

Part 2 – Textbook Lab 1-1

In this section, we will analyze Lab01-01.exe and Lab01-01.dll.

1. Upload "Lab01-01.exe and Lab01-01.dll" to <http://www.VirusTotal.com/> and view the reports. Does one of the files match existing antivirus signatures? Add a screenshot and provide an explanation below:

For, Lab01-01.exe, there are 51 antivirus signatures! And its detection rate is 51/70. VirusTotal also provides checksum of this virus to identify it.

The screenshot shows the VirusTotal analysis page for the file Lab01-01.exe. The file is identified by the hash 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47. It is 16.00 KB in size and was uploaded on 2022-09-14 14:41:11 UTC. The file is flagged as malicious by 51 security vendors and 1 sandbox. The community score is 100. The file is identified as a Trojan (Trojan/Win32.Agent.C957604) by AhnLab-V3, ALYac, and Arcabit. It is also identified as a Trojan (Trojan/Win32.Aenjaris.2be749b4) by AhnLab-V3, ALYac, and Arcabit. The file is identified as a Trojan (Trojan/Win32.Aenjaris.2be749b4) by AhnLab-V3, ALYac, and Arcabit. The file is identified as a Trojan (Trojan/Win32.Aenjaris.2be749b4) by AhnLab-V3, ALYac, and Arcabit.

Security Vendor	Detection	Signature
AhnLab-V3	ⓘ	Trojan/Win32.Agent.C957604
ALYac	ⓘ	Trojan.Agent.16384SS
Arcabit	ⓘ	Trojan/Win32.Aenjaris.2be749b4
AVG	ⓘ	Win32/Malware-gen
BitDefender	ⓘ	Gen Variant/Win32.113694
Comodo	ⓘ	Malware/@#3eb40f99afetz
Cybereason	ⓘ	Malicious.82141a
Cynet	ⓘ	Malicious (score: 99)
Avast	ⓘ	Win32/Malware-gen
Avira (no cloud)	ⓘ	HEUR/AGEN.1223661
ClamAV	ⓘ	Win/Malware.Agent-6342616-0
CrowdStrike Falcon	ⓘ	Win/malicious_confidence_100% (W)
Cylance	ⓘ	Unsafe
Cyren	ⓘ	W32/Ilse.CK.gen/Eldorado

[Image] Security Vendors' Analysis

51 security vendors and 1 sandbox flagged this file as malicious

58898bd42c5bd3bf9b1389f0ee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab01-01.exe
Size: 16.00 KB
Uploaded: 2022-09-14 14:41:11 UTC
1 day ago
EXE

Community Score: 51/70

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Basic Properties

MD5	bb7425b82141a1c0f7d60e5106676bb1
SHA-1	9dca39ac1bd36d877fbb0025ee88daff0627cbb
SHA-256	58898bd42c5bd3bf9b1389f0ee5b39cd59180e8370eb9ea838a0b327bd6fe47
Vhash	014036151d1bza0f-z
Authenticash	094eed7cfc959fd9ba704d5fe0b965b7bbb6ca09d302870935dc0508d940ba2c
Imphash	2b5f75aa75c7ed7c687be49d63605
Rich PE header hash	6a52cc2e068db82b4715556d89a96
SSDEEP	96:18Y5CuDzp17S5eVIV2cFL+31znx9+NNoyM:v6Y71755erCZ+FznxcNNoyM
TLSH	T17C72B44376E51CB1EF2811B6429283FC927DE0604766F2EE78731A46D432893793CADB
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
TriD	Microsoft Visual C++ compiled executable (generic) (40.3%)
TriD	Win32 Dynamic Link Library (generic) (16%)
TriD	Win16 NE executable (generic) (12.3%)
TriD	Win32 Executable (generic) (11%)
TriD	Win32 Executable MS Visual FoxPro 7 (5.4%)

[Image] Checksum information about the virus

For, Lab01-01.dll, there are 45 antivirus signatures! And its detection rate is 45/69. VirusTotal also provides checksum of this virus to identify it.

45 security vendors and no sandboxes flagged this file as malicious

f50e42c8dffaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab07-03.dll
Size: 160.00 KB
Uploaded: 2022-09-16 03:12:21 UTC
18 minutes ago
DLL

Community Score: 45/69

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Security Vendors' Analysis

Alibaba	Trojan.Win32/Skeeyah.7fb0ebff	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan.Generic.ASMalwS.3E79	Arcabit	Trojan.Ulisse.D19D44
Avast	Win32.Malware-gen	AVG	Win32.Malware-gen
BitDefender	Gen.Variant.Ulisse.105796	BitDefenderTheta	Gen.NN.ZedraF.34646.kq4@aGkQVip
ClamAV	Win.Malware.Agent-6369668-0	Comodo	Malware@#2dsw4alnce61
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Skeeyah.AK.gen/Eldorado
Elastic	Malicious (high Confidence)	Emsisoft	Gen.Variant.Ulisse.105796 (B)

[Image] Security Vendors' Analysis

45 / 69

45 security vendors and no sandboxes flagged this file as malicious

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab07-03.dll
160.00 KB
2022-09-16 03:12:21 UTC
18 minutes ago

amadio pedr via-tor

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Basic Properties

MD5	290934c61de9176ad582fdd55f0a669
SHA-1	a4b35de71ca20fe776dc72d12fb2886736f43c22
SHA-256	f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Vhash	115046151d151b2505tza7z
Authenticash	f2186e6806b44e6d2106a3e528010511a5fb450448be8cb026dbc16894e080b5
Imphash	850a88b585d7874d0431e8e45d74606
Rich PE header hash	0a70ae41bf95138a8e844adbcb01dea
SSDEEP	48 aVD3M6gl4PXtLceRoCpbDla1XBtz2Wuw009WuwazHSz MhMAzLcgt5z2Wz0sWz9HS
TLSH	T10AF32EB39BE08BFFD5280B37029B49B3347A560039405AB5762C83D2F9562AD56DE1A
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win32 Dynamic Link Library (generic) (29.6%)
TrID	Win16 NE executable (generic) (22.7%)
TrID	Win32 Executable (generic) (20.3%)
TrID	OS/2 Executable (generic) (9.1%)
TrID	Generic Win/DOS Executable (9%)
File size	160.00 KB (163840 bytes)

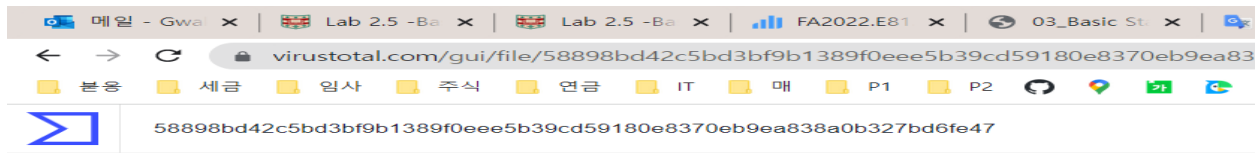
[Image] Checksum information about the virus

2. When was 'lab01-01.exe' compiled?

Use the space below to explain where you found this header, and report the compile time.

I found the compilation time stamp on VirusTotal detail information.

It was 2010-12-19 16:16:19 UC



Portable Executable Info

Compiler Products

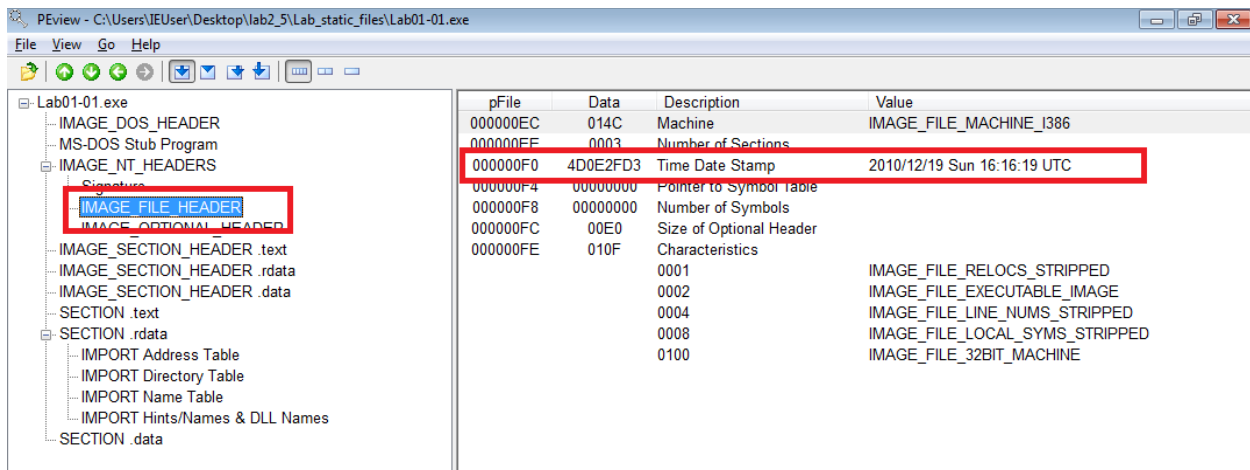
id: 12, version: 7291 count=1
 [C] VS98 (6.0) build 8168 count=11
 id: 14, version: 7299 count=1
 [LNK] VS98 (6.0) imp/exp build 8168 count=2
 [---] Unmarked objects count=27
 id: 19, version: 8034 count=3
 [C++] VS98 (6.0) build 8168 count=2

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-12-19 16:16:19 UTC
Entry Point	6176
Contained Sections	3

[Image] VirusTotal also shows us Compilation Timepstamp!

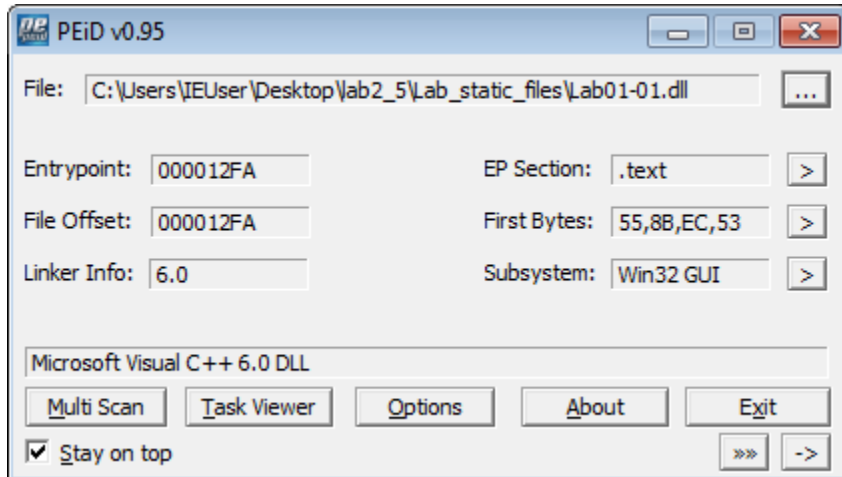
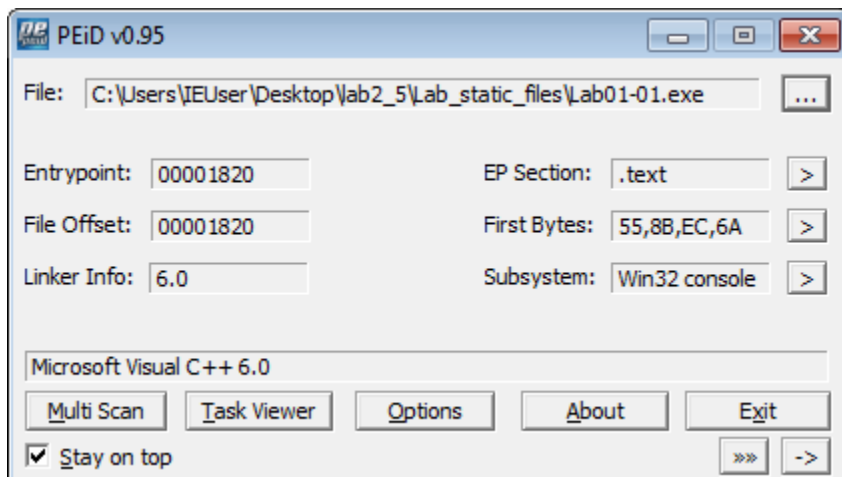
And I found also the time stamp on 'IMAGE_FILE_HEADER' using PEView.



[Image] PEView also shows us Compilation Timepstamp from the 'IMAGE_FILE_HEADER'

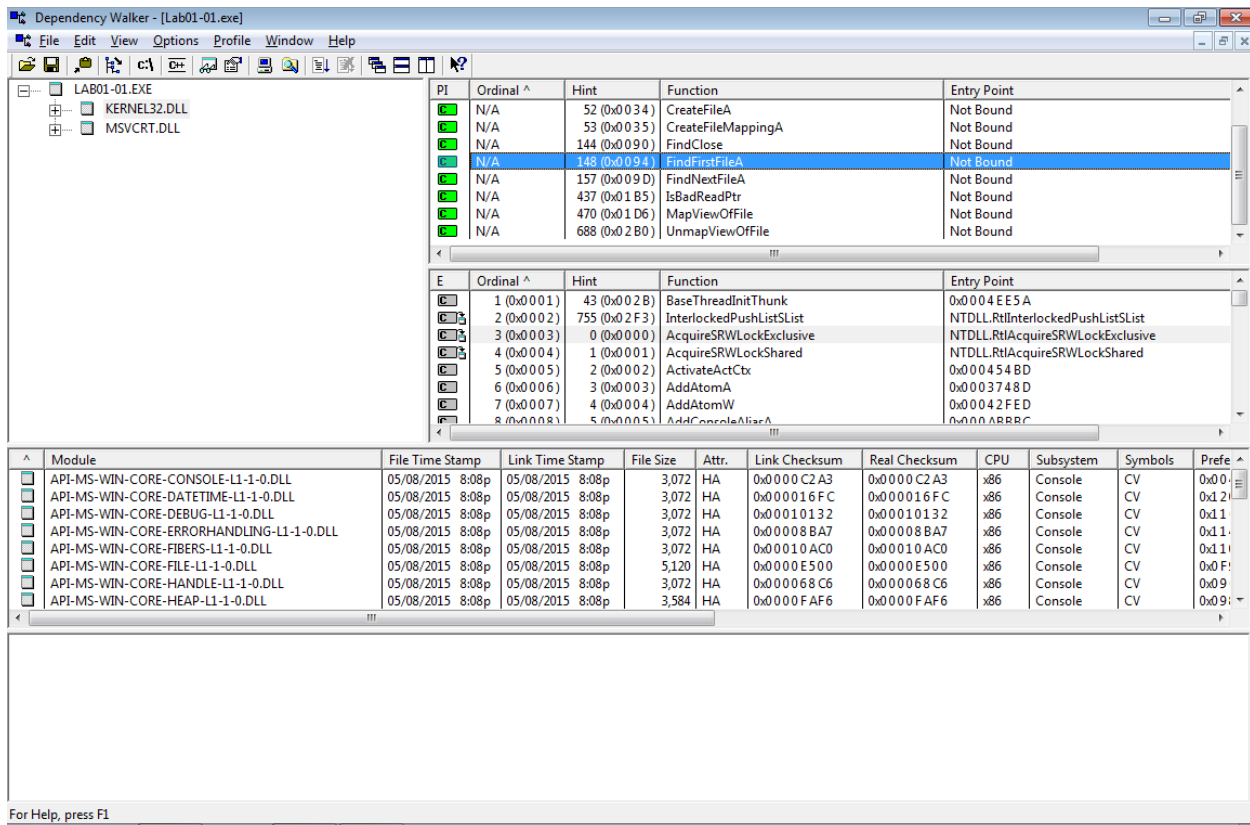
3. Use PEiD to determine what tool was used to build the program. What is it? Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?

For Lab01-01.exe and Lab01-01.dll, they were compiled by Microsoft Visual C++ 6.0. And there was no sign of any indication of packed or obfuscation. Also, I can see lots of strings when I checked through a PEXview.



4. Use dependency Walker to and look for imports and exports of 'lab01-01.exe'.
Do any imports hint at what this program does? If so, which imports are they?

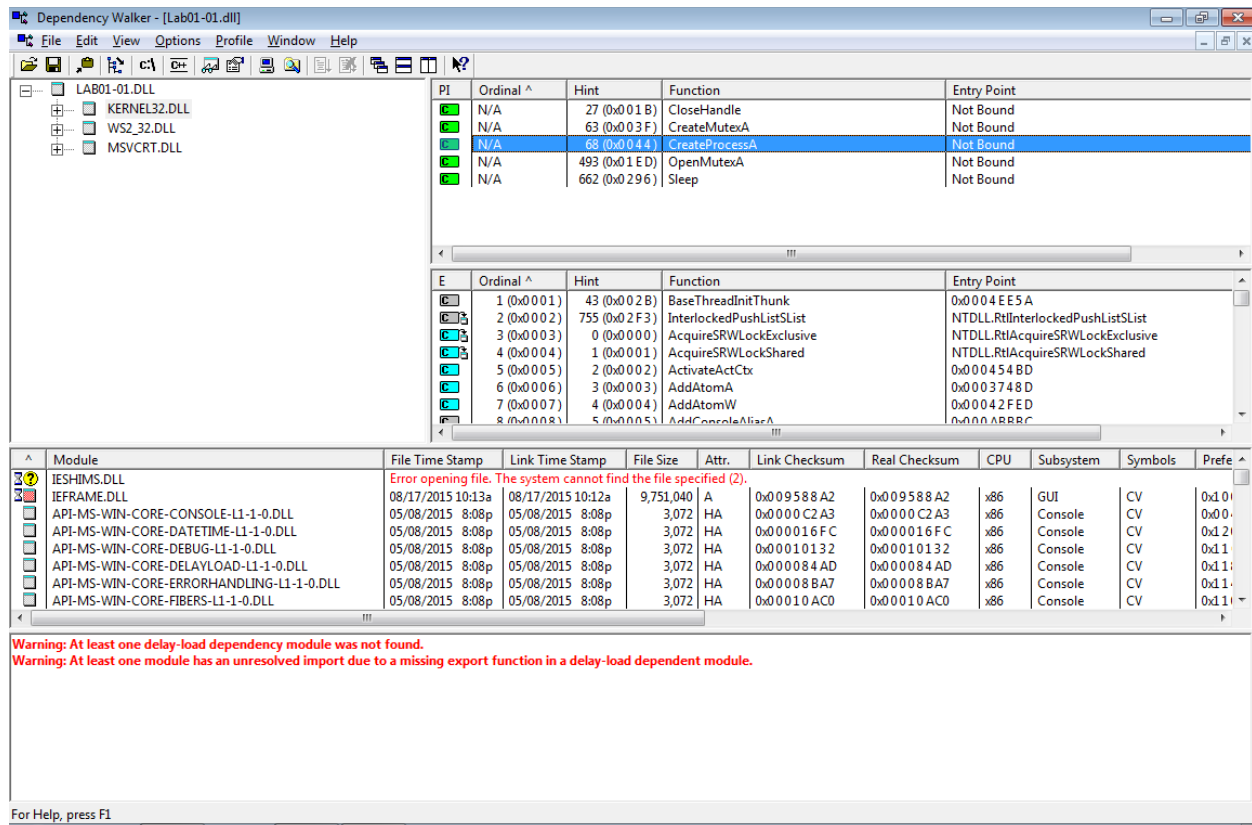
I think this file is trying to read all the files(FindFrstFileA, FindNextFileA) and create a file as a result(CreateFileA, CreateFileMappingA).



[Image] Dependency Walker shows us imported functions from dll

5. Use dependency Walker to and look for imports and exports of 'Lab01-01.dll'. Does it import the same functions from kernel32.dll? What can you learn from this?

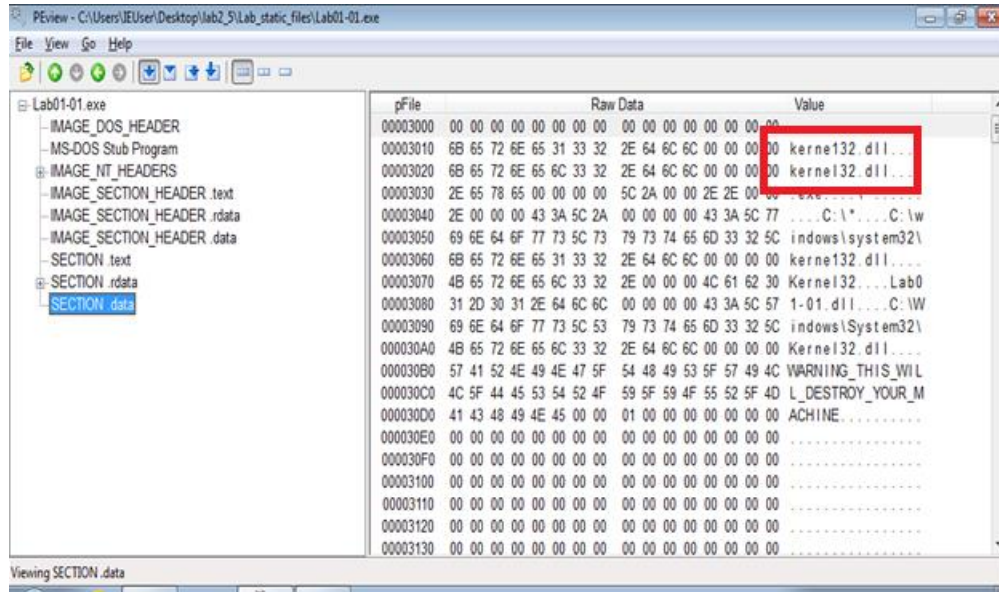
This dll file does not import the same functions from kernel32.dll. Maybe, it is trying to create process cause I can notice this file import 'CreateProcessA' from kernel32.dll.



[Image] Dependency Walker shows us imported functions from dll

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

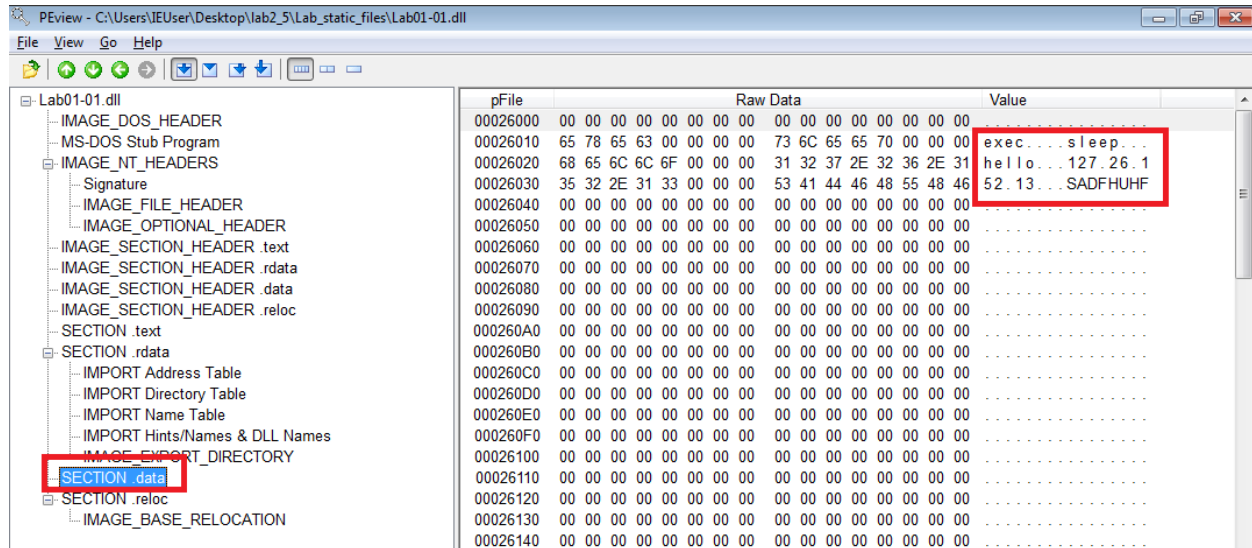
This file has a weird string on 'SECTION.data' when I check with PEView. It was 'C:\windows\system32\kerne123.dll'. The file name was kerne132.dll not kernel32.dll! I think it is probably an attempt to deceive the DLL.



[Image] In 'SECTION.data', there was a weird file name.

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

There was a IP address in Lab01-01.dll file's 'SECTION.data'. It could be a sign of using networking!



[Image] In 'SECTION.data' of dll file, there was a IP address

8. When considering all your findings, can you make an educated guess about the purpose of these two files (.exe and .dll)?

Exe file is trying to find some files and create a new file.

And Dll file is also trying to create a Process and use a network!

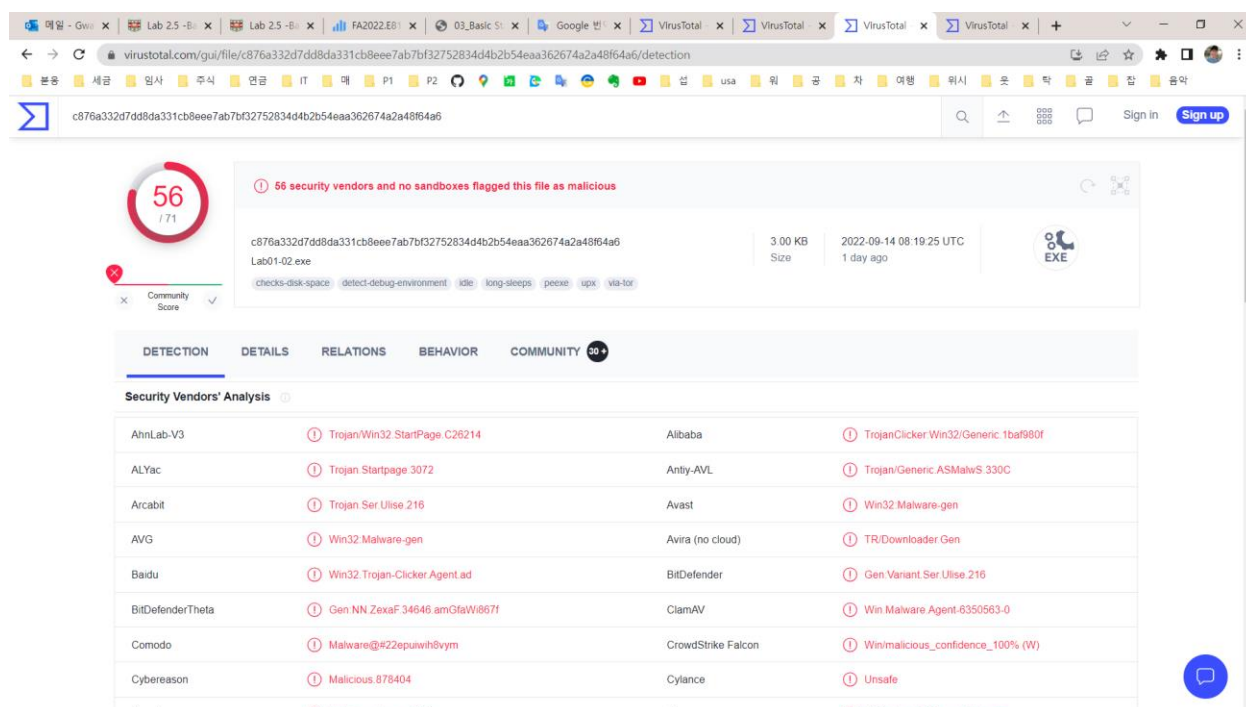
Considering all of these, this program creates a new file and sends and receives information over the network like a backdoor!

Part 3 – Textbook Lab 1-2

In this section, we will analyze Lab01-02.exe.

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

For, Lab01-02.exe, there are 56 antivirus signatures! And its detection rate is 56/71. VirusTotal also provides checksum of this virus to identify it. If so many virus programs find it, it seems to be a famous virus.



The screenshot shows the VirusTotal analysis page for the file Lab01-02.exe. The file has been detected by 56 out of 71 security vendors, resulting in a 100% detection rate. The file is identified as Trojan/Win32.StartPage.C26214. The page displays a table of security vendors and their respective detections.

Security Vendor	Detection
AhnLab-V3	Trojan/Win32.StartPage.C26214
Alibaba	TrojanClicker.Win32/Generic.1ba1980f
ALYac	Trojan.Startpage.3072
Antiy-AVL	Trojan/Generic.ASMalwS.330C
Arcabit	Trojan.Ser.Usise.216
Avast	Win32/Malware-gen
AVG	Win32/Malware-gen
Avira (no cloud)	TR/Downloader.Gen
Baidu	Win32.Trojan-Clicker.Agent.ad
BitDefender	Gen.Variant.Ser.Usise.216
BitDefender/Theta	Gen.NN.ZexaF.34646.amGfaW/867f
ClamAV	Win.Malware.Agent.6350563-0
Comodo	Malware/@#22epuivth8vym
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.878404
Cylance	Unsafe

[Image] Security Vendors' Analysis

56 / 71

56 security vendors and no sandboxes flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

3.00 KB
Size

2022-09-14 08:19:25 UTC
1 day ago

EXE

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 56+

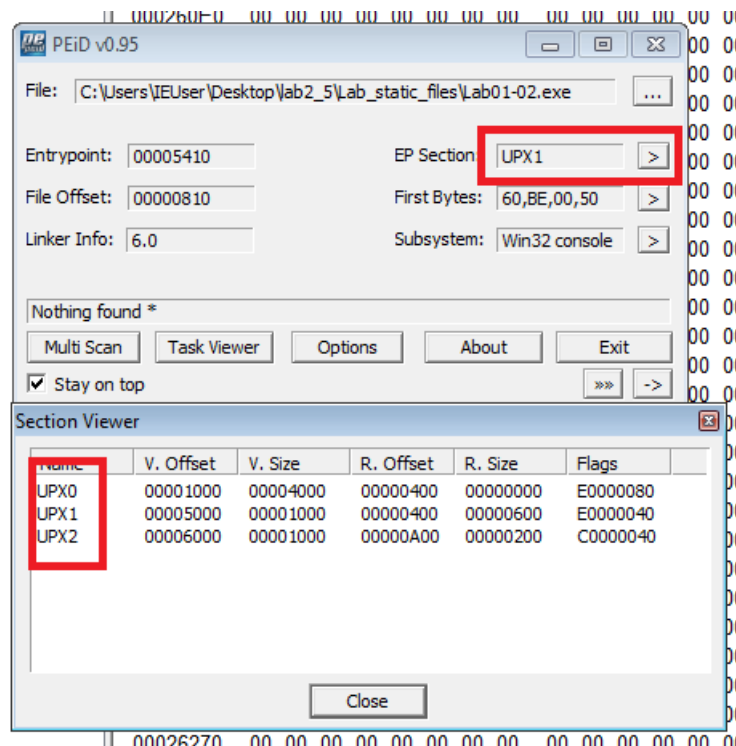
Basic Properties

MD5	8363436878404da0ae3e46991e355b83
SHA-1	5a016facbcb77e2009a01ea5c67b39af209c3fcb
SHA-256	c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Vhash	03303e07d10192601pz1bz
Authenticash	c0dd97382560a28cc053de86b9505ea78390147de7021744eb49d9b55e3d152f
Imphash	096aa05b8a2e1f2dc66fc73a1a978a7b
Rich PE header hash	0560c880c8133e98d13ab271ab4c687
SSDEEP	48 atUKzxRhviNZEVtbn4m3ZUJSsJY8JTalclOBgs 0UkKttf4KOJzcK
TLSH	T18351B8ABFE65CFAC24E0B3B03DBC920356EA0D04BFD43C16A9D7497E89B1548855610
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
TrID	UPX compressed Win32 Executable (35.7%)
TrID	Win32 EXE Yoda's Crypter (35%)
TrID	Win32 Dynamic Link Library (generic) (8.6%)
TrID	Win16 NE executable (generic) (6.6%)
TrID	Win32 Executable (generic) (5.9%)

[Image] Checksum information about the virus

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.

For Lab01-02.exe, there is an indication of packed. When see the EP Section, there was no text, rdata, data rather than 'UPX1'. Maybe, this is packed with UPX.



I tried to unpack this file using 'upx' command and it successfully unpacked. I download upx exe file from the web site(<https://github.com/upx/upx/releases/tag/v3.96>). The command was 'upx -d [filename]'. I can see the file has changed since unpacking.

```
C:\Windows\system32\cmd.exe
-t test compressed file          -U display version number
-h give more help                -L display software license

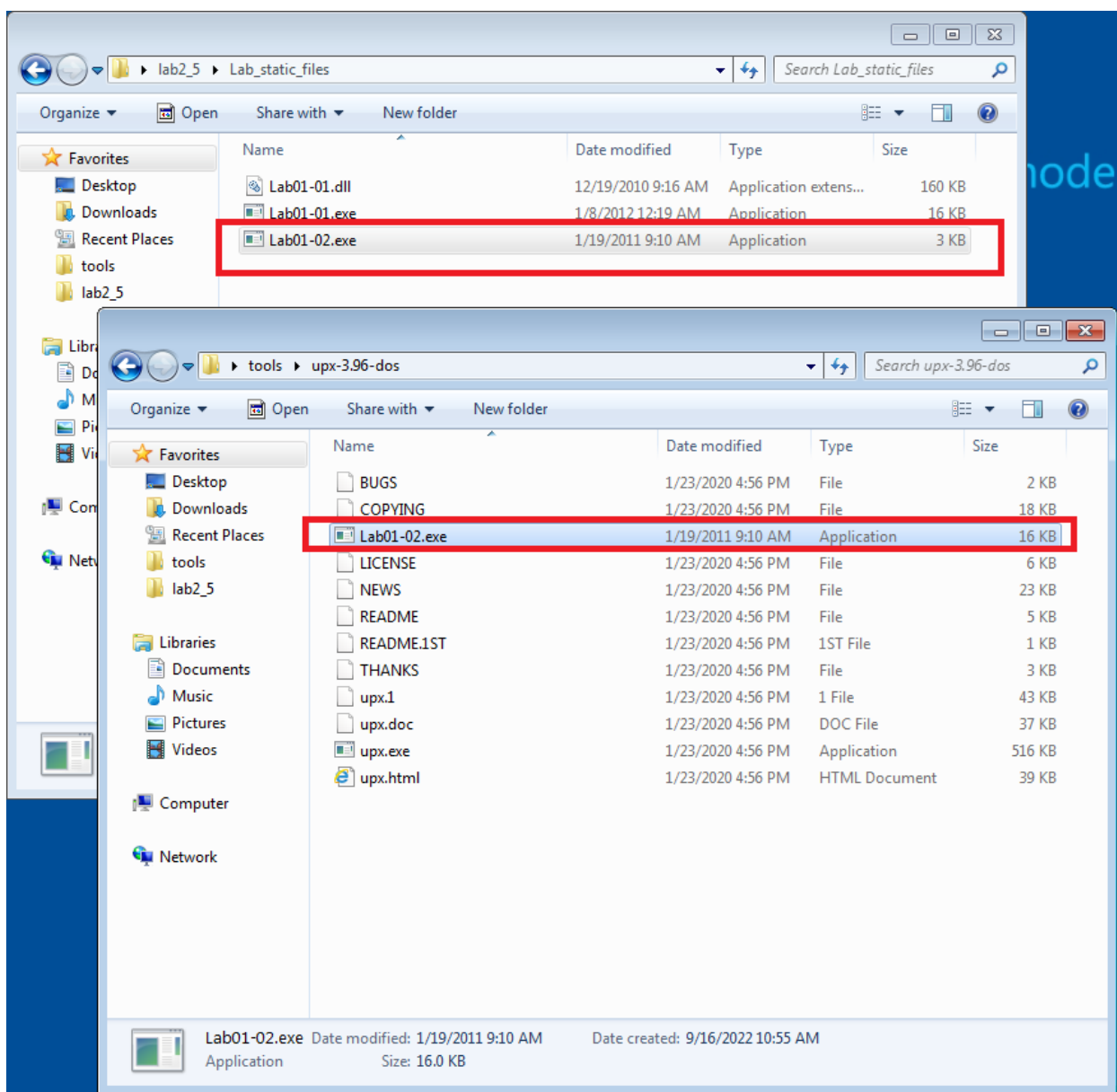
Options:
-q be quiet                      -v be verbose
-o FILE write output to 'FILE'
-f force compression of suspicious files
-k keep backup files
file.. executables to <de>compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io
C:\Users\IEUser\Desktop\tools\UPX-3~1.96->upx -d Lab01-02.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2020
UPX 3.96d Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

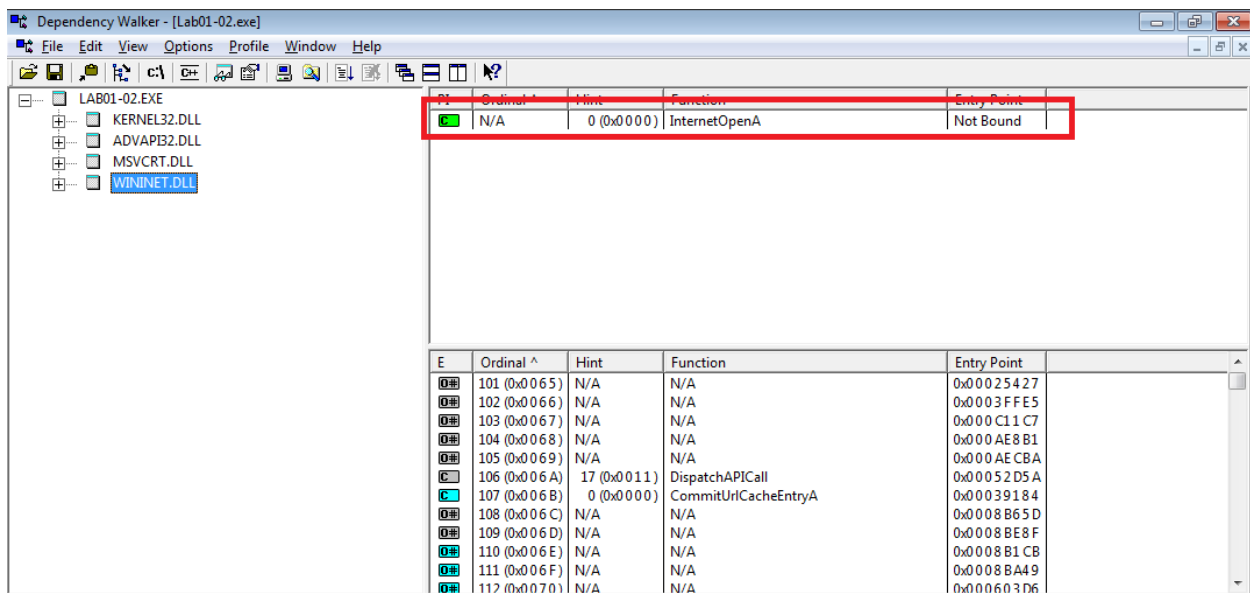
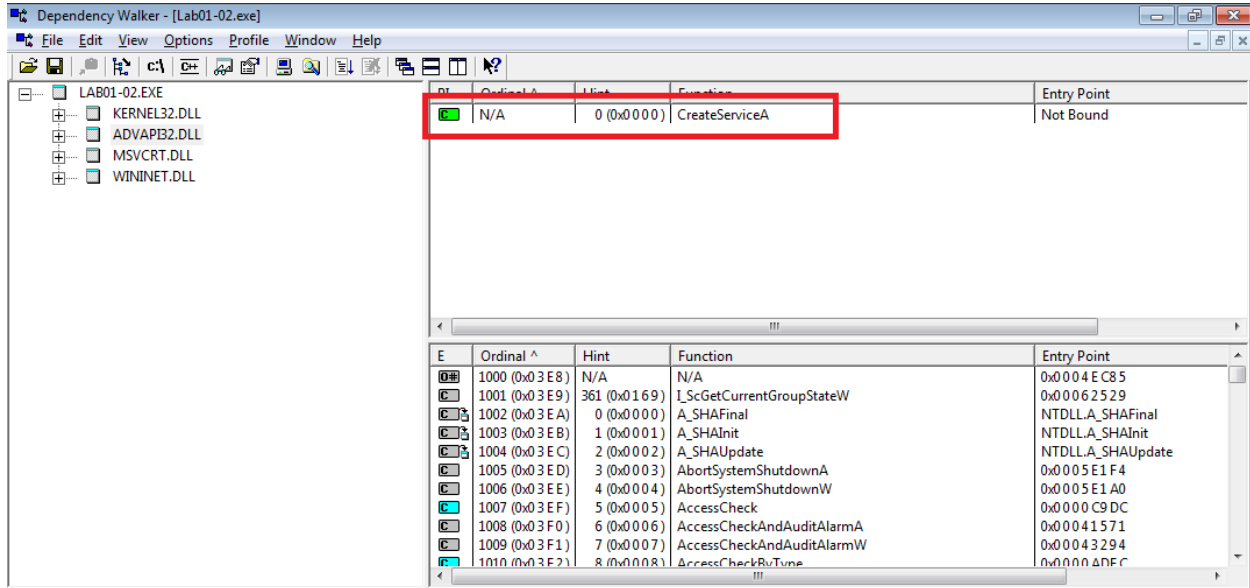
File size      Ratio      Format      Name
-----
16384 <-      3072      18.75%     win32/pe     Lab01-02.exe

Unpacked 1 file.
C:\Users\IEUser\Desktop\tools\UPX-3~1.96->
```



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

It imports 'CreateServiceA' from ADVAPI32.DLL and 'InternetOpenA' from WININET.DLL. This exe file seems to make a new service using Internet access.



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

After unpacking this file, I could find a url '<http://www.malwareanalysisbook.com>'.
The string could be used to identify this malware!

