PROFESSIONAL TRAINING COURSE

2 Days Course on

Introductory Malware Analysis

Two Sigma Technologies
Suite B, 19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,
68100 Batu Caves, Selangor
Tel : 03-61880601/ 019-3863400 Fax :03-61880602
zurina@2-sigma.com
www.2-sigma.com

Course Overview

If you’ve been looking for an intense, methodological intro training class on malware analysis, you’ve come to the right place. Our malware analysis training class provides an in-depth look into the world of malware and reverse engineering. Weaving complex methods with practical application, our training ensures the highest level of comprehension regarding identifying, isolating and defending against malware.

Specifically, you’ll learn how to perform dynamic and static analysis on all major files types, how to carve malicious executable from documents and how to recognize common malware tactics. You’ll also learn about tools and techniques for “run time” analysis, debugging and disassembling malicious binaries and network traffic analysis. Never again will you have to worry about malware harming you or your organization, because this training will provide you with all of the knowledge you need to know to combat it. Malware doesn’t have to be your problem.

OBJECTIVES

At the end of this program participants will be able to achieve the following objectives:

- How to perform dynamic and static analysis on all major files types
- How to carve malicious executable from documents and how to recognize common malware tactics and debug and disassemble malicious binaries
- Industry used tools and best practices for malware analysis and defense

Course Settings

Date	Refer to Calendar
Venue	Refer to Calendar
Fee	Call Us
Timings	0900-1700 (2 Days)
Inclusive	Certificates, notes and meals
Audience	Lecturers, instructors, IT Officers, Information Security Professionals, Malware Research Engineers, Information System Analyst, Network Security Analyst, Undergraduates, Postgraduates

Technologies Learnt

Technologies that you will learn and develops throughout the course:

- Network Traffic Analysis
- Networking – TCP/IP
- Internal Operating System
- Software Vulnerabilities
- Tools to detect malicious sample
- Disassembling tools

Course Schedule

Day 1	
09.00am – 10.00am	**Introduction to Malware analysis: Network Traffic Filtering and Analysis** • Review Introduction to malware multi-dimensional infection vectors • Practice of network traffic capturing and malware extraction
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	• Malware families pattern recognition and classification • Deep tracing/decoding of the network blueprints for threat type **Introduction to Malware analysis: Vulnerabilities & Online Malware Analysis tools** • Review of TCP/IP architecture and its misused by malwares
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	• Review of windows internals, security feature and loopholes • Introduction to malware types and software flaws • Discussion of popular malware families. • Online tools to perform malware analysis
Day 2	
09.00am – 10.00am	**Advanced Malware analysis: Disassembling windows Malwares and Evasion** • Introduction to different binary disassembling
10.00am – 10.30am	Breakfast
10.30am – 12.45pm	• Disassembling of windows executable using disassembling tools
12.45pm – 02.15pm	Lunch
02.15pm – 05.00pm	• Anti-Debugger and Anti-Emulation tricks used by malware • Review of a latest blog/report about a popular malware

Instructors

Ali Hussain is a Cyber Security technology research professional having in depth knowledge of emerging Cyber Threats and detection technologies, innovation, and latest trends in the area of Anti-Malware research. He has 6years of experience in the Anti Malware professional services, research and training industry at different levels. He has worked with numbers of international organizations and currently he is working with FSKTM Security Lab, Wisma R&D, University of Malaya.

More Information

Two Sigma Technologies
19-2, Jalan PGN 1A/1, Pinggiran Batu Caves,
68100 Batu Caves, Selangor
Tel: 03-61880601/ 019-3863400 Fax: 03-61880602

To register, please email to zurina@2-sigma.com or fax the registration form to 03-61880602, we will contact you for further action.