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

Name:

Assigned: 2/8/2023

Due: 2/15/2023 at 5:30pm

Download and extract hw1.zip on a virtual machine. The password to the zip file is “infected”. It contains hw1\_1.infected and hw1\_2.infected, which are malware samples. **Do NOT run them!**

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

You will submit your own, much revised, copy of this Word document. On this occasion, we will NOT accept PDF documents. Word files only! Submit through Blackboard in the usual way. Reminder: work that you submit for credit is to be YOUR work. Do **not** share screenshots. We can detect this easily!

**Part 1: hw1\_1.infected (50 pts)**

1) Find the following hashes for hw1\_1.infected. (2 pts)

MD5:

SHA-265:

2) In a few sentences, describe why hashes like MD5, SHA-1, and SHA-256 are useful to malware analysts (8 pts)

3) Which PE section in hw1\_1.infected contains executable code? What is the virtual size and raw size of this section? How did you find this information? (7 pts)

4) What is the exact date and time (to the second) that hw1\_1.infected was compiled? How did you find this information? (4 pts)

5) Do any of the Windows API functions imported by hw1\_1.infected suggest that it is able to connect to the internet? Do any of the strings in hw1\_1.infected suggest that it is able to connect to the internet? Why might this be suspicious? (10 pts)

6) List three other Windows API functions imported by hw1\_1.infected that you believe are suspicious. For each function, list what the function does and how hw1\_1.infected could use it for malicious purposes (12 pts).

Function 1:

Function 2:

Function 3:

7) One of the strings in hw1\_1.infected is a registry key that is commonly used to give malware persistence. What is the string and how does it maintain persistence? (7 pts)

**Part 2: hw1\_2.infected (50 pts)**

1) Find the following hashes for hw1\_2.infected. (2 pts)

MD5:

SHA-265:

2) In a few sentences, explain why malware authors pack their malware. How could you analyze the malware, even if it’s packed? (8 pts)

3) List three indicators that hw1\_2.infected is packed. What is the name of the packer it was packed with? (15 pts)

Indicator 1:

Indicator 2:

Indicator 3:

Name of packer:

4) Unpack hw1\_2.infected and describe how you unpacked it. What is the MD5 of the unpacked file? What is the SHA-265 of the unpacked file? Attach a screenshot of your hashes. (8 pts)

5) Use Resource Hacker to save the first resource in the unpacked file as a .bin file. What is the MD5 of the saved resource? (2 pts)

6) 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 type of file is it? What are files of this type used for? Attach a screenshot of the Resource Hacker window. Make sure to include the first 4 bytes in the screenshot. (12 pts)

7) Based on the file type of the saved resource, how would you continue to investigate its contents? List two different approaches. (3 pts)