301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

CYBERPHOENIX

Malware Analysis Training

This 4-day instructor-led training is aimed at It security professionals in a malware analyst or forensic investigator job role.

Course Overview

This course serves as a guide for instructing students on how to analyze malware once discovered within a Windows operating system. Since malicious software plays a role in almost every security incident or computer intrusion, the knowledge and skills attained through this class prove beneficial to individuals seeking to advance within the malware analyst profession. While this training focuses on Windows operating systems, the skills learned easily transfer to other operating systems.

Course Outline

Static Analysis

- Anti-Virus Scanning to Confirm Malware
- Hashes for Malware Identification
- Extracting Information from File Strings, Functions and Headers

Analyzing Malware in a Virtual Machine

- The Virtual Machine Structure
- Creating and Using Your Malware Analysis Machine
- Risks of Using VMware
- Introduction to the Record/Replay Feature of VMware

Dynamic Analysis

- Malware Sandbox

- Launching Executable Malware
- Windows Process Monitor
- Process Explorer – Microsoft Task Manager
- Regshot Comparisons
- Faking a Network
- Wireshark
- NetSim
- Using the Dynamic Tools for a Malware Analysis Setup

Disassembly

- Levels of Abstraction
- Reverse-Engineering
- x86 Architecture

Interactive Disassembler Professional (IDA Pro)

- Loading an Executable in IDA Pro
- IDA Pro Interface
- *xref* in IDA Pro
- IDA Pro Function Analysis
- 5 Graphing Options
- Disassembly Modification Features
- Extending Functionality with Plug-ins

C Code Constructs

- Local and Global Variables
- Disassembling Math Operations
- if Statements
- Loops and Repetitive Tasks
- Function Calls
- switch Statements
- Arrays and Structures
- Linked List

Malware Targeted to Windows Functionalities

- Windows API
- Windows Registry

- Networking API
- Uncovering Transfer Executions from Malware
- Kernel and User Modes
- Native API

Debugging

- Source and Low Level Debuggers
- Debugging a Program
- Gaining Control through Exceptions
- Modifying Program Execution

OllyDbg – x86 Debugger

- Loading Executables
- OllyDbg Interface and Memory Map
- Threads and Stacks
- Code Execution
- OllyDbg Supported Breakpoints
- Loading and Debugging DLLs
- Tracing Technique
- Exceptions and Patching
- Shellcode Analysis and Assistance Features
- Plug-Ins
- Scriptable Debugging

WinDbg – Kernel Debugger

- Kernel Code and Device Drivers
- Preparing for Kernel Debugging
- Using the WinDbg Functionality
- Symbols for Microsoft Functions and Variables
- Constructing Files from Kernel Space
- Rootkits
- Kernel Issues with Latest Versions of Windows

Malware Characteristics

- Downloaders and Launchers
- Backdoors

- Credential Stealing Programs
- Malware Persistence Mechanisms
- Escalating Privileges
- Rootkit Forms

Covert Launching Techniques

- Launchers
- Process Injection
- Process Replacement
- Windows Hook Injection
- Detours Library
- Asynchronous Procedure Call (APC) Injection

Data Encoding

- Purpose of Encoding
- Simple Encoding Techniques – Ciphers
- Modern Cryptography
- Encoding Schemes
- Decoding Content

Network-Based Countermeasures

- Network Countermeasures
- Techniques for Secure Online Investigation
- Content-Based Network Countermeasures
- Dynamic and Static Analysis
- Perspective of the Attacker

Anti-Disassembly

- Overview of Anti-Disassembly
- Exploiting Weaknesses within Disassembler Algorithms
- Techniques for Exploiting Assumptions
- Obscuring Flow Control
- Stack-Frame Construction Analysis

Anti-Debugging

- Detecting Windows Debuggers
- Debugging Behavior
- Interfering with Debugger Operation
- Vulnerabilities in Debugger Software

Anti-VM Techniques

- Artifacts
- Vulnerable Instructions
- VMware Settings
- Exploiting the VMware Vulnerabilities

Packers and Unpacking

- Anatomy of a Packer
- Packed Program Identification
- Three Unpacking Options
- Automated and Manual Unpacking Programs
- Tips and Techniques for Packers
- Analyzing a Malware Piece without Fully Unpacking
- Packing DLLs

Analyzing Shellcode

- Loading and Running Shellcode
- PIC (Position-Independent Code)
- Identifying the Execution Location
- Manual Symbol Resolution
- Shellcode Encodings
- NOP Slide
- Locating Shellcode

C++ Language Analysis

- Object-Oriented Programming
- Virtual and Nonvirtual Functions

- Constructor and Destructor Functions

Malware for 64-bit Architecture

- Overview of the 64-bit Process and Code
- Windows 64-bit vs. 32-bit Architecture
- Microsoft's WOW64
- 64-bit Codes for Additional Insight to Malware Functionality

Malware Analysis Training FAQs

Who should take this course?

This course is designed for CIO Officers, Forensics Investigators, and Malware Analysts.

What is the recommended experience for this course?

Students should have:
– At least two years of networking experience
– CompTIA Network+, CompTIA Security+, Certified Ethical Hacker (CEH) or hold equivalent experience and knowledge
– Basic understanding of C++ and assembly language

Starting at **$1,990**

ATTENTION
Government Employees & Government Contractors call 240.667.7757 for GSA Pricing.

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

GSA

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Included in this **Malware Analysis Training**

- 4 days instructor-led training
- Malware Analysis Training training book
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*
- Eligible for MyCAA scholarship
- This course maps to the NICE framework

**available only at participating locations. Not provided with Live Online class format.*