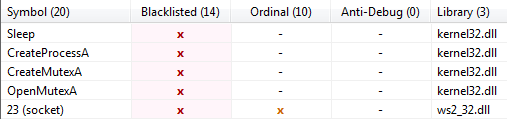
**Sample Lab01-01.exe**

1. Yes, the file matches “22/55” existing antivirus signatures. The first submission of the file was on “2012-02-16 07:31:54 UTC ( 4 years ago )”.
2. The file’s compilation timestamp was “2010-12-19 16:16:19”.
3. No, examining the file with PEiD v0.95 shows the addresses of its “.text” and “.data”, meaning that the file was not packed or obfuscated. It also shows that the executable was compiled with “Microsoft Visual C++ 6.0”.
4. The executable imports KERNEL32.dll and MSVCRT.dll.
   1. Some of the main imports are all in KERNEL32.dll “FindFirstFileA”, “CopyFileA”, and “CreateFileA”. This leads me to believe that this executable deals with file manipulation.
5. …
6. Looking at “Lab01-01.dll” in pestudio 8.51, it has an imported library of ws2\_32.dll which is blacklisted and also a “Windows Socket 2.0 32-Bit DLL”.P:\CMPSC443\Git\CMPSC443\Lab06\Lab01-01.dll-ImportedLibraries.PNG

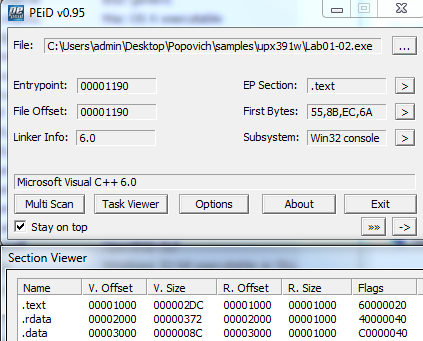
Going off of that, it has an imported symbol of “23 (socket)” which is blacklisted and ordinal. 

Lastly, it contains an ASCII string of “127.26.152.13” which is an obvious IP address.

1. …

**Task 1 – Sample Lab01-02.exe**

1. Yes, the file matches “36/55” existing antivirus definitions. The first submission of the file was on “2011-07-02 17:02:09 UTC ( 4 years, 7 months ago )”.
2. Yes, examining the file with PEiD v0.95 reports that the executable was packed with “UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo”. The file is able to be unpacked with UPX.



1. The executable imports ADVAPI32.dll, KERNEL32.DLL, MSVCRT.dll, and WININET.dll. The following imports hint at this programs’ functionality:
   1. CreateServiceA in ADVAPI32.dll is used likely to create a process.
   2. InternetOpenA in WININET.dll is used likely to communicate via an internet socket.
2. Looking at “Lab01-02.dll” in pestudio 8.51, as mentioned above, it imports wininet.dll.

P:\CMPSC443\Git\CMPSC443\Lab06\Lab01-02.dll-ImportedLibraries.PNG

Looking at its ASCII strings, it has “http://w” and “ysisbook.co”. We could use these strings in combination with Wireshark as a network-based indicator.

**Task 2 – Sample Lab01-03.exe**

1. Yes, the file matches “44/55” existing antivirus signatures. The first submission of the file was on “2011-07-04 22:00:08 UTC ( 4 years, 7 months ago )”
2. Yes, examining the file with PEiD v0.95 reports that the executable was packed with “FSG 1.0 -> dulek/xt”.
   1. Unpack …
3. The executable imports KERNEL32.dll. In KERNEL32.dll it uses LoadLibraryA and GetProcAddress. Unfortunately these don’t give too much of an indication of what the executable does.
4. …

**Task 3 – Sample Lab 01-04.exe**

1. Yes, the file matches “45/55” existing antivirus signatures. The first submission of the file was on “2011-07-06 00:05:42 UTC ( 4 years, 7 months ago )”
2. No, examining the file with PEiD v0.95 shows the addresses of its “.text” and “.data”, meaning that the file was not packed or obfuscated.
3. The file’s compilation timestamp was “2019-08-30 22:26:59”.
4. …