Malware Discovery and Basic Analysis

Course Description:

Malware Discovery and Malware Analysis is an essential skill for today's Information Security, Security Operations Center (SOC), and IT professionals. This course is perfect for people wanting to improve and get faster at Incident Response.

This course focuses on performing fast triage and how to discover if a system has malware, how to build a malware analysis lab and perform basic malware analysis quickly. The goal and objective to apply the results to Malware Management with actionable information to improve your Information Security program. Tools and techniques used and steps to analyze malware to determine if a system is clean or truly infected will be covered. The concept of Malware Management, Malware Discovery and Basic Malware Analysis will be discussed with exercises linking the three concepts together.

This course is intended to expose and improve attendee's ability to quickly evaluate a system for everyday commodity malware that you might get in email phishing or surfing to advanced targeted malware. The focus will be on Windows systems; but will touch on some tools for Apple and Linux systems as well.

All attendees will get a copy of ***LOG-MD Professional*** as part of the class.

Day 1

- Introductions, Goals & Objectives and Terms & Concepts
- Malware Management & Labs
- Lunch
- Malware Discovery & Labs
- Types of Analysis and Malware Analysis flows
- Malware Analysis Data Labs
- Questions and Discussion

Day 2

- Complete Building a Malware Analysis Lab
- Malware Analysis Introduction
- Malware Analysis Tools
- Lunch
- Automated Analysis & Lab
- Basic Malware Analysis & Lab
- Logging for Malware
- Questions and Discussion

Requirements:

1. Barebones laptop is recommended with re-imaging after the course OR
2. Laptop running a Virtual Machine (VirtualBox, VMWare, ESXi, Parallels, etc.)
3. Windows 7, 8 or 10
4. Microsoft Office, PDF Reader (FoxIt), Notepad++ & 7Zip
5. A list of tools (Except Office) will be provided on USB Card on the day of the training
6. Malware samples will be provided

- ***WARNING***: Real Malware samples will be used in the labs. Even though the malware samples used are well understood and can be disabled and remediated, it is still real malware and it is highly recommended the systems used be re-image upon completion of the course.