**CMSC 691 Malware Analysis HW 2**

Name:

Assigned: 2/17/2025

Due: 2/26/2025 by 11:59pm

Download hw2.7z onto your analysis VM and extract it. 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>

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

Hint: Chapter 3 of the Practical Malware Analysis book is a great resource, and other parts of the book may be helpful as well!

**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 all of these steps, showing a successful ping command while FakeNet-NG is running. Make sure that your screenshot includes the **entire screen** of your VM, or you will not receive credit. (10 pts)

Screenshot:

2) Run FLOSS on hw2.exe. Investigate the strings that FLOSS was able to decode – one of them is a domain name. What is the domain name that appears in the decoded strings? (6 pts)

Once you have completed questions 1 and 2, **take a snapshot of your VM**. You will need to revert your VM back to this snapshot later, to restore your VM to a clean state. Read the rest of the questions in Part 1, get any tools you want to use ready, and then run hw2.exe. You should run hw2.exe from an **Administrator command prompt** so that it has the correct privileges.

3) After the malware runs for about a minute, start Wireshark and open the .pcap file created by your FakeNet-NG session. Search for the DNS query that the malware made to the domain from question 2. Provide a screenshot of this DNS query in WireShark below. Make sure that your screenshot includes the entire screen of your VM, or you will not receive credit. (8 pts)

Screenshot:

4) The malware creates an established connection. Run the netstat command in your VM’s command prompt to find it. (You will need to pass the correct flags to netstat, and be careful when reading its output – line wrapping may list information about a connection on multiple lines). What is the destination port of this connection? (8 pts)

5) 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 (by filtering on the Process Create operation). Make sure that your screenshot includes the entire screen of your VM, or you will not receive credit. (8 pts)

Name:

PID:

Screenshot:

**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. You should run hw2\_2.exe from an **Administrator command prompt** so that it has the correct privileges.

1) What is the full file path that hw2\_2.exe copies itself to? Give proof that this file is an exact copy of hw2\_2.exe. (8 pts)

File path:

Proof that the two files are identical:

2) hw2\_2.exe creates two DLL files when it is run. What are the full file paths of these DLLs? (6 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 using examples from both the strings and imports. (12 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 using examples from both the strings and imports. (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 your VM. It is tricky to find – we recommend using Regshot and scanning the full C:\ drive to help find it. What is the full path of this folder? Provide a screenshot of this folder’s creation in Regshot. Also, provide a screenshot of showing this folder’s creation in Process Monitor (Procmon) by filtering on the CreateFile operation. Make sure that your screenshots include the entire screen of your VM, or you will not receive credit. (8 pts)

Full path of folder:

Screenshot of Regshot:

Screenshot of Procmon:

7) Wait for a few minutes until hw2\_2.exe creates one or more child processes in Process Explorer. You may have to interact with the VM for the child process(es) to be created. 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, by filtering on the QueryDirectory operation. (8 pts)

Screenshot: