

Advanced Reverse Engineering Malware

Overview

Four days of Expert Reverse Engineering Malware Instruction from a senior instructor with real-world experience and deep knowledge of course content.

Target Audience

Course Objectives

- Gain the in-demand career skills of a reverse engineer. Very few information security professionals, incident response analysts and vulnerability researchers have the ability to reverse malware efficiently. You will undoubtedly be at the top of your professional field.
- Learn the methodologies, tools, and manual malware reversing techniques used in real world situations in our reversing lab.
- Move beyond automated "sandbox" testing of malware.
- More than interesting theories and lectures, get your hands dirty in our dedicated reversing lab in this security training course.

Course Outline

IDA configuration and scripts

IDA Plugin architecture and setup

The Windows Kernel

Understanding the Kernel API

Overview of rootkit technologies

Introduction to WinDBG for Kernel Debugging

Reversing a Rootkit

Deep Dive into the PE/COFF File Format

PE/COFF File format abuse

[Register Online](#)

Schedule

Class Length: 4 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

PE Antireversing techniques: Deobfuscating executables for IDA

Packers: Overview and techniques for defeating them

Packers: Study of ASPack, UPX, PEXcompact, others

AntiRE Techniques: Detecting debuggers, virtual machines, and other tricks

Process / DLL injection

VM Based Packers Unpacking Themida

Obfuscation: Usermode obfuscation methods

Analyzing physical memory with memoryze

64bit ReverseEngineering with IDA

Packers: Study of 64bit packers

Remote debugging with IDA

Understanding and reversing binary protocols

Protocol Reversing

Reversing a botnet C&C protocol