

# Dinamik Davranışsal Analiz ile DLL Yükleme Anomalilerinin Tespiti ve Güvenlik Mimarisinin Tasarımı

## ## Özet

Modern işletim sistemlerinde dinamik bağlantı kitaplıkları (DLL) hem yazılım modülerliği hem de esne

### ## 1. Giriş

... (The full thesis content continues with detailed sections)

### ## 1. Giriş

Bu çalışmanın amacı; DLL yükleme anomalilerini tespit etmek ve güvenlik analiz mimarisi tasarlamaktır.

## ## 2. Teorik Arka Plan

Bu bölümde DLL injection teknikleri (CreateRemoteThread, Reflective Injection, APC, Process Hollowin

## ## 3. Mimari Tasarım

Proposed Architecture: Behavior Engine, Process & Memory Monitor, DLL Anomaly Engine, Kernel Syscall

### ### 3.1 Behavior Engine

Behavior Engine, API zincirlerini, permission değişikliklerini ve process lifecycle'le korelasyon ile

### ### 3.2 Process & Memory Monitor

Memory map snapshot'ları, VAD değişiklikleri, RWX bölge tespiti, handle izinleri izlenir.

### ### 3.3 DLL Anomaly Engine

Yüklenen DLL'lerin imza ve hash doğrulaması, path kontrolü, in-memory only yükleme detektörleri tart

## ## 4. Uygulama Örnekleri

Bu bölümde örnek izleme kodları (memory scan, ETW listener) verilmiştir. Bu kodlar yalnızca veri top

## ## 5. Deneysel Tasarım

Özelleştirilmiş bir VM üzerinde test senaryoları tanımlanır; benign ve malicious-benzeri yükleme dizileri kar

## ## 6. Değerlendirme

Risk skorlarının doğruluğu, false positive/negative analizi, performans yükü değerlendirilir.

## ## 7. Sonuç

Mimari, DLL tabanlı bellek manipülasyonların tespit etmeye yardımcı olur ve olay sonrasında adli veriy

## ## Kaynaklar

[1] Microsoft ETW documentation

