



THE HIGHEST QUALITY CYBER SECURITY TRAINING

We believe your cyber security team deserves a better learning experience

ADVANCED REVERSE ENGINEERING



5 days



Course Overview

This course follows up on the introduction and completes the budding reverse engineering skills of students against modern, APT-related malware.

We start by discussing how malware conceals its behaviour to prevent reverse engineering including the following: encryption, compression, mangling and self-unpacking shims.

We then present how malware hides itself to persist on a system, either as a user-mode program, or as a kernel-mode module.

Other covered subjects include communication features for communicating with other processes, command and control infrastructure, malware implemented using exotic runtime technologies, and signature malware behaviour, such as keylogging and privilege elevation.

Materials to bring +

Laptop computer able to run 64-bits virtual machines.


VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

Course prerequisites

Intro to Reverse Engineering



Course Breakdown

- 
- Day 1** APTs and their configurations
- Mangling
 - Compression
 - Encryption
 - Self-unpacking
- Day 2** Malware hiding techniques
- Code injection
 - API hooking
 - Hook injection
 - APC injection
 - Process hollowing
 - SSDT hooking
 - Filter drivers
- Day 3** Malware communication
- Inter-process communication
 - Configuration files
 - File transfer
 - C2 communication
- Day 4** Strangely constructed malware
- C++
 - COM
 - Delphi
- Day 5** Recognizing typical constructs
- Key logging
 - Shell redirection
 - Privilege escalation
 - Driver/service installation