**CMSC 449 Malware Analysis HW 2**

Name: \_\_\_\_\_\_\_\_\_\_\_\_

Assigned: 2/20/2023

Due: 3/1/2023 at 5:30pm

For this assignment you will need to work on the Windows 7 version of the Flare VM which 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 and extract hw2.7z on a virtual machine. The password to the zip file is “infected”, without the quotes. The file contains hw2.exe and hw2\_2.exe, which are live malware samples.

<https://drive.google.com/file/d/1bwVFu0XDHgSu_5iqpeWCdgX8vTzj6OCv/view?usp=sharing>

Take a snapshot of your VM before starting this homework assignment!

**You should only run the malware while your VM is not connected to the internet and/or FakeNet-NG has been configured!**

LATE PENALTY: Assignments turned in late -5 points first 24 hours, -10 points 24-48 hours late, -50 points after that.

**Part 1: hw2.exe (40 pts)**

1) Follow the FakeNet-NG network configuration instructions that have been posted on the course web site. Provide a screenshot of your VM once you have completed step 9, showing a successful ping command while FakeNet-NG is running. (10 pts)

2) Run FLOSS on hw2.exe. What domain name is encoded within the file? (6 pts)

At this point, take a snapshot of your VM. Read the following questions, get any tools you want to use ready, and then run hw2.exe.

3) After the malware runs for about a minute, open the .pcap file of your FakeNet-NG session using Wireshark. Provide a screenshot of the DNS query that the malware made to the domain from question 2. (8 pts)

4)What is the source port from the DNS query? What is the destination port? Include a screenshot of both below in Wireshark, make sure the DNS query is included. (4pts)

5) The malware creates an established connection. What is the destination port of this connection? Describe how you found your answer. (8 pts)

6) What is the name of the process that hw2.exe creates? What is its PID? Provide a screenshot of this process being created in ProcMon (8 pts)

**Part 2: hw2\_2.exe (60 pts)**

Revert your VM to the snapshot you took after setting up FakeNet-NG in Part 1. Make sure that FakeNet-NG is still running. Read the following questions, get any tools you want to use ready, and then run hw2\_2.exe.

1) What is the full file path that hw2\_2.exe copies itself to? Show that this file is an exact copy of hw2\_2.exe. (6 pts)

2) hw2\_2.exe creates two DLL files when it is run. What are the full paths of these files? (4 pts)

a)

b)

3) Perform static analysis on the DLL file from question 2 whose MD5 hash begins with d1497574. Based on your analysis, what do you believe the purpose of this file is? Justify your answer. (10 pts)

4) Perform static analysis on the DLL file from question 2 whose MD5 hash begins with 5fb08aa8. Based on your analysis, what do you believe the purpose of this file is? Justify your answer. (10 pts)

5) How does the malware gain persistence? Which file is made persistent? (8 pts)

6) hw2\_2.exe creates a folder somewhere on the system. What is the full path of this folder? Provide a screenshot of procmon showing this folder’s creation. (8 pts)

Wait for a few minutes until hw2\_2.exe creates one or more child processes, then answer questions 7-8.

7) One of hw2\_2.exe’s child processes tries to query the contents of the directory from question 6. Provide a screenshot of this query in procmon. (6 pts)

8) One (or more) of the child processes of hw2\_2.exe loads a DLL that is not signed by Microsoft. What is the full path of this DLL file? (If you see multiple answers, just choose one – any will be accepted) How did you find this information? (8 pts)