**CMSC 691 Malware Analysis HW 7**

Name:

Assigned: 4/23/2025

Due: 5/5/2025 by 11:59pm

Download hw7.7z onto your Flare VM and extract it. The password is “infected”. Set your VM’s network adapter to “not attached”. Take a snapshot of your VM when your VM is set up because you will likely need to revert multiple times. You are not required to run x32dbg as an administrator.

hw7.7z:

* <https://drive.google.com/file/d/1zUtRjFPBDz9wbPOxxNrPf2AohbRaMky9/view?usp=drive_link>

Hint: Chapter 18 of PMA is a great reference for this homework!

**Part 1: Unpacking hw7\_1.exe (30 pts)**

Answer the following questions about hw7\_1.exe.

1) What section contains the packed data? Justify your answer. (4 pts)

2) What section does the unpacking stub begin in? Justify your answer. (4 pts)

3) Use the first method (locating the tail jump in IDA Pro) to find the tail jump. What is the address of the OEP? In a few sentences, describe how you found the OEP. Unlike the files shown in class, the boilerplate code after the entrypoint includes a call to GetStartupInfoA, not GetVersion and GetCommandlineA. (8 pts)

Address of OEP:

Description:

4) Open Notepad on your VM and type your full name into it. Provide a screenshot of x32dbg showing execution paused at the OEP. Make sure that your screenshot also shows your full name. (8 pts)

5) Use Scylla to dump the unpacked file from memory and then fix the dump. Provide a screenshot of Scylla showing which DLLs were identified, and how many imports were found for each DLL. Also, make sure that the screenshot also shows your full name in Notepad. (6 pts)

**Part 2: Unpacking hw7\_2.exe (30 pts)**

Answer the following questions about hw7\_2.exe.

6) What section contains the packed data? Justify your answer. (4 pts)

7) What section does the unpacking stub begin in? Justify your answer. (4 pts)

8) Use the second method (PUSHA/PUSHAD instruction) to find the tail jump. Hint: Step through the first ~2 dozen instructions of the program in the debugger until you find (and step over) the PUSHAD instruction. What is the address of the OEP? In a few sentences, describe how you found the OEP. (8 pts)

Address of OEP:

Description:

9) Open Notepad on your VM and type your full name into it. Provide a screenshot of x32dbg showing execution paused at the OEP. Make sure that your screenshot also shows your full name. (8 pts)

10) Use Scylla to dump the unpacked file from memory and then fix the dump. Provide a screenshot of Scylla showing which DLLs were identified, and how many imports were found for each DLL. Also, make sure that the screenshot also shows your full name in Notepad. (6 pts)

**Part 3: Unpacking hw7\_3.exe (40 pts)**

Answer the following questions about hw7\_3.exe.

11) What section contains the packed data? Justify your answer. If the section name is not printable, you may use the section number that appears in Detect It Easy. (4 pts)

12) What section does the unupacking stub begin in? Justify your answer. If the section name is not printable, you may use the section number that appears in Detect It Easy. (4 pts)

13) Use the third method (setting breakpoints on LoadLibrary/GetProcAddress) to find the tail jump. Then, answer the following questions:

1. What is the name of the final DLL which was loaded by LoadLibraryA / LoadLibraryW in the unpacking stub? (5 pts)
2. What is the name of the final function which was loaded by GetProcAddress in the unpacking stub? (5 pts)
3. What is the address of the OEP? (6 pts)

14) Open Notepad on your VM and type your full name into it. Provide a screenshot of x32dbg showing execution paused at the OEP. Make sure that your screenshot also shows your full name. (10 pts)

15) Use Scylla to dump the unpacked file from memory and then fix the dump. Provide a screenshot of Scylla showing which DLLs were identified, and how many imports were found for each DLL. Also, make sure that the screenshot also shows your full name in Notepad. (6 pts)