



INTERMEDIATE MALWARE ANALYSIS

COURSE DESCRIPTION

Equipped with the behavioral Malware Analysis knowledge from the Basic Malware Analysis course you're ready to adventure into more advanced malware topics by attending the Intermediate Malware Analysis course. We start off the IMA course by teaching the fundamentals of the most commonly used programming languages in current Malware Development. Since looking at assembly code in a debugger can be frustrating and time consuming without a previous understanding of programming fundamentals and compiler operations you'll learn basic development skills in C and C++ as well as assembly code so that in the second week of the course you'll be able to understand the static code analysis with confidence and clarity. During the second week of instruction we introduce you to the Olly Debugger. Olly is the popular choice amongst Reverse Engineers and Malware Analysts worldwide. Through controlled evaluation using the debugger we'll teach you how to identify exactly what the malware specimen does and how it's doing it. After you've mastered the evaluation portion of the class we'll teach you how to patch the specimen to make it inactive or crack the program to allow full access to areas that have been hidden or encrypted by the malware developer.

THE STUDENT WILL LEARN:

Students who attend this class will graduate with the following advanced analysis skills:

- + Object oriented code development fundamentals
- + Assembly language fundamentals including:
 - Conversion methodology from source code to assembly code
 - Intel CPU memory management and structures
 - CPU control flows and order of operations
- + Olly Debugger including:
 - Tool overview
 - Useful Plug-ins and Add-ons
 - Breakpoint fundamentals and usage
 - Patching and assembling executables
 - Decrypting and decoding packed executables

PREREQUISITES:

- + Completion of Basic Malware Analysis course (required)
- + A strong understanding of operating systems is encouraged
- + Basic scripting language is recommended

COURSE INFORMATION:

10 days, MF, 80 hours. A certificate of completion will be given at the end of the course. Each student will be provided with a preconfigured laptop with all course training software.