CS4238 Homework 4: Malware Analysis

Instructions

Due date & time: 14 November 2021, 23:59 SGT. This is an **individual** project. You MUST finish the implementation and report independently.

The deadline is a soft deadline. If you need a few extra days due to the load of last week, please request an extension before the deadline.

Instruction:

- Malware samples are in HW4-files.zip. Password: infectednus

Part 1 – x86 Disassembly and IDA Pro (5 marks)

Recommended Reading:

- Chapters 4 and 5 from "Practical Malware Analysis" textbook.

Instruction:

- Review http://opensecuritytraining.info/IntroX86.html if you need additional ramp up into x86 assembly code. This is highly recommended since the rest of the class will be highly focused on analyzing x86 assembly code.
- Keep using your basic static and dynamic analysis skills, but the focus here is on learning to review x86 code and using IDA Pro.

HW-B-1.exe

(Hint: printf() is 0x401089, main() is 0x401060)

1. Focus on the main() method. What is stored in EAX prior to the function call at 0x40107D?
2. Focus on the function that starts at 0x401000. What does 0x62, 0x63, 0x73 likely correspond to?
3. What coding construct is likely a major part of this function?
4. What does this function (0x401000) do?
5. What does this overall program do?

Part 2 – Code Constructs in Malware (5 marks)

Recommended Reading:

- Chapter 6 from "Practical Malware Analysis" textbook.

Instruction:

- The focus of these questions is to work towards recognizing individual constructs common in malware.

HW-B-3.exe

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

Part 3 – Malware Functionality (5 marks)

Recommended Reading:

- Chapters 11 and 12 from "Practical Malware Analysis" textbook.

Hint-1: These binaries can only be run in 32-bit Windows. Please use a Win7 32-bit VM for this analysis. we have uploaded a VM image for VirtualBox:
https://drive.google.com/file/d/1U0VVRozitW4PzyCXe0CCkt-yxDPzxovN/view

Hint-2: The DLL file has to be renamed to another filename for the EXE loader to work)

HW-B-8a.exe & HW-B-8b.dll

1. Run HW-B-8a.exe from the command line. What happens?
2. What method does HW-B-8a.exe use to perform covert launching?
3. What process is targeted by the malware?
4. What file(s) do HW-B-8b.dll create?
5. What is the content of these files?