MALWARE ANALYSIS & REVERSE ENGINEERING

3 Days Programme
24 CPE's
Laptop Required

In this course the attendees will learn how to analyze a piece of Malware. This advanced course explores in depth about some of the advanced malware tools and Techniques. It is specially designed for forensic investigators, incident responders, security engineers who are involved in performing live forensics and investigations during an Incident response process & help them acquire the knowledge and skills and examine malicious programs that target and infect various systems.

This course will teach the attendees:

- How to build an isolated, controlled environment to safely analyze the behaviour of malicious program.
- Allow dissemblers and debuggers to analyze the inner working of malicious processes.
- How to derive various IOC's from Malicious programs and use them to perform Threat Hunting and detecting lateral movements.

This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

DETAILED COURSE DESCRIPTION

DAY 1

During the first day the attendees will learn how to safely execute suspicious code in the controlled environment along with most important security precautions. Teach the trainees how to perform basic static, behavioural, network and automatic analyses – what tools can be used, what to look for, what can be found. Give the trainees the opportunity to use various popular tools during the analyses and let them decide what tools are best suited for different type of analyses. Present common malicious software behaviours and patterns – which can be later used to create proper signature.

Static Analysis
- Sending sample to the analysis
- Detecting packers and protectors
- Strings extraction and analysis
- PE structure and headers analysis
- Import table analysis
- PE resources analysis
- Searching for embedded objects

Behavioural Analysis
- Executing malware sample
- Process Explorer analysis
- Regshot analysis
- Process Monitor analysis
- Searching for Rootkit artifacts

DAY 2

During this day, the attendees will learn the fundamentals of Advanced Static Analysis. They will have the opportunity to disassemble live malware samples with the help of IDA disassembler to determine their functionality and gain additional knowledge of how malicious code works.

During the first part of the day, the attendees will be introduced to the IDA disassembler, which is currently most widely used disassembler. They will learn how to navigate through the code, use different views and functions, as well as how to enhance and comment disassembled code.
During the later part of the day, they will learn how to find key parts in the code and how to analyze disassembled functions. Finally, they will learn basic anti-disassembly techniques.

.

- Introduction to IDA Pro
  - Opening and Closing samples
  - IDA Pro interface
  - Disassembly view
  - Basic Navigation
  - Functions
  - Enhancing assembly code
- Recognizing important functions using call graphs and cross references
- Functional analysis
- Analysis of network function, Winmain and Thread function
- Anti-disassembly Techniques
- Linear sweeps Vs recursive dissemblers
- Analysis of Anti-disassembly techniques

WHO SHOULD ATTEND

- Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- Technologists who have informally experimented with aspects of malware analysis prior to the course and are looking to formalize and expand their expertise in this area
- Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

DAY 3

During this day, the attendees will learn practical elements of Advanced Dynamic Analysis and debugging of malicious code. Using a debugger to analyze artifacts helps the attendees to understand how the malicious code operates and gives them more details than the behavioural analysis. If the original sample is packed then then attendees will unpack it first with the help of a debugger if necessary, before proceeding with the static analysis.

- Introduction to OllyDbg interface
  - Basic Debugging and Code Navigation
  - Breakpoints
  - Execution Flow Manipulation
  - Plugins
- Unpacking Artifacts
  - Packers and protectors
  - Unpacking UPX packed samples
  - Unpacking a Dyre Samples
- Anti-Debugging and Anti-analysis Techniques
- Basic Patching with Olydbg
- Process Creation and Injection
- Process Hollowing
- Following Child processes of Tinba Banking Trojan
- Decoding hidden strings in Tinba

Technical Pre-Requisites

Malware Reverse Engineering is a very advanced level training that cover some of the advanced tools for analyzing and reverse engineer malware at a code level.

- All attendees must have a general idea about core programming concepts such as variables, loops and functions in order to quickly grasp the relevant concepts in this area; however, no programming experience is necessary.
- Attendees should have prior experience in Windows Malware Analysis.
- The Attendees should be already familiar with x86 assembly language and principles of malicious artefact analysis.
- The Attendees should also have knowledge about Microsoft Windows system internals

Laptop Requirements

- CPU: 64-bit Intel i5/i7 - x64 bit 2.0+ GHz processor or more
- 16 GB RAM or greater
- Wireless 802.11 compatibility
- 200 GB of Hard Disk Drive
- Admin level access to the host operating system as well as guest OS
- Disable credential guard
- VMWare fusion or VMWare workstation
- 64-bit version of Windows 7(or above) or Mac OSX(10.12 or above)
- Install 7-zip on your host OS