

Malicious Software: Effective Discovery and Countermeasures



Days: 1

Prerequisites: In order to have a successful learning experience, students should have existing knowledge of, and support experience with, networked desktop and notebook computers, as well as advanced user-level skills in Windows Vista, Windows XP, Windows 7, or Windows 10.

Audience: This course is ideal for IT professionals who combat malware on computer systems.

Description: Viruses, Rootkits, Trojans, Botnets, Ransomware—they can all be summed up as “Malware”, or Malicious Software, the computer technician’s #1 problem.

Malicious software removal can take anywhere from 3 hours to 3 days, or even longer, depending on the scope of the infection. Technicians usually want to “image” the computer; restoring the computer to a pristine state from a copy of the hard drive. Unfortunately, the end-user gets the machine back and all too often it gets re-infected again.

Viruses and other system contaminants have progressed to the point where commercial anti-virus applications may not be able to remove the infection. The virus can disable detection tools, thus allowing the malware to infest the local computer, as well as other systems on the network.

This course is designed to supply the technician with the theory and skills necessary to combat malware on their computer systems.

OUTLINE:

MODULE 1: COURSE INTRODUCTION

MODULE 2: TERMINOLOGY AND PROBLEM DESCRIPTIONS.

- Windows Registry: structure, modification, keys targeted by malicious software, editing and repair.
- Registry editing lab.

MODULE 3: VIRUS CREATION: OVERVIEW OF TOOLS USED BY HACKERS TO CREATE VIRUSES.

- Build your own virus lab.
- Malware remediation: procedures to remove malicious software, detection and termination of viral processes, recovery procedures.
- Malware detection and remediation lab.



Baton Rouge | Lafayette | New Orleans

www.lantecctc.com