**CMSC 691 Malware Analysis HW 4**

Name:

Assigned: 3/17/2025

Due: Thursday, 3/27/2025

Download hw4.7z onto your malware analysis VM and extract it with the password “infected”.

hw4.7z link:

* <https://drive.google.com/file/d/1XgE471vciUQ1XqwkiRNxmQFdzU1E9eT9/view?usp=drive_link>

Hint: Chapters 4, 5, and 6 of your Practical Malware Analysis textbook are very useful references!

**hw4.infected (100 pts)**

In this assignment, you will investigate hw4.infected using IDA Pro. To open hw4.infected in IDA Pro, make sure to search for “All files” in the file explorer. Answer the following questions.

1) What is the address of the string ServerMain in hw4.infected? (6 pts)

2) There is one cross-reference (XREF) to the string ServerMain in hw4.infected. What is the address of the instruction that references the string ServerMain in hw4.infected? (6 pts)

3) How many XREFs are there to the function sub\_10001989? (6 pts)

4) How many local variables does sub\_10001989 have? (4 pts)

5) How many parameters does sub\_10001989 have? (4 pts)

6) In a web browser, navigate to <https://docs.microsoft.com> and search for the LoadLibraryA function. In a few sentences, describe what the function does. Make sure to be clear about what a “module” is. (4 pts)

7) Navigate to the address 0x1000430C. Provide a detailed analysis of the code between 0x1000430C and 0x1000435C. Be specific about what will be stored inside of the global variable dword\_1008EF94 when the code finishes. (18 pts)

8) What is the name of the malicious technique that the malware is using between 0x1000430C and 0x1000435C? (6 pts)

9) Search <https://docs.microsoft.com> for the CreateThread function. Briefly summarize the difference between a process and a thread. (4 pts)

10) Continuing to look at the CreateThread documentation, describe the purpose of the lpStartAddress argument. (4 pts)

11) In IDA Pro, navigate to the address 0x10003E25. When the malware calls CreateThread here, what is the address of the code that will be executed? (6 pts)

12) Investigate the code that is run by the call to CreateThread at 0x10003E25. Within this code, the malware calls the Sleep function twice. For how many **seconds** will the malware sleep the first time the Sleep function is called? How many seconds will it sleep the second time? Give your answers in decimal, not hex. (14 pts)

13) Navigate to the address 0x10005B05. Provide a detailed analysis of the code between 0x10005B05 and 0x10005B26. Make sure to describe the name of the mutex that is created. (18 pts)