Practical – Dynamic Analysis of Windows Malware

Two virtual machines, one Windows-based the other Linux/Unix, have 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 and dynamic 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. **Finally, remember to write a report about what you have found.**

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 Dynamic (this may take some time)
3. Click on VM icon at bottom of screen
4. Select MW_Ubuntu in the left-hand pane.
5. Click Start
6. Login using 'labuser' as username and 'malware' as password
7. **Click on Oracle VM Virtual Box Manager icon at bottom of screen.**
8. Select MW_Windows in left-hand pane
9. Click Start
10. Click on Labuser with password 'malware'
11. Using Windows Explorer on VM navigate to C:\Labs

Part 1

Analyze the malware found in the file Lab06-01.exe using basic static analysis tools.

1. What are this malware's imports and strings?

Hint – use PEView to examine SECTION.rdata -> IMPORT Address Table

Part 2

We will now analyse the malware in Lab06-02.exe using basic dynamic analysis. This will involve using both host-based and network-based tools. Because this malware attempts to access resources on the network, we will set up a virtual network to allow the malware to run. Firstly we will set everything up, then we will analyse all the host-based events, and finally we will analyse all the network-based events.

1. Run strings to see if there are any network-based signatures.

Setup Instructions

We will now set up the dynamic analysis tools needed for the rest of this practical

1. Run ProcessMonitor
   Clear out all existing events and create a filter for *Process Name* is *Lab06-02.exe*
2. Start Process Explorer
3. Run apateDNS.exe.
   In the DNS Reply IP textbox enter 192.168.117.169 and click on Start Server button
4. Start the MW-Ubuntu virtual machine.
   This will take a moment to boot into the command line.
   The username is ‘labuser’ and the password is ‘malware’
5. In the Ubuntu virtual machine command line type *sudo inetsim* and enter the password *malware*
6. On the Windows machine, set up network traffic logging using Wireshark.
   When Wireshark starts, double click on ‘Local Area Connection’
7. Run the malware file Lab06-02.exe

2. Examine the Lab06-02.exe process in Process Explorer. What do you notice?

   Hint – Does it create any mutants? Has it loaded any DLLs?

3. Use Process Monitor to look for additional information

   Hint – Set up three filters. One on Process Name *Lab06-02.exe* and two more on Operation is *RegSetValue* and Operation is *Writefile*

4. Check to see whether the malware has made any changes to the registry.

   Hint – use Regshot

Part 3

Analyze the malware found in file Lab06-02.exe using network-based dynamic tools. Note that the Lab06-02.exe will close after some time, but you can restart it again as many times as needed.

1. Run the malware Lab06-02.exe and check if there were any DNS requests

   Hint – Use ApateDNS

2. Review the network traffic generated by the malware

   Hint – Use Wireshark

3. Check to see whether the malware attempts to make any HTTP or TCP connections.

   Hint – Use Netcat on the Ubuntu Virtual Machine
   If inetsim is running you can stop it by pressing *ctrl-c*
   Listen on port 80 using netcat by typing *sudo nc –l –p 80*
   Enter the password *malware*
   In Windows run Lab06-02.exe and monitor its requests using netcat on Ubuntu