



## Malicious Software Analysis

A Five-Day Course

Malicious code is responsible for many of today's security problems. Understanding how it works can help in understanding and controlling the attacks on your computer. This course includes an examination of the processes of infection, replication, communication and coordination. In addition to the classroom instruction, this course contains instructor demonstration and hands-on labs. We will examine current detection and eradication techniques and explore avoidance and prevention methods.

We'll review the history of malicious code, and introduce you to the taxonomy of malicious software. We will take a look at what malicious code does and how it works. Together, we'll examine the code of a number of well-known attacks and write our own programs to explore a variety of aspects of malicious code. Then we will explore the detection methods in use, their effectiveness and the challenge of tracking an ever-changing target. This detailed analysis will provide insight into the challenges faced in defeating malicious code and provide students with the opportunity to explore defensive concepts.

The course topics include viruses, worms, Trojan horses, root kits, bots and other types of malicious code.

### Course Contents

#### Trojan Horses

- Program Wrappers
- Command Substitution

#### Backdoors

- Network and Port-less
- Trapdoors

#### Rootkits

- User-mode Rootkits
- Kernel-mode Rootkits

#### Viruses

- Infection
- Propagation
- Evolution
- Payloads
- Defense

#### Worms

- Exploit
- Propagation
- Target Selection
- Scanning Engine
- Payloads
- Defense
- Future

#### Mobile Code

- Spyware
- Data Theft
- Resource Theft

#### Robots

- IRC Bots

### Who Should Attend

System administrators, web administrators, support analysts, network engineers and IT managers, as well as network personnel, security personnel, savvy home computer users, and anyone else interested in keeping their systems safe from attackers would benefit.

Knowledge of software development and code is a plus. This is an advanced level course.

#### What You'll Learn

- The characteristics and method of attack.
- How to defend against each type of attack.
- How malicious software compromises systems.
- How to identify malicious software.
- How detection systems identify malicious code.

#### What You'll Do

- Perform detailed analysis of malicious code.
- Write code which illustrates malicious software techniques.
- Examine how detection systems work
- Evaluate defensive options.

#### What You'll Take Home

- An understanding of how malware works
- The expertise to evaluate defensive measures against malicious code.
- Your personal copy of *Malware: Fighting Malicious Code*.