CMPSC 443 Lab 3: Malware Analysis 2 – Advanced Static Analysis

Student name: Matt Popovich

# Lab Description

The goal of the labs for this chapter is to help you to understand the overall functionality of a program by analyzing code constructs using IDA pro. Each lab will guide you through discovering and analyzing a new code construct. Each lab builds on the previous one, thus creating a single, complicated piece of malware with four constructs. Once you’ve finished working through the labs, you should be able to more easily recognize these individual constructs when you encounter them in malware.

## Task 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?

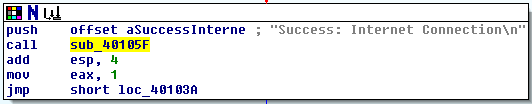
P:\CMPSC443\Git\CMPSC443\Lab07\Task1-CodeConstruct.PNG

“jz short loc\_40102B” is found in “sub\_401000” which is an instruction to jump to “short loc\_40102B” if the value at address “ebp+var\_4” is equal to zero.

This can be thought of as a C “if” condition.

2. What is the subroutine located at **0x40105F**?

This subroutine is called after a string is pushed onto the stack, leading me to believe that it is some sort of “print” subroutine.



3. What is the purpose of this program?

Based on this program’s call to the Windows API “InternetGetConnectedState” and the strings “Success: Internet Connection” and “Error 1.1: No Internet”, the program’s purpose is probably to determine whether the computer is connected to the internet or not.

## Task 2

Analyze the malware found in the file Lab06-02.exe.

**Questions**

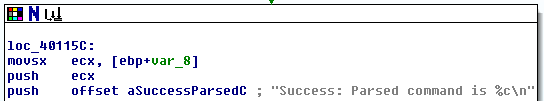
1. What operation does the first subroutine called by main perform?

The first subroutine called by main is “sub\_401000”. This subroutine is the program of Task1, it checks to see whether the computer is connected to the internet or not.

2. What is the subroutine located at **0x40117F**?

This subroutine is the same as Task1’s question2. It is a print subroutine.

3. What does the second subroutine called by main do?

The second subroutine called by main is “sub\_401040”. This subroutine sends a request for “http://www.practicalmalwareanalysis.com” with the internet agent being “Internet Explorer 7.5/pma”. With the response from the server it attempts to read the file and parse a command from the file. 

4. What type of code construct is used in this subroutine?

There are many “jnz” commands issued in this subroutine, all acting as “if” statements, some are even nested “if” statements.

5. Are there any network-based indicators for this program?

Yes, as explained in #3, this subroutine sends a request for “http://www.practicalmalwareanalysis.com” and attempts to read the file in the response. To do this, it calls “ds:InternetOpenA”, “ds:InternetOpenUrlA”, “ds:InternetReadFile”, and “ds:InternetClosehandle”.

6. What is the purpose of this malware?

This malware downloads a file from “http://www.practicalmalwareanalysis.com” then parses a command from the downloaded file.

This could be common activity from botnet or any malware that needs instructions from a master.

## Task 3

In this lab, we’ll analyze the malware found in the file Lab06-03.exe.

Questions

1. Compare the calls in main to Lab 6-2’s main method. What is the new function called from main?

Lab 6-2’s “main” method calls “sub\_401000” followed by “sub\_401040”, and lastly “sub\_40117F”.

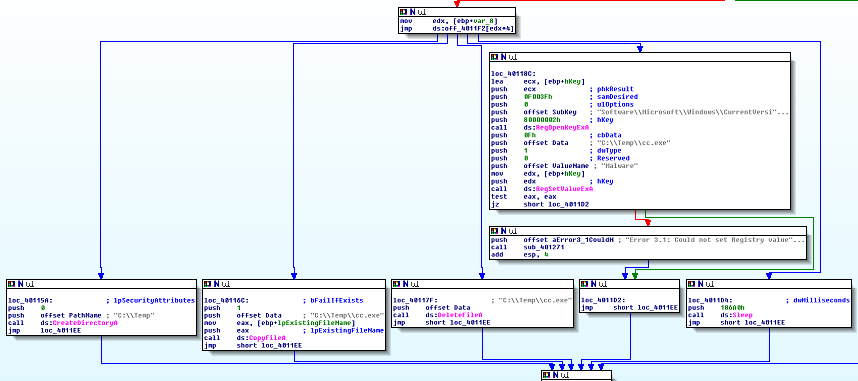
Lab 6-3’s “main” method calls the same functions as Lab 6-2 plus “sub\_401130”.

2. What parameters does this new function take?

This new function, “sub\_401130” takes “lpExistingFileName” and “char” as parameters.

3. What major code construct does this function contain?

This function contains a switch statement, which executes the next piece of code based on what the command received from the downloaded file is.



4. What can this function do?

This function does a different action based on the command. The possible actions are “CreateDirectoryA”, “CopyFileA”, “DeleteFileA”, “RegOpenKeyExA”, and “RegSetValueExA”.

5. Are there any host-based indicators for this malware?

The Windows API calls mentioned in #4 are all host-based indicators. Creating directories, modifying files, modifying the registry, etc.

6. What is the purpose of this malware?

This malware expands on 6-2’s malware. Once it reads the command from the downloaded file, it now executes that command, modifying the host’s machine.

## Task 4

In this lab, we’ll analyze the malware found in the file Lab06-04.exe.

Questions

1. What is the difference between the calls made from the main method in Labs 6-3 and 6-4?

All of the calls are the same between the two executables except before calling the function that downloads a file, it pushes a counter variable. This variable is then appended to the end of the client identifier.

2. What new code construct has been added to main?

“main” now has a loop encompassing the subroutine that downloads and executes a command from a remote server.

3. What is the difference between this lab’s parse HTML function and those of the previous labs?

This HTML function gets passed the loop’s counting variable and is then appended to the end of the client identifier.

4. How long will this program run? (Assume that it is connected to the Internet.)

This program is set to loop 0x5A0 = 1440 times. Each loop calls a sleep function for 0xEA60 = 60,000ms = 60 seconds.

1440 \* 60 seconds = 86400 seconds = 1440 minutes = 24 hours.

5. Are there any new network-based indicators for this malware?

The only new network-based indicator is the counter variable which is appended to the end of the client’s identifier.

6. What is the purpose of this malware?

Every minute this malware reads commands from a host and executes them. It will do this for 24 hours before exiting.

# Submission

|  |
| --- |
| Please submit a pdf or word report with brief answers to all questions. |