2025

Mitre Att&ck Framework

BİLGEHAN BAYRAK

17.02.2025

İçindekiler

GİRİŞ

Bu rapor, Mitre ATT&CK Framework'ün temel bileşenlerini, önemini ve güvenlik uzmanları için sağladığı faydaları detaylı bir şekilde incelemek amacıyla hazırlanmıştır. Siber güvenlik alanında, saldırganların kullandığı teknikler ve yöntemler sürekli olarak evrim geçirmektedir. Mitre ATT&CK Framework, tehdit aktörlerinin davranışlarını modelleyerek güvenlik ekiplerine proaktif savunma mekanizmaları geliştirme imkânı sunar.

Bu raporda aşağıdaki konular ele alınacaktır:

- Mitre ATT&CK tablosunun ne olduğu ve neden önemli olduğu
- Framework'te bulunan taktik ve tekniklerin önemi
- TTP (Tactics, Techniques, and Procedures) kavramı
- TTP-Based Threat Hunting ve Detection Engineering'in incelenmesi
- 2022 Ukraine Electric Power Attack (C0034) saldırısının detaylandırılması
- Bir şirketin siber saldırıya uğraması üzerine bir senaryo oluşturularak Mitre ATT&CK metodolojisinin uygulanması

Bu rapor, güvenlik analistleri, tehdit avcıları (Threat Hunters) ve olay müdahale ekipleri için yol gösterici bir kaynak olarak hazırlanmıştır.

MİTRE ATT&CK TABLOSU NEDİR?

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework, siber saldırganların sistemlere nasıl saldırdığını modelleyen bir bilgi tabanıdır. Saldırganların kullandığı yöntemleri, teknikleri ve prosedürleri (TTP) içerir. Bu framework, saldırgan davranışlarını daha iyi anlamak ve savunma mekanizmalarını geliştirmek için kullanılır.

MİTRE ATT&CK TABLOSU NEDEN ÖNEMLİDİR?

- Siber tehdit istihbaratı için temel referans kaynağıdır.
- Organizasyonların güvenlik açıklarını değerlendirmesine yardımcı olur.
- Tehdit avcılığı (Threat Hunting) ve saldırı tespiti (Detection Engineering) süreçlerinde kullanılır.
- Savunma stratejileri oluşturmak ve güvenlik çözümlerini güçlendirmek için rehberlik eder.
- Saldırı yüzeyini analiz etmeye ve önleyici güvenlik tedbirleri geliştirmeye olanak tanır.

MİTRE ATT&CK FRAMEWORK'DE BULUNAN TAKTİK VE TEKNİKLERİN ÖNEMİ

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber tehdit aktörlerinin kullandığı saldırı yöntemlerini sistematik bir şekilde belgeleyen ve sınıflandıran bir çerçevedir. Bu framework, saldırganların izlediği adımları anlamak, tespit etmek ve savunma mekanizmaları geliştirmek için güvenlik uzmanlarına rehberlik eder.

- **Mitre ATT&CK'in Yapısı**

  Mitre ATT&CK Framework, **taktikler** ve **teknikler** olmak üzere iki temel bileşene sahiptir:

  1. **Taktikler:** Saldırganların belirli bir aşamada gerçekleştirmek istediği genel hedeflerdir. Örneğin, **İlk Erişim (Initial Access)** taktiği, bir saldırganın hedef sisteme giriş yapmaya çalıştığı aşamayı tanımlar.
  2. **Teknikler:** Saldırganların belirli bir taktiği gerçekleştirmek için kullandıkları spesifik yöntemlerdir. Örneğin, **Kimlik Avı (Phishing)** tekniği, saldırganların sosyal mühendislik yoluyla hedeflerinden kimlik bilgilerini ele geçirmeye çalıştığı bir yöntemdir.

Taktikler ve teknikler, saldırı sürecinin farklı aşamalarını detaylandırarak güvenlik ekiplerinin tehditleri daha iyi anlamasını ve saldırılara karşı etkili savunma önlemleri geliştirmesini sağlar.

- **Mitre ATT&CK'in Siber Güvenlikteki Önemi**

  Mitre ATT&CK, birçok siber güvenlik alanında kullanılarak organizasyonların güvenlik duruşlarını geliştirmelerine yardımcı olur. Aşağıda, bu framework'ün başlıca kullanım alanları detaylandırılmıştır:

  1. SIEM ve SOC Ortamlarında Saldırı Tespit Sistemleri Oluşturma

  - SIEM (Security Information and Event Management) sistemleri, tehditleri tespit etmek için logları analiz eder.
  - Mitre ATT&CK, SOC (Security Operations Center) analistlerinin loglardan tehdit aktörlerinin taktik ve tekniklerini tanımlamasına yardımcı olur.
  - SIEM kurallarını ve korelasyon motorlarını Mitre ATT&CK tekniklerine göre yapılandırarak saldırıları daha iyi tespit etmek mümkündür.

  🔹 **Örnek:** SIEM üzerinde **PowerShell Execution (T1059.001)** tekniğini izleyerek, saldırganların sistemde kötü amaçlı komutlar çalıştırmasını tespit etmek.

2. Saldırı Simülasyonları ve Kırmızı Ekip Çalışmaları İçin Rehberlik Etme

- Mavi ve kırmızı takım çalışmaları için Mitre ATT&CK, saldırı simülasyonları gerçekleştirmeye yardımcı olur.
- Kırmızı ekipler (Red Team), tehdit aktörlerinin kullandığı teknikleri simüle ederek savunma mekanizmalarını test edebilir.
- Mavi ekipler (Blue Team), bu saldırılara karşı savunma stratejileri geliştirerek tespit ve yanıt süreçlerini iyileştirebilir.

🔹 **Örnek:** Kırmızı ekip, **Credential Dumping (T1003)** tekniğini kullanarak bir sistemde hassas kimlik bilgilerini ele geçirmeye çalışırken, mavi ekip bu aktiviteyi tespit etmek için SIEM kurallarını test eder.

3. Olay Müdahale Sürecinde Kullanımı

- Olay müdahale ekipleri, saldırıların analizini yaparken Mitre ATT&CK tekniklerini referans alarak saldırının aşamalarını belirleyebilir.
- Saldırı sırasında kullanılan teknikler tespit edilerek olayın kaynağı, kullanılan araçlar ve saldırganın amacı anlaşılabilir.
- Bu analiz sayesinde gelecekte benzer saldırıların önlenmesi için uygun güvenlik önlemleri alınabilir.

🔹 **Örnek:** Bir organizasyonda gerçekleşen saldırıda **Lateral Movement (T1021.002 - SMB/Windows Admin Shares)** tekniği kullanılmışsa, olay müdahale ekibi, saldırganın ağ içinde nasıl yayıldığını analiz edebilir.

4. Siber Tehdit İstihbaratı ile Güvenlik Politikalarının Oluşturulması

- Mitre ATT&CK, tehdit istihbaratı ekiplerine saldırı gruplarının (APT grupları gibi) hangi teknikleri kullandığını anlamada yardımcı olur.
- Bu bilgiler, organizasyonların güvenlik politikalarını ve önleyici kontrollerini şekillendirmek için kullanılabilir.
- Yeni tehditler ortaya çıktıkça, güvenlik ekipleri saldırganların en güncel tekniklerine karşı hazırlıklı olabilir.,

🔹 **Örnek:** Bir APT (Advanced Persistent Threat) grubu, belirli bir sektöre yönelik **Spear Phishing (T1566.001)** saldırıları gerçekleştiriyorsa, bu bilgi kullanılarak çalışanlara yönelik bilinçlendirme eğitimleri düzenlenebilir ve e-posta filtreleme politikaları geliştirilebilir.

TTP (TACTİCS, TECHNİQUES, AND PROCEDURES) NEDİR?

Siber güvenlik alanında sıkça kullanılan **TTP (Tactics, Techniques, and Procedures)** kavramı, tehdit aktörlerinin saldırıları nasıl gerçekleştirdiğini anlamamıza yardımcı olur.

- **Tactics (Taktikler):** Saldırganların genel hedeflerini ifade eder.
- **Techniques (Teknikler):** Bu hedeflere ulaşmak için kullanılan spesifik yöntemlerdir.
- **Procedures (Prosedürler):** Gerçek saldırılarda tekniklerin nasıl uygulandığını detaylandıran somut örneklerdir.

Bu yapı, siber tehditleri analiz eden güvenlik ekipleri için saldırganların izlediği adımları daha iyi anlamayı sağlar ve savunma stratejilerini oluştururken kritik bir rehber görevi görür.

1. **Taktikler (Tactics)**

   Taktikler, saldırganların belirli bir aşamadaki amaçlarını tanımlar. **MITRE ATT&CK Framework** gibi tehdit modelleri, saldırıları **taktiklere** göre kategorize eder.

   Bazı yaygın taktikler şunlardır:

   🔹 **Keşif (Reconnaissance)** → Hedef sistem veya organizasyon hakkında bilgi toplama.
   🔹 **İlk Erişim (Initial Access)** → Sisteme ilk girişin sağlanması
   🔹 **Yürütme (Execution)** → Kötü amaçlı kodun çalıştırılması
   🔹 **Kalıcılık (Persistence)** → Saldırganın erişimini kaybetmemek için sistemde kalıcı değişiklikler yapması.
   🔹 **Savunmadan Kaçınma (Defense Evasion)** → Antivirüs ve güvenlik önlemlerinden kaçınma.
   🔹 **Kimlik Bilgilerini Elde Etme (Credential Access)** → Kullanıcı adı ve şifre gibi bilgilerin ele geçirilmesi.
   🔹 **Yanal Hareket (Lateral Movement)** → Saldırganın ağ içinde diğer sistemlere yayılması.
   🔹 **Etkiler (Impact)** → Veri silme, fidye yazılımı kullanma veya hizmetleri devre dışı bırakma gibi zarar verme amaçlı adımlar.

2. Teknikler (Techniques)

Teknikler, saldırganların yukarıda bahsedilen **taktikleri gerçekleştirmek için** kullandıkları yöntemlerdir. Bir taktik, birden fazla teknik içerebilir.

Örnek Teknikler:

- **Keşif (Reconnaissance) → Açık Kaynak Taraması (T1590)**
  - Saldırganlar, hedef sistemler hakkında bilgi toplamak için Shodan, Google Dorking veya WHOIS sorguları gibi araçları kullanabilir.
- **İlk Erişim (Initial Access) → Kimlik Avı (Phishing) (T1566)**
  - Saldırgan, bir çalışanı kandırarak kötü amaçlı bir bağlantıya tıklamasını veya zararlı bir ek açmasını sağlayabilir.
- **Kimlik Bilgilerini Elde Etme (Credential Access) → Mimikatz Kullanımı (T1003)**
  - Windows sistemlerde Mimikatz aracıyla RAM üzerindeki şifrelerin ele geçirilmesi.
- **Savunmadan Kaçınma (Defense Evasion) → Güvenlik Günlüklerini Silme (T1070)**
  - Saldırgan, tespit edilmemek için Windows Event Logs veya Linux syslog kayıtlarını silebilir.
- **Yanal Hareket (Lateral Movement) → SMB Üzerinden Komut Çalıştırma (T1021.002)**
  - Saldırgan, bir sistemden diğerine geçmek için SMB protokolü üzerinden uzaktan komut çalıştırabilir.

Bu teknikler saldırganların izlediği stratejileri anlamak ve tespit etmek için kritik öneme sahiptir.

3. Prosedürler (Procedures)

Prosedürler, belirli bir saldırı grubunun teknikleri nasıl uyguladığına dair gerçek dünya senaryolarını gösterir. Yani prosedürler, teorik tekniklerin gerçek saldırılarda nasıl kullanıldığını açıklar.

Örneğin, **APT29 (Cozy Bear)** adlı bir tehdit aktörü şu prosedürü kullanabilir:

- **Taktik:** Kimlik Bilgilerini Ele Geçirme (**Credential Access**)
- **Teknik:** LSASS Belleğini Dumplama (**T1003.001**)
- **Prosedür:**
  - APT29, hedef sistemde **Mimikatz** veya **ProcDump** kullanarak **LSASS (Local Security Authority Subsystem Service)** belleğinden şifreleri çeker.
  - Elde edilen kimlik bilgileriyle yanal hareket gerçekleştirilerek diğer sistemlere erişilir.

Başka bir örnek olarak, **Emotet zararlı yazılımı** şu prosedürü kullanabilir:

- **Taktik:** İlk Erişim (**Initial Access**)
- **Teknik:** Kimlik Avı ile Kötü Amaçlı Makro Çalıştırma (**T1204.002**)
- **Prosedür:**
  - Hedef kullanıcıya zararlı bir Word dosyası gönderilir.
  - Kullanıcı dosyayı açıp "Makroları Etkinleştir" dediğinde, zararlı kod çalıştırılarak saldırganın sistemde komut yürütmesine olanak tanır.

Bu tür prosedürlerin anlaşılması, güvenlik ekiplerinin **tehdit aktörlerinin nasıl çalıştığını daha iyi modellemesine** yardımcı olur.

TTP'LERİN KULLANIM ALANLARI

TTP konsepti, birçok farklı siber güvenlik alanında kritik bir rol oynar:

1. **Tehdit Avcılığı (Threat Hunting)**
   - Güvenlik analistleri, tehdit aktörlerinin hangi TTP'leri kullandığını analiz ederek ağda saldırgan izleri arar.
2. **SIEM ve Güvenlik Analizi**
   - SIEM kuralları, belirli TTP'leri tanıyacak şekilde yapılandırılabilir.
3. **Saldırı Simülasyonları (Red Team - Blue Team Egzersizleri)**
   - Red Team, saldırı simülasyonu yaparken TTP'leri uygular, Blue Team ise bu saldırıları tespit etmeye çalışır.
4. **Siber Tehdit İstihbaratı (Cyber Threat Intelligence - CTI)**
   - Tehdit istihbarat ekipleri, APT gruplarının kullandığı TTP'leri analiz ederek savunma stratejileri geliştirir.
5. **Olay Müdahale (Incident Response)**
   - Olay müdahale ekipleri, bir saldırıyı analiz ederken hangi TTP'lerin kullanıldığını belirleyerek saldırıyı hızlıca tespit edebilir.

TTP-BASED THREAT HUNTİNG VE DETECTİON ENGİNEERİNG

Siber güvenlikte **Threat Hunting (Tehdit Avcılığı)** ve **Detection Engineering (Algılama Mühendisliği)**, tehditleri önceden tespit etmek ve saldırılara karşı daha etkili bir savunma mekanizması oluşturmak için kritik öneme sahiptir. **TTP-Based (Taktik, Teknik ve Prosedür Temelli) yaklaşım**, saldırganların izlediği yolları anlamayı ve buna uygun koruma yöntemleri geliştirmeyi sağlar.

1. TTP-Based Threat Hunting (TTP Temelli Tehdit Avcılığı)

Tehdit avcılığı (Threat Hunting), proaktif bir siber güvenlik yaklaşımıdır. Amaç, bilinen veya bilinmeyen tehditleri tespit etmek için sistem günlüklerini (loglarını) analiz ederek saldırganların izlerini aramaktır.

Neden TTP-Based Threat Hunting?

- Saldırganlar, **IOCs (Indicators of Compromise – Bulaşma Göstergeleri)** değiştirerek algılamadan kaçabilir, ancak **TTP'leri büyük ölçüde değişmez**.
- Yalnızca imza bazlı tespit sistemlerine güvenmek (örneğin antivirüsler), gelişmiş tehditleri gözden kaçırabilir.
- APT (Advanced Persistent Threat) grupları, benzer **Taktik, Teknik ve Prosedürleri (TTP'leri)** kullanır.

TTP-Based Threat Hunting Adımları

TTP Belirleme → Avlanılacak belirli bir TTP seçilir. Örneğin, **Kimlik Bilgisi Çalma (Credential Dumping – T1003)**.
Log Kaynaklarını Tanımlama → Belirlenen TTP'ye dair izler hangi loglarda olabilir? (Windows Event Logs, Sysmon, UFW logları vb.)
Hipotez Oluşturma → "Saldırganlar Mimikatz kullanarak LSASS belleğinden şifreleri alabilir mi?" gibi bir senaryo belirlenir.
Veri Analizi ve Log İnceleme → SIEM (Security Information and Event Management) sistemleri veya özel sorgular kullanılarak ilgili olaylar aranır.
Anomali Tespiti → Normal davranıştan sapmalar analiz edilir.
Sonuçları Değerlendirme ve Alarm Mekanizmaları Kurma → Eğer bir saldırı izi tespit edilirse, bunu gelecekte daha hızlı algılamak için SIEM kuralları yazılır.

Örnek: Windows Event ID 4624 Kullanılarak Oturum Açma İzleme

Taktik: Kimlik Bilgilerini Elde Etme (**Credential Access**)
Teknik: Zorla Şifre Deneme (**Brute Force – T1110**)

Tehdit Avcılığı Süreci:

- **Windows Event ID 4624** başarılı oturum açma olaylarını kaydeder.
- Normal kullanıcı davranışlarını analiz ederek, aynı hesap üzerinden çok fazla başarısız giriş denemesi olup olmadığı kontrol edilir.
- **Olası saldırı senaryoları:**
    - Kısa sürede birçok giriş denemesi (brute-force saldırısı)
    - Normal dışı saatlerde veya coğrafi konumlardan girişler
    - Aynı IP adresinden farklı hesaplarla oturum açma girişimleri

2. Detection Engineering (Algılama Mühendisliği)

Algılama mühendisliği, tehditleri otomatik olarak tespit edebilmek için güvenlik çözümlerine yönelik özel kurallar ve mekanizmalar geliştirme sürecidir. Bu süreçte **MITRE ATT&CK Framework** gibi tehdit modelleme araçları kullanılarak etkili algılama mekanizmaları oluşturulur.

Neden Detection Engineering?

- Gelişmiş saldırılar, geleneksel imza tabanlı güvenlik çözümleriyle tespit edilemeyebilir.
- SIEM ve EDR (Endpoint Detection & Response) sistemlerinin daha etkin çalışmasını sağlar.
- Yanlış pozitifleri (false positive) azaltarak daha doğru alarm mekanizmaları oluşturur.

Detection Engineering Adımları

Tehdit Modelleme → Saldırganların kullandığı teknikler belirlenir (**MITRE ATT&CK** kullanarak).
Log Kaynaklarının Belirlenmesi → İzlenmesi gereken sistem günlükleri ve olay türleri seçilir.
Kural Yazma ve Algılama Mekanizmaları Geliştirme → SIEM, EDR ve IDS/IPS sistemlerine özel kurallar yazılır.
Test ve Optimizasyon → Yanlış pozitifleri azaltmak için kurallar test edilir ve iyileştirilir.

Örnek: SIEM İçin Mimikatz Algılama Kuralı

Taktik: Kimlik Bilgilerini Elde Etme (**Credential Access**)
Teknik: LSASS Belleğinden Şifre Çekme (**T1003.001**)

Algılama Süreci:

- Mimikatz, **LSASS.exe** belleğini dumplayarak kimlik bilgilerini çalabilir.
- Windows Event Loglarında **Event ID 4688** incelenerek LSASS.exe işlemi kontrol edilir.
- **Sysmon ID 10**, bellek okuma işlemlerini izlemek için kullanılabilir.

3. TTP-BASED THREAT HUNTİNG VE DETECTİON ENGİNEERİNG ARASINDAKİ FARKLAR

Özellik	TTP-Based Threat Hunting	Detection Engineering
Yaklaşım	Proaktif (Önleyici)	Reaktif (Otomatik Algılama)
Hedef	Belirli bir TTP'nin izlerini aramak	Algılama kuralları geliştirerek tehditleri tespit etmek
Kullanım Alanı	SOC, Mavi Takım, Tehdit Avcılığı	SIEM, IDS, EDR gibi güvenlik çözümleri
Örnek Araçlar	KQL, Splunk, Sysmon, Zeek	SIEM (Elastic, Splunk), Suricata, Snort
Örnek Olay	Windows Event ID 4624 ile anormal giriş denemeleri	LSASS bellek erişimi tespit eden SIEM kuralı

2022 UKRAİNE ELECTRİC POWER ATTACK (C0034) İNCELEMESİ

Bu saldırıda kullanılan teknikler ve TID değerleri aşağıdaki gibidir:

1. **Keşif (Reconnaissance)**
    - T1598.002: **Phishing for Information: Spearphishing Link**
    - T1595.002: **Active Scanning: Vulnerability Scanning**
2. **Başlangıç Erişimi (Initial Access)**
    - T1566.001: **Spearphishing Attachment**
    - T1078.003: **Valid Accounts: Local Accounts**
3. **Yanal Hareket (Lateral Movement)**
    - T1021.002: **Remote Services: SMB/Windows Admin Shares**
    - T1570: **Lateral Tool Transfer**
4. **Etki (Impact)**
    - T1499.001: **Endpoint Denial of Service: Application or System Exploitation**
    - T1489: **Service Stop**
5. **Komuta ve Kontrol (Command and Control)**
    - T1071.001: **Application Layer Protocol: Web Protocols**
    - T1095: **Non-Application Layer Protocol**

ŞİRKET HACKLENMESİ ÜZERİNE SENARYO

Bir finans şirketi, tehdit aktörleri tarafından hedef alınmıştır. Saldırganlar aşağıdaki adımları izleyerek şirketin sistemine sızmıştır:

1. Keşif (Reconnaissance)

Saldırganlar şirketin güvenlik açıklarını araştırarak bilgi toplamıştır.

- T1595.002: **Vulnerability Scanning**
- T1598.002: **Spearphishing Link**

2. Başlangıç Erişimi (Initial Access)

Sosyal mühendislik kullanarak bir çalışana zararlı dosya içeren bir e-posta gönderilmiştir.

- T1566.001: **Spearphishing Attachment**
- T1078.003: **Valid Accounts: Local Accounts**

3. Yanal Hareket (Lateral Movement)

Saldırgan, ağ içinde başka sistemlere erişim sağlamak için yetkili hesapları kullanmıştır.

- T1021.002: **Remote Services: SMB/Windows Admin Shares**
- T1570: **Lateral Tool Transfer**

4. Kalıcılık (Persistence)

Saldırgan, sistemde uzun süre kalmak için geri kapılar yerleştirmiştir.

- T1053.005: **Scheduled Task/Job: Scheduled Task**
- T1546.003: **Event Triggered Execution: Windows Management Instrumentation Event Subscription**

5. Etki (Impact)

Saldırganlar sistemin belirli bölümlerini devre dışı bırakmıştır.

- T1489: **Service Stop**
- T1499.001: **Endpoint Denial of Service: Application or System Exploitation**

6. Veri Çıkarma (Exfiltration)

Saldırganlar, ele geçirilen hassas verileri dışarıya sızdırmıştır.

- T1567.002: **Exfiltration Over Web Service**
- T1048.002: **Exfiltration Over Asymmetric Encrypted Non-C2 Protocol**

KAYNAKÇA

1. https://attack.mitre.org/
2. https://www.siberkavram.com/2020/09/mitreattackframework.html
3. https://www.fortinet.com/resources/cyberglossary/mitre-attck
4. https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e
5. https://www.ibm.com/think/topics/mitre-attack
6. https://chatgpt.com/
7. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/mitre-attack-framework/