Practical – Advanced Static Analysis of Windows Malware

A virtual machine has been provided for this practical. This is a safe environment for doing malware analysis without harming the lab computer or university network.

**** Please note - all activity on lab computers is monitored and recorded by Information Services. Please don't try to remove malware from the virtual machine or run it on the lab computers. Thank you. ****

Introduction

In this practical we will analyse several example Windows malware files using freely available static analysis tools. Please refer to your lecture notes for more information on the appropriate tools. Hint – these tools are very powerful so we can't include everything in the notes. Feel free to use google to find more information on each one. Please write a report for each piece of malware analysis in a Word document.

Starting the Virtual Machine

Follow these instructions to start the virtual machine and open a folder containing the required programs and example malware for analysis:

1. Using Windows Explorer browse to S:\Labs2020-21\CSC3059\
2. Click on CSC3059 Dynamic1 (this may take some time)
3. Click on VM icon at bottom of screen
4. Select MW_Windows in left-hand pane
5. Click Start
6. Click on Labuser with password 'malware'
7. Click on IDA Pro Free Icon at bottom of VM
8. Select New on pop-up Window (do not select previous)
9. Go to File►Open

Starting the Practical

The malware files needed for the practical are stored on the virtual machine at:
C:\Labs\BinaryCollection\Chapter_6L\

Practical – Advanced Static Analysis of Windows Malware

Part 1

Open malware file Lab06-01.exe. Work your way through CSC3059 Week7 Lecture 3 to familiarise yourself with IDA.

- Open the different disassembly Window Modes
- Navigate around IDA
- Use cross-references
- Visualise the different graphing options

Part 2

Analyse the malware found in the file Lab06-01.exe using IDA.

1. What is the major code construct found in the only subroutine called by main?
2. What is the subroutine located at 0x40105F?

    - Hint - Use the x-refs feature to find places where this function is called. Then examine the context of how the function is used.

3. What is the overall purpose of this program?

Part 3

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

1. What operation does the first subroutine called by main perform?
2. What is the subroutine located at 0x40117F?
3. What does the second subroutine called by main, located at 0x401040, do?
4. What is the major type of code construct used in subroutine sub_401040?
5. Are there any network-based indicators for this program?
6. What is the purpose of this malware?