Almost every Incident Response requires analysis of attacker malware such as trojans, back doors, or rootkits. Incident Responders must be able to perform rapid analysis on malware encountered to determine the purpose of the malicious code. During malware analysis, the analyst must determine how it operates, what functionality is built in and what attacker controlled domains or Internet Protocol (IP) addresses it communicates with. Failing to understand the malware functionality threatens all remediation efforts. This course developed and taught by MANDIANT malware analysts, provides an introduction to the tools and methodologies used to perform dynamic and static analysis on portable executable programs found on Windows systems.

Duration 2 days

Who Should Attend Information technology staff, information security staff, corporate investigators or others requiring an understanding of how malware functions and the steps and processes involved in Malware Analysis.

Prerequisites General knowledge of computer and operating system fundamentals is required. Some exposure to software development and experience in assembly and C programming languages is recommended.

Students Will Learn
- The primary types of malware
- How to create a safe malware analysis environment
- Malware analysis shortcuts
- The malware analysis and reporting process
- Legal issues involving malware analysis and reverse engineering
- Methodology differences between static and dynamic analysis
- Binary, decimal, hexadecimal conversion
- Code, compilers and compilation
- The tools used to identify obfuscation methods and the tools used by analysts to recover the “hidden” or obfuscated data
- The fundamentals of assembly language programming
- How to perform dynamic analysis with virtual machines and monitoring tools to capture system, registry and network activity generated during malware analysis

Exercises & Labs
- Dynamic and static analysis of unknown binary
- Real-world intrusion case study including analysis of the actual malware found in the case
- Using VMware to create a safe analysis environment
- Binary creation and analysis
- Converting numbers between base systems

Course Materials
- Student manual
- Class handouts
- Course certificate
- MANDIANT gear

Suggested Next Courses
- MANDIANT Intermediate Malware Analysis
- MANDIANT Advanced Malware Analysis
- MANDIANT Enterprise Incident Response

Contact 1.800.647.7020
education@mandiant.com
www.mandiant.com/education.htm
**Case Study**

Instructors will provide an in-depth review of an actual intrusion case that involved the use of multiple pieces of malware. Discussion will focus on four of the malicious binaries that were discovered, how they were discovered, how they contributed to the overall intrusion and the results of their analysis.

**Introduction to Malware**

Students will learn about basic malware analysis methodology and gain hands-on experience with tools commonly used in malware analysis. Students will also learn the importance of and how to create a “safe” environment for the purpose of analyzing malware.

**Introduction to Programming Concepts: C, Assembly (x86), & Windows**

Students will learn about the C and assembly programming languages and explore the basic looping processes, how mathematical functions are performed, how x86 processors handle assembly instructions and memory.

**Numbering Systems: Bits and Bytes**

Students will learn about the binary, decimal and hexadecimal numbering systems and how to convert numbers between each system. Students will also learn about little/big endian bit ordering, signed and unsigned numbers and floating point and character sets.

**Basic Malware Analysis Tools**

Students will learn about a variety of tools that can be used to facilitate analysis of commonly used malware. Students will also learn about MD5 checksums, how to generate them and their use to identify known malware. Instructors will demonstrate “shortcuts” to give the malware analyst a “head-start” in the analysis process.

**Class Exercises**

Students will create sample C programs to better understand how malware authors create binary executable programs. Students will explore various analysis tools to perform analysis functions throughout the course.

In the final exercise, students will use all of the tools and techniques presented to determine the functionality and purpose of a suspicious file found on a compromised system.