REVERSE ENGINEERING MALWARE COURSE

Students will be taught the fundamentals of malicious code analysis beginning with the configuration of a malware analysis lab in order to gain an understanding of the components of a malware analysis toolbox and to discover each component that contributes to either behavioral or code analysis techniques. In most instances, one is unlikely to have the source code to a piece of malware. To understand malicious code at its core, students will use a disassembler to decompose, execute, and trace each step of the program. Students will then learn how to patch the executable and change its behavior for a more advantageous outcome. Malware analysis is not just about tracing code, but also about understanding the effect on its environment. Hands-on exercises are used throughout the course to examine the effects of various types of malware that run natively on a Windows platform, such as botnets and rootkits. Students will trace back the infection and identify the initial vulnerability that was used to exploit and implant the malware within the system. Students will be challenged to analyze the entirety of an event. Using behavior analysis techniques, Students will be able to not only create signatures based off the malicious code, but also develop techniques to discover and prevent this type of malicious code in their own networks.

HIGH LEVEL OUTLINE

- Fundamentals of Malicious Code Analysis
- Attribution of Malware
- Behavioral (Environment), Static (Disassemble), Dynamic (Debug) Analysis
- Defeating Defensive Techniques in Malware
- Crafting Detection and Defenses

CHIRON METHODOLOGY DOMAIN

DISCOVERY AND COUNTER-INFILTRATION PROFESSIONAL™ (DCIP)™

DURATION

5 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with VMware Player or Workstation
- Familiarity with programming languages
- Familiarity Assembly and Operating Systems

PHONE: 410.672.1552 x 109 **FAX:** 410.672.3187 **ADDRESS** 7021 Columbia Gateway Dr. Suite 250 Columbia, MD 21046

REVERSE ENGINEERING MALWARE COURSE

COURSE SCHEDULE

DAY 1: FUNDAMENTALS OF MALICIOUS CODE ANALYSIS

OUTLINE

- Introduction to Malware Analysis
- Malware Types & Definitions
- Malware Analysis Techniques Overview
  - Binary Analysis
    - Static Analysis
    - Dynamic Analysis
    - Behavioral Analysis
  - Memory Analysis
    - Hard Disk Analysis
    - Volatile Memory Analysis
  - Network Analysis
- Virtual Lab Environment Setup & Configuration
  - Windows VM
  - Linux VM
  - Automated Analysis Sandbox VM
- Establishing a Baseline of Systems & Network State
- Malware Analysis Tools Overview
  - Network Sniffers
  - Debuggers & Disassemblers
  - Windows: Olly/WinDbg/Immunity
  - Linux: Gdb / Edb
- Memory Forensics: Windows: Volatility
- Disassembler / Unpack:
  - Windows: Ida Pro
  - Linux: objdump
  - All: UPX
- Sandbox: CuckooSandbox
- Environment Baseliners
  - Windows: SysInternals
- Detection and Defense
  - Yara fingerprint creation
  - Snort signature creation
- Open Source Research Resources
  - Virus Scanners
  - Sandboxes
  - Website Black/White Lists
  - Reputation Databases

DAY 2-3: ATTRIBUTION AND ANALYSIS OF MALWARE

OUTLINE

- Malware Author Tactics, Techniques, Procedures
  - Goals and Motivations
  - Skill Level
- Characteristics of Malware
  - Sophistication
    - Code Complexity
    - Obfuscation
    - Anti-Detection Methodologies
  - Persistence Techniques
  - Virulence / Threat Level
- Malware Analysis
- Static Analysis: viewing it before execution
  - Diassembling the binary
  - Identifying file type, packer, other characteristics
  - Identifying function calls, execution flow
- Malware Analysis (continued)
  - Dynamic: viewing it in action
    - Debugging the malware
    - Tracking changes in the baseline
    - Behavior – viewing the environment interactions before/during/after execution
    - Environment changes (file system changes)
    - Memory Analysis
    - Network Sniffing
  - Sandboxes
    - Automation and simplification
  - Browser Attack Vectors
    - Javascript attack deobfuscation
- Research Phase

REVERSE ENGINEERING MALWARE COURSE

COURSE SCHEDULE

DAY 4: MALWARE DEFENSIVE/OBFUSCATIVE TECHNIQUES

OUTLINE

- Uncovering Defensive Techniques in Malware
  - Identifying packed code
  - Unpacking binaries
  - Identifying debugger and virtual machine detection algorithms
  - Defeating detection algorithms to continue execution
  - Examining various types of malware
    - Botnets
    - Rootkits
    - DLL Injections & side loading
- B. Detection & Defense
  - Virus and Code Scanners
    - Yara Overview
    - Creating custom YARA signatures
    - Grouping and identifying malicious binaries and variants
  - Network Scanners
    - Pivoting from infected hosts to network data and vice versa
    - Creating signatures based on network traffic

DAY 5: CULMINATION EXERCISE

OUTLINE

- Analysis of malicious binaries
- Analyzing partial samples (non-functioning)
- Identifying malicious activity
  - Locating command and control servers
  - Identifying command and control techniques
  - Patching binaries to benefit analysis
- Identifying rootkits
- Creating identification signatures
  - Network-based signatures
  - File-based rules