# MAL500

## REVERSE ENGINEERING MALWARE

MAL500 - Reverse Engineering Malware is an intermediate course that exposes students to the theoretical knowledge and hands-on techniques to analyze malware of greater complexity.

Students will learn to analyze malicious Windows programs, debug user-mode and kernel-mode malware with WinDbg, identify common malware functionality, in addition to reversing covert and encoded malware.

### TARGET AUDIENCE

Junior malware analysts and reverse engineers who want to increase their skills to better understand more complex malicious code

### OBJECTIVE

Provide students with a working knowledge of analyzing malicious Windows programs, debugging user-mode & kernel-mode malware, identifying common malware functionality, & other related topics

CYBRScore™

## DAY 1

Malware targeting Windows victims is prolific, and understanding how this malware interacts with the complex Windows operating system and API is a challenge not to be taken lightly.

In the first part of this course, students dive straight into Windows API and its myriad functions, inputs, and outputs as they relate to reverse engineering malware targeted against Windows victims. Networking APIs, as well as threads and mutexes are examined in-depth. The day is spent trying to solve the Gordian knot that is Windows malware.

### Topics List

- Windows API
- Handles & file system functions
- Common registry functions & autoruns
- Networking APIs
- Processes, threads & mutexes
- COM objects

## DAY 2

Being able to debug a program is crucial to reverse engineering and malware analysis. On Day 2 students are introduced to the concept of debugging and extensively exposed to OllyDbg, its functionality, tools and plugins. Breakpoints, and tracing are used as part of the overall reversing process to unravel complex malware specimens.

### Topics List

- Kernel vs. User-mode debugging
- Software & hardware breakpoints
- Modifying program execution & patching
- OllyDbg overview
- Memory maps
- Executing code, breakpoints & tracing
- OllyDbg plugins

## DAY 3

On Day 3, students are introduced to the broad and complex topic of kernel debugging. This includes core principles of this interesting sub-topic, as well as a demonstration of how to configure an environment, analyze kernel objects, and look at rootkits. Day 3 closes with the discovering and reversing of a variety of malicious functionality malware executes across several labs.

### Topics List

- Kernel debugging with WinDbg
- Configuring kernel debugging environment
- Analyzing functions, structures and driver objects
- Rootkit analysis
- Downloaders, launchers & backdoors
- Analyzing various persistence mechanisms & user-mode rootkits

## DAY 4

Day 4 switches gears and delves into the complex world of covert malware. Students learn about a variety of techniques malware uses to hide its activities, and how to identify indicators of this type of activity. Process injection, hooks, and detours are looked at as part of this interesting module of the course.

### Topics List

- Covert malware
- Abusing resource section of PE file
- Process injection & process replacement
- Windows hooks & detours
- APC injection from kernel space

## DAY 5

On the final day of class, students learn how malware authors use a variety of encoding mechanisms to obfuscate data, and how to analyze them. XOR, BASE64 and custom encoding mechanisms are explored and analyzed.

After the course, students have 90 days to challenge the optional CYBRScore-enabled certification associated with MAL400. The certification presents a malware specimen to the challenger that must be analyzed using the techniques and tools learned in this course. Our behind-the-scenes scoring engine will track progress throughout against a rubric of core skills that must be demonstrated in the hands-on analysis.

### Topics List

- Analyzing encoding algorithms
- XOR, BASE64 & custom encoding
- Common crypto algorithms
- KANAL
- Custom decoding scripts in Python
- Instrumentation for generic decryption

# MAL500

REVERSE ENGINEERING MALWARE

CYBRScore™