Lab 1-1 Solutions

1. These files were written specifically for this book, so as of this writing, you should not find a signature for them on VirusTotal.com. Of course, if these files become part of the antivirus signatures as a result of the publication of this book, the results will be different.
2. Both files were compiled on December 19, 2010, within 1 minute of each other.
3. There are no indications that either file is packed or obfuscated.
4. The interesting imports from Lab01-01.exe are FindFirstFile, FindNextFile, and CopyFile. These imports tell us that the program searches the filesystem and copies files. The most interesting imports from Lab01-01.dll are CreateProcess and Sleep. We also see that this file imports functions from WS2_32.dll, which provides network functionality.
5. Examine C:\Windows\System32\kerne132.dll for additional malicious activity. Note that the file kerne132.dll, with the number 1 instead of the letter l, is meant to look like the system file kernel32.dll. This file can be used as a host indicator to search for the malware.
6. The .dll file contains a reference to local IP address 127.26.152.13. This address is an artifact of this program having been created for educational and not malicious purposes. If this was real malware, the IP address should be routable, and it would be a good network-based indicator for use in identifying this malware.
7. The .dll file is probably a backdoor. The .exe file is used to install or run the DLL.

Lab 1-2 Solutions

1. As of this writing, the file matches 3 of 41 antivirus signatures.
2. There are several indications that the program is packed with UPX. You can unpack it by downloading UPX and running upx –d.
3. After unpacking the file, you'll see that the most interesting imports are CreateService, InternetOpen, and InternetOpenURL.
4. You should check infected machines for a service called Malservice and for network traffic to http://www.malwareanalysisbook.com/.

Lab 1-3 Solutions

1. As of this writing, 25 of 43 virus engines identify this sample as malware.
2. The file is packed, but we can't unpack it at this time.
3. This question can't be answered without unpacking the file.
4. This question can't be answered without unpacking the file.

Lab 1-4 Solutions

1. As of this writing, 16 of 43 antivirus engines identify this as malicious code that downloads and/or drops additional malware onto a system.
2. There are no indications that the file is packed or obfuscated.
3. According to the file header, this program was compiled in August 2019. Clearly, the compile time is faked, and we can't determine when the file was compiled.
4. The imports from advapi32.dll indicate that the program is doing something with permissions. The imports from WinExec and WriteFile, along with the results from VirusTotal.com, tell us that the program writes a file to disk and then executes it. There are also imports for reading information from the resource section of the file.
5. The string \system32\wupdmgr.exe indicates that this program could create or modify a file at that location. The string www.malwareanalysisbook.com/ updater.exe probably indicates where additional malware is stored, ready for download.
6. The resource section contains another PE executable. Use Resource Hacker to save the resource as binary data, and then analyze the binary file as you would analyze any executable. The executable in the resource section is a downloader program that downloads additional malware.