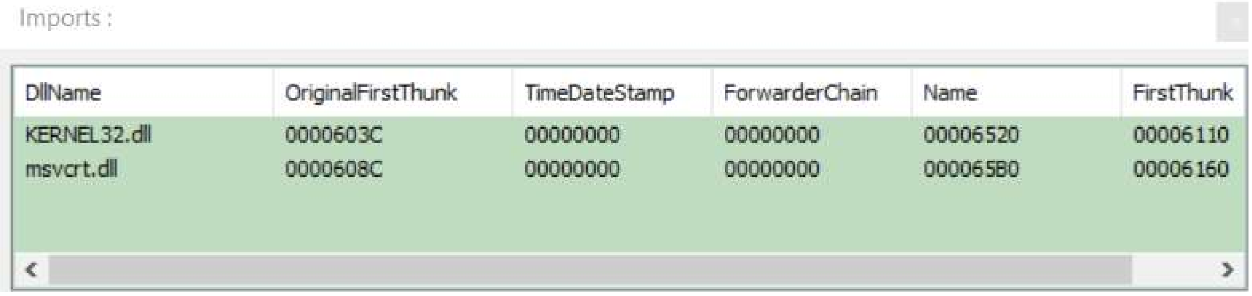
Josh Levy – EECS 349 HW2

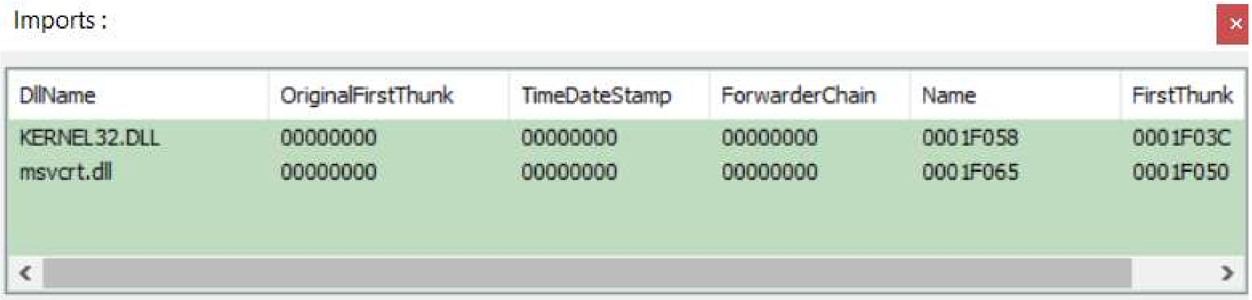
1. The code file is main.c, the executable produced is PE-Import-original.exe
2. The import table for the original .exe looks like this:



Imports :

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0000603C	00000000	00000000	00006520	00006110
msvcrt.dll	0000608C	00000000	00000000	000065B0	00006160

3. The packed .exe. is PE-Import-packed.exe. Its import table is as follows:

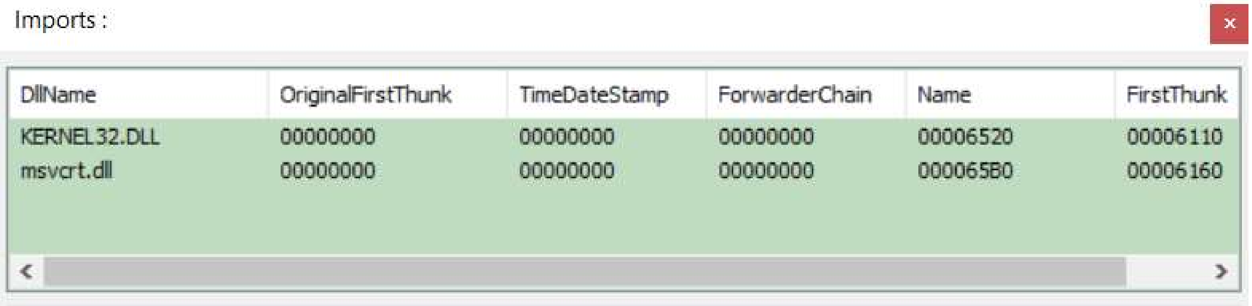


Imports :

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	0001F058	0001F03C
msvcrt.dll	00000000	00000000	00000000	0001F065	0001F050

The names of the dll's being used are the same, althouogh it appears they are in different locations in local memory after packing. This makes sense, as the packing compresses the file and moves references around.

The unpacked file is PE-Import-unpacked.exe. Its import table is as follows:

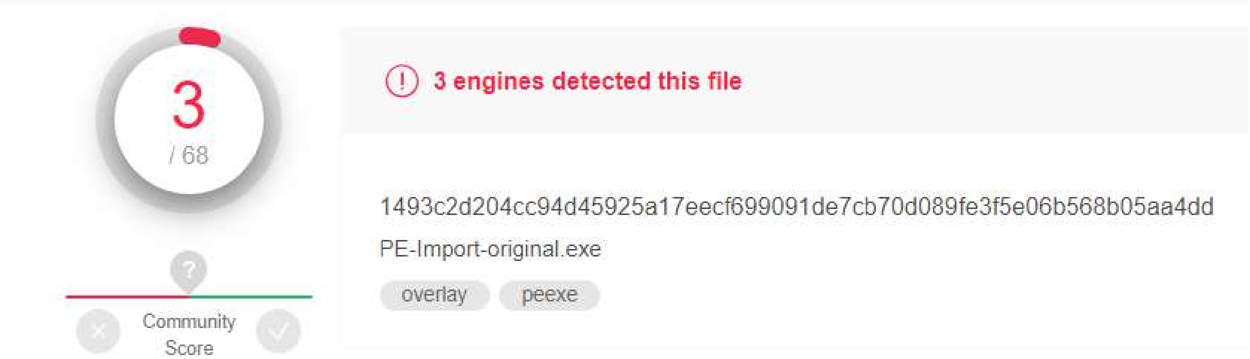


Imports :

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.DLL	00000000	00000000	00000000	00006520	00006110
msvcrt.dll	00000000	00000000	00000000	000065B0	00006160

This is completely identical to the original file's import table.

4. As a baseline, scan the original exe to see how many flag it as dangerous:



3 engines detected this file

1493c2d204cc94d45925a17eecf699091de7cb70d089fe3f5e06b568b05aa4dd

PE-Import-original.exe

I then scan the packed version to see how this changes the results. At this point the GUI for the website broke so I couldn’t take any more screenshots,but compressing the executable increased the number of engines that flagged it to 6.

To further test the effects of packing, I used upx with the --brute flag to maximize the compression. This made a total of 8 engines flag the program. Compressing the file to a .zip archive, however, made only 1 engine flag it.

I also attempted to obfuscate the code in a way that produced multiple compiler warnings. The source code for this is in obfuscated.c, and the resulting executable is PE-Import-obfuscated.exe. Only 2 engines flagged this as dangerous, so this method seems ineffective.