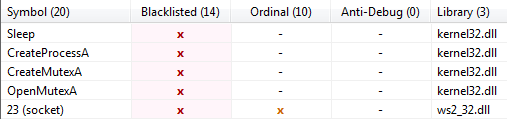
**Sample Lab01-01.exe**

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. In pestudio 8.51, this file has an imported symbol of “CreateProcessA”, which can be seen in the second screenshot below. Because it creates processes, we could find those processes running in the Task Manager to identify that this virus is currently running.
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

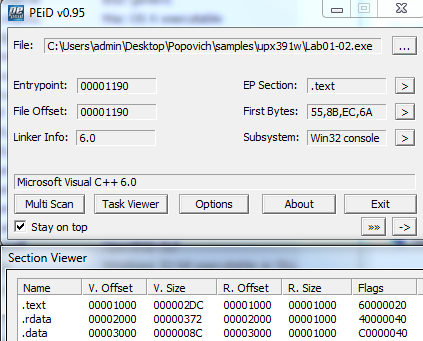
Going off of that, it has an imported symbol of “23 (socket)” which is blacklisted and ordinal. 

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

1. The file references creating and modifying files, creating processes, and even references an IP address. This leaves the door wide open for many different malicious tasks.

**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”. Because this file is packed with FSG and not UPX, we are unable to unpack it.
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. Because we are unable to unpack this file, we don’t know a whole lot about this file. We know it “LoadLibraryA”, so we might be able to check if the host machine has loaded that library, but that’s about it.

**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. It also shows that the executable was compiled with “Microsoft Visual C++ 6.0”.
3. The file’s compilation timestamp was “2019-08-30 22:26:59”, which is a red flag being that it’s 3 years in the future.
4. The executable imports “ADVAPI32.dll”, “KERNEL32.dll”, and “MSVCRT.dll”.
   1. In “KERNEL32.dll” it uses “MoveFileA”, “LoadResource”, “OpenProcess”, “WriteFile”, “CreateFileA”, and “LoadLibraryA”. This leads me to believe that this executable deals with file manipulation.
5. Looking at the file in pestudio 8.51, the Strings section gives us some insights on how to locate this executable on host machines. On the host, we could look in the task manager to see if “winlogon.exe”, “wupdmgr.exe”, “winup.exe”, or “updater.exe” is running. For a network-based indicator we could look in Wireshark for the url “http://www.practicalmalwareanalysis.com/updater.exe”.
6. Any of the strings found in Resource Hacker were found in pestudio 8.51. Resource Hacker showed that “winup.exe”, “wupdmgrd.exe”, and the URL are all located near each other in the binary, alluding that they might be being used in conjunction with one another, possibly downloading or updating itself or more malware.