Module - 08

**Automated sandboxes**

# Sandboxes

**Lab Description:** This lab will present three samples; each sample will have at least one question to answer.

**Lab Environment:** Use of variety of tools is encouraged for this lab but not needed. Do not execute any of these files or go to any of the links. It is recommended to do this lab in a virtualized environment. Some tools that can be used are: VirusTotal, Malwr, Cuckoo, JSDetox, or other sandboxes.

**Lab Files that are Needed:**

samples.zip – includes the samples to be analyzed. The password to unzip this file is “infected”.

### **Lab Exercise 1:**

*Learning Outcomes 1 & 3*

Analyze Sample “f55663305088f33b013c5a86bc9520a6” and answer the following questions. Answer and explanations should be included with each answer:

1. What is the Detection rate?
2. What is the first submission date?
3. What is the original name of this sample?
4. What is the entry point for this sample?
5. What is the SHA-256 hash?

**LAB EXERCISE 2:**

*Learning Outcomes 1, 2, & 3*

Analyze the following URL’s and answer the questions with each. Screenshots and explanations should be included with each answer if possible:

* http://bigdiscountsonline.info/
* http://otticaduepuntozero.it
* http://rankedcaut.ru
* http://www.ritmicapiemonte.it/

1. What was the Detection rate on Virus total?
2. Do any of these results surprise you?

**LAB EXERCISE 3:**

*Learning Outcomes 1, 2, & 3*

Analyze Sample “69f27b07404cf9c51dd2d2e40fca4d65” and answer the following questions. Screenshots and explanations should be included with each answer:

1. In your previous lab, you told me if this sample was packed or obfuscated. Using a sandbox, find information to support your choice or reverse it.
2. Did your answer changed from last time? If so, why did it change?

## What to submit

Submissions should be neatly organized. Each question should include at least one screenshot and a brief explanation if possible.