**First Malware Analysis Course**

# Objective

A one-day course focused around rapid triage of malicious content and next steps. These steps can be taken by a small team when targeted by specific malware. After completion of this process you can hand off to your AV vendor with a summary of your findings and links to any reports that you have generated. The aim is to complete this process in about 30 minutes, have a definite answer whether something is malware or not, and give the AV vendor enough to go on as a starting point.

# Learning objectives

After this course, you will be able to

* Understand and strategies the use of malware analysis tools
* Understand aspects of the cybercrime ecosystem and the role played by malware
* Be able to model attacks and think strategically about defenses
* Be able to analyze malware to a high level quickly and securely
* Be able to share your conclusions with others

# Timings

The total duration of the course is 450 minutes (7.5 hours)

|  |  |  |
| --- | --- | --- |
| **Module** | **Title** | **Duration** |
| 1 | The malware ecosystem | 120 minutes |
| 2 | Analyzing malware artefacts | 240 minutes |
| 3 | Sharing artefact information | 90 minutes |

# Content

## Module 1: The malware ecosystem

The first module focuses on the threat landscape and how it changes. It discusses the types of malware and how they fit into the criminal ecosystem. This module also contains a discussion of attack modelling, following the MITRE model, discusses the kill chain, and finishes with an overview of techniques attackers use to compromise platforms.

Overview

* The threat landscape and how it changes
  + What is a threat landscape
  + How does it change
  + How to become aware of these changes
* Overview of compromise techniques
  + Malicious download
  + Downloaders through scripts
  + Malicious documents
* Discuss models for cyberattack and what they mean for defense

## Module 2: Analyzing Malware Artefacts

The second module focuses on the practical aspects of analyzing malicious artefacts. The focus is on getting the right combination of accuracy and speed. During practical attacks it is quite often to answer the question ‘is this malicious’ with a high degree of accuracy without going into the details. This module will cover how to quickly and reliably analyze artefacts of which you assume they are malicious.

The focus will be on a number of tools that will assist in answering these questions quickly

1. Automated sandboxing
2. Packers and packing
3. Dynamic analysis / reverse engineering, packet analysis
4. Volatiliy
5. Yara signatures

Overview

* Rapid triage of suspicious artefacts
* Malicious document analysis
* Current techniques used by malware
* Use of electronic sandboxes
  + Virustotal
  + Hybrid Analysis
  + Malwr
* On-host analysis tools
  + Yara
  + Volatility
* Analysis of reports

## Module 3: Sharing Artefact information

In this module we discuss how you can share the findings of a brief investigation to best effect.

Overview

* Malware families and categorization
* Relationships to the AV market
* TLP and IEP sharing
* Threat intelligence sharing formats
  + MISP
  + STIX / TAXII
* IBM Xforce for malware research

# Example Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Component** | **Duration** | **Cumulative** |
| 8:30-9:30 | Module 1: Theory | 60 minutes | 60 minutes |
| 9:30 - 10.00 | Module 1: Incident Lab | 30 minutes | 90 minutes |
| 10:00-10:30 | Module 1: Environment Demo / Lab | 30 minutes | 120 minutes |
| 10:30-11:00 | BREAK |  |  |
| 11:00-12:00 | Module 2: Theory 2.0 and 2.1, Lab | 60 minutes | 180 minutes |
| 12:00-13:00 | LUNCH |  |  |
| 13:00-14:00 | Module 2: Theory 2.2, Lab 2.2 | 60 minutes | 240 minutes |
| 14:00-14:30 | Module 2: Theory 2.3, Lab 2.3 | 30 minutes | 270 minutes |
| 14:30-15:00 | BREAK |  |  |
| 15:00-16:00 | Module 2: Theory 2.4, Lab 2.4 | 60 minutes | 330 minutes |
| 16:00-16:30 | Module 2: Theory 2.5, Lab 2.5 | 30 minutes | 360 minutes |
| 16:30-17:30 | Module 3: Theory, Demos, final discussion | 60 minutes | 420 minutes |