Assignment 1 Report

Group Name: Aw, Snap!
Group Members: Weijia Sun, Xinyu Lyu, Mengmei Ye

1.

This is the result for Lab01-01.dll

This is the result for Lab01-01.exe

Yes, both of the files match the existing antivirus signatures.

2

Lab01-01.exe

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-12-19 16:16:38
Entry Point	4858
Contained Sections	4

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	926	4096	1.9	65d3ddf9778db8d01e57b5825fbd93ad
.rdata	8192	147398	147456	0.03	530532a38a38ea1219e691b8f16d10e9
.data	155648	108	4096	0.11	0211086333be22ae2620b568fde46fe3
.reloc	159744	516	4096	0.26	a082f3572d17cd40272b3bcfd96b7b2d

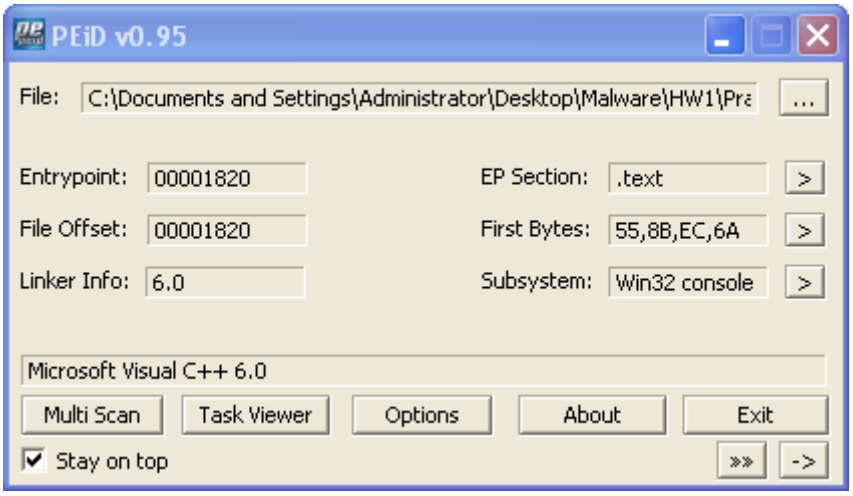
Imports

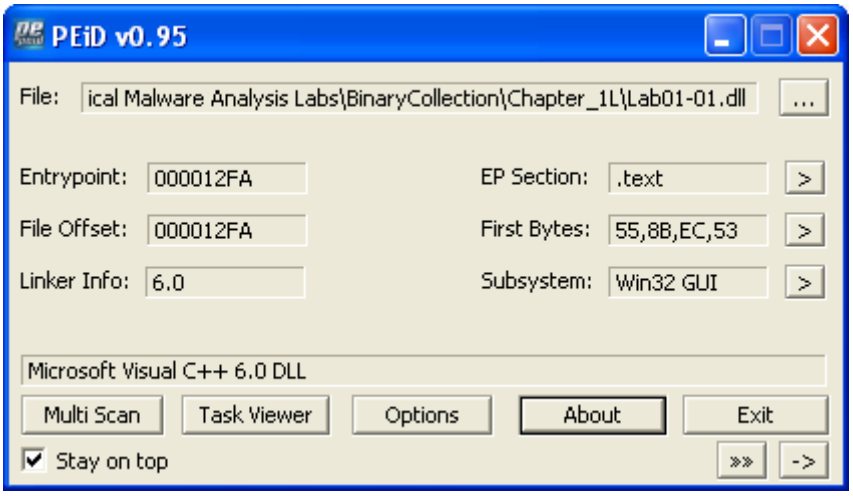
- KERNEL32.dll
- MSVCRT.dll
- WS2_32.dll

As is shown in the above attached figure, these files were compiled on 2010-12-19.

3

We used the PEiD to analyze the file. Here are the results:





From the pictures above, we can see Microsoft Visual C++ was the compiler. It also indicates that the subsystem is Win32 GUI which means the malware had a GUI before. However, there are no indicators showing these files has been packed or obfuscated.

4

The imports of Lab01-01.exe contain:

```
CreateFileA
FindNextFileA
FindFirstFileA
CopyFileA
```

According to these imports, this malware might want to search for a specific file and copy it.

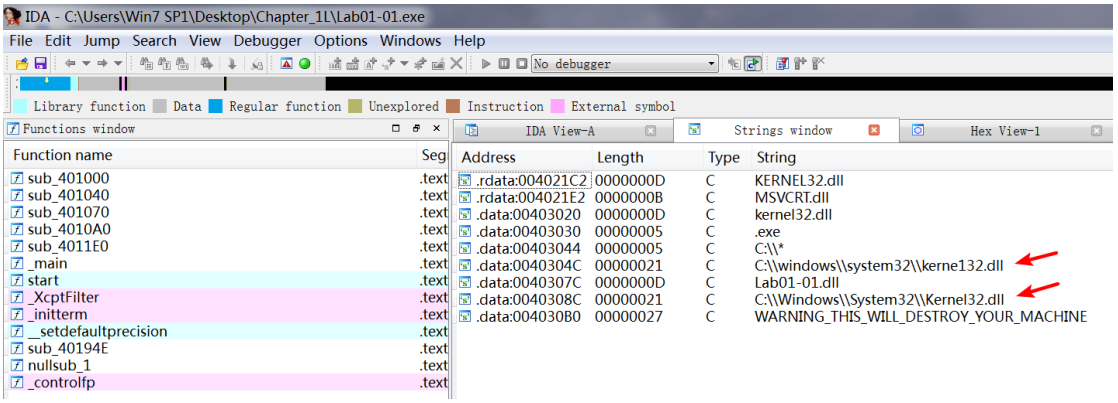
The imports of Lab01-01.dll contain:

```
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
CloseHandle
socket
inet_addr
connect
send
recv
closesocket
```

According to these imports, the malware might want to communicate with a specific server since there is some import about socket connections.

5

Examine C:\Windows System32 kerne132.dll for additional malicious activity. Note that the file kerne132.dll, with the number 1 instead of the letter l, is meant to look like the system file kernel32.dll. This file can be used as a host indicator to search for the malware.



6

The *.dll* file contains a reference to local IP address 127.26.152.13. Network activity to 127.26.152.13 would be a network-based indicator of the malware being present on a system.

7

Based on all the information above, we think the .dll file probably contains a backdoor and the .exe file is executable to install and run the dll file.