Case Western Reserve University

Department of Computer and Data Sciences

EECS 349&444: Computer Security

Assignment Date:	10/08/2019
Due Date:	10/12/2019 @ 9:00pm
First Name:	
Last Name:	
Google Drive Link:	
Abstract of the feedback:	

* This is the first question of HW2 which contains 20 points. You are asked to finish individually. Any submitted work that it copied from any source or too similar to be an independent write-up will not be given credit. Please follow the instruction below for your submission (due 10/12@9pm).

Mimic You: Malware

Problem 1 (20 pts). Please follow the instructions below for implementation. Please submit your code and description of your solutions in GitHub and only post your GitHub link in Canvas.

HW2-Q1: Mimic You – Malware!

- **Step 1:** Write a program using c programming language to implement the following functions and produce a binary named PE-Import.exe.
  - Check if "PE-1.txt" exists in the root directory;
  - If not, then create "PE-1.txt" in the root directory and write "I want to learn PE file format!" in the file.
  - If yes, check whether the file contains the string of "I want to learn PE file format!": if the string exists in that file, print the content in the file to Stdout; if not, append the string in the file.
- **Step 2:** Use PE edit tool (e.g., Exeinfo PE: http://exeinfo.atwebpages.com/) to check the content in the Import Table for your program PE-Import.exe.

HW2-Q1: Original PE vs. Packed PE (Cont.)

- **Step 3.1:** Use UPX to pack the PE-Import.exe.

Ultimate Packer for eXecutables

- **Step 3.2:** Use PE edit tool (e.g., Exeinfo PE: http://exeinfo.atwebpages.com/) to check the content in the Import Tables for the packed PE-Import.exe.
- **Step 3.3:** Use UPX to unpack PE-Import.exe; then use PE edit tool to check the content in the Import Tables for the unpacked PE-Import.exe.

HW2-Q1: Applying Techniques to Produce FNs (Cont.)

- **Step 4:** Given PE-Import.exe (*B1*), *please adopt the technique(s) introduced in class (e.g., packing, encryption, obfuscation, etc.) to fool the anti-malware scanner(s)' detection.*

  https://www.virustotal.com/gui/file/5d3663691080248b563a943b240732f50bc9fb1702c326eb6461bae066c45f9e/detection

Due: (20pts) 10/12/2019 at 9:00pm.