# Rapor 5 - Linux Ortamlarında Fidye Yazılımı Davranış Dinamikleri ve Tespit Taksonomisi

## 1. YÖNETİCİ ÖZETİ

Bu rapor, modern fidye yazılımlarının evrimleşen saldırı tekniklerini ve özellikle Linux tabanlı sistemlerde sergiledikleri davranışsal kalıpları analiz etmektedir. Çalışma, bitirme projesi kapsamında geliştirilen eBPF (Extended Berkeley Packet Filter) tabanlı tespit aracının teorik zeminini oluşturmaktadır. Rapor kapsamında; saldırı yaşam döngüsü (Kill Chain), şifreleme stratejileri (aralıklı şifreleme, entropi değişimi) ve sistem manipülasyon teknikleri incelenmiş; bu davranışların çekirdek seviyesindeki izdüşümleri tanımlanmıştır. Amaç, statik imza tabanlı tespit yöntemlerinin yetersiz kaldığı güncel tehditlere karşı, davranışsal analize dayalı proaktif bir savunma modelinin gerekliliğini ortaya koymaktır.

## 2. GİRİŞ VE PROBLEM TANIMI

Geleneksel güvenlik yaklaşımları, zararlı yazılımları hash değerleri veya bilinen dosya imzaları üzerinden tanımlayan "reaktif" yöntemlere dayanmaktadır. Ancak saldırganların geliştirdiği polimorfik (şekil değiştiren) ve metamorfik algoritmalar, zararlı yazılımın her kurban için farklı bir imza üretmesini sağlayarak bu savunma hatlarını etkisiz kılmaktadır.

Günümüzde fidye yazılımları, sadece bir "dosya" olmaktan çıkmış; sistem araçlarını kötüye kullanan (Living off the Land - LotL), dosyasız çalışabilen ve çapraz platform (Windows/Linux/ESXi) desteği sunan karmaşık "süreçler" haline gelmiştir. Bu bağlamda, tehdidi "dosyanın ne olduğu" üzerinden değil, "sistemin ne yaptığı" üzerinden analiz eden davranışsal tespit mekanizmaları, sıfırıncı gün (zero-day) saldırılarına karşı tek geçerli savunma paradigması olarak öne çıkmaktadır.

## 3. TARİHSEL BAĞLAM VE LİNUX TEHDİT PEYZAJI

Fidye yazılımları tarihsel olarak Windows işletim sistemlerini hedef alsa da, son yıllarda bulut altyapılarının ve sanallaştırma platformlarının (VMware ESXi, Docker, Kubernetes) Linux üzerine inşa edilmesi, saldırganların odağını bu alana kaydırmıştır.

- **WannaCry (2017):** Windows tabanlı olsa da, solucan (worm) özelliğiyle ağ üzerindeki yayılma hızının önemini kanıtlamış ve davranışsal ağ analizinin gerekliliğini ortaya koymuştur.
- **Linux.Encoder.1 (2015):** Linux sunucularını hedef alan ilk büyük fidye yazılımlarından biridir. Web dizinlerini (/var/www) hedef almasıyla bilinir.
- **LockBit (Linux/ESXi Varyantları):** Günümüzün en aktif tehditlerinden biri olan LockBit

grubu, özellikle VMware ESXi sunucularını hedef alan Linux tabanlı ELF (Executable and Linkable Format) dosyaları geliştirmektedir. Bu varyantlar, sanal makineleri şifrelemeden önce kapatmak için gelişmiş komut satırı araçları kullanır.
- **BlackCat (ALPHV):** Rust programlama dili ile yazılarak hem Windows hem de Linux üzerinde çalışabilen, yüksek performanslı ve analiz edilmesi zor modern bir tehdit örneğidir.

2024 ve sonrası trendler, saldırganların "Çifte Şantaj" (Double Extortion) modelini benimsediğini ve Linux sunucularındaki veritabanlarını hedef aldığını göstermektedir.

# 4. FİDYE YAZILIMI SALDIRI YAŞAM DÖNGÜSÜ (KILL CHAIN ANALİZİ)

Lockheed Martin'in "Cyber Kill Chain" modeli, fidye yazılımı saldırılarına uyarlandığında, projenin odaklandığı tespit noktaları daha net anlaşılmaktadır. Projemiz, özellikle 5. ve 6. aşamalara (Kurulum ve Eylem) odaklanmaktadır.

1. **Keşif (Reconnaissance):** Hedef sistemin taranması.
2. **Silahlanma (Weaponization):** Zararlı kodun hazırlanması.
3. **İletim (Delivery):** Phishing veya RDP/SSH brute-force ile sisteme giriş.
4. **İstismar (Exploitation):** Güvenlik açıklarının kullanılması.
5. **Yerleşme (Installation):** Kalıcılık sağlanması ve C2 (Komuta Kontrol) sunucusu ile iletişim.
6. **Komuta ve Kontrol (C2):** Şifreleme anahtarlarının indirilmesi.
7. **Hedefteki Eylemler (Actions on Objectives):** Şifreleme, veri çalma ve fidye notu bırakma.

# 5. DAVRANIŞSAL TAKSONOMİ VE TEKNİK GÖSTERGELER

Geliştirilen eBPF ajanı, aşağıdaki davranışsal anomalileri tespit etmek üzere kurgulanmıştır.

## 5.1. Kriptografik Davranışlar ve Entropi

Fidye yazılımlarının temel amacı, dosyayı okunamaz hale getirmektir. Bu işlem, dosya içeriğinin rastgelelik seviyesini (Shannon Entropisi) değiştirir.

- **Shannon Entropisi:** Normal metin dosyaları veya kod dosyaları düşük entropiye sahiptir. Şifrelenmiş veya sıkıştırılmış veriler ise maksimum entropiye (8.0 bit/byte'a yakın) sahiptir. Bir sürecin kısa sürede çok sayıda dosyanın entropisini aniden yükseltmesi, en güçlü davranışsal göstergedir.
- **Aralıklı Şifreleme (Intermittent Encryption):** Modern zararlılar (örn: LockBit, BlackCat), tespit edilmemek ve hızı artırmak için dosyanın tamamını şifrelemek yerine, sadece belirli bloklarını (örn: her 16 baytta bir) şifreler. Bu durum, I/O tabanlı tespit sistemlerini atlatmayı amaçlar. Geliştireceğimiz araç, bu tür "parçalı" yazma işlemlerini de analiz edebilecek

hassasiyete sahip olmalıdır.

### 5.2. Dosya Sistemi Anomalileri (I/O Bursts)

- **Dosya Gezinme (Traversal):** Fidye yazılımları, dosya sistemini sistematik bir şekilde (Genellikle Derinlemesine - DFS veya Genişlemesine - BFS algoritmalarıyla) tarar.
- **Yüksek Frekanslı Erişim:** İnsan kullanımıyla mümkün olmayacak hızda (örn: milisaniyeler içinde) open, read, write, close döngüsü gerçekleşir.
- **Kanarya Dosyalar (Canary Files):** Sistemin belirli yerlerine yerleştirilen tuzak dosyaların değiştirilmesi, erken uyarı sistemi olarak kullanılabilir.

### 5.3. Sistem Manipülasyonu ve "Living off the Land"

Linux fidye yazılımları, şifreleme öncesinde sistemi hazırlar:

- **Hizmet Durdurma:** Veritabanı dosyalarının (MySQL, MongoDB) kilitlenmesini önlemek ve şifrelemeyi garantilemek için systemctl stop komutları kullanılır.
- **Yedek Silme:** rm -rf /backup/* veya bulut yedekleme ajanlarının durdurulması.
- **Log Temizleme:** Adli analizi zorlaştırmak için dmesg, /var/log/syslog veya bash_history temizlenir.

## 6. PROJE MİMARİSİYLE ENTEGRASYON (EŞLEŞTİRME)

Teorik analizler sonucunda belirlenen davranışlar, eBPF projesinde aşağıdaki teknik karşılıkları bulmaktadır:

| Davranışsal Gösterge | Sistem Çağrısı (eBPF Tracepoint) | Tespit Mantığı (User Space) |
|---|---|---|
| **Yoğun Dosya Şifreleme** | sys_enter_write, sys_enter_openat | **Hız Limiti:** 1 saniyede X'ten fazla dosya değiştirme. |
| **Uzantı Değiştirme** | sys_enter_renameat | **Regex:** Bilinen fidye uzantıları (örn: .locked, .enc) veya toplu değişim. |
| **Gölge Kopya/Yedek Silme** | sys_enter_execve, sys_enter_unlinkat | **İmza/Yol Analizi:** Kritik dizinlerdeki silme işlemleri veya rm, dd kullanımı. |
| **Servis Durdurma** | sys_enter_kill, sys_enter_execve | **Proses Analizi:** Veritabanı veya güvenlik servislerinin durdurulması. |

# 7. SONUÇ VE ÖNERİLER

Fidye yazılımları, özellikle Linux sunucularını hedef alan varyantlarıyla giderek daha sofistike hale gelmektedir. "Kısmi şifreleme" gibi atlatma teknikleri, sadece dosya içeriğine bakan sistemleri yanıltabilirken; çekirdek seviyesindeki (kernel-level) I/O davranışlarını izleyen eBPF tabanlı yaklaşımlar, bu tehditleri gerçek zamanlı olarak yakalama potansiyeline sahiptir.

Bu projede geliştirilecek prototip, teorik olarak incelenen bu davranış setlerini (hız, entropi değişimi, sistem komutları) birleştirerek hibrit bir tespit motoru sunmayı hedeflemelidir. Gelecek çalışmalarda, entropi hesaplamasının eBPF tarafında (in-kernel) yapılması performans açısından değerlendirilmelidir.