

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

## ## Özeti

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

### ## 1. Giriş

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

### ## 1. Giriş

Bu çalışmaın amacı; DLL yükleme anomalilerini tespit etmek ve güvenlik analizi mimarisini tasarlamaktır.

### ## 2. Teorik Arka Plan

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

### ## 3. Mimari Tasarımı

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

#### ### 3.1 Behavior Engine

Behavior Engine, API zincirlerini, permission deñilikliklerini ve process lifecycle'ini korelasyon ile

#### ### 3.2 Process & Memory Monitor

Memory map snapshot'ları, VAD deñiliklikleri, 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 tarafından

### ## 4. Uygulama Örnekleri

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

### ## 5. Deneysel Tasarımı

Çözüm bir VM üzerinde test senaryoları tanımlanır; benign ve malicious-benzeri yükleme dizileri kullanılır.

### ## 6. Değerlendirme

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

### ## 7. Sonuç

Mimari, DLL tabanlı bellek manipülasyonlarını tespit etmeye yardımcı olur ve olay sonrası adli veriyi

### ## Kaynaklar

[1] Microsoft ETW documentation

## [2] Windows Internals