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, it is recommended to do this lab in a virtualized environment. Some tools that can be used are: VirusTotal, Malwr, Cuckoo, JSDetox, or other custom setups.

**Lab Files that are Needed:**

Sample\_08.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. Screenshots and explanations should be included with each answer:

1. What is the Detection rate? – **46/65**
2. What is the first submission date? - **2015-08-19**
3. What is the original name of this sample? - **Totalcmd-Admin**
4. What is the entry point for this sample? **0x67cd**
5. What is the SHA-256 hash? – **4dbaf54f29e432a16ab267b388c6a9cabd002549c8309e52974dae004794a0db**

**May change with time**

**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?

**Big – 0/68**

**Ritmi – 2/65**

**Rankedcaut – 3/64**

**Ottica – 2/64**

1. Do any of these results surprise you?

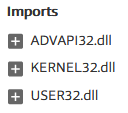
**Opinion based question. Needs to be well thought out and have evidence to support the answer.**

**LAB EXERCISE 3:**

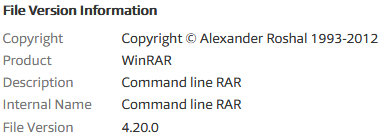
*Learning Outcomes 1, 2, & 3*

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.



**Low amount of imports is an indicator of it being packed.**



**RAR is a file extractor**

**Few imports, has a file extractor as file type**

**Most likely obfuscated in some way may not be packed.**

1. Did your answer change from last time? If so why, did it change? – **Depends on student logic**

## What to submit

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