Anaisy Garcia

PID: 5734454

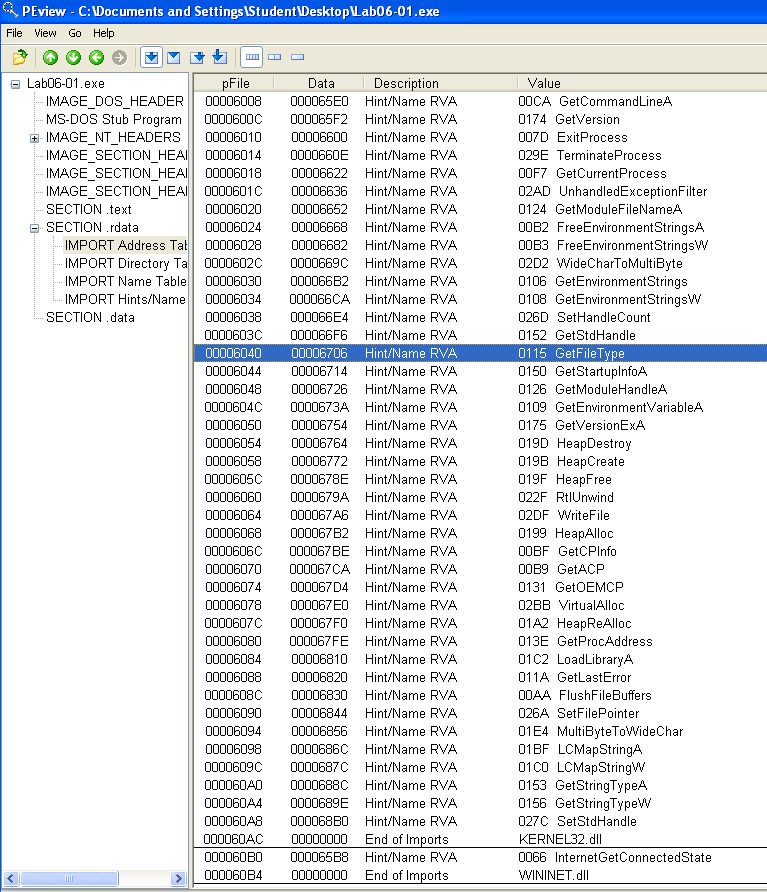
Lab 6-1

In this lab, you will analyze the malware found in the file Lab06-01.exe.

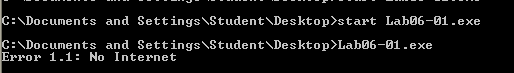
Questions

1. What is the major code construct found in the only subroutine called by main?

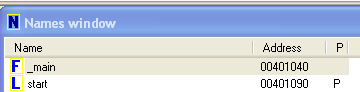
The imports show that this program uses an import called internetGetConnectedState.



Running the code by double clicking does nothing but running through command prompt using “start Lab06-01.exe”, shows up another command prompt open and then it disappears. It also shows up on process explorer and disappears as well as process monitor. Running through command line again without the start in front gives us an error that says, “Error 1.1: No Internet”.

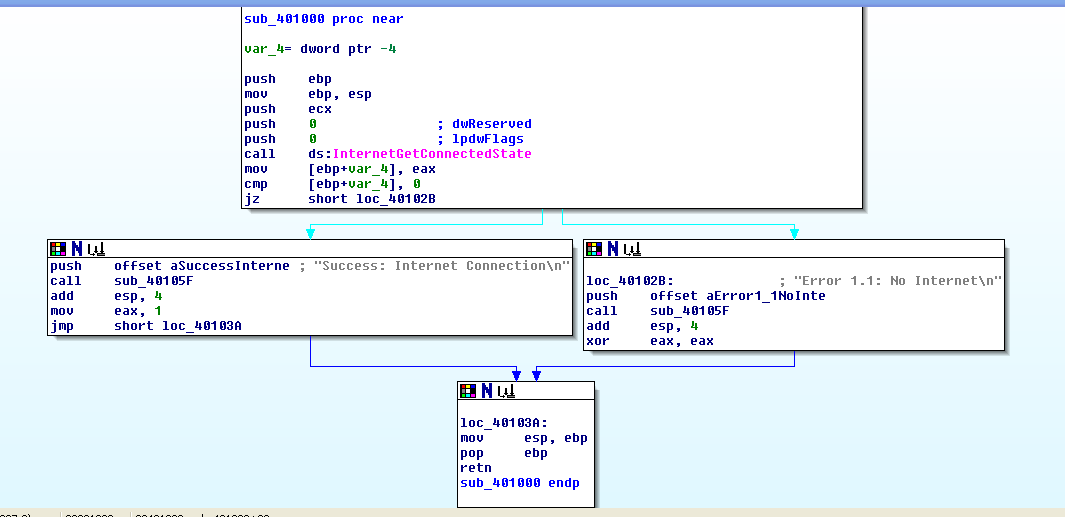


Running in IDAPro and finding main shows us that this program calls sub\_00401000 this is where the major code construct is located.



2. What is the subroutine located at 0x40105F?

This subroutine could be a print statement because the program is calling this subroutine after each \n string.



3. What is the purpose of this program?

This programs purpose is to check if there’s an active internet connection. Then prints this onto the console so the person using this malware or the malware itself knows there’s no connect.

