Kurumsal Ağlarda Malware (Zararlı Yazılım) Analizi Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

In recent years, **complex and stealthy cyber-attacks (APT – Advanced Persistent Threats)** have become a serious challenge for enterprises.
At the core of these advanced attacks lies **malware** — malicious software designed to evade traditional defenses and compromise systems.

This course focuses on identifying, analyzing, and removing **malware that traditional security solutions (Antivirus, HIPS, etc.) fail to detect** in corporate environments.

Participants will gain hands-on experience with **real-world malware samples**, learning both **static and dynamic analysis techniques** to monitor malware behavior, network traffic, and system impact.

Who Should Attend

This training is ideal for professionals involved in enterprise cybersecurity operations, including:

- System and Network Administrators
- IT Auditors
- SOC (Security Operations Center) Analysts
- Information Security Teams
- Incident Response and Digital Forensics Specialists

What You Will Learn

By the end of this course, participants will:

- Identify and analyze malware in enterprise systems
- Apply static and dynamic malware analysis methods
- Recognize APT-style malware behaviors
- Contain, remove, and prevent malware infections effectively

Outline

Introduction to Malware

- Types of malware (Trojan, Worm, Ransomware, Rootkit, Spyware, etc.)
- Understanding APT (Advanced Persistent Threat)

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- The role of malware in modern cyber-attacks

Fundamentals of Malware Analysis

- Static vs Dynamic analysis
- Setting up a safe analysis environment (sandbox, VM isolation)
- Monitoring and capturing malware activity

Static Analysis Techniques

- File inspection and metadata extraction
- Hash, PE header, and string analysis
- Antivirus signature comparison

Dynamic Analysis Techniques

- Executing malware in a controlled environment
- Observing system behavior (Registry, Files, Network)
- Process and thread inspection

Network Traffic and Command & Control (C2) Detection

- Identifying C2 communication patterns
- DNS, HTTP, and HTTPS-based traffic analysis
- Detecting anomalies in network traffic

Malware Response in Enterprise Networks

- Isolating infected systems
- Malware cleanup and eradication procedures
- Removing persistence mechanisms

Reporting and Incident Management

- Creating professional malware analysis reports
- Documenting findings and technical indicators
- Integrating malware analysis into incident response workflows