Malware Analysis
Fall 2015
Lab 07 - Covert Malware Launching

This week, rather than analyzing samples, we'll be doing a little development. It will help solidify your understanding of the Windows Internals and APIs related to this chapter. When you install Visual Studio, be sure to install the Professional version instead of the Community version (available for free to students). You won't be needing it for this lab, but you will later.

Part A

You will be using the Microsoft Detours library to hook several API calls

1. (5 pts) Hook MessageBox and change the message box title
2. (5 pts) Hook CreateFile and log the filename/path
3. (5 pts) Hook Sleep so that it doesn't actually sleep

4. (10 pts) Inject this DLL into a 2 different programs and describe the results.

I recommend **stripping down** and modifying the 'tracemem' sample to suit your needs. You'll lose points if there is injection/hooking code left over from the sample.

To build…

1. Extract the archive
2. Open a Visual Studio Developer command prompt (it's in your taskbar)
3. cd to the extracted directory
    - e.g. `cd C:\Users\IEUser\Desktop\MS_Detours\`
4. type `nmake`

To use…

1. start `.\bin.x86\syelogd.exe` to view log output
2. start a process with your dll
    - `.\bin.x86\withdll.exe /d:.\bin.x86\trcmem32.dll calc.exe`

Part B

To better understand DLL injection, you will write code that performs this technique. Write a c++ program that takes as input a DLL and a PID and injects the given DLL into the specified process.

e.g. `my_inject.exe C:\mydll.dll 1280`

You may NOT use existing DLL injection frameworks or libraries for this assignment. I expect to see the API calls described in Listing 12-1 of the PMA book.

You must also provide a DLL that, when injected, displays a message box containing the window title of the injected process.