**CMSC 691 Malware Analysis HW 5**

Name:

Assigned: 3/31/2025

Due: 4/9/2025

Download hw5.7z onto your malware analysis VM and extract it with the password “infected”.

hw5.7z link:

* <https://drive.google.com/file/d/1s4mmJpCTWBqXOfNLIzDSjC8hV-pXEjeu/view?usp=sharing>

**hw5.infected (100 pts)**

Answer the following questions about hw5.infected using Ghidra.

1) How many DLL files does the malware import functions from? (4 pts)

2) What is the address of the string “kbdax2.dll”? (4 pts)

3) What is the address of the ServiceMain export? (4 pts)

4) How many parameters does the function FUN\_10003060 take? How many local variables does it have? (6 pts)

5) How many times is WriteFile called inside of hw5.infected? (5 pts)

6) In what function is GetEnvironmentVariableA called? (5 pts)

7) Describe in detail what the malware is doing between the addresses 0x100018DC and 0x10001937. (15 pts)

8) Investigate the call to GetModuleHandleA at 0x10002593. What DLL will this function return a handle for? Justify your answer with analysis from hw5.infected. (15 pts)

9) Describe in detail what the malware is doing between the addresses 0x10001210 and 0x100012425. Make sure to be specific about how the first and second arguments of FUN\_10001210 are used in this code snippet. (15 pts)

10) The function FUN\_10001580 calls FUN\_10001210 at 0x100015DA. Using your analysis from question 9, what will be the name of the file created when execution reaches the call to CreateFileA at 0x10001268? (15 pts)

11) Investigate the global variable DAT\_10011444. Rename this variable in Ghidra, and then justify your naming choice with analysis from hw5.infected. Then, provide a screenshot of your renamed variable. (12 pts)

Screenshot: