CSC 471 Spring 2022 Lab 4

Dr. Si Chen

Build a Dynamic Heuristic Analysis Tool for Detection of Unknown Malware

The goals of this lab:

- Understanding the concepts of the anti-virus system
- Understanding the concept of heuristic detection.

Objectives and Targets

In today's society virus makers have a large set of obfuscation tools to avoid classic signature detection used by antivirus software. Therefore there is a need to identify new and obfuscated viruses in a better way. One option is to look at the behavior of a program by executing the program in a virtual environment to determine if it is malicious or benign. This approach is called dynamic heuristic analysis.

In this lab, you are asked to develop a new heuristic dynamic analysis tool for detecting unknown ransomware.

Target 1: generate log file

Steps:

1). In a Windows XP environment. Download ransomware sample and a monitor program from our course website.

```
https://www.cs.wcupa.edu/schen/malware2022/download/ransomware.zip
```

2). Unzip the file with password, then create a new folder test under C: , copy all files to that folder.

3). Rename virus.exe_ to virus.exe 4). Double click and run Monitor.exe

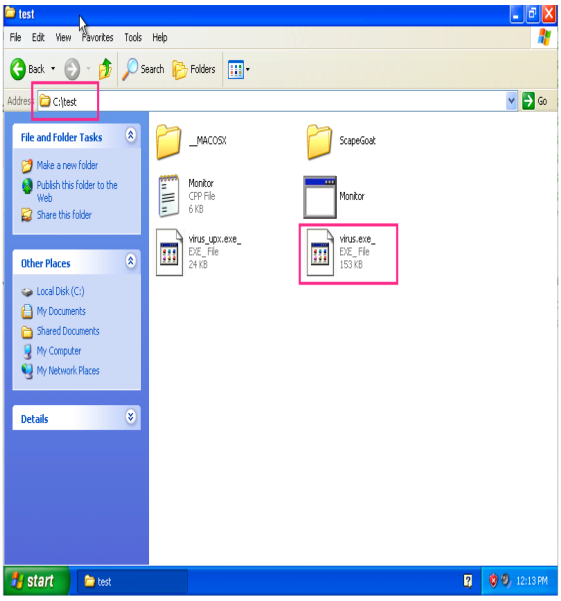

Figure 1: Step 2

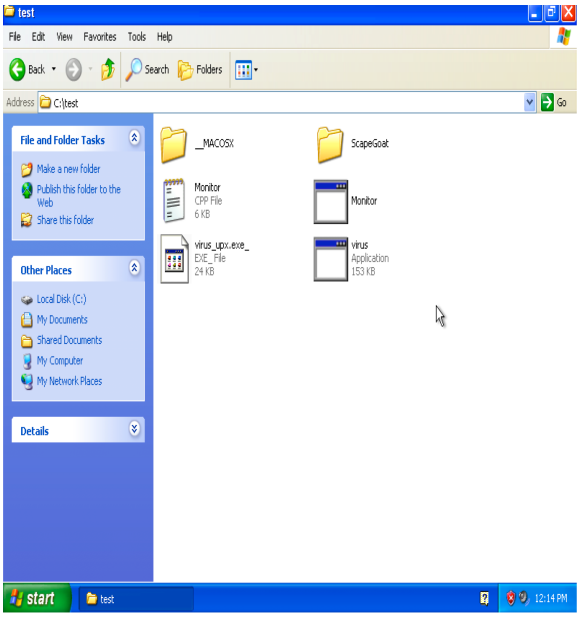

Figure 2: Step 3

5). Double click and run virus.exe

6). Close Monitor.exe

7). Open log.txt which contains the log data recorded by Monitor.exe. It should record all the activities that happened in this folder.

Target 2: Analysis Log file and implement heuristic rules

8). Please create a runnable program on BadgerCTF (recommend using Python on BadgerCTF). This program should be able to read the log.txt file and detect if these logged activities are malicious or not based on the following rules:

1. More than three word documents (docx) in ScapeGoat folder have been renamed.
2. More than 3 files in ScapeGoat folder have been modified.
3. The number of file self-deletes(a file been created and then deleted) activity is larger than or equal to 1.

A program is malicious ransomware if and only if it violates all three rules. And your program should then output:

```
malware detected - HEUR:Trojan- Ransom.DocxEncrypt.Generic
```

Deliverables: 1). A detailed project report in PDF format to describe what you have done, including screenshots and code snippets.

2). DO NOT upload malware sample to D2L.

More...

Please check lecture video

Submission

- The lab due date is available on our course website. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.
- Your submission should include: A **detailed project report in PDF format** to describe what you have done, including screenshots and code snippets.
- **No copy or cheating is tolerated**. If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.