Falynne Armstrong

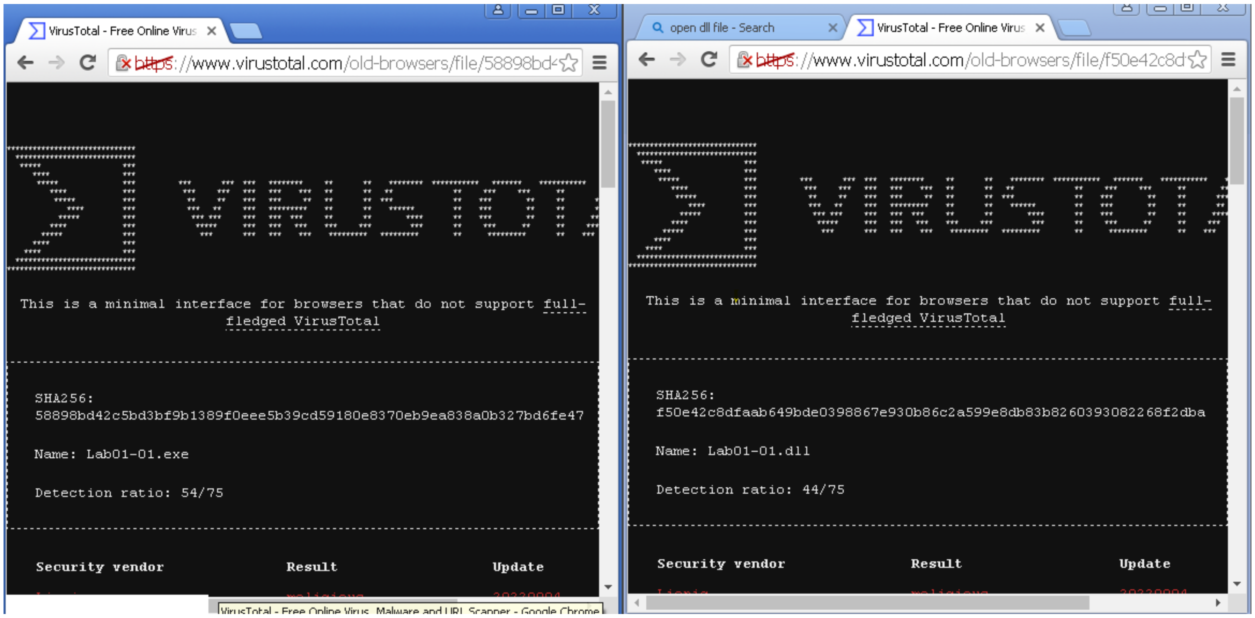
Malware

Lab 1

September 4, 2022

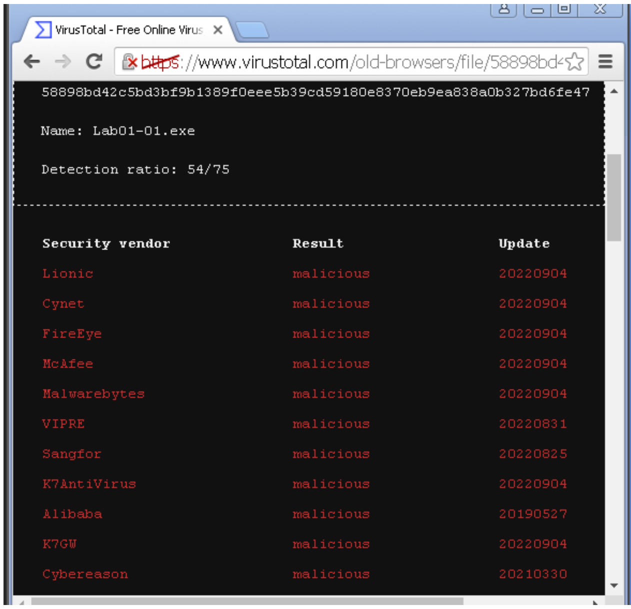
Lab 1-1

-First, I followed the instructions of the lab stating to upload the given *.dll* file and *.exe* file to VirusTotal. At first, I was using the recent website with the files. But I realized that using the newest website was not analyzing the files once uploaded. After realizing that I used the older version of VirusTotal since in this lab we are using an older model of chrome browser, I used the link https://www.virustotal.com/old-browsers/.


VirusTotal - Free Online Virus
https://www.virustotal.com/old-browsers/file/58898bd4
VIRUSTOTAL
open dll file - Search
VirusTotal - Free Online Virus
https://www.virustotal.com/old-browsers/file/f50e42c8d
VIRUSTOTAL
VirusTotal - Free Online Virus, Malware and URL Scanner - Google Chrome

```
This is a minimal interface for browsers that do not support full-
fledged VirusTotal

SHA256:
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

Name: Lab01-01.exe

Detection ratio: 54/75

Security vendor          Result          Update
```

```
This is a minimal interface for browsers that do not support full-
fledged VirusTotal

SHA256:
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

Name: Lab01-01.dll

Detection ratio: 44/75

Security vendor          Result          Update
```



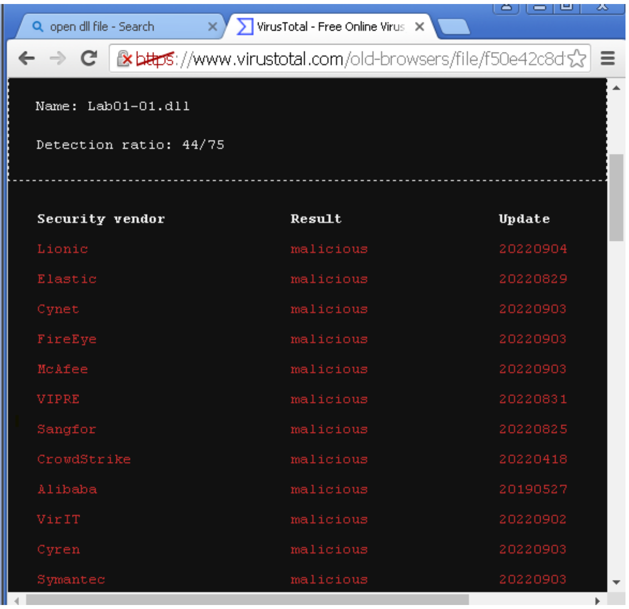
VirusTotal - Free Online Virus
https://www.virustotal.com/old-browsers/file/58898bd

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

Name: Lab01-01.exe

Detection ratio: 54/75

Security vendor	Result	Update
Lionic	malicious	20220904
Cynet	malicious	20220904
FireEye	malicious	20220904
McAfee	malicious	20220904
Malwarebytes	malicious	20220904
VIPRE	malicious	20220831
Sangfor	malicious	20220825
K7AntiVirus	malicious	20220904
Alibaba	malicious	20190527
K7GW	malicious	20220904
Cybereason	malicious	20210330



open dll file - Search
VirusTotal - Free Online Virus
https://www.virustotal.com/old-browsers/file/f50e42c8d

Name: Lab01-01.dll

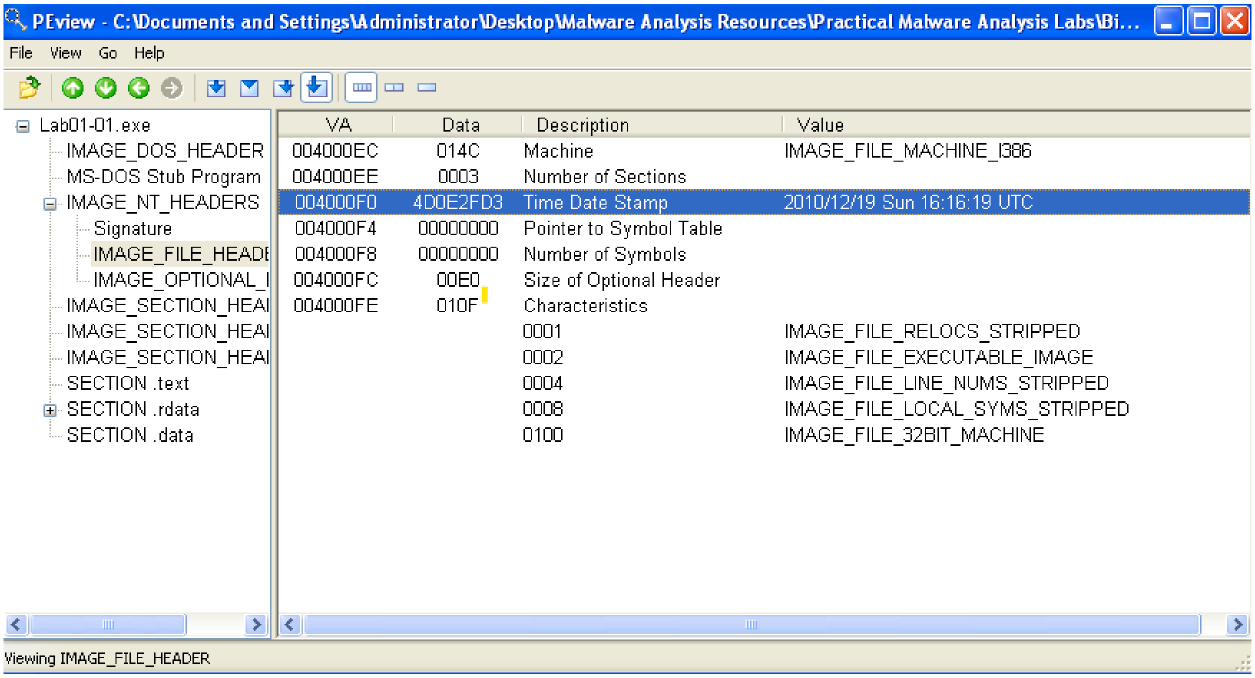
Detection ratio: 44/75

Security vendor	Result	Update
Lionic	malicious	20220904
Elastic	malicious	20220829
Cynet	malicious	20220903
FireEye	malicious	20220903
McAfee	malicious	20220903
VIPRE	malicious	20220831
Sangfor	malicious	20220825
CrowdStrike	malicious	20220418
Alibaba	malicious	20190527
VirIT	malicious	20220902
Cyren	malicious	20220903
Symantec	malicious	20220903

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

   -First, I uploaded the lab files to VirusTotal. Once done I was able to investigate and research the given name of the antiviruses. Yes, with the screenshot provided above, there are matching antivirus signatures 54/75 and 44/75.

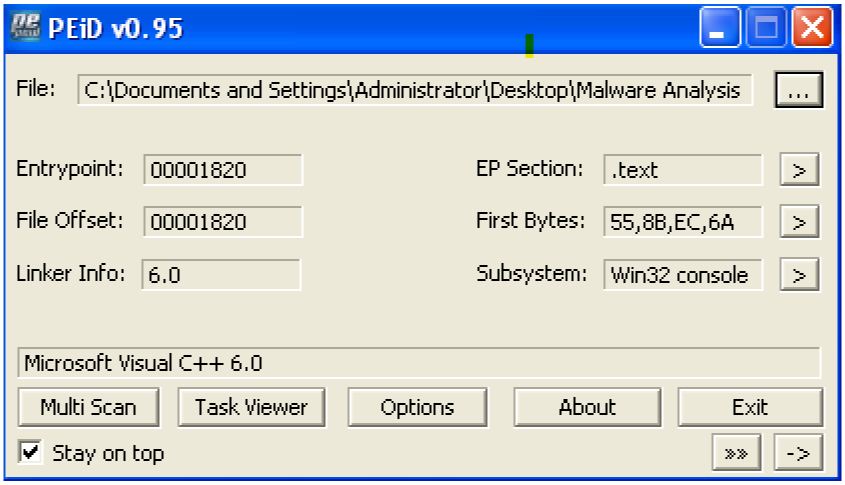
2. When were these files compiled?



VA	Data	Description	Value
004000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
004000EE	0003	Number of Sections	
004000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
004000F4	00000000	Pointer to Symbol Table	
004000F8	00000000	Number of Symbols	
004000FC	00E0	Size of Optional Header	
004000FE	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

- Using the PEView Application given with the virtual machine and uploading Lab 1-1.exe to the application, I found that the files were compiled on *2010/12/19 Sun 16:16:19.*

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



PEiD v0.95

File: C:\Documents and Settings\Administrator\Desktop\Malware Analysis

Entrypoint: 00001820

File Offset: 00001820

Linker Info: 6.0

EP Section: .text

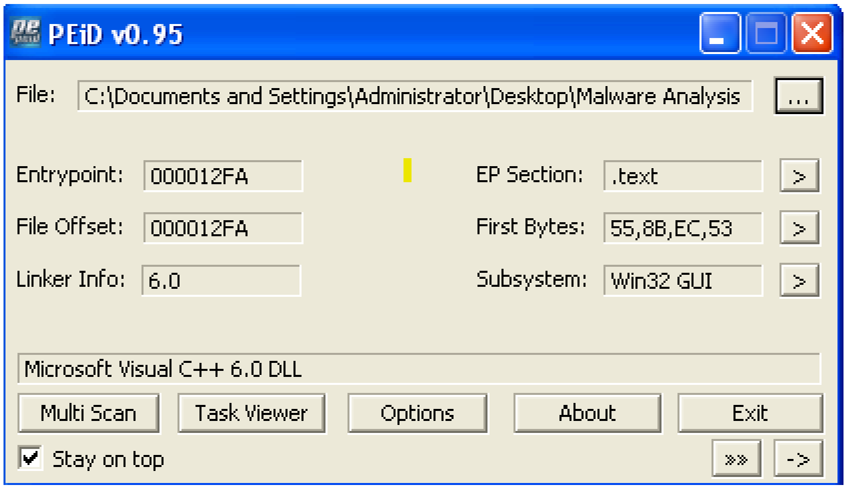
First Bytes: 55,8B,EC,6A

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

Lab 1-1.exe analysis



PEiD v0.95

File: C:\Documents and Settings\Administrator\Desktop\Malware Analysis

Entrypoint: 000012FA

File Offset: 000012FA

Linker Info: 6.0

EP Section: .text

First Bytes: 55,8B,EC,53

Subsystem: Win32 GUI

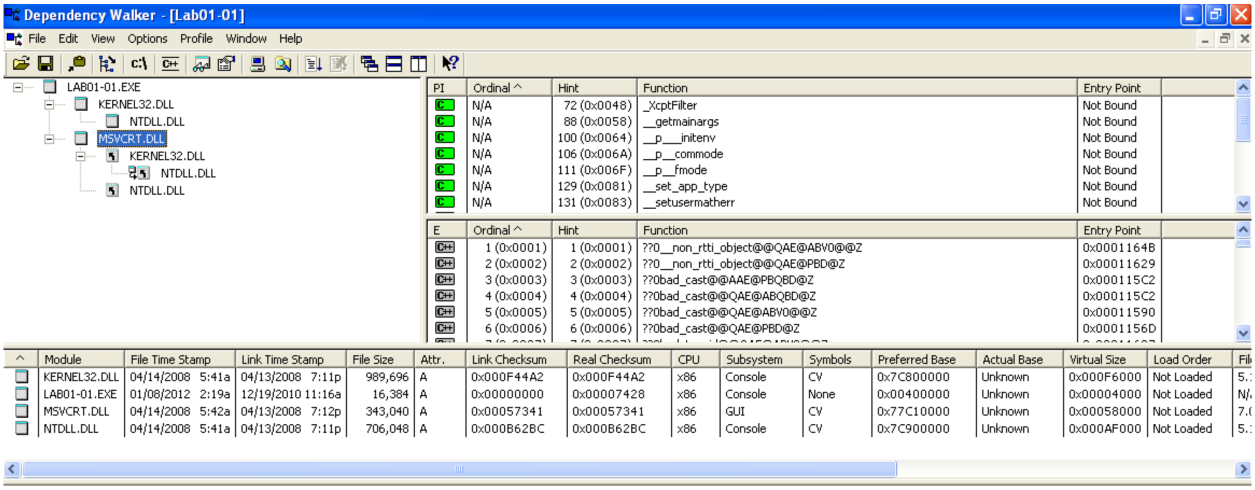
Microsoft Visual C++ 6.0 DLL

☑ Stay on top

Lab 1-1.dll analysis

-After the analysis, PEView was used to detect whether the files were packed or obfuscated. I found out that the files are not packed if the files were packed PEView would give the result of *packed.*

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


Dependency Walker - [Lab01-01]
File Edit View Options Profile Window Help

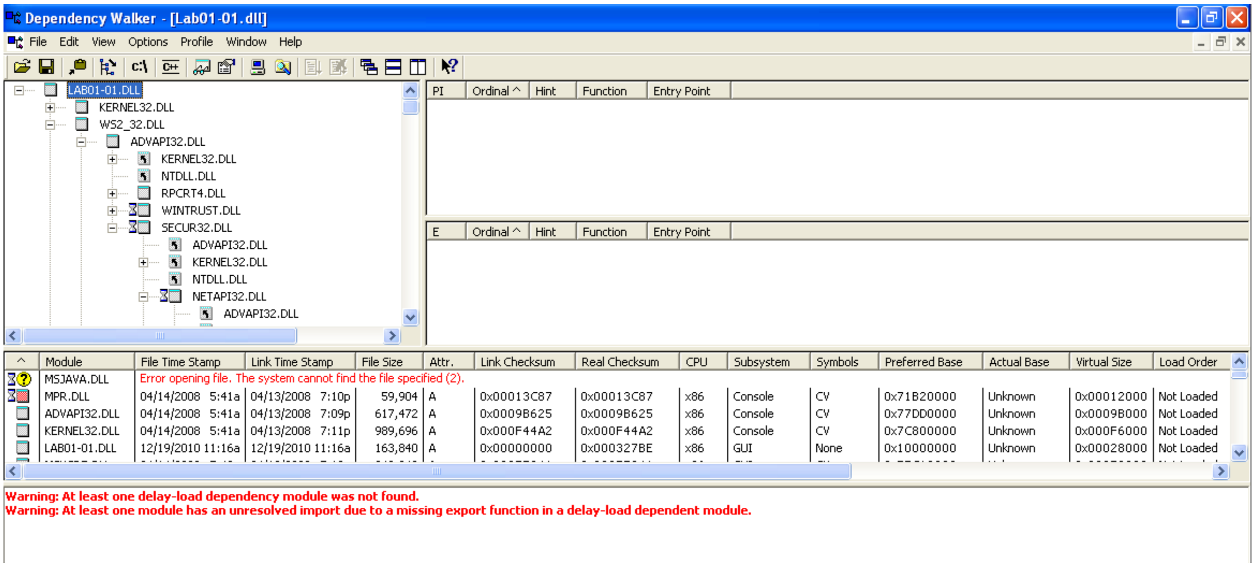
```
LAB01-01.EXE
    KERNEL32.DLL
        NTDLL.DLL
    MSVCRT.DLL
        KERNEL32.DLL
            NTDLL.DLL
        NTDLL.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	72 (0x0048)	_XcptFilter	Not Bound
C	N/A	88 (0x0058)	__getmainargs	Not Bound
C	N/A	100 (0x0064)	__p___initenv	Not Bound
C	N/A	106 (0x006A)	__p__commode	Not Bound
C	N/A	111 (0x006F)	__p__fmode	Not Bound
C	N/A	129 (0x0081)	__set_app_type	Not Bound
C	N/A	131 (0x0083)	__setusermatherr	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C++	1 (0x0001)	1 (0x0001)	??0__non_rtti_object@@QAE@ABV0@@Z	0x0001164B
C++	2 (0x0002)	2 (0x0002)	??0__non_rtti_object@@QAE@PBD@Z	0x00011629
C++	3 (0x0003)	3 (0x0003)	??0bad_cast@@AAE@PBQBD@Z	0x000115C2
C++	4 (0x0004)	4 (0x0004)	??0bad_cast@@QAE@ABQBD@Z	0x000115C2
C++	5 (0x0005)	5 (0x0005)	??0bad_cast@@QAE@ABV0@@Z	0x00011590
C++	6 (0x0006)	6 (0x0006)	??0bad_cast@@QAE@PBD@Z	0x0001156D

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	Fil
	KERNEL32.DLL	04/14/2008 5:41a	04/13/2008 7:11p	989,696	A	0x000F44A2	0x000F44A2	x86	Console	CV	0x7C800000	Unknown	0x000F6000	Not Loaded	5.:
	LAB01-01.EXE	01/08/2012 2:19a	12/19/2010 11:16a	16,384	A	0x00000000	0x00007428	x86	Console	None	0x00400000	Unknown	0x00004000	Not Loaded	N/.
	MSVCRT.DLL	04/14/2008 5:42a	04/13/2008 7:12p	343,040	A	0x00057341	0x00057341	x86	GUI	CV	0x77C10000	Unknown	0x00058000	Not Loaded	7.(
	NTDLL.DLL	04/14/2008 5:41a	04/13/2008 7:11p	706,048	A	0x000B62BC	0x000B62BC	x86	Console	CV	0x7C900000	Unknown	0x000AF000	Not Loaded	5.:

Lab 1-1.exe


Dependency Walker - [Lab01-01.dll]
File Edit View Options Profile Window Help

```
LAB01-01.DLL
    KERNEL32.DLL
    WS2_32.DLL
        ADVAPI32.DLL
            KERNEL32.DLL
            NTDLL.DLL
            RPCRT4.DLL
            WINTRUST.DLL
            SECUR32.DLL
                ADVAPI32.DLL
                KERNEL32.DLL
                NTDLL.DLL
                NETAPI32.DLL
                    ADVAPI32.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point

E	Ordinal ^	Hint	Function	Entry Point

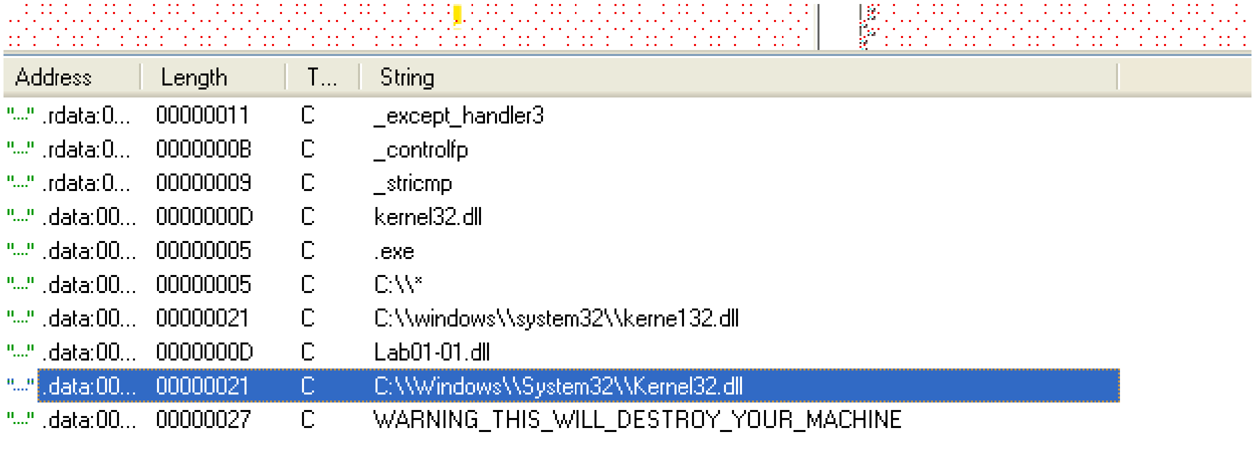
^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order
	MSJAVA.DLL	Error opening file. The system cannot find the file specified (2).												
	MPR.DLL	04/14/2008 5:41a	04/13/2008 7:10p	59,904	A	0x00013C87	0x00013C87	x86	Console	CV	0x71B20000	Unknown	0x00012000	Not Loaded
	ADVAPI32.DLL	04/14/2008 5:41a	04/13/2008 7:09p	617,472	A	0x0009B625	0x0009B625	x86	Console	CV	0x77DD0000	Unknown	0x0009B000	Not Loaded
	KERNEL32.DLL	04/14/2008 5:41a	04/13/2008 7:11p	989,696	A	0x000F44A2	0x000F44A2	x86	Console	CV	0x7C800000	Unknown	0x000F6000	Not Loaded
	LAB01-01.DLL	12/19/2010 11:16a	12/19/2010 11:16a	163,840	A	0x00000000	0x000327BE	x86	GUI	None	0x10000000	Unknown	0x00028000	Not Loaded

Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

Lab 1-1.dll

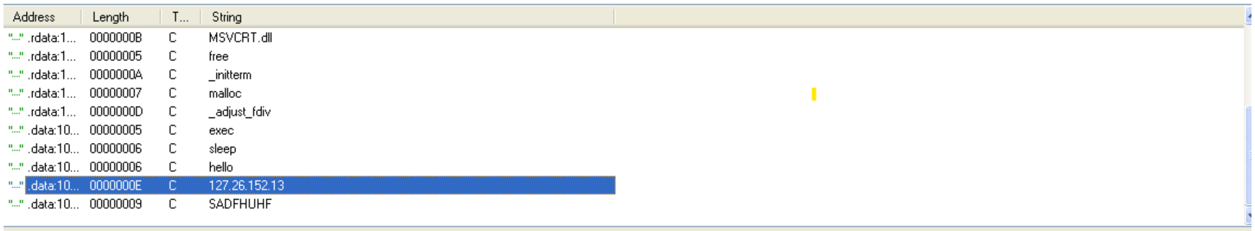
-To analyze the imports I used the application, Dependency Walker. After opening both *.exe* and *.dll* files, I could get a closer look at the import names and research the functions of the imports. Although Lab1-1.dll had very many for the lab , I only researched a few imports as this would be tedious to research all imports given. The malware hints that the function is moving and creating files.

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



Address	Length	T...	String
"..." .rdata:0...	00000011	C	_except_handler3
"..." .rdata:0...	0000000B	C	_controlfp
"..." .rdata:0...	00000009	C	_stricmp
"..." .data:00...	0000000D	C	kernel32.dll
"..." .data:00...	00000005	C	.exe
"..." .data:00...	00000005	C	C:\*
"..." .data:00...	00000021	C	C:\\windows\\system32\\kerne132.dll
"..." .data:00...	0000000D	C	Lab01-01.dll
"..." .data:00...	00000021	C	C:\\Windows\\System32\\Kernel32.dll
"..." .data:00...	00000027	C	WARNING_THIS_WILL_DESTROY_YOUR_MACHINE

Lab1-1.exe



Address	Length	T...	String
"..." .rdata:1...	0000000B	C	MSVCRT.dll
"..." .rdata:1...	00000005	C	free
"..." .rdata:1...	0000000A	C	_initterm
"..." .rdata:1...	00000007	C	malloc
"..." .rdata:1...	0000000D	C	_adjust_fdiv
"..." .data:10...	00000005	C	exec
"..." .data:10...	00000006	C	sleep
"..." .data:10...	00000006	C	hello
"..." .data:10...	0000000E	C	127.26.152.13
"..." .data:10...	00000009	C	SADFHUHF

Lab1-1.dll

-The host-based indicators hints are the *C:\\Windows\\System32\\Kernel32.dll* and the IP address that is given in the second screenshot. I found this information using IDAPro and opened open files using the strings function in the application.

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

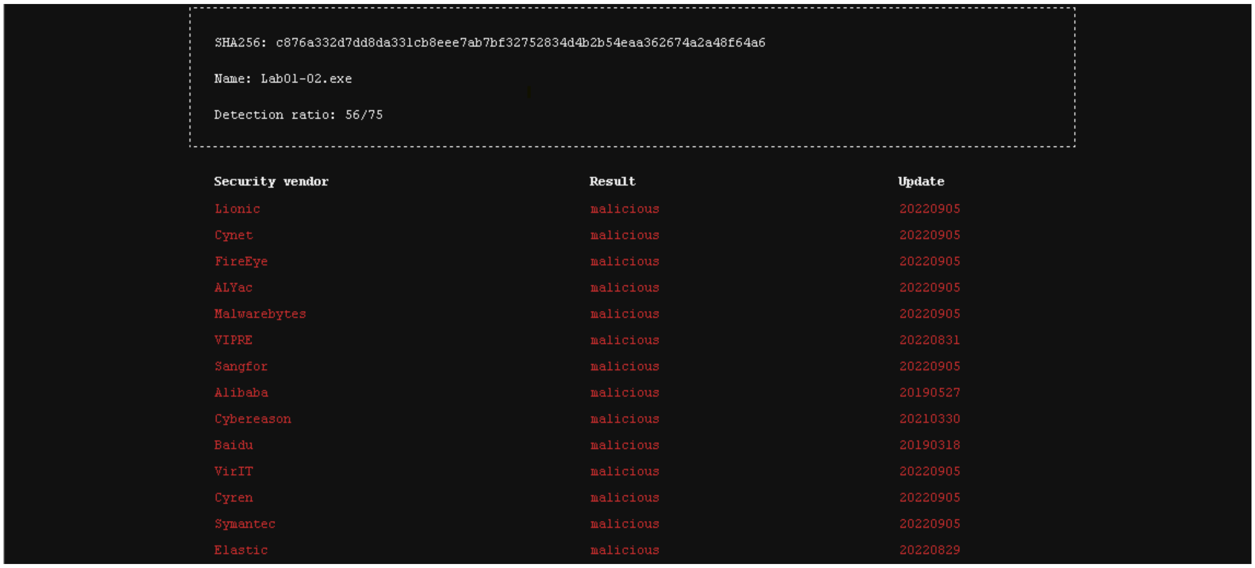
   -Within analyzing the application, I was able to network-based indicators. The network-based indicator is the IP address given in the *Lab1-1.dll* screenshot given above. With finding this IP address, it confirms that there are infected machines with this malware.

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

- After analyzing my observations and notes from the lab, I was able to get a result of the purpose of the files. The purpose of these files could be to download files.

Lab 1-2

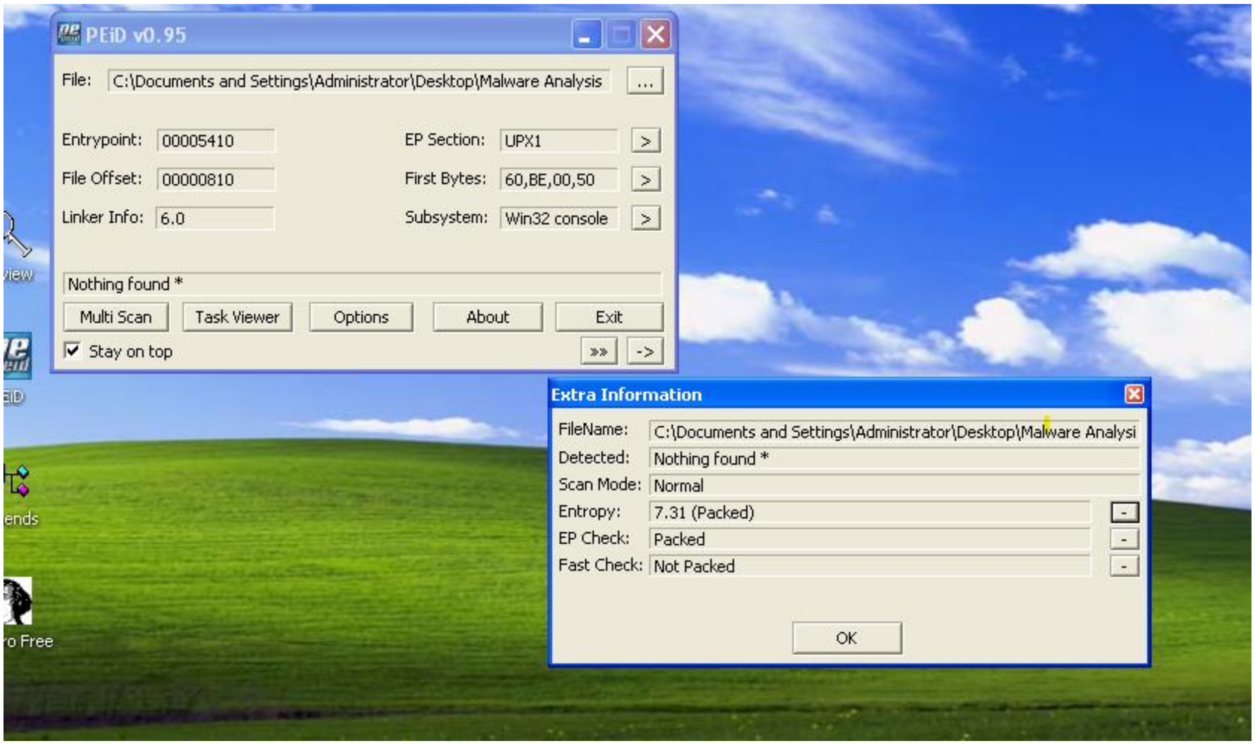
1. Upload the Lab01-02.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?



```
SHA256: c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Name: Lab01-02.exe

Detection ratio: 56/75

Security vendor                 Result                      Update
Lionic                          malicious                   20220905
Cynet                           malicious                   20220905
FireEye                         malicious                   20220905
ALYac                           malicious                   20220905
Malwarebytes                    malicious                   20220905
VIPRE                           malicious                   20220831
Sangfor                         malicious                   20220905
Alibaba                         malicious                   20190527
Cybereason                      malicious                   20210330
Baidu                           malicious                   20190318
VirIT                           malicious                   20220905
Cyren                           malicious                   20220905
Symantec                        malicious                   20220905
Elastic                         malicious                   20220829
```

- First, I uploaded the lab files to VirusTotal. Once done I was able to investigate and research the given name of the antiviruses. Yes, 56/75 matches antivirus definitions when uploading Lab1-2 to VirusTotal.

2. 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.



PEiD v0.95

File: C:\Documents and Settings\Administrator\Desktop\Malware Analysis

Entrypoint: 00005410

File Offset: 00000810

Linker Info: 6.0

EP Section: UPX1

First Bytes: 60,BE,00,50

Subsystem: Win32 console

Nothing found *

☑ Stay on top

Extra Information

FileName: C:\Documents and Settings\Administrator\Desktop\Malware Analysi

Detected: Nothing found *

Scan Mode: Normal

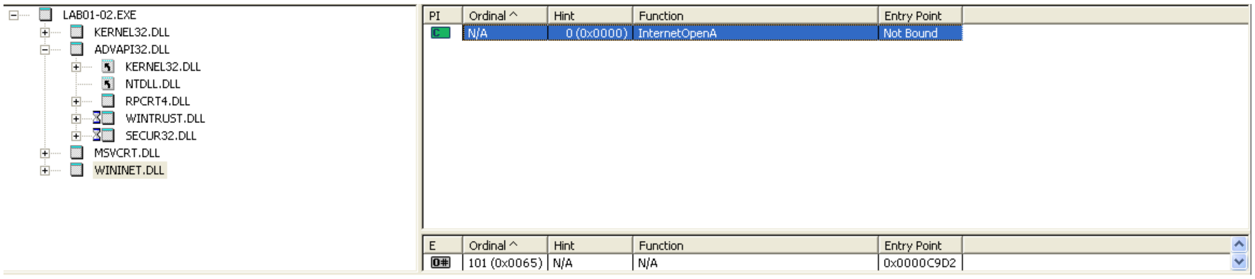
Entropy: 7.31 (Packed)

EP Check: Packed

Fast Check: Not Packed

- Using PEiD I was able to find out that the file was packed but when fast checking it is not detected as packed. I found out that the files are not packed if the files were packed PEView would give the result of *packed.*

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



```
LAB01-02.EXE
  KERNEL32.DLL
  ADVAPI32.DLL
    KERNEL32.DLL
    NTDLL.DLL
    RPCRT4.DLL
    WINTRUST.DLL
    SECUR32.DLL
  MSVCRT.DLL
  WININET.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	InternetOpenA	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
0#	101 (0x0065)	N/A	N/A	0x0000C9D2

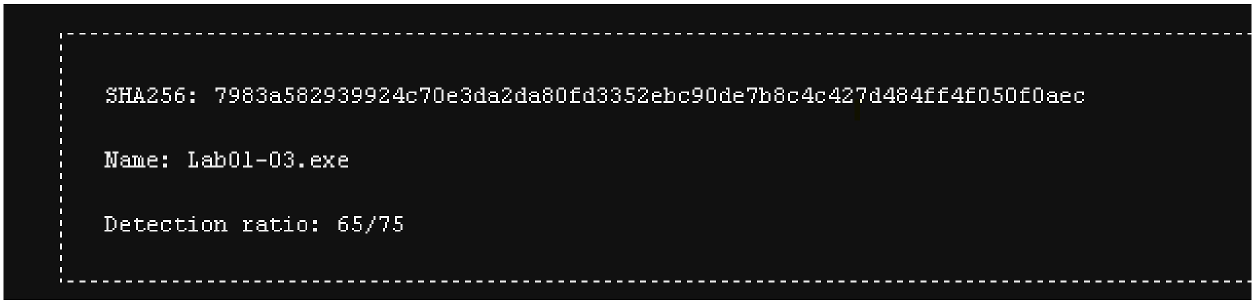
- The imports are telling me that the program is using the Internet as well as *CreateServiceA,* I believe that the malware may be creating a service for itself in the program.

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

- When analyzing the host based indicator, I was able to find a webpage. The host-based indicator that I found using IdaPro was a URL that is labeled as [*http://www.malwareanalysisbook.com*](http://www.malwareanalysisbook.com)

Lab 1-3

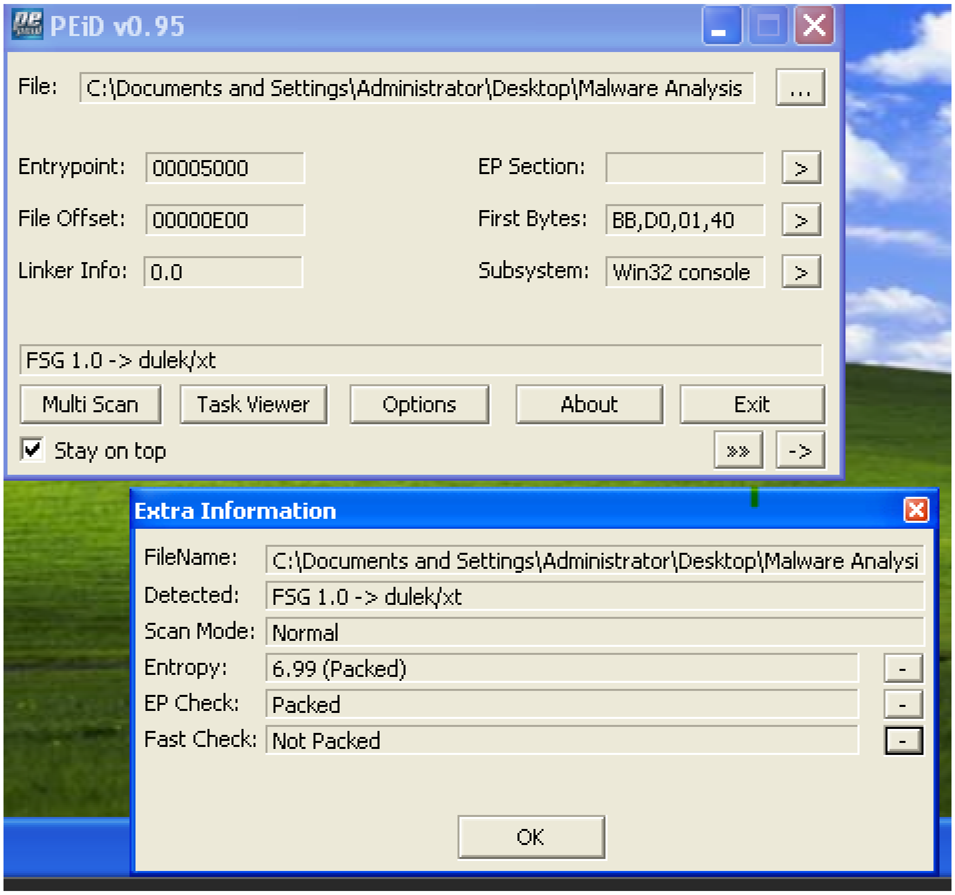
1. Upload the Lab01-03.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?



```
SHA256: 7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

Name: Lab01-03.exe

Detection ratio: 65/75
```

- First, I uploaded the lab files to VirusTotal. Once done I was able to investigate and research the given name of the antiviruses. I was able to find that 65/75 matches existing antivirus definitions.

2. 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.



File: C:\Documents and Settings\Administrator\Desktop\Malware Analysis

Entrypoint: 00005000

EP Section:

File Offset: 00000E00

First Bytes: BB,D0,01,40

Linker Info: 0.0

Subsystem: Win32 console

FSG 1.0 -> dulek/xt

☑ Stay on top

Extra Information

FileName: C:\Documents and Settings\Administrator\Desktop\Malware Analysi

Detected: FSG 1.0 -> dulek/xt

Scan Mode: Normal

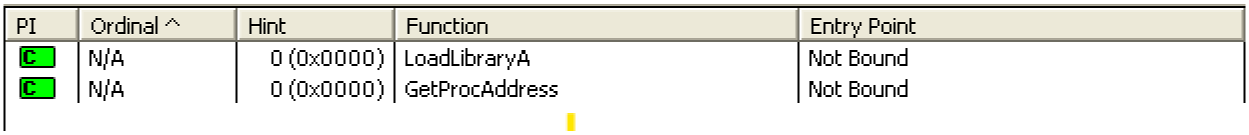
Entropy: 6.99 (Packed)

EP Check: Packed

Fast Check: Not Packed

- *Lab1-03.exe* is packed, I was able to indicate this using the application PEiD. I was not able to unpack this file as I could not find an unpacker for FSG 1.0. Though when fast checking the program it gives a result of *not packed*.

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



PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	LoadLibraryA	Not Bound
C	N/A	0 (0x0000)	GetProcAddress	Not Bound

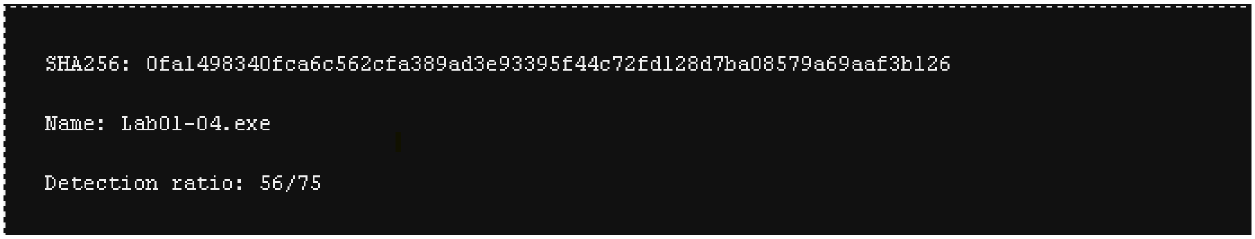
- I believe that these functionalities aren't hinting more at showing the process of the program. Although since I was not able to unpack the program, I could not find any hints as well.

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

-Since I was not able to unpack the file, I could not get any results of host or network-based indicators.

Lab 1-4

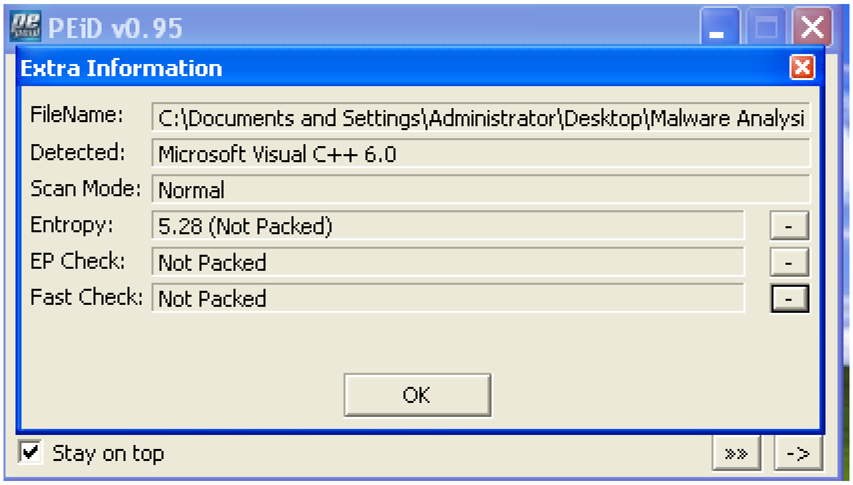
1. Upload the Lab01-04.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?



```
SHA256: 0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

Name: Lab01-04.exe

Detection ratio: 56/75
```

- First, I uploaded the lab files to VirusTotal. Once done I was able to investigate and research the given name of the antiviruses. After I was able to analyze and discover that 56/75 matches existing antivirus definitions.

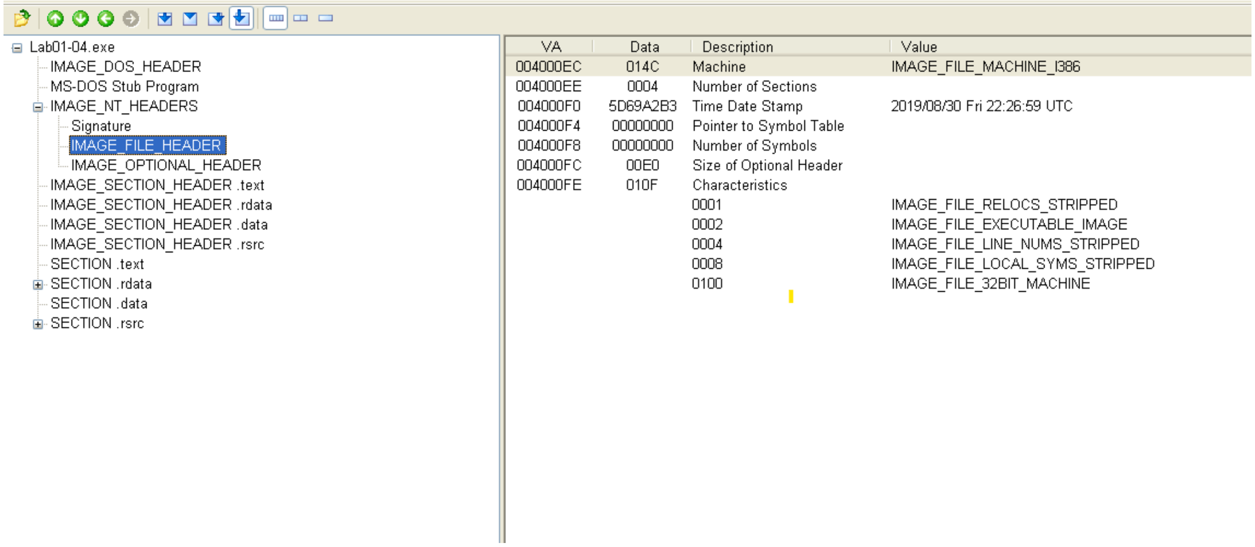
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.



FileName: C:\Documents and Settings\Administrator\Desktop\Malware Analysi
Detected: Microsoft Visual C++ 6.0
Scan Mode: Normal
Entropy: 5.28 (Not Packed)
EP Check: Not Packed
Fast Check: Not Packed

- Yes, there are indicators that the file is not packed, after uploading the Lab-04.exe to PEiD.

3. When was this program compiled?

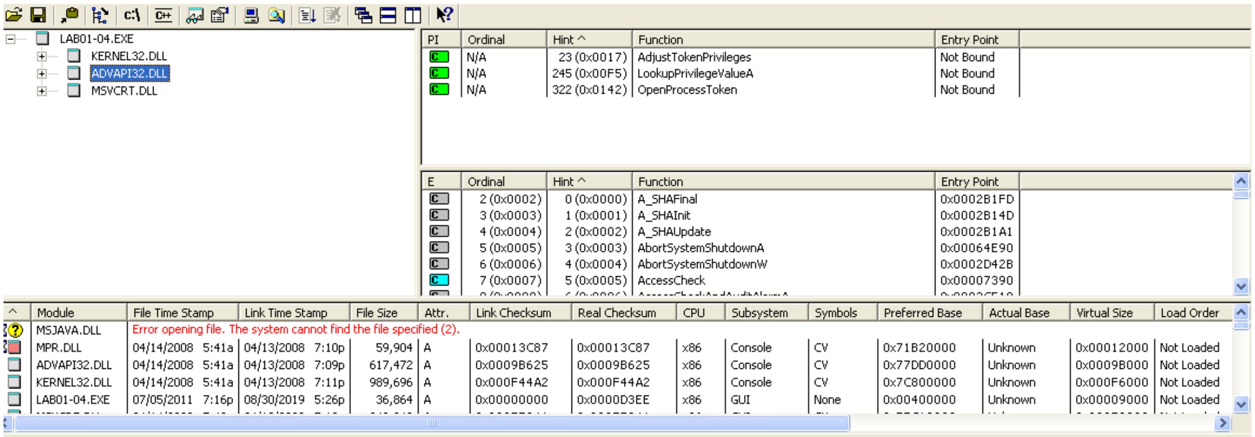


- Lab01-04.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
    - Signature
    - IMAGE_FILE_HEADER
    - IMAGE_OPTIONAL_HEADER
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .rsrc
  - SECTION .text
  - SECTION .rdata
  - SECTION .data
  - SECTION .rsrc

VA	Data	Description	Value
004000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
004000EE	0004	Number of Sections	
004000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
004000F4	00000000	Pointer to Symbol Table	
004000F8	00000000	Number of Symbols	
004000FC	00E0	Size of Optional Header	
004000FE	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

- After uploading the program to PEView I was able to view when the program was compiled. The program was compiled on *2019/08/30 Fri 22:26:59*.

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



- LAB01-04.EXE
  - KERNEL32.DLL
  - ADVAPI32.DLL
  - MSVCRT.DLL

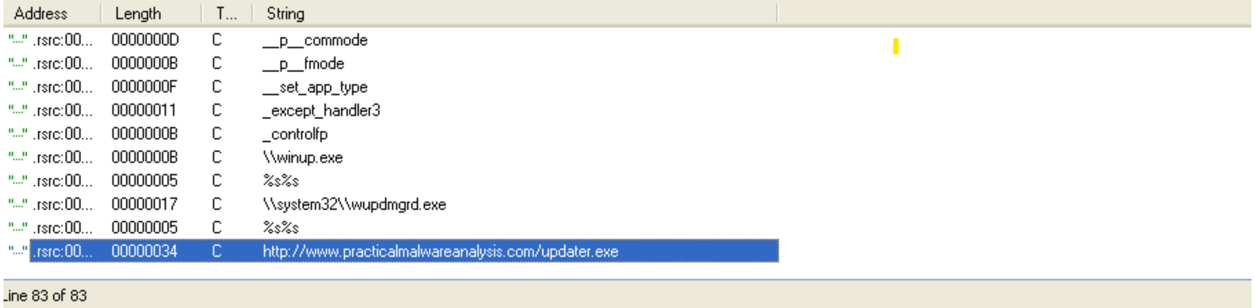
PI	Ordinal	Hint ^	Function	Entry Point
C	N/A	23 (0x0017)	AdjustTokenPrivileges	Not Bound
C	N/A	245 (0x00F5)	LookupPrivilegeValueA	Not Bound
C	N/A	322 (0x0142)	OpenProcessToken	Not Bound

E	Ordinal	Hint ^	Function	Entry Point
C	2 (0x0002)	0 (0x0000)	A_SHAFinal	0x0002B1FD
C	3 (0x0003)	1 (0x0001)	A_SHAInit	0x0002B14D
C	4 (0x0004)	2 (0x0002)	A_SHAUpdate	0x0002B1A1
C	5 (0x0005)	3 (0x0003)	AbortSystemShutdownA	0x00064E90
C	6 (0x0006)	4 (0x0004)	AbortSystemShutdownW	0x0002D42B
C	7 (0x0007)	5 (0x0005)	AccessCheck	0x00007390

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order
MSJAVA.DLL	Error opening file. The system cannot find the file specified (2).												
MPR.DLL	04/14/2008 5:41a	04/13/2008 7:10p	59,904	A	0x00013C87	0x00013C87	x86	Console	CV	0x71B20000	Unknown	0x00012000	Not Loaded
ADVAPI32.DLL	04/14/2008 5:41a	04/13/2008 7:09p	617,472	A	0x0009B625	0x0009B625	x86	Console	CV	0x77DD0000	Unknown	0x0009B000	Not Loaded
KERNEL32.DLL	04/14/2008 5:41a	04/13/2008 7:11p	989,696	A	0x000F44A2	0x000F44A2	x86	Console	CV	0x7C800000	Unknown	0x000F6000	Not Loaded
LAB01-04.EXE	07/05/2011 7:16p	08/30/2019 5:26p	36,864	A	0x00000000	0x0000D3EE	x86	GUI	None	0x00400000	Unknown	0x00009000	Not Loaded

-After analyzing and discovering the functionalities of file, I was able to also find beneficial functionalities for the files. Some hints with the program's functionality are having privileges, opening a process, and using a Windows executable.

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

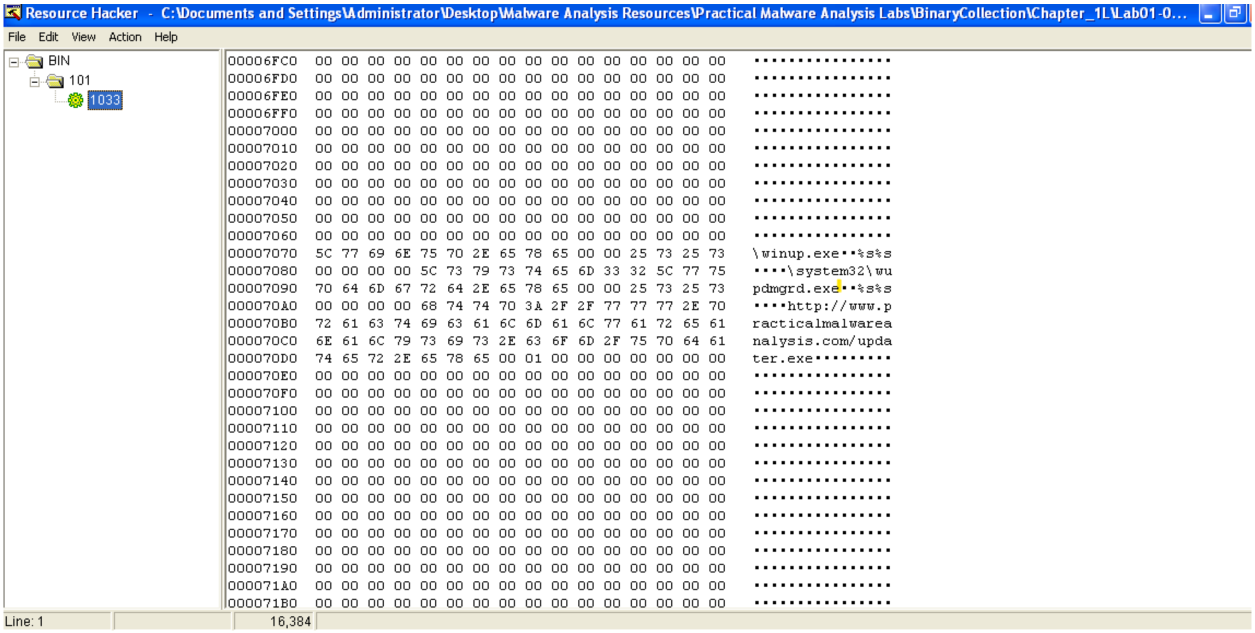


Address	Length	T...	String
"..." .rsrc:00...	0000000D	C	__p__commode
"..." .rsrc:00...	0000000B	C	__p__fmode
"..." .rsrc:00...	0000000F	C	__set_app_type
"..." .rsrc:00...	00000011	C	_except_handler3
"..." .rsrc:00...	0000000B	C	_controlfp
"..." .rsrc:00...	0000000B	C	\\winup.exe
"..." .rsrc:00...	00000005	C	%s%s
"..." .rsrc:00...	00000017	C	\\system32\\wupdmgrd.exe
"..." .rsrc:00...	00000005	C	%s%s
"..." .rsrc:00...	00000034	C	http://www.practicalmalwareanalysis.com/updater.exe

Line 83 of 83

-In IdaPro I was able to find an indicator that was labeled http://www.practicalmalwareanalysis.com/updater.exe. Within this website, I believe that the infected malware is coming from a updater that is an extension file.

5. 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?



Resource Hacker - C:\Documents and Settings\Administrator\Desktop\Malware Analysis Resources\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-0...

```
00006FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00006FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00006FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00006FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007070  5C 77 69 6E 75 70 2E 65 78 65 00 00 25 73 25 73   \winup.exe··%s%s
00007080  00 00 00 00 5C 73 79 73 74 65 6D 33 32 5C 77 75   ····\system32\wu
00007090  70 64 6D 67 72 64 2E 65 78 65 00 00 25 73 25 73   pdmgrd.exe··%s%s
000070A0  00 00 00 00 68 74 74 70 3A 2F 2F 77 77 77 2E 70   ····http://www.p
000070B0  72 61 63 74 69 63 61 6C 6D 61 6C 77 61 72 65 61   racticalmalwarea
000070C0  6E 61 6C 79 73 69 73 2E 63 6F 6D 2F 75 70 64 61   nalysis.com/upda
000070D0  74 65 72 2E 65 78 65 00 01 00 00 00 00 00 00 00   ter.exe·········
000070E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
000070F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
00007190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
000071A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
000071B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ················
```

Line: 1   16,384

- After uploading the file to Resource Hacker, I found that you can create a downloadable from the file that has even more malware that could end up ruining your machine.