Proj 15: Malware Behavior (Lab 12-1) (25 pts.)

What you need:

- A Windows 2008 Server virtual machine with the tools we have been using installed.

Purpose

You will practice the techniques in chapter 12: Covert Malware Launching.

Follow the Book

Follow the instructions for **Lab 12-1** in the textbook. There are more detailed solutions in the back of the book. The only purpose of this document is to explain what images to turn in.

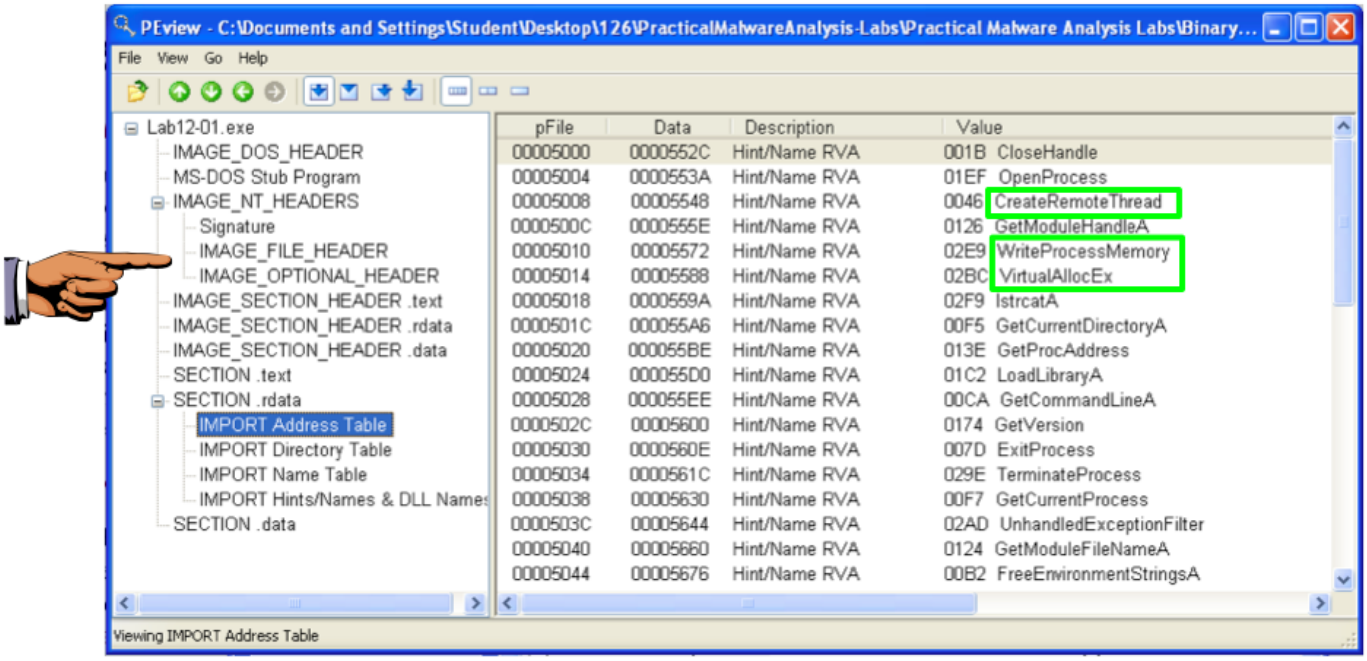
Imports

Examine **Lab12-01.exe** in PEView. Find these three imports, which are used in process injection:

- **CreateRemoteThread**
- **WriteProcessMemory**
- **VirtualAllocEx**

Save an image containing the three imports, highlighted below, with the filename "**Proj 15a from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

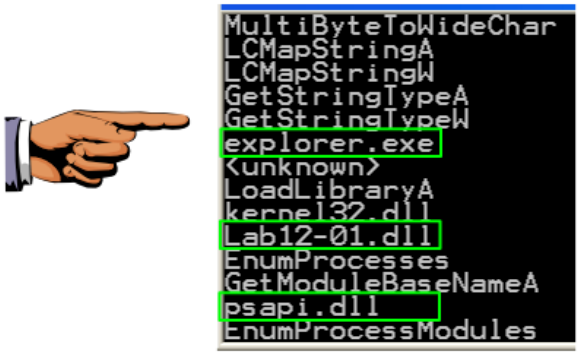


Strings

Examine the strings in **Lab12-01.exe**. Find these three strings, which show the process being injected, the DLL file used, and *psapi.dll*, which is used for process enumeration:

- **explorer.exe**
- **Lab12-01.dll**
- **psapi.dll**

Save an image showing the three strings highlighted below, with the filename "**Proj 15b from YOUR NAME**".

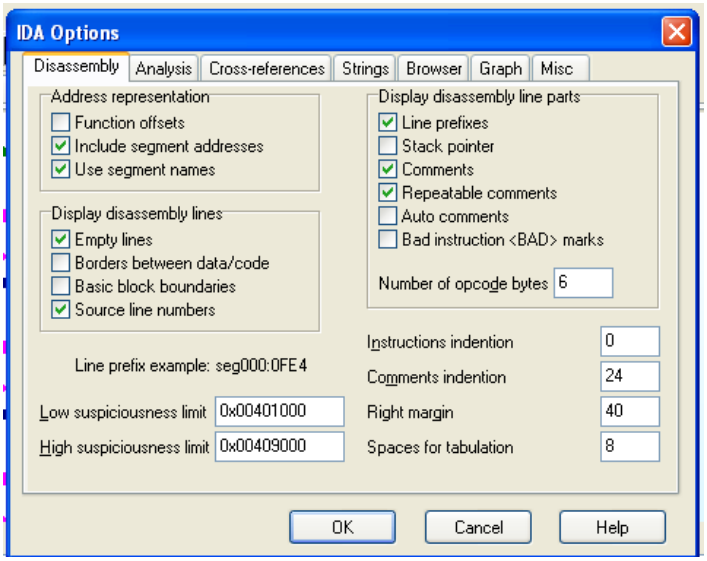


IDA Pro

Load **Lab12-01.exe** in IDA Pro Free.

Click **Options**, **General**.

Check "**Line Prefixes**" and set the "Number of opcode bytes" to **6**, as shown below.



Find the code shown below, near the start of main():

```
0040111F 68 B0 60 40 00    push    offset ProcName ; "EnumProcessModules"
00401124 68 A4 60 40 00    push    offset LibFileName ; "psapi.dll"
00401129 FF 15 24 50 40 00 call    ds:LoadLibraryA
0040112F 50                push    eax             ; hModule
00401130 FF 15 20 50 40 00 call    ds:GetProcAddress
00401136 A3 14 87 40 00    mov     dword_408714, eax
0040113B 68 90 60 40 00    push    offset aGetmodulebasen ; "GetModuleBaseNameA"
00401140 68 A4 60 40 00    push    offset LibFileName ; "psapi.dll"
00401145 FF 15 24 50 40 00 call    ds:LoadLibraryA
0040114B 50                push    eax             ; hModule
0040114C FF 15 20 50 40 00 call    ds:GetProcAddress
00401152 A3 0C 87 40 00    mov     dword_40870C, eax
00401157 68 80 60 40 00    push    offset aEnumprocesses ; "EnumProcesses"
0040115C 68 A4 60 40 00    push    offset LibFileName ; "psapi.dll"
00401161 FF 15 24 50 40 00 call    ds:LoadLibraryA
00401167 50                push    eax             ; hModule
00401168 FF 15 20 50 40 00 call    ds:GetProcAddress
0040116E A3 10 87 40 00    mov     dword_408710, eax
```

This code uses *psapi* three times to locate a Windows API function and store its address in a numerical address. This obfuscates the code, so later calls to these functions will be difficult to recognize.

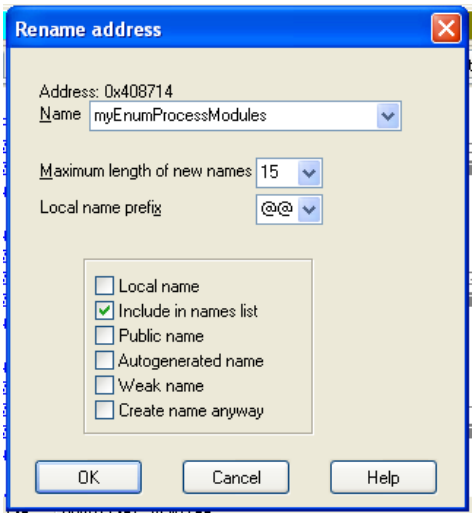
We'll assign labels to these memory addresses in IDA Pro to make later analysis easier.

The first section of code assigns a pointer to the function EnumProcessModules.

In the line starting with address 00401136, right-click **dword_408714** and click **Rename**.

Enter a new Name of **myEnumProcessModules** in the box, as shown below. Click **OK**.

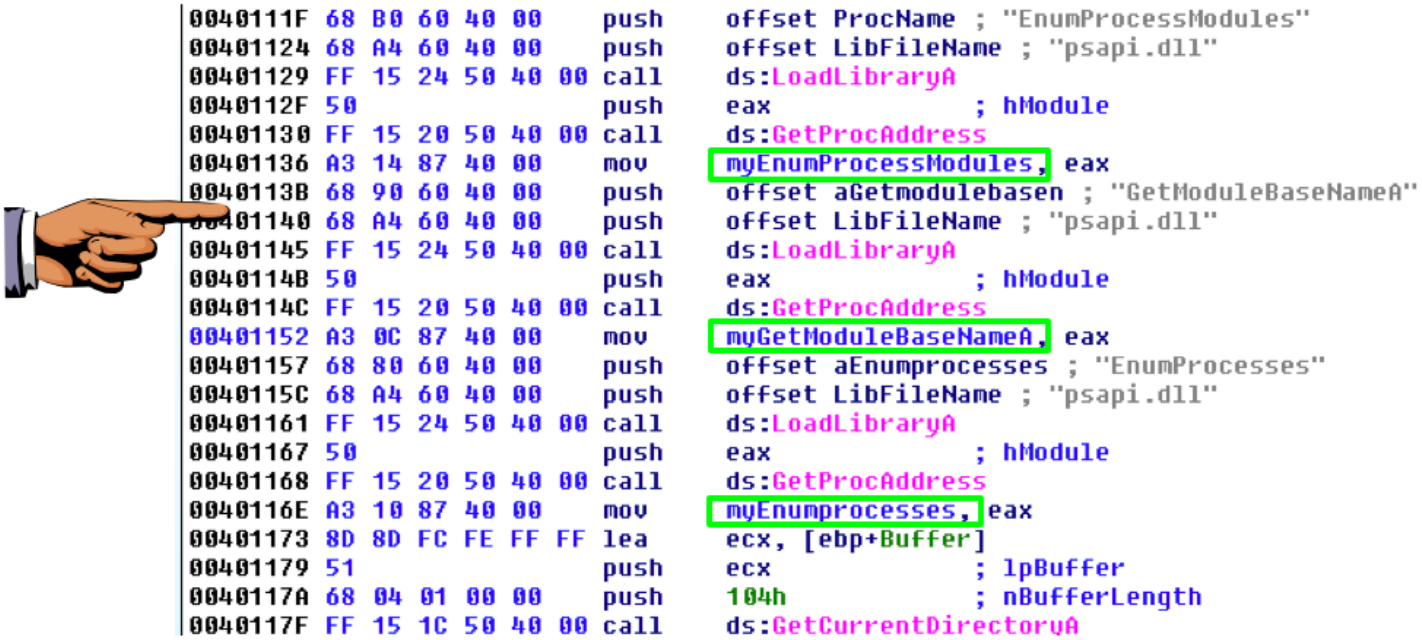
Increase the length limit when you are prompted to.



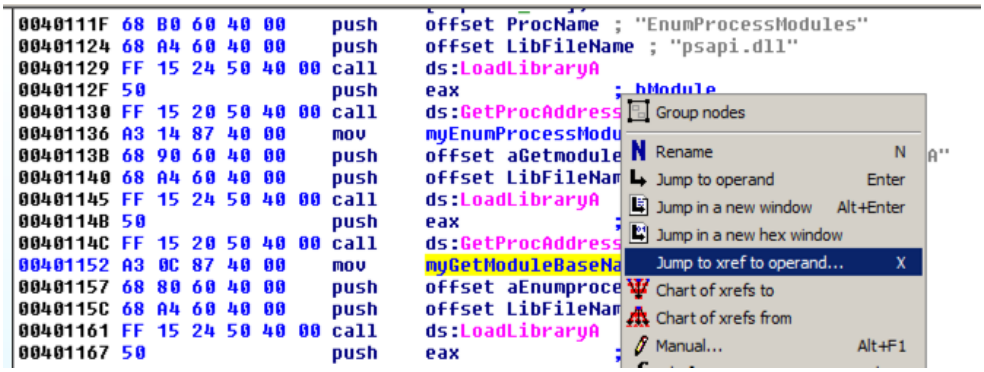
Repeat the process to rename **dword_40870C** to **myGetModuleBaseNameA**

Repeat the process to rename **dword_408710** to **myEnumProcesses**

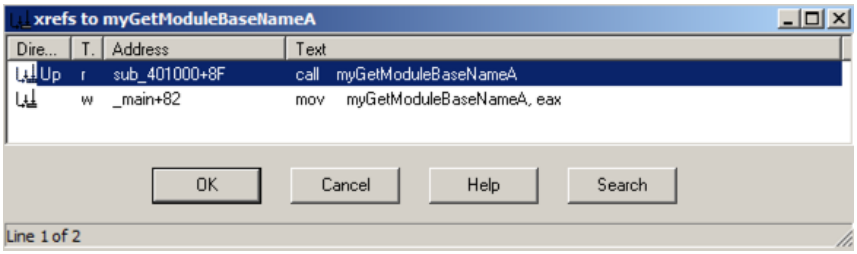
Save an image showing the three renamed locations, as shown below, with the filename "**Proj 15c from YOUR NAME**".



Right-click **myGetModuleBaseNameA** and click "**Jump tp xrefs of operand**", as shown below:



An xrefs box pops up, as shown below, showing that this address is only used once, in sub_401000.



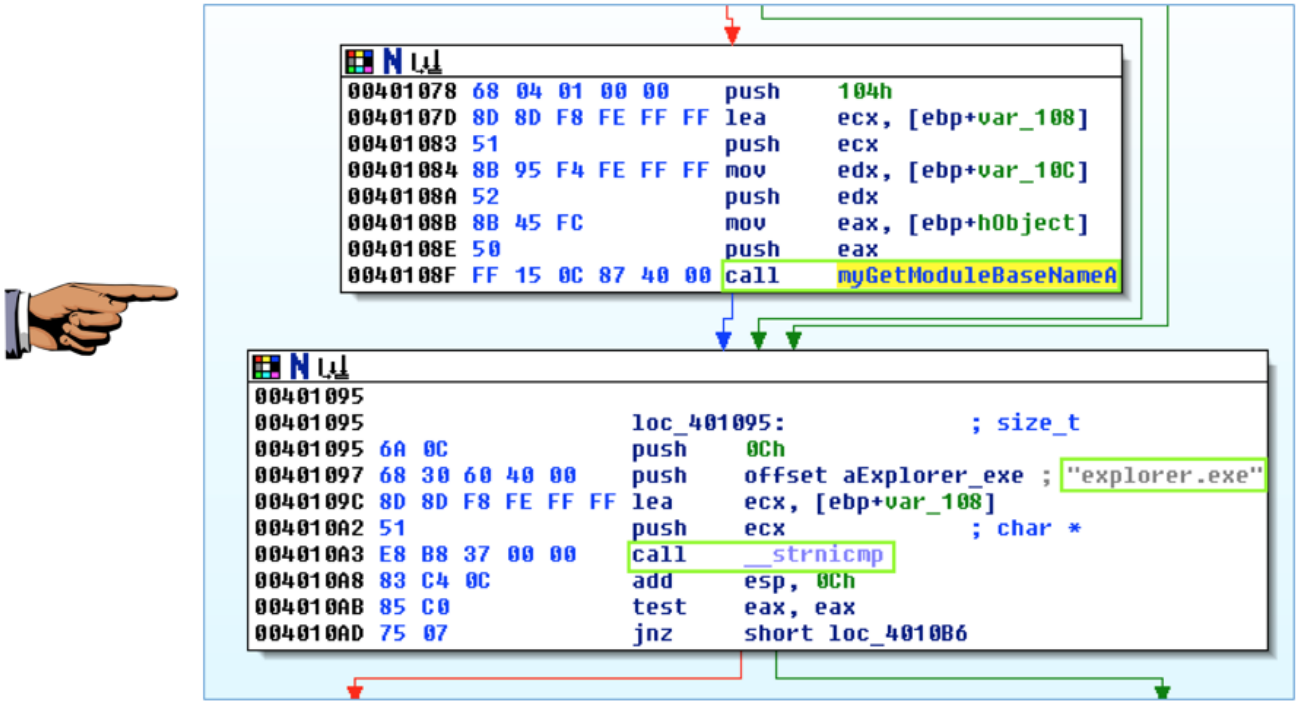
In the xrefs box, click **OK**.

This routine enumerates the modules and compares each module name to "explorer.exe", to find the module into which to inject code.

Make sure you can see these three items on your screen, as shown below:

- **call myGetModuleBaseNameA**
- **"explorer.exe"**
- **call __strnicmp**

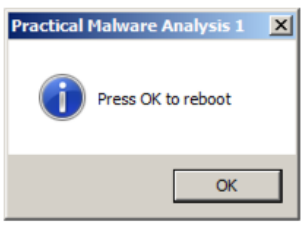
Save an image showing the three items highlighted below, with the filename "**Proj 15d from YOUR NAME**".



Process Explorer

Close IDA Pro. Double-click **Lab12-01.exe** to run the malware.

A box pops up saying "Press OK to reboot". as shown below. Drag this box out of the way.



Open Process Explorer.

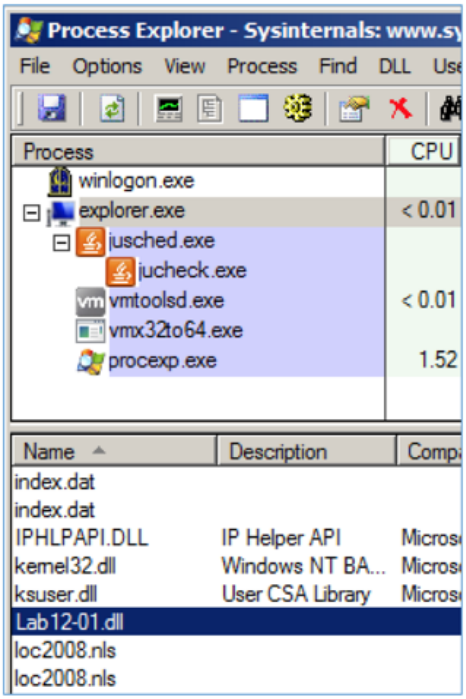
In the upper pane, scroll to the bottom of the list. Click **explorer.exe** to select it.

In Process Explorer, from the menu bar, click **View** and make sure "**Show Lower Pane**" is checked.

In Process Explorer, from the menu bar, click **View**, "**Lower Pane View**", **DLLs**.

In the lower pane, find the **Lab12-01.dll** that has been injected into explorer.exe, as shown below.

Save an image showing the **Lab12-01.dll** library, as highlighted below, with the filename "**Proj 15e from YOUR NAME**".



Turning in your Project

Email the images to cnit.126sam@gmail.com with the subject line: **Proj 15 from YOUR NAME**

Last modified 4-18-16