Song Yang ([sea.yang@rutgers.edu](mailto:sea.yang@rutgers.edu))

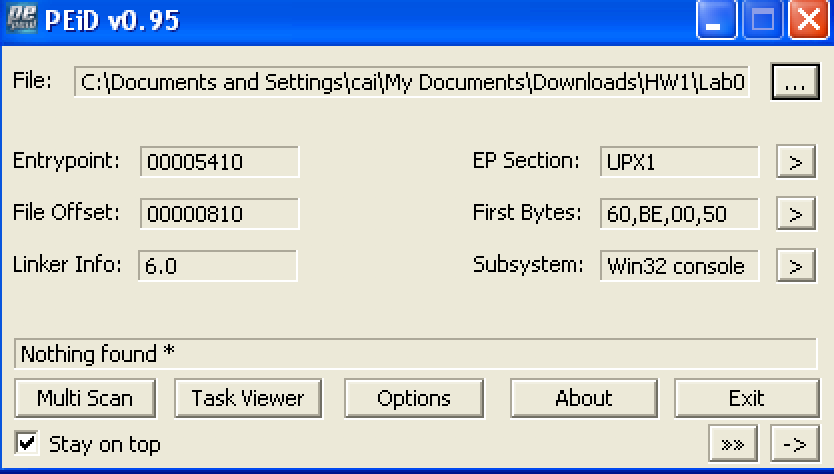
Xin Yang ([xin.yang@rutgers.edu](mailto:xin.yang@rutgers.edu))

Zhuohang Li ([zl299@scarletmaik.rutgers.edu](mailto:zl299@scarletmaik.rutgers.edu))

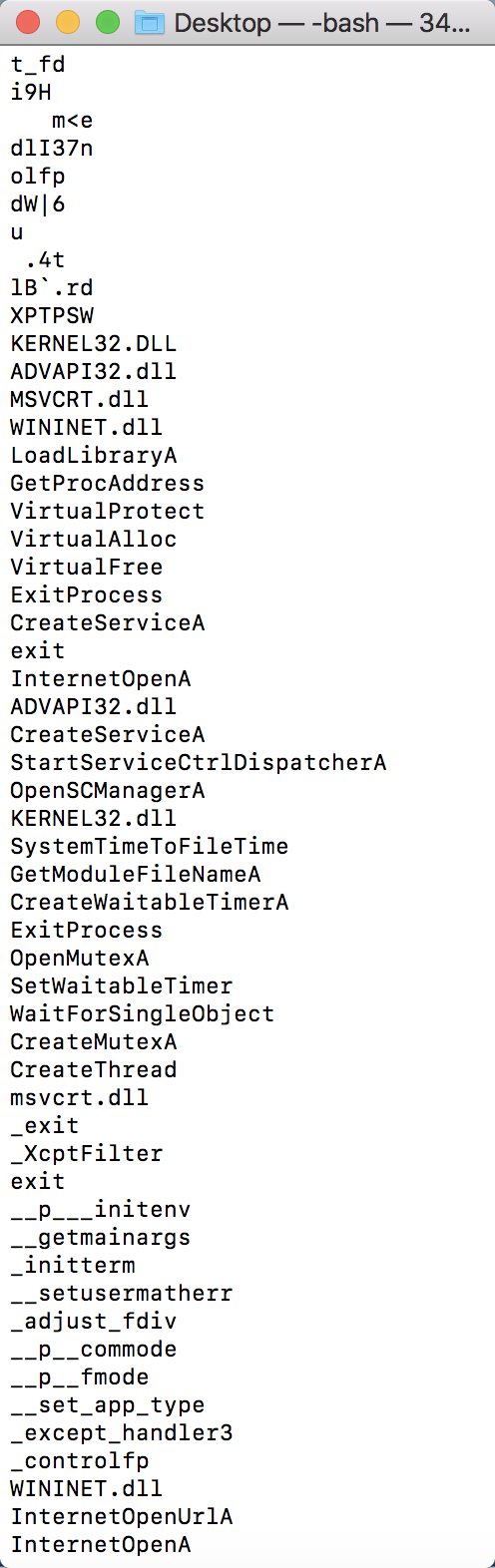
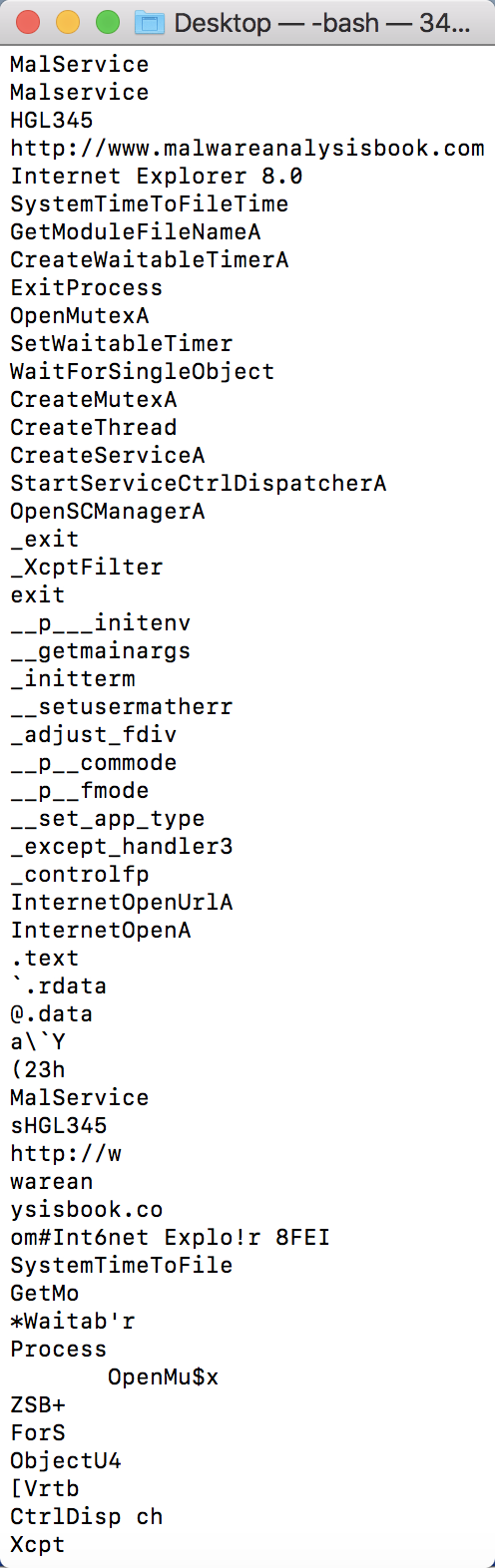
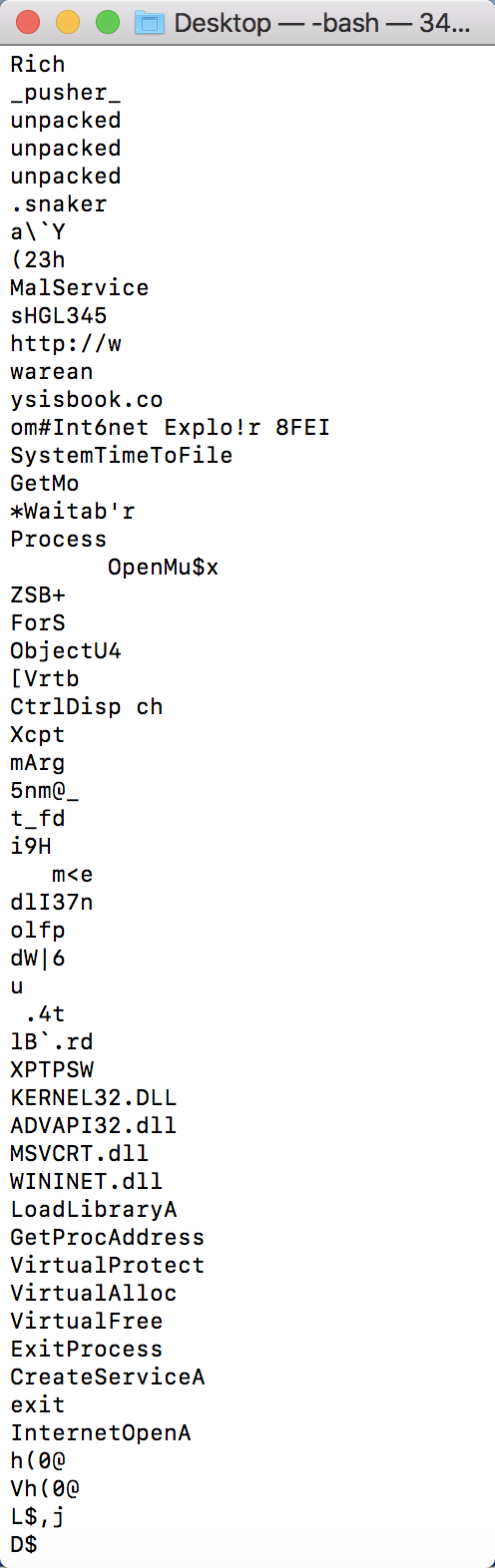
Homework 1

Lab01-02.exe:

1. Yes. Detection ratio is 42/67. Mostly marked with Trojan generic downloader.
2. The file is packed with UPX and we are able to unpack it using UPX unpacker plugin.

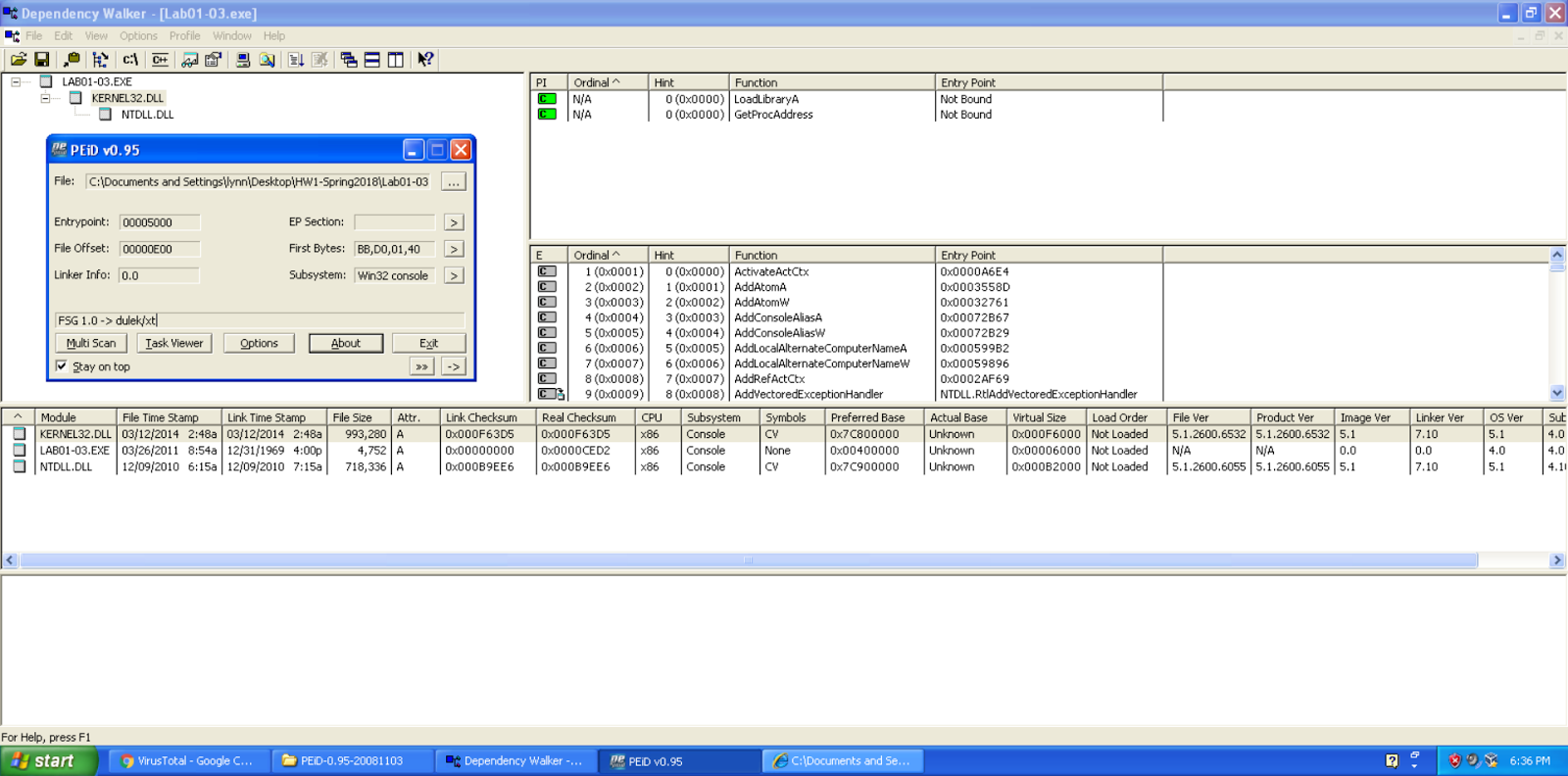


1. Yes. Imports are ‘LoadLibraryA’, ‘GetProcAddress’, ‘CreateServiceA’ and ‘InternetOpenA’. These indicate that this program has something to do with creating service and connecting to the Internet.
2. As is shown below, we can see an URL ‘<http://www.malwareanalysisbook.com>’ and a service named ‘MalService’ in the strings of the unpacked file. These could be used to identify the malware.

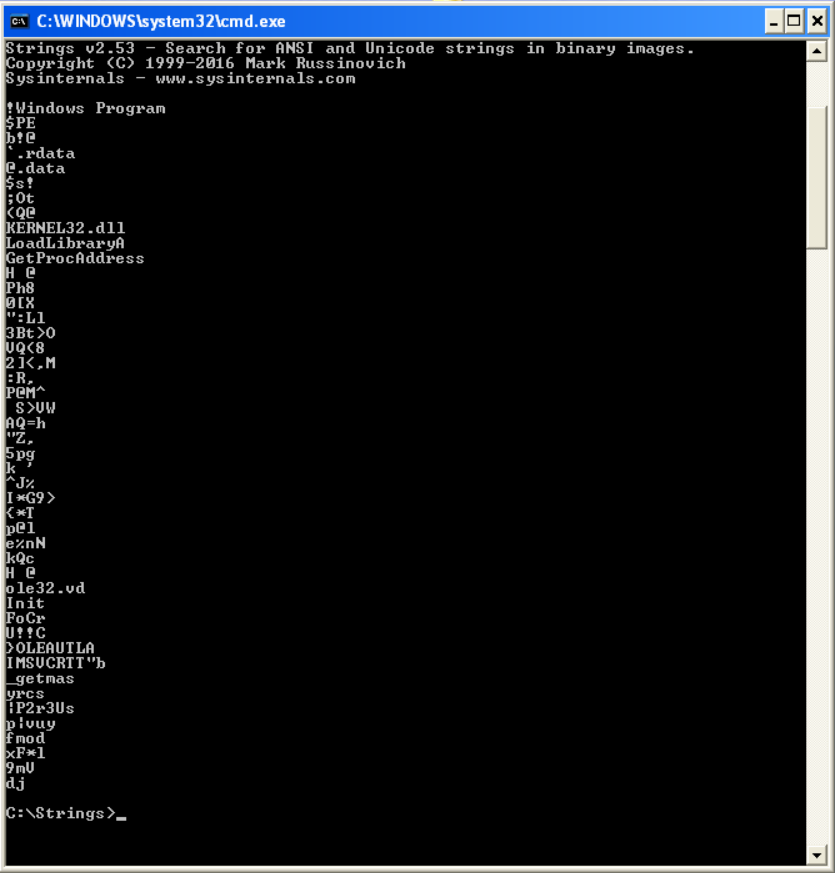


Lab01-03.exe:

1. It could be Packer/Trojan/generic/Genome
2. The file is packed. as PEiD showed in the picture, it is packed with FSG 1.0 -> dulek/xt . PEiD cannot find the original entry point of this package so it still cannot be unpacked.
3. We saw 2 function called at first they are ‘LoadLibraryA’ and ‘GetProcaddress’, but they should be part of the package and not the origin program.

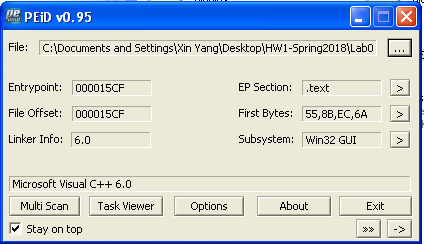


1. As is still packed, and Strings result below, the only message we know is the function mentioned above. No network hints, and we need to unpack.

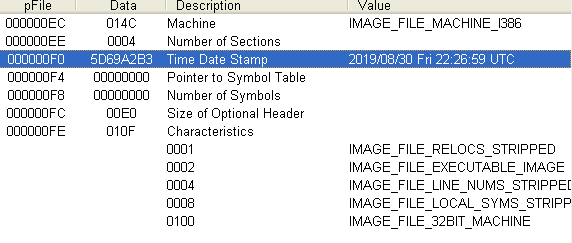


Lab01-04.exe:

1. Yes, 54/67 antivirus platforms in virustotal report this as a Trojan, keywords are generic, downloader.
2. The virtual size and raw size looks fine. Also from PEiD we can tell it’s unpacked, and with dependency walker we can tell the imports clearly.



1. As PEview showed, it’s compiled in 2019/08/30 Fri 22:26:59 UTC, it’s in the future so the time is changed by the malware writer.



1. There’re LoadLibraryA, CreateFileA, FindResourceA, GetModuleHandleA, GetWindowsDirectoryA, MoveFileA, GetTempPathA in kernel32.dll, and LookupPrivilegeValueA, AdjustTokenPrivileges in advapi32.dll. We can infer that this malware is going to import some wierd libraries and change or download some files, also it would change the permission.
2. By running ‘strings’ command, there’re words like \system32\wupdmgr.exe and \winup.exe and URLDownloadToFileA, this might hint this malware will download or change files in the above directories. Also there’s a URL “<http://www.practicalmalwareanalysis.com/updater.exe>”, this should be the server which this malware tries to connect to.
3. Using Resource Hacker, the only resource in BIN is 101:1033, and the contents are all hex. With the hex reader at the right part, we can see there are contents about the library and imported functions such as KERNEL32.dll, MSVCRT.dll, urlmon.dll and suspicious functions GetWindowsDirectoryA, WinExec, URLDownloadToFileA, which make us think this malware is going to download some files and execute, also it may replace some dll files.

