Lab_03-1

1. There is a DLL, extracted with ResourceHacker
2. Answers:
    a. WriteFile writes to file, such as a log or writing more malware
    b. LoadResource can load the DLL mentioned before
    c. IsDebuggerPresent could make dynamic analysis differently due to different behavior
3. Answers:
    a. http://rpis.ec network signature potentially
    b. regsvr32 /s C:\Windows\atidrv.dll could be an attempt to hide more malware. Maybe the DLL?
    c. C:\Users\IEUser\Downloads\BHOinCPP_src\Release\launch.pdb BHOInCPP is an example project from CodeProject
4. It unpacks and registers a DLL on the system
5. 0002df01-0000-0000-c000-000000000046 (Internet Explorer)
6. D30C1661-CDAF-11D0-8A3E-00C04FC9E26E (IWebBrowser2)
7. 0xa4 and 0x2c

Lab_03-2

1. MD5: bf4f5b4ff7ed9c7275496c07f9836028. I didn't run through virus total because the VM isn't network connected, but apparently it open a file in the C drive called "java.exe" and uses DNS
2. Answers:
    a. GetDriveType determines if a drive is removable, fixed, CD, RAM, or network
    b. GetLogicalDrives gets bitmask representing the currently available disk drives
    c. FileTimeToSystemTime converts a file time to the system time format, in UTC
3. Answers:
    a. SOFTWARE\Microsoft\Windows\CurrentVersion\Run persistence mechanism
    b. \java.exe may be the persistence file
    c. cmd.exe, appears to execute system commands
4. It uses the Run key mentioned above to run on startup (probably with the java.exe file)
5. List Processes: 0x00402310, Remote Shell: 0x00402490 and 0x00402660, Send Files: 0x00402210
6. List Processes: 7, Remote Shell: 9 and 10, Send Files: 6
7. No
8. Lists processes: CreateToolhelp32Snapshot, Process32First, Process32Next; Remote Shell: CreateProcessA, PeekNamedPipe, WriteFile; Upload File: CreateFileA, CreateFileMappingA, MapViewOfFile
9. Command 2 lists directory contents, 5 downloads a file, and 8 kills a process