Malware Reverse Engineering – HW1

NOTE:

- **Download the malware sample inside the Windows XP VM. You can download the image file of the Windows XP VM from: https://clemson.box.com/s/5imn4ykyam1v6r7bi7fx4hwjsziy07yg**
- **NEVER on your host machine.**
- **The download link of the malware samples used in Assignment 1 is https://clemson.box.com/s/tgm0msx0uw1upsmm9wsk5yhk6qkjygpx**

Problem 1 – static analysis (30 pts):

Lab 1-4 (page 28) in the textbook. The name of the malware sample is Assignment1-1.malware.

Problem 2 – static analysis (15 pts):

Perform basic static analysis on the given malware (Assignment1-2.malware) and then answer the following questions:

1. What is the md5sum? What of interest does VirusTotal Report?
2. List a few imports or sets of imports and describe how the malware might use them.
3. What are a few strings that stick out to you and why?

Problem 3 – reading assignment (10 pts):

Read the article in the following link for the general techniques used by malware to detect virtual environment, and the countermeasures.
https://resources.infosecinstitute.com/how-malware-detects-virtualized-environment-and-its-countermeasures-an-overview/#gref

Problem 4 – dynamic analysis (45 pts):

Perform basic dynamic analysis on the malware of Problem 2 (Assignment1-2.malware) and then answer the following questions:

1. What happens when you run this malware? Is it what you expected and why?
2. Name a procmon filter and why you used it.
3. Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?
4. Are there any network-based signatures? (URLs, packet contents. etc) If so, what are they?
5. Is there anything that impeded your analysis? How so? How might you overcome this?
6. What do you think is the purpose of this malware?