Module D1: Sandboxing and other techniques for the safe execution/opening of files of unknown origin and/or functionality.

# SANDBOXING

**Lab Description:** The objective of this lab is see the effects of your analysis instruments on the sandbox and to minimize the effects of these instruments.

**Lab Environment:** This is intended to be an interactive lab with the instructor providing guidance to extend student demonstrations of very basic SRE skills. The exercise should be run in a protected environment as it may deal with malware. It can be run in the SRE class virtual environment.

**LAB EXERCISE/STEP 1**

The instructor needs to clearly express the following warning:

WARNING: The binary can be found in your VM, but can also be downloaded from https://nullify.cc/binary.exe NOTE: this is not a benign binary, and may trigger Anti-Virus or other similar security tools. DO NOT EXECUTE THIS BINARY ON ANY SYSTEM. The safest approach is to examine this within the environment you have been provided.

**LAB EXERCISE/STEP 2**

# Exercise:

1. In your SysInternals folder, launch, and then close procexp.exe and procmon.exe
2. Launch and then close IDA Pro
3. Launch and then close Immunity Debugger
4. Now take a snapshot of the Windows registry using regshot
   * Launch regshot
   * Choose the HTML document format
   * Choose 1st shot (no need to save)

(You have now captured the state of the registry prior to infection.)

1. Open a new program (can be a malware sample, or can be something benign, like Microsoft Word or a browser)
2. Launch procexp.exe to see a list of processes running on the Windows system
3. Launch procmon.exe to see a list of events taking place on the system. (procmon will generate a lot of noise so we will build a filter to focus on just the events generated by our malware)

* Open the filter dialog (Ctrl-L)
* Use the editing tools at the top of the dialog to create a filter that to show results from your chosen process
* Click the Add button, then click OK.

# What to submit

Instructor Notes: This example includes dynamic analysis of malware.

For this reason, this is intended to be an in-class exercise with the instructor and students working on the assignment in parallel to ensure that the learning objectives for this module are met (rather than measuring a student’s ability to search the web.)

**Options –**

Instructors can require students to answer the following questions (or similar) to demonstrate that they have met the objectives:

1. What is the purpose of opening and closing tools without performing any additional actions with the tools?