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?

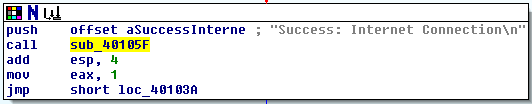
P:\CMPSC443\Git\CMPSC443\Lab07\Task1-CodeConstruct.PNG

“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**

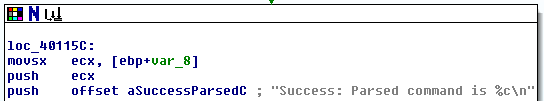
1. What operation does the first subroutine called by main perform?

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?

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

6. What is the purpose of this malware?

## 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?

2. What parameters does this new function take?

3. What major code construct does this function contain?

4. What can this function do?

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

6. What is the purpose of this malware?

## 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?

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

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

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

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

6. What is the purpose of this malware?

# Submission

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