**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.

텍스트이(가) 표시된 사진

자동 생성된 설명

[Image] Security Vendors’ Analysis

텍스트이(가) 표시된 사진

자동 생성된 설명

[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.

텍스트이(가) 표시된 사진

자동 생성된 설명

[Image] Security Vendors’ Analysis

텍스트이(가) 표시된 사진

자동 생성된 설명

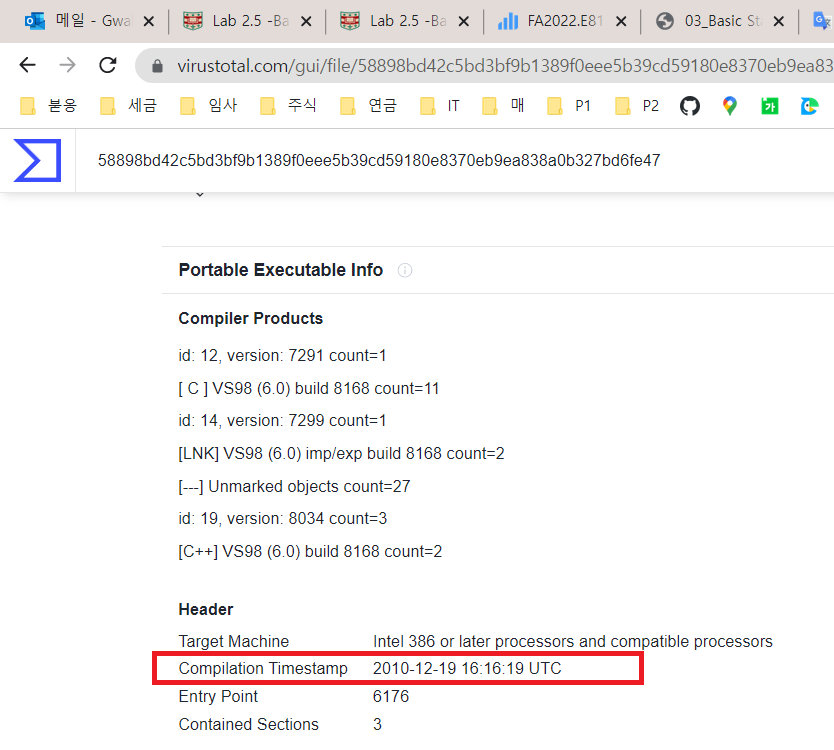
[Image] Checksum information about the virus

2. When was ‘lab01-01.exe’ compiled?

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

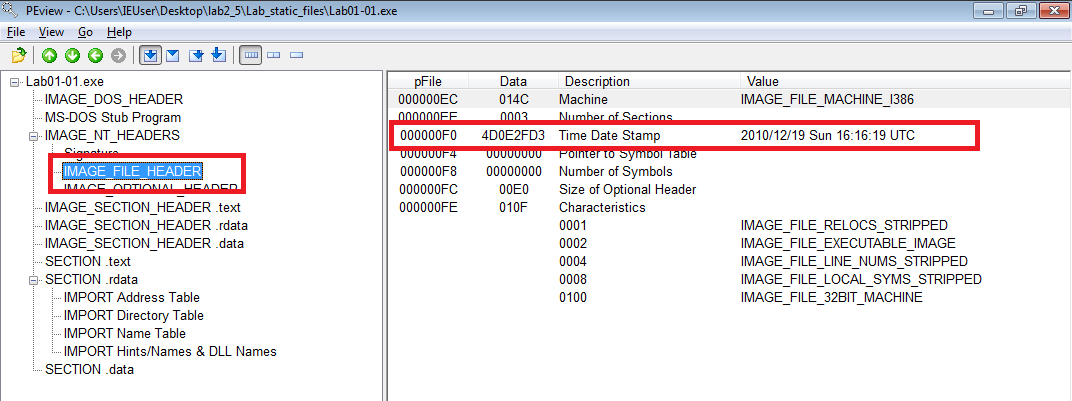
I found the compilation time stamp on VirusTotal detail information.

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



[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 PEView.

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

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).

테이블이(가) 표시된 사진

자동 생성된 설명

[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.

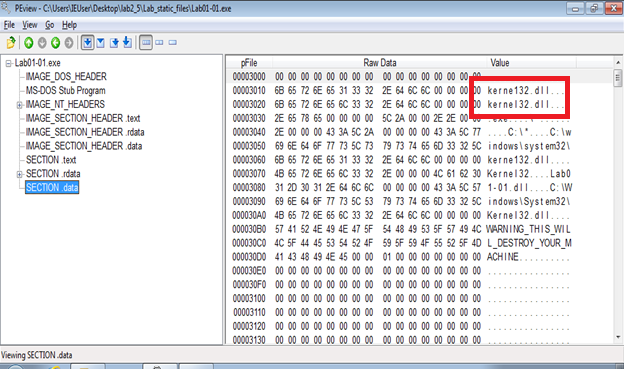
테이블이(가) 표시된 사진

자동 생성된 설명

[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?

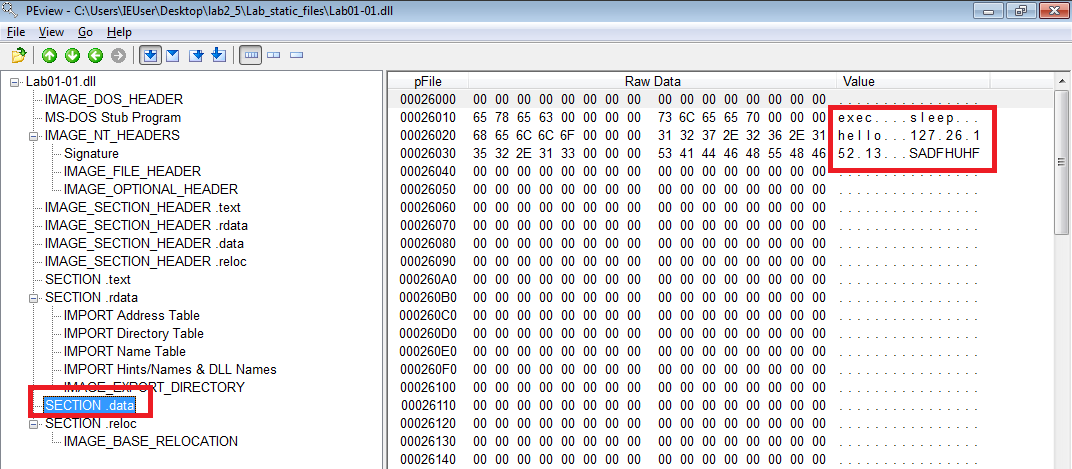
This file has a weird string on ‘SECTION.data’ when I check with PEView. It was ‘C:\windows\system32\kerne123.dll’. The file name was kerne132.dll not kernel32.dll! I think it is probably an attempt to deceive the DLL.



[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.

텍스트이(가) 표시된 사진

자동 생성된 설명

[Image] Security Vendors’ Analysis

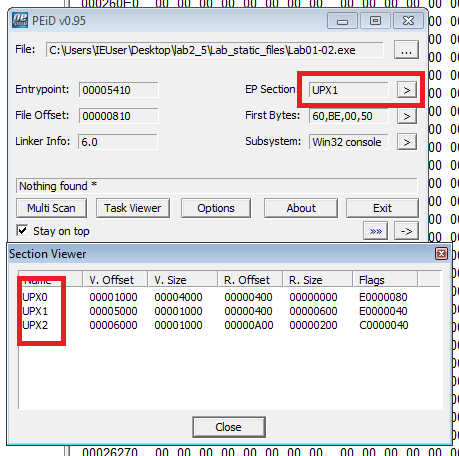
텍스트이(가) 표시된 사진

자동 생성된 설명

[Image] Checksum information about the virus

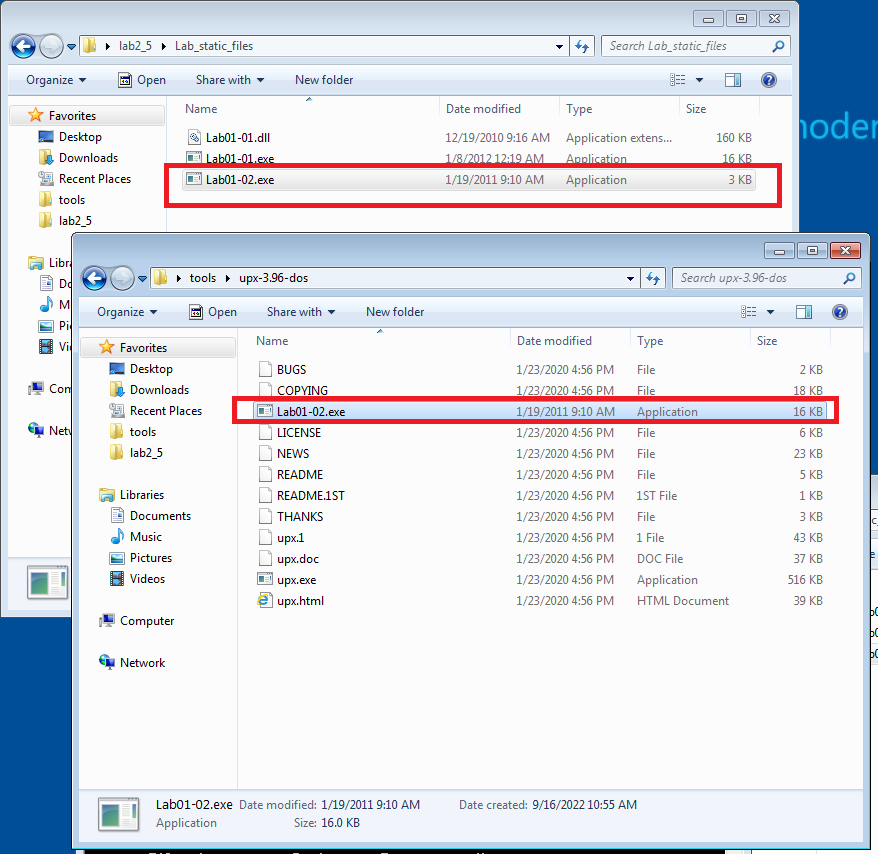
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

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.



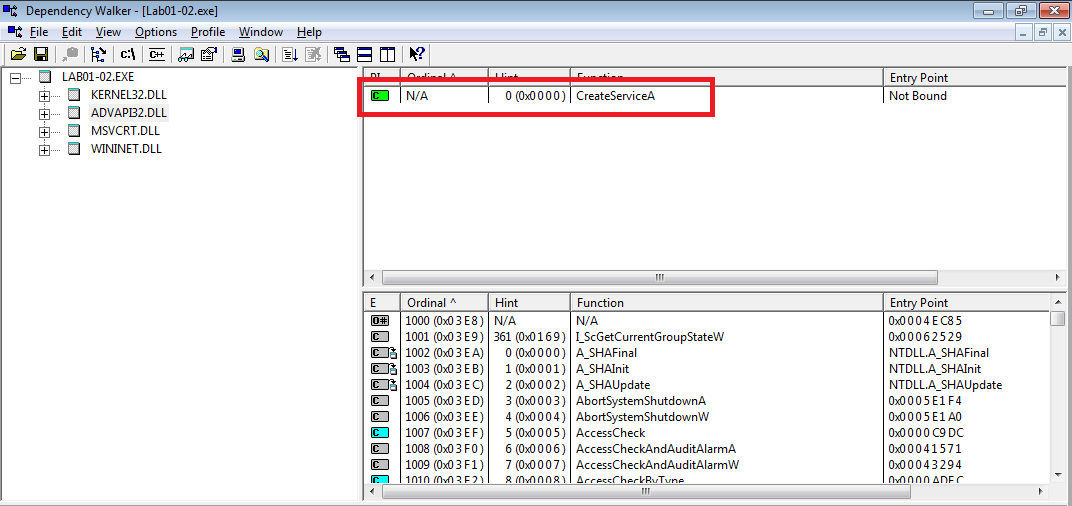
I tried to unpack this file using ‘upx’ command and it successfully unpacked. I download upx exe file from the web site(https://github.com/upx/upx/releases/tag/v3.96). The command was ‘upx -d [filename]’. I can see the file has changed since unpacking.

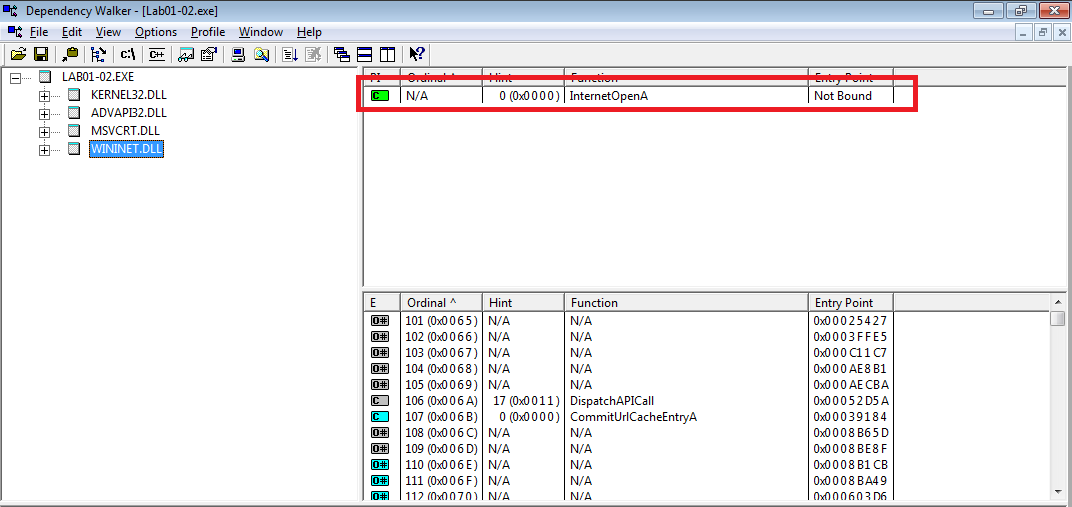
텍스트이(가) 표시된 사진

자동 생성된 설명

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!

