Lab 3-1 Solutions

1. The malware appears to be packed. The only import is ExitProcess, although the strings appear to be mostly clear and not obfuscated.
2. The malware creates a mutex named WinVMX32, copies itself into *C:\ Windows\System32\vmx32to64.exe*. and installs itself to run on system startup by creating the registry key HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run\VideoDriver set to the copy location.
3. The malware beacons a consistently sized 256-byte packet containing seemingly random data after resolving *www.practicalmalwareanalysis.com*.

Lab 3-2 Solutions

1. To install the malware as a service, run the malware's exported installA function via *rundll32.exe* with rundll32.exe Lab03-02.dll,installA.
2. To run the malware, start the service it installs using the net command net start IPRIP.
3. Use Process Explorer to determine which process is running the service. Since the malware will be running within one of the *svchost.exe* files on the system, hover over each one until you see the service name, or search for *Lab03-02.dll* using the Find DLL feature of Process Explorer.
4. In procmon you can filter on the PID you found using Process Explorer.
5. By default, the malware installs as the service IPRIP with a display name of Intranet Network Awareness (INA+) and description of "Depends INA+, Col- lects and stores network configuration and location information, and notifies applications when this information changes." It installs itself for persistence in the registry at HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ Parameters\ServiceDll: %CurrentDirectory%\Lab03-02.dll. If you rename *Lab03-02.dll* to something else, such as *malware.dll*, then it writes *malware.dll* into the registry key, instead of using the name *Lab03-02.dll*.
6. The malware resolves the domain name *practicalmalwareanalysis.com* and connects to that host over port 80 using what appears to be HTTP. It does a GET request for *serve.html* and uses the User-Agent %ComputerName% Windows XP 6.11.

Lab 3-3 Solutions

1. The malware performs process replacement on *svchost.exe*.
2. Comparing the disk image of *svchost.exe* with its memory image shows that they are not the same. The memory image has strings such as practicalmalwareanalysis.log and [ENTER], but the disk image has neither.
3. The malware creates the log file *practicalmalwareanalysis.log*.
4. The program performs process replacement on *svchost.exe* to launch a keylogger.

Lab 3-4 Solutions

1. When you run this malware by double-clicking it, the program immedi- ately deletes itself.
2. We suspect that we may need to provide a command-line argument or a missing component to the program.
3. We try using the command-line parameters shown in the strings listing (like -in), but doing so is not fruitful. More in-depth analysis is required.