Module - 07

**Detecting packing and obfuscation**

# detecting packing and obfuscation

**Lab Description:** The goal of this lab is to analyze executable files in the PE file format to detect packing and code obfuscation techniques. Perform analysis on the following samples, ensure that for each question you provide detailed information supporting your conclusion. This may include screenshots, description of your analysis, sections, imports and strings.

**Lab Environment:** This lab contains malware and should be analyzed in a safe lab environment. If unsure how-to setup a safe lab environment, refer to lesson 01. The following tools will aid in your analysis:

* PE Studio
* Strings utility
* IDA Pro (free or demo)

**Lab Files that are Needed:**

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

### **Lab Exercise 1:**

Analyze Sample “63d3fbc397585a45b01b456aab953abb” and answer the following questions. Screenshots and explanations should be included with each answer:

1. Based off just the imports, what can you tell about the sample?
2. What does dumping strings tell you about the sample?
3. What do you notice about the sections table?
4. Is this sample packed or obfuscated? What led to this conclusion?

**LAB EXERCISE 2:**

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

1. Based off just the imports, what can you tell about the sample?
2. What does dumping strings tell you about the sample?
3. How does the sections table differ from the first sample?
4. Is this sample packed or obfuscated? What led to this conclusion?

**LAB EXERCISE 3:**

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

1. Is this program packed or obfuscated? What can you tell about it?

## What to submit

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