# CNIT 58100 CFM: CYBERFORENSICS OF MALWARE – LAB 2 & 3 (PART 1)

**Ibrahim Waziri Jr**

PhD in Information Security (CERIAS)

Lab 2 & 3 – Part 1

Due on: September 10th, 2014 (Week 2)

Instructor: **Associate Prof Sam Liles**

Purdue University

2014

# Abstract

This lab covers the skills discussed in chapter 2 and 3 of the text. The practice covered in these labs is all based on malware analysis. The malware files used are provided as an extension of the text for practical purposes.

Each of the labs consists of multiple questions that require short answers. Depending on the question, certain special tools might be required to fully analyze the malware and find answers to the question.

This paper provides answers to Chapter 2 and 3 labs. The lab uses 4 different files which are: *Lab03-01.exe, Lab03-02.dll, Lab03-03.exe*, and *Lab03-04.exe*. These files are malwares and therefore could be harmful if used for non-training purposes.

The tools used to analyze the files used in this lab are: Virustools, PEview, Resource Hacker, Wireshark, Procmon, ApateDNS, and Regshot. The results collected after analyzing the files includes: malware's imports and strings, processes under which the malware is running, malware indicators, network-based signatures for the malware, malware behavior etc.

## Lab 3-1

Analyze the malware found in the file Lab03-01.exe using basic dynamic analysis tools.

**Questions:**

Q1: What are this malware's imports and strings?

Q2: What are the malware's host-based indicators?

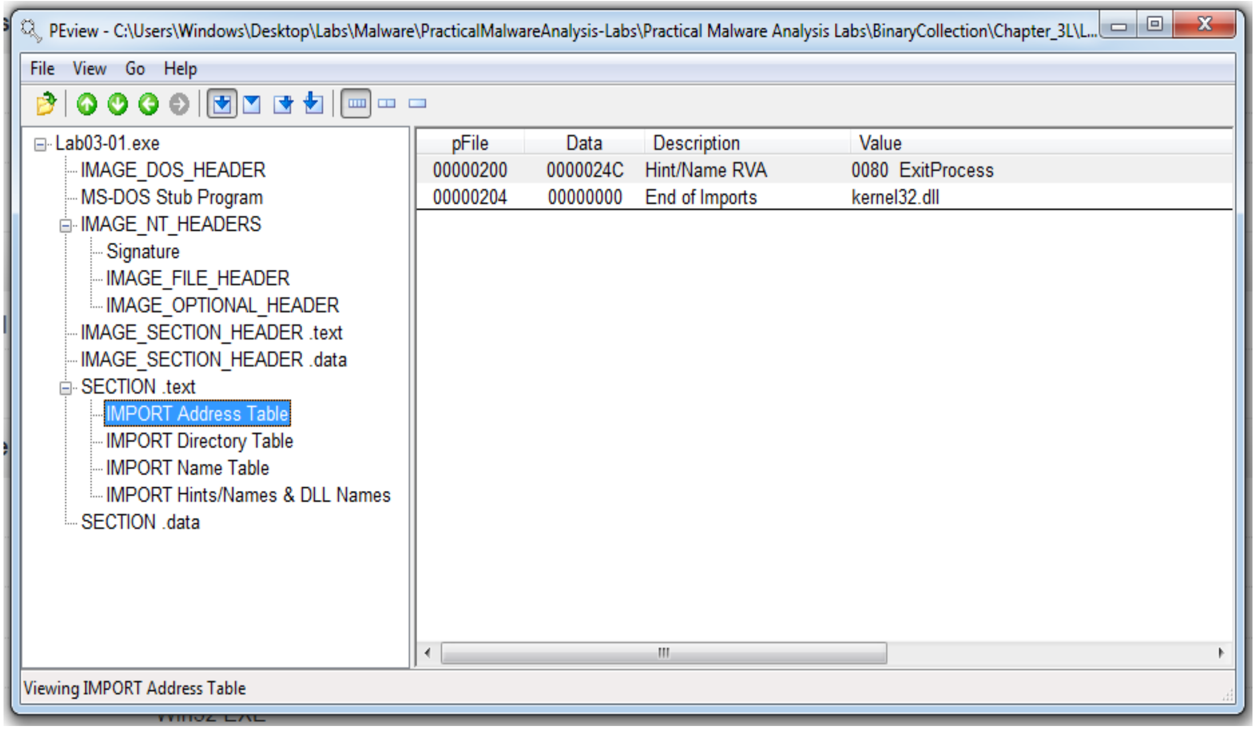
Q3: Are there any useful network-based signatures for this malware? If so, what are they?

**Answers:**

1: First, the malware is packed. And it only has one import *ExitProcess*. However the strings are clear.

Analyzing the malware using basic analysis technique and looking at the malware's PEview file structure and strings. Proves that only *kernel32.dll* is imported.

Figure 1 and 2 below shows the basic analysis of the malware using PEview and virustotal.

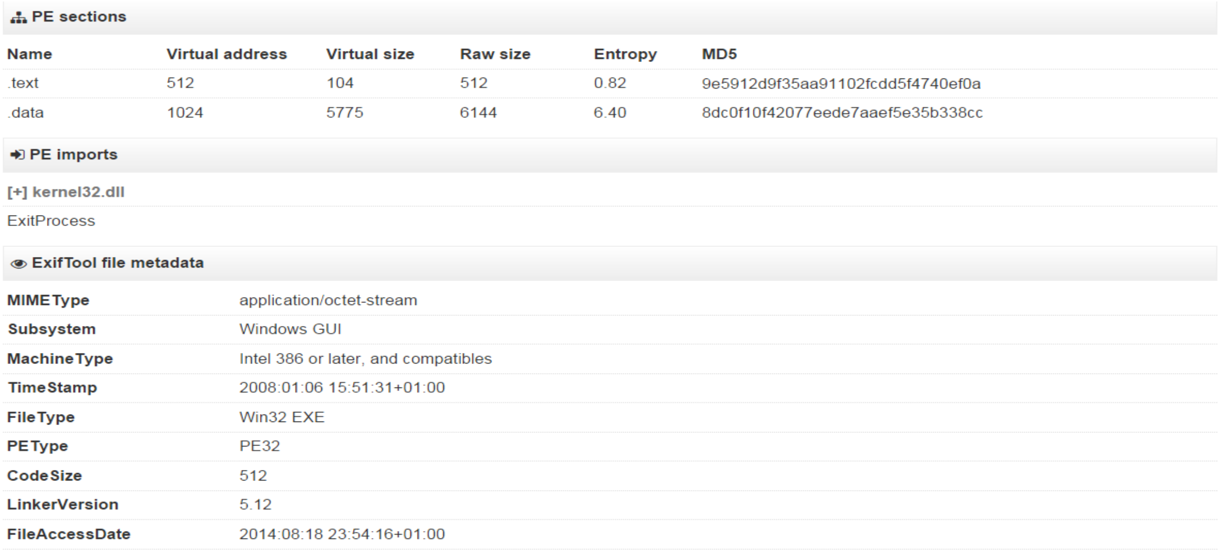


PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\L...

| pFile | Data | Description | Value |
|---|---|---|---|
| 00000200 | 0000024C | Hint/Name RVA | 0080 ExitProcess |
| 00000204 | 00000000 | End of Imports | kernel32.dll |

Viewing IMPORT Address Table

Figure 1: Lab03-01.exe Import analysis using PEview



PE sections

| Name | Virtual address | Virtual size | Raw size | Entropy | MD5 |
|---|---|---|---|---|---|
| .text | 512 | 104 | 512 | 0.82 | 9e5912d9f35aa91102fcdd5f4740ef0a |
| .data | 1024 | 5775 | 6144 | 6.40 | 8dc0f10f42077eede7aaef5e35b338cc |

PE imports

[+] kernel32.dll

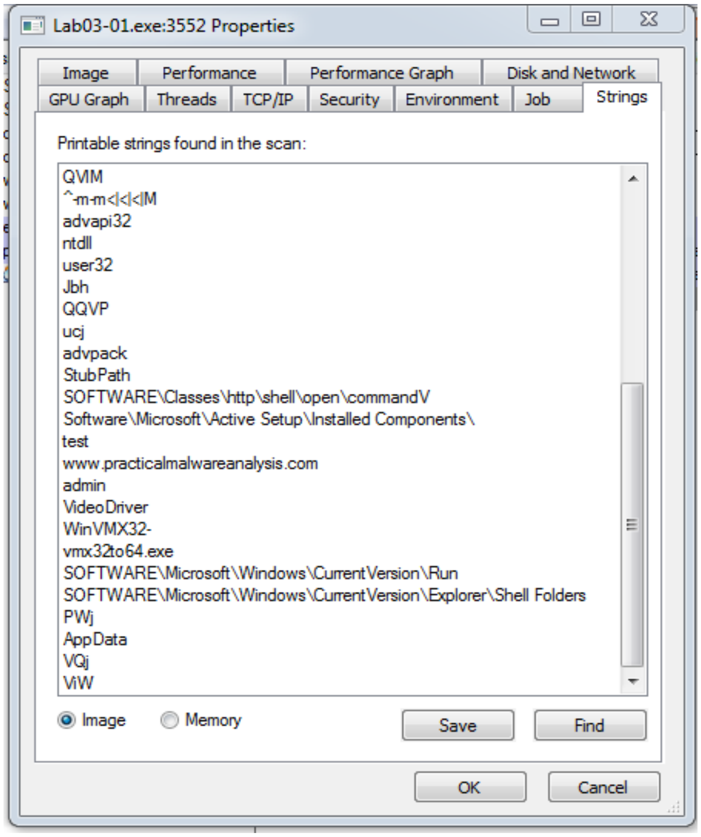
ExitProcess

ExifTool file metadata

| | |
|---|---|
| MIMEType | application/octet-stream |
| Subsystem | Windows GUI |
| MachineType | Intel 386 or later, and compatibles |
| TimeStamp | 2008:01:06 15:51:31+01:00 |
| FileType | Win32 EXE |
| PEType | PE32 |
| CodeSize | 512 |
| LinkerVersion | 5.12 |
| FileAccessDate | 2014:08:18 23:54:16+01:00 |

Figure 2: Lab03-01.exe Import analysis using virustotal

Considering the file is packed, we wouldn’t expect to see strings; however there are some interesting strings such as *WInVMX32, VideoDriver* etc.Figure 3 below shows the strings captured using process explorer.

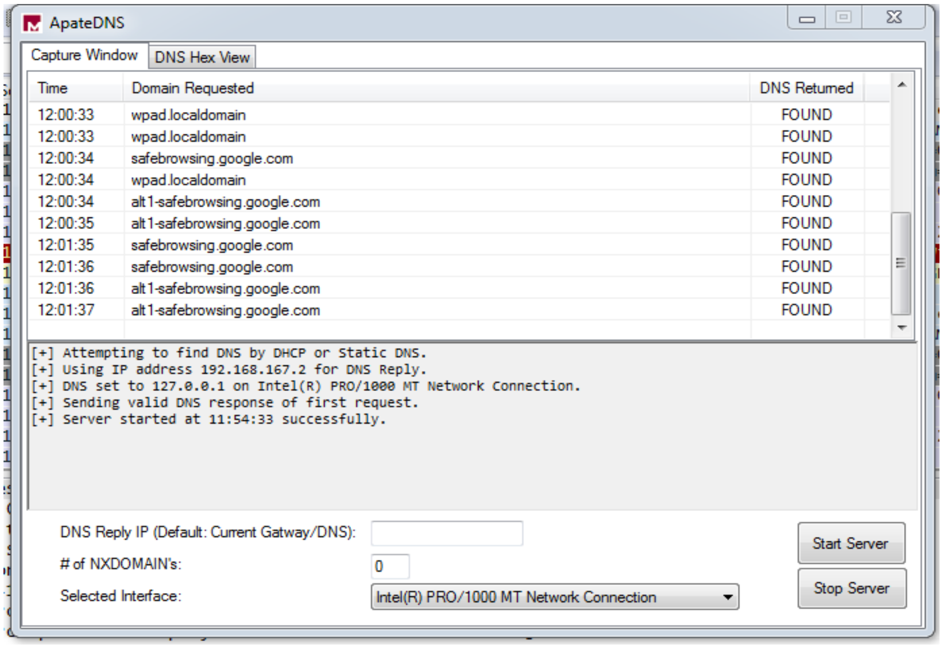


Printable strings found in the scan:

```
QVIM
^-m-m<|<|<|M
advapi32
ntdll
user32
Jbh
QQVP
ucj
advpack
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
VQj
ViW
```

Figure 3: Lab03-01.exe strings captured using Process Explorer

2. One of the host-based indicators is a mutex created by the malware. As seen in the strings in figure 3 above. The mutex *WinVMX32* is created by the malware. Before running the malware, we run **Procmon** and clear all the events. Using **ApateDNS** and **Wireshark** as shown in figure 4 and 5 below:



| Time | Domain Requested | DNS Returned |
|---|---|---|
| 12:00:33 | wpad.localdomain | FOUND |
| 12:00:33 | wpad.localdomain | FOUND |
| 12:00:34 | safebrowsing.google.com | FOUND |
| 12:00:34 | wpad.localdomain | FOUND |
| 12:00:34 | alt1-safebrowsing.google.com | FOUND |
| 12:00:35 | alt1-safebrowsing.google.com | FOUND |
| 12:01:35 | safebrowsing.google.com | FOUND |
| 12:01:36 | safebrowsing.google.com | FOUND |
| 12:01:36 | alt1-safebrowsing.google.com | FOUND |
| 12:01:37 | alt1-safebrowsing.google.com | FOUND |

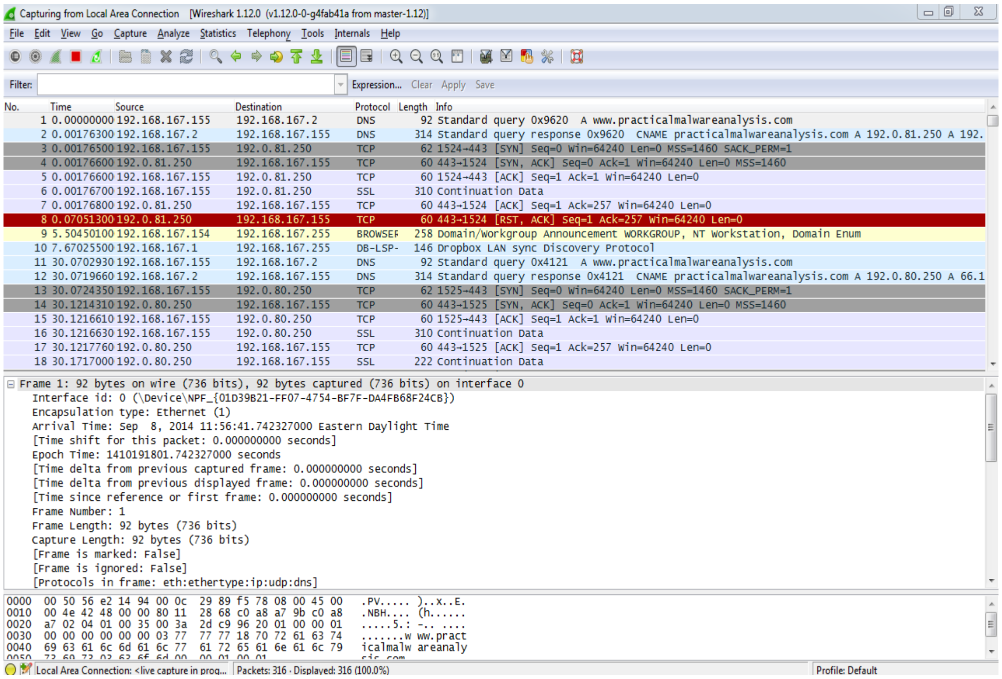
```
[+] Attempting to find DNS by DHCP or Static DNS.
[+] Using IP address 192.168.167.2 for DNS Reply.
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Network Connection.
[+] Sending valid DNS response of first request.
[+] Server started at 11:54:33 successfully.
```

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

# of NXDOMAIN's: 0

Selected Interface: Intel(R) PRO/1000 MT Network Connection

Figure 4: ApateDNS



```
No.  Time       Source          Destination     Protocol Length Info
   1 0.00000000 192.168.167.155 192.168.167.2   DNS       92 Standard query 0x9620  A www.practicalmalwareanalysis.com
   2 0.00176300 192.168.167.2   192.168.167.155 DNS      314 Standard query response 0x9620  CNAME practicalmalwareanalysis.com A 192.0.81.250 A 192.
   3 0.00176500 192.168.167.155 192.0.81.250    TCP       62 1524→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   4 0.00176600 192.0.81.250    192.168.167.155 TCP       60 443→1524 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   5 0.00176600 192.168.167.155 192.0.81.250    TCP       60 1524→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   6 0.00176700 192.168.167.155 192.0.81.250    SSL      310 Continuation Data
   7 0.00176800 192.0.81.250    192.168.167.155 TCP       60 443→1524 [ACK] Seq=1 Ack=257 Win=64240 Len=0
   8 0.07051300 192.0.81.250    192.168.167.155 TCP       60 443→1524 [RST, ACK] Seq=1 Ack=257 Win=64240 Len=0
   9 5.50450100 192.168.167.154 192.168.167.255 BROWSEF  258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
  10 7.67025500 192.168.167.1   192.168.167.255 DB-LSP-  146 Dropbox LAN sync Discovery Protocol
  11 30.0702930 192.168.167.155 192.168.167.2   DNS       92 Standard query 0x4121  A www.practicalmalwareanalysis.com
  12 30.0719660 192.168.167.2   192.168.167.155 DNS      314 Standard query response 0x4121  CNAME practicalmalwareanalysis.com A 192.0.80.250 A 66.1
  13 30.0724350 192.168.167.155 192.0.80.250    TCP       62 1525→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  14 30.1214310 192.0.80.250    192.168.167.155 TCP       60 443→1525 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  15 30.1216610 192.168.167.155 192.0.80.250    TCP       60 1525→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  16 30.1216630 192.168.167.155 192.0.80.250    SSL      310 Continuation Data
  17 30.1217760 192.0.80.250    192.168.167.155 TCP       60 443→1525 [ACK] Seq=1 Ack=257 Win=64240 Len=0
  18 30.1717000 192.0.80.250    192.168.167.155 SSL      222 Continuation Data
```

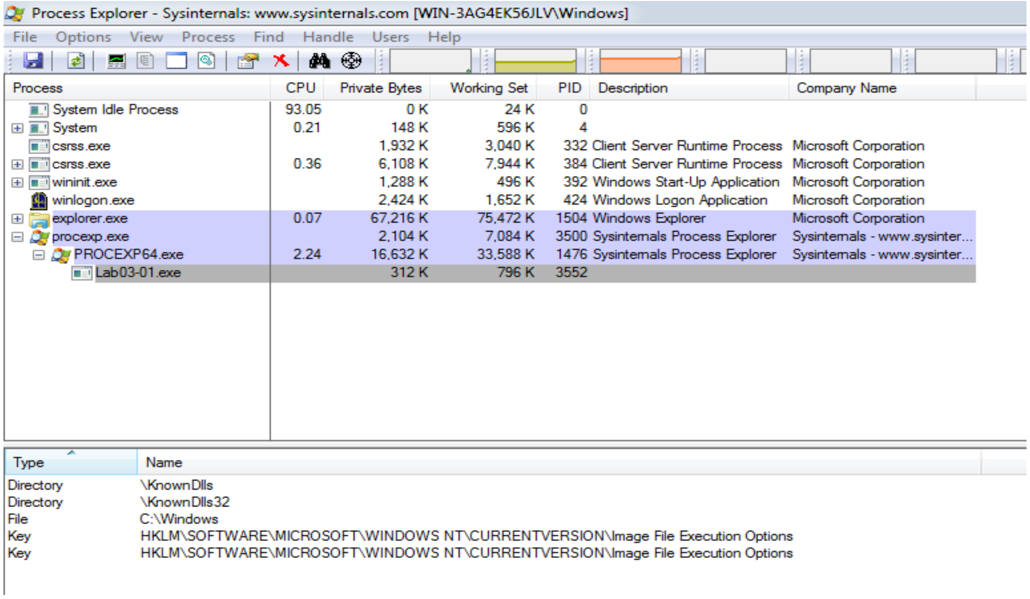
```
⊟ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
    Interface id: 0 (\Device\NPF_{01D39B21-FF07-4754-BF7F-DA4FB68F24CB})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep  8, 2014 11:56:41.742327000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1410191801.742327000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 92 bytes (736 bits)
    Capture Length: 92 bytes (736 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
```

```
0000  00 50 56 e2 14 94 00 0c  29 89 f5 78 08 00 45 00   .PV..... )..x..E.
0010  00 4e 42 48 00 00 80 11  28 68 c0 a8 a7 9b c0 a8   .NBH.... (h......
0020  a7 02 04 01 00 35 00 3a  2d c9 96 20 01 00 00 01   .....5.: -.. ....
0030  00 00 00 00 00 00 03 77  77 77 18 70 72 61 63 74   .......w ww.pract
0040  69 63 61 6c 6d 61 6c 77  61 72 65 61 6e 61 6c 79   icalmalw areanaly
```

Local Area Connection: <live capture in prog... | Packets: 316 · Displayed: 316 (100.0%) | Profile: Default

Figure 5: Wireshark.

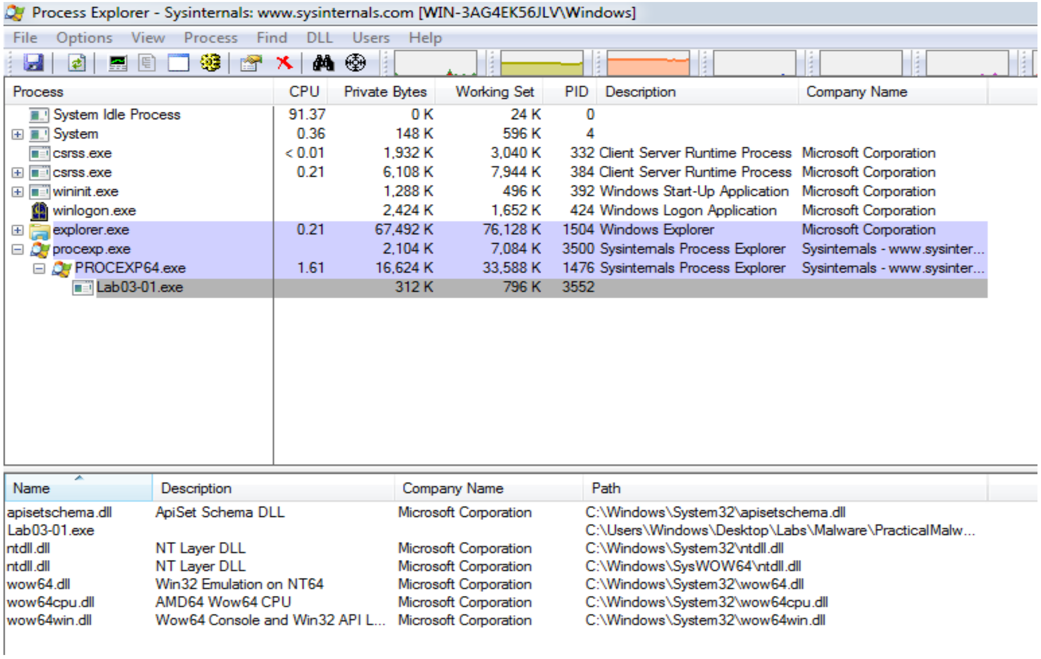
After setting up a virtual network using **ApateDNS** and **Wireshark**. We then begin examine the **Process Explorer**. As shown in Figure 6 and 7 below, we view the handles by clicking *Lab03-01.exe* in the process listing and select **View** then **Lower Pane View** and then**Handles**. In other to view the DLLs we select **View, Lower Pane View** and then **DLLs**. Viewing the DLL shows us that the malware has dynamic loaded DLLs which means that is has networking functionality.


Process Explorer - Sysinternals: www.sysinternals.com [WIN-3AG4EK56JLV\Windows]
File Options View Process Find Handle Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|---|---|---|---|---|---|---|
| System Idle Process | 93.05 | 0 K | 24 K | 0 | | |
| System | 0.21 | 148 K | 596 K | 4 | | |
| csrss.exe | | 1,932 K | 3,040 K | 332 | Client Server Runtime Process | Microsoft Corporation |
| csrss.exe | 0.36 | 6,108 K | 7,944 K | 384 | Client Server Runtime Process | Microsoft Corporation |
| wininit.exe | | 1,288 K | 496 K | 392 | Windows Start-Up Application | Microsoft Corporation |
| winlogon.exe | | 2,424 K | 1,652 K | 424 | Windows Logon Application | Microsoft Corporation |
| explorer.exe | 0.07 | 67,216 K | 75,472 K | 1504 | Windows Explorer | Microsoft Corporation |
| procexp.exe | | 2,104 K | 7,084 K | 3500 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| PROCEXP64.exe | 2.24 | 16,632 K | 33,588 K | 1476 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| Lab03-01.exe | | 312 K | 796 K | 3552 | | |

| Type | Name |
|---|---|
| Directory | \KnownDlls |
| Directory | \KnownDlls32 |
| File | C:\Windows |
| Key | HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options |
| Key | HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options |

Figure 6: Lab03-01.exe handles using Process Explorer


Process Explorer - Sysinternals: www.sysinternals.com [WIN-3AG4EK56JLV\Windows]
File Options View Process Find DLL Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|---|---|---|---|---|---|---|
| System Idle Process | 91.37 | 0 K | 24 K | 0 | | |
| System | 0.36 | 148 K | 596 K | 4 | | |
| csrss.exe | < 0.01 | 1,932 K | 3,040 K | 332 | Client Server Runtime Process | Microsoft Corporation |
| csrss.exe | 0.21 | 6,108 K | 7,944 K | 384 | Client Server Runtime Process | Microsoft Corporation |
| wininit.exe | | 1,288 K | 496 K | 392 | Windows Start-Up Application | Microsoft Corporation |
| winlogon.exe | | 2,424 K | 1,652 K | 424 | Windows Logon Application | Microsoft Corporation |
| explorer.exe | 0.21 | 67,492 K | 76,128 K | 1504 | Windows Explorer | Microsoft Corporation |
| procexp.exe | | 2,104 K | 7,084 K | 3500 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| PROCEXP64.exe | 1.61 | 16,624 K | 33,588 K | 1476 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| Lab03-01.exe | | 312 K | 796 K | 3552 | | |

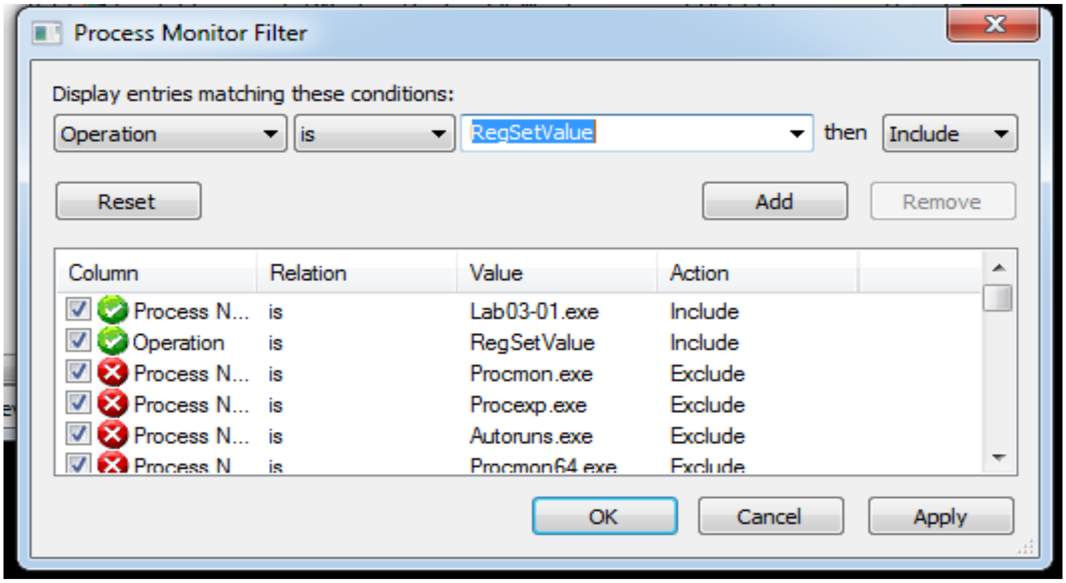
| Name | Description | Company Name | Path |
|---|---|---|---|
| apisetschema.dll | ApiSet Schema DLL | Microsoft Corporation | C:\Windows\System32\apisetschema.dll |
| Lab03-01.exe | | | C:\Users\Windows\Desktop\Labs\Malware\PracticalMalw... |
| ntdll.dll | NT Layer DLL | Microsoft Corporation | C:\Windows\System32\ntdll.dll |
| ntdll.dll | NT Layer DLL | Microsoft Corporation | C:\Windows\SysWOW64\ntdll.dll |
| wow64.dll | Win32 Emulation on NT64 | Microsoft Corporation | C:\Windows\System32\wow64.dll |
| wow64cpu.dll | AMD64 Wow64 CPU | Microsoft Corporation | C:\Windows\System32\wow64cpu.dll |
| wow64win.dll | Wow64 Console and Win32 API L... | Microsoft Corporation | C:\Windows\System32\wow64win.dll |

Figure 7: Lab03-01.exe DLL’s using Process Explorer

3. Some network-based signatures for this malware can be viewed by filtering using **Procmon**.

The figures below show a filter process of *Lab03-01.exe* using **Procmon.** To filter, we bring the filter dialog by selecting **Filter→Filter** and then set the 3 filters we need. The filters are one on the **Process Name** and two on the **Operation**.

Figure 8 and 9 shows the filters on Operation which are *RegSetValue* and *WriteFile.*

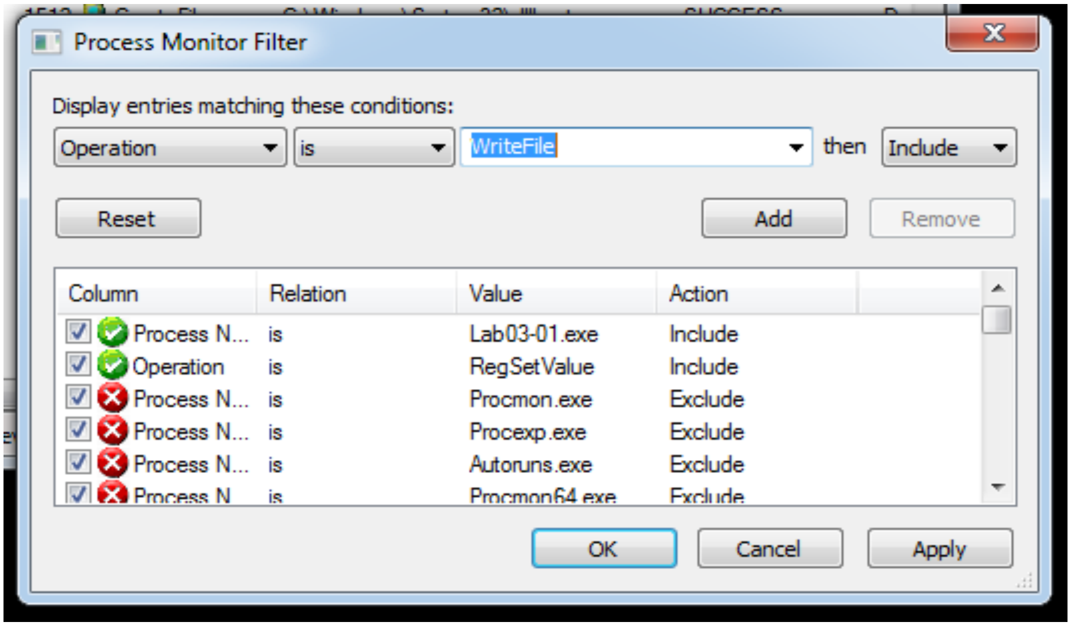


Display entries matching these conditions:

Operation | is | RegSetValue | then | Include

| Column | Relation | Value | Action |
|---|---|---|---|
| ☑ ✓ Process N... | is | Lab03-01.exe | Include |
| ☑ ✓ Operation | is | RegSetValue | Include |
| ☑ ☒ Process N... | is | Procmon.exe | Exclude |
| ☑ ☒ Process N... | is | Procexp.exe | Exclude |
| ☑ ☒ Process N... | is | Autoruns.exe | Exclude |
| ☑ ☒ Process N... | is | Procmon64.exe | Exclude |

Figure 8: lab03-01.exe *RegSetValue* filter using **Procmon**



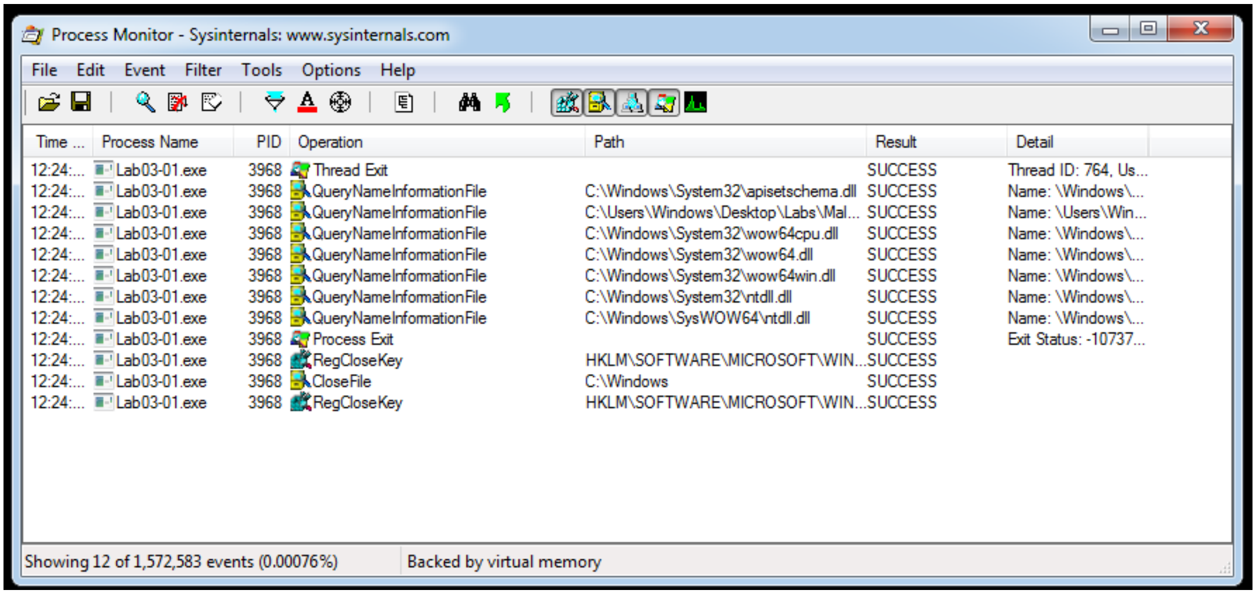
Display entries matching these conditions:

Operation | is | WriteFile | then | Include

| Column | Relation | Value | Action |
|---|---|---|---|
| ☑ ✓ Process N... | is | Lab03-01.exe | Include |
| ☑ ✓ Operation | is | RegSetValue | Include |
| ☑ ☒ Process N... | is | Procmon.exe | Exclude |
| ☑ ☒ Process N... | is | Procexp.exe | Exclude |
| ☑ ☒ Process N... | is | Autoruns.exe | Exclude |
| ☑ ☒ Process N... | is | Procmon64.exe | Exclude |

Figure 9: Lab03-01.exe *WriteFile* filter using **Procmon**

Figure 10 below shows the results of the **Procmon** filters:



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 12:24:... | Lab03-01.exe | 3968 | Thread Exit | | SUCCESS | Thread ID: 764, Us... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Windows\System32\apisetschema.dll | SUCCESS | Name: \Windows\... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Users\Windows\Desktop\Labs\Mal... | SUCCESS | Name: \Users\Win... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Windows\System32\wow64cpu.dll | SUCCESS | Name: \Windows\... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Windows\System32\wow64.dll | SUCCESS | Name: \Windows\... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Windows\System32\wow64win.dll | SUCCESS | Name: \Windows\... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Windows\System32\ntdll.dll | SUCCESS | Name: \Windows\... |
| 12:24:... | Lab03-01.exe | 3968 | QueryNameInformationFile | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Name: \Windows\... |
| 12:24:... | Lab03-01.exe | 3968 | Process Exit | | SUCCESS | Exit Status: -10737... |
| 12:24:... | Lab03-01.exe | 3968 | RegCloseKey | HKLM\SOFTWARE\MICROSOFT\WIN... | SUCCESS | |
| 12:24:... | Lab03-01.exe | 3968 | CloseFile | C:\Windows | SUCCESS | |
| 12:24:... | Lab03-01.exe | 3968 | RegCloseKey | HKLM\SOFTWARE\MICROSOFT\WIN... | SUCCESS | |

Showing 12 of 1,572,583 events (0.00076%) Backed by virtual memory

Figure 10: **Procmon** Filtered result with 3 filter sets.

## Lab 3-2

Analyze the malware found in the file Lab03-02.dll using dynamic analysis tools.

### Questions:

Q1: How can you get this malware to install itself?

Q2: How could you get this malware to run after installation?

Q3: How can you find the process under which this malware is running?

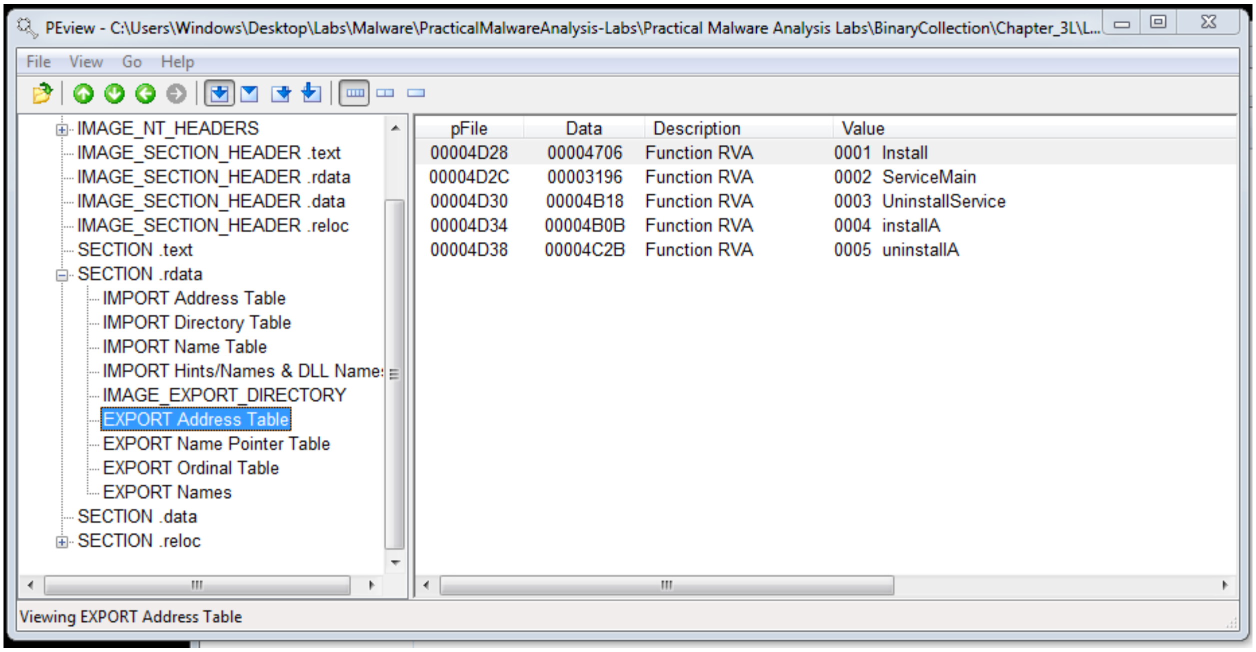
Q4: Which filters could you set in order to use procmon to glean information?

Q5: What are the malware's host-based indicators?

Q6: Are there any useful network-based signatures for this malware?

### Solutions:

1. To install the malware we begin by analyzing the malware. Running the malware in PEview shows that the file has 5 exports: *Install, ServiceMain, UninstallService, installA* and *uninstallA*.Figure 11 shows Lab03-02.dll exports using PEview:

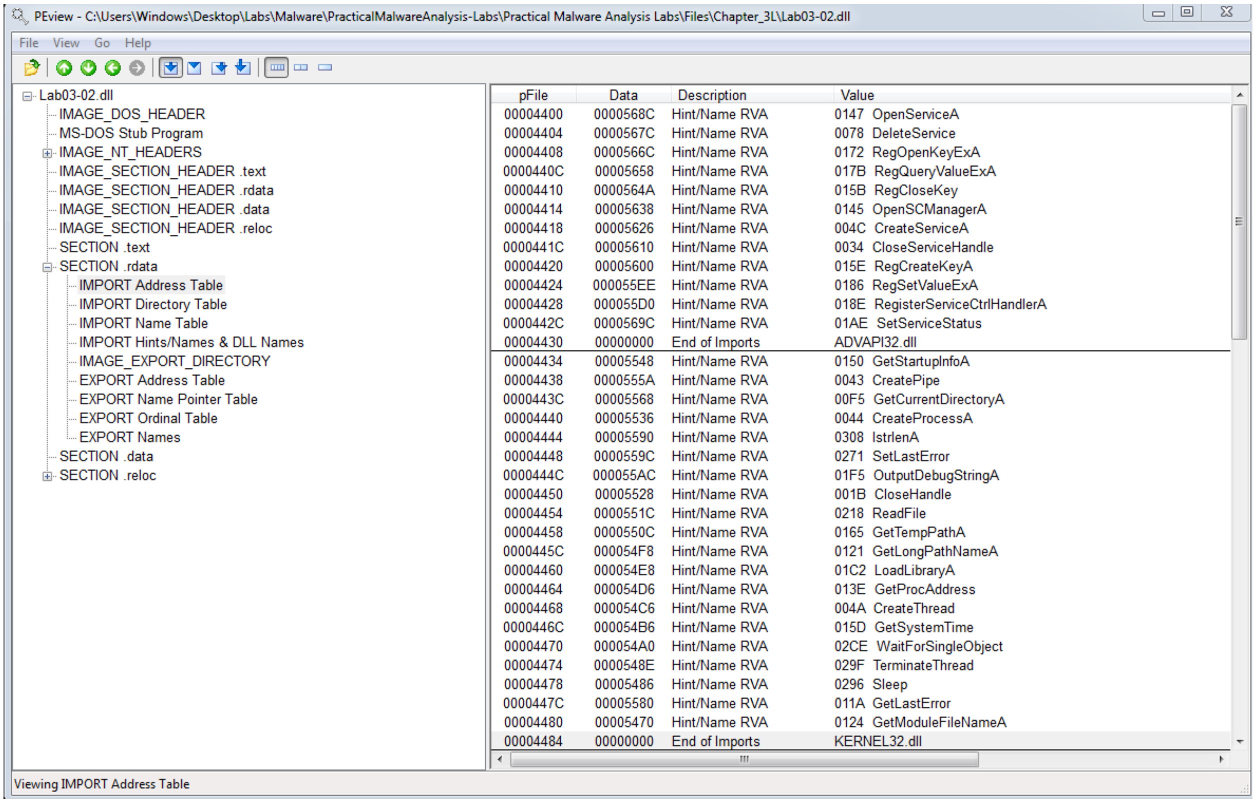


PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\L...
File View Go Help
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
IMAGE_EXPORT_DIRECTORY
EXPORT Address Table
EXPORT Name Pointer Table
EXPORT Ordinal Table
EXPORT Names
SECTION .data
SECTION .reloc
Viewing EXPORT Address Table

| pFile | Data | Description | Value |
|---|---|---|---|
| 00004D28 | 00004706 | Function RVA | 0001 Install |
| 00004D2C | 00003196 | Function RVA | 0002 ServiceMain |
| 00004D30 | 00004B18 | Function RVA | 0003 UninstallService |
| 00004D34 | 00004B0B | Function RVA | 0004 installA |
| 00004D38 | 00004C2B | Function RVA | 0005 uninstallA |

Figure 11: Lab03-02.dll exports using PEview

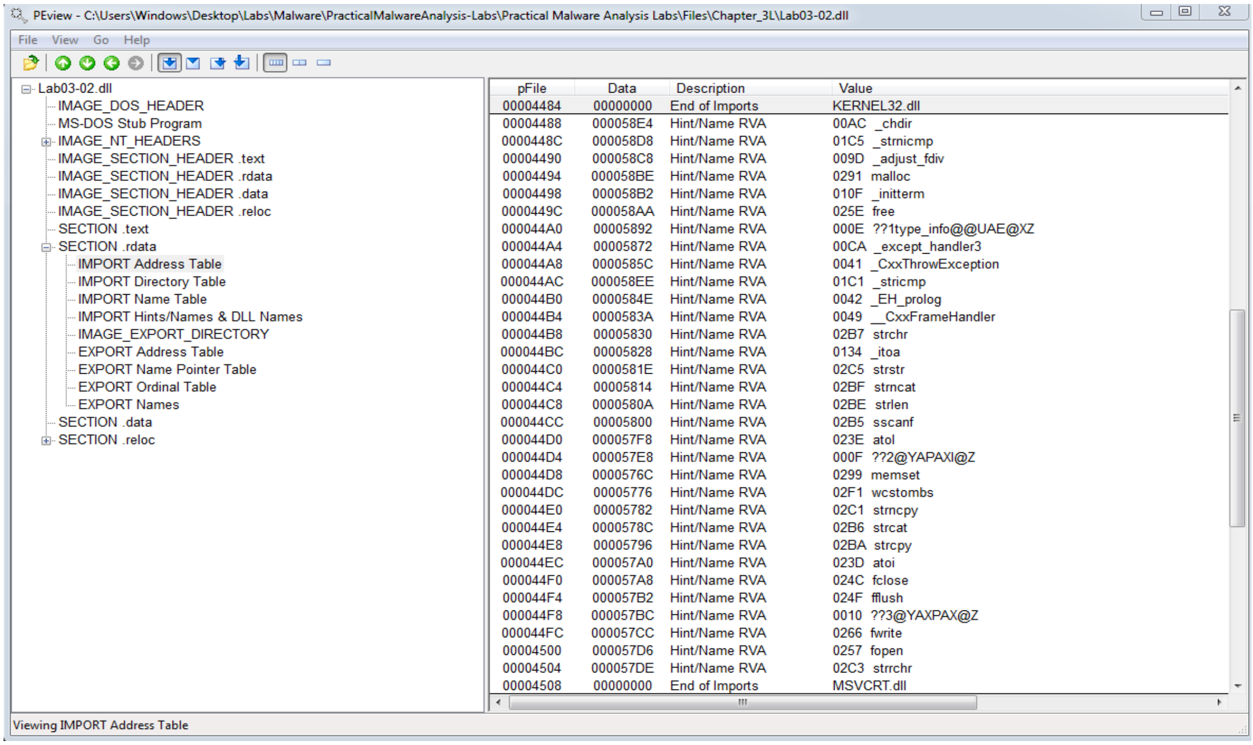
We also view the imports of the file using PEview asw shown in Figure 12, 13 and 14. Below:



PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\Files\Chapter_3L\Lab03-02.dll
File View Go Help
Lab03-02.dll
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 .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
IMAGE_EXPORT_DIRECTORY
EXPORT Address Table
EXPORT Name Pointer Table
EXPORT Ordinal Table
EXPORT Names
SECTION .data
SECTION .reloc
Viewing IMPORT Address Table

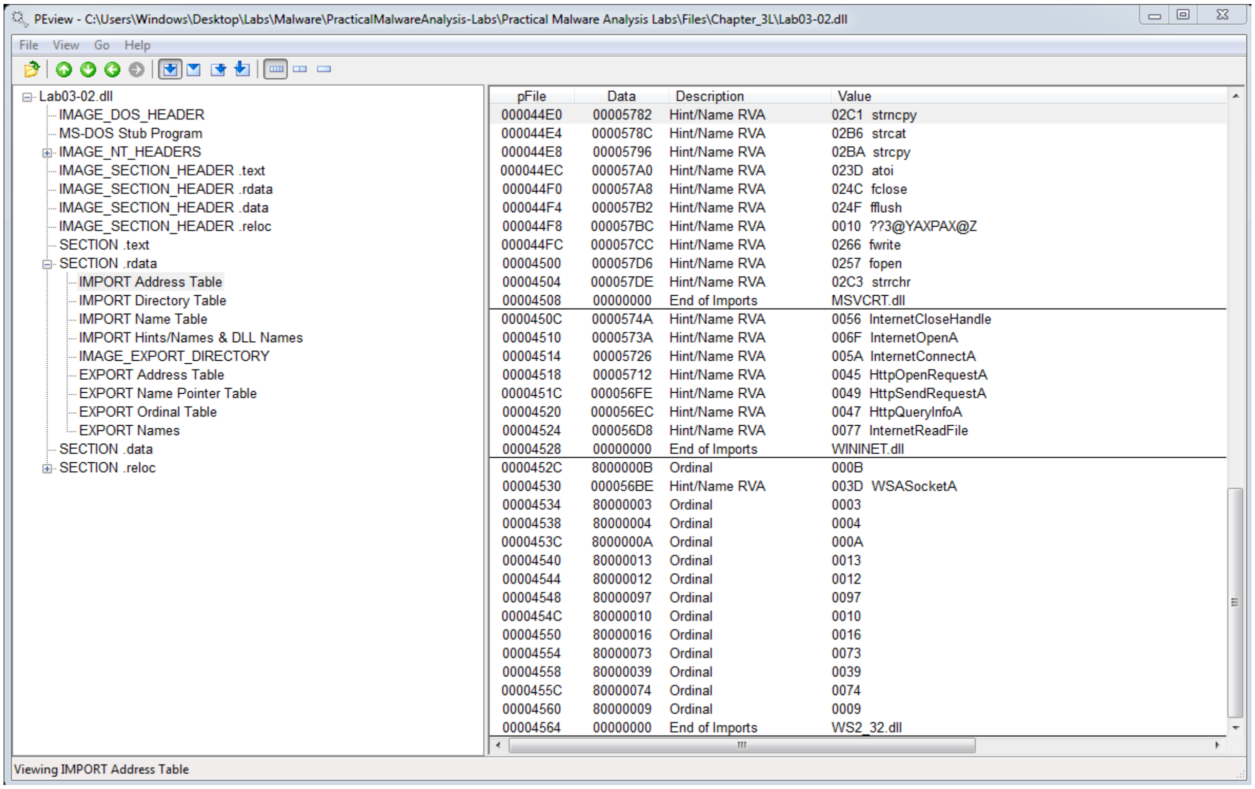
| pFile | Data | Description | Value |
|---|---|---|---|
| 00004400 | 0000568C | Hint/Name RVA | 0147 OpenServiceA |
| 00004404 | 0000567C | Hint/Name RVA | 0078 DeleteService |
| 00004408 | 0000566C | Hint/Name RVA | 0172 RegOpenKeyExA |
| 0000440C | 00005658 | Hint/Name RVA | 017B RegQueryValueExA |
| 00004410 | 0000564A | Hint/Name RVA | 015B RegCloseKey |
| 00004414 | 00005638 | Hint/Name RVA | 0145 OpenSCManagerA |
| 00004418 | 00005626 | Hint/Name RVA | 004C CreateServiceA |
| 0000441C | 00005610 | Hint/Name RVA | 0034 CloseServiceHandle |
| 00004420 | 00005600 | Hint/Name RVA | 015E RegCreateKeyA |
| 00004424 | 000055EE | Hint/Name RVA | 0186 RegSetValueExA |
| 00004428 | 000055D0 | Hint/Name RVA | 018E RegisterServiceCtrlHandlerA |
| 0000442C | 0000569C | Hint/Name RVA | 01AE SetServiceStatus |
| 00004430 | 00000000 | End of Imports | ADVAPI32.dll |
| 00004434 | 00005548 | Hint/Name RVA | 0150 GetStartupInfoA |
| 00004438 | 0000555A | Hint/Name RVA | 0043 CreatePipe |
| 0000443C | 00005568 | Hint/Name RVA | 00F5 GetCurrentDirectoryA |
| 00004440 | 00005536 | Hint/Name RVA | 0044 CreateProcessA |
| 00004444 | 00005590 | Hint/Name RVA | 0308 lstrlenA |
| 00004448 | 0000559C | Hint/Name RVA | 0271 SetLastError |
| 0000444C | 000055AC | Hint/Name RVA | 01F5 OutputDebugStringA |
| 00004450 | 00005528 | Hint/Name RVA | 001B CloseHandle |
| 00004454 | 0000551C | Hint/Name RVA | 0218 ReadFile |
| 00004458 | 0000550C | Hint/Name RVA | 0165 GetTempPathA |
| 0000445C | 000054F8 | Hint/Name RVA | 0121 GetLongPathNameA |
| 00004460 | 000054E8 | Hint/Name RVA | 01C2 LoadLibraryA |
| 00004464 | 000054D6 | Hint/Name RVA | 013E GetProcAddress |
| 00004468 | 000054C6 | Hint/Name RVA | 004A CreateThread |
| 0000446C | 000054B6 | Hint/Name RVA | 015D GetSystemTime |
| 00004470 | 000054A0 | Hint/Name RVA | 02CE WaitForSingleObject |
| 00004474 | 0000548E | Hint/Name RVA | 029F TerminateThread |
| 00004478 | 00005486 | Hint/Name RVA | 0296 Sleep |
| 0000447C | 00005580 | Hint/Name RVA | 011A GetLastError |
| 00004480 | 00005470 | Hint/Name RVA | 0124 GetModuleFileNameA |
| 00004484 | 00000000 | End of Imports | KERNEL32.dll |

Figure 12: Lab03-02.dll imports using PEview


PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\Files\Chapter_3L\Lab03-02.dll
File View Go Help
Lab03-02.dll
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 .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
IMAGE_EXPORT_DIRECTORY
EXPORT Address Table
EXPORT Name Pointer Table
EXPORT Ordinal Table
EXPORT Names
SECTION .data
SECTION .reloc
Viewing IMPORT Address Table

| pFile | Data | Description | Value |
|---|---|---|---|
| 00004484 | 00000000 | End of Imports | KERNEL32.dll |
| 00004488 | 000058E4 | Hint/Name RVA | 00AC _chdir |
| 0000448C | 000058D8 | Hint/Name RVA | 01C5 _strnicmp |
| 00004490 | 000058C8 | Hint/Name RVA | 009D _adjust_fdiv |
| 00004494 | 000058BE | Hint/Name RVA | 0291 malloc |
| 00004498 | 000058B2 | Hint/Name RVA | 010F _initterm |
| 0000449C | 000058AA | Hint/Name RVA | 025E free |
| 000044A0 | 00005892 | Hint/Name RVA | 000E ??1type_info@@UAE@XZ |
| 000044A4 | 00005872 | Hint/Name RVA | 00CA _except_handler3 |
| 000044A8 | 0000585C | Hint/Name RVA | 0041 _CxxThrowException |
| 000044AC | 000058EE | Hint/Name RVA | 01C1 _stricmp |
| 000044B0 | 0000584E | Hint/Name RVA | 0042 _EH_prolog |
| 000044B4 | 0000583A | Hint/Name RVA | 0049 __CxxFrameHandler |
| 000044B8 | 00005830 | Hint/Name RVA | 02B7 strchr |
| 000044BC | 00005828 | Hint/Name RVA | 0134 _itoa |
| 000044C0 | 0000581E | Hint/Name RVA | 02C5 strstr |
| 000044C4 | 00005814 | Hint/Name RVA | 02BF strncat |
| 000044C8 | 0000580A | Hint/Name RVA | 02BE strlen |
| 000044CC | 00005800 | Hint/Name RVA | 02B5 sscanf |
| 000044D0 | 000057F8 | Hint/Name RVA | 023E atol |
| 000044D4 | 000057E8 | Hint/Name RVA | 000F ??2@YAPAXI@Z |
| 000044D8 | 0000576C | Hint/Name RVA | 0299 memset |
| 000044DC | 00005776 | Hint/Name RVA | 02F1 wcstombs |
| 000044E0 | 00005782 | Hint/Name RVA | 02C1 strncpy |
| 000044E4 | 0000578C | Hint/Name RVA | 02B6 strcat |
| 000044E8 | 00005796 | Hint/Name RVA | 02BA strcpy |
| 000044EC | 000057A0 | Hint/Name RVA | 023D atoi |
| 000044F0 | 000057A8 | Hint/Name RVA | 024C fclose |
| 000044F4 | 000057B2 | Hint/Name RVA | 024F fflush |
| 000044F8 | 000057BC | Hint/Name RVA | 0010 ??3@YAXPAX@Z |
| 000044FC | 000057CC | Hint/Name RVA | 0266 fwrite |
| 00004500 | 000057D6 | Hint/Name RVA | 0257 fopen |
| 00004504 | 000057DE | Hint/Name RVA | 02C3 strrchr |
| 00004508 | 00000000 | End of Imports | MSVCRT.dll |

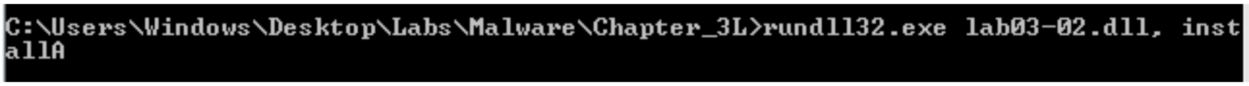
Figure 13: Lab03-02.dll imports using PEview


PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\Files\Chapter_3L\Lab03-02.dll
File View Go Help
Lab03-02.dll
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 .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
IMAGE_EXPORT_DIRECTORY
EXPORT Address Table
EXPORT Name Pointer Table
EXPORT Ordinal Table
EXPORT Names
SECTION .data
SECTION .reloc
Viewing IMPORT Address Table

| pFile | Data | Description | Value |
|---|---|---|---|
| 000044E0 | 00005782 | Hint/Name RVA | 02C1 strncpy |
| 000044E4 | 0000578C | Hint/Name RVA | 02B6 strcat |
| 000044E8 | 00005796 | Hint/Name RVA | 02BA strcpy |
| 000044EC | 000057A0 | Hint/Name RVA | 023D atoi |
| 000044F0 | 000057A8 | Hint/Name RVA | 024C fclose |
| 000044F4 | 000057B2 | Hint/Name RVA | 024F fflush |
| 000044F8 | 000057BC | Hint/Name RVA | 0010 ??3@YAXPAX@Z |
| 000044FC | 000057CC | Hint/Name RVA | 0266 fwrite |
| 00004500 | 000057D6 | Hint/Name RVA | 0257 fopen |
| 00004504 | 000057DE | Hint/Name RVA | 02C3 strrchr |
| 00004508 | 00000000 | End of Imports | MSVCRT.dll |
| 0000450C | 0000574A | Hint/Name RVA | 0056 InternetCloseHandle |
| 00004510 | 0000573A | Hint/Name RVA | 006F InternetOpenA |
| 00004514 | 00005726 | Hint/Name RVA | 005A InternetConnectA |
| 00004518 | 00005712 | Hint/Name RVA | 0045 HttpOpenRequestA |
| 0000451C | 000056FE | Hint/Name RVA | 0049 HttpSendRequestA |
| 00004520 | 000056EC | Hint/Name RVA | 0047 HttpQueryInfoA |
| 00004524 | 000056D8 | Hint/Name RVA | 0077 InternetReadFile |
| 00004528 | 00000000 | End of Imports | WININET.dll |
| 0000452C | 8000000B | Ordinal | 000B |
| 00004530 | 000056BE | Hint/Name RVA | 003D WSASocketA |
| 00004534 | 80000003 | Ordinal | 0003 |
| 00004538 | 80000004 | Ordinal | 0004 |
| 0000453C | 8000000A | Ordinal | 000A |
| 00004540 | 80000013 | Ordinal | 0013 |
| 00004544 | 80000012 | Ordinal | 0012 |
| 00004548 | 80000097 | Ordinal | 0097 |
| 0000454C | 80000010 | Ordinal | 0010 |
| 00004550 | 80000016 | Ordinal | 0016 |
| 00004554 | 80000073 | Ordinal | 0073 |
| 00004558 | 80000039 | Ordinal | 0039 |
| 0000455C | 80000074 | Ordinal | 0074 |
| 00004560 | 80000009 | Ordinal | 0009 |
| 00004564 | 00000000 | End of Imports | WS2_32.dll |

Figure 14: Lab03-02.dll imports using PEview

After examining the exports files, the malware can be installed using the rundll32.exe function with rundll32.exe Lab03-02.dll, installA. As shown in Fig 15 below:

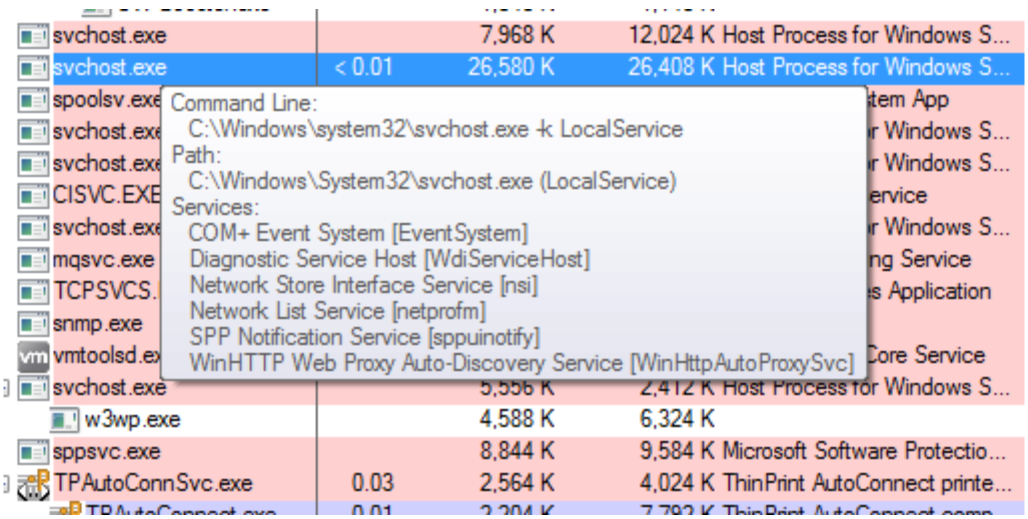


```
C:\Users\Windows\Desktop\Labs\Malware\Chapter_3L>rundll32.exe lab03-02.dll, inst
allA
```

Figure 15: *rundll32.exe Lab03-02.dll, installA.*

2. To run the malware, start the service it installs using the net command net start IPRIP. This is done using the cmd.
3. Using the Process Explorer and hovering over the svchost.exe files. We can find the process under which the malware is running.

As shown in Fig 16 below: The process under which the malware is running is svchost.exe

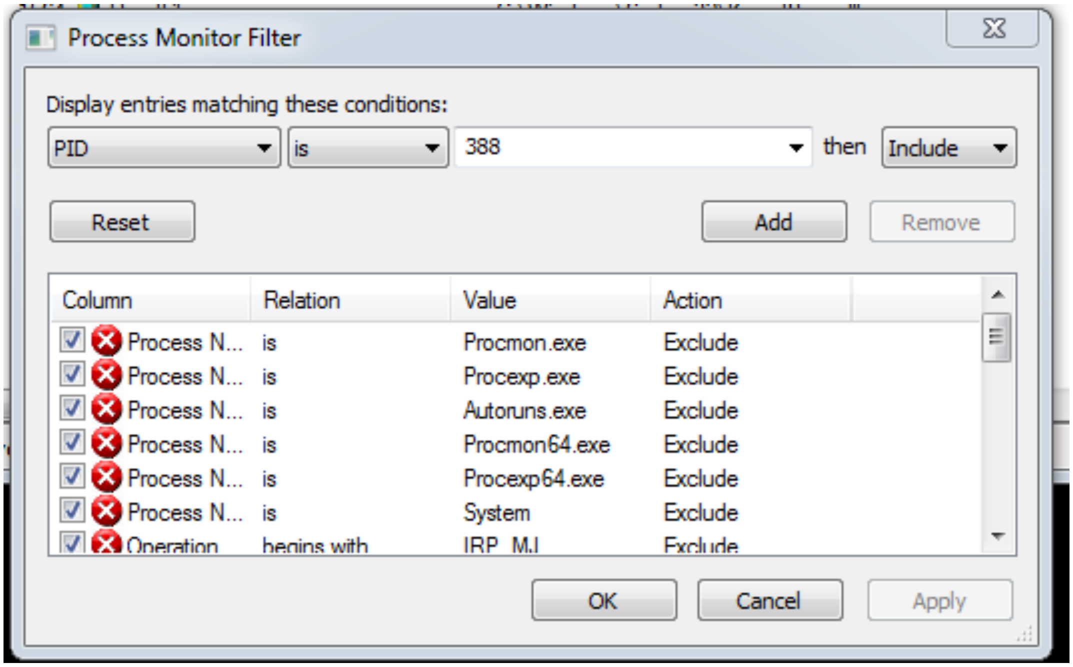


```
svchost.exe                     7,968 K    12,024 K Host Process for Windows S...
svchost.exe        < 0.01      26,580 K    26,408 K Host Process for Windows S...
spoolsv.exe                                         tem App
svchost.exe                                         r Windows S...
svchost.exe                                         r Windows S...
CISVC.EXE                                           ervice
svchost.exe                                         r Windows S...
mqsvc.exe                                           ng Service
TCPSVCS.                                            s Application
snmp.exe
vmtoolsd.ex                                         Core Service
svchost.exe                     5,556 K     2,412 K Host Process for Windows S...
  w3wp.exe                      4,588 K     6,324 K
sppsvc.exe                      8,844 K     9,584 K Microsoft Software Protectio...
TPAutoConnSvc.exe  0.03         2,564 K     4,024 K ThinPrint AutoConnect printe...
```

```
Command Line:
  C:\Windows\system32\svchost.exe -k LocalService
Path:
  C:\Windows\System32\svchost.exe (LocalService)
Services:
  COM+ Event System [EventSystem]
  Diagnostic Service Host [WdiServiceHost]
  Network Store Interface Service [nsi]
  Network List Service [netprofm]
  SPP Notification Service [sppuinotify]
  WinHTTP Web Proxy Auto-Discovery Service [WinHttpAutoProxySvc]
```

Figure 16: Examining Service Malware in Process Explorer.

4. The PID we found in the process explorer which is 388 can be used as a filter in **Procmon**. To filter in **Procmon** it follows the same method we used in Figure 8 and 9 above.Figure 17 shows **Procmon** filtered using PID.



Display entries matching these conditions:

PID ▾ | is ▾ | 388 ▾ | then | Include ▾

| | Column | Relation | Value | Action |
|---|---|---|---|---|
| ☑ | Process N... | is | Procmon.exe | Exclude |
| ☑ | Process N... | is | Procexp.exe | Exclude |
| ☑ | Process N... | is | Autoruns.exe | Exclude |
| ☑ | Process N... | is | Procmon64.exe | Exclude |
| ☑ | Process N... | is | Procexp64.exe | Exclude |
| ☑ | Process N... | is | System | Exclude |
| ☑ | Operation | begins with | IRP_MJ | Exclude |

Figure 17: PID 388 Filtered using **Procmon**.

5. After examining the malware in Process Explorer, the malware installs a service IPRIP with a display name Internet Network Awareness (INA+). That indicates that the malware is a host-based indicator.
6. After thorough analysis. We couldn't find any useful signatures for the malware.

## Lab 3-3

Execute the malware found in the file Lab03-03.exe while monitoring it using basic dynamic analysis tools in a safe environment.

### Questions:

Q1: What do you notice when monitoring this malware with Process Explorer?

Q2: Can you identify any live memory modifications?

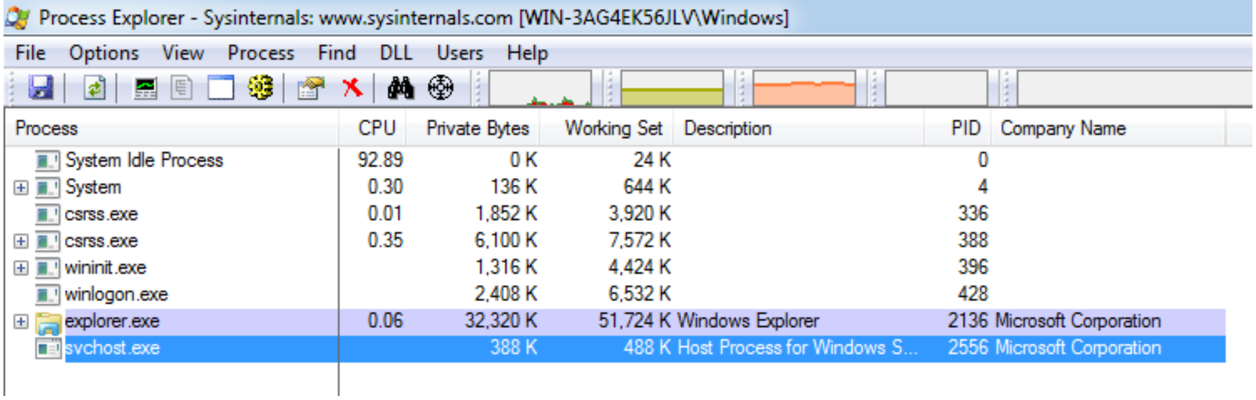
Q3: What are the malware's host-based indicators?

Q4: What is the purpose of this program?

### Solutions:

1. We begin by analyzing the malware using **Process Explorer** and **Procmon**. Because **Procmon** events stream by quickly, so we use **File, Capture Events** to turn off event

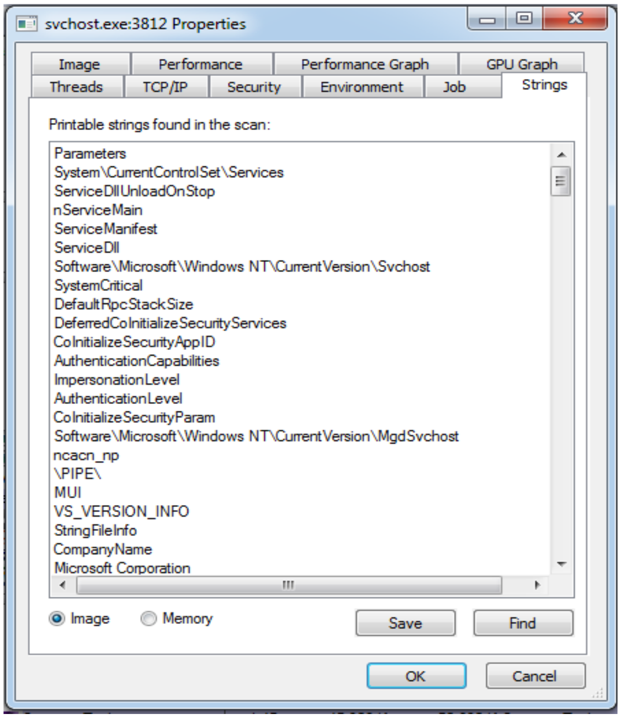
capture. When we run *Lab03-03.exe* by double clicking the file, it becomes visible inside **Process Explorer.** As shown in figure below. The *svchost.exe* is created and run as an orphaned process. The fact that *svchost.exe* is orphaned is highly unusual and highly suspicious.


Process Explorer - Sysinternals: www.sysinternals.com [WIN-3AG4EK56JLV\Windows]
File
Options
View
Process
Find
DLL
Users
Help

| Process | CPU | Private Bytes | Working Set | Description | PID | Company Name |
|---|---|---|---|---|---|---|
| System Idle Process | 92.89 | 0 K | 24 K | | 0 | |
| System | 0.30 | 136 K | 644 K | | 4 | |
| csrss.exe | 0.01 | 1,852 K | 3,920 K | | 336 | |
| csrss.exe | 0.35 | 6,100 K | 7,572 K | | 388 | |
| wininit.exe | | 1,316 K | 4,424 K | | 396 | |
| winlogon.exe | | 2,408 K | 6,532 K | | 428 | |
| explorer.exe | 0.06 | 32,320 K | 51,724 K | Windows Explorer | 2136 | Microsoft Corporation |
| svchost.exe | | 388 K | 488 K | Host Process for Windows S... | 2556 | Microsoft Corporation |

Figure 18: Process Explorer view of orphaned svchost.exe

2. Viewing the strings of the *svchost.exe* in the **Process Explorer**, and toggling between Image & Memory will show the difference or identify any live memory modification. However we can view the strings in Image and not that of the Memory. Shown in Figure 19 below is the string of the svchost.exe file viewed under the image.



Printable strings found in the scan:

```
Parameters
System\CurrentControlSet\Services
ServiceDllUnloadOnStop
nServiceMain
ServiceManifest
ServiceDll
Software\Microsoft\Windows NT\CurrentVersion\Svchost
SystemCritical
DefaultRpcStackSize
DeferredCoInitializeSecurityServices
CoInitializeSecurityAppID
AuthenticationCapabilities
ImpersonationLevel
AuthenticationLevel
CoInitializeSecurityParam
Software\Microsoft\Windows NT\CurrentVersion\MgdSvchost
ncacn_np
\PIPE\
MUI
VS_VERSION_INFO
StringFileInfo
CompanyName
Microsoft Corporation
```

● Image ○ Memory

Figure 19: svchost.exe strings

3. The malware creates the log file practicalmalwareanalysis.log. This can be viewed by viewing the strings of the svchost.exe file

4. Carefully analyzing the strings, one can conclude that the file is a Keylogger. The program performs process replacement on svchost.exe to launch the Keylogger.

## Lab 3-4

Analyze the malware found in the file Lab03-04.exe using basic dynamic analysis tools.

### Questions:

Q1: What happens when you run this file?

Q2: What is causing the roadblock in dynamic analysis?

Q3: Are there other ways to run this program?

### Solutions:

When you try to run this malware, it automatically deletes itself and therefore cannot be analyzed.

## Conclusion

This lab aims to provide a dynamic analysis of a malware. Also a part of the basic analysis is used to properly analyze these malwares. However advanced and more sophisticated tools are used, such as Wireshark and ApateDNS which aims at controlling the network. The lab provides answers to what malware imports and strings are, host and network based indicators of a malware. Network based signatures of malware are also found.

Lastly the lab provide answers to malware behaviours such as how it operates and install itself. This lab provides an indepth knowledge of malware monitoring process.