**CMSC 491/691 Malware Analysis HW 3**

Name:

Assigned: 3/7/2023

Due: 3/16/2023 by 11:59pm

For this assignment you will need to work on the Windows 7 version of the Flare VM. You can download and install from the course web site or this web site

<https://drive.google.com/file/d/1L0Pr02GlwhRLAsmrRc-J0v8Gm3_ShaAG/view?usp=sharing>

Download hw3.zip onto your Flare VM and extract it with the password “infected”. Use either IDA Pro or Ghidra to analyze the malware sample (This homework will use the naming conventions from Ghidra). Make sure to upload a PDF and Word Document of your homework. Chapters 4, 5, and 6 of **Practical Malware Analysis** may be useful! A late penalty of 10% per day will apply to assignments turned in on March 17 or later.

**Part 1: hw3.exe (50 pts)**

1) How many functions are imported from SHELL32.dll? (5 pts)

2) How many unique functions call WriteFile? (5 pts)

3) At what address does hw3.exe call gethostbyname? What argument is passed? (5 pts)

4) How many references to LoadLibraryA are in hw3.exe? For the LoadLibrary call(s), what is the value of the argument passed? (7pts)

5) Provide a detailed analysis of what FUN\_401630 does. What file attribute is assigned at address 4016b3? Given this functionality, what can you guess the second argument at address 401647 is? (10 pts)

6) Provide a detailed analysis of what FUN\_4016c6 does. Make sure to describe any Windows APIs present in the function. (8 pts)

7) Provide a detailed analysis of what FUN\_401722 does. Choose a new, descriptive name for function FUN\_401722. Justify why you chose this name and provide a screenshot of IDA or Ghidra showing that you have renamed the function. (10 pts)

**Part 2: kjlib.dll and kjpost.dll (50 pts)**

Next, configure the network settings of your Flare VM so that it is safe to run malware. You can either run FakeNet-NG or completely disconnect the VM from the network by changings its network adapter to **“Not Attached”** in the VirtualBox network settings. Once you have done this, run the malware **with administrator privileges.** Then, answer the following questions about kjlib.dll and kjpost.dll, which the malware creates.

1) What is the address of kjlib.dll’s StartHooking export? (4 pts)

2) Use the Strings window to locate the string “kjlib.dll” in the disassembly. Where is that string located? (4 pts)

3) How many local variable and parameters has IDA/Ghidra recognized for the function Fun\_100014cc (in Ghidra) or (Function **fn** in IDA) at 0x100014cc? (6 pts)

4) Navigate to FUN\_100014CC. What is happening at address 10001522 inside the function? (7 pts)

5) The buffer that receives the output in Question 4 is copied to a global variable at address 10001536. How many XREFs are there to this global variable? (8 pts)

6) After CreateFileA is called inside of FUN\_100014CC, its return value is moved into a global variable. What does the 5th parameter of CreateFileA specify about the file? (4 pts)

7) Investigate the XREFs of the global variable in #6. Choose a new name for this variable based on your analysis and justify why you chose this name. (5 pts)

Open kjpost.dll in IDA or Ghidra and answer the following question:

8) Provide a detailed analysis of what FUN\_100016da in kjpost.dll does. (6 pts)

9) Investigate FUN\_100012f6 and give brief overview of what this function is trying to achieve (6 pts)