**CMSC 491/691 Malware Analysis HW 4**

Name:

Assigned: 4/12/2023

Due: 4/19/2023 by 5:30pm

Download hw4.7z onto your Flare VM and extract it. The password is “infected”. Set your VM’s network adapter to “not attached”. Open hw4.exe in IDA or Ghidra and **run the Debugger** of your choice **as Administrator**, as the malware requires Administrator privileges to run properly. Take a snapshot of your VM when your tools are set up because you will likely need to revert multiple times.

Please provide screenshots as you see fit. Remember, they can only strengthen your answers.

Hint: Chapters 9, 11, and 12 of your Practical Malware Analysis textbook are very useful references!

**Part 1: hw4.exe (75 pts)**

Use your debugger, aided by IDA or Ghidra, to answer the following questions.

1) What is the value of the first argument to CreateFileA when it is called at 0x4012AA? What is the desired access mode? (Expecting the name of the access mode, not an integer) (5 pts)

2) What is the value of the first argument to CreateFileA when it is called at 0x40135E? What is the desired access mode? (Expecting the name of the access mode, not an integer) (5 pts)

3) Provide an in-depth analysis of the instructions between 0x40136A and 0x401395. Make sure to be specific about any files and file attributes that are read or modified. Why might the malware be doing this? (15 pts)

4) What is the value of the second argument to SetFileAttributesA when it is called at 0x4013A7? (Expecting the names of the attributes, not an integer) What is the name of the file that SetFileAttributesA modifies, and why might the malware be doing this? (8 pts)

5) What is the value of the second argument to RegCreateKeyExA when FUN\_4011b4 is called at 0x4017C8? (5 pts)

6) The call to RegCreateKeyExA in question 5 fails and returns an integer that corresponds to an error code. What is the name of this error code? (5 pts)

7) Because the call to RegCreateKeyExA in question 5 fails, the JNZ at 0x4011EF will jump to 0x401217. Use the debugger to force the program not to take this jump. Describe how you did this and provide a screenshot of the debugger window with execution paused at 0x4011F1 (12 pts).

8) Provide a detailed analysis of the instructions between 0x401857 and 0x40188a. Why might the malware be doing this? (12 pts)

9) What is unusual about the instructions between 0x4019AA and 0x4019C1? Why might the malware be doing this? (8 pts)

**Part 2: File Created by hw4.exe (25 pts)**

Use Ghidra to analyze the file created by hw4.exe in question 2 (Hint: keep in mind the attributes of this file when searching for it. The file’s md5 begins with 3288c303 if you want to confirm that you have the correct file). Answer the following questions. IDA fails to correctly analyze parts of this file, so Ghidra is recommended. You will not need to use a debugger.

10) Provide a detailed analysis of the instructions between 0x404F4D and 0x404F79. What is the name of this technique? (8 pts)

11) Investigate the Windows API functions that are called between 0x4040FA and 0x404284. Which of the following techniques from PMA chapter 12 most closely describes what the malware is doing: DLL injection, direct injection, or process replacement? Justify your answer. (10 pts)

12) FUN\_4047EC can open a registry key and query one of its values. Answer the following questions about FUN\_4047EC when it is called within FUN\_404DA0.

 a) What is the name of the subkey that is opened? (2 pts)

 b) What is the name of the value that is opened? (2 pts)

 c) Why might the malware be doing this? (3 pts)