CSCD Cohort 6 – Project – Malware Analysis

(Optional and can be performed individually or in groups)

Deliverable: Report Due Date: 15th Jan 2022

Instructions: This homework requires you to run cuckoo on files that are marked as malware and those marked as benign applications. Inspect the reports generated by cuckoo on each individual malware and then answer the questions in a typed (using MS word or latex) form, generate a pdf file and upload it on Talentsprint Portal.

Download the zip file from Git-Link and extract the two directories – Malware and Benign. Submit each file individually to cuckoo sandbox that you have installed on your host – and get all the reports at the appropriate directory.

In case if participants are unable to setup Cuckoo and generate reports. I may share the JSON reports to answer the questions. It is recommended that you must use Cuckoo to generate reports. Please make a request if you need JSON reports.

Before you do the experiments, ensure that you followed all the instructions for installation of cuckoo sandbox VM – and it is configured with host only networking. Otherwise, the malware you analyze by affect your machine while being executed in the guest VM.

Once you have all the reports – answer the following questions by analyzing the reports manually.

1. **[10 points]** From the reports on the malware – do you see one or more malware trying to detect that it is being executed on a virtual machine? What are the indications you are finding – which makes you believe it (they) is (are) trying to detect whether it is running on a VM?

2. **[5 points]** Count the number of files created by each malware and add them up as count1. Count the number of files created by the benign applications, and add them up as count 2? Do you see any marked difference between count1 and count2? Explain.

3. **[5 points]** Count the number of files delete by each malware and add them up as count3. Count the number of files created by the benign applications, and add them up as count 4? Do you see any marked difference between count3 and count 4? Explain.

4. **[5 points]** Count the number of files written to by each malware and add them up as count5. Count the number of files written to by the benign applications, and add them up as count 6? Do you see any marked difference? Explain.

5. **[5 points]** Which category of files (malware or benign) are creating more directories?

6. **[5 points]** While category of files (malware or benign) opened more registry keys?

7. **[5 points]** Are any of the files trying to resolve any URL names to IP addresses? If so, which category (malware or benign) are they?

8. **[10 points]** Which category of files on average imported more DLLs? What APIs are being imported and exported (make two lists – one combined list for all DLLs and imported functions by malware files, and another combined list of all DLLs and imported functions by benign files)? Make some observations on the differences between the two lists.