# Kurumsal Ağlarda Malware (Zararlı Yazılım) Analizi Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

## Overview

Son yıllarda artan **karmaşık ve hedef odaklı siber saldırılar (APT – Advanced Persistent Threat)**, klasik savunma çözümlerinin ötesine geçmeyi zorunlu hale getirmiştir.
Bu saldırıların en önemli bileşenlerinden biri olan **zararlı yazılımlar (malware)**, kurumların bilgi güvenliği için ciddi tehdit oluşturmaktadır.

Bu eğitim, kurumsal ağlarda **geleneksel güvenlik yazılımlarının (Antivirüs, HIPS vb.) tespit edemediği zararlı yazılımların analiz edilmesini, etkilerinin belirlenmesini ve sistemden tamamen temizlenmesini** öğretmeyi amaçlar.

Katılımcılar, gerçek zararlı örnekleri üzerinde çalışarak hem **statik hem de dinamik analiz tekniklerini** öğrenecek,
malware'in sistemdeki davranışlarını izleme, ağ trafiğini analiz etme ve etkilerini raporlama becerisi kazanacaktır.

## Who Should Attend

Bu eğitim aşağıdaki uzmanlar için özel olarak tasarlanmıştır:

- Sistem ve ağ yöneticileri
- IT denetçileri
- SOC (Security Operation Center) çalışanları
- Bilgi güvenliği analistleri ve ekipleri
- Siber olay müdahale ekipleri

## What You Will Learn

Eğitim sonunda katılımcılar:

- Kurumsal sistemlerdeki zararlı yazılımları tanıyabilir ve analiz edebilir.
- Statik ve dinamik analiz tekniklerini profesyonelce uygulayabilir.
- APT tabanlı saldırılarda kullanılan malware türlerini ayırt edebilir.
- Enfekte sistemleri temizleyip, tekrar bulaşmayı önleyecek adımları atabilir.

## Outline

### Zararlı Yazılımlara Giriş

# Kurumsal Ağlarda Malware (Zararlı Yazılım) Analizi Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

- Malware türleri (Trojan, Worm, Ransomware, Rootkit, Spyware vb.)
- APT (Advanced Persistent Threat) kavramı
- Zararlı yazılımların siber saldırılardaki rolü

## Malware Analizi Temelleri

- Statik analiz ve dinamik analiz farkları
- Güvenli analiz ortamının oluşturulması (sandbox, VM izolasyonu)
- Malware davranışlarını gözlemleme yöntemleri

## Statik Analiz Teknikleri

- Dosya inceleme yöntemleri
- Hash, PE header, string ve metadata analizi
- Antivirus signature karşılaştırması

## Dinamik Analiz Teknikleri

- Malware çalıştırma ve davranış takibi
- Registry, dosya sistemi ve ağ trafiği değişimlerinin izlenmesi
- Process ve thread analizi

## Ağ Trafiği Analizi ve Komuta Kontrol (C2) Tespiti

- Komuta kontrol (C2) bağlantılarının izlenmesi
- DNS, HTTP, HTTPS tabanlı iletişim analizi
- Anormal trafik tespiti

## Kurumsal Ortamlarda Malware Müdahalesi

- Enfekte sistemin izole edilmesi
- Malware temizleme prosedürleri
- Kalıcılık (persistence) mekanizmalarının kaldırılması

## Malware Raporlama ve Olay Yönetimi

- Malware analiz raporu oluşturma
- Bulguların dokümantasyonu
- Olay yönetimi süreçlerine entegrasyon

# Kurumsal Ağlarda Malware (Zararlı Yazılım) Analizi Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com