FireEye Cyber Defense Summit 2017

Malware Analysis Crash Course (2 days)

This course provides a rapid introduction to the tools and methodologies used to perform malware analysis on executables found on Windows systems using a practical, hands-on approach. Students will learn how to find the functionality of a program by analyzing disassembly and by watching how it modifies a system and its resources as it runs in a debugger. Students will learn how to extract host and network-based indicators from a malicious program. Students will be taught about dynamic analysis and the Windows APIs most often used by malware authors. Each section is filled with in-class demonstrations and hands-on labs with real malware where the students practice what they have learned.

What You Will Learn

- Hands-on malware dissection
- How to create a safe malware analysis environment
- How to quickly extract network and host-based indicators
- How to perform dynamic analysis using system monitoring utilities to capture the file system, registry, and network activity generated by malware
- How to debug malware and modify control flow and logic of software
- To analyze assembly code after a crash course in the Intel x86 assembly language
- Windows internals and APIs
- How to use key analysis tools like IDA Pro and OllyDbg
- What to look for when analyzing a piece of malware
- The art of malware analysis - not just running tools

Modules Included

- Basic Static Analysis – Learn to quickly perform a malware autopsy using a variety of techniques and tools without running the malware.
- Basic Dynamic Analysis – Learn to analyze running malware by observing file system changes, function calls, network communications and other indicators.
- Disassembly – Learn the basics and build a foundation of the x86 assembly language, recognize code constructs in the disassembly and learn how to use IDA Pro THE tool for disassembly analysis.
- Windows Internals – Learn a wide range of Windows-specific concepts that are relevant to analyzing Windows malware. The module covers fundamentals of Windows architecture, Windows API functions and common programming patterns used by malware to communicate, establish persistence, modify file system and registry.
- Debugging – Learn how debuggers work and how they can be used to monitor and change malware behavior, as it runs, at a low level.

Who Should Attend

This course is intended for software developers, information security professionals, incident responders, computer security researchers, puzzle lovers, corporate investigators, or others requiring an understanding of how malware works and the steps and processes involved in performing malware analysis.

FireEye Cyber Defense Summit 2017

Course Prerequisites

- Students must have excellent knowledge of computer and operating system fundamentals; computer programming fundamentals and Windows Internals experience is highly recommended.

What Students Should Bring

- Students must bring their own laptop computer with VMware Workstation 10+ or VMWare Fusion 7+ installed. Laptops should have at least 30GB of free space.
- A licensed copy of IDA Pro is highly recommended to participate in ALL labs, but the free version can be used in most cases.

What Students Will Be Provided With

- A student manual.
- Class handouts.
- FireEye/Mandiant gear.