CS4238 Homework 3: Basic Malware Static Analysis and Dynamic Analysis

1 Instructions

Due date & time: 1 November 2021, 23:59 SGT. This is an **individual** project. You MUST finish the implementation and report independently.

2 Assignment Tasks

Instruction:

- Perform malware analysis using basic static analysis techniques. Answer all questions using only basic static analysis techniques for these two binaries provided.
- Malware samples are in HW3-files.zip. **Password:** infectednus

Basic Static Analysis (5 marks)

Recommended Reading:

Chapters 0 and 1 from "Practical Malware Analysis" textbook.

Task 1: Answer the following questions after analyzing HW-A-1.exe

1. Upload the file to https://www.virustotal.com. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. When was this program compiled?
4. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
5. What host- or network-based indicators could be used to identify this malware on infected machines?

Task 2: Answer the following questions after analyzing HW-A-2.exe

1. Upload the file to https://www.virustotal.com. Does it match any existing antivirus definitions?
2. When was this program compiled?
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?
5. This file has multiple resources in its resource section. What are their respective MD5 or SHA hashes? (Resources should be in BIN format)
6. What are the differences between the resources?

Basic Static and Dynamic Analysis (5 marks)

Recommended Reading:

Chapters 2 and 3 from "Practical Malware Analysis" textbook.

Task 3: Answer the following questions after analyzing HW-A-3.exe

1. Are there any indications that this file is packed or obfuscated?
2. When was this program compiled?
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What can you observe using Basic Static Analysis techniques?
5. What do you observe through dynamic analysis?
6. List the potential host-based indicators of this malware.
7. List the potential network-based indicators of this malware.
8. How many different domains do you think the malware can connect to? What are those domains?

PE File Format (5 marks)

Task 4: Write a Python script that uses the pefile API (https://code.google.com/p/pefile/). The script should perform the following operations. (Include your code and screenshots of the results in running the script in the report) The script takes a PE format file inputted from the command line.

1. Output the following to standard output:
   a. Identify the file type as DLL or EXE or SYS regardless of the file's extension.
   b. Total number of imported DLLs.
   c. Total number of imported functions.
   d. Output the compile time.
2. Alert the user if the entry point of the code is not in a section with the name ".text", ".code", "CODE", or "INIT".
3. Automatically use the PEiD database that comes with pefile to identify packers. Confirm that this works with UPX. Output the detection to standard output.
4. Calculate and output the entropy for each section. Alert the user when you suspect that a section maybe packed or compressed.
5. Alert the user when there is a zero sized section.
6. Compare the PE Optional Header checksum with the actual checksum. Alert the user when they don't match up.
7. If there is a resource section, dump the first resource (of any type) to a file on disk.