ITSC 303

Malware Analysis

Final Project - Weekly Report 1

D’Artagnan Boocock & Coleton Sanheim

25/03/2022

**Sample Selection**

We have chosen to use the malware samples provided in the Practical Malware Analysis textbook. These files are available at <https://github.com/mikesiko/PracticalMalwareAnalysis-Labs>

This GitHub page contains two 7zip files. One of which (PracticalMalwareAnalysis-Labs.7z) is a self-extracting archive while the other (PracticalMalwareAnalysis-Labs-Windows7.7z) contains two windows binaries. For the time being these files will remain zipped on the analysis machine until we are prepared to begin the static analysis phase.

**Lab configuration**

We have chosen to configure our lab environment such that shared clipboard as well as drag-and-drop are disabled on all the virtual machines. Samples will be handled in password-protected archives and will be transferred to target machines via a local webserver (hosted on the sniffing machine) as necessary. This step will ensure shared-folder exploits are avoided entirely. The Three vulnerable machines have been snapshotted in their current (healthy) state prior to beginning our analysis.

**Virtual Environment**

We have chosen to use VirtualBox to simulate our virtual environments because it has sufficient security functionality for malware analysis and is highly user-friendly. Notably, the two of us have roughly one year of experience with this virtual environment.

**Host Machine**

The host machine we will be using has an 8 core (16 thread) processor with 32GB of RAM. The host machine has been backed-up and a restore point has been saved just as a precaution.

**Network Topology**

All our virtual machines except for the analysis machine are configured in a NAT network on the 10.0.2.x/24 subnet off the host machine. The analysis machine will be isolated from the NAT Network to avoid any possible interference with the analysis machine once we begin the dynamic analysis.

2 Windows 7 Victim machines:

1. This machine uses a single processor with 4GB of RAM and will be used for dynamic analysis. IP address: 10.0.2.12 with internet connection
2. This machine uses a single processor with 4GB of RAM and will be used to check for malware propagation during the dynamic analysis stage. IP address: 10.0.2.11 with internet connection

1 sniffer machine (Kali), configured with 1 processor and 4GB of RAM. It has been given IP address: 10.0.2.4 with internet connection

1 analysis machine (Win7). This machine will have 2 processors and 4GB of RAM. It will be used to perform all static analysis during this project. This machine will use the NAT network to receive the file and then the network adapter will be disabled once the transfer is complete. It currently has IP address: 10.0.2.9