LABS

**Lab 7-1**

Analyze the malware found in the file ***Lab07-01.exe*.**

Questions

1. How does this program ensure that it continues running (achieves persistence) when computer is restarted?
2. Why does the program use a mutex?
3. What is a good host-based signature to use for detecting this program?
4. What is a good network-based signature for detecting this malware?
5. What is the purpose of this program?
6. When will this program finish executing?

**Lab 7-2**

Analyze the malware found in the file ***Lab07-01.exe*.**

Questions

1. How does this program achieve persistence?
2. What is the purpose of this program?
3. When will the program finish executing?

**Lab 7-3**

Analyze the malware found in the file ***Lab07-03.exe*.**

**Lab 7-1 Solutions**

**Short Answers**

**Lab 7-2 Solutions**

**Short Answers**

1. This program only executes once. It does not persistence.
2. This program displays a webpage to the user.
3. Program exits after displaying the webpage.

Detailed Analysis

**Lab 7-3 Solutions**

**Short Answers**