Computer Science for Future Presidents

Tufts University

Fall 2020

Assignment 8: Malware

Lab Assignment

Due: 11 pm EST November 11

## Lab Objectives:

1. Analyze real malware; and
2. Understand basic techniques of malware writers.

## Part 1: Malware Sample, PCAP

In Lab 3, you used Wireshark and learned how to analyze network traffic via PCAP files. For this part, you are given a PCAP to analyze, this time, malicious traffic. Download malware.pcap from the course website at <https://www.cs.tufts.edu/comp/12/lab8/malware.pcap>. Answer the following questions:

1. Scan the PCAP file at VirusTotal (<https://www.virustotal.com>). VirusTotal is an online service providing malware analysis of files and URLs (read “How It Works” on their website). What is the malware detection ratio?
2. Using Wireshark, open up the PCAP file for analysis. List malicious IP addresses and domains found in this PCAP.
3. List the suspicious filenames that are associated with this malware.
4. Reconstruct the conversations via right-clicking on a packet and select “Follow TCP stream”. Do you notice anything peculiar in any of the conversations? Please describe.
5. What is the intent and purpose of this malware? Better yet, what is this piece of malware better known as? Briefly describe how you came to your conclusion. List resources that you used.

## Part 2: Malware Sample, Binary

For this part, you are given a piece of software to analyze. Download <https://www.cs.tufts.edu/comp/12/lab8/sample.zip>, and unzip to get the actual piece of malware. Answer the following questions:

1. For which computing platform is this malware built?
2. Upload the malware to VirusTotal for analysis. What is the detection ratio of this malware?
3. List all the suspicious URLs and domains that this malware uses.
4. Provide a brief synopsis of what you think this malware really does. Show all evidence including any references. Citing appropriately is important; please remember to do so.
5. Is this computing platform prone to malware? How can a user of this computing platform prevent or mitigate against the threat of malware?