MITRE ATT&CK Framework Raporu

Hazırlayan: Sema Nimet Ünal  
Tarih: 17.02.2025

İçindekiler

[1. Giriş 3](#_Toc190679715)

[2. MITRE ATT&CK Framework 3](#_Toc190679716)

[2.1 MITRE ATT&CK Tablosu Neden Önemlidir? 3](#_Toc190679717)

[2.2 MITRE ATT&CK Framework’de Bulunan Taktik ve Tekniklerin Önemi 3](#_Toc190679718)

[2.3 TTP Nedir? 3](#_Toc190679719)

[2.4 TTP-Based Threat Hunting ve Detection Engineering 3](#_Toc190679720)

[2.5 2022 Ukraine Electric Power Attack (C0034) İncelemesi 3](#_Toc190679721)

[2.6.1. Keşif (Reconnaissance) 5](#_Toc190679722)

[2.6.2. İlk Erişim (Initial Access) 5](#_Toc190679723)

[2.6.3. Kalıcılık (Persistence) 5](#_Toc190679724)

[2.6.4. Yetki Yükseltme (Privilege Escalation) 6](#_Toc190679725)

[2.6.5. Yanal Hareket (Lateral Movement) 6](#_Toc190679726)

[2.6.6. Komuta ve Kontrol (Command and Control) 6](#_Toc190679727)

[2.6.7. Etki (Impact) 6](#_Toc190679728)

[3. Sonuç 7](#_Toc190679729)

[4. Kaynakça 7](#_Toc190679730)

# 1. Giriş

Bu rapor, MITRE ATT&CK Framework’ün temel bileşenlerini ve kullanım alanlarını açıklamak amacıyla hazırlanmıştır. Siber güvenlik uzmanları için kritik bir kaynak olan MITRE ATT&CK, tehdit aktörlerinin saldırı yöntemlerini anlamada büyük bir rol oynar.

# 2. MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) saldırganların siber saldırılar sırasında kullandıkları taktikleri, teknikleri ve prosedürleri (TTP) içeren bir bilgi tabanıdır.

## 2.1 MITRE ATT&CK Tablosu Neden Önemlidir?

* Siber saldırıları anlamak ve analiz etmek için kullanılır.
* Tehdit avcılığı ve saldırı tespiti için güvenlik ekiplerine rehberlik eder.
* Kurumların tehdit modelleme süreçlerini geliştirmesine yardımcı olur.

## 2.2 MITRE ATT&CK Framework’de Bulunan Taktik ve Tekniklerin Önemi

* Taktikler: Saldırganların belirli hedeflere ulaşmak için izlediği ana adımlardır.
* Teknikler: Her taktik içinde saldırganların kullandığı belirli yöntemleri ifade eder.

## 2.3 TTP Nedir?

TTP (Tactics, Techniques, and Procedures) saldırganların belirli bir hedefe ulaşmak için izledikleri yolları tanımlayan bir kavramdır.

## 2.4 TTP-Based Threat Hunting ve Detection Engineering

* Threat Hunting: Sistemlerdeki şüpheli etkinlikleri proaktif olarak araştırma sürecidir.
* Detection Engineering: Güvenlik sistemleri için özel tespit kuralları geliştirme sürecidir.

## 2.5 2022 Ukraine Electric Power Attack (C0034) İncelemesi

Kampanya Açıklaması: 2022 yılında Ukrayna'nın enerji altyapısını hedef alan **Sandworm Team** tarafından gerçekleştirilen bu saldırı, kritik altyapıyı etkisiz hale getirmek için birden fazla teknik kullanmıştır. Saldırıda **GOGETTER, Neo-REGEORG, CaddyWiper** gibi zararlı yazılımlar ile birlikte **Living off the Land (LotL)** tekniklerinden yararlanılmıştır. Amaç, **Ukrayna elektrik şebekesini sabote ederek SCADA sistemleri üzerinden yetkisiz komutlar göndermek** ve operasyonel teknolojiyi kesintiye uğratmaktır.

**Kullanılan Teknikler (MITRE ATT&CK)**

| **TID** | **Taktik** | **Teknik** | **Açıklama** |
| --- | --- | --- | --- |
| **T1059.001** | Komuta ve Kontrol | **PowerShell Kullanımı** | Sandworm Team, **TANKTRAP** adında bir PowerShell aracı kullanarak kötü amaçlı yazılımı Windows Group Policy üzerinden dağıtmıştır. |
| **T1543.002** | Kalıcılık | **Systemd Servis Değişikliği** | GOGETTER kötü amaçlı yazılımının sistem açılışında çalışmasını sağlamak için **Systemd servis yapılandırmaları değiştirilmiştir**. |
| **T1485** | Etki | **Veri Silme (Data Wiping)** | **CaddyWiper** kötü amaçlı yazılımı, **OT sistemlerindeki kritik dosyaları, harici sürücüleri ve sistem disk bölümlerini silmek** için kullanılmıştır. |
| **T1484.001** | Kalıcılık | **Grup Politikası (GPO) Değiştirme** | Sandworm Team, kötü amaçlı yazılımın dağıtımı için **Windows Group Policy Object (GPO) ayarlarını değiştirmiştir**. |
| **T1570** | Yanal Hareket | **Lateral Tool Transfer** | **CaddyWiper’in çalıştırılabilir dosyası (msserver.exe)**, bir GPO aracılığıyla hedef sistemlere taşınmıştır. |
| **T1036.004** | Savunmadan Kaçınma | **Masquerade Task or Service** | GOGETTER, meşru görünen bir **Systemd hizmeti gibi gösterilerek gizlenmiştir**. |
| **T1095** | Komuta ve Kontrol | **Non-Application Layer Protocol** | **TLS tabanlı bir tünelleme tekniği** kullanılarak saldırganın uzaktan erişimi sağlanmıştır. |
| **T1572** | Komuta ve Kontrol | **Protokol Tünelleme** | **GOGETTER**, "Yamux" kullanarak **şifrelenmiş bir C2 kanalı** oluşturmuştur. |
| **T1053.005** | Yürütme | **Zamanlanmış Görev (Scheduled Task)** | CaddyWiper’ın belirli bir zamanda çalıştırılması için **GPO ile zamanlanmış görevler** oluşturulmuştur. |
| **T1505.003** | Kalıcılık | **Web Shell Kullanımı** | **Neo-REGEORG web shell**, dışarıdan komut yürütmek için internet üzerinden erişilebilen bir sunucuya yerleştirilmiştir. |
| **T0895** | Keşif | **Autorun Image** | SCADA sunucularında bir **ISO imajı (a.iso) bağlanarak otomatik olarak zararlı bir VBS betiği çalıştırılmıştır**. |
| **T0807** | Yürütme | **Komut Satırı Arayüzü (Command-Line Interface)** | Sandworm Team, **MicroSCADA SCIL-API’yi kullanarak scilc.exe komutlarını yürütmüştür**. |
| **T0853** | Yürütme | **Scripting** | **lun.vbs** adlı bir **VBS betiği, SCADA sistemlerinde zararlı komutları çalıştırmak için kullanılmıştır**. |
| **T0894** | Savunmadan Kaçınma | **Sistem Binary Proxy Kullanımı** | **MicroSCADA scilc.exe** dosyası ile **saldırgan tanımlı komutlar (s1.txt) yürütülmüştür**. |
| **T0855** | Etki | **Yetkisiz Komut Mesajı (Unauthorized Command Message)** | **MicroSCADA üzerinden substation cihazlarına yetkisiz komutlar gönderilmiştir**. |

2.6 Senaryo: X Şirketine Yönelik Siber Saldırı ve MITRE ATT&CK Analizi

X, uluslararası pazarda faaliyet gösteren büyük bir finansal teknoloji şirketidir. Şirket, müşteri bilgilerini içeren büyük veri tabanları, finansal işlem sistemleri ve uzaktan çalışanlar için bir VPN altyapısı gibi kritik sistemlere sahiptir. Ancak, gelişmiş bir tehdit aktörü (APT grubu), X şirketini hedef alarak aşamalı bir saldırı planı uygular.

Aşağıda, saldırının MITRE ATT&CK Framework kullanılarak analiz edilmiş aşamaları bulunmaktadır.

Saldırı Aşamaları ve Kullanılan Teknikler

## 2.6.1. Keşif (Reconnaissance)

Amaç: Şirket hakkında açık kaynaklardan bilgi toplamak, çalışanların e-posta adreslerini ve güvenlik açıklarını belirlemek.  
 Teknik: Açık Kaynak Taraması (OSINT) – T1595  
 Açıklama:

* Saldırgan, X'nin çalışanlarını ve altyapısını analiz etmek için LinkedIn, şirket web sitesi, GitHub ve Shodan gibi kaynakları kullanır.
* LinkedIn üzerinden X'nin BT ekibinde çalışan bazı kişileri belirler.
* Shodan kullanarak, X'nin dışa açık RDP (Remote Desktop Protocol) sunucularını ve eski yazılım sürümlerini tespit eder.

## 2.6.2. İlk Erişim (Initial Access)

Amaç: Hedef sisteme erişim sağlamak.  
 Teknik: Phishing – T1566  
 Açıklama:

* Saldırgan, X’nin BT yöneticisini taklit eden sahte bir e-posta hazırlar ve içerisine zararlı bir Excel makrosu ekler.
* "Acil! Şirket Politikaları Güncellemesi" başlıklı e-posta, şirket içi güvenlik duyurusu gibi gösterilerek çalışanlara gönderilir.
* Bir çalışan belgeyi açtığında, gizli bir PowerShell komutu çalıştırılarak saldırganın sistemine bağlantı kurulur.

## 2.6.3. Kalıcılık (Persistence)

Amaç: Sistemde kalıcı bir arka kapı oluşturmak.  
 Teknik: Kötü Amaçlı Makro (Malicious Macro) – T1204  
 Açıklama:

* Çalışan, phishing e-postasındaki dosyayı açtığında makrolar etkinleştirilir ve saldırganın yüklediği "Cobalt Strike" implantı çalıştırılır.
* Bu implant, saldırganın tekrar bağlantı kurabilmesi için bir arka kapı (backdoor) oluşturur.
* Aynı zamanda Windows Başlangıç klasörüne (Startup Folder) bir kötü amaçlı yürütülebilir dosya eklenerek saldırının kalıcı hale gelmesi sağlanır.

## 2.6.4. Yetki Yükseltme (Privilege Escalation)

Amaç: Yönetici (Admin) yetkilerine ulaşmak.  
 Teknik: Keşfedilmemiş Güvenlik Açıklarından Yararlanma – T1068  
 Açıklama:

* Saldırgan, sistemin eski bir Windows sürümü kullandığını fark eder.
* Çalıştırdığı "Mimikatz" aracıyla, sistemdeki hassas kimlik bilgilerini (NTLM Hashleri ve Kerberos Biletleri) çalar.
* Yerel yönetici hesaplarına erişim sağlayarak saldırıyı genişletir.

## 2.6.5. Yanal Hareket (Lateral Movement)

Amaç: Şirket içindeki diğer sistemlere erişmek ve saldırıyı yaymak.  
Teknik: RDP Kullanımı – T1076  
 Açıklama:

* Elde edilen yönetici kimlik bilgileriyle, şirketin merkezi dosya sunucusuna ve muhasebe departmanının makinelerine RDP üzerinden bağlanır.
* Ağ trafiğine yakalanmamak için meşru IT yönetim araçları (PsExec, WinRM) kullanarak sistemler arasında hareket eder.
* Şirketin yedekleme sunucularını ve kritik veri tabanlarını hedeflemeye başlar.

## 2.6.6. Komuta ve Kontrol (Command and Control)

Amaç: Şirket ağı dışındaki saldırganın komutlarını çalıştırmak.  
 Teknik: Gizli C2 (Command & Control) Tünelleme – T1572  
 Açıklama:

* Saldırgan, ağ trafiğini gizlemek için zararlı iletişimini DNS Tunneling ve HTTPS üzerinden şifrelenmiş bir C2 kanalı aracılığıyla yürütür.
* Siber güvenlik ekiplerinin izleme sistemlerinden kaçınmak için şirket içi meşru PowerShell komutları kullanılarak veri aktarımı gerçekleştirilir.

## 2.6.7. Etki (Impact)

Amaç: Şirketin işleyişini aksatmak ve fidye talep etmek.  
Teknik: Veri Şifreleme (Ransomware) – T1486  
 Açıklama:

* Saldırgan, tüm kritik dosyaları AES-256 ile şifreleyen bir fidye yazılımı (ransomware) çalıştırır.
* Şirketin tüm müşteri veritabanları, finansal belgeleri ve e-posta sunucuları şifrelenir.
* Sistem yöneticilerine, Bitcoin karşılığında şifre çözme anahtarının verileceğini belirten bir not bırakılır.

Bu senaryo, bir şirketin MITRE ATT&CK Framework kullanılarak nasıl hedef alınabileceğini göstermektedir. X şirketinin güvenlik açıklarını istismar eden tehdit aktörü:  
OSINT teknikleriyle hedef bilgisi topladı.  
 Phishing saldırısıyla başlangıç erişimi sağladı.  
 Yetki yükselterek yönetici seviyesine erişti.  
 Yanal hareketle tüm sisteme yayıldı.  
 Tüm kritik verileri şifreleyerek fidye talep etti.

Bu tür saldırıları önlemek için:  
Çalışanlar phishing saldırılarına karşı bilinçlendirilmeli.  
 Çok Faktörlü Kimlik Doğrulama (MFA): Hassas sistemlere erişim koruma altına alınmalı.  
 Güncellemeler: Yazılım ve sistemler düzenli olarak güncellenmeli.  
Ağ İzleme: Şüpheli aktiviteler için IDS/IPS sistemleri kullanılmalı.  
Yedekleme Stratejisi: Kritik verilerin offline yedekleri tutulmalı.

Bu saldırı, MITRE ATT&CK çerçevesine göre analiz edildiğinde, saldırganların hangi teknikleri hangi aşamalarda kullandığını net bir şekilde göstermektedir. Şirketler bu modelle kendi güvenlik stratejilerini oluşturabilir ve önleyici tedbirler alabilir.

# 3. Sonuç

Bu rapor, MITRE ATT&CK Framework’ü detaylı bir şekilde ele almıştır. Siber güvenlik uzmanlarının tehdit avcılığı ve tespit mühendisliği süreçlerinde bu modeli nasıl kullanabileceği açıklanmıştır. Senaryo çalışması ile MITRE ATT&CK tablosu kullanılarak bir siber saldırının nasıl analiz edileceği gösterilmiştir.

# 4. Kaynakça

1. <https://attack.mitre.org/>