MITRE ATT&CK

HAZIRLAYAN: HALİL İBRAHİM KORKUDAN

TARİH:17.02.2025

Giriş

Siber tehditlerin giderek daha karmaşık hale geldiği günümüzde, tehdit aktörlerinin kullandığı tekniklerin anlaşılması ve etkili savunma stratejilerinin geliştirilmesi kritik bir öneme sahiptir. Bu bağlamda, MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) çerçevesi, siber saldırganların kullandığı taktik ve teknikleri sistematik bir şekilde belgeleyen ve güvenlik ekiplerine yol gösteren bir model sunmaktadır (MITRE, 2023).

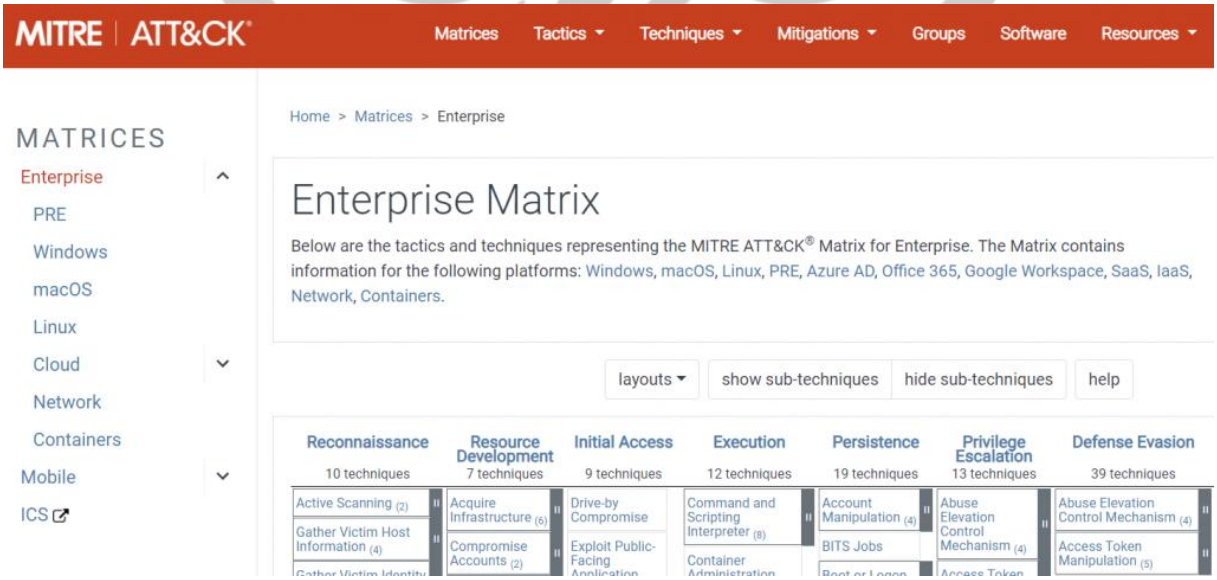
Siber tehditlerin sayısı ve karmaşıklığı arttıkça, savunma stratejileri de bu tehditlere uyum sağlamak zorundadır. Geleneksel antivirüs ve firewall sistemleri, gelişmiş siber saldırı tekniklerine karşı yetersiz kalabilmektedir. MITRE ATT&CK çerçevesi, bu noktada tehdit avcılığı (threat hunting), olay müdahalesi (incident response) ve algılama mühendisliği (detection engineering) gibi konularda yol gösterici olmaktadır.

Bu makalede, MITRE ATT&CK çerçevesinin temel bilesenleri, kullanım alanları, siber güvenlik alanındaki stratejik önemi ve pratik uygulamaları detaylı bir şekilde ele alınacaktır.

MITRE ATT&CK Nedir?

MITRE ATT&CK, tehdit aktörlerinin siber saldırılarında kullandığı taktik, teknik ve prosedürleri (TTP'ler) belgeleyen açık bir bilgi tabanıdır (MITRE, 2023). İlk olarak 2013 yılında MITRE Corporation tarafından geliştirilmiş olup, siber güvenlik uzmanlarına tehdit avcılığı (threat hunting), olay müdahalesi (incident response) ve savunma mekanizmalarını güçlendirme konusunda rehberlik etmektedir.

MITRE ATT&CK sistemi, organizasyonların siber tehditleri daha iyi anlamasını sağlayan detaylı bir yapı sunmaktadır. ATT&CK matrisi, farklı siber tehditleri ve saldırgan gruplarını belgeleyerek, siber güvenlik ekiplerinin daha etkili koruma stratejileri oluşturmasına yardımcı olmaktadır.

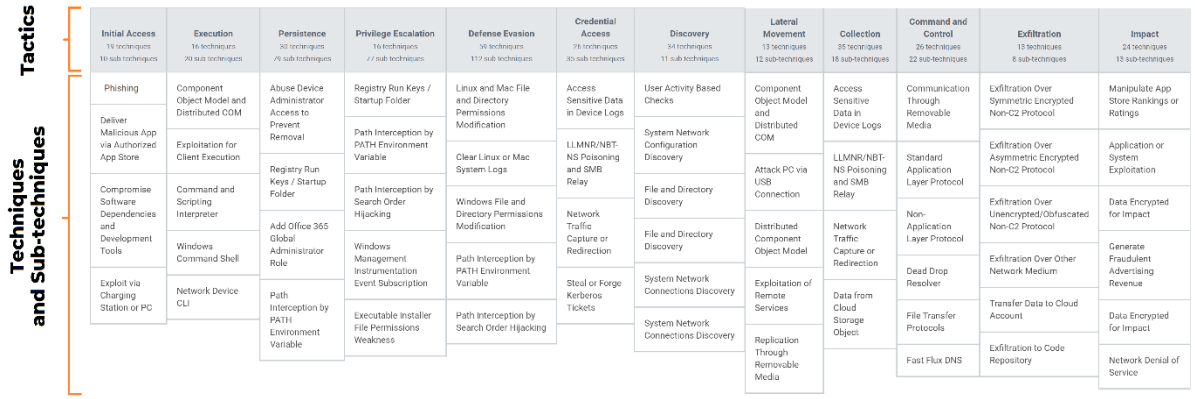


MITRE ATT&CK Matrisleri

MITRE ATT&CK çerçevesi, farklı operasyonel alanlara göre çeşitli matrisler sunmaktadır:

- Enterprise ATT&CK: Kurumsal sistemlere yönelik siber saldırıları analiz eder.
- Mobile ATT&CK: Mobil tehditleri ele alır ve Android/iOS zafiyetlerini inceler.
- ICS ATT&CK: Endüstriyel kontrol sistemlerine (ICS) yönelik siber tehditleri değerlendirir.
- PRE-ATT&CK: Saldırganların hedef belirleme ve bilgi toplama aşamalarına odaklanır.

Bu matrisler, farklı ortamlara ve tehdit türlerine yönelik özel yaklaşımlar geliştirmek için kullanılmaktadır. Örneğin, Mobile ATT&CK matrisi, mobil uygulamalardaki siber tehditleri analiz ederken, ICS ATT&CK matrisi, enerji santralleri ve fabrikalar gibi kritik altyapılara yönelik siber tehditleri değerlendirmek için kullanılır.



MITRE ATT&CK'ın Kullanım Alanları

MITRE ATT&CK çerçevesi, farklı siber güvenlik disiplinlerinde etkin bir şekilde kullanılmaktadır. Organizasyonlar, bu modeli kullanarak tehditleri belirleyebilir, savunmalarını geliştirebilir ve siber olaylara daha hızlı yanıt verebilir.

Tehdit Avcılığı (Threat Hunting)

Güvenlik ekipleri, MITRE ATT&CK veritabanını kullanarak tehdit aktörlerinin davranışlarını analiz edebilir ve potansiyel tehditleri önceden tespit edebilir.

Bu bağlamda, tehdit avcılığı, pasif izleme yerine aktif araştırma yöntemlerini benimseyerek, tehditlerin daha erken tespit edilmesini sağlar. Geleneksel antivirüs sistemlerinin algılayamayacağı sofistike siber saldırıları belirlemek için kullanılabilir.

Olay Müdahalesi (Incident Response)

Bir siber saldırı meydana geldiğinde, güvenlik ekipleri saldırının ne aşamada olduğunu belirlemek için MITRE ATT&CK çerçevesinden faydalanır. ATT&CK matrisi, olayın belirli

bir saldırı tekniğine mi dayandığını yoksa çok aşamalı bir saldırının parçası mı olduğunu anlamada yardımcı olur.

Savunma Geliştirme ve Risk Değerlendirme

MITRE ATT&CK, organizasyonların mevcut güvenlik önlemlerini değerlendirmesi ve savunma stratejilerini geliştirmesi için bir temel oluşturur. Siber güvenlik ekipleri, saldırı tekniklerine karşı özel olarak yapılandırılmış güvenlik kontrolleri uygulayarak sistemlerini daha dirençli hale getirebilirler.

Eğitim ve Farkındalık

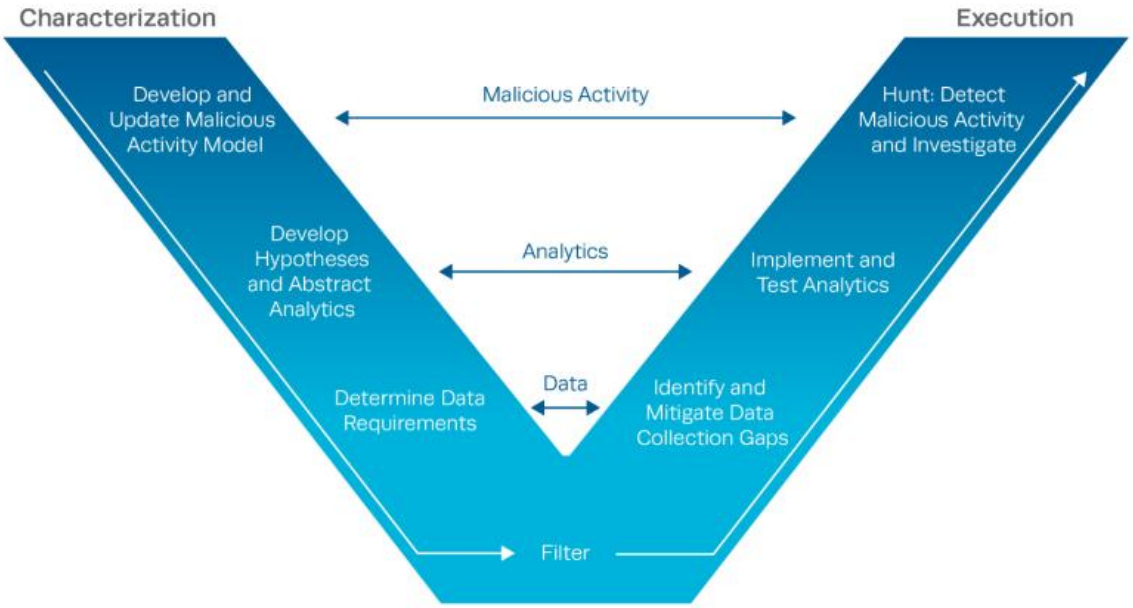
MITRE ATT&CK, siber güvenlik uzmanları için eğitim materyalleri sunarak tehdit aktörlerinin tekniklerini öğrenmelerini sağlar. Bu, özellikle kırmızı takım (red team) ve mavi takım (blue team) tatbikatlarında oldukça yararlıdır.

MITRE ATT&CK Tabanlı Algılama ve Tehdit Avcılığı

TTP-based Threat Hunting ve Detection Engineering, MITRE ATT&CK çerçevesinin siber tehditlerin erken tespit edilmesinde nasıl kullanılabileceğini ortaya koymaktadır.

TTP-Based Threat Hunting

Bu yöntem, tehdit avcılarının saldırganların izlediği belirli teknikleri ve prosedürleri tanımlayarak anormallikleri belirlemesini sağlar. SIEM (Security Information and Event Management) sistemleri ve EDR (Endpoint Detection and Response) çözümleri ile kullanılarak tehditlerin tespiti güçlendirilir.



Detection Engineering

Algılama mühendisliği, siber tehditlerin daha etkili tespit edilmesi için özel kurallar ve analiz yöntemleri geliştirme sürecidir. MITRE ATT&CK, saldırı tekniklerine dayalı olarak SIEM kurallarının oluşturulmasına yardımcı olur ve güvenlik olaylarının daha doğru sınıflandırılmasını sağlar.

2022 Ukrayna Elektrik Santrali Saldırısı

2022 yılında Sandworm grubu, Ukrayna'daki bir elektrik şirketinin SCADA sistemlerine yönelik büyük bir siber saldırı düzenledi. Bu saldırıda GOGETTER, Neo-REGEORG, CaddyWiper gibi zararlı yazılımlar ve Living off the Land (LotL) teknikleri kullanılarak sisteme yetkisiz erişim sağlandı.

SCADA sistemleri, enerji, su, petrol ve doğalgaz gibi kritik altyapıları uzaktan kontrol etmek için kullanılır. Bu nedenle, saldırının hedefi büyük bir kesintiye ve operasyonel kayıplara yol açabilecek kritik bir sistemdi.

Kullanılan Teknikler:

1. PowerShell Kullanımı (T1059.001) – Saldırganlar, PowerShell üzerinden zararlı komutlar çalıştırarak sistem üzerinde kontrol sağladı.
2. Systemd Servisleri (T1543.002) – Linux sistemlerinde GOGETTER zararlısının kalıcılığını sağlamak için Systemd ayarları değiştirildi.
3. Veri İmhası (T1485) – CaddyWiper kötü amaçlı yazılımı, SCADA ile ilgili dosyaları ve disk bölümlerini kalıcı olarak sildi.
4. Grup İlkesi Değiştirme (T1484.001) – Zararlı yazılımlar, Windows Group Policy (GPO) üzerinden dağıtıldı.
5. Lateral Hareket (T1570) – Kötü amaçlı yazılımlar, ağ içinde yayılmak için farklı sistemlere taşındı.
6. Gizlenme (T1036.004) – Zararlı yazılımlar, güvenilir sistem servisleri gibi gösterilerek tespit edilmekten kaçındı.
7. Komuta ve Kontrol (T1095, T1572) – Saldırganlar, güvenlik önlemlerini aşmak için şifrelenmiş tüneller aracılığıyla uzaktan erişim sağladı.
8. Zamanlanmış Görevler (T1053.005) – Zararlı yazılımlar belirli zamanlarda otomatik olarak çalıştırıldı.
9. Web Shell Kullanımı (T1505.003) – İnternet erişimi olan sunuculara web shell yüklenerek uzaktan erişim elde edildi.
10. ISO Görüntüsü ile Saldırı (T0895) – SCADA sistemine bağlı sanal makinelere, otomatik çalıştırılan kötü amaçlı ISO dosyaları yüklendi.
11. Komut Satırı Kullanımı (T0807) – SCADA sistemlerinde komut çalıştırmak için SCIL-API kullanıldı.
12. Betik Kullanımı (T0853) – Saldırganlar, PowerShell ve Visual Basic betikleriyle zararlı yazılımlarını çalıştırdı.
13. Yetkisiz Komut Mesajları (T0855) – SCADA sistemine yetkisiz komutlar gönderilerek uzaktaki trafolar kontrol edildi.

Havacılık ve Uzay Şirketine Yönelik APT Saldırısı Senaryosu

Senaryo Özeti:
Uluslararası rekabetin yoğun olduğu havacılık ve uzay sektöründe faaliyet gösteren, ileri teknoloji ürünleri geliştiren bir şirket, APT grubu tarafından hedef alınmaktadır. Saldırganlar, şirketin uçak tasarımı, uydu teknolojileri ve diğer stratejik verilerini ele geçirerek rakip ülkelere teknik ve ekonomik avantaj sağlamayı amaçlamaktadır.

Saldırı Aşamaları:

1. Keşif (Reconnaissance):
    - T1595 – Active Scanning:
      Saldırganlar, şirketin web siteleri, API'leri ve sunucularını aktif olarak tarayarak kullanılan teknolojiler, yazılımlar ve potansiyel güvenlik açıkları hakkında detaylı bilgi toplar.
    - T1589 – Gather Victim Identity Information:
      Sosyal medya, sektörel konferanslar ve sızdırılmış veritabanları üzerinden şirket çalışanlarının kimlik bilgileri ve iletişim detayları elde edilir.
2. Erişim Kazanma (Initial Access):
    - T1071.001 – Application Layer Protocol: Web Protocols:
      Şirketin müşterilere yönelik portalında bulunan bir güvenlik açığı kullanılarak sisteme ilk erişim sağlanır.
    - T1190 – Exploit Public-Facing Application:
      Kamuya açık bir web uygulaması veya API üzerindeki zafiyetten yararlanılarak, saldırganlar sisteme zararlı komutlar göndermeyi başarır.
3. Savunmadan Kaçınma (Defense Evasion):
    - T1564.003 – Impair Defenses: Time-Based Evasion:
      Saldırganlar, sistemdeki olağan trafik desenlerine uyum sağlayarak, belirli saat dilimlerinde saldırı aktivitelerini normal görünüme kavuşturur ve tespit riskini düşürür.
    - T1222 – File and Directory Permissions Modification:
      Kritik dosya ve dizin izinleri değiştirilerek, güvenlik yazılımlarının devre dışı bırakılması veya işlevlerinin bozulması sağlanır.
4. Yanal Hareket (Lateral Movement):
    - T1210 – Exploitation of Remote Services:
      Şirket içindeki diğer sistemlere ve Ar-Ge laboratuvarlarındaki bilgisayarlara erişim sağlamak amacıyla, uzaktan hizmetlerdeki güvenlik açıklarından faydalanılır.
    - T1091 – Replication Through Removable Media:
      Şirket bünyesinde kullanılan USB bellek ve benzeri taşınabilir medyalar aracılığıyla zararlı yazılım, iç ağa yayılır.

5. Etki (Impact):
    - T1489 – Service Stop:
      Üretim ve tasarım süreçlerini yöneten sunuculara yönelik hizmet durdurma komutları uygulanır; bu da şirketin operasyonel faaliyetlerinin kesintiye uğramasına yol açar.
    - T1491.001 – Defacement: Internal Defacement:
      Şirket içi iletişim platformlarında manipüle edilmiş mesajlar gösterilerek çalışanlar arasında korku ve panik yaratılır.
    - T1486 – Data Encrypted for Impact (Ransomware):
      Kritik tasarım ve proje verileri şifrelenir; fidye talep edilerek şirketin bilgi akışı kesintiye uğratılır.

MITRE ATT&CK Tekniği Tablosu

Aşama	Teknik	MITRE Kodu	Açıklama
Keşif	Active Scanning	T1595	Şirketin web siteleri, API'leri ve sunucuları aktif taranarak bilgi toplanır.
Keşif	Gather Victim Identity Information	T1589	Sosyal medya, konferanslar ve sızdırılmış veriler üzerinden çalışan bilgileri elde edilir.
Erişim Kazanma	Web Protocol Exploitation	T1071.001	Web tabanlı uygulamalarda bulunan güvenlik açıkları kullanılarak sisteme giriş sağlanır.
Erişim Kazanma	Exploit Public-Facing Application	T1190	Kamuya açık uygulamalardaki zaafiyetler istismar edilerek zararlı komutlar gönderilir.
Savunmadan Kaçınma	Time-Based Evasion	T1564.003	Saldırı aktiviteleri, normal trafik desenlerine uyum sağlayacak şekilde zamanlanır.
Savunmadan Kaçınma	File and Directory Permissions Modification	T1222	Kritik dosya izinleri değiştirilerek savunma mekanizmaları etkisiz hale getirilir.
Yanal Hareket	Exploitation of Remote Services	T1210	Uzak hizmetlerdeki açıklar kullanılarak şirket içindeki diğer sistemlere geçiş sağlanır.

Aşama	Teknik	MITRE Kodu	Açıklama
Yanal Hareket	Replication Through Removable Media	T1091	Taşınabilir medyalar (ör. USB bellek) aracılığıyla zararlı yazılım, iç ağa yayılır.
Etki	Service Stop	T1489	Üretim ve tasarım sunucularına hizmet durdurma komutları uygulanarak operasyonlar kesintiye uğrar.
Etki	Internal Defacement	T1491.001	Şirket içi iletişim kanallarında panik yaratacak manipüle edilmiş mesajlar gösterilir.
Etki	Data Encrypted for Impact (Ransomware)	T1486	Kritik veriler şifrelenerek fidye talep edilir, erişim engellenir.

Bu senaryo, havacılık ve uzay sektöründeki stratejik verilerin hedef alınması ve şirketin operasyonlarının kesintiye uğratılması üzerinden, APT gruplarının kullandığı MITRE ATT&CK tekniklerine dayanmaktadır. Her aşamada kullanılan teknikler, saldırganların hem erişim sağlamasını hem de verileri çalarak ya da sistemleri işlevsiz hale getirerek etki yaratmasını sağlamaktadır.

Sonuç

MITRE ATT&CK çerçevesi, siber güvenlik alanında sistemli ve proaktif bir yaklaşım sunarak tehdit aktörlerinin stratejilerini anlamada ve etkili savunma mekanizmaları geliştirmede kritik bir rol oynamaktadır. TTP-Based Threat Hunting ve Detection Engineering gibi yöntemlerle entegre edildiğinde, siber saldırılara karşı daha etkin koruma sağlanabilmektedir.

Bu makale, MITRE ATT&CK'ın temel yapısını ve uygulama alanlarını inceleyerek, siber güvenlik uzmanlarına bu modelin nasıl etkin kullanılabileceği konusunda yol göstermeyi amaçlamıştır.

Kaynaklar

- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*.
- https://docs.lumu.io/portal/en/kb/articles/attack-matrix
- https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html
- https://www.feroot.com/education-center/what-are-tactics-techniques-and-procedures-ttps/
- https://letsdefend.io/blog/how-to-become-a-detection-engineer
- https://attack.mitre.org/