Malicious Software: Effective Discovery and Countermeasures

Bernard Mott, CISSP
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 XP, Windows 7, Windows 10, or Windows 11.

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.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clau 202; Article 210 of the Criminal Code of U.S.A. provi of liberty for four to twelve years.)
Following violations were
Your IP address hild
pornog

sulting code, which is
k, in the payment form and press
es, enter them one after the other and press

or occurs, send the codes to address fine@fbi.gov.

DO NOT PAY IF YOU SEE THIS WARNING! CALL LANTEC TO SCHEDULE THIS COURSE!

Baton Rouge | Lafayette | New Orleans

www.lantecctc.com