Malware Analysis

Course Summary

Description

Viruses, Trojans, Ransomware, Adware, Worms, Spybots, Rootkits, and Botnets: These are just a fraction of the threats that may be spying on someone's activities, stealing their information, their resources, or their money—maybe even carrying out illegal activities on some victims behalf; the worst part is that all of this could be happening without a user even being aware.
Advanced Malware is out there, deploying military grade cyber-security patterns, as well as applying impressive hiding, infecting, and mutating techniques, which may target an organization or an individual's personal device at all times. The danger is everywhere, and it is real. Luckily, there are means to mitigate, and respond.

In this intensive hands-on course, you will learn to analyze, detect, and apply anti-malware solutions by learning the patterns of thought, and techniques of an attacker.
While the course is mostly targeting modern Windows and Linux malware and techniques, with some focus on iOS and Android, the course can be customized to focus on any of the leading desktops, servers, or mobile operating systems. While the course is mostly focused on the X86 architecture sets, In depth ARM discussion can be presented per the client's requirement.

Objectives
By the end of this course, students will be able to:

- Understand what the different types of malware are, and the damage that they cause
- Design and protect against shellcodes and code injection at multiple levels
- Construct simple malware and devise mechanisms to classify and prevent its execution
- Design malware analysis testbeds for your organization
- Apply advanced anti-detection techniques to strengthen your malware
- Apply advanced debugging and research techniques to classify advanced malware

Topics

- Introduction to Malware Types and Damage
- Binary Exploitation Overview
- Exploit Piggy-backing on Higher Level Technologies
- The Mobile Malware Landscape
- Attacker's View I: Malware construction
- Defender's View I: Classification and Analysis
- Attacker's View II: Advanced attacking and hiding techniques
- Defender's View II: Advanced defending techniques

Audience

Security personnel at all levels, who has practical software development experience.

Prerequisites

- To take this course, you must have basic knowledge in C and X86 (or ARM) architecture
- Python experience is recommended, but is not required
- Experience with software development and debugging, or Network Administration is highly recommended

Duration

Four days

ProTech "Charting the Course ...

protechtraining.com

... to Your Success!"

Malware Analysis

Course Outline

I. Introduction to Malware Types and Damage
- A. What is malware? Malware types: An introduction to a landscape under attack
- B. Malware development process overview
- C. Attacker's motivation (hint: $$$)
- D. Distribution techniques
- E. Social engineering as a leading distribution mechanism
- F. Distributed ecosystem, botnets, Command & Control, tracing and hiding wars
- G. Case studies

II. Binary Exploitation Overview
- A. Buffer Overflows and stack smashing attacks
- B. String format errors
- C. Integer overflows
- D. Heap overflows and heap spraying techniques
- E. Compiler and Operating System mitigation techniques
- F. Return Oriented Programming and mitigation techniques

III. Exploit Piggy-backing on Higher Level Technologies
- A. PDF
- B. Flash
- C. Java applets
- D. Javascript
- E. Email contents, attached images
- F. Video payload

IV. **The Mobile Malware Landscape**
- A. Mobile application store landscape
- B. Jailbroken/rooted/developer phone dangers
- C. Sandboxing and malware capabilities
- D. iOS/Android malware scanning techniques
- E. Deep linking and pivoted clickjacking techniques
- F. Android attack vector use cases: Signature validation, stagefright, rootkits

V. Attacker's View I: Malware construction
- A. Binary constructions vs. Payload construction
- B. Fuzzing techniques
- C. Malware execution
- D. Botnet construction and Command & Control (C&C) design
- E. Remote shells: Binding shell, reverse shell
- F. Construction and Integration with Metasploit framework
- G. Launching an attack

VI. Defender's View I: Classification and Analysis
- A. Testing environment design
- B. Virtual Machine boxing and isolation levels
- C. Network and filesystem re-routing tools
- D. Surface Analysis and fingerprinting techniques
- E. Dynamic analysis and instrumentation
- F. Tools and labs vary per Operating System
- G. Static Analysis and reverse engineering
- H. Tools and labs vary per Operating System
- I. Attacker tracing

VII. Attacker's View II: Advanced attacking and hiding techniques
- A. Infection methodologies
- B. Anti-Fingerprinting considerations, mutation methodologies
- C. Anti-Testing environment considerations
- D. Anti-Reversing considerations
- E. Compiler and linker options, executable packing, UPX, obfuscation
- F. Virtual Machine detection and conditional execution
- G. Anti-debugging and anti-tracing techniques
- H. Anti Firewall techniques, Subliminal Channels, ICMP

Malware Analysis

Course Outline (cont'd)

VIII. Defender's View II: Advanced defending techniques

A. Advanced fingerprinting detection in presence of code mutations
B. Anti-VM technique detection
C. Physical testing environment and proper isolation
D. Live debugging and code unpacking
E. Identifying and coping with anti-debugging and anti-tracing techniques
F. Shellcode discovery and anti-virus techniques
G. Network analysis, utilizing Intrusion Prevention/Detection Systems
H. Logging, auditing, instability, system inspection techniques
I. Honeypot techniques