CMPSC 443 Lab 8: Dynamic Analysis

# Lab Description

Note: you are supposed to use a Windows VM to finish all these labs

**Part I: basic dynamic analysis**

## Task 1

Analyze the malware found in the file *Lab06-04.exe*. You need to use ApateDNS to setup a DNS server that directs all DNS request to the local IP. Meanwhile, you may use python simplehttpserver (the command is “python –m SimpleHTTPServer 80”) to launch a web server that handles any HTTP request from the malware.

You need to explore the malware behavior based on the prior setup. Please provide a detailed paragraph of malware actions with screenshots for submission.

**Part II: advanced dynamic analysis**

## Task 2:

Analyze the malware found in the file *Lab09-01.exe* using OllyDbg and IDA Pro to answer the following questions.

1. How can you get this malware to install itself?

2. What are the command-line options for this program? What is the password requirement?

3. What are the host-based indicators of this malware?

4. What are the different actions this malware can be instructed to take via the network?

5. Are there any useful network-based signatures for this malware?

# Submission

|  |
| --- |
| * Please write a report to answer all questions. * Screenshots needed for task 1. |