Anaisy Garcia PID:5734454

Questions1. Upload the Lab01-04.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?

Yes. The exe had 54/69 matches.

2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

There are no indications that wither files are packed or obfuscated. Using PEiD does not indicate it is packed. The book also states, “Packed and obfuscated code will often include at least the functions LoadLibrary and GetProcAddress, which are used to load and gain access to additional function.” These files do not include this.

3. When was this program compiled?

The exe was created “Creation Time 2019-08-30 22:26:59”. This doesn’t seem correct because the book was copyrighted 2012.

4. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?

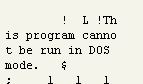
The exe file has imports from the ADVAPI32.dll, KERNEL32.dll, and MSVCRT.dll library which deals with access to advanced functionality, handles the memory management, input/output operations, and interrupts, and is part of the Microsoft C runtime. From the ADVAPI32.dll library the imports OpenProcessToken and LookupPrivilegeValue show that this exe looks for the privilege and then opens a process. From the KERNEL32.dll library the imports CreateFileA, WriteFile, and WinExec which tells us the program creates a file, writes a file, and then probably executes the file.

5. What host- or network-based indicators could be used to identify this malware on infected machines?

When the file Lab01-04 was put into the strings program, a website can be seen all the way at the bottom.  This could’ve either been placed here on purpose or be the website from the person who created this virus. Strings shows us a file destination  this could be where the file creates and modifies the file.

6. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

When this file is loaded into resource hacker, we see it is a binary file with hexadecimal values. Here we see a string that may be an error message or a warning.



A quick google search says “That message is from the basic header that every Windows (PE format) executable has. … It's 16-bit executable code (like a DOS .COM file), intended to be displayed when you try to run the program on MS-DOS or similar pre-Windows systems. Windows' program loader typically skips over it.” This mean that this exe file has another exe file within it. When we put the Lab01-04 file into PEviewer, under SECTION.rsrc we see a part that says “URLDownloadToFile” which tells us it downloads a file from the internet and “WinExec” tells us it executes the file it downloaded.

