Lab 02 Basic Analysis

This lab will have you working through some basic static and dynamic analysis on malware samples. By the end of the lab, you will have found evidence to guide a more thorough analysis of the binaries.

Lab Files

The malware samples are contained within password-protected zip archives with the password: **infected**

Please ensure you are handling the malicious files appropriately. File hashes of the lab samples are:

- MD5 (sample01.exe) = e210880ff042f6a94f333f9b99d4b23e

Lab Instructions

Complete the following tasks in your analysis environment or using the IA lab. All work should be original, discovered, and reported on by you. Do not rely upon a single source of information (i.e., an online sandbox) to answer all questions. Use the tools and utilities available on your VM in conjunction with such sources.

sample01

There are two main portions of analysis for this sample. On your Windows VM, perform some basic static and dynamic analysis to answer the following questions.

Static Analysis

1. What file type of file is sample01? Be specific (e.g., a PE file can be a .exe, .dll, or .sys).

2. Is the file packed? If it is, identify the packer and try to unpack it before moving on. If it's not packed, provide some evidence of how you know.

3. Find interesting strings in the binary (IPs, URLs, API calls, imports, etc.).

4. Look at the imports of the binary. Gather interesting functions and a brief description of what they do.

5. Use the MD5 hash of the file to determine if the file appears to be malicious. If so, determine what is it (e.g, trojan, C2, or a specific malware family)?

© MichaelHam

Dynamic Analysis

It is strongly recommended to take snapshots of your VMs before running the binary. This file should be *safe*, but it's a great habit to get into!

1. Use Regshot to take a snapshot of your VMs registry before running the binary.

2. Start Process Monitor, Process Explorer, and Wireshark.
    a. Watch Process Explorer to see the process ID (PID) of the sample.
    b. When you see the PID, add that as a Parent PID filter in Process Monitor. This should filter all events except those stemming from the binary.

3. Run the binary, interact with it, and let the monitoring tools collect some data.

4. Stop all of the monitoring tools when you're done, and take a second registry snapshot with Regshot to see what changed.

5. Based on your overall analysis, come up with a brief summary of what this binary does. Comment on whether or not it appears to be malicious and how it changes the machine (adds registry keys, drops files, etc.). What would the risk or impact be to a user that ran the binary based on what you found?

© Michael Ham