# MİTRE ATT&CK FRAMEWORK VE PYRAMİD OF PAİN RAPORU

**Hazırlayan:Muhammed Ali ZENGİN**

**17.02.2025**

# İçindekiler

# 1.Giriş

Siber tehdit aktörleri, gelişen teknolojilerle birlikte daha karmaşık saldırı teknikleri geliştirmektedir. Bu tehditleri anlamak ve etkili savunma stratejileri oluşturmak amacıyla güvenlik uzmanları, çeşitli metodolojiler ve çerçeveler kullanmaktadır. Mitre ATT&CK Framework, saldırganların kullandığı teknikleri, taktikleri ve prosedürleri sistematik bir şekilde kategorize eden kapsamlı bir bilgi tabanı sunarken, Pyramid of Pain ise saldırganların davranışlarını analiz ederek, onları en çok zorlayan savunma önlemlerini belirlemeye yardımcı olur. Bu raporda, her iki kavramın siber güvenlikteki rolü ve önemi detaylı bir şekilde ele alınacaktır.

## 2.Mitre ATT&CK Tablosu Nedir?

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber tehdit aktörlerinin saldırılarında kullandığı taktikleri, teknikleri ve prosedürleri (TTP) detaylandıran kapsamlı bir bilgi tabanıdır. MITRE tarafından geliştirilen bu framework, saldırganların siber sistemleri nasıl hedef aldığını, hangi yollarla hareket ettiğini ve hangi teknikleri tercih ettiğini anlamak için kritik bir rehber görevi görmektedir.

### 2.1.Mitre ATT&CK Tablosu Neden Önemlidir?

**Saldırıların Deşifre Edilmesi:** ATT&CK tablosu, güvenlik uzmanlarının saldırganların izlediği yolları anlamasına yardımcı olur.
**Tehdit Avcılığı (Threat Hunting)**: Siber güvenlik ekipleri, geçmiş saldırı tekniklerini analiz ederek olası tehditleri öngörüp erken müdahale edebilir.
**Savunma Stratejisi Geliştirme**: Organizasyonlar, bu framework'ü kullanarak güvenlik altyapılarını saldırganlara karşı daha dayanıklı hale getirebilir.
**Olay Müdahalesi (Incident Response)**: Bir saldırı sonrası detaylı adli analiz yapmak için kullanılır.
**Simülasyon ve Test**: Güvenlik ekipleri, saldırı tekniklerini simüle ederek savunma mekanizmalarını değerlendirme imkanı bulur.

### 2.2.Mitre ATT&CK Framework'de Bulunan Taktik ve Tekniklerin Önemi

Mitre ATT&CK, saldırıları üç ana kategoriye ayırır: **Taktikler (Tactics), Teknikler (Techniques) ve Alt Teknikler (Sub-Techniques)**.

**Taktikler**: Saldırganların belirli hedeflere ulaşmak için izlediği genel stratejilerdir (örneğin, İlk Erişim, Yanal Hareket, Veri Çıkışı).

**Teknikler**: Taktikleri uygulamak için kullanılan spesifik yöntemlerdir (örneğin, Kimlik Bilgisi Hırsızlığı, PowerShell Kullanımı).
**Alt Teknikler**: Tekniklerin daha spesifik alt bileşenleridir (örneğin, Kimlik Bilgisi Hırsızlığı - LSASS Damping).

Bu yapı, güvenlik uzmanlarının saldırıları daha iyi analiz ederek güçlü savunma mekanizmaları oluşturmasına yardımcı olur.

### 2.3.TTP Nedir?

TTP, **Tactics (Taktikler), Techniques (Teknikler) ve Procedures (Prosedürler)** kavramlarının birleşimidir.

**Taktikler (Tactics):** Saldırganların ulaşmak istediği genel hedefler.
**Teknikler (Techniques):** Bu hedeflere ulaşmak için kullanılan yöntemler.
**Prosedürler (Procedures):** Tehdit aktörlerinin teknikleri uygulama biçimleri.

TTP'ler, saldırgan davranışlarını analiz ederek tehditleri daha etkili şekilde tespit etmeyi mümkün kılar.

## 2.4.TTP-Based Threat Hunting ve Detection Engineering Nedir?

**TTP-Based Threat Hunting**: Güvenlik uzmanları, geçmiş saldırıların TTP'lerini analiz ederek gelecekteki tehditleri öngörmeye ve erken tespit etmeye çalışır.
**Detection Engineering**: Siber tehditlerin otomatik olarak tespit edilmesini sağlamak için güvenlik sistemleri (SIEM, EDR, IDS) üzerinde kurallar ve algılama mekanizmaları geliştirilir. Bu süreçte ATT&CK tablosundaki teknikler referans alınır.

## 2.5.2022 Ukraine Electric Power Attack (C0034)

Sandworm Team, Ukrayna'daki bir elektrik dağıtım şirketinin SCADA sistemine sızarak yetkisiz komutlar gönderdi. Saldırıda GOGETTER, Neo-REGEORG, CaddyWiper gibi zararlı yazılımlar ve sistemde var olan yönetim araçları (Living off the Land - LotL) kullanıldı. Bu saldırıda kullanılan teknikler şu şekildedir:

**T1059.001 - PowerShell Kullanımı**

Saldırganlar, TANKTRAP adlı özel bir PowerShell aracını kullanarak Windows Group Policy (GPO) üzerinden zararlı yazılımları yaydı ve çalıştırdı.

**T1543.002 - Systemd Servisi ile Kalıcılık**

Linux sistemlerinde GOGETTER zararlısını kalıcı hale getirmek için bir Systemd servisi oluşturuldu. Bu servis, sistem kullanıcı girişlerini kabul ettiğinde otomatik olarak çalıştırıldı.

**T1485 - Veri Silme (Wiper Kullanımı)**

Sandworm Team, saldırının etkisini artırmak için CaddyWiper zararlısını devreye sokarak SCADA sistemlerine ait dosyaları, harici sürücüleri ve fiziksel disk bölümlerini sildi.

**T1484.001 - Group Policy (GPO) Değiştirme**

Saldırganlar, Group Policy Objects (GPO) kullanarak kötü amaçlı yazılımları dağıttı ve sistemlere yayılmasını sağladı.

**T1570 - Lateral Tool Transfer**

Saldırı sırasında CaddyWiper zararlısı, GPO kullanılarak saldırganların kontrolündeki bir sahneleme sunucusundan hedef sistemlere taşındı.

**T1036.004 - Servisleri Maskeleme**

Saldırganlar, Linux sistemlerde Systemd servislerini değiştirerek GOGETTER'ı meşru bir sistem servisi gibi gösterdi.

**T1095 - TLS Tabanlı Tünelleme ile C2 İletişimi**

Saldırganlar, TLS tünelleme kullanarak Komuta ve Kontrol (C2) sunucularıyla şifreli bir bağlantı kurdu.

**T1572 - Protokol Tünelleme**

GOGETTER zararlısı, Yamux protokolü üzerinden bir TLS tabanlı tünel oluşturarak dış sunucularla iletişim sağladı.

**T1053.005 - Zamanlanmış Görevler ile Saldırı Planlama**

CaddyWiper, Windows sistemlerde Scheduled Tasks ile zamanlanarak belirli bir saatte çalıştırıldı.

**T1505.003 - Web Shell Kullanımı**

Saldırganlar, Neo-REGEORG adlı web shell'i, dış dünyaya açık bir sunucuya yükleyerek uzaktan erişim ve veri transferi sağladı.

**T0895 (ICS) - Autorun Image Kullanımı**

SCADA sistemine bağlı bir sanal makineye, a.iso adında bir ISO imajı yüklendi. Sistem, CD-ROM otorun özelliği açık olduğu için içindeki VBS scriptini otomatik olarak çalıştırdı.

**T0807 (ICS) - Komut Satırı Arayüzü (CLI) Kullanımı**

Saldırganlar, SCIL-API kullanarak MicroSCADA platformunda komutları doğrudan çalıştırdı.

**T0853 (ICS) - Scripting Kullanımı**

lun.vbs adlı bir Visual Basic scripti, n.bat dosyasını çalıştırarak MicroSCADA yazılımına komut gönderdi.

**T0894 (ICS) - Sistem İkili Dosyalarının Kötüye Kullanımı**

scilc.exe adlı bir MicroSCADA uygulama bileşeni, saldırganların tanımladığı s1.txt dosyasındaki komutları çalıştırarak SCADA sistemlerine yetkisiz komutlar gönderdi.

**T0855 (ICS) - Yetkisiz SCADA Komutları Gönderme**

SCIL-API kullanılarak, enerji altyapısındaki cihazlara yetkisiz SCADA komutları gönderildi ve sistemlerin kontrolü ele geçirilmeye çalışıldı.

## 2.6.Senaryo

XYZ Teknoloji adlı bir şirket, siber saldırıya uğradı. Tehdit aktörleri, şirketin kritik sistemlerine sızarak verileri ele geçirdi ve fidye yazılımı ile sistemleri kilitledi. Saldırı, aşağıdaki aşamalarda gerçekleşir:

1. Keşif (Reconnaissance)

Saldırganlar, şirket hakkında bilgi toplamak için:

T1595.002 - Açık Port ve Servis Keşfi: Şirketin internet üzerindeki açık sistemlerini tespit etti.

T1598 - Sosyal Mühendislik: LinkedIn ve şirket web sitesi üzerinden çalışan bilgileri topladı.

2. Başlangıç Erişimi (Initial Access)

T1566.002 - Spear Phishing: Şirket çalışanlarına sahte e-postalar göndererek kötü amaçlı dosya açtırdı.

T1204.002 - Kötü Amaçlı Dosya Açtırma: Açılan belge ile zararlı yazılım çalıştırıldı.

3. Yetki Yükseltme & Kalıcılık (Privilege Escalation & Persistence)

T1548.002 - UAC Atlama: Saldırganlar yönetici yetkisi kazandı.

T1547.001 - Kalıcılık İçin Başlangıç Servisi: Zararlı bir program Windows başlangıcına eklendi.

4. Yanal Hareket & Komuta Kontrolü (Lateral Movement & C2)

T1021.002 - Uzak Masaüstü Protokolü (RDP) Kullanımı: Şirketin iç ağına yayıldılar.

T1572 - Protokol Tünelleme: Ağ güvenlik sistemlerinden saklanmak için trafik şifreledi.

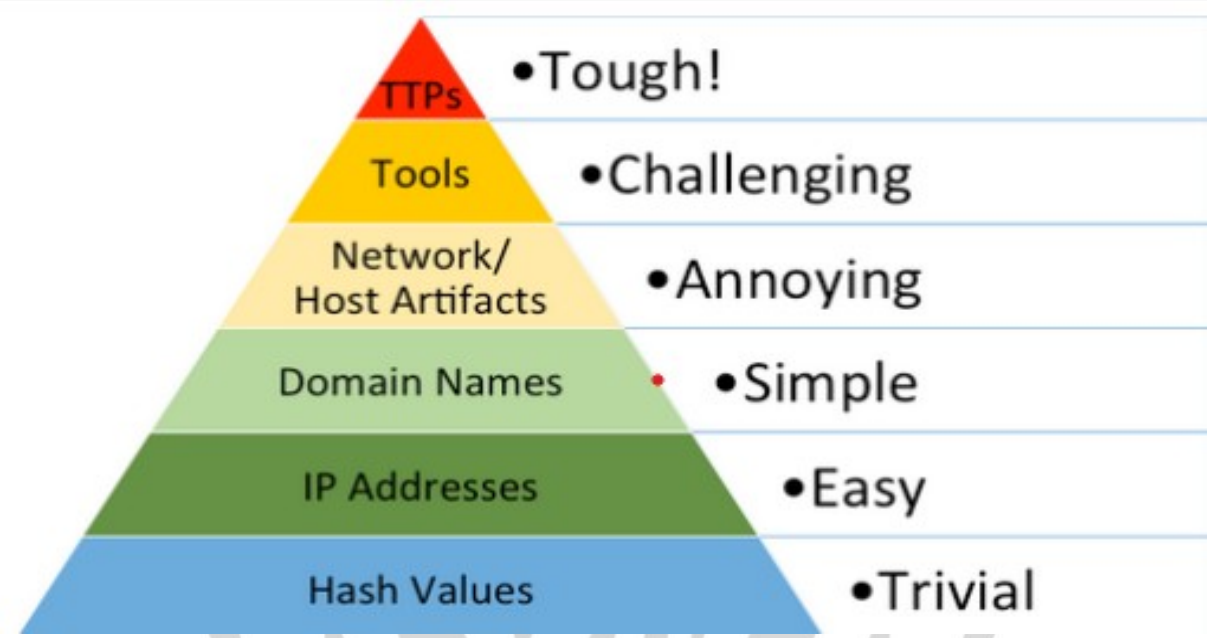
5. Veri Çalma & Fidye Yazılımı (Exfiltration & Impact)

T1041 - Veri Sızdırma: Müşteri verileri saldırganların sunucularına aktarıldı.

T1486 - Fidye Yazılımı Kullanımı: Tüm sistemler şifrelenerek fidye talep edildi

## 3.Pyramid of Pain

Pyramid of Pain (Acı Piramidi), David Bianco tarafından geliştirilen ve siber güvenlik savunmaları bağlamında, bir saldırganın tespit edilmekten kaçınma ve saldırısına devam etme sürecinde karşılaşacağı zorluk seviyeleri ile maliyeti gösteren kavramsal bir çerçevedir. Saldırganların davranışlarını analiz etme ve önlem alma konusunda bir rehber niteliği taşır. Piramidin alt kısmından üste doğru çıkıldıkça, saldırgana yaratılan zorluk seviyesi de artar.




## 3.1.Katmanlar

**1.Hash values:** Hash değerleri en küçük değişikliklerle bile tamamen değiştiğinden, saldırganlar kolayca yeni hash değerleri üretebilir ve tespit edilmekten kaçınabilir. Dolayısıyla, "hash values" piramidin en alt katmanında yer alır.

**2.IP Addresses:**Saldırganlar için IP adreslerini değiştirmek oldukça kolaydır. Bunun nedeni, proxy sunucuları ve VPN'ler gibi araç ve tekniklerin kullanılmasıdır. Ayrıca, İnternet Servis Sağlayıcıları (ISP'ler) tarafından atanan dinamik IP adresleri, kullanıcıların IP adreslerinin sık sık değişmesine neden olur. Bu da saldırganların bağlantıyı kesip tekrar bağlanarak yeni bir IP adresi almasını mümkün kılar.

**3.Domain Names:**Domain isimlerini engellemek, saldırganın yeni bir domain oluşturmasını gerektirir. Bu, onlara biraz daha maliyet ve zorluk çıkarır.IP adreslerini engellemekten çok daha etkili olabilir.

**4.Network/Host Artifacts:**Hedef cihazda bırakılan izler veya dosyalar. Bunları değiştirmek, saldırganın sistemdeki erişimini yeniden yapılandırmasını gerektirir.bu artıkları etkisiz hale getirmek veya bunlara karşı önlem almak, saldırganlar için ciddi bir rahatsızlık kaynağı olabilir.

**5.Tools**:Saldırganların kullandığı araçları engellemek, operasyonlarını ciddi anlamda zorlaştırır. Çünkü yeni araçlar bulmak veya mevcut araçları değiştirmek zaman alıcı ve yüksek maliyetlidir. Saldırganlara en fazla zarar veren engellerden biridir.

**6.Tactics, Techniques & Procedures (TTPs):**Piramidin en üstünde yer alan TTP'ler, saldırganın tüm operasyon tarzını değiştirmesini gerektirir ve ona en fazla acıyı verir.

## 4.Sonuç;

Bu raporda, MITRE ATT&CK Framework ve Pyramid of Pain kavramlarının siber güvenlikteki rolü incelenmiştir. Siber tehditlerin daha iyi anlaşılması ve engellenmesi için, sadece bireysel saldırı göstergelerine değil, saldırganların genel strateji ve taktiklerine odaklanmak gereklidir. Kuruluşlar, güvenlik politikalarını bu çerçeveler doğrultusunda şekillendirerek saldırganları daha fazla maliyet ve çaba harcamaya zorlayabilir, böylece daha etkili bir savunma hattı oluşturabilirler.

## 5.Kaynaklar;

https://attack.mitre.org/

https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain

https://cybershieldcommunity.com/pyramid-of-pain/