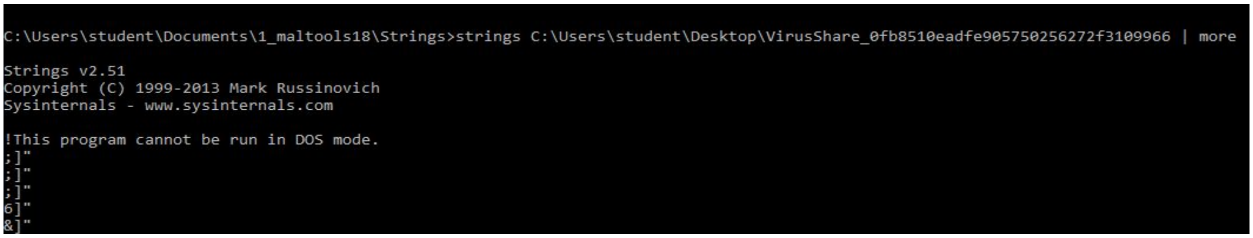
**Negatives →**

| |
|---|
| ● Malware authors can change the code/signature to evade detection |
| ● Malware can be “obfuscated” or packed |
| ● Unable to identify certain advanced behaviors or elements of the malware |

---

**Strings:** Run strings on sample malware file to examine [**ip addresses, web addresses, Processes** ]
‘Find string’ command specifies keywords that can help search the file for relevant and possibly malicious code parts

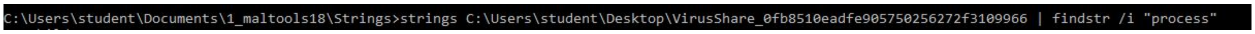
| |
|---|
| **→ strings c:\Users\students\Desktop\VirusShare_0fb8510eadfe905750256272f3109966** |
| **→ findstr /i “http”  or “www”** |
| **→ find str /i “process”** |



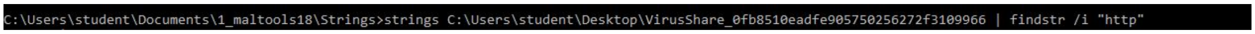
```
C:\Users\student\Documents\1_maltools18\Strings>strings C:\Users\student\Desktop\VirusShare_0fb8510eadfe905750256272f3109966 | more

Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
;]"
;]"
;]"
6]"
&]"
```



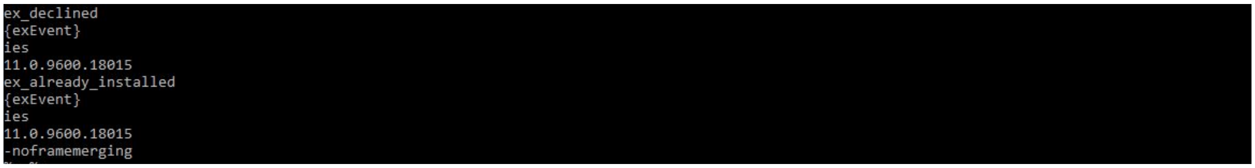
```
C:\Users\student\Documents\1_maltools18\Strings>strings C:\Users\student\Desktop\VirusShare_0fb8510eadfe905750256272f3109966 | findstr /i "process"
```



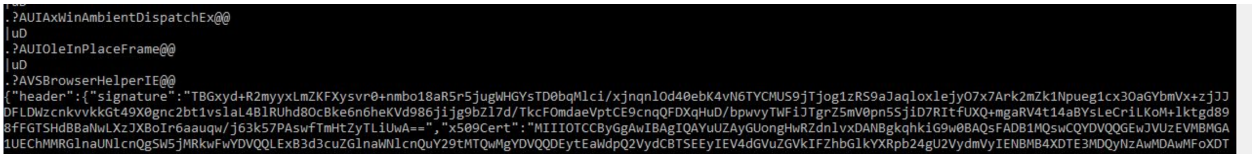
```
C:\Users\student\Documents\1_maltools18\Strings>strings C:\Users\student\Desktop\VirusShare_0fb8510eadfe905750256272f3109966 | findstr /i "http"
```

**NOTES:**

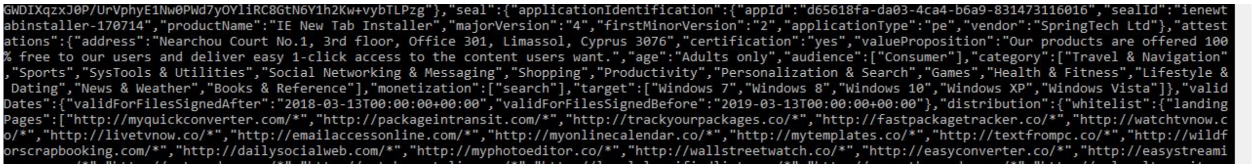
While running these commands, several web addresses and ip addresses were found. However without further knowledge of what the malware does, it is difficult to determine if these findings indicate anything important/malicious.



```
ex_declined
{exEvent}
ies
11.0.9600.18015
ex_already_installed
{exEvent}
ies
11.0.9600.18015
-noframemerging
```



```
.?AUIAxWinAmbientDispatchEx@@
|uD
.?AUIOleInPlaceFrame@@
|uD
.?AVSBrowserHelperIE@@
{"header":{"signature":"TBGxyd+R2myyxLmZKFXysvr0+nmbo18aR5r5jugWHGYsTD0bqMlci/xjnqnlOd40ebK4vN6TYCMUS9jTjog1zRS9aJaqloxlejyO7x7Ark2mZk1Npueg1cx3OaGYbmVx+zjJJ
DFLDWzcnkvvkkGt49X0gnc2bt1vslaL4BlRUhd8OcBke6n6heKVd986jijg9bZl7d/TkcFOmdaeVptCE9cnqQFDXqHuD/bpwvyTWFiJTgrZ5mV0pn5SjiD7RItfUXQ+mgaRV4t14aBYsLeCriLKoM+lktgd89
8fFGTSHdBBaNwLXzJXBoIr6aauqw/j63k57PAswfTmHtZyTLiUwA==","x509Cert":"MIIIOTCCByGgAwIBAgIQAYuUZAyGUongHwRZdnlvxDANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQGEwJVUzEVMBMGA
1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMTQwMgYDVQQDEytEaWdpQ2VydCBTSEEyIEV4dGVuZGVkIFZhbGlkYXRpb24gU2VydmVyIENBMB4XDTE3MDQyNzAwMDAwMFoXDT
```



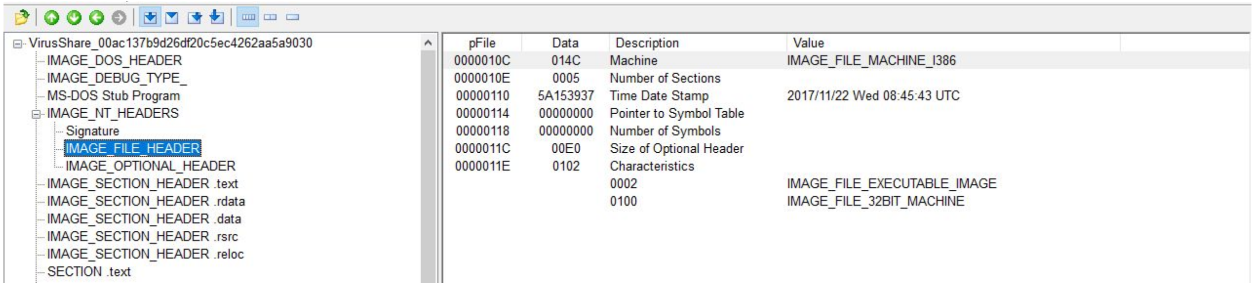
```
GWDIXqzxJ0P/UrVphyE1Nw0PWd7yOYliRC8GtN6Y1h2Kw+vybTLPzg"},"seal":{"applicationIdentification":{"appId":"d65618fa-da03-4ca4-b6a9-831473116016","sealId":"ienewt
abinstaller-170714","productName":"IE New Tab Installer","majorVersion":"4","firstMinorVersion":"2","applicationType":"pe","vendor":"SpringTech Ltd"},"attest
ations":{"address":"Nearchou Court No.1, 3rd floor, Office 301, Limassol, Cyprus 3076","certification":"yes","valueProposition":"Our products are offered 100
% free to our users and deliver easy 1-click access to the content users want.","age":"Adults only","audience":["Consumer"],"category":["Travel & Navigation"
,"Sports","SysTools & Utilities","Social Networking & Messaging","Shopping","Productivity","Personalization & Search","Games","Health & Fitness","Lifestyle &
 Dating","News & Weather","Books & Reference"],"monetization":["search"],"target":["Windows 7","Windows 8","Windows 10","Windows XP","Windows Vista"]},"valid
Dates":{"validForFilesSignedAfter":"2018-03-13T00:00:00+00:00","validForFilesSignedBefore":"2019-03-13T00:00:00+00:00"},"distribution":{"whitelist":{"landing
Pages":["http://myquickconverter.com/*","http://packageintransit.com/*","http://trackyourpackages.co/*","http://fastpackagetracker.co/*","http://watchtvnow.c
o/*","http://livetvnow.co/*","http://emailaccessonline.com/*","http://myonlinecalendar.co/*","http://mytemplates.co/*","http://textfrompc.co/*","http://wildf
orscrapbooking.com/*","http://dailysocialweb.com/*","http://myphotoeditor.co/*","http://wallstreetwatch.co/*","http://easyconverter.co/*","http://easystreami
```

---

## PEView:

### Image NT headers

- Image file header subsection shows date the program was compiled(usually)
- Ex: dates can be changed (be set to future dates)



```
VirusShare_00ac137b9d26df20c5ec4262aa5a9030
  IMAGE_DOS_HEADER
  IMAGE_DEBUG_TYPE_
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
```

| pFile | Data | Description | Value |
|---|---|---|---|
| 0000010C | 014C | Machine | IMAGE_FILE_MACHINE_I386 |
| 0000010E | 0005 | Number of Sections | |
| 00000110 | 5A153937 | Time Date Stamp | 2017/11/22 Wed 08:45:43 UTC |
| 00000114 | 00000000 | Pointer to Symbol Table | |
| 00000118 | 00000000 | Number of Symbols | |
| 0000011C | 00E0 | Size of Optional Header | |
| 0000011E | 0102 | Characteristics | |
| | | 0002 | IMAGE_FILE_EXECUTABLE_IMAGE |
| | | 0100 | IMAGE_FILE_32BIT_MACHINE |

### Image_Section_Header.text

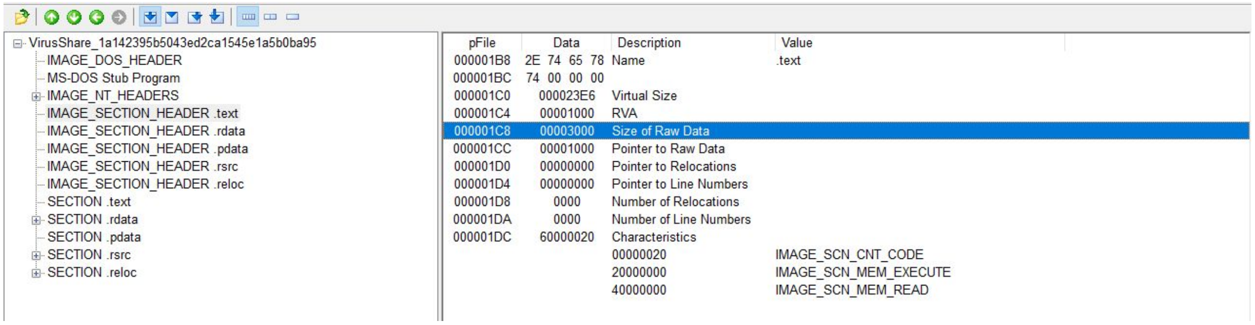
→ Compare **virtual size** to size of **raw data**

→ These sizes should be comparable **unless the program was packed.**

**Results**: After uploading many **virusshare** malware samples to compare virtual size/raw size, **all were comparable**. The next logical step = look for UPX notation for the various sections that would also indicate a packed file. For these particular malware samples, this was not found.

**NOTE:** Sometimes if the malware was designed by experienced authors and not script

| |
|---|
| kiddies using Zues, then UPX may not be called the same thing, therefore sometimes you may need to look in other places for imports |

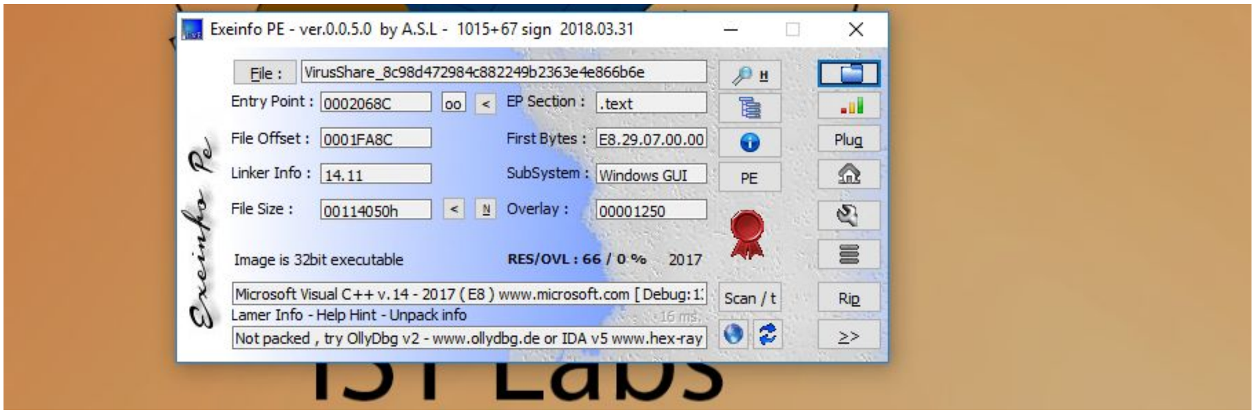


```
VirusShare_1a142395b5043ed2ca1545e1a5b0ba95
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .pdata
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rdata
  SECTION .pdata
  SECTION .rsrc
  SECTION .reloc
```

| pFile | Data | Description | Value |
|---|---|---|---|
| 000001B8 | 2E 74 65 78 | Name | .text |
| 000001BC | 74 00 00 00 | | |
| 000001C0 | 000023E6 | Virtual Size | |
| 000001C4 | 00001000 | RVA | |
| 000001C8 | 00003000 | Size of Raw Data | |
| 000001CC | 00001000 | Pointer to Raw Data | |
| 000001D0 | 00000000 | Pointer to Relocations | |
| 000001D4 | 00000000 | Pointer to Line Numbers | |
| 000001D8 | 0000 | Number of Relocations | |
| 000001DA | 0000 | Number of Line Numbers | |
| 000001DC | 60000020 | Characteristics | |
| | | 00000020 | IMAGE_SCN_CNT_CODE |
| | | 20000000 | IMAGE_SCN_MEM_EXECUTE |
| | | 40000000 | IMAGE_SCN_MEM_READ |

## Section .rdata

| |
|---|
| **Import tables** → are used by pe's that are importing function calls from libraries(dll's) |
| **Export tables** → Dll(libraries) export the addresses of the functions that dll contains to pe's |



Exeinfo PE - ver.0.0.5.0 by A.S.L - 1015+67 sign 2018.03.31

File : VirusShare_8c98d472984c882249b2363e4e866b6e

Entry Point : 0002068C

EP Section : .text

File Offset : 0001FA8C

First Bytes : E8.29.07.00.00

Linker Info : 14.11

SubSystem : Windows GUI

File Size : 00114050h

Overlay : 00001250

Image is 32bit executable

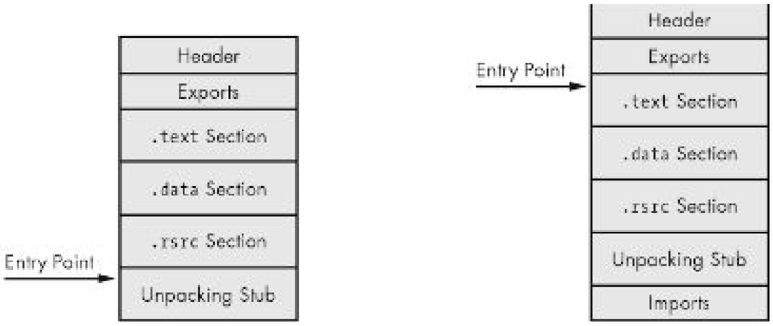
RES/OVL : 66 / 0 % 2017

Microsoft Visual C++ v.14 - 2017 ( E8 ) www.microsoft.com [ Debug:1

Lamer Info - Help Hint - Unpack info 16 ms.

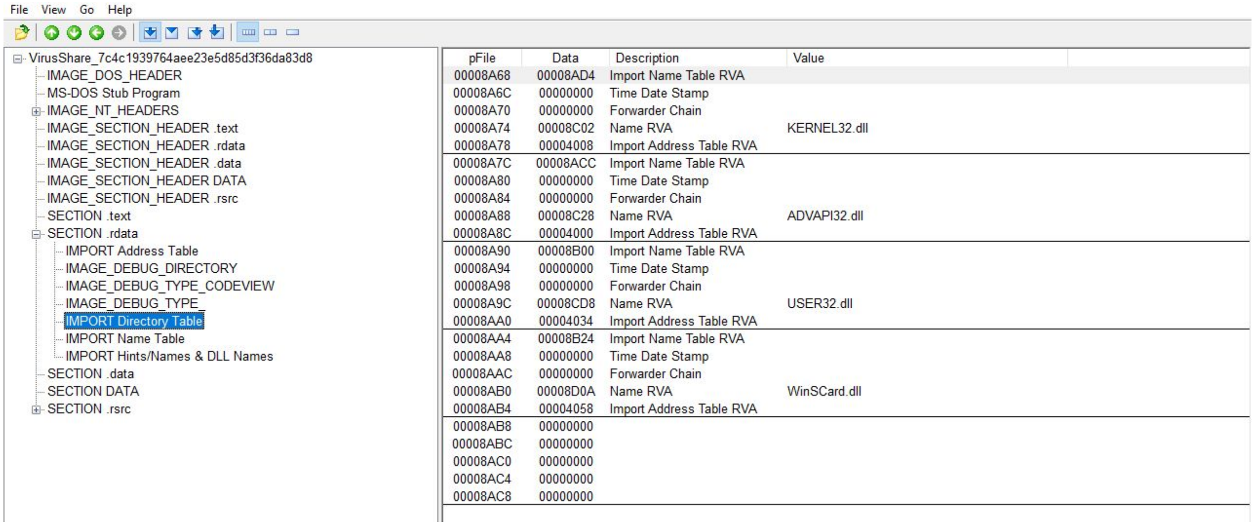
Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

Exeinfo is an additional tool that may help find specific **entry points** and **offsets** to determine malware samples that have been **packed.**



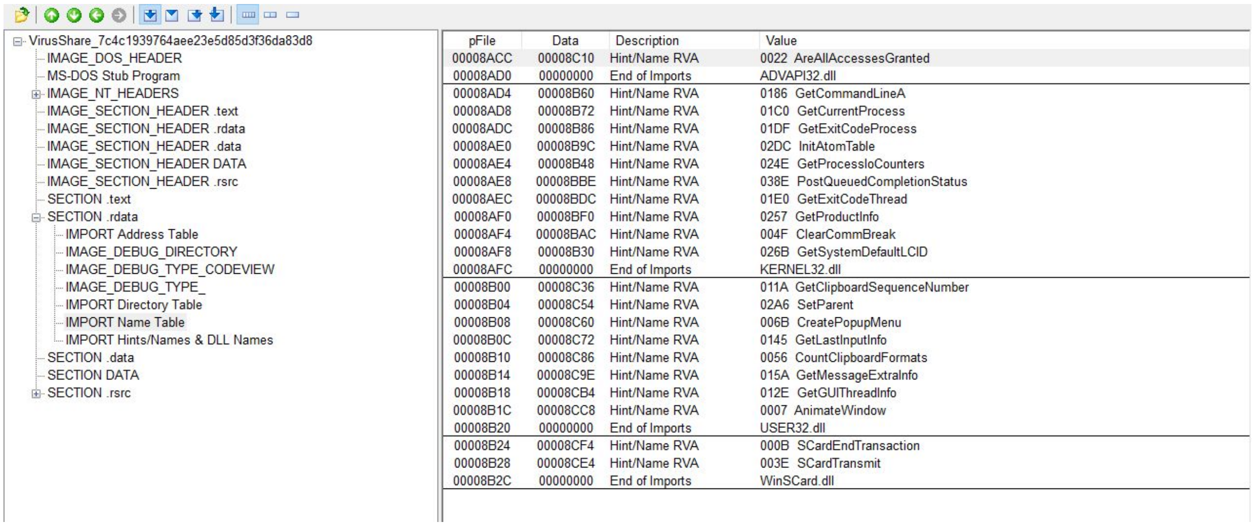
**NOTES: Directory table** only shows the initial imports, which subsequently import all the others seen in the **address** and **name tables.**

**Directory Table: →**



| pFile | Data | Description | Value |
|---|---|---|---|
| 00008A68 | 00008AD4 | Import Name Table RVA | |
| 00008A6C | 00000000 | Time Date Stamp | |
| 00008A70 | 00000000 | Forwarder Chain | |
| 00008A74 | 00008C02 | Name RVA | KERNEL32.dll |
| 00008A78 | 00004008 | Import Address Table RVA | |
| 00008A7C | 00008ACC | Import Name Table RVA | |
| 00008A80 | 00000000 | Time Date Stamp | |
| 00008A84 | 00000000 | Forwarder Chain | |
| 00008A88 | 00008C28 | Name RVA | ADVAPI32.dll |
| 00008A8C | 00004000 | Import Address Table RVA | |
| 00008A90 | 00008B00 | Import Name Table RVA | |
| 00008A94 | 00000000 | Time Date Stamp | |
| 00008A98 | 00000000 | Forwarder Chain | |
| 00008A9C | 00008CD8 | Name RVA | USER32.dll |
| 00008AA0 | 00004034 | Import Address Table RVA | |
| 00008AA4 | 00008B24 | Import Name Table RVA | |
| 00008AA8 | 00000000 | Time Date Stamp | |
| 00008AAC | 00000000 | Forwarder Chain | |
| 00008AB0 | 00008D0A | Name RVA | WinSCard.dll |
| 00008AB4 | 00004058 | Import Address Table RVA | |
| 00008AB8 | 00000000 | | |
| 00008ABC | 00000000 | | |
| 00008AC0 | 00000000 | | |
| 00008AC4 | 00000000 | | |
| 00008AC8 | 00000000 | | |

**Name Table: →**


VirusShare_7c4c1939764aee23e5d85d3f36da83d8
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER DATA
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMAGE_DEBUG_DIRECTORY
IMAGE_DEBUG_TYPE_CODEVIEW
IMAGE_DEBUG_TYPE_
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION DATA
SECTION .rsrc

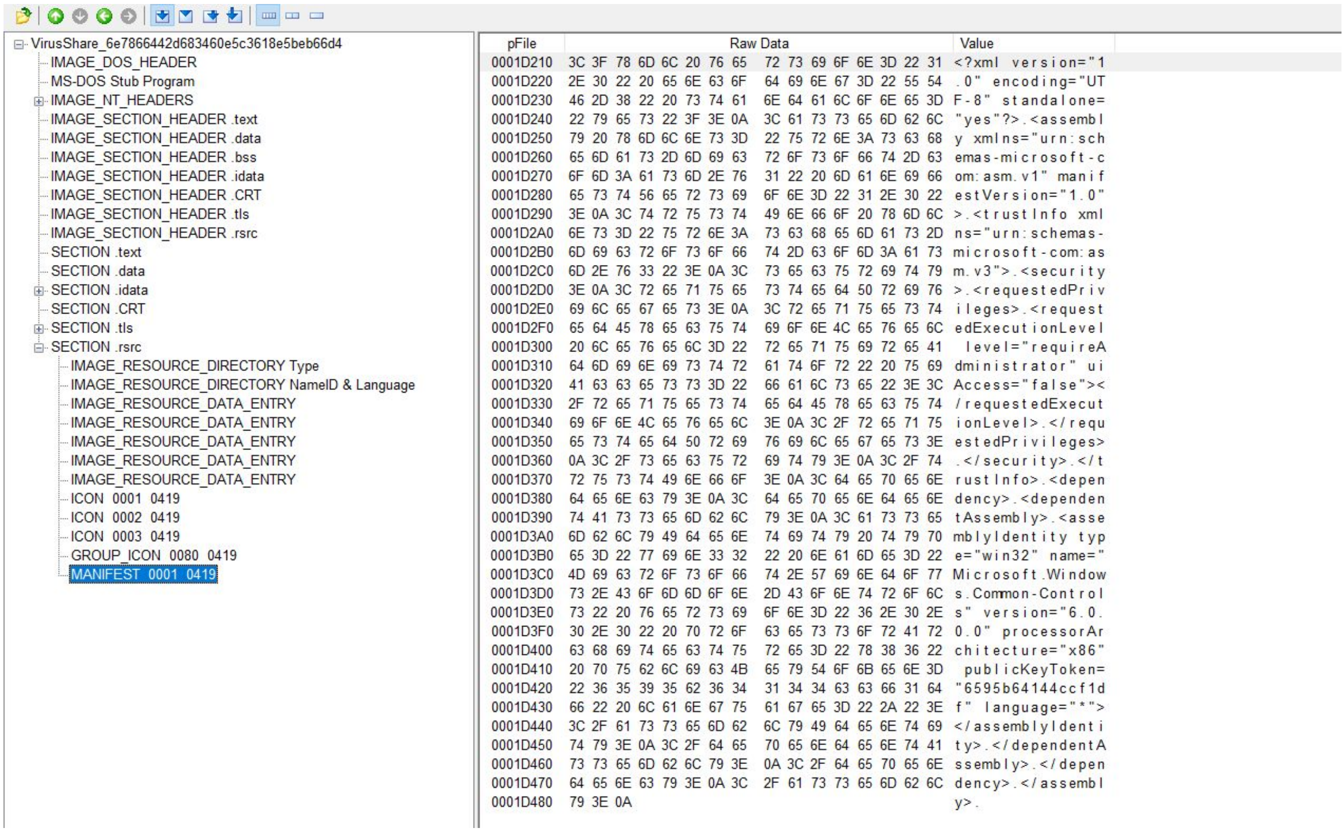
| pFile | Data | Description | Value |
|---|---|---|---|
| 00008ACC | 00008C10 | Hint/Name RVA | 0022 AreAllAccessesGranted |
| 00008AD0 | 00000000 | End of Imports | ADVAPI32.dll |
| 00008AD4 | 00008B60 | Hint/Name RVA | 0186 GetCommandLineA |
| 00008AD8 | 00008B72 | Hint/Name RVA | 01C0 GetCurrentProcess |
| 00008ADC | 00008B86 | Hint/Name RVA | 01DF GetExitCodeProcess |
| 00008AE0 | 00008B9C | Hint/Name RVA | 02DC InitAtomTable |
| 00008AE4 | 00008B48 | Hint/Name RVA | 024E GetProcessIoCounters |
| 00008AE8 | 00008BBE | Hint/Name RVA | 038E PostQueuedCompletionStatus |
| 00008AEC | 00008BDC | Hint/Name RVA | 01E0 GetExitCodeThread |
| 00008AF0 | 00008BF0 | Hint/Name RVA | 0257 GetProductInfo |
| 00008AF4 | 00008BAC | Hint/Name RVA | 004F ClearCommBreak |
| 00008AF8 | 00008B30 | Hint/Name RVA | 026B GetSystemDefaultLCID |
| 00008AFC | 00000000 | End of Imports | KERNEL32.dll |
| 00008B00 | 00008C36 | Hint/Name RVA | 011A GetClipboardSequenceNumber |
| 00008B04 | 00008C54 | Hint/Name RVA | 02A6 SetParent |
| 00008B08 | 00008C60 | Hint/Name RVA | 006B CreatePopupMenu |
| 00008B0C | 00008C72 | Hint/Name RVA | 0145 GetLastInputInfo |
| 00008B10 | 00008C86 | Hint/Name RVA | 0056 CountClipboardFormats |
| 00008B14 | 00008C9E | Hint/Name RVA | 015A GetMessageExtraInfo |
| 00008B18 | 00008CB4 | Hint/Name RVA | 012E GetGUIThreadInfo |
| 00008B1C | 00008CC8 | Hint/Name RVA | 0007 AnimateWindow |
| 00008B20 | 00000000 | End of Imports | USER32.dll |
| 00008B24 | 00008CF4 | Hint/Name RVA | 000B SCardEndTransaction |
| 00008B28 | 00008CE4 | Hint/Name RVA | 003E SCardTransmit |
| 00008B2C | 00000000 | End of Imports | WinSCard.dll |

---

## Section .RSRC:

| |
|---|
| Ex: Image_resource_Data_Entry/Name/Language, Image Resource Directory String |
| **When clicking through each of these sections, all indications(BIN) point to the fact that inside this resource section is another executable (binary)** |

NOTES: The **MZ** header is a dead giveaway(why?) Because these are the initials of an author, It’s a signature for PE files. This and “this program cannot be run in DOS mode”, will usually be found together and indicate malware is present.



```
VirusShare_6e7866442d683460e5c3618e5beb66d4
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  ⊞ IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .data
    IMAGE_SECTION_HEADER .bss
    IMAGE_SECTION_HEADER .idata
    IMAGE_SECTION_HEADER .CRT
    IMAGE_SECTION_HEADER .tls
    IMAGE_SECTION_HEADER .rsrc
    SECTION .text
    SECTION .data
  ⊞ SECTION .idata
    SECTION .CRT
  ⊞ SECTION .tls
  ⊟ SECTION .rsrc
        IMAGE_RESOURCE_DIRECTORY Type
        IMAGE_RESOURCE_DIRECTORY NameID & Language
        IMAGE_RESOURCE_DATA_ENTRY
        IMAGE_RESOURCE_DATA_ENTRY
        IMAGE_RESOURCE_DATA_ENTRY
        IMAGE_RESOURCE_DATA_ENTRY
        IMAGE_RESOURCE_DATA_ENTRY
        ICON  0001  0419
        ICON  0002  0419
        ICON  0003  0419
        GROUP_ICON  0080  0419
        MANIFEST  0001  0419
```

```
pFile     Raw Data                                          Value
0001D210  3C 3F 78 6D 6C 20 76 65  72 73 69 6F 6E 3D 22 31  <?xml version="1
0001D220  2E 30 22 20 65 6E 63 6F  64 69 6E 67 3D 22 55 54  .0" encoding="UT
0001D230  46 2D 38 22 20 73 74 61  6E 64 61 6C 6F 6E 65 3D  F-8" standalone=
0001D240  22 79 65 73 22 3F 3E 0A  3C 61 73 73 65 6D 62 6C  "yes"?>.<assembl
0001D250  79 20 78 6D 6C 6E 73 3D  22 75 72 6E 3A 73 63 68  y xmlns="urn:sch
0001D260  65 6D 61 73 2D 6D 69 63  72 6F 73 6F 66 74 2D 63  emas-microsoft-c
0001D270  6F 6D 3A 61 73 6D 2E 76  31 22 20 6D 61 6E 69 66  om:asm.v1" manif
0001D280  65 73 74 56 65 72 73 69  6F 6E 3D 22 31 2E 30 22  estVersion="1.0"
0001D290  3E 0A 3C 74 72 75 73 74  49 6E 66 6F 20 78 6D 6C  >.<trustInfo xml
0001D2A0  6E 73 3D 22 75 72 6E 3A  73 63 68 65 6D 61 73 2D  ns="urn:schemas-
0001D2B0  6D 69 63 72 6F 73 6F 66  74 2D 63 6F 6D 3A 61 73  microsoft-com:as
0001D2C0  6D 2E 76 33 22 3E 0A 3C  73 65 63 75 72 69 74 79  m.v3">.<security
0001D2D0  3E 0A 3C 72 65 71 75 65  73 74 65 64 50 72 69 76  >.<requestedPriv
0001D2E0  69 6C 65 67 65 73 3E 0A  3C 72 65 71 75 65 73 74  ileges>.<request
0001D2F0  65 64 45 78 65 63 75 74  69 6F 6E 4C 65 76 65 6C  edExecutionLevel
0001D300  20 6C 65 76 65 6C 3D 22  72 65 71 75 69 72 65 41   level="requireA
0001D310  64 6D 69 6E 69 73 74 72  61 74 6F 72 22 20 75 69  dministrator" ui
0001D320  41 63 63 65 73 73 3D 22  66 61 6C 73 65 22 3E 3C  Access="false"><
0001D330  2F 72 65 71 75 65 73 74  65 64 45 78 65 63 75 74  /requestedExecut
0001D340  69 6F 6E 4C 65 76 65 6C  3E 0A 3C 2F 72 65 71 75  ionLevel>.</requ
0001D350  65 73 74 65 64 50 72 69  76 69 6C 65 67 65 73 3E  estedPrivileges>
0001D360  0A 3C 2F 73 65 63 75 72  69 74 79 3E 0A 3C 2F 74  .</security>.</t
0001D370  72 75 73 74 49 6E 66 6F  3E 0A 3C 64 65 70 65 6E  rustInfo>.<depen
0001D380  64 65 6E 63 79 3E 0A 3C  64 65 70 65 6E 64 65 6E  dency>.<dependen
0001D390  74 41 73 73 65 6D 62 6C  79 3E 0A 3C 61 73 73 65  tAssembly>.<asse
0001D3A0  6D 62 6C 79 49 64 65 6E  74 69 74 79 20 74 79 70  mblyIdentity typ
0001D3B0  65 3D 22 77 69 6E 33 32  22 20 6E 61 6D 65 3D 22  e="win32" name="
0001D3C0  4D 69 63 72 6F 73 6F 66  74 2E 57 69 6E 64 6F 77  Microsoft.Window
0001D3D0  73 2E 43 6F 6D 6D 6F 6E  2D 43 6F 6E 74 72 6F 6C  s.Common-Control
0001D3E0  73 22 20 76 65 72 73 69  6F 6E 3D 22 36 2E 30 2E  s" version="6.0.
0001D3F0  30 2E 30 22 20 70 72 6F  63 65 73 73 6F 72 41 72  0.0" processorAr
0001D400  63 68 69 74 65 63 74 75  72 65 3D 22 78 38 36 22  chitecture="x86"
0001D410  20 70 75 62 6C 69 63 4B  65 79 54 6F 6B 65 6E 3D   publicKeyToken=
0001D420  22 36 35 39 35 62 36 34  31 34 34 63 63 66 31 64  "6595b64144ccf1d
0001D430  66 22 20 6C 61 6E 67 75  61 67 65 3D 22 2A 22 3E  f" language="*">
0001D440  3C 2F 61 73 73 65 6D 62  6C 79 49 64 65 6E 74 69  </assemblyIdenti
0001D450  74 79 3E 0A 3C 2F 64 65  70 65 6E 64 65 6E 74 41  ty>.</dependentA
0001D460  73 73 65 6D 62 6C 79 3E  0A 3C 2F 64 65 70 65 6E  ssembly>.</depen
0001D470  64 65 6E 63 79 3E 0A 3C  2F 61 73 73 65 6D 62 6C  dency>.</assembl
0001D480  79 3E 0A                                          y>.
```

**Results**: Unable to locate bin values in any **rsrc sections.** Saw values like ‘icon’, ‘bitmap’, ‘dialogue’ ‘string’, etc,. but not ‘bin’. However did see ‘manifest’ with what appears to also look like interesting inputs. Without understanding the purpose of the malware, it is difficult say.

**B**ecause no binary was found in many virusshare malware samples, Resource Hacker will be skipped. But, if we did run resource hacker→

After opening the file we should see that it is indeed it’s own binary file

Now, when we look at the imports → we can see that things will be executed / downloaded

## Section UPX:

NOTES**:** When expanding the UPX section and viewing the different input tables, you can see imports but in a packed file, it is common for more imports to be called.

### How to decompress a compressed file and save it as a new file

```
Upx(invoke application) -o(output) “absolute reference of destination file .exe“ -d(decompress)
“path to file that we want to decompress”
```

### Result: When you look through the import tables, imports should be greatly expanded

Unfortunately, running over 50 virusshare malware samples through peview did not recreate the UPX section.

### PART 2:
### Basic Dynamic Analysis

---

Involves executing malware, finding artifacts created on system (folders/files, services, keys)
→ This is only meant to be a second step in the analysis process

### Sandboxes:

- By running the malware in a sandbox, you mitigate the risk of infecting your system
- Sandboxes automate most of the basic dynamic analysis process
- Most sandboxes will not identify or categorize the malware, instead they will provide log output, leaving the determinations up to the analysts

### RegShot:

Steps to using RegShot:

→ Take a snapshot of the state of the system with reg shot

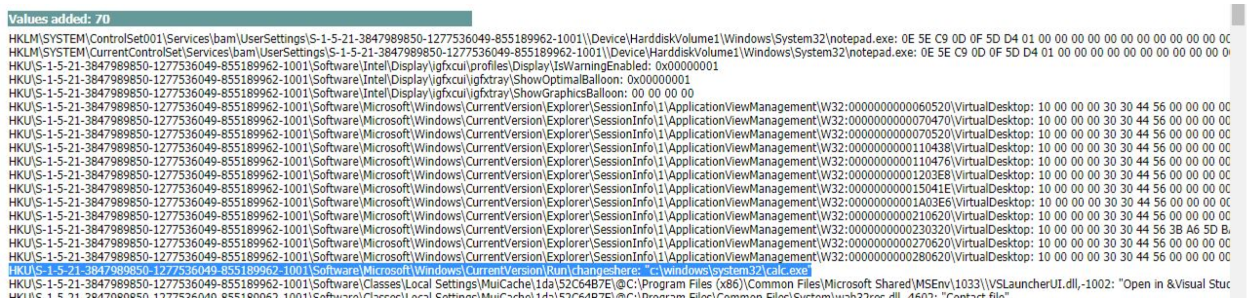
→ Simulate malware going into a certain file directory using registry editor regedit

→ Create value that starts application .exe and/ or write to hard drive by making a new folder and file

Then, take a second shot & click compare..

**Results:** Should present in an html file and indicate changes in “files added”,  “folders added”, “Values added”

### Values added = C:\windows\system32\calc.exe



```
Values added: 70
HKLM\SYSTEM\ControlSet001\Services\bam\UserSettings\S-1-5-21-3847989850-1277536049-855189962-1001\\Device\HarddiskVolume1\Windows\System32\notepad.exe: 0E 5E C9 0D 0F 5D D4 01 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-3847989850-1277536049-855189962-1001\\Device\HarddiskVolume1\Windows\System32\notepad.exe: 0E 5E C9 0D 0F 5D D4 01 00 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Intel\Display\igfxcui\profiles\Display\IsWarningEnabled: 0x00000001
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Intel\Display\igfxcui\igfxtray\ShowOptimalBalloon: 0x00000001
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Intel\Display\igfxcui\igfxtray\ShowGraphicsBalloon: 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000060520\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000070470\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000070520\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000110438\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000110476\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001203E8\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000015041E\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001A03E6\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 0C
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000210620\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000230320\VirtualDesktop: 10 00 00 00 30 30 44 56 3B A6 5D B
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000270620\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000280620\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Microsoft\Windows\CurrentVersion\Run\changeshere: "c:\windows\system32\calc.exe"
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Classes\Local Settings\MuiCache\1da\52C64B7E\@C:\Program Files (x86)\Common Files\Microsoft Shared\MSEnv\1033\\VSLauncherUI.dll,-1002: "Open in &Visual Stuc
HKU\S-1-5-21-3847989850-1277536049-855189962-1001\Software\Classes\Local Settings\MuiCache\1da\52C64B7E\@C:\Program Files\Common Files\System\wab32res.dll,-4602: "Contact file"
```

## Process Explorer:

### How to analyze current processes with Process Explorer:

→ The process column on the left will list current processes. Ex: chrome.exe

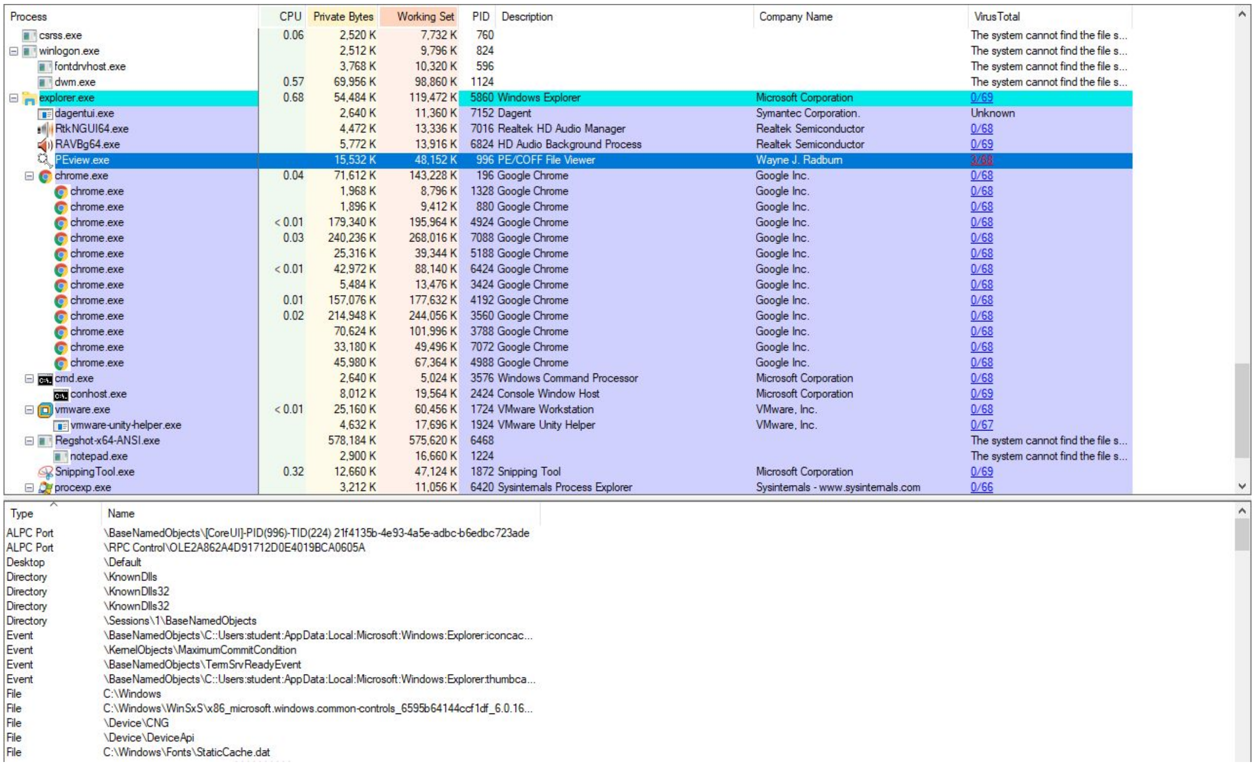
→ In the lower pane, you can see all the associated handles

→ A process handle is an integer value that identifies a process to windows

→ Process explorer also allows you to check virustotal and include the results

→ Check to see if virustotal flags any of the processes

**Looks like virustotal spotted some malware inside PEView. I thought this was pretty cool.**

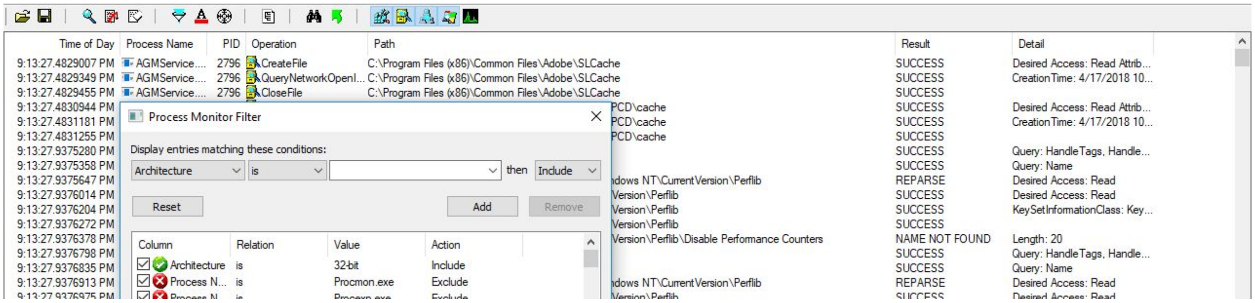


| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | VirusTotal |
|---|---|---|---|---|---|---|---|
| csrss.exe | 0.06 | 2,520 K | 7,732 K | 760 | | | The system cannot find the file s... |
| winlogon.exe | | 2,512 K | 9,796 K | 824 | | | The system cannot find the file s... |
| fontdrvhost.exe | | 3,768 K | 10,320 K | 596 | | | The system cannot find the file s... |
| dwm.exe | 0.57 | 69,956 K | 98,860 K | 1124 | | | The system cannot find the file s... |
| explorer.exe | 0.68 | 54,484 K | 119,472 K | 5860 | Windows Explorer | Microsoft Corporation | 0/69 |
| dagentui.exe | | 2,640 K | 11,360 K | 7152 | Dagent | Symantec Corporation. | Unknown |
| RtkNGUI64.exe | | 4,472 K | 13,336 K | 7016 | Realtek HD Audio Manager | Realtek Semiconductor | 0/68 |
| RAVBg64.exe | | 5,772 K | 13,916 K | 6824 | HD Audio Background Process | Realtek Semiconductor | 0/69 |
| PEview.exe | | 15,532 K | 48,152 K | 996 | PE/COFF File Viewer | Wayne J. Radburn | 3/68 |
| chrome.exe | 0.04 | 71,612 K | 143,228 K | 196 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 1,968 K | 8,796 K | 1328 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 1,896 K | 9,412 K | 880 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | < 0.01 | 179,340 K | 195,964 K | 4924 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | 0.03 | 240,236 K | 268,016 K | 7088 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 25,316 K | 39,344 K | 5188 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | < 0.01 | 42,972 K | 88,140 K | 6424 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 5,484 K | 13,476 K | 3424 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | 0.01 | 157,076 K | 177,632 K | 4192 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | 0.02 | 214,948 K | 244,056 K | 3560 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 70,624 K | 101,996 K | 3788 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 33,180 K | 49,496 K | 7072 | Google Chrome | Google Inc. | 0/68 |
| chrome.exe | | 45,980 K | 67,364 K | 4988 | Google Chrome | Google Inc. | 0/68 |
| cmd.exe | | 2,640 K | 5,024 K | 3576 | Windows Command Processor | Microsoft Corporation | 0/68 |
| conhost.exe | | 8,012 K | 19,564 K | 2424 | Console Window Host | Microsoft Corporation | 0/69 |
| vmware.exe | < 0.01 | 25,160 K | 60,456 K | 1724 | VMware Workstation | VMware, Inc. | 0/68 |
| vmware-unity-helper.exe | | 4,632 K | 17,696 K | 1924 | VMware Unity Helper | VMware, Inc. | 0/67 |
| Regshot-x64-ANSI.exe | | 578,184 K | 575,620 K | 6468 | | | The system cannot find the file s... |
| notepad.exe | | 2,900 K | 16,660 K | 1224 | | | The system cannot find the file s... |
| SnippingTool.exe | 0.32 | 12,660 K | 47,124 K | 1872 | Snipping Tool | Microsoft Corporation | 0/69 |
| procexp.exe | | 3,212 K | 11,056 K | 6420 | Sysinternals Process Explorer | Sysinternals - www.sysinternals.com | 0/66 |

| Type | Name |
|---|---|
| ALPC Port | \BaseNamedObjects\[CoreUI]-PID(996)-TID(224) 21f4135b-4e93-4a5e-adbc-b6edbc723ade |
| ALPC Port | \RPC Control\OLE2A862A4D91712D0E4019BCA0605A |
| Desktop | \Default |
| Directory | \KnownDlls |
| Directory | \KnownDlls32 |
| Directory | \KnownDlls32 |
| Directory | \Sessions\1\BaseNamedObjects |
| Event | \BaseNamedObjects\C::Users:student:AppData:Local:Microsoft:Windows:Explorer:iconcac... |
| Event | \KernelObjects\MaximumCommitCondition |
| Event | \BaseNamedObjects\TermSrvReadyEvent |
| Event | \BaseNamedObjects\C::Users:student:AppData:Local:Microsoft:Windows:Explorer:thumbca... |
| File | C:\Windows |
| File | C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.16... |
| File | \Device\CNG |
| File | \Device\DeviceApi |
| File | C:\Windows\Fonts\StaticCache.dat |

## Process Monitor:

| |
|---|
| → Process monitor will allow you to see activity with registry keys, processes and DLL’s |
| → Use the filter to reduce the events (ex: architecture) |
| → See related registry keys, processes and DLL’s |
| → The process tree also displays a hierarchical look at all the processes |



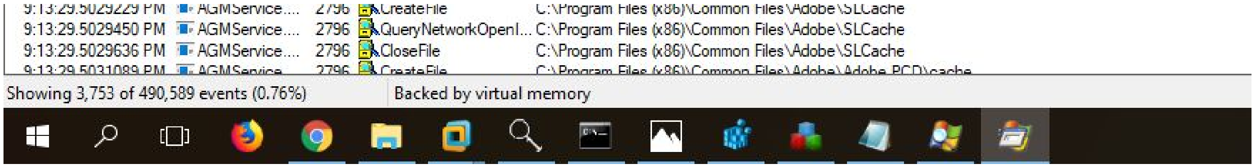
```
Time of Day          Process Name     PID   Operation            Path                                              Result            Detail
9:13:27.4829007 PM   AGMService....   2796  CreateFile           C:\Program Files (x86)\Common Files\Adobe\SLCache  SUCCESS           Desired Access: Read Attrib...
9:13:27.4829349 PM   AGMService....   2796  QueryNetworkOpenI... C:\Program Files (x86)\Common Files\Adobe\SLCache  SUCCESS           CreationTime: 4/17/2018 10...
9:13:27.4829455 PM   AGMService....   2796  CloseFile            C:\Program Files (x86)\Common Files\Adobe\SLCache  SUCCESS
9:13:27.4830944 PM                                               PCD\cache                                          SUCCESS           Desired Access: Read Attrib...
9:13:27.4831181 PM                                               PCD\cache                                          SUCCESS           CreationTime: 4/17/2018 10...
9:13:27.4831255 PM                                               PCD\cache                                          SUCCESS
9:13:27.9375280 PM                                                                                                  SUCCESS           Query: HandleTags, Handle...
9:13:27.9375358 PM                                                                                                  SUCCESS           Query: Name
9:13:27.9375647 PM                                               ıdows NT\CurrentVersion\Perflib                    REPARSE           Desired Access: Read
9:13:27.9376014 PM                                               Version\Perflib                                    SUCCESS           Desired Access: Read
9:13:27.9376204 PM                                               Version\Perflib                                    SUCCESS           KeySetInformationClass: Key...
9:13:27.9376272 PM                                               Version\Perflib                                    SUCCESS
9:13:27.9376378 PM                                               Version\Perflib\Disable Performance Counters       NAME NOT FOUND    Length: 20
9:13:27.9376798 PM                                                                                                  SUCCESS           Query: HandleTags, Handle...
9:13:27.9376835 PM                                                                                                  SUCCESS           Query: Name
9:13:27.9376913 PM                                               ıdows NT\CurrentVersion\Perflib                    REPARSE           Desired Access: Read
9:13:27.9376975 PM                                               Version\Perflib                                    SUCCESS           Desired Access: Read
```

Process Monitor Filter

Display entries matching these conditions:

Architecture | is | | then | Include

| Column | Relation | Value | Action |
|---|---|---|---|
| ☑ Architecture | is | 32-bit | Include |
| ☑ Process N... | is | Procmon.exe | Exclude |
| ☑ Process N... | is | Procexp.exe | Exclude |

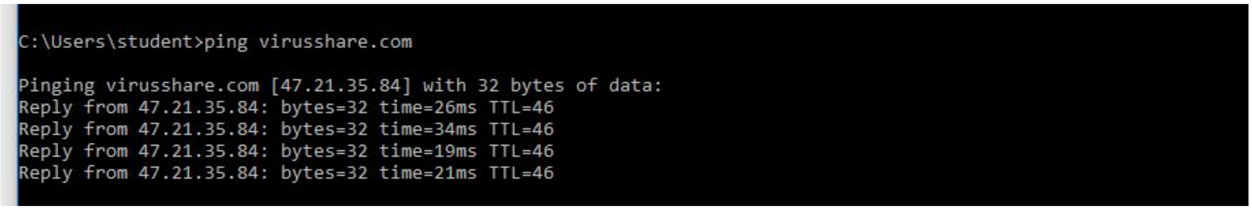


```
9:13:29.5029229 PM   AGMService....   2796  CreateFile           C:\Program Files (x86)\Common Files\Adobe\SLCache
9:13:29.5029450 PM   AGMService....   2796  QueryNetworkOpenI... C:\Program Files (x86)\Common Files\Adobe\SLCache
9:13:29.5029636 PM   AGMService....   2796  CloseFile            C:\Program Files (x86)\Common Files\Adobe\SLCache
9:13:29.5031089 PM   AGMService....   2796  CreateFile           C:\Program Files (x86)\Common Files\Adobe\Adobe PCD\cache
Showing 3,753 of 490,589 events (0.76%)     Backed by virtual memory
```

## ApateDNS

- FQDN’s (fully qualified domain names) can be embedded inside malware
- These are more common than Ip’s  b/c the host of those services can frequently change. https://serverfault.com/questions/788862/why-should-i-use-an-fqdn-instead-of-the-servers-ip-address
- set up a fake DNS server to spoof responses from what the the fake DNS server
- put a loopback address of 127.0.01
- This is will be the reply for any question that the malware asks the dns server
- Netstat -an | more
- Port 53 (dns) should be open and running on the local machine When running ipconfig /all → the DNS server will be queriing the fake dns local machine 127.0.0.1
- With the apatedns window open, ping any random website, to receive a successful reply in cmd. But also you will see the FQDN in the apatedns window

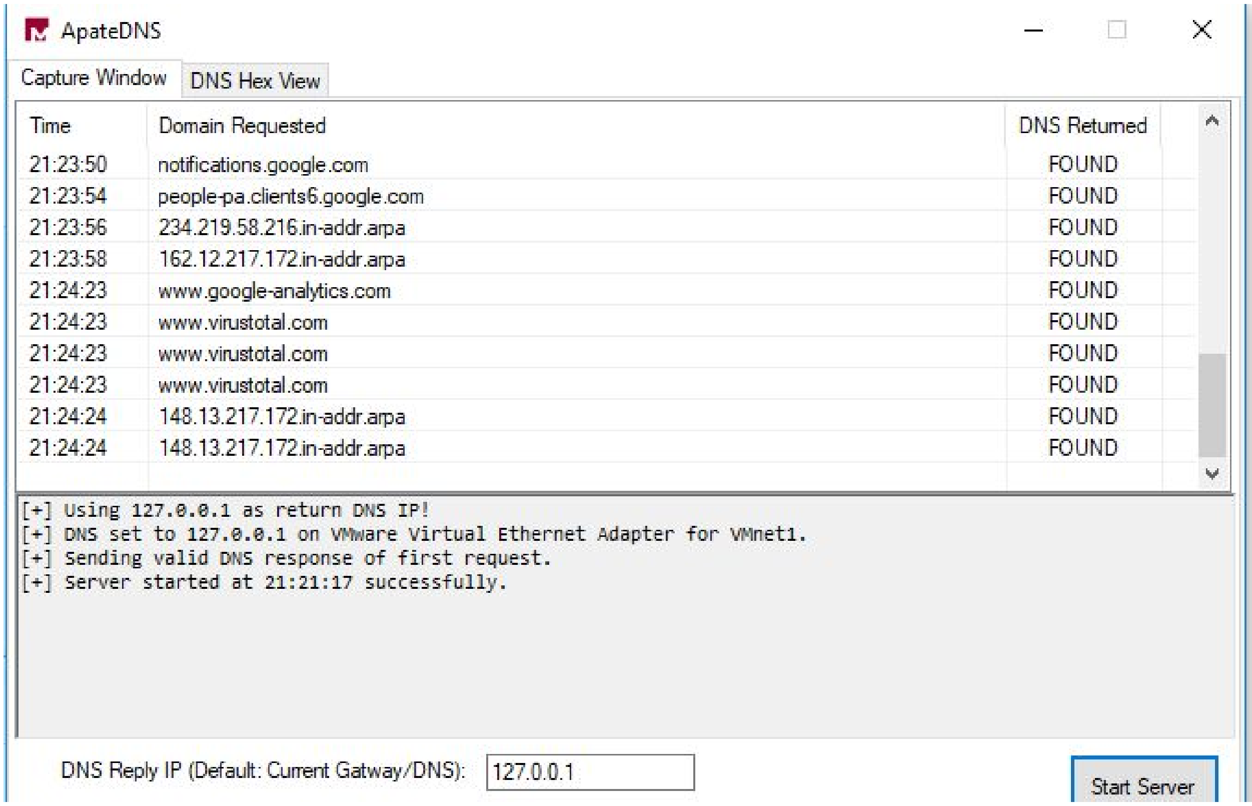
**NOTE: ping any random website, to receive a successful reply in cmd.**



```
C:\Users\student>ping virusshare.com

Pinging virusshare.com [47.21.35.84] with 32 bytes of data:
Reply from 47.21.35.84: bytes=32 time=26ms TTL=46
Reply from 47.21.35.84: bytes=32 time=34ms TTL=46
Reply from 47.21.35.84: bytes=32 time=19ms TTL=46
Reply from 47.21.35.84: bytes=32 time=21ms TTL=46
```

**NOTE: See the FQDN in the apatedns window**



| Time | Domain Requested | DNS Returned |
|---|---|---|
| 21:23:50 | notifications.google.com | FOUND |
| 21:23:54 | people-pa.clients6.google.com | FOUND |
| 21:23:56 | 234.219.58.216.in-addr.arpa | FOUND |
| 21:23:58 | 162.12.217.172.in-addr.arpa | FOUND |
| 21:24:23 | www.google-analytics.com | FOUND |
| 21:24:23 | www.virustotal.com | FOUND |
| 21:24:23 | www.virustotal.com | FOUND |
| 21:24:23 | www.virustotal.com | FOUND |
| 21:24:24 | 148.13.217.172.in-addr.arpa | FOUND |
| 21:24:24 | 148.13.217.172.in-addr.arpa | FOUND |

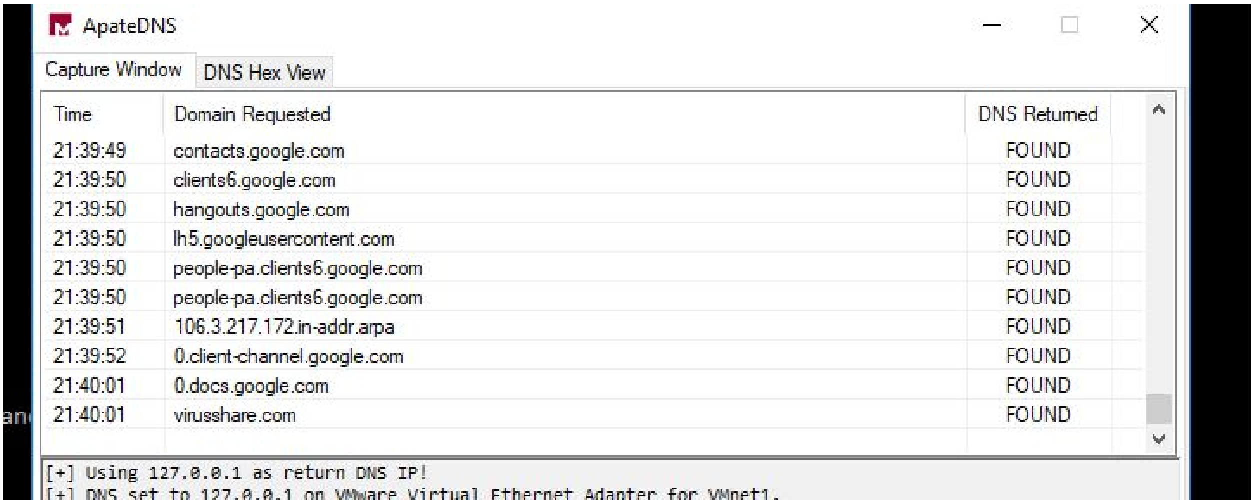
```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on VMware Virtual Ethernet Adapter for VMnet1.
[+] Sending valid DNS response of first request.
[+] Server started at 21:21:17 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1

## Netcat:

- Restart apateDNS to spoof all dns replies (127.0.0.1) 0 NX domains
- netcat listener on port 80(common malware port) (cd to netcat directory, nc -l -p 80)
- Visit website and watch all the information sent from the malware to its c2 server (of course this is just a simulation), but if real maware was communicating with its c2 server, we would see the actual commands !

**NOTE: watch all the information sent from the malware to its c2 server**



| Time | Domain Requested | DNS Returned |
|---|---|---|
| 21:39:49 | contacts.google.com | FOUND |
| 21:39:50 | clients6.google.com | FOUND |
| 21:39:50 | hangouts.google.com | FOUND |
| 21:39:50 | lh5.googleusercontent.com | FOUND |
| 21:39:50 | people-pa.clients6.google.com | FOUND |
| 21:39:50 | people-pa.clients6.google.com | FOUND |
| 21:39:51 | 106.3.217.172.in-addr.arpa | FOUND |
| 21:39:52 | 0.client-channel.google.com | FOUND |
| 21:40:01 | 0.docs.google.com | FOUND |
| 21:40:01 | virusshare.com | FOUND |

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on VMware Virtual Ethernet Adapter for VMnet1.
```