ITSC 303

Malware Analysis

Final Project - Weekly Report 3

D’Artagnan Boocock & Coleton Sanheim

01/04/2022

**Sample Selection**

We have chosen to analyze the two following samples:

1. Lab19-03.pdf



1. Lab10-01.exe



Sample #1 caught our attention because the sample is a pdf file. Upon first inspection the file could either be an exploited pdf file or some form of trojan payload making use of a pdf template to create a parallel thread.

Sample #2 was selected because the sample has an icon which means the file is either a mask or another trojan.

We believe it will prove useful to compare the two samples during the analysis process.

**Handling Procedure**

The self-extracting archive will be downloaded from:

<https://github.com/mikesiko/PracticalMalwareAnalysis-Labs/blob/master/PracticalMalwareAnalysis-Labs.7z>

This 7-zip file can be handled safely as the samples contained within require execution to detonate. We will download the archive to the primary Win7 machine (10.0.2.12). The analysis machine can be temporarily connected to the internet and the zip will be downloaded directly.

Once the 7-zip file is on each machine an exe (self-extracting archive) can be extracted. The exe will be run and directed to extract to a folder called “Final” on the Desktop of the respective machines.

Graphical user interface, application, Word

Description automatically generated

The samples can be found in .\Practical Malware Analysis Labs\BinaryCollection\Chapter\_10L and .\Practical Malware Analysis Labs\BinaryCollection\Chapter\_19L respectively. These will be copied to the C:\Users\SAIT\_ITSC303\Desktop\Final folder for the rest of the analysis process.