Malware Analysis

Index: **BT220**
Duration: **40 hours**

Description
Malware Analysis is the study and close examination of malware to understand its origins, purpose, and potential impact on the system. Malware analysts accomplish their tasks by using various tools and expert-level knowledge to understand not only what a piece of malware can do but also how it does it. This course provides participants with the practical skills and knowledge to be able to analyze malware and exposes them to a critical set of tools required for their tasks.

Target Audience
The course targets participants with a foundation understanding of the internet, who wish to gain advanced capabilities in open-source intelligence.

- Cybersecurity practitioners
- Cyber forensics analysts
- Security engineers/researchers
- Incident responders
- Junior malware analysts or reverse engineers
- Software developers
- IT security administrators

Pre-requisites
- ThinkCyber Level-1 courses

Objectives
- Malware analysis using both Dynamic and Static analysis methods
- Assembly language to examine malware
- Reverse engineering malware using various tools
- The first glimpse into Windows kernel

Module 1: Introduction to Malware Analysis

In the first module, students will study different types of malware and see how they operate, understand how the anti-virus works, and will eventually develop an idea of how to approach a malicious file and where to find it.

- **Introduction to Malware Analysis**
  - Malware Analysis Definitions
  - Types of Malware
  - Different Behaviors of Malware Types
    - Behavioral Analysis
    - Code Analysis
    - Memory Analysis
  - Security Mechanisms
  - How the Anti-Virus Works
  - Understanding PE Format
  - Hash and File Identification
  - Windows Libraries and Processes
  - Windows APIs
  - Setting Up a Safe Environment for Inspecting Malware
    - Building and Configuring Virtual Machine
    - Malware Analysis Tools
      - Process Hacker
      - Process Monitor
      - Regshot
      - API Monitor
      - IDA
- **Extracting malware from data segments**
  - Network PCAP file
  - Volatile Memory (RAM)
  - Basics of Volatile Memory Malicious Activity Research
    - Network Connections
    - Malfind
    - Process
    - DLL
    - Memdump

Module 2: Basic Static Analysis

Basic static analysis allows the malware-researcher to inspect the influences of malware on the system, while it is in a static stage, that is, in code format. This phase is critical for collecting information about the malware for more advanced stages of the research.

- **Basic Static Analysis**
  - Security Concerns
    - Double-Click Prevention
    - Auto-run Prevention
  - First Analysis with Strings
    - Identify Libraries
    - Identify Patterns
    - Identify the Domain
    - Identify Windows Functions
  - PE file Sections
    - Common Sections
    - Anomaly Sections
  - Information Gathering from PE
    - Timestamp
    - GUI or CLI Application
    - Virtual Memory Allocation
    - Entry Point
  - Analyzing Program Dependency Libraries
    - Exports and Imports
    - Function Calls by Ordinal Number
  - Resources Section Anomaly
  - VirusTotal
  - Database of File Hashes
  - Writing Static Analysis Report

Module 3: Basic Dynamic Analysis

Basic Dynamic Analysis is the initial method of inspecting and analyzing malware. During this stage, students will activate the malware in a protected sandbox environment and analyze its effects on the system. Various tools for malware analysis will be introduced and used by participants during this module.

- **Basic Dynamic Analysis**
  - Organize and Isolate your Environment
  - New Malware System
    - Identifying Virtual Machines
    - Searching for Ports
    - Testing Network Traffic
  - Snapshot System
  - Analyzing Processes
    - Procmon
    - Process Explorer
  - Registry Analysis
  - Monitoring Registry Changes
  - Analyzing Autoruns
  - Network Traffic Monitoring with Wireshark
  - Faking Network Traffic and Configure Proxies
  - DNS Monitoring
  - Simulating Internet Services
  - Analyzing Findings

Module 4: Assembly x86

This module will introduce the basics of Assembly language, which is the closest to computer binary language that can be read by humans. Familiarization with Assembly will allow students to gain a closer insight into what lies at the base of the malware's code and how it was meant to operate when activated and is an entry ticket into the world of reverse engineering.

- **Assembly Language Basics**
  - x86 Processor Architecture
  - Understanding Buses and Data Traffic
  - Syscalls Table
  - Number and Character Representation
  - Basic Assembly x86 Programming
    - Standard Output
    - Registers
    - Variables and Reserves
    - Strings in Assembly
    - Working with Numbers
    - Jumps and Flags