ALTAY TAKIMI

Mitre Att&ack Framework
Pyramid of Pain

SEBAHATTİN GÖKCEN ÖZDEN
23/02/2025

Giriş

Bu rapor, siber güvenlik alanında önemli iki kavramı ve bir senaryo analizini incelemeyi hedeflemektedir: **Mitre ATT&CK Tablosu** ve **Pyramid of Pain Modeli**. Ayrıca, bir finans şirketine yönelik siber saldırı senaryosu üzerinden tehdit aktörlerinin davranışlarını ve bu tehditlere karşı alınabilecek önlemleri açıklamayı amaçlamaktadır.

- **Mitre ATT&CK Tablosu**, siber tehdit aktörlerinin kullandığı taktikleri, teknikleri ve prosedürleri (TTP'ler) sistematik bir şekilde belgeleyen bir çerçevedir. Güvenlik ekiplerine, tehditleri daha iyi anlama, tespit etme ve savunma stratejileri geliştirme imkanı sunar.

- **Pyramid of Pain Modeli**, tehdit göstergelerinin (Indicators of Compromise - IoC) zorluk derecesini ve saldırganlar için değiştirilme maliyetini hiyerarşik bir yapıda sınıflandırır. Bu model, savunmacıların daha etkili ve proaktif stratejiler geliştirmesine yardımcı olur.

- **Senaryo Analizi**, bir finans şirketinin hacklenme sürecini Mitre ATT&CK çerçevesine dayandırarak taktik ve teknikleri açıklayacak ve gerçek dünya uygulamalarını örnekleyecektir.

Raporun temel amacı, bu kavramları derinlemesine ele alarak siber güvenlik profesyonellerine rehberlik etmek ve tehditlerle mücadelede bilinçli yaklaşımlar sunmaktır.

1) Mitre ATT&CK Tablosu

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Tablosu, siber tehdit aktörlerinin gerçek dünyada kullandıkları taktikleri, teknikleri ve prosedürleri (TTP'ler) sistematik bir şekilde belgeleyen bir bilgi tabanı ve çerçevedir. MITRE Corporation tarafından geliştirilen bu tablo, siber saldırıların yaşam döngüsünü anlamak ve savunmayı geliştirmek için kullanılır. Tablo, genellikle bir matris formatında sunulur ve her sütun bir "taktik" (örneğin, İlk Erişim, Kalıcılık, Veri Çıkarma) temsil ederken, her taktiğin altında ilgili "teknikler" (örneğin, Phishing, Kaba Kuvvet Saldırısı) listelenir. TID (Technique ID) değerleri, her tekniğe özgü bir tanımlayıcıdır.

ATT&CK çerçevesi, işletim sistemlerine (Windows, Linux, macOS), platformlara (Mobil, Bulut) ve endüstriyel kontrol sistemlerine (ICS) göre farklı matrisler içerir.

2) Mitre ATT&CK Tablosunun Önemi

Mitre att&ack tablosu, siber güvenlik alanında çalışan profesyoneller veya siber güvenlik vakasını ele alanların atağın yapısını ve aşamasını anlamak için el kitabı niteliğindedir.
Tehdit aktörlerinin davranışlarını standardize ederek ekiplerin arasında iletişimi kolaylaştırır ve bu hızlı bir aksiyon imkanı sağlar. Bu da saldırganın kullandığı teknikleri tanıyarak proaktif savunmayı mümkün kılar.

Organizasyonların hangi taktik ve tekniklere karşı savunmasız olduğunu belirlemesine yardımcı olur. Bu gözlemleme proaktifliği kırmızı takım ve mavi takım egzersizlerini planlamak ve güvenlik açıklarını kapatmak için rehberlik yapar. Ayrıca mitre attack table gerçek dünya gözlemlerine dayalı olarak sürekli güncellenir ,bu da güncel tehditlere karşı hazırlıklı olmayı sağlar. Elinde bu yol haritası olan takımlar elbette tehditleri anlama ,tespit etme ve buna karşı savunma geliştirmek için avantaj sağlar.

3) Mitre Attack Framework' de Taktik ve Tekniklerin Önemi

Taktik, bir saldırganın neyi başarmaya çalıştığını (nedenini) temsil eder. Örneğin, "Credential Access" (Kimlik Bilgisi Erişimi), bir saldırganın sistemde daha fazla kontrol elde etmek için kimlik bilgilerini çalmaya çalıştığını gösterir.

Teknik ise; Taktiklerin nasıl gerçekleştirildiğini (yöntemini) açıklar. Örneğin, "Phishing" (T1566), kimlik bilgilerini çalmak için kullanılan bir tekniktir. Teknikler, savunucuların spesifik tehditlere karşı önlem almasını sağlar.

4) TTP

Taktikler, Teknikler ve Prosedürler (TTP) terimi, bir tehdit aktörünün davranışını ve bir siber saldırıyı yürütmek için yapılandırılmış bir çerçeveyi tanımlar. Aktörler, hacktivistler ve hobi bilgisayar korsanlarından özerk siber suçlulara, yeraltı çetelerine ve devlet destekli düşmanlara kadar değişebilir. TTP şu sorulara cevap verir neden, nasıl , ne şekilde. Taktik ,teknik ve prosedürler bu sorulara cevap verir.

5)TTP-Based Threat Hunting ve Detection Engineering

TTP-Based Threat Hunting: Tehdit avcılığı, mevcut güvenlik kontrollerini aşan tehditleri proaktif olarak aramaktır. TTP tabanlı tehdit avcılığı, Mitre ATT&CK çerçevesindeki taktik ve teknikleri rehber alarak ağda anormal davranışları veya potansiyel tehditleri tespit etmeyi amaçlar. Örneğin, "Credential Dumping" (T1003) tekniğini aramak için sistem logları incelenebilir.

Detection Engineering: TTP'lere dayalı tespit mühendisliği, att&ck çerçevesindeki teknikleri tespit edecek güvenlik algılama kuralları (örneğin, SIEM kuralları) tasarlamayı ve optimize etmeyi içerir. Bu, tehditlerin otomatik olarak algılanmasını sağlar.

6)2022 Ukraine Electric Power Attack (C0034) İncelemesi

Tactic: Initial Access (İlk Erişim)

- **Technique: Supply Chain Compromise (T1195) - TID: T1195**
  - Saldırganlar, Ukrayna'daki enerji şirketlerinin tedarik zincirine sızarak kötü amaçlı yazılım dağıttı.

Tactic: Execution (Yürütme)

- **Technique: Command and Scripting Interpreter (T1059) - TID: T1059**
  - Kötü amaçlı komut dosyaları kullanılarak sistemlerde kod çalıştırıldı.

Tactic: Persistence (Kalıcılık)

- **Technique: Boot or Logon Autostart Execution (T1547)** - TID: T1547
  - Sistem yeniden başlatıldığında otomatik olarak çalışacak mekanizmalar oluşturuldu.

Tactic: Command and Control (Komuta ve Kontrol)

- **Technique: Application Layer Protocol (T1071)** - TID: T1071
  - Saldırganlar, C2 sunucularıyla iletişim kurmak için HTTP gibi protokoller kullandı.

Tactic: Impact (Etki)

- **Technique: Service Stop (T1489)** - TID: T1489
  - Elektrik şebekesinin çalışmasını durdurmak için hizmetler devre dışı bırakıldı.

7) Şirket Hacklemek

Senaryoda bir sigorta şirketini hayal edelim oldukça popüler ve güçlü.Motivasyonum da kanser hastası eşimin masraflarını karşılamayı red etmesi. Bu duygusal açıdan olabilecek tüm riskleri göze almalı sağlıyor.

1.Keşif aşaması

1.1 Active Scanning -TID:T1595 & T1594
Şirketin ağını tarayarak açık portları ve hizmetleri ve şirkete bağlı diğer alt hizmetlerin varlığını araştırırım.

1.2 Bilgi Toplama -TID: T1591
OSINT'in kalbi linkedin aracılığı ile çalışanlar ve organizasyon yapısı hakkında bilgi toplarım.

2.İlk Erişim

2.1 Pishing -TID:T1566
Çalışanlara sahte e-postalar göndererek kötü amaçlı bir malware indirmelerini sağlarım

2.2 Uygulama istismarı- TID: T1190
Şirketin web uygulamasındaki bir güvenlik açığı kullanarak erişim sağlama yöntemini denerim.

3.Kalıcılık

3.1 Hesap Oluşturma -TID: T1136
Sistemde kalıcı erişim için yeni bir yönetici hesabı oluştururum.

3.2 Zamanlanmış Görev -TID:T1053
Kötü amaçlı yazılımın düzenli çalışması için bir zamanlanmış görev eklenir.

4.Kimlik Bilgisi Erişimi

4.1 Kimlik Dökümü -TID:T10003
SAM dosyasından kimlik bilgileri çalınır.

4.2 Brute Force -TID : 1110
Zayıf parolalara sahip hesaplara erişim sağlamak için kaba kuvvet saldırısı da değerlendirilir.

5.Veri Çıkarma

5.1 C2 üzerinden çıkarma - TID:T1041
Çalınan veriler , komuta ve kontrol sunucusuna HTTP üzerinden gönderilir.

5.2 Veri Şifreleme - TID:T1486
Veriler şifrelendi ve fidye talep edildi.

8. Pyramid of Pain

Pyramid of Pain (Acı Piramidi), David J. Bianco tarafından geliştirilen bir modeldir ve siber güvenlikte tehdit göstergelerinin (Indicators of Compromise - IoC) tespit edilme zorluğunu ve

saldırganlar için değiştirilme maliyetini hiyerarşik olarak sınıflandırır. Piramit, tabandan tepeye doğru zorluk derecesini artırır.

Pyramid of Pain Seviyeleri

1. Hash Değerleri

   Tanım: Kötü amaçlı dosyaların benzersiz kimlikleri (örneğin, MD5, SHA-1).

   Kolaylık: Tespit edilmesi ve engellenmesi kolaydır.

   Saldırgan için Maliyet: Dosyayı hafifçe değiştirerek hash değeri kolayca değiştirilebilir.

   Örnek: Bir virüsün hash'ini engellemek.

2. IP Adresleri

   Tanım: Saldırganın kullandığı sunucuların IP'leri.

   Kolaylık: Firewall kurallarıyla engellenebilir.

   Saldırgan için Maliyet: Yeni bir IP almak nispeten kolaydır.

   Örnek: C2 sunucusunun IP'sini bloklamak.

3. Alan Adları

   Tanım: Saldırganın kullandığı sunucuların IP'leri.

   Kolaylık: Firewall kurallarıyla engellenebilir.

   Saldırgan için Maliyet: Yeni bir IP almak nispeten kolaydır.

   Örnek: C2 sunucusunun IP'sini bloklamak.

4. Ağ/Host Eserler

   Tanım: Saldırı sırasında bırakılan izler (örneğin, HTTP başlıkları).

   Kolaylık: Daha spesifik tespit gerektirir.

   Saldırgan için Maliyet: Değiştirmek daha fazla çaba gerektirir.

   Örnek: Belirli bir User-Agent dizesini izlemek.

5. Araçlar

   Tanım: Saldırganın kullandığı yazılım veya araçlar (örneğin, Mimikatz).

   Kolaylık: Araçların davranışlarını tespit etmek zordur.

Saldırgan için Maliyet: Yeni bir araç geliştirmek veya değiştirmek zaman alır.

Örnek: Mimikatz kullanımını tespit etmek.

6.TTPs

Tanım: Saldırganın davranış modelleri (örneğin, Credential Dumping).

Kolaylık: Tespit edilmesi en zordur, ancak en değerli bilgiyi sağlar.

Saldırgan için Maliyet: TTP'leri değiştirmek, operasyonel stratejiyi tamamen yenilemeyi gerektirir.

Örnek: Phishing ile kimlik avı yapıldığını tespit etmek.

Pyramid of Pain'in Önemi

- **Savunmacılar için:** Piramidin üst seviyelerine odaklanmak (örneğin, TTP'ler), saldırganları daha etkili bir şekilde durdurur, çünkü bu seviyelerde değişiklik yapmak onlar için maliyetlidir.
- **Saldırganlar için:** Alt seviyelerdeki göstergeleri (hash, IP) değiştirmek kolay olduğundan, savunmacıların yalnızca bunlara odaklanması etkisizdir.
- **Stratejik Kullanım:** Mitre ATT&CK ile birleştirildiğinde, TTP'lere odaklanarak uzun vadeli savunma stratejileri geliştirilebilir.

Sonuç

Yapılan analiz ve araştırmalar sonucunda aşağıdaki önemli bulgular elde edilmiştir:

- **Mitre ATT&CK Tablosu'nun Katkıları**: Bu çerçeve, siber güvenlik ekipleri için standardize edilmiş bir dil sağlayarak ekipler arası iletişimi kolaylaştırmaktadır. Tehdit avcılığı ve tespit mühendisliği süreçlerinde kritik bir rol oynar; tehditlerin sistematik bir şekilde analiz edilmesine ve proaktif savunma stratejilerinin oluşturulmasına olanak tanır.
- **Pyramid of Pain Modeli'nin Önemi**: Model, savunmacıların tehditlere karşı daha sofistike ve uzun vadeli yaklaşımlar benimsemesini teşvik eder. Özellikle piramidin üst seviyelerinde yer alan TTP'lere (Taktikler, Teknikler ve Prosedürler) odaklanmak, saldırganların operasyonlarını ciddi şekilde zorlaştırır ve savunmayı güçlendirir.
- **Senaryo Analizinden Çıkarımlar**: Finans şirketi hacklenme senaryosu, tehdit aktörlerinin keşif, erişim sağlama, veri çalma ve fidye talebi gibi sofistike yöntemlerini gözler önüne sermiştir. Bu analiz, Mitre ATT&CK çerçevesinin pratik kullanımını ve alınabilecek önlemleri net bir şekilde ortaya koymuştur.

Bu bilgiler, siber güvenlik profesyonellerinin tehditlerle mücadelede daha bilinçli ve etkili stratejiler geliştirmelerine katkı sağlayacak niteliktedir.

REFERANSLAR

1.) https://attack.mitre.org/
2.) https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
3.) https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
4.) https://www.sans.org/white-papers/