**CMSC 449/691 Malware Analysis HW 1**

Name:

Assigned: Monday 2/10/2025

Due: Monday 2/17/2025 at 11:59pm

Download and extract hw1.zip on your malware analysis VM. The password to the zip file is **infected**. The zip file contains hw1\_1.infected and hw1\_2.infected, which are malicious files. They have been given the .infected extension so that they cannot be run by double clicking them. **Do NOT run them!**

* <https://drive.google.com/file/d/19-gKiEPJJqbnn6xp3imRWshLgUHUrUZG/view?usp=sharing>

Hint: Chapter 1 and Appendix A of Practical Malware Analysis are very useful references! Other parts of the textbook may be helpful as well.

**Part 1: hw1\_1.infected (60 pts)**

1) What is the MD5 hash digest of hw1\_1.infected? For this and any other questions asking for a hash, you may provide a screenshot of the hash value rather than typing it out. (2 pts)

2) Upload the unpacked hw1\_1.infected to VirusTotal. What is the file’s Import hash (Imphash)? (2 pts)

3) In a few sentences, describe what an Import hash is, and why it is useful to malware analysts. (6 pts)

4) Which PE section in hw1\_1.infected contains executable code? What is the virtual size of this section? How did you find this information? (6 pts)

5) What is the exact date and time (to the second) that hw1\_1.infected was compiled? How did you find this information? (5 pts)

6) How many DLL files does hw1\_1.infected import functions from? (4 pts)

7) How many total functions does hw1\_1.infected import from ADVAPI32.dll? (4 pts)

8) List three functions imported by hw1\_1.infected that you believe are suspicious (i.e. would not ordinarily be used by legitimate programs). For each function, name the DLL that the function was imported from, summarize what the function does, and describe how hw1\_1.infected could use it for malicious purposes. You will lose points if common functions (such as strcpy, CreateFileA, WriteFileA, and GetCommandLineA) are given. (15 pts)

Function 1:

Function 2:

Function 3:

9) Run the strings (or floss) command on hw1\_1.infected. Multiple strings include the name of a DLL that is not listed in the malware’s Import Address Table. What is the name of that DLL? (4 pts)

10) Search the internet for the name of the DLL you found in #9. Investigate the other strings in the file. Based on these, what do you think the purpose of hw1\_1.infected is? Justify your answer. (12 pts)

**Part 2: hw1\_2.infected (40 pts)**

1) What is the MD5 hash digest of hw1\_2.infected? (2 pts)

2) List three features of hw1\_2.infected which indicate that the file is packed. What is the name of the packer it was packed with? (15 pts)

Indicator 1:

Indicator 2:

Indicator 3:

Name of packer:

3) Unpack hw1\_2.infected and provide the command you used to unpack it. What is the MD5 digest of the unpacked file? (6 pts)

How you unpacked it:

MD5 of unpacked file:

Use Resource Hacker to save the first resource in the unpacked file as a BIN file. Then, answer questions 4 and 5.

4) The first few bytes of a file usually indicate what type of file it is. What are the first 4 bytes of the saved resource? Based on these bytes, what file extension should it have? What are files of this type typically used for? (8 pts)

5) Based on the file type of the saved BIN file resource, continue to investigate its contents. Rename the BIN file so that it has the correct file extension. Then, research how to open this kind of file. Describe what you find when you open it. (7 pts)