MITRE ATT&CK FRAMEWORK

ALTAY

HAZIRLAYAN: UMUT EMRE KARACAER
TARİH: 17.02.2025

İÇERİK

GİRİŞ:

Günümüz siber tehdit ortamında, gelişmiş saldırı grupları (APT) ve bireysel tehdit aktörleri, şirketlere ve kritik altyapılara zarar vermek amacıyla karmaşık teknikler kullanmaktadır. MITRE ATT&CK Framework, bu saldırıları daha iyi anlamak, analiz etmek ve savunma stratejileri geliştirmek için oluşturulmuş kapsamlı bir bilgi tabanıdır.

Bu raporda, MITRE ATT&CK çerçevesinde siber saldırı taktik ve teknikleri detaylı şekilde ele alınarak, gerçek dünyadan bir örnek olay olan 2022 Ukraine Electric Power Attack (C0034) incelenmiştir. Ayrıca, kurumsal bir şirket olan "X" Şirketi'ne yönelik kurgusal bir siber saldırı senaryosu oluşturularak, saldırganların keşif aşamasından sistem üzerinde kalıcılık sağlamasına ve nihai zarar verme aşamasına kadar izlediği yol haritası analiz edilmiştir.

Raporda, MITRE ATT&CK'ün sunduğu taktik ve teknikler detaylandırılmış, TTP (Tactics, Techniques, and Procedures) tabanlı tehdit avcılığı ve tespit mühendisliği konuları ele alınmış ve APT gruplarının oluşturduğu tehditler ile korunma yöntemleri tartışılmıştır.

Bu çalışma, güvenlik uzmanlarına siber tehditleri anlamada rehberlik etmeyi, saldırı vektörlerini daha iyi analiz etmeyi ve etkin bir savunma stratejisi geliştirmeyi amaçlamaktadır.

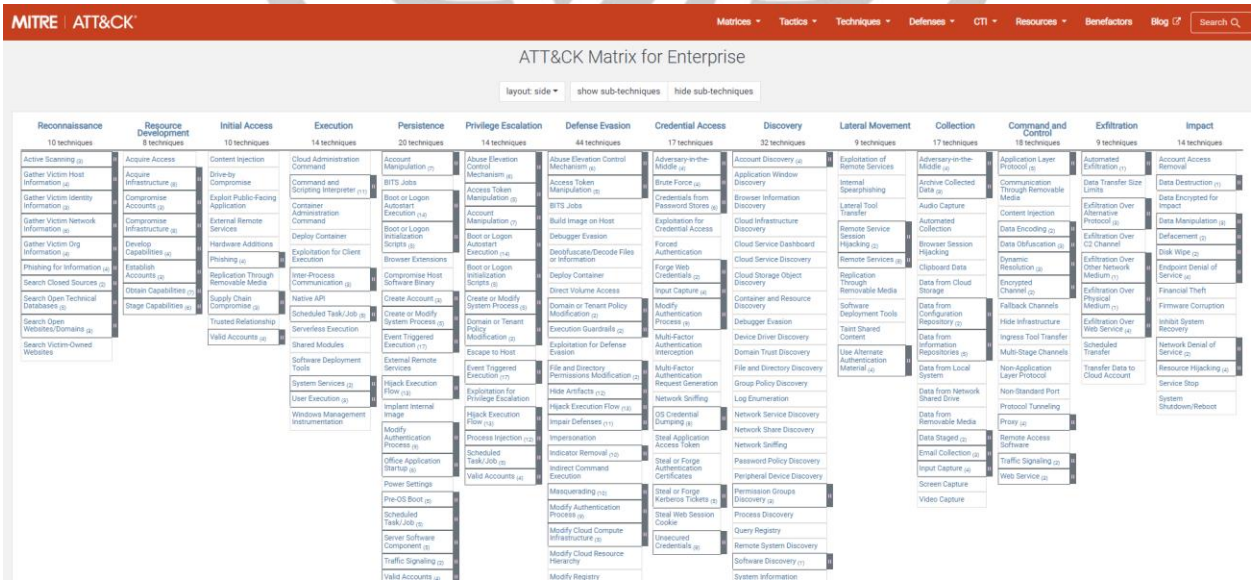
MITRE ATT&CK FRAMEWORK NEDİR?:

MITRE ATT&CK Framework, siber güvenlik alanında saldırganların kullandığı taktikleri, teknikleri ve ortak bilgiyi tanımlamak için kullanılan bir bilgi tabanıdır. **MITRE Corporation** tarafından geliştirilmiştir. Framework, savunma ve saldırı taraflarına, güvenlik uzmanlarına ve siber güvenlik araştırmacılarına yardımcı olmak için tasarlanmıştır.

MITRE ATT&CK Framework'un temel amacı, savunma taraflarının saldırganların kullanabileceği taktikleri ve teknikleri anlamalarına ve siber saldırılarla mücadele ederken daha etkili olmalarına yardımcı olmaktır. Bu şekilde, güvenlik uzmanları ve kurumlar, siber saldırılara karşı daha iyi savunma stratejileri geliştirebilir ve olası saldırıları tespit ve önleme konusunda daha proaktif bir tutum alabilirler.

MITRE ATT&CK, sürecin her adımını detaylandırarak savunma ekiplerine rehberlik eder. Yani, bir saldırganın kullandığı her teknik bir **TID** (Teknik Kimlik Numarası) ile tanımlanır. Mesela, T1059.001 (PowerShell Kullanımı), saldırganın sistemde kötü amaçlı komutlar çalıştırmasını ifade eder.

Bu çerçeve, SOC analistleri, siber güvenlik uzmanları ve kırmızı/mavi takım çalışmaları için çok önemlidir çünkü hangi saldırı tekniklerinin tespit edilmesi gerektiğini anlamalarına yardımcı olur.



MITRE ATT&CK TABLOSU NEDEN ÖNEMLİDİR?:

1. Saldırıları Daha İyi Anlamayı Sağlar:

MITRE ATT&CK, saldırganların izlediği adımları taktikler ve teknikler halinde tanımlar. Bir saldırının nasıl başladığını, nasıl ilerlediğini ve ne tür zararlar verebileceğini göstererek güvenlik ekiplerinin olayları daha iyi anlamasına yardımcı olur.

2. Tehdit Avı (Threat Hunting) ve Tespit Mekanizmalarını Geliştirir:

SOC ekipleri ve güvenlik analistleri, MITRE ATT&CK tablosunu kullanarak sistemde anormal davranışları tespit edebilir. Örneğin, bir saldırgan T1078 (Geçerli Kullanıcı Hesaplarını Ele Geçirme) tekniğini kullanıyorsa, SIEM sistemleri buna karşı özel kurallar yazabilir.

3. Siber Savunma Stratejilerini Güçlendirir:

Şirketler, MITRE ATT&CK kullanarak zayıf noktalarını belirleyebilir ve eksik olan güvenlik önlemlerini tamamlayabilir. Örneğin, bir firma T1566 (Oltalama Saldırıları - Phishing) saldırılarına karşı çalışan eğitimlerini artırabilir ve e-posta filtrelerini geliştirebilir.

4. Kırmızı ve Mavi Takım Çalışmalarına Kılavuzluk Eder:

Kırmızı Takım (Red Team): Saldırgan gibi düşünüp zafiyetleri test eden ekipler, MITRE ATT&CK tablosundan ilham alarak gerçek saldırı senaryoları oluşturabilir.
Mavi Takım (Blue Team): Savunma ekipleri, belirlenen saldırı tekniklerine karşı önlem alabilir ve saldırı tespit sistemlerini güçlendirebilir.

5. Standart Bir Tehdit Modeli Sunar:

MITRE ATT&CK, tüm güvenlik ekiplerinin aynı dili konuşmasını sağlar. Örneğin, bir SOC analisti "Saldırgan T1059 (Komut Satırı Kullanımı) tekniğini kullanarak zararlı PowerShell çalıştırdı" dediğinde, herkes ne demek istediğini anlayabilir.

6. Tehdit Aktörlerini ve Kampanyaları Analiz Etmeye Yardımcı Olur:

MITRE ATT&CK, belirli hacker gruplarının (APT grupları gibi) hangi teknikleri kullandığını belgeler. Örneğin, APT29 (Cozy Bear) grubu genellikle TTP'leri arasında T1071.001 (Web Protokolleri Kullanımı) yöntemini kullanır. Bu bilgi, belirli saldırılara karşı savunma mekanizmalarını güçlendirmek için kullanılabilir.

MITRE ATT&CK TABLOSU TAKTİKLER VE TEKNİKLER:

MITRE ATT&CK Framework, saldırganların siber saldırıları nasıl gerçekleştirdiğini anlamamızı sağlayan kapsamlı bir modeldir. Bu framework içinde taktikler ve teknikler, bir saldırının adım adım nasıl ilerlediğini gösterir ve siber güvenlik ekiplerine tehditleri tespit etme, analiz etme ve engelleme konusunda rehberlik eder.

Siber saldırganların bir şirkete sızarken izlediği belirli adımlar vardır. İşte bu adımları, yani taktikleri ve kullanılan bazı teknikleri, adım adım anlatacağım. Bunu bir hırsızın bir eve girmesi gibi düşünelim.

1. Keşif (Reconnaissance) – "Önce Eve Göz At":

Saldırgan, sistemde alacağı aksiyonlarda kullanabileceği tüm bilgileri toplamaya çalıştığı evredir. Bu evrede hedefleri doğrultusunda sistem hakkında aktif ve pasif bilgi toplayacaktır.

Pasif Bilgi Toplama;

Hedef sisteme doğrudan erişim sağlanmadan internet üzerindeki servislerden veya bilgi almak için web sitelerini kullanarak hedef sistem hakkında bilgi toplama yöntemidir.

Aktif Bilgi Toplama;

Hedef sisteme doğrudan erişim ya da tarama ile yapılan bilgi toplama tekniğidir. Sistem ile etkileşime geçildiğinden izin alınmadan yapılan bir bilgi toplama girişimi, Türk Ceza Kanunu 243. maddesi uyarınca bilişim suçu olarak kabul edilmektedir. Aktif bilgi toplanan sistem bilgilerine; bilişim sisteminin altyapı ve personel bilgileri gibi hassas verilerini içerebilmektedir.

Bir hırsız bir eve girmeden önce etrafı inceler. Güvenlik kamerası var mı? Kapılar kilitli mi? Evde biri var mı?

Siber saldırganlar da aynı şekilde önce hedeflerini analiz eder.

- Açık portları tararlar.
- Çalışanların sosyal medya hesaplarını incelerler.
- Kimlerin hangi sistemlere erişimi olduğunu öğrenmeye çalışırlar.

Örnek Teknikler:

- T1595 (Ağ Servislerini Keşfetme) → Şirketin açık sunucularını ve portlarını taramak için Nmap gibi araçlar kullanılır.
- T1598 (Kimlik Avı ile Bilgi Toplama) → LinkedIn'den çalışanları bulup hedefli oltalama (phishing) saldırıları düzenlenebilir.

2.Kaynak Geliştirme (Resource Development) – "Hırsızlık İçin Araçları Hazırla":

Kaynak Geliştirme, saldırganların hedeflerini destekleyici konumda kullanabileceği kaynakları oluşturmasını sağlayan tekniklerden oluştuğu evredir. Bu kaynaklar saldırganın sistemdeki kontrolünü desteklemek için gerekli altyapının desteklenmesi, sunucu ve ağ hizmetleri, hesap işlemleri de dahildir.

Hırsız eve girmeden önce bazı hazırlıklar yapar: Sahte anahtar, eldiven, çalıntı kimlik… Saldırganlar da benzer şekilde saldırıya geçmeden önce bazı kaynakları hazırlar:

- Sahte web siteleri oluştururlar.
- Ele geçirilmiş e-posta hesapları kullanırlar.
- Botnetler veya kötü amaçlı yazılımlar hazırlarlar.

Örnek Teknikler:

- T1583 (Kötü Amaçlı Alan Adları Kaydetme) → Saldırgan, çalışanları kandırmak için şirketin resmi web sitesine çok benzeyen bir alan adı alır (örneğin: g00gle.com).
- T1584 (Sahte Sosyal Medya Hesapları Açma) → Şirketin BT yöneticisi gibi görünen sahte hesaplarla çalışanlara mesaj atarlar.

3.İlk Erişim (Initial Access) – "Eve Girme Yöntemini Bul":

Bir ağ veya sistemde ilk erişimi elde etmek için çeşitli giriş vektörlerini kullanan tekniklerden oluşur. Bu evrede saldırgan, hedefli kimlik avı ve halka açık web sunucuları gibi çeşitli sistemlerin zafiyetlerden yararlanarak erişim sağlayabilir.

Şimdi hırsız eve girmeye çalışıyor. Kapıyı açmak için birkaç yöntemi var:

- Kapıyı açık unutan birini bulup içeri girmek (şifresi zayıf olan hesapları hacklemek)
- Pencereyi kırmak (sistemdeki bir açığı kullanmak)
- Bir çalışana kendini postacı gibi tanıtıp kapıyı açtırmak (oltalama saldırısı)

Örnek Teknikler:

- T1566 (Oltalama - Phishing) → Çalışana "Hesabınızın şifresi sıfırlandı, buraya tıklayın" şeklinde bir e-posta gönderilir.
- T1190 (Web Açıklarından Yararlanma) → Eğer şirketin web sitesinde bir güvenlik açığı varsa, bu açık kullanılarak sisteme sızılabilir.

4.Çalıştırma (Execution) – "Evde Dolaşmaya Başla":

Saldırganın, lokal veya uzak bir sistemde kodun çalıştırılmasına neden olan tekniklerden oluşur. Kötü amaçlı kod çalıştıran teknikler, bir ağı keşfetmek veya veri sızıntısı gibi daha geniş hedeflere ulaşmak için genellikle diğer tüm taktiklerden gelen tekniklerle eşleştirilir.

Hırsız içeri girdikten sonra artık bazı şeyleri çalıştırması gerekiyor:

- Işıkları kapatıp güvenlik kamerasını devre dışı bırakmak (antivirüsü kapatmak)
- Şifreli dolapları açmak için bir alet kullanmak (PowerShell çalıştırmak)

Örnek Teknikler:

- T1059 (Komut Satırı Kullanımı) → Windows PowerShell veya Linux komut satırı ile kötü amaçlı komutlar çalıştırmak.
- T1203 (Ofis Makroları Kullanımı) → Bir çalışana kötü amaçlı bir Word dosyası gönderip, içindeki makroyu çalıştırmasını sağlamak.

5.Kalıcılık (Persistence) – "Eve Geri Dönebilmek İçin İz Bırak":

Saldırganın, eriştiği sisteme olan erişiminin sona ermemesi ve sistemde olan ilerleyişini devam ettirebilmesi için kullandığı çeşitli tekniklerin uygulandığı evredir. Örneğin sisteme bulaştırdığı zararlı bir yazılım ile makinenin her başlangıcında sistemde saldırganın da yetki sahibi olmasını sağlayabilir, kimlik bilgilerini değiştirebilir ve mevcut erişimi engelleyici faaliyetlerde bulunabilmektedir.

Hırsız eve girip çıktığında, bir daha kolayca geri dönebilmek için önlem alır:

- Anahtar kopyası yapar (arka kapı bırakır)
- Eve girmenin başka yollarını belirler (çalışanın şifresini çalar)

Örnek Teknikler:

- T1547 (Başlangıçta Çalışan Programlar Eklemek) → Bilgisayar her açıldığında zararlı yazılımın çalışmasını sağlamak.
- T1136 (Sistemde Yeni Hesap Açmak) → Yetkili bir hesap oluşturarak sisteme daha sonra tekrar girebilmek.

6.Yetki Yükseltme (Privilege Escalation) – "Evin Sahibi Gibi Davran":

Saldırganın eriştiği sistemde mevcut yetkisini yükseltmeyi amaçlayan teknikleri içerir. Bulunduğu sistemde almayı hedeflediği aksiyonlar için bazı yetki ve izinlere ihtiyaç duyacaktır. Bu noktada; sistem zayıflıklarından, yanlış yapılandırmalardan ve güvenlik açıklarından yararlanacaktır.

Şimdi hırsız sadece içeri girmekle yetinmiyor, evin anahtarlarını istiyor!

- Çilingir gibi davranıp anahtarları çoğaltıyor (admin yetkisi kazanıyor)
- Dolapları açmak için şifreleri ele geçiriyor (kullanıcı haklarını artırıyor)

Örnek Teknikler:

- T1055 (Kod Enjeksiyonu) → Başka bir güvenilir programın içine kötü amaçlı kod enjekte etmek.
- T1134 (Yetki Devir Alma) → Daha yüksek yetkilere sahip başka bir hesap üzerinden işlem yapmak.

7.Savunmadan Kaçınma (Defense Evasion) – "Gizlenmek İçin Önlemler Al":

Saldırganın, sistem için alınan güvenlik önlemlerini atlatmasını sağlayan teknikleri içerir. Bu evrede savunmadan kaçınması için kullanılan teknikler arasında; güvenlik yazılımının kaldırılması/devre dışı bırakılması veya veri ve komut dosyalarının gizlenmesi/şifrelenmesi yer almaktadır.

- SYSTEM/root yetkisi
- Local admin yetkisi
- Yönetici erişimine sahip gibi görünen kullanıcı hesabı

Belirli bir sisteme erişimi olan veya işlevi yerine getiren kullanıcı hesapları, yükseltilmiş yetki örneklerinden bazılarıdır.

Hırsız, yakalanmamak için bazı önlemler alır:

- Parmak izi bırakmamak için eldiven giyer (log kayıtlarını siler)
- Güvenlik kameralarını devre dışı bırakır (antivirüsü kapatır)

Örnek Teknikler:

- T1070 (Logları Silmek) → Olay kayıtlarını ve izleri temizlemek.
- T1562 (Antivirüsü Devre Dışı Bırakmak) → Güvenlik yazılımını kapatmak.

8.Kimlik Bilgilerini Toplama (Credential Access) – "Evin Kasasını Açmak":

Saldırganın hesap kulanıcı adı ve parola bilgisi gibi gizli olan erişim bilgilerini çalma tekniklerinin kullanıldığı evredir. Saldırgan bilgileri elde edilmeye çalışırken keylogging, Brute Force saldırısı, parola yöneticisi alanlarına gerçekleştireceği ataklar ile kimlik bilgisi dökümü elde etmeyi hedefler. Aynı zamanda MFA pasifleştirme, web sitesi cookie bilgilerini çalma ve ağ koklama yöntemlerini de hedefi doğrultusunda kullanması mümkündür.

Hırsız eve girdikten sonra kasayı açmak isteyebilir. Şifreleri çalarsa, evin ana sahibinden farksız olur. Siber saldırganlar da sistemlerdeki şifreleri, kimlik bilgilerini ve anahtarları ele geçirmek için farklı teknikler kullanır.

Örnek Teknikler:

- T1003 (LSASS Bellek Dökümü ile Şifre Çalma) → Windows işletim sisteminde Mimikatz gibi araçlarla RAM'den şifreleri almak.
- T1555 (Tarayıcıda Kayıtlı Şifreleri Çekmek) → Kullanıcıların tarayıcılarında sakladıkları şifreleri ele geçirmek.

9.Keşif (Discovery) – "Evin Planını Çıkarmak":

Saldırganın, hedeflemiş olduğu sistem ve ağ hakkında bilgi edinmesi için kullanacağı tekniklerden oluşan evredir. Saldırganın sistemde bulunan mevcut hesaplara, güvenlik yazılımlarına ve sistem bilgilerine ait incelemede ve keşifte bulunduğu evredir.

Hırsız içeri girdikten sonra nerede ne var öğrenmek için evi dolaşır. Siber saldırgan da ağ içinde keşif yaparak hangi cihazların bağlı olduğunu, kimlerin oturum açtığını ve nerede hassas veriler olduğunu anlamaya çalışır.

Örnek Teknikler:

- T1087 (Kullanıcı Hesaplarını Keşfetme) → Sistemde kimlerin oturum açtığını görmek için net user gibi komutlar kullanmak.
- T1018 (Ağ Topolojisini Keşfetmek) → Şirketin ağı içinde hangi sistemlerin bulunduğunu anlamak için taramalar yapmak.

10.Yanal Hareket (Lateral Movement) – "Evin Diğer Odalarına Geç":

Saldırganın hedefleri doğrultusunda ağda ilerlemesini sağlayan teknikleri içerir. Yanal Hareketi gerçekleştirmek için saldırganın kendi uzaktan erişim araçlarını kurması, daha gizli olabilecek yerel ağ ve işletim sistemi araçlarıyla meşru kimlik bilgilerini kullanması mümkündür. SSH ve RDP protokollerinin ele geçirilmesi, Windows uzaktan yönetimi, uzak hizmet oturumu ele geçirilmesi mümkündür.

Hırsız artık mutfaktan çıkıp yatak odasına geçmek istiyor. Şimdi, eve tek bir noktadan değil, farklı odalardan da erişim sağlaması gerekiyor.

Örnek Teknikler:

- T1021 (Uzak Masaüstü Protokolü - RDP Kullanımı) → Ele geçirilen bir bilgisayardan diğerine geçiş yapmak.
- T1080 (Sahte Ağ Paylaşımları Açmak) → Kurbanın dosyalarını ele geçirmek için zararlı bir ağ paylaşımı açmak.

11.Veri Toplama (Collection) – "Değerli Eşyaları Çantaya Koymak":

Saldırganın hedef sistemde belirlemiş olduğu kritik bilgileri elde etmesi ve bu bilgileri topladığı evredir. Elde edilen kaynakları arasında çeşitli sürücü türleri, tarayıcılar, ses, video ve e-posta bilgileri bulunmaktadır. Yaygın toplama yöntemleri arasında ekran görüntüsünü ve klavye girişlerini alma da yer almaktadır. Bu bilgileri; Winzip, 7Zip ve WinRAR gibi çeşitli yazılımlarla, elde ettiği dosyaları sıkıştırarak dosyanın taşınabilirliğini kolaylaştırmaktadır. Ayrıca saldırganın, lokal sistemlerden ve Sharepoint gibi paylaşım noktalarından da bilgileri elde etmesi mümkündür.

Hırsız evin içindeki değerli eşyaları toplar. Siber saldırganlar da aynı şekilde önemli dosyaları, müşteri verilerini veya finansal bilgileri ele geçirirler.

Örnek Teknikler:

- T1560 (Arşivleme - ZIP, RAR Kullanımı) → Ele geçirilen verileri sıkıştırıp göndermeden önce saklamak.
- T1119 (Veritabanı Dökümü Alma) → SQL sorguları ile veritabanlarından müşteri bilgilerini çekmek.

12.Komuta ve Kontrol (Command and Control – C2) – "Hırsızın Uzakta Olmasına Rağmen Evdeki Cihazları Yönetmesi":

Saldırganın, ele geçirdiği ağdaki diğer sistemlerle iletişim kurmak için kullanacağı tekniklerden oluştuğu evredir. Saldırgan, bulunduğu ağ içerisindeyken fark edilmemek için mevcut trafiği taklit eder. Saldırganlar, oluşturdukları trafiğin içeriğini tespit edilmesini daha zor hale getirmek için ASCII, Unicode, Base64, MIME gibi sistemlerle verileri kodlaması, veri aktarımında kullanılacak birincil kanallara ek olarak yan kanalları kullanması, çeşitli protokollerle komuta ve kontrolü sağlaması mümkündür.

Hırsız eve girse de sürekli orada kalmak zorunda değil. Uzaktan erişim sağlayarak evin ışıklarını açıp kapatabilir. Siber saldırganlar da uzaktan kontrol edilen bir sistem kullanır.

Örnek Teknikler:

- T1071 (Şifrelenmiş Trafik Kullanımı) → Ağdaki izleri gizlemek için veri iletişimini şifrelemek.
- T1572 (Tor veya VPN Kullanımı) → Kimliklerini gizlemek için anonim ağları kullanmak.

13.Veri Sızdırma (Exfiltration) – "Çantayla Evden Çıkmak":

Saldırganın, sistemlerden elde ettiği verileri çalmak için kullanacağı tekniklerden oluşur. Bu amaçla saldırgan, tespit edilmeyi önlemek adına verileri paketler, sıkıştırır veya şifreler.

Hırsız eve girdi, keşif yaptı, değerli eşyaları topladı. Şimdi bunları çaktırmadan dışarı çıkarması gerekiyor. Siber saldırganlar da ele geçirilen verileri şirketten dışarıya sızdırır.

Örnek Teknikler:

- T1041 (C2 Kanalı Üzerinden Veri Sızdırma) → Ele geçirilen verileri saldırganın kontrol ettiği sunucuya göndermek.
- T1020 (Şifrelenmiş Dosyalar ile Veri Kaçırma) → Verileri önce şifreleyip, sonra dışarı aktarmak.

14.Etki (Impact) – "Evi Ateşe Vermek":

Saldırganların operasyonel süreçleri manipüle ederek kullanılabilirliği bozmak veya bütünlüğü tehlikeye atmak için kullandığı tekniklerden oluşan evredir. Saldırganlar tarafından; verileri yok etmek, bozmak, verilere erişilebilirliği engellemek gibi hedeflere ulaşmak amacıyla kullanılmaktadır.

Hırsız her şeyi aldıktan sonra son darbeyi vurabilir:

- Evi yakar (verileri şifreleyip fidye ister)
- Kapıları kilitleyip içeri kimsenin girmesini engeller (sistemleri çökertir)

Örnek Teknikler:

- T1486 (Fidye Yazılımı ile Şifreleme) → Sistem dosyalarını şifreleyerek fidye istemek.
- T1529 (Servisleri Durdurma) → Şirketin kritik sistemlerini devre dışı bırakmak.

TTP NEDİR? (TACTİCS, TECHNİQUES, AND PROCEDURES):

TTP, **Tactics** (Taktikler), **Techniques** (Teknikler) ve **Procedures** (Prosedürler) kelimelerinin baş harflerinden oluşan bir kısaltmadır. Siber güvenlikte, özellikle tehdit istihbaratı ve saldırı analizlerinde çok önemli bir kavramdır.

1.Taktikler (Tactics) - "Neden?":

Saldırganın amacını gösterir.

- Örneğin, bir saldırgan kimlik bilgilerini ele geçirmek (Credential Access) istiyorsa, bu bir taktiktir.

2.Teknikler (Techniques) - "Nasıl?":

Saldırganın hedefe ulaşmak için kullandığı yöntemlerdir.

- Örneğin, kimlik bilgilerini ele geçirmek için LSASS belleğini dökmek (T1003 - Credential Dumping) bir tekniktir.

3.Prosedürler (Procedures) - "Ne Şekilde?":

Saldırganın belirli bir tekniği uygulama şeklidir.

- Örneğin, LSASS bellek dökümünü almak için Mimikatz kullanmak bir prosedürdür.

TTP-BASED THREAT HUNTING VE DETECTION ENGINEERING:

Siber güvenlikte saldırganları tespit etmek ve onlara karşı savunma yapmak için TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı) ve Detection Engineering (Tespit Mühendisliği) gibi kavramlar kullanılır.

1.TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı):

Tehdit avcılığı (Threat Hunting), güvenlik analistlerinin bilinen saldırı tekniklerini (TTP'leri) kullanarak ağda gizli tehditleri proaktif olarak araması sürecidir.

Önemli Noktalar:

- Proaktif bir yaklaşımdır. Yani SIEM gibi sistemlerin otomatik tespit edemediği tehditleri manuel olarak araştırırız.
- MITRE ATT&CK gibi çerçevelerdeki Taktik, Teknik ve Prosedürleri (TTP'leri) kullanarak saldırı izlerini ararız.

Örnek bir senaryo:
Bir tehdit avcısı, "LSASS bellek dökümü alma" (T1003 - Credential Dumping) tekniğinin kullanılıp kullanılmadığını anlamak için olay günlüklerinde belirli komutları araştırır.
Windows olay günlüklerinde sekurlsa::logonpasswords veya mimikatz.exe gibi ifadeleri arar.

TTP-Based Threat Hunting'in Avantajları:

- SIEM'in algılayamadığı saldırıları yakalama şansı artırılır.
- Daha karmaşık ve sofistike saldırılar erken fark edilir.
- Olay yanıt süreci hızlanır.

2.Detection Engineering (Tespit Mühendisliği):

Detection Engineering, güvenlik olaylarını otomatik tespit edebilmek için özel kurallar, imzalar ve analiz yöntemleri geliştirme sürecidir.

Önemli Noktalar:

- SIEM ve XDR gibi sistemler için özel algılama kuralları yazılır.
- TTP'ler temel alınarak kötü amaçlı etkinlikleri algılamak için log analizi, imza tabanlı algılama (YARA, Sigma), davranış analizi (ML, UEBA) gibi yöntemler kullanılır.

Örnek bir senaryo:
"LSASS Bellek Dökümü Alma" saldırısını Windows Event Log ID 4688 ile izleyip otomatik uyarı verecek bir SIEM kuralı yazılır.
Wazuh, Splunk veya ELK üzerinde Sigma kuralları oluşturularak kötü amaçlı işlemleri tespit eden özel filtreler eklenir.

Detection Engineering'in Avantajları:

- Tehditleri otomatik olarak algılama yeteneği gelişir.
- Yanlış pozitifleri azaltarak daha doğru ve hızlı uyarılar sağlanır.
- Yeni ortaya çıkan saldırı tekniklerine karşı dinamik ve sürekli gelişen kurallar oluşturulabilir.

Threat Hunting vs. Detection Engineering Farkı:

Threat Hunting tehditleri manuel olarak avlar, MITRE ATT&CK TTP'lerini kullanarak saldırıları araştırır. Detection Engineering ise algılama sistemleri için otomatik kurallar ve imzalar oluşturur, tehditleri tespit etmeyi hızlandırır.

APT GRUPLARI:

Siber güvenlik tehditlerinin sürekli olarak evrim geçirdiği günümüzde, geleneksel siber suçlar artık yalnızca bireylerin veya basit suç gruplarının faaliyet gösterdiği alanlar değil. Bu tehditlerin en ciddi ve sofistike biçimlerinden biri, gelişmiş kalıcı tehdit (APT) gruplarıdır. APT grupları, uzun süreli ve hedef odaklı saldırılar gerçekleştirerek kuruluşları hedefler ve bilgilerini ele geçirmeye çalışır.

Gelişmiş Kalıcı Tehdit (APT), hedeflerine karşı çok yönlü ve uzun vadeli planlanmış siber saldırılar gerçekleştiren karmaşık gruplardır. Bu gruplar, genellikle devlet destekli olabilirler ve bilgi toplamak, casusluk yapmak, ağları etkisiz hale getirmek veya sabotaj düzenlemek gibi amaçlarla faaliyet gösterirler. APT gruplarının tipik olarak diğer siber suç gruplarından ayıran birkaç özellik vardır:

- **Gelişmiş Yetenekler:** APT grupları, sıradan siber suçlardan daha fazla kaynak ve yeteneğe sahiptir. Bu gruplar genellikle gelişmiş siber araçlar ve teknikler kullanarak hedeflerine sızarlar.
- **Uzun Süreli Faaliyet:** APT grupları, hedeflerine sızdıktan sonra uzun bir süre boyunca faaliyet gösterebilirler. Bu, onlara kurum içinde derinlemesine kök salma ve bilgi toplama fırsatı verir.
- **Hedef Odaklılık:** APT grupları, belirli kurumları veya sektörleri hedef alarak belirli bilgilere ulaşmayı amaçlarlar. Bu genellikle casusluk veya finansal kazanç için yapılır.

APT Gruplarının Tehlikeleri:

APT gruplarının faaliyetleri birçok ciddi tehlikeyi beraberinde getirebilir:

- **Hassas Bilgi Sızıntısı:** APT grupları, kurumların hassas bilgilerine erişebilir ve bunları sızdırabilir. Bu, ticari sırların, müşteri verilerinin veya devlet sırlarının ifşası gibi sonuçlar doğurabilir.
- **Altyapı Zararı:** APT grupları, kurumların ağ altyapısına zarar verebilir veya hizmetlerini engelleyebilir. Bu, iş sürekliliği sorunlarına ve mali kayıplara neden olabilir.
- **Güvenilirlik Kaybı:** Bir kurumun APT saldırısına uğraması, müşterileri ve paydaşları için güvenilirlik kaybına neden olabilir. Bu da itibar kaybı ve müşteri kaybıyla sonuçlanabilir.

Kurumların Korunma Yöntemleri:

Kurumlar, APT gruplarının tehditlerine karşı kendilerini korumak için bir dizi adım atabilirler:

- **Bilinçli Farkındalık:** Kurumlar, çalışanlarını ve yöneticilerini APT saldırılarının potansiyel tehlikeleri konusunda bilinçlendirmelidir. Farkındalık eğitimleri ve düzenli güvenlik güncellemeleri önemlidir.
- **Güvenlik Duvarları:** Güçlü güvenlik duvarları ve ağ güvenliği önlemleri, APT gruplarının kuruma sızmasını engelleyebilir veya en azından zorlaştırabilir.
- **Gelişmiş Tehdit Tespiti:** Kurumlar, gelişmiş tehdit tespit sistemleri kullanarak APT saldırılarını tespit etmeye çalışmalıdır. Davranışsal analiz ve tehdit istihbaratı gibi tekniklerle erken uyarı sistemleri kurulabilir.
- **Güncel Yazılım ve Yama Yönetimi:** Kurumlar, yazılımlarını düzenli olarak güncellemeli ve güvenlik açıklarını kapatmak için yamaları uygulamalıdır. Güncel yazılım ve sistemler, APT gruplarının kolay hedef olmasını engeller.
- **İş Sürekliliği Planları:** APT saldırılarına karşı hazırlıklı olmak için kurumlar iş sürekliliği ve felaket kurtarma planları oluşturmalıdır. Bu planlar, saldırı sonrası toparlanmayı hızlandırabilir.

Gelişmiş Kalıcı Tehdit (APT) grupları, günümüzdeki en ciddi siber güvenlik tehditlerinden biridir. Bu gruplar, kurumların verilerini çalmak, altyapılarını etkisiz hale getirmek ve itibarlarını zedelemek gibi zararlar verebilir. Ancak, kurumlar doğru önlemleri alarak ve güvenlik stratejilerini güçlendirerek bu tehditlere karşı korunabilirler. Bilinçli farkındalık, güvenlik duvarları, tehdit tespiti sistemleri ve iş sürekliliği planları gibi önlemler, APT gruplarının etkisini azaltmaya yardımcı olabilir.

Bilinen Bazı APT Grupları ve Ülkeler:

1.APT28 (Fancy Bear) – Rusya:

Rusya bağlantılı olduğu düşünülen bir APT grubudur.
Genellikle NATO, savunma sanayi, seçim sistemleri ve hükümetleri hedef alır.

Taktikler:

- Kimlik Avı (Phishing) saldırıları
- Zero-day açıkları kullanma
- Oltalama e-postalarıyla kötü amaçlı yazılım yayma

Örnek saldırılar:

- 2016 ABD Başkanlık Seçimleri'nde Demokratik Parti'ye siber saldırı.
- Avrupa Parlamentosu ve NATO ülkelerine yönelik saldırılar.

2.APT29 (Cozy Bear) – Rusya:

Rus istihbarat servisi (SVR) ile bağlantılı olduğu düşünülen bir grup.
Diplomatik kurumları, devlet dairelerini ve şirketleri hedef alır.

Taktikler:

- Tedarik zinciri saldırıları
- Kimlik bilgisi çalma (Credential Dumping - T1003)
- Kötü amaçlı PowerShell betikleri kullanma

Örnek saldırılar:

- 2020'de SolarWinds saldırısı → ABD hükümetine yönelik büyük ölçekli bir saldırı gerçekleştirdi.

3.APT41 – Çin:

Çin hükümetiyle bağlantılı bir grup olduğu düşünülüyor.
Hem devlet destekli casusluk hem de finansal kazanç amaçlı siber saldırılar gerçekleştiriyorlar.

Taktikler:

- Zararlı yazılım bulaştırma (Malware Deployment)
- Mobil uygulamalara saldırılar
- Bulut sistemlerine sızma

Örnek saldırılar:

- 2021'de VPN açıklarını kullanarak ABD ve Avrupa'daki şirketlere saldırılar.
- Oyun endüstrisine ve finans sektörüne yönelik saldırılar.

4.Lazarus Group – Kuzey Kore:

Kuzey Kore destekli olduğu düşünülen APT grubudur.
Genellikle finans sektörü ve devletler hedef alınır.

Taktikler:

- Banka sistemlerine sızarak para çalma
- Kripto para borsalarına saldırılar
- Zero-day açıklarını kullanma

Örnek saldırılar:

- 2014 Sony Pictures hacki → Kuzey Kore'yi eleştiren "The Interview" filmi nedeniyle Sony'ye saldırı düzenlediler.
- 2017 WannaCry saldırısı → Dünya çapında büyük bir fidye yazılım saldırısı gerçekleştirdiler.

5.APT33 – İran:

İran destekli olduğu düşünülen bir grup.
Genellikle Ortadoğu'daki enerji ve havacılık sektörünü hedef alır.

Taktikler:

- Fidye yazılım ve yıkıcı saldırılar
- Kimlik avı saldırılarıyla bilgi çalma
- Gizli casusluk operasyonları

Örnek saldırılar:

- Suudi Arabistan'daki petrol şirketlerine yönelik saldırılar.
- ABD ve Avrupa'daki kritik altyapıları hedef alan siber casusluk girişimleri.

2022 UKRAINE ELECTRIC POWER ATTACK C0034:

2022 Ukrayna Elektrik Gücü Saldırısı (Kampanya C0034), **Sandworm Team** tarafından Ukrayna'daki bir elektrik hizmet sağlayıcısına yönelik gerçekleştirilen bir siber saldırıdır. Bu saldırıda, **GOGETTER**, **Neo-REGEORG**, **CaddyWiper** gibi zararlı yazılımlar ve sistemde mevcut araçlar kullanılarak **SCADA** sisteminden yetkisiz komutlar gönderilmiştir.

Saldırıda kullanılan teknikler ve bunların **TID** değerleri aşağıda listelenmiştir:

1.Komut ve Betik Yorumlayıcı: PowerShell (T1059.001):
Saldırganlar, TANKTRAP adlı bir PowerShell aracını kullanarak Windows Group Policy üzerinden bir silici (wiper) yaymış ve çalıştırmıştır.

2.Sistem Süreci Oluşturma veya Değiştirme: Systemd Servisi (T1543.002):
GOGETTER zararlı yazılımının kalıcılığını sağlamak için Systemd yapılandırılmış ve WantedBy=multi-user.target ayarıyla sistem kullanıcı girişlerini kabul etmeye başladığında çalışması sağlanmıştır.

3.Veri İmhası (T1485):
CaddyWiper, OT (Operasyonel Teknoloji) sistemleriyle ilgili dosyaları, haritalanmış sürücüleri ve fiziksel disk bölümlerini silmek için kullanılmıştır.

4.Etki Alanı veya Kiracı Politikası Değiştirme: Grup Politikası Değiştirme (T1484.001):
Saldırganlar, kötü amaçlı yazılımları dağıtmak ve çalıştırmak için Grup Politikası Nesneleri'ni (GPO) kullanmıştır.

5.Yanal Araç Transferi (T1570):
CaddyWiper'ın msserver.exe adlı çalıştırılabilir dosyası, bir GPO aracılığıyla bir aşama sunucusundan yerel diske kopyalanmıştır.

6.Kılık Değiştirme: Görev veya Servis Maskesi (T1036.004):
GOGETTER zararlı yazılımı, Systemd servis birimleri kullanılarak meşru veya meşru görünen servisler olarak gizlenmiştir.

7.Uygulama Katmanı Dışı Protokol (T1095):
Komuta ve Kontrol (C2) iletişimleri, TLS tabanlı bir tünel içinde proxy'lenmiştir.

8.Protokol Tünelleme (T1572):
GOGETTER tünelleme yazılımı, harici sunucularla "Yamux" TLS tabanlı C2 kanalı oluşturmak için kullanılmıştır.

9.Zamanlanmış Görev/İş: Zamanlanmış Görev (T1053.005):
CaddyWiper, belirli bir zamanda çalıştırılmak üzere bir GPO aracılığıyla Zamanlanmış Görev olarak yapılandırılmıştır.

10.Sunucu Yazılım Bileşeni: Web Shell (T1505.003):
Neo-REGEORG web shell'i, internet üzerinden erişilebilen bir sunucuya yerleştirilmiştir.

11.Otomatik Çalıştırma İmajı (T0895):
Saldırganlar, SCADA sunucusunu çalıştıran sanal makineye a.iso adlı bir ISO imajı bağlamış ve bu imaj içindeki kötü amaçlı VBS betiği, işletim sisteminin CD-ROM imajlarını otomatik çalıştırma özelliği nedeniyle yürütülmüştür.

12.Komut Satırı Arayüzü (T0807):
2022 Ukrayna Elektrik Şebekesi Saldırısı sırasında Sandworm grubu, MicroSCADA platformundaki SCIL-API'yi kullanarak scilc.exe ikili dosyası aracılığıyla komutlar çalıştırdı.

13.Betik(Scripting) (T0853):
2022 Ukrayna Elektrik Şebekesi Saldırısı sırasında Sandworm grubu, lun.vbs adlı bir Visual Basic betiğini kullanarak n.bat dosyasını çalıştırdı. Bu betik, ardından MicroSCADA scilc.exe komutunu çalıştırdı.

14.Sistem İkili Dosya Proxy Yürütme (T0894):
2022 Ukrayna Elektrik Şebekesi Saldırısı sırasında Sandworm grubu, MicroSCADA uygulama ikili dosyası olan scilc.exe'yi çalıştırarak, saldırgan tarafından tanımlanan s1.txt dosyasında belirtilen bir dizi SCADA komutunu gönderdi.
Çalıştırılan komut: C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt
Bu komut, SCADA yazılımını kullanarak uzaktaki trafo merkezlerine yetkisiz komut mesajları göndermek için kullanıldı.

15.Yetkisiz Komut Mesajı (T0855):
2022 Ukrayna Elektrik Şebekesi Saldırısı sırasında Sandworm grubu, MicroSCADA SCIL-API'yi kullanarak trafo merkezi cihazlarına yetkisiz komutlar gönderen bir dizi SCADA talimatı belirledi ve uyguladı.

Bu tekniklerin birleşimi, saldırganların Ukrayna'nın elektrik altyapısına yetkisiz erişim sağlamalarına ve operasyonel süreçleri kesintiye uğratmalarına olanak tanımıştır.

ÖRNEK SENARYO: "X" ŞİRKETİNİN HACKLENME SENARYOSU:

Saldırganlar, X Şirketi hakkında bilgi toplamak için açık kaynaklardan ve oltalama yöntemleriyle çalışan bilgilerini ele geçirir. Daha sonra sahte e-postalar ve zararlı dosyalar hazırlayarak çalışanlara phishing saldırıları düzenlerler.

Bir çalışanın zararlı makroyu içeren Excel dosyasını açmasıyla saldırganlar sistemde yürütme sağlar ve kalıcılık için zararlı servisler oluşturur. Yetki yükseltme ile yönetici hakları elde edip savunmadan kaçınırlar.

Son olarak, kimlik bilgilerini çalarak şirketin ağında yanal hareket gerçekleştirirler ve büyük bir fidye yazılım saldırısıyla sistemleri şifreleyerek hizmeti durdurmak için DDos saldırısı gerçekleştirirler.

SENARYONUN MITRE ATT&CK TABLOSUNDAKİ YERİ:

1.Keşif (Reconnaissance):

Saldırganlar, hedef şirket hakkında bilgi toplamak için keşif aşamasına başlar.

- **T1598 - Phishing for Information:**
  LinkedIn, Facebook ve Twitter gibi sosyal medya platformlarından şirket çalışanlarını ve pozisyonlarını araştırırlar.
  Çalışanların e-posta adreslerini ve iletişim bilgilerini toplamak için sahte iş ilanları ve forumları kullanırlar.
- **T1596 - Search Open Website/Domain:**
  WHOIS sorguları yaparak şirketin alt alan adlarını (subdomain) keşfederler.
  Şirketin kariyer ve iletişim sayfalarından çalışan e-posta formatını belirlerler.

2.Kaynak Geliştirme (Resource Development):

Saldırganlar, ele geçirdikleri çalışan bilgilerini kullanarak sahte oltalama saldırıları hazırlarlar.

- **T1587 - Develop Capabilities:**
  Oltalama saldırıları için Gophish ve Evilginx gibi araçlar kullanarak sahte e-posta kampanyaları hazırlarlar.
- **T1585 - Establish Accounts:**
  Gerçekçi görünümlü saldırılar düzenleyebilmek için, benzer alan adlarına sahip sahte e-posta adresleri ve LinkedIn hesapları oluştururlar.

3.Başlangıç Erişimi (Initial Access):

Saldırganlar, oltalama saldırılarıyla şirket çalışanlarını hedef alarak zararlı yazılımlarını bulaştırmaya çalışır.

- **T1566.001 - Spear Phishing Attachment:**
  Şirket içi finans raporu adı altında, içinde zararlı Excel makrosu bulunan bir e-posta gönderirler.
  Çalışanlardan biri Excel dosyasını açar ve makroyu çalıştırır.
- **T1566.002 - Spear Phishing Link:**
  Şirket içi sistemlere giriş yapmaları gerektiğini iddia eden sahte bir web sitesi hazırlarlar. Çalışanları bu kimlik avı (phishing) sitesine yönlendiren bir e-posta göndererek giriş yapmalarını sağlarlar.

4.Yürütme (Execution):

Saldırganlar, sistem üzerinde zararlı yazılımlarını çalıştırır.

- **T1053.005 - Scheduled Task/Job:**
  Windows'ta "System Update" adıyla gizlenmiş bir görev oluştururlar. Bu görev, her 30 dakikada bir saldırganın komut dosyasını çalıştırır.
- **T1569.002 - System Services:**
  Zararlı yazılım, Windows hizmeti (service) olarak kendini sisteme ekler.
  Saldırganın komut almasını sağlayan bir arka kapı (backdoor) oluşturur.

5.Kalıcılık (Persistence):]

Saldırganlar, sistemde uzun süre kalabilmek için çeşitli yöntemler kullanır.

- **T1543.003 - Windows Service:**
  Kendi zararlı yazılımlarını Windows servisleri listesine ekleyerek kalıcılığı sağlarlar.
- **T1547.001 - Registry Run Keys / Startup Folder:**
  Windows Registry'ye ekleme yaparak, her yeniden başlatmada zararlı yazılımın çalışmasını sağlarlar.

6.Yetki Yükseltme (Privilege Escalation):]

Saldırganlar, sistem üzerinde yönetici haklarına sahip olabilmek için yetki yükseltme saldırıları gerçekleştirir.

- **T1068 - Exploitation for Privilege Escalation:**
  Windows'ta eski bir güvenlik açığını kullanarak Sistem (NT AUTHORITY\SYSTEM) hakları elde ederler.
- **T1621 - Windows Token Impersonation:**
  Yetkili bir kullanıcının erişim anahtarlarını (tokenlerini) çalarak, kendilerini yönetici gibi gösterirler.

7.Savunmadan Kaçınma (Defense Evasion):
Tespit edilmemek için çeşitli önlemler alırlar.

- **T1562.001 - Disable or Modify Tools:**
  Windows Defender ve diğer güvenlik yazılımlarını devre dışı bırakırlar.
- **T1070.004 - File Deletion:**
  Windows olay loglarını temizleyerek izlerini silerler.

8.Kimlik Bilgisi Erişimi (Credential Access):
Şirket içindeki hesaplara erişebilmek için şifreleri çalarlar.

- **T1003.001 - LSASS Memory Dumping:**
  Mimikatz aracı ile LSASS belleğini dökerek kullanıcı şifrelerini çekerler.
- **T1555.003 - Credentials from Web Browsers:**
  Çalışanların tarayıcılarına kaydettiği VPN ve e-posta hesaplarının şifrelerini çekerler.

9.Yanal Hareket (Lateral Movement):
Şirket iç ağında daha fazla cihaza erişim sağlarlar.

- **T1021.001 - Remote Desktop Protocol (RDP):**
  Ele geçirilen hesap bilgileriyle farklı sunuculara RDP bağlantısı yaparlar.
- **T1075 - Pass the Hash:**
  NTLM hash'lerini kullanarak diğer sistemlere şifre girmeden bağlanırlar.

10.Etki (Impact):
Saldırının son aşamasında, şirketi zarara uğratacak işlemler gerçekleştirirler.

- **T1486 - Data Encrypted for Impact (Ransomware):**
  Şirketin kritik verilerini şifreleyerek fidye talep ederler.
- **T1499 - Endpoint Denial of Service (DDoS Attack):**
  Sunuculara hizmet reddi (DDoS) saldırısı düzenleyerek sistemlerin çalışmasını durdururlar.

SONUÇ:

Siber saldırılar giderek daha sofistike hale gelmekte ve tehdit aktörleri, kurumsal ağlara sızmak ve uzun vadeli zararlar vermek için gelişmiş taktikler uygulamaktadır. Bu raporda ele alınan MITRE ATT&CK Framework, siber tehditleri anlamak ve bunlara karşı etkili güvenlik önlemleri almak için kritik bir araçtır.

2022 Ukraine Electric Power Attack (C0034) örneği, devlet destekli saldırganların nasıl organize ve sistematik bir şekilde altyapılara zarar verebildiğini göstermektedir. Ayrıca, X Şirketi'ne yönelik senaryo, saldırganların izlediği adımları detaylandırarak bir saldırının nasıl ilerleyebileceğini açıklamaktadır.

Siber güvenlik ekiplerinin MITRE ATT&CK çerçevesini kullanarak tehdit avcılığı yapması, saldırı tespit mühendisliği geliştirmesi ve APT gruplarına karşı önleyici tedbirler alması büyük önem taşımaktadır. Savunma ekiplerinin, tehdit aktörlerinin kullandığı TTP'leri iyi analiz etmesi, saldırıları daha hızlı tespit etmelerine ve önlem almalarına olanak sağlar.

Sonuç olarak, MITRE ATT&CK Framework yalnızca bir bilgi tabanı değil, aynı zamanda tehdit istihbaratı, güvenlik izleme ve olay müdahalesi süreçlerinde kritik bir rehberdir. Kurumların bu çerçeveyi benimsemesi, güvenlik farkındalığını artırarak siber saldırılara karşı daha dirençli hale gelmelerini sağlayacaktır.

KAYNAKÇA:

https://attack.mitre.org/
https://attack.mitre.org/techniques/enterprise/
https://attack.mitre.org/tactics/enterprise/
https://attack.mitre.org/campaigns/C0034/
https://app.tidalcyber.com/campaigns/a79e06d1-df08-5c72-9180-2c373274f889
https://cyberartspro.com/mitre-attack-framework-nedir/
http://berqnet.com/blog/mitre-attck-framework
https://sibertim.com/siber-guvenlikte-apt-gruplari/
https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e