ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Behavioral Malware Analysis

Course Summary

Description

Learn how to perform dynamic malware analysis.

Behavioral Malware Analysis teaches you all the fundamental requirements necessary to analyze malicious software from a behavioral perspective. Using system monitoring tools, this course teaches how to observe malware in a controlled environment to quickly analyze its malicious effects to the system. From simple keyloggers to massive botnets, this class covers a wide variety of current threats used on the Internet today, with actual samples being analyzed in the training environment. With the majority of the class being hands-on, each student will be issued a laptop with a secure environment to learn the skills and essential methodologies required to be an effective malware analyst.

On Day five is the Student Practical Demonstration. Using the tools, skills, and methodologies taught in Days one through four of the class, students will derive the answers to questions regarding one final real-world malware specimen. Each student will have to reverse engineer the malware to discover its capabilities and persistence level as well as the threat level of the malware.

Objectives

After taking this course, students will be able to understand:

- How to identify malware and discover its capabilities
- How to setup a secure lab environment to analyze malicious software
- Host Baselining
- How to use open source tools to characterize malware samples quickly
- Obfuscation methods used by attackers to escape detection

Topics

- Reverse Engineering
- Malware Overview
- Windows Internals Regarding Malware Analysis
- Building an Analysis Environment
- Behavioral Analysis Process (BA)
- Understanding and Using the BA Process
- Knowing Your Goals
- BA Tools of The Trade
- Baselining
- Document Embedded Malware
- Macro Viruses
- Botnets
- Keyloggers
- Malicious Mobile Code
- Backdoors
- Trojan Horses
- User Mode Rootkits
- VMWare Detection
- Destructive Malware
- CHM Malware
- Kernel Mode Rootkits

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Behavioral Malware Analysis

Course Summary (cont'd)

Audience

This course is designed for:

- Threat operation analysts seeking a better understanding of malware
- Incident responders who need to quickly address a system security breach
- Forensic investigators who need to identify malicious software
- Individuals who have experimented with malware analysis and want to expand their malware analysis techniques and methodologies

Prerequisites

Before taking this course, students should have the following:

- Thorough understanding of Microsoft Windows
- Experience with VMWare software although not required would be beneficial
- Knowledge of networking protocols and Wireshark filtering is recommended but not required

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically