Malware Reverse Engineering

Course Summary

Description

Malware Reverse Engineering is an in-depth look at modern day malware. Focused on static analysis, this course will teach you to reverse, patch and crack programs to gain full access to the underlying code. You will learn to use debugging and disassembly to fully understand exactly what a sample's capabilities are.

Topics

- Converting Source Code to Assembly
- Intel CPU Memory Management and Structures
- CPU Control Flows
- IDAPro, OllyDBG, and other Common Tools
- Stepping, Stepping Over and Running Code using a Debugger
- Breakpoint Fundamentals and Usage
- Patching and Assembling Executables
- Decrypting and Unpacking Protected Programs

Audience

This course is designed for:

- Malware Analysts
- Software Engineers
- Forensic Investigators
- Tier 3 Incident Responders

Prerequisites

This is an intense debugging and disassembly course. Significant experience with assembly language is required to fully benefit from this course. C Programming and the Assembly for Reverse Engineers course are recommended prerequisites for those lacking programming and assembly experience.

Duration

Five days