|  |  |  |
| --- | --- | --- |
| C:\Users\thg\Desktop\ICT Logo\ICT_4C.jpg | | |
| Week | Malware Analysis Tools and Techniques | Duration |
| 1 | Basic Static Analysis - Practical | 120 mins |

**Lesson Objectives**

Perform Basic Static Analysis on unknown Portable Executable with the following tools:

* PEView
* Dependency Walker
* PEiD
* Strings

Submit your answers on MeL.

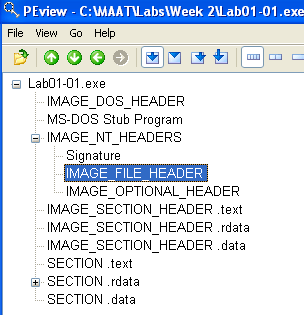
# Lab 01 [40 mins]

Refer to the files: lab01-01.exe and lab01-01.dll.

**Question 1**

When were these files compiled? 19/12/2010

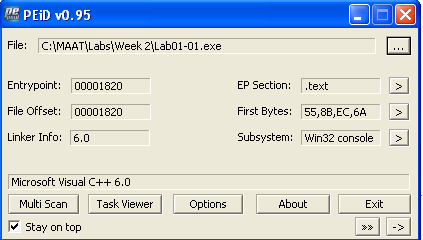
(*hint: use PEview)*



**Question 2**

Were these files packed? No, there is no indication of file packed

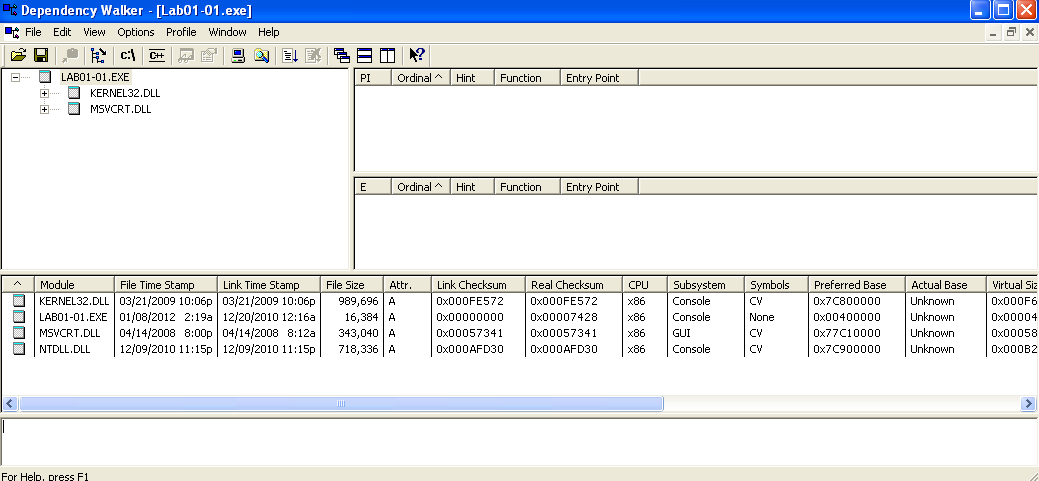
(*hint: use PEiD)*

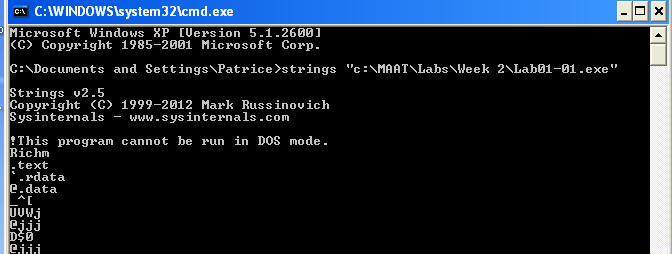


**Question 3**

What could be the functionalities of this malware, the exe and the dll, based on the imports? The exe file imported FindFirstFileA, FindNextFileA, CreateFileA and CopyFileA, which mean it is looking for a file and trying to copy to somewhere and maybe create a fake file to replace it. The dll file imported CreateProcessA and Sleep, which tell us it creates a process which run at the background. It also imported WS2\_32.dll which mean it have function to access the internet.

(*hint: use Dependency Walker and Strings)*





**Question 4**

What are some host-based indicators of this malware? 127.26.152.13

(*hint: is there any file being installed?)*

**Question 5**

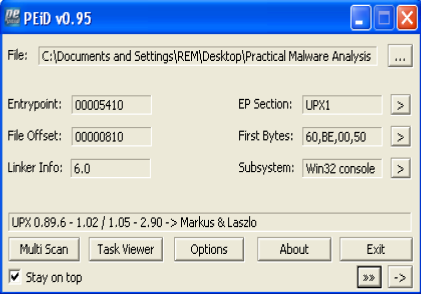
What could be the purpose of this malware? The exe is a malware installer that install the dll file which is a backdoor malware.

# Lab 02 [80 mins]

Refer to the files: Lab01-02.exe and Lab01-03.exe

**Question 1**

Are the files packed? If so, what are the indicators and how could you unpack it?



The lab01-02.exe file is packed using UPX 0.89.6. To unpack the file, we need to download UPX and run the decompression command “upx -d”

The lab01-03.exe file is packed using FSG 1.0. We maybe able to unpack the file using OllyDump, but we still haven’t learn.

**Question 2**

What are the imports of the malware? For lab01-02.exe, there is KERNEL32.DLL, ADVAPI32.DLL, MSVCRT.DLL and WININET.DLL.

For lab01-03.exe, I’m not able to unpack it, so I cannot find any import.

**Question 3**

What important functions are imported in the DLL?

For lab01-02.exe, there is CreateServiceA, StartServiceCtrlDispatcherA, OpenSCManager, InternetOpenA, InternetOpenUrlA.

**Question 4**

What could be the functionality of the malware based on the import of the malware?

Base one the import, we can guest that the malware create and trigger a service which let it connect to the internet.

**Question 5**

What could be some host-based indicators? MalService, HGL345

**Question 6**

What could be some of the network-based indicators? http://www.malwareanalysisbook.com