CNIT 58100 CFM: CYBERFORENSICS OF MALWARE – LAB 1 (PART 1)

Ibrahim Waziri Jr

PhD in Information Security (CERIAS)

Lab – Part 1

Due on: September 3rd, 2014

Instructor: **Associate Prof Sam Liles**

Purdue University

2014

Abstract

This lab covers the skills discussed in chapter 1 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 1 labs. The lab uses 5 different files which are: *Lab01-01.dll*, *Lab01-01.exe, Lab01-02.exe, Lab01-03.exe, and Lab01-04.exe*. These files are malwares are therefore could be harmful if used for non-training purposes.

The tools used to analyze the files used in this lab are: Virustools, PEview, PEiD, Resource Hacker, and String. The results collected after analyzing the files includes: existing virus definitions, indications whether the files are packed or obfuscated, compilation date, imports, host or network based indicators and file resource.

Lab 1-1

This lab uses the files Lab01-01.exe and Lab01-01.dll

Questions:

Q1. Upload the files to http://www.virustotal.com/ and view the reports. Does either file match any existing antivirus signatures?

Q2. When were these files compiled?

Q3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?

Q4. Do any imports hint at what this malware does? If so, which imports are they?

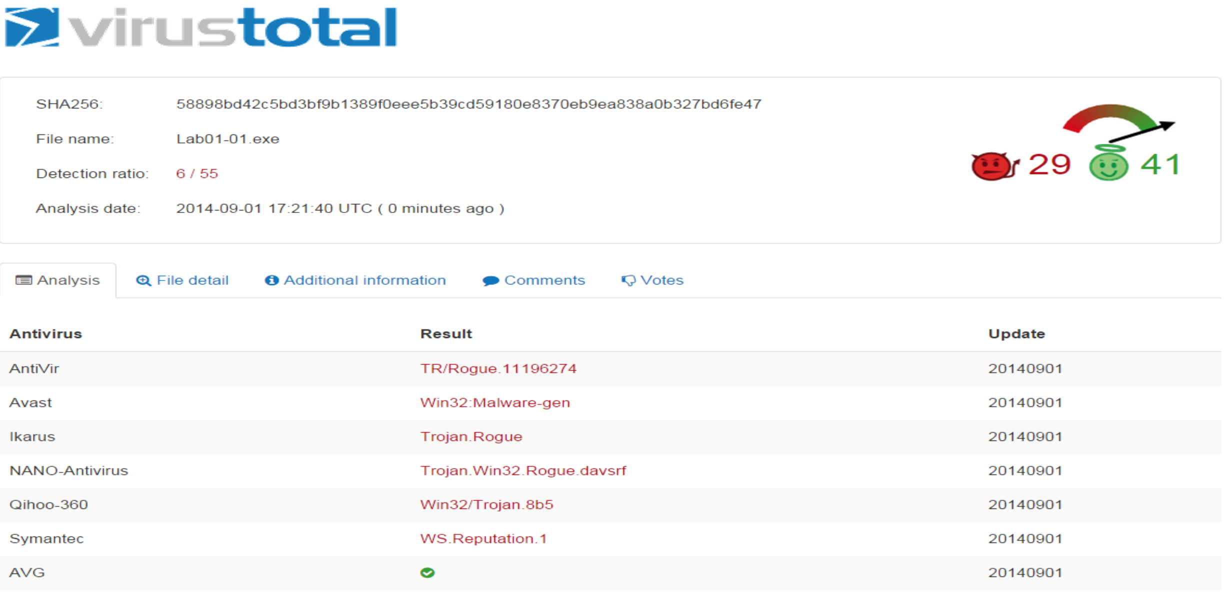
Q5. Are there any other files or host-based indicators that you could look for on infected systems?

Q6. What network-based indicators could be used to find this malware on infected machines?

Q7. What would you guess is the purpose of these files?

Answers:

1: Both files *Lab01-01.exe* and *Lab01-01.dll* were uploaded to http://www.virustotal.com/ and the front page which is the analysis shows that both files match existing antivirus signatures. As shown in figure 1 and 2 below for both files respectively.



SHA256: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

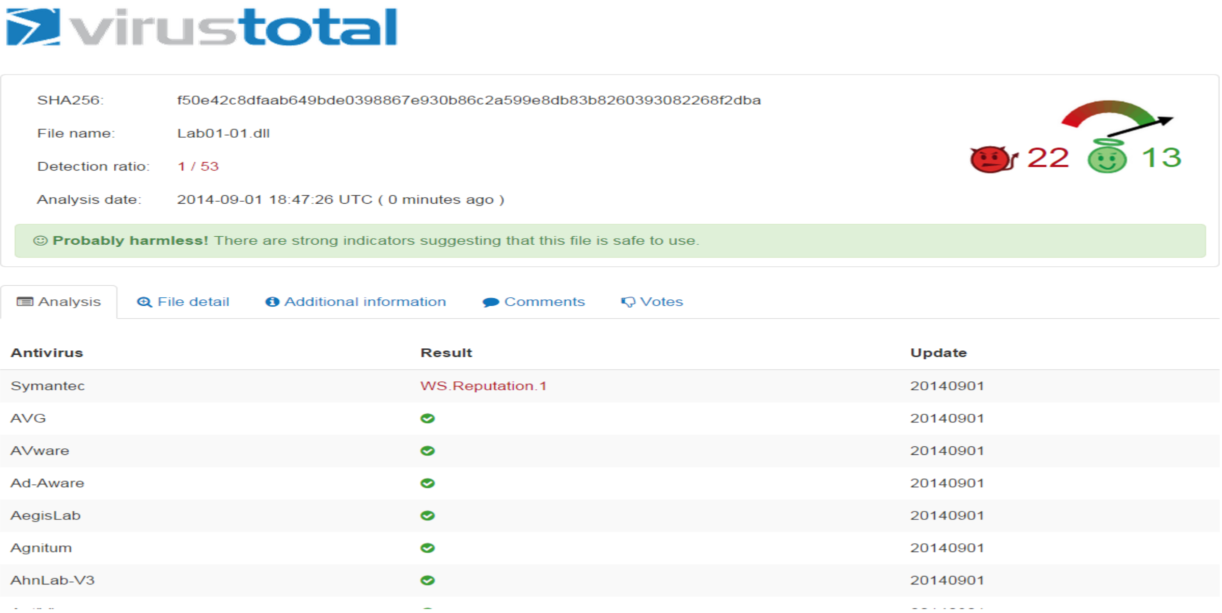
File name: Lab01-01.exe

Detection ratio: 6 / 55

Analysis date: 2014-09-01 17:21:40 UTC (0 minutes ago)

Antivirus	Result	Update
AntiVir	TR/Rogue.11196274	20140901
Avast	Win32:Malware-gen	20140901
Ikarus	Trojan.Rogue	20140901
NANO-Antivirus	Trojan.Win32.Rogue.davsrf	20140901
Qihoo-360	Win32/Trojan.8b5	20140901
Symantec	WS.Reputation.1	20140901
AVG	✓	20140901

Figure 1: Lab01-01.exe Analysis



SHA256:	f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
File name:	Lab01-01.dll
Detection ratio:	1 / 53
Analysis date:	2014-09-01 18:47:26 UTC (0 minutes ago)

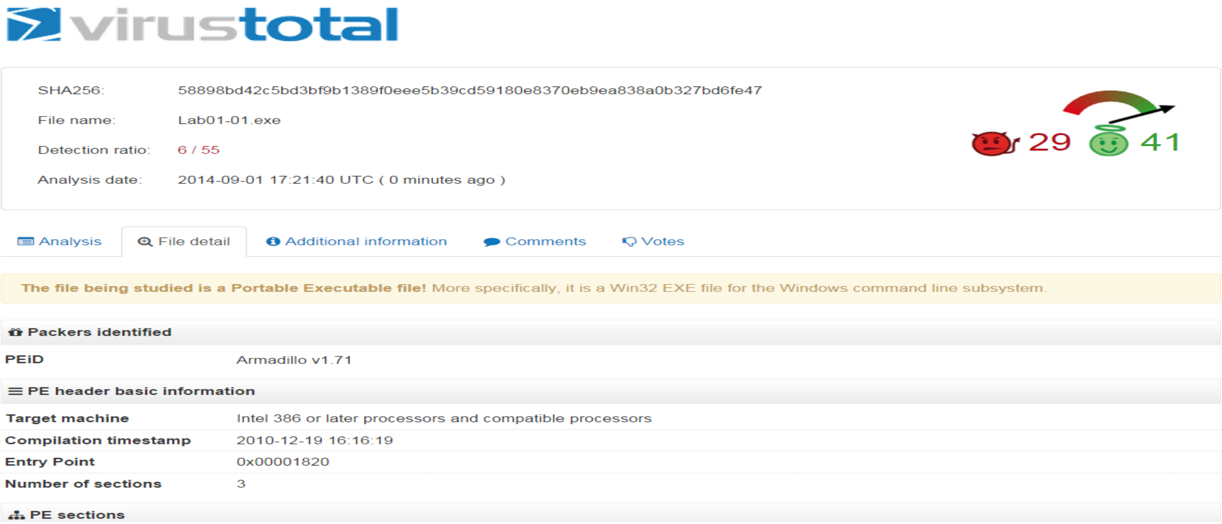
☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

Antivirus	Result	Update
Symantec	WS.Reputation.1	20140901
AVG	✓	20140901
AVware	✓	20140901
Ad-Aware	✓	20140901
AegisLab	✓	20140901
Agnitum	✓	20140901
AhnLab-V3	✓	20140901

Figure 2: Lab01-01.dll Analysis

2: Navigating to the next column “File detail” on the http://www.virustotal.com/ shows the compilation date and time of each file. The compilation date for both *Lab01-01.exe* and *Lab01-01.dll* are: 2010-12-19.

The compilation time could also be viewed using the PEView by uploading the files and navigating to the **IMAGE_NT_HEADERS** then **IMAGE_FILE_HEADER** viewing the Time Date Stamp field. Figure 3, 4, 5 and 6 below shows the compilation date and time for both files.



SHA256:	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
File name:	Lab01-01.exe
Detection ratio:	6 / 55
Analysis date:	2014-09-01 17:21:40 UTC (0 minutes ago)

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows command line subsystem.

Packers identified

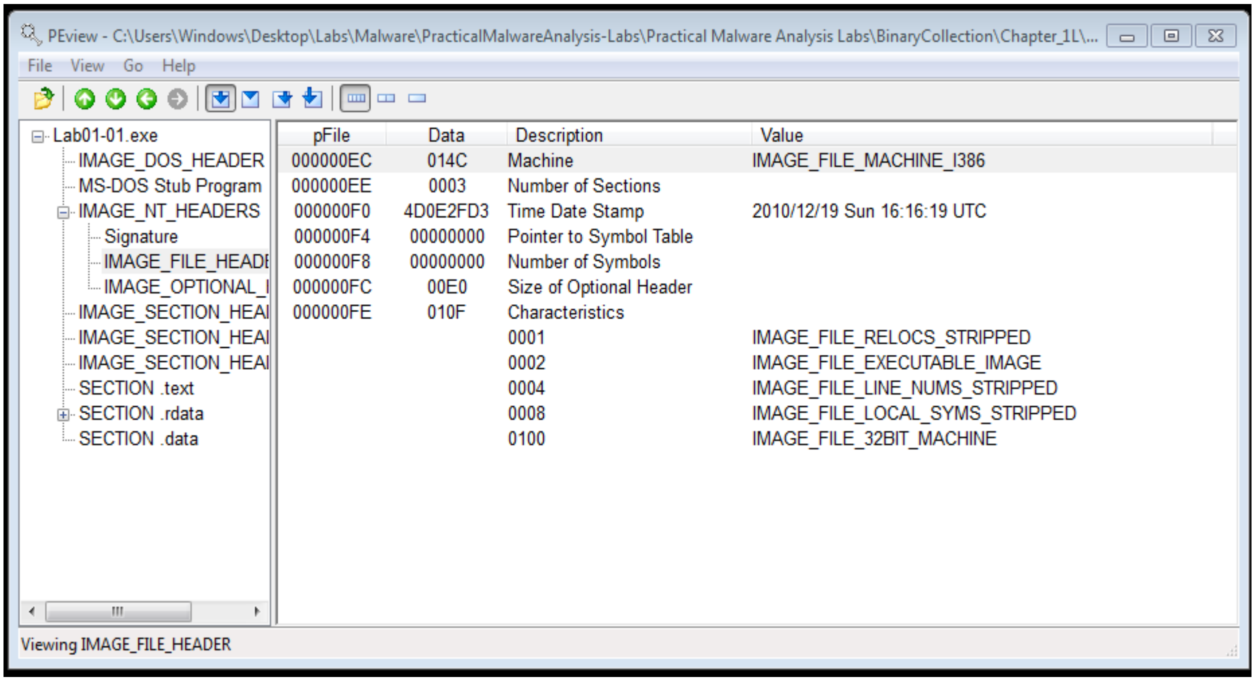
PEiD	Armadillo v1.71

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2010-12-19 16:16:19
Entry Point	0x00001820
Number of sections	3

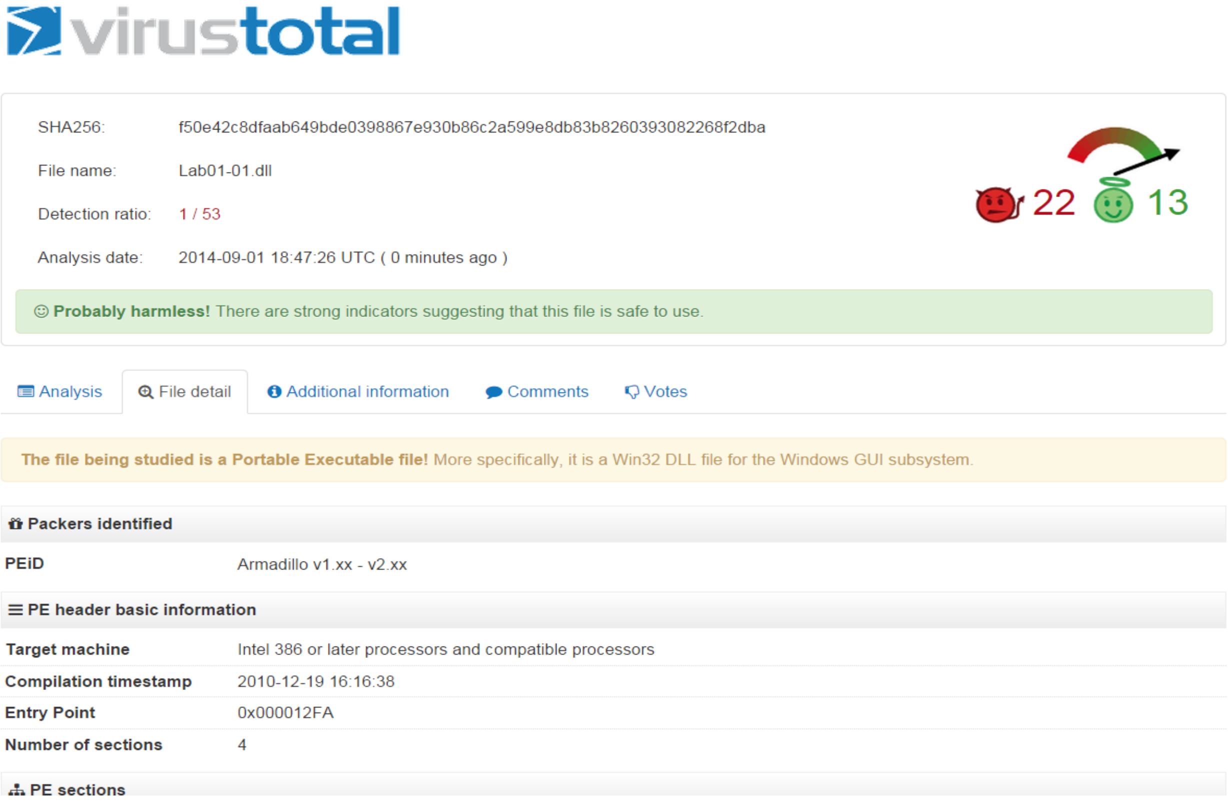
PE sections

Figure 3: Lab01-01.exe Compilation Timestamp using www.virustotal.com



pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

Figure 4: Lab01-01.exe Compilation Timestamp using PEview



SHA256: f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

File name: Lab01-01.dll

Detection ratio: 1 / 53

Analysis date: 2014-09-01 18:47:26 UTC (0 minutes ago)

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

The file being studied is a Portable Executable file! More specifically, it is a Win32 DLL file for the Windows GUI subsystem.

Packers identified

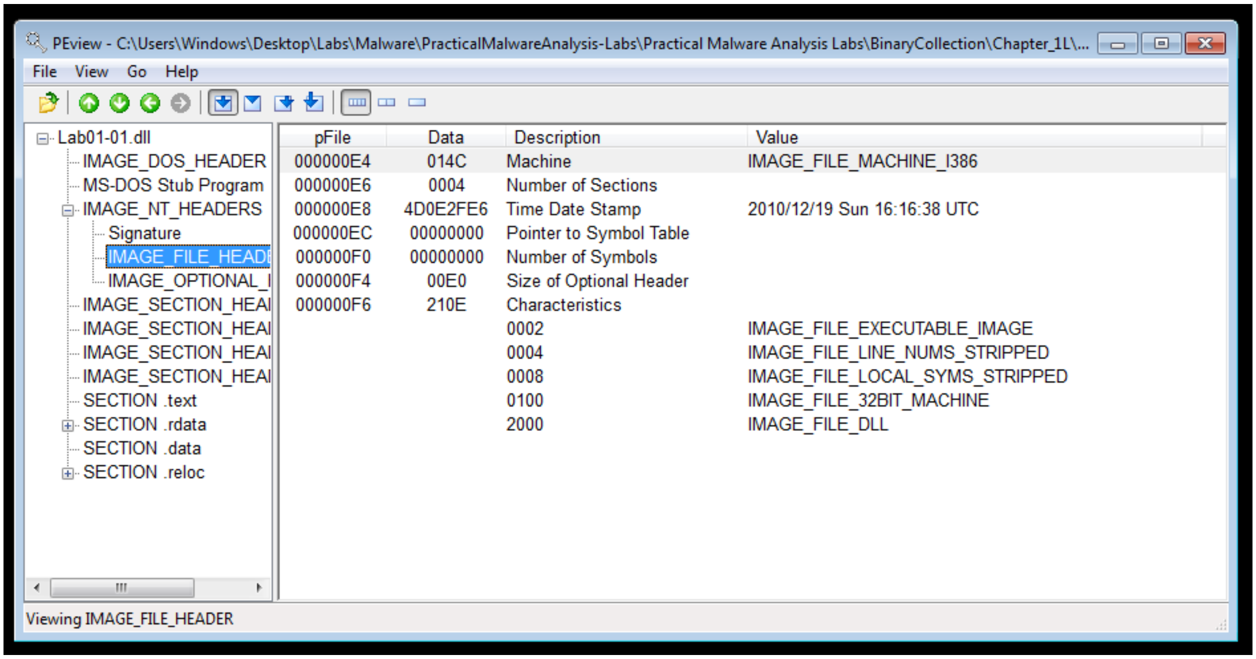
PEiD	Armadillo v1.xx - v2.xx

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2010-12-19 16:16:38
Entry Point	0x000012FA
Number of sections	4

PE sections

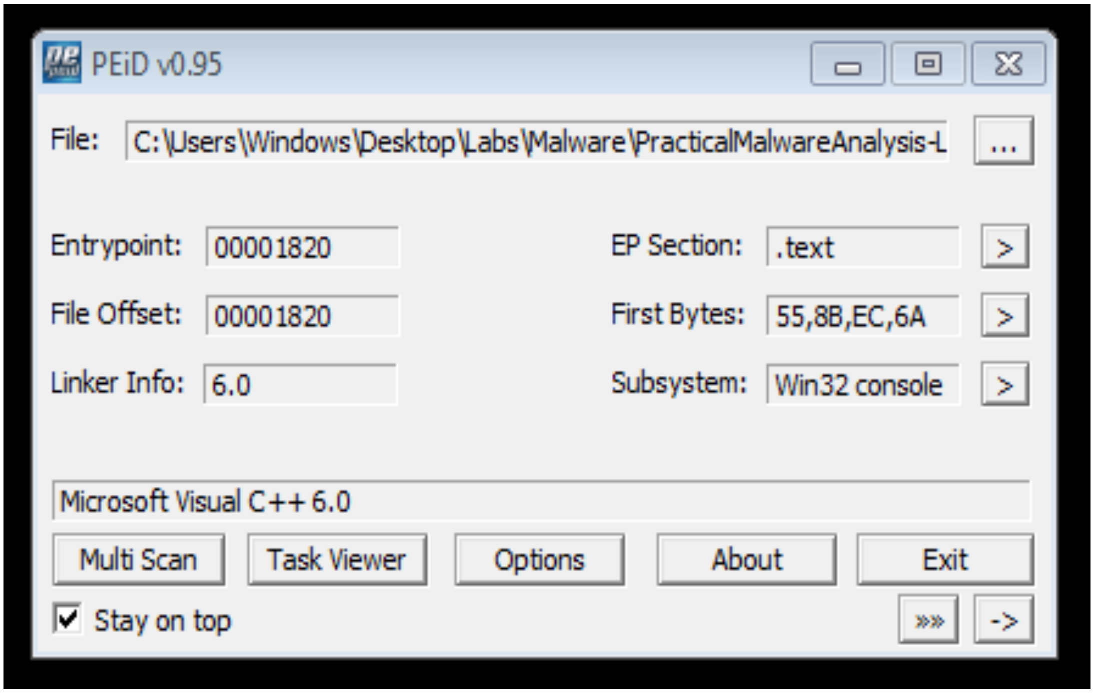
Figure 5: Lab01-01.dll Compilation Timestamp using www.virustotal.com



pFile	Data	Description	Value
000000E4	014C	Machine	IMAGE_FILE_MACHINE_I386
000000E6	0004	Number of Sections	
000000E8	4D0E2FE6	Time Date Stamp	2010/12/19 Sun 16:16:38 UTC
000000EC	00000000	Pointer to Symbol Table	
000000F0	00000000	Number of Symbols	
000000F4	00E0	Size of Optional Header	
000000F6	210E	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE
		2000	IMAGE_FILE_DLL

Figure 6: Lab01-01.dll Compilation Timestamp using PEview

3. PEiD shows that both files are unpacked and were compiled with Microsoft Visual C++. To view this, upload the respective file to PEiD and analyze. The figure below shows both files uploaded to PEiD and analyzed.



File: C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-L

Entrypoint: 00001820

EP Section: .text

File Offset: 00001820

First Bytes: 55,8B,EC,6A

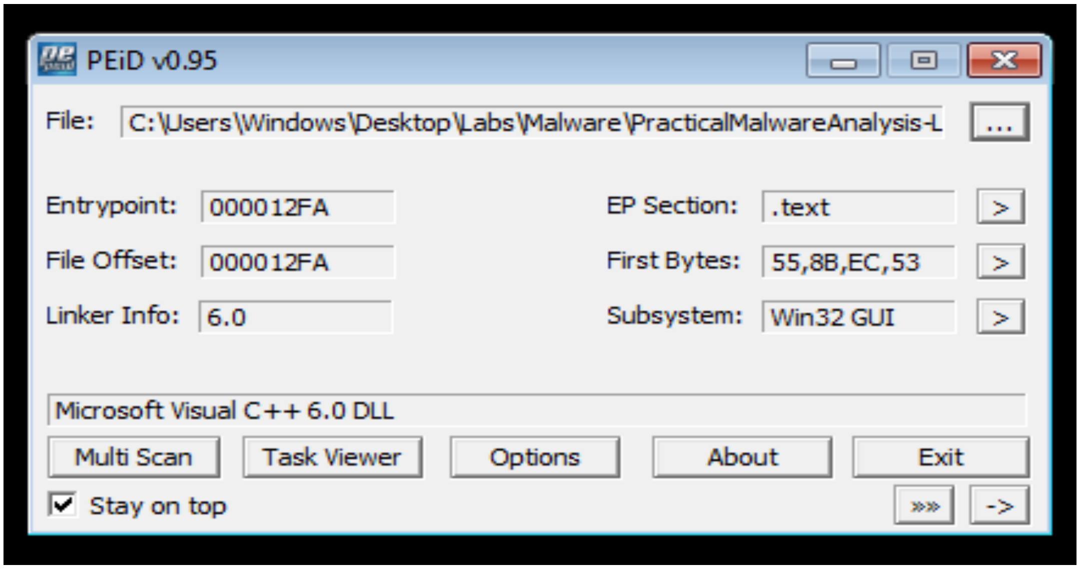
Linker Info: 6.0

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

Figure 7: Lab01-01.exe uploaded and analyzed using PEiD



File: C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-L

Entrypoint: 000012FA

File Offset: 000012FA

Linker Info: 6.0

EP Section: .text

First Bytes: 55,8B,EC,53

Subsystem: Win32 GUI

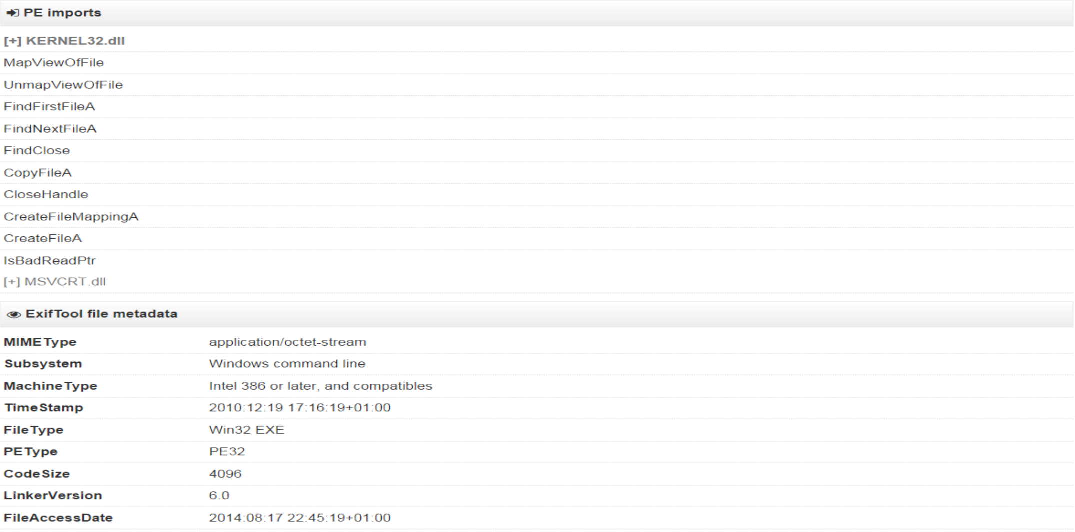
Microsoft Visual C++ 6.0 DLL

☑ Stay on top

Figure 8: Lab01-01.dll uploaded and analyzed using PEiD

4. For the Lab01-01.exe, the import shows us that this malware is used to manipulate files, the PE imports shows 2 different imports: **KERNEL32.dll** which includes files like *MapViewOfFile, FindFirstFileA, FindClose, CreateFileA* etc. could all the attributed to creating and change the behavior of files. Under the different import **MSVCRT.dll**, it include file like exit, this could be directive files used to command or instruct files.

The figures below shows both files under the **KERNEL32.dll** and **MSVCRT.dll** imports of *Lab01-01.exe*



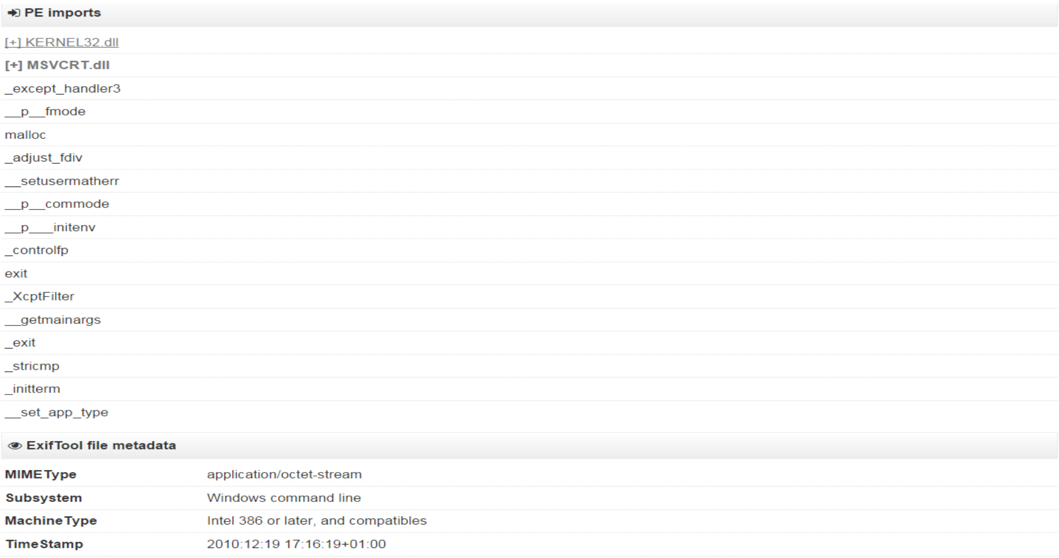
PE imports

[+] KERNEL32.dll
MapViewOfFile
UnmapViewOfFile
FindFirstFileA
FindNextFileA
FindClose
CopyFileA
CloseHandle
CreateFileMappingA
CreateFileA
IsBadReadPtr
[+] MSVCRT.dll

ExifTool file metadata

MIMEType	application/octet-stream
Subsystem	Windows command line
MachineType	Intel 386 or later, and compatibles
TimeStamp	2010:12:19 17:16:19+01:00
FileType	Win32 EXE
PEType	PE32
CodeSize	4096
LinkerVersion	6.0
FileAccessDate	2014:08:17 22:45:19+01:00

Figure 9: Lab01-01.exe KERNEL32.dll import



PE imports

[+] KERNEL32.dll
[+] MSVCRT.dll
_except_handler3
__p__fmode
malloc
_adjust_fdiv
__setusermatherr
__p__commode
__p___initenv
_controlfp
exit
_XcptFilter
__getmainargs
_exit
_stricmp
_initterm
__set_app_type

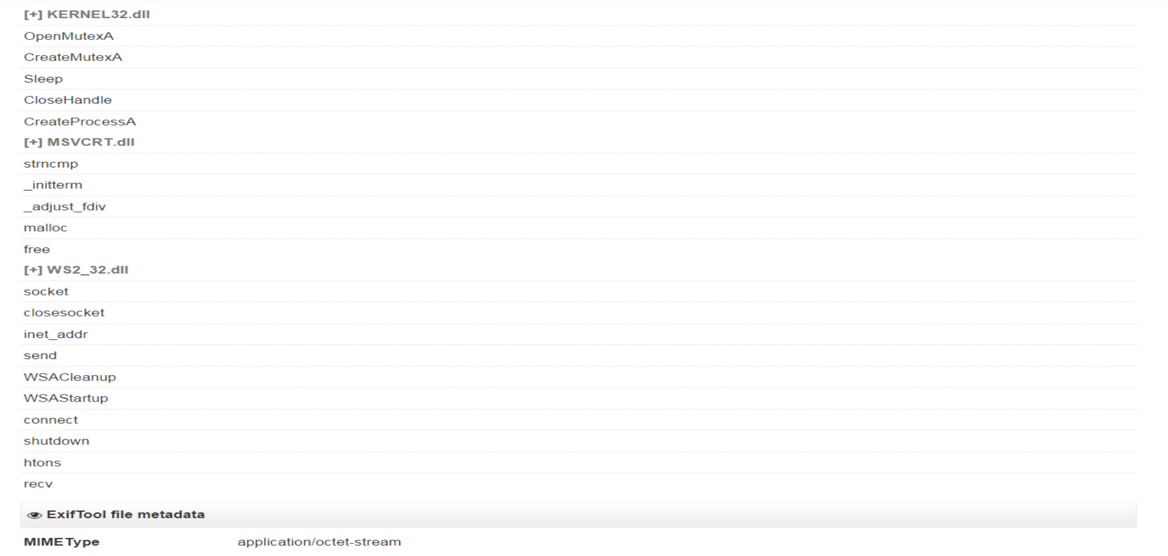
ExifTool file metadata

MIMEType	application/octet-stream
Subsystem	Windows command line
MachineType	Intel 386 or later, and compatibles
TimeStamp	2010:12:19 17:16:19+01:00

Figure 10: Lab01-01.exe MSVCRT.dll import

As for the *Lab01-01.dll* imports: The PE imports of the www.virustotal.com page shows 3 different imports which are: **KERNEL32.dll, MSVCRT.dll** and **WS2_32.dll**. From all indications it shows that the .exe and .dll files of Lab01-01 are of the same behavior, expanding the **KERNEL32.dll** file shows files such as *Sleep, CloseHandle and CreateProcessA*. These files can be concluded as manipulative files used to control and change the behavior of the victim.

Also the **MSVCRT.dll** and **WS2_32.dll** have files such as free, shutdown, send etc. These files command the behavior of how a file should act. The figure below shows the *Lab01-01.dll* imports.



[+] KERNEL32.dll
OpenMutexA
CreateMutexA
Sleep
CloseHandle
CreateProcessA
[+] MSVCRT.dll
strncmp
_initterm
_adjust_fdiv
malloc
free
[+] WS2_32.dll
socket
closesocket
inet_addr
send
WSACleanup
WSAStartup
connect
shutdown
htons
recv

ExifTool file metadata

MIMEType	application/octet-stream

Figure 11: Lab01-01.dll KERNEL32.dll, MSVCRT.dll, and WS2_32.dll imports

5. Yes! We can take a look at the *inet_addr* configuration file usually located in system32 of windows or the localhost for UNIX to see if the network or host configuration has been altered.

   Taking a look at Figure 11, we can see that the WS2_32.dll contains a file *inet_addr*, from a networking point of view; the *inet_addr* can be used to covert or manipulate the IP address of any host, without the host knowing what is going on.

6. IP address and subnets are always a good start in identifying infected machines. Thoroughly analyzing the IP address and knowing where the address routes to, or if it redirects to a certain location is a good network-based indicator to use on malware systems. Most times malwares don't really change the behavior of the victim, but in most cases if reroutes all information and data to a specific drop point, usually the dumping site of the fraudster. Carefully analyzing the addresses of the host and network could be a great indicator for analyzing malware in infected systems.

7. From my guess I will say the *Lab01-01.exe* is an executable file, probably used to execute the malware.

   And the *Lab01-01.dll* is a library (considering that all .dll files are libraries) that contain codes that can be used by more than one program at the same time. It is mostly like the file that contains the malware to be executed by the .exe.

Lab 1-2

Questions:

Q1: Upload the *Lab01-02.exe* file to http://www.virustotal.com/. Does it match any existing definitions?

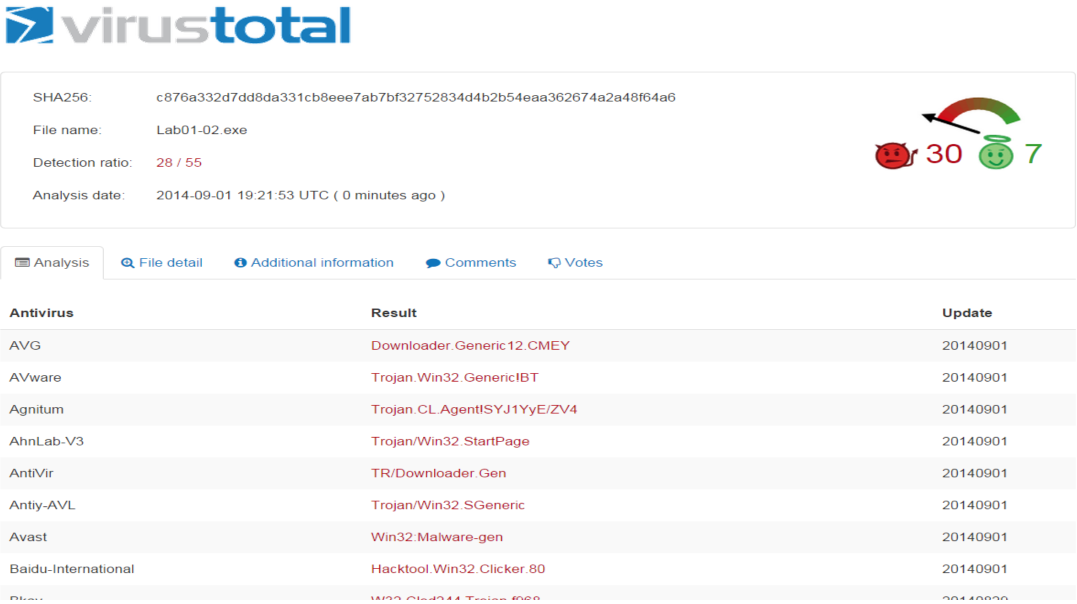
Q2: Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

Q3: Do any imports hint at this program functionality? If so, which imports are they and what do they tell you?

Q4: What host or network-based indicators could be used to identify this malware on infected machine?

Solution:

1. Yes it does! The *Lab01-02.exe* file was uploaded to http://www.virustotal.com/ and it matches existing antivirus definitions as shown in the figure below:



SHA256: c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

File name: Lab01-02.exe

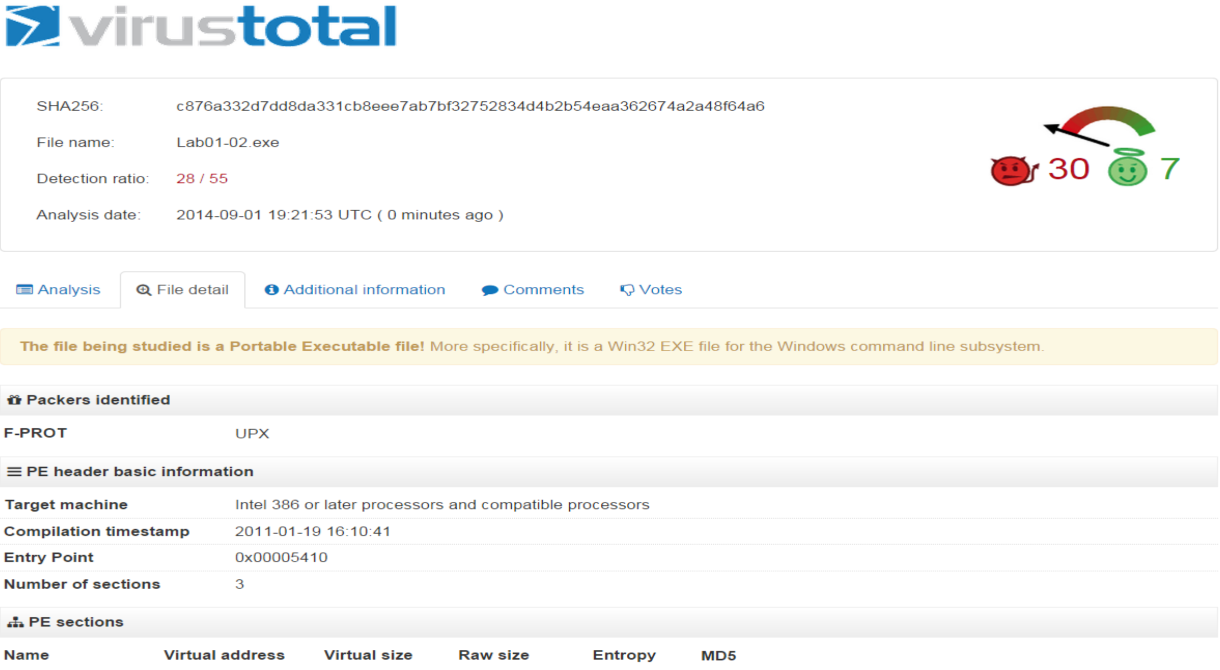
Detection ratio: 28 / 55

Analysis date: 2014-09-01 19:21:53 UTC (0 minutes ago)

Antivirus	Result	Update
AVG	Downloader.Generic12.CMEY	20140901
AVware	Trojan.Win32.GenericIBT	20140901
Agnitum	Trojan.CL.Agent!SYJ1YyE/ZV4	20140901
AhnLab-V3	Trojan/Win32.StartPage	20140901
AntiVir	TR/Downloader.Gen	20140901
Antiy-AVL	Trojan/Win32.SGeneric	20140901
Avast	Win32:Malware-gen	20140901
Baidu-International	Hacktool.Win32.Clicker.80	20140901
Bkav	W32.Clod244.Trojan.f068	20140830

Figure 12: Lab01-02.exe definitions

2. Navigating to the file details tab in http://virustotal.com/ under the packet identified – **F-PROT** shows that the file is packed with UPX, also opening the file with PEview, some indicators such as **IMAGE_SECTION_HEADER UPX0, IMAGE_SECTION_HEADER UPX1** and **IMAGE_SECTION_HEADER UPX2** identified the file as UPX packed. The figures below using http://virustotal.com/ and PEview shows the file UPX packed.



SHA256: c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

File name: Lab01-02.exe

Detection ratio: 28 / 55

Analysis date: 2014-09-01 19:21:53 UTC (0 minutes ago)

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows command line subsystem.

Packers identified

F-PROT	UPX

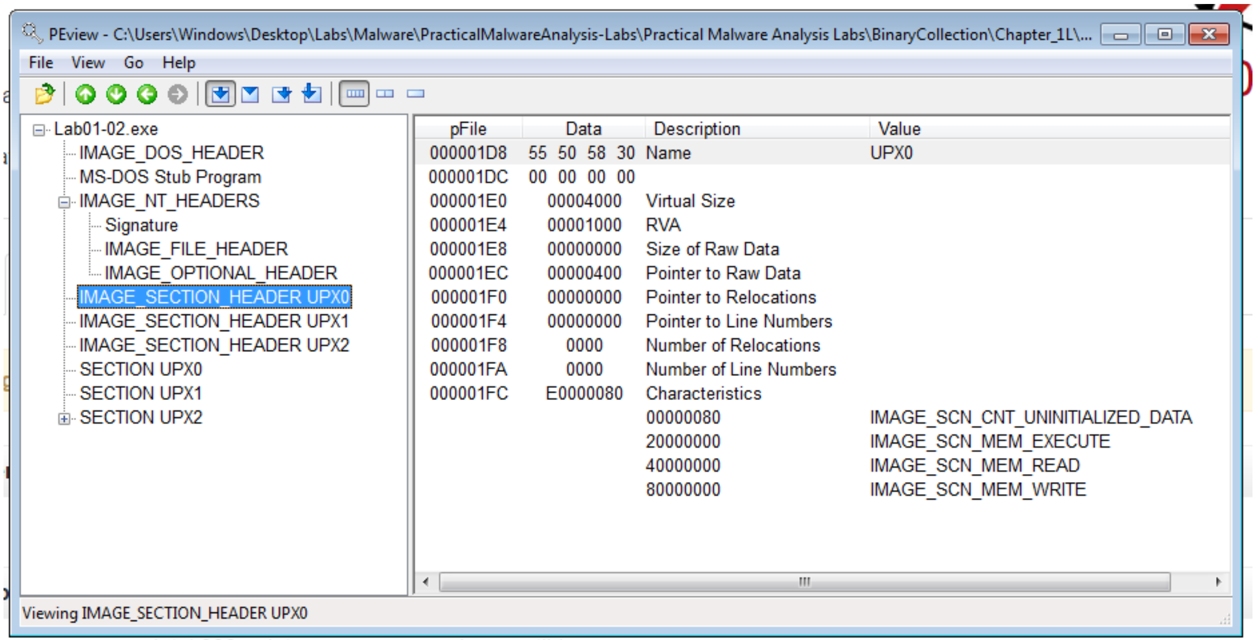
PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2011-01-19 16:10:41
Entry Point	0x00005410
Number of sections	3

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5

Figure 13: *Lab01-02.exe* UPX-packed using www.virustotal.com


PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\...
File
View
Go
Help

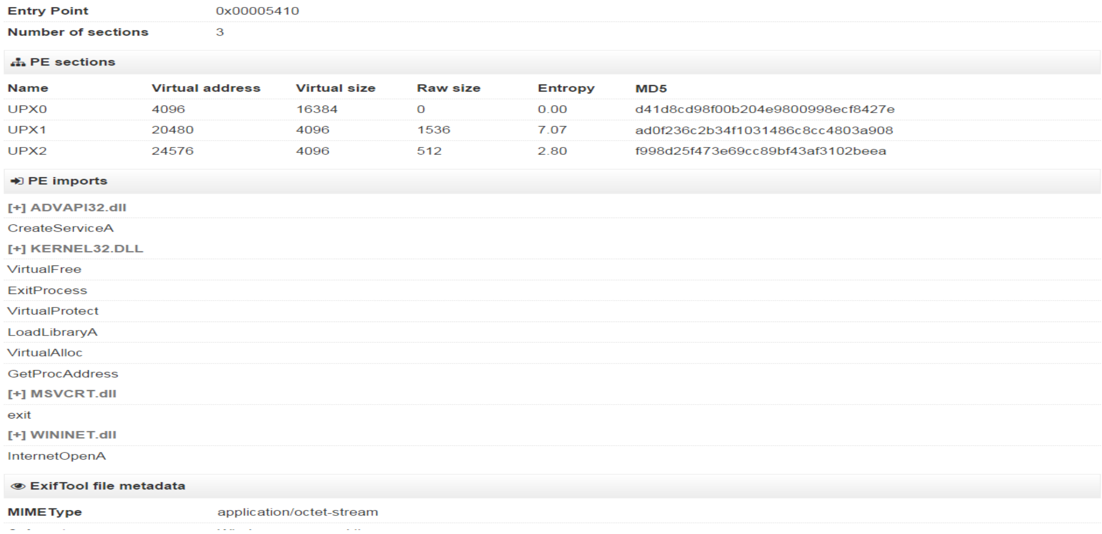
```
Lab01-02.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER UPX0
  IMAGE_SECTION_HEADER UPX1
  IMAGE_SECTION_HEADER UPX2
  SECTION UPX0
  SECTION UPX1
  SECTION UPX2
```

pFile	Data	Description	Value
000001D8	55 50 58 30	Name	UPX0
000001DC	00 00 00 00		
000001E0	00004000	Virtual Size	
000001E4	00001000	RVA	
000001E8	00000000	Size of Raw Data	
000001EC	00000400	Pointer to Raw Data	
000001F0	00000000	Pointer to Relocations	
000001F4	00000000	Pointer to Line Numbers	
000001F8	0000	Number of Relocations	
000001FA	0000	Number of Line Numbers	
000001FC	E0000080	Characteristics	
		00000080	IMAGE_SCN_CNT_UNINITIALIZED_DATA
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ
		80000000	IMAGE_SCN_MEM_WRITE

Viewing IMAGE_SECTION_HEADER UPX0

Figure 14: *Lab01-02.exe* UPX-packed using PEview

3. As shown in the www.virustotal.com figure below: the imports are **ADVAPI32.dll** with the *CreateServiceA* in it, **KERNEL32.DLL** with *VirtualFree, ExitProcess, VirtualProtect, LoadLibraryA, VirtualAlloc,* and *GetProcAddress*. **MSVCRT.dll** with exit, and finally **WININET.dll** with *InternetOpenA* in it. The imports files with much consideration will be the *CreateService, InternetOpen, ExitProcess* and *GetProcAddress.* From these files we could tell that the files connect to a network, obviously the Internet, and it manipulates and changes the data of the victim's computer or device.



Entry Point	0x00005410
Number of sections	3

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
UPX0	4096	16384	0	0.00	d41d8cd98f00b204e9800998ecf8427e
UPX1	20480	4096	1536	7.07	ad0f236c2b34f1031486c8cc4803a908
UPX2	24576	4096	512	2.80	f998d25f473e69cc89bf43af3102beea

PE imports

[+] ADVAPI32.dll
CreateServiceA
[+] KERNEL32.DLL
VirtualFree
ExitProcess
VirtualProtect
LoadLibraryA
VirtualAlloc
GetProcAddress
[+] MSVCRT.dll
exit
[+] WININET.dll
InternetOpenA

ExifTool file metadata

MIMEType	application/octet-stream

Figure 15: Lab01-02.exe imports

4. From the previous lab, same approach could be used to identify this malware on infected system. Which is IP address and subnets is always a good start in identifying infected machines. Thoroughly analyzing the IP address and knowing where the address routes to, or if it redirects to a certain location is a good network-based indicator to use on malware systems. Most times malwares don't really change the behavior of the victim, but in most cases if reroutes all information and data to a specific drop point, usually the dumping site of the fraudster. Carefully analyzing the addresses of the host and network could be a great indicator for analyzing malware in infected systems.

Lab 1-3

Questions:

Q1: Upload the *Lab01-03.exe* file to the http://virustotal.com/. Does it match any existing antivirus definitions?

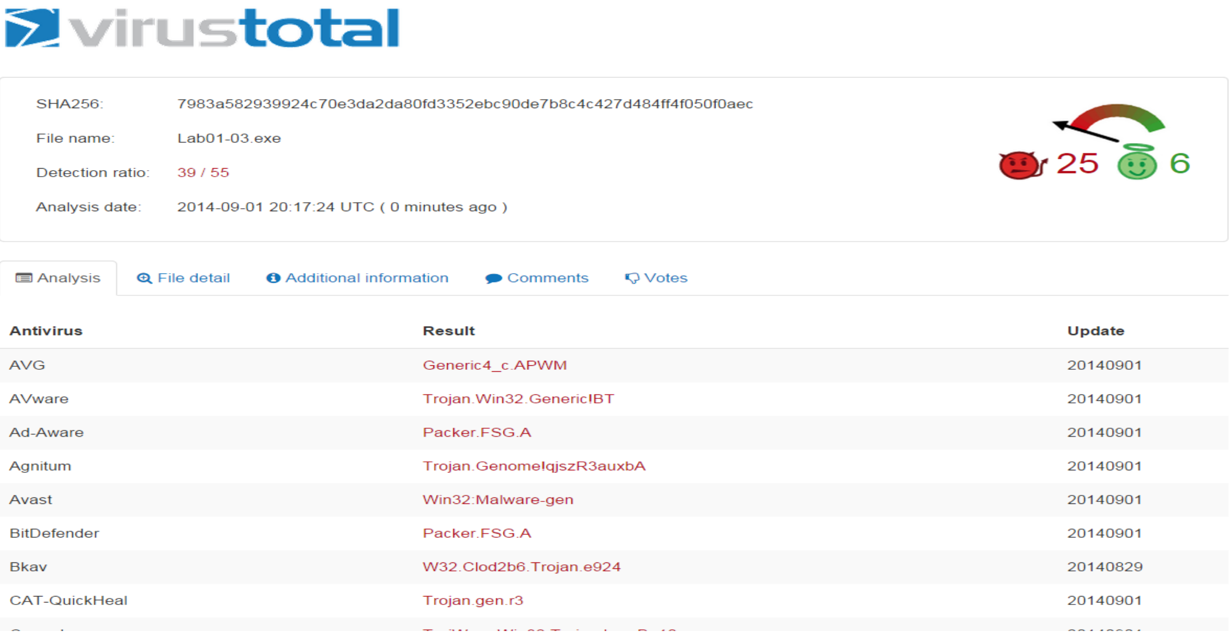
Q2: Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

Q3: Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

Q4: What host or network-based indicators could be used to identify this malware on infected machines?

Solution:

1. Like all the previous labs, yes it does! Figure below shows the existing antivirus definitions.



virustotal

SHA256: 7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

File name: Lab01-03.exe

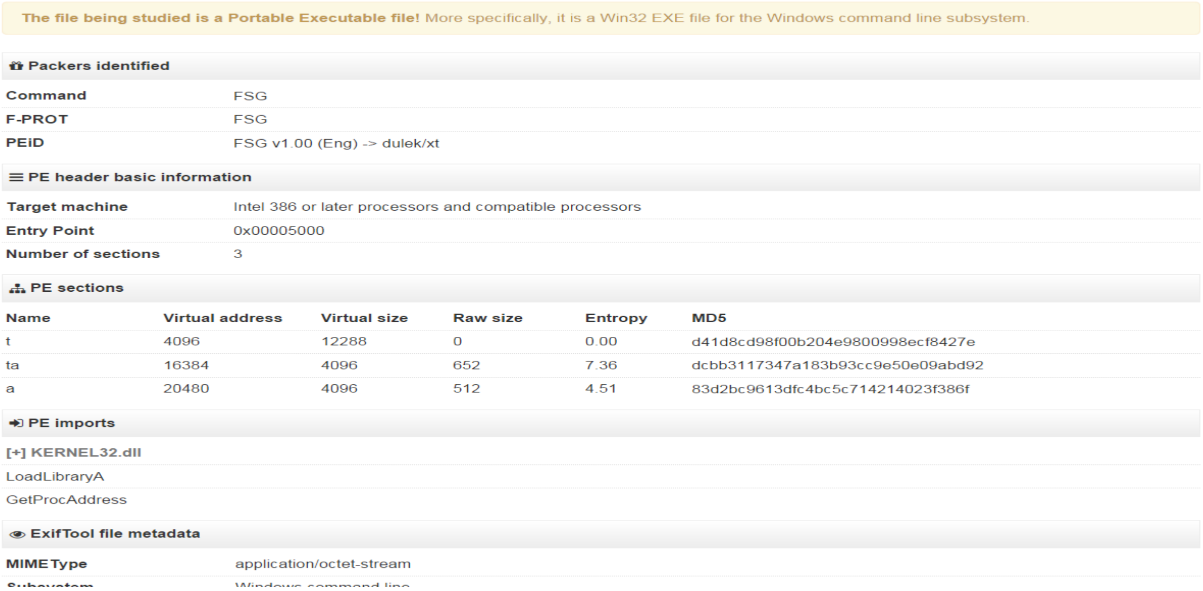
Detection ratio: 39 / 55

Analysis date: 2014-09-01 20:17:24 UTC (0 minutes ago)

Antivirus	Result	Update
AVG	Generic4_c.APWM	20140901
AVware	Trojan.Win32.Generic!BT	20140901
Ad-Aware	Packer.FSG.A	20140901
Agnitum	Trojan.GenomeIqjszR3auxbA	20140901
Avast	Win32:Malware-gen	20140901
BitDefender	Packer.FSG.A	20140901
Bkav	W32.Clod2b6.Trojan.e924	20140829
CAT-QuickHeal	Trojan.gen.r3	20140901

Figure 16: Lab01-03.exe antivirus definition

2. From www.virustotal.com we can see that the file is **FSG**-packed (as shown in the Figure below). However the file could not be analyzed when tried with PEview.



The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows command line subsystem.

Packers identified

Command	FSG
F-PROT	FSG
PEiD	FSG v1.00 (Eng) -> dulek/xt

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Entry Point	0x00005000
Number of sections	3

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
t	4096	12288	0	0.00	d41d8cd98f00b204e9800998ecf8427e
ta	16384	4096	652	7.36	dcbb3117347a183b93cc9e50e09abd92
a	20480	4096	512	4.51	83d2bc9613dfc4bc5c714214023f386f

PE imports

[+] KERNEL32.dll

LoadLibraryA

GetProcAddress

ExifTool file metadata

MIMEType	application/octet-stream
Subsystem	Windows command line

Figure 17: Lab01-03.exe FSG-Packed

3. Considering the file could not be analyzed using PEview and www.virustotal.com only shows 1 import which is **KERNEL32.dll** with files *LoadLibraryA* and *GetProcAddress* (as seen in figure above), we don't have sufficient information to tell what the file does.

4. As a result of lack of imports, we don't have sufficient information to answer this question.

Lab 1-4

Questions:

Q1: Upload the file *Lab01-04.exe* file to http://virustotal.com/. Does it match any existing antivirus definitions?

Q2: Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

Q3: When was this program compiled?

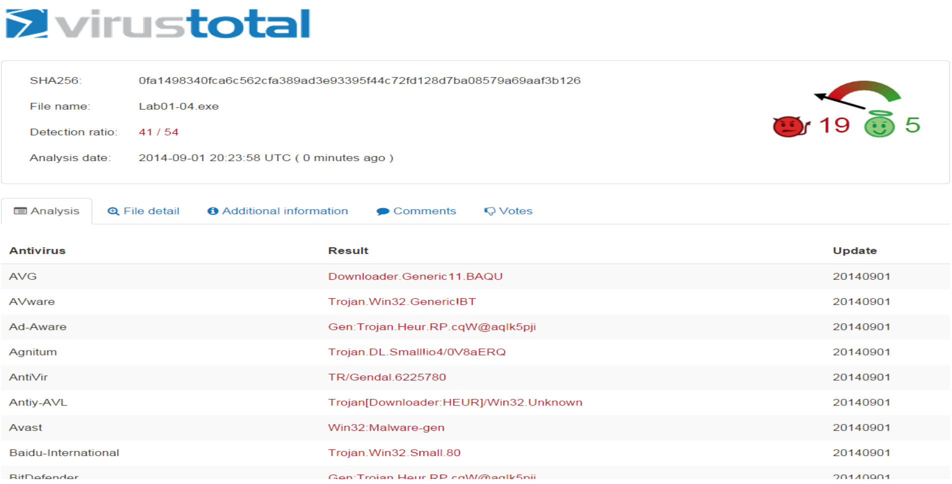
Q4: Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?

Q5: What host or network-based indicators could be used to identify this malware on infected machines?

Q6: This file has one resource in the resource section. Use resource hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

Solution:

1. Yes it does! The figure below shows the existing antivirus definitions from www.virustotal.com



SHA256: 0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

File name: Lab01-04.exe

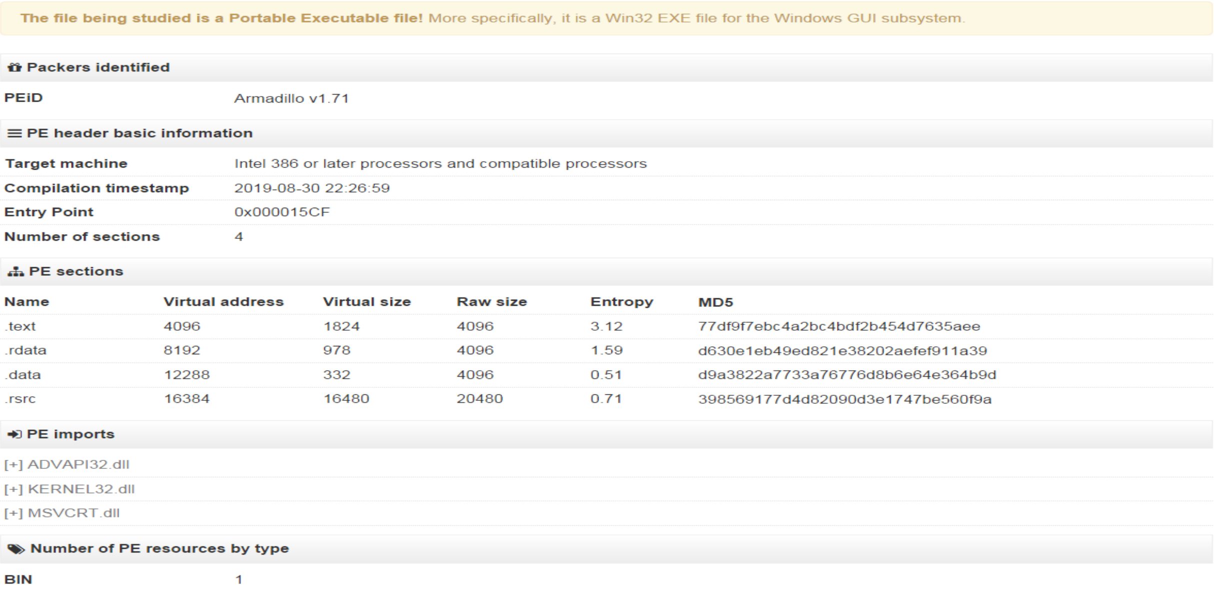
Detection ratio: 41 / 54

Analysis date: 2014-09-01 20:23:58 UTC (0 minutes ago)

Antivirus	Result	Update
AVG	Downloader.Generic11.BAQU	20140901
AVware	Trojan.Win32.Generic!BT	20140901
Ad-Aware	Gen:Trojan.Heur.RP.cqW@aqlk5pji	20140901
Agnitum	Trojan.DL.Small!io4/0V8aERQ	20140901
AntiVir	TR/Gendal.6225780	20140901
Antiy-AVL	Trojan[Downloader:HEUR]/Win32.Unknown	20140901
Avast	Win32:Malware-gen	20140901
Baidu-International	Trojan.Win32.Small.80	20140901
BitDefender	Gen:Trojan.Heur.RP.cqW@aqlk5pji	20140901

Figure 18: Lab01-04.exe virus definitions

2. As shown in figures below. The results from both www.virustotal.com and PEview did not show that the file is packed or obfuscated.



The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

Packers identified

PEiD	Armadillo v1.71

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2019-08-30 22:26:59
Entry Point	0x000015CF
Number of sections	4

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	1824	4096	3.12	77df9f7ebc4a2bc4bdf2b454d7635aee
.rdata	8192	978	4096	1.59	d630e1eb49ed821e38202aefef911a39
.data	12288	332	4096	0.51	d9a3822a7733a76776d8b6e64e364b9d
.rsrc	16384	16480	20480	0.71	398569177d4d82090d3e1747be560f9a

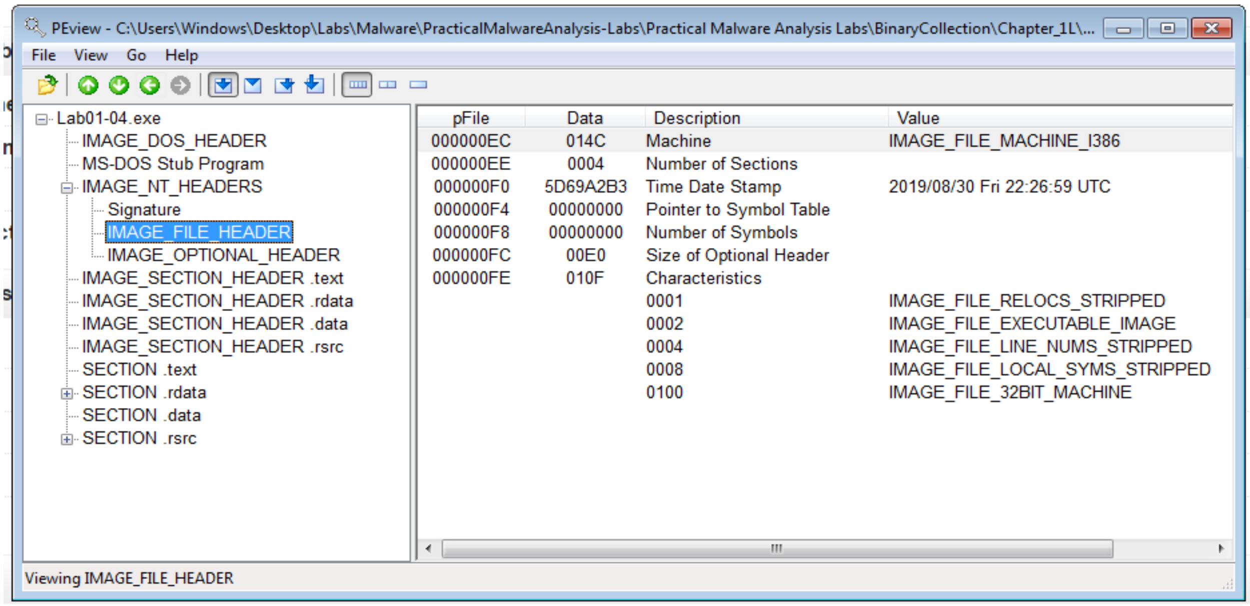
PE imports

[+] ADVAPI32.dll
[+] KERNEL32.dll
[+] MSVCRT.dll

Number of PE resources by type

BIN	1

Figure 19 – *Lab01-04.exe* packing information from www.virustotal.com

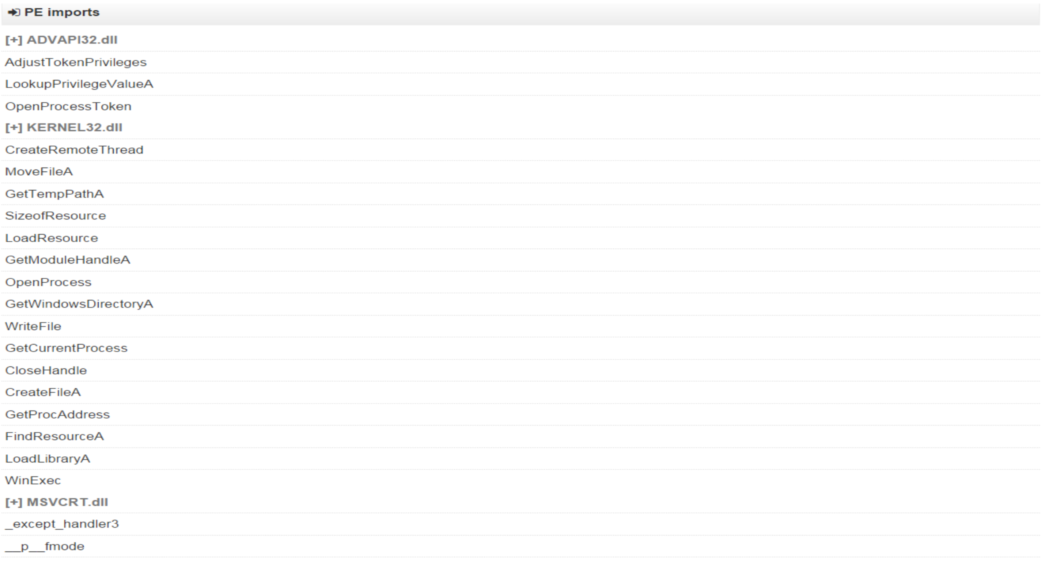

PEview - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\...
File
View
Go
Help
Lab01-04.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .rsrc
Viewing IMAGE_FILE_HEADER

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

Figure 20: *Lab01-04.exe* packing information from PEview

3. According to the information on both figures above, the file was compiled 2019/08/30. Obviously this is wrong, and therefore the compilation date cannot be determined.

4. From the figure below, some of the imports, especially the ones under ADVAPI32.dll can be attributed to files permissions. Also the import from KERNEL32.dll and MSVCRT.dll tells us that the program manipulates files by reading/writing and also executes to disk.



```
PE imports
[+] ADVAPI32.dll
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
[+] KERNEL32.dll
CreateRemoteThread
MoveFileA
GetTempPathA
SizeofResource
LoadResource
GetModuleHandleA
OpenProcess
GetWindowsDirectoryA
WriteFile
GetCurrentProcess
CloseHandle
CreateFileA
GetProcAddress
FindResourceA
LoadLibraryA
WinExec
[+] MSVCRT.dll
_except_handler3
__p__fmode
```

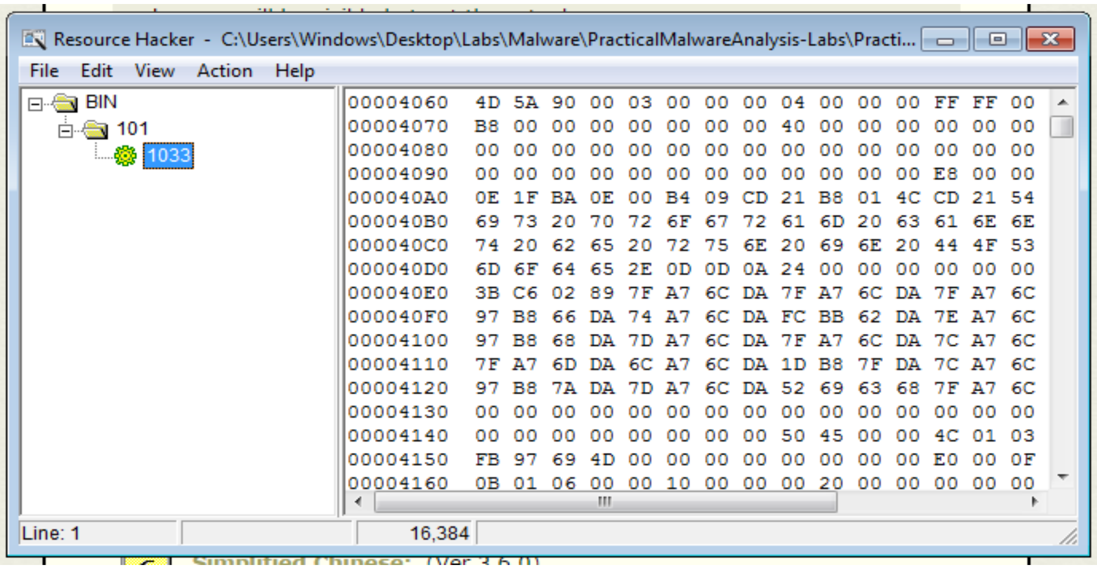
Figure21: Lab01-04.exe imports

5. Same approach used in previous labs can be followed. IP address and subnets is always a good start in identifying infected machines. Thoroughly analyzing the IP address and knowing where the address routes to, or if it redirects to a certain location is a good network-based indicator to use on malware systems. Most times malwares don't really change the behavior of the victim, but in most cases if reroutes all information and data to a specific drop point, usually the dumping site of the fraudster. Carefully analyzing the addresses of the host and network could be a great indicator for analyzing malware in infected systems.

6. As shown in the figure below, Resource Hacker was used to examine the program, however the result from Resource Hacker was difficult to analyze, considering everything is in binary format. To continue analyzing the file we had to view it in PEview.

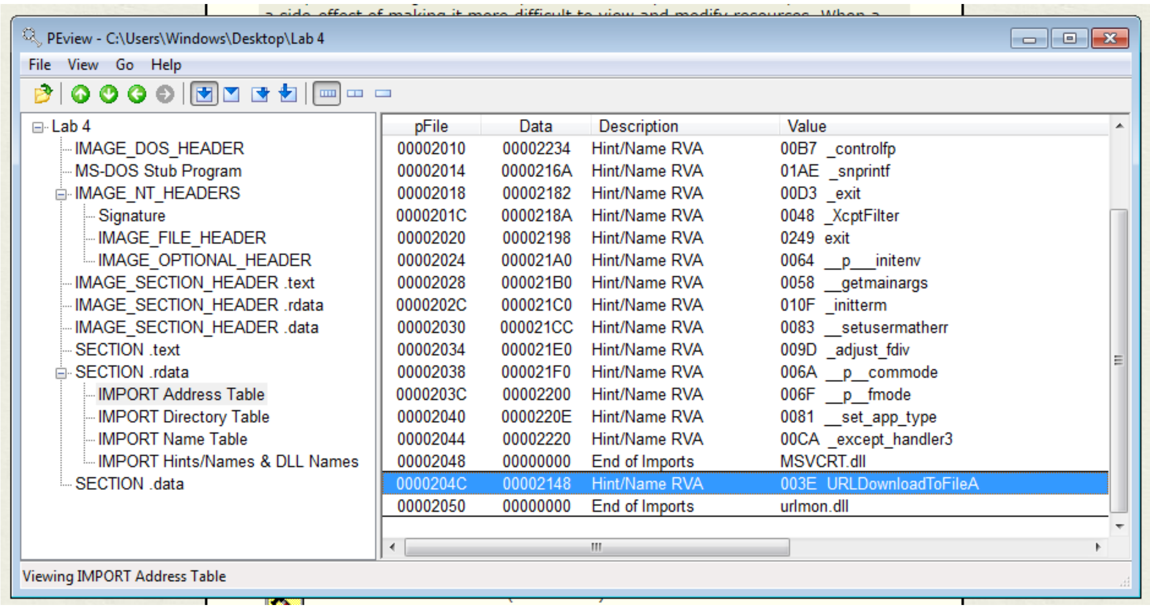
   In other to do that, first we had to save the resource as binary files by clicking on Action and then Save resource as a binary file. After saving the resource file, we then open it using PEview as shown in the figure below.

Looking at the imports, there is a file *URLDownloadToFile*, this is a common file used by malicious downloaders. There is also another file *WinExec* which probably executes the downloaded file.


Resource Hacker - C:\Users\Windows\Desktop\Labs\Malware\PracticalMalwareAnalysis-Labs\Practi...
File
Edit
View
Action
Help
BIN
101
1033
Line: 1
16,384

```
00004060  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00
00004070  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00
00004080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004090  00 00 00 00 00 00 00 00 00 00 00 E8 00 00
000040A0  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54
000040B0  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E
000040C0  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53
000040D0  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00
000040E0  3B C6 02 89 7F A7 6C DA 7F A7 6C DA 7F A7 6C
000040F0  97 B8 66 DA 74 A7 6C DA FC BB 62 DA 7E A7 6C
00004100  97 B8 68 DA 7D A7 6C DA 7F A7 6C DA 7C A7 6C
00004110  7F A7 6D DA 6C A7 6C DA 1D B8 7F DA 7C A7 6C
00004120  97 B8 7A DA 7D A7 6C DA 52 69 63 68 7F A7 6C
00004130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004140  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03
00004150  FB 97 69 4D 00 00 00 00 00 00 00 00 E0 00 0F
00004160  0B 01 06 00 00 10 00 00 00 20 00 00 00 00 00
```

Figure 22: Lab01-04.exe analyzed using Resource Hacker



pFile	Data	Description	Value
00002010	00002234	Hint/Name RVA	00B7 _controlfp
00002014	0000216A	Hint/Name RVA	01AE _snprintf
00002018	00002182	Hint/Name RVA	00D3 _exit
0000201C	0000218A	Hint/Name RVA	0048 _XcptFilter
00002020	00002198	Hint/Name RVA	0249 exit
00002024	000021A0	Hint/Name RVA	0064 __p___initenv
00002028	000021B0	Hint/Name RVA	0058 __getmainargs
0000202C	000021C0	Hint/Name RVA	010F _initterm
00002030	000021CC	Hint/Name RVA	0083 __setusermatherr
00002034	000021E0	Hint/Name RVA	009D _adjust_fdiv
00002038	000021F0	Hint/Name RVA	006A __p__commode
0000203C	00002200	Hint/Name RVA	006F __p__fmode
00002040	0000220E	Hint/Name RVA	0081 __set_app_type
00002044	00002220	Hint/Name RVA	00CA _except_handler3
00002048	00000000	End of Imports	MSVCRT.dll
0000204C	00002148	Hint/Name RVA	003E URLDownloadToFileA
00002050	00000000	End of Imports	urlmon.dll

Figure 23: Lab01-04 analyzed using PEview after saving resource as a binary file.

Conclusion

This lab aims to provide knowledge of what a malware does and how it could be analyzed. What attributes of a malware means what. Upon completion of this lab, we can understand how to find out if a program is a malware or not by uploading the file to www.virustotal.com. We can also view the compilation date of the program, which gives us an idea and an update about when the program was created; we can do that through the PEview program. We could also use some special tools such as Strings, Resource Hacker and PEiD to analyze the program more if it is a malware or not. Conclusion can be made after thoroughly analyzing the imports of each program, which clearly tells us what the program is designed to do.