HW1

**Problem 1 – Lab 1-4**

1. According to VirusTotal, this file matches the signature of the existing antivirus definition of “VirusShare”.
2. This file does not appear to be packed based on PEiD, but does appear somewhat obfuscated as there are mostly strings containing calls to Windows functions. There are a lot of these function calls however.
3. This program was compiled using Microsoft Visual C++ 6.0 on November 3, 2008.
4. A few imports that hint at the program’s functionality include CreateFileA, MoveFileA, and WriteFile, suggest that this virus will likely create and move a file somewhere within the computer. WinExec also suggests that it will then execute this file/executable.
5. On the network-side, the program appears to make a web request to practicalmalwareanalysis.com, specifically an updater, so any request to this web host would be a cause for concern with this virus and might entail that the machine in question was infected. If the resulting files from this updater were able to be determined, their existence on a machine would also be a host-based way to determine if the machine was infected.
6. From Resource hacker, the one BIN resource file seems to indicated that this executable cannot be run on DOS mode, and it makes a web call to http://practicalmalwareanalysis.com/updater.exe.

**Problem 2 – Assignment 1-2**

1. The MD5sum for this file is 02658bc9801f98dfdf167accf57f6a36. VirusTotal provides info on various hashes for the file being analyzed and compares this hash against other databases to see if they recognize this hash as a virus. Also, various behaviors for the virus are listed such as which files it may delete, and what processes it terminates.
2. Some imports from this virus are WriteFile, ReadFile, Sleep, CreatePipe, and CloseHandle. These imports could be used to create and run a file executable as well as possibly closing a window or specific windows on the computer.
3. There are many interesting strings in the program. A few say “download complete” or “upload complete” signifying that the virus likely downloads something to the machine and also attempts to upload some data to source online or at least pretends to. There are also a few strings that say “Microsoft Corporation” which likely means the virus pretends to be a product of Microsoft to make the user trust the virus and the changes it is making to the host machine.

**Problem 3 – Reading Assignment**

**Problem 4 – Dynamic analysis on Assignment 1-2**