**CMSC 449 Spring 2023 Malware Analysis Midterm**

Name:

Assigned: Wednesday 3/29/2023

Due: Wednesday 4/5/2023 by 5:30pm

Do notdiscuss this midterm with other students; absolutely **NO** collaboration is allowed. You may use any of the resources and tools discussed in class to answer the questions. You may ask the TAs or me clarification questions.

Please provide supporting evidence for your answers. Even though not all questions ask for screenshots, you are always free to do so.

For this midterm you should to work on the Windows 7 version of the Flare VM to guarantee that the midterm malware is 100% functional. That VM can be downloaded from the course website. Download and extract the malware onto your Flare VM. The password to the zip file is “infected”. The zip file contains midterm.exe, which is a live malware sample.

Submit your completed exam as a DOCX file (not PDF) using Blackboard as usual.

**Part 1: Basic Static Analysis (30 pts)**

1) Is this midterm.exe packed? List 3 features of the file that indicate whether it is or is not packed. If the malware is packed, be sure to also include information about the type of packer used and how did you determine that (10 pts)

a)

b)

c)

What type of packer was used? How do you know?

2) Unpack midterm.exe. What command did you use to unpack it? What are the SHA-1 and MD5 hashes of the packed and unpacked files? (8 pts)   
MD5 of midterm.exe before unpacking: MD5 of midterm.exe after unpacking: SHA-1 of midterm.exe before unpacking: SHA-1 of midterm.exe after unpacking:

3) Investigate the strings of the unpacked midterm.exe. Select three strings you believe are suspicious. For each one, describe how you found it, and why you think it’s suspicious. (12 pts)

String 1) (2 points)

String 2) (2 points)

String 3) (2 points)

Based on your analysis, what type of malware is this, and what does it do? (6 points)

**Part 2: Basic Dynamic Analysis (30 pts)**

Follow the FakeNet-NG guide to configure the network settings of your Flare VM. You should only run the malware while your VM is not connected to the internet! Run midterm.exe and answer questions 4-6. You can run either the packed or unpacked version of the malware.

4) What port does midterm.exe listen on? How did you find this information? (6 pts)

The malware starts a telnet server which listens on the port you found in question 4. A malware actor can connect to this port remotely and interact with the malware. While midterm.exe is running, open a command prompt on your VM and run the following command:

nc 127.0.0.1 [port number from question 4]

5) Once you have run the nc command, type “?” to list the different commands that the midterm.exe can execute. (10 pts total)

What does this list of commands tell you about this malware? (2 pts)?   
  
Provide a screenshot of your command prompt window, showing the list of commands below (2pts):

Pick two of the commands to explore and describe in detail what they do.

Command 1:(3 points)

Command 2: (3 points)

6) The malware will install itself if provided with the “i” command. Using a dynamic analysis tool, investigate how the malware makes itself persistent. For the questions below, be specific and describe how you found this information. (10 pts total)

What is the malware sample’s persistence mechanism? (4 pts):

What is the path of the persistence mechanism that allows the malware to stay persistent [Hint: The path here is not a traditional directory path. It's something that is similar to a directory path] (3 pts)?

What is the full path of the file that is made persistent? (3 pts)

7) What category of malware do you believe midterm.exe belongs to now that you have completed the dynamic analysis? Make sure to justify your answer with the analysis you performed in the previous three questions. (4 pts)

**Part 3: Advanced Static Analysis (40 pts)**

Load the midterm.exe into IDA or Ghidra, then answer the following questions.

8) How many DLLs does the malware import from? How many functions does the malware import from ADVAPI32.DLL? (6 pts)

9) How many distinct functions call FUN\_401474? What is the purpose of FUN\_401474? (10 pts)

10) What is the purpose of FUN\_402180? (6 pts)

11) What is the malware doing from 0x401ca5 to 0x401ce6. Why might the malware be doing this? (10 pts)

12) Which function is responsible for granting the malware persistence? How did you find this information? (8 pts)