Assignment 2: Malware Analysis

Set: 16/04/2021, Due: 22/05/2021

Your assignment is on Malware Analysis, which is based on the Lectures and Previous labs. The assignment is an individual assignment and is worth 25% of the module marking. You will be assessed on your ability to carry out a successful memory forensics investigation and report the artifacts and malicious activities analysed.

Marks Breakdown

You will be given two memory samples of infected machines and task associated with each memory sample. You are required to submit a forensics investigation report on each of the memory sample. To help you with constructing your report, Task-1/Task-2 guide you to cover the main points that should be included in the report. Once you have completed the two tasks you need to submit one report that contain the results of your investigation in PDF format.

25 Mark For all tasks. Which is broken down into:

- **3 Mark:** For clarity of your description.
- **10 Mark:** For Task-1 question (breakdown below)
- **12 Mark:** For Task-2 question (breakdown below)

Submission Instructions

Please Submit your solution a report to this link `https://handin.ecs.soton.ac.uk`.

Deadline

The assignment deadline is on 22/5/2021

Experimental Setup

We will use the same setup of Lab-3 to work with Volatility and Analyse the memory samples below.

Download Lab-3 from `https://git.soton.ac.uk/comp6236/lab3`

1 Task-1

Task-1 is concerned the with memory sample shared with you in the malware analysis lab (memory.bin.7z). To download the memory image follow the following instructions:

```
wget https://sotonac-my.sharepoint.com/:u:/g/personal/aa1m20_soton_ac_uk/
    ↪ ES5CQfhJDJJLqgr6zdzAI40BXK364UAk-Y8o85z5ylk-0g?e=BfAUlS
sudo apt-get install p7zip
7za e memory.bin.7z
```

- What is the relevant profile to be used to analyse the provided memory image? (1 Mark)
- Can you identify a malicious DLL? Explain your findings. (1 Mark)
- What is the PID of the process that's hosting the DLL? (1 Mark)
- Dump the DLL to disk using either its name or base address. Compute the SHA1 of the dumped file. (1 Mark)
- Analyze the unpacked file with strings, peframe, or any other utilities at your disposal. What indicators of compromise can you find that might help you? (3 Marks)
- Is this malware likely to be involved with a particular botnet? (3 Marks)

2 Task-2

In this task you are provided with the memory sample mem2.7z. In this memory dump there is a "hidden process". Can you find it?

```
wget mhttps://sotonac-my.sharepoint.com/:u:/r/personal/aa1m20_soton_ac_uk/
    ↪ Documents/Courses/COMP6236/dkom.mem.7z?csf=1&web=1&e=8PBUdS
sudo apt-get install p7zip
7za e dkom.mem.7z
```

- What is the relevant profile to be used to analyse the provided memory image? (1 Mark)
- Which process is hidden? (2 Marks)
- What process hiding technique were used? (3 Marks)
- Is Volatility's psscan able to find the hidden process? (1 Mark)
- Dump the hidden process to disk. Who compiled the application and what tool was used? (2 Mark)
- What is the hidden process' thread doing? (3 Marks)