ALTAY

MITRE ATT&CK

FRAMEWORK

16.02.2025

MEHMET MERMER

SİBERVATAN

İÇİNDEKİLER

GİRİŞ

Siber güvenlik dünyasında tehdit aktörlerinin kullandığı yöntemleri anlamak ve etkili savunma stratejileri geliştirmek kritik bir öneme sahiptir. MITRE ATT&CK Framework, siber saldırıların nasıl gerçekleştirildiğini detaylandıran ve savunma ekiplerine rehberlik eden bir bilgi tabanıdır. Bu framework, saldırganların hedef sistemleri istismar etmek için kullandıkları Taktikler, Teknikler ve Prosedürler hakkında kapsamlı bir rehber sunar. Güvenlik ekipleri, MITRE ATT&CK çerçevesi sayesinde tehdit aktörlerinin izlediği yolları daha iyi analiz edebilir ve saldırılara karşı daha etkili savunma önlemleri alabilir.

Bu raporda, MITRE ATT&CK Framework'ünün yapısını ve önemini inceleyerek, tehdit avcılığı ve saldırı tespit mühendisliği yaklaşımlarını ele alacağız. Siber tehditlerle mücadelede TTP tabanlı bir yaklaşımın, saldırganların tekniklerini daha iyi anlamamızı sağladığını ve bu sayede saldırı yüzeyini daraltarak tehditleri erken tespit edebildiğimizi göstereceğiz. Ayrıca, 2022 Ukraine Electric Power Attack olayında kullanılan teknikleri ve TID değerlerini analiz ederek, gerçek dünyada MITRE ATT&CK Framework'ünün nasıl uygulandığını inceleyeceğiz.

Son olarak, bir şirketin hacklenmesi üzerine oluşturulan senaryo ile tehdit aktörlerinin izlediği adımları, kullanılan taktik ve teknikleri MITRE ATT&CK tablosu eşliğinde açıklayacağız. Bu senaryo, bir saldırının keşif aşamasından son aşamasına kadar nasıl ilerlediğini anlamamıza yardımcı olacak ve savunma ekiplerinin benzer saldırıları nasıl tespit edebileceğine dair içgörüler sağlayacaktır.

MITRE ATT&CK TABLOSU NEDİR?

1958'de kurulan tarafsız bir kuruluş olan MITRE Corporation, ABD'nin çeşitli alanlarda faaliyet gösteren devlet kurumları için çalışmaktadır. MITRE ATT&CK, MITRE Corp tarafından 2013 yılında geliştirilmiş ve piyasaya sürülmüştür. MITRE ATT&CK çerçevesi, saldırgan davranışının fiilen gözlemlenmesiyle toplanan siber saldırgan taktikleri ve tekniklerinden oluşan kapsamlı bir bilgi tabanıdır. Dünya genelindeki tehdit gruplarının kullanmış olduğu stratejilerin analiz edilerek derlendiği, sürekli güncellenen modeldir. Siber güvenlik alanında bilgi sahibi olmak isteyen herkes için başucu kaynağı niteliğindedir. Bu sistem, ücretsiz olup herkese açıktır.

MITRE ATT&CK, siber saldırganlar tarafından kullanılan taktik, teknik ve prosedürleri (TTP) kataloglayarak siber tehdit modellemesi ve savunma stratejisi geliştirmek için yapılandırılmış bir yaklaşım sunar. Her teknik için MITRE ATT&CK, önceden gerçekleşmiş dünya örneklerini de içerir. Örnekler, belirli bir teknik kullanılarak yapılan geçmiş siber saldırı vakalarını tanımlar.

Siber tehdit senaryoları sürekli değiştiğinden, MITRE ATT&CK verileri de düzenli olarak güncellenir. Yeni siber saldırı örnekleri eklenirken, artık kullanılmayanlar güncellenir veya kaldırılır. Çeşitli araçlarla entegre ederek kullanabilen veri tabanı siber güvenlik olaylarına müdahale süresini kısaltır. Siber güvenlik stratejileri bu veri tabanı ile güçlendirerek, siber tehditlere karşı hazırlıklı olunabilir.

MITRE ATT&CK Framework'un içeriği;

MITRE ATT&CK, teknik açıklamalarını matris yapısında organize eder. Matris, hem dikeyde hem de yatayda çalışarak siber saldırıların detaylı haritasını sunar. Aradığınızı kolayca bulmanıza izin veren organize yapısı sayesinde potansiyel saldırı vektörlerini kolayca görselleştirebilir, ardından değerlendirebilir.

1. ***Enterprise ATT&CK Matrisi***
   MITRE ATT&CK Enterprise Matrisi, siber güvenlikteki en yaygın kullanılan araçlardan biridir. Özellikle işletmelerde kullanılan Windows, macOS, ve Linux işletim sistemleri üzerine odaklanır. Saldırı tespit edildiğinde, matris saldırının hangi aşamada olduğunu ve hangi tekniklerin kullanıldığını belirlemeye yardımcı olur, böylece müdahale ekipleri daha hızlı ve etkin hareket edebilir. Enterprise matrisi, siber saldırı süreçlerinin farklı aşamalarını temsil eden 14 ana taktik kategorisi içerir. Tüm taktikler aşamalarla birbirini takip eden saldırı zincirinden oluşur.

2. ***Mobile ATT&CK Matrisi***
   Mobile matrisi, mobil cihazlara yönelik tehditlerle ilgili Android ve iOS işletim sistemlerine odaklanır. Cihaz bazlı konfigürasyon hatalarından mobil uygulamalara kadar çeşitli açılardan zafiyet verileri bulunur. Mobil ortamlarda kullanılan gelişen taktikleri anlamak için önemli bir araçtır ve güvenlik ekiplerinin mobil cihazlardaki hassas verileri korumak için sağlam stratejiler geliştirmesine yardımcı olur.

3. ***ICS ATT&CK Matrisi***
   ICS Matrisi, endüstriyel kontrol sistemlerine yönelik siber tehditleri ele alır. Kritik altyapıların korunmasında önemli rol oynayan matris, enerji santralleri, su arıtma tesisleri gibi yerlerde sıklıkla kullanılır. Potansiyel saldırıları analiz ederek şehirlerin refahını güvende tutar. ICS matrisi, fiziksel proseslerin ve bunların siber dünyayla olan etkileşimlerinin güvenliğine odaklanır. Herhangi bir şüpheli eylem durumunda güvenlik operasyon merkezi (SOC) ile, ICS ATT&CK Matrisini kullanarak tehditleri analiz edebilir, uygun müdahale stratejilerini geliştirebilir.

MITRE ATT&CK TABLOSU NEDEN ÖNEMLİDİR?

MITRE ATT&CK Tablosu, saldırganların izlediği adımları detaylı bir şekilde kategorize eden ve güvenlik uzmanlarına tehditleri daha iyi anlama ve savunma oluşturma fırsatı sunan bir çerçevedir. Anlık güvenlik önlemleri sağlamanın yanı sıra uzun vadeli stratejik planlama ve sürekli iyileştirme için de temel oluşturur. Sağladığı faydalar aşağıdaki gibi sıralanabilir:

- Veri tabanı her kesimin anlayabileceği kapsamlı bir terminoloji seti sunar. Bu sayede farklı departmanlar, organizasyonlar, hatta farklı endüstriler arasında savunma stratejileri üzerine açık ve tutarlı iletişim kurulabilir. Ortak dil kullanımı, işbirliğiyle birlikte bilgi paylaşımını teşvik eder, bu da daha etkili tehdit koordinasyonu sağlar.

- MITRE ATT&CK, siber saldırıları daha iyi anlamayı sağlar, böylece olası saldırılar gerçekleşmeden önce savunma stratejileri geliştirebilirsiniz. Proaktif yaklaşım sayesinde, potansiyel zafiyetler önceden tespit edilir ve kapatılır.
- Sürekli güncellenen bir framework olması sebebiyle en yeni tehdit senaryolarının saldırı teknikleri hakkında dahi bilgiler sunar.
- MITRE ATT&CK, güvenlik önlemlerinin etkinliğini değerlendirmek için somut alan sunar. Analizlerle sağlanan ölçülebilirlik ve bilinçli bütçe atamalarına imkan tanır.

Bu veri tabanı, modern siber güvenlik dünyasında bir zorunluluk haline gelmiş olup, tehdit aktörlerinin faaliyetlerini anlamak ve savunma stratejilerini geliştirmek için vazgeçilmez bir araçtır. MITRE ATT&CK tablosunun aktif olarak kullanılması, organizasyonların saldırılara karşı daha dirençli olmasını ve tehditleri etkili bir şekilde yönetilmesini sağlar.

TTP NEDİR? (Tactics, Techniques, and Procedures)

MITRE ATT&CK çerçevesi, tehdit aktörlerinin taktikleri, teknikleri ve prosedürlerinin kapsamlı bir matrisini sağlar. Güvenlik topluluğunun paylaşılan bilgisine dayanarak, kuruluşların hızla gelişen siber tehditleri anlamalarına ve azaltmalarına yardımcı olur ve güvenlik duruşlarını iyileştirir.

TTP kavramı, siber güvenlik profesyonellerinin siber saldırıları anlamalarına, siber saldırıların izini sürmelerine ve savunma stratejileri geliştirmelerine yardımcı olur. Siber güvenlik uzmanları, saldırganların teknik, taktik ve prosedürlerini analiz ederek, gelecekteki saldırıları önlemek veya siber saldırıları tespit etmek için savunma stratejileri geliştirebilirler. Ayrıca, TTP analizi, siber saldırıların başarılı bir şekilde tespit edilmesine ve karşı önlemlerin alınmasına olanak tanır.

1. ***TAKTİK (Tactics)***

   Saldırganların amaçlarına ulaşmak için kullandığı geniş stratejilerdir. Örneğin, başlıca taktiklerden biri sızdırmadır. MITRE ATT&CK sınıflandırmasında, sızdırma, saldırganların sistemlerinizden veri çalmak için kullanabilecekleri tüm teknikleri içermektedir. Saldırganlar verileri sızdırırken, yazılım kontrolleriniz tarafından algılanmamak için genellikle varlıklarını dikkatli bir şekilde paketler ve kamufle ederler. Bu kamuflaj, sıkıştırma veya şifreleme kullanımını, aktarım boyutunu sınırlamayı, komuta ve kontrol kanallarında ve diğer faaliyetlerinde kullandıklarından farklı bir protokol kullanmayı içerebilir.

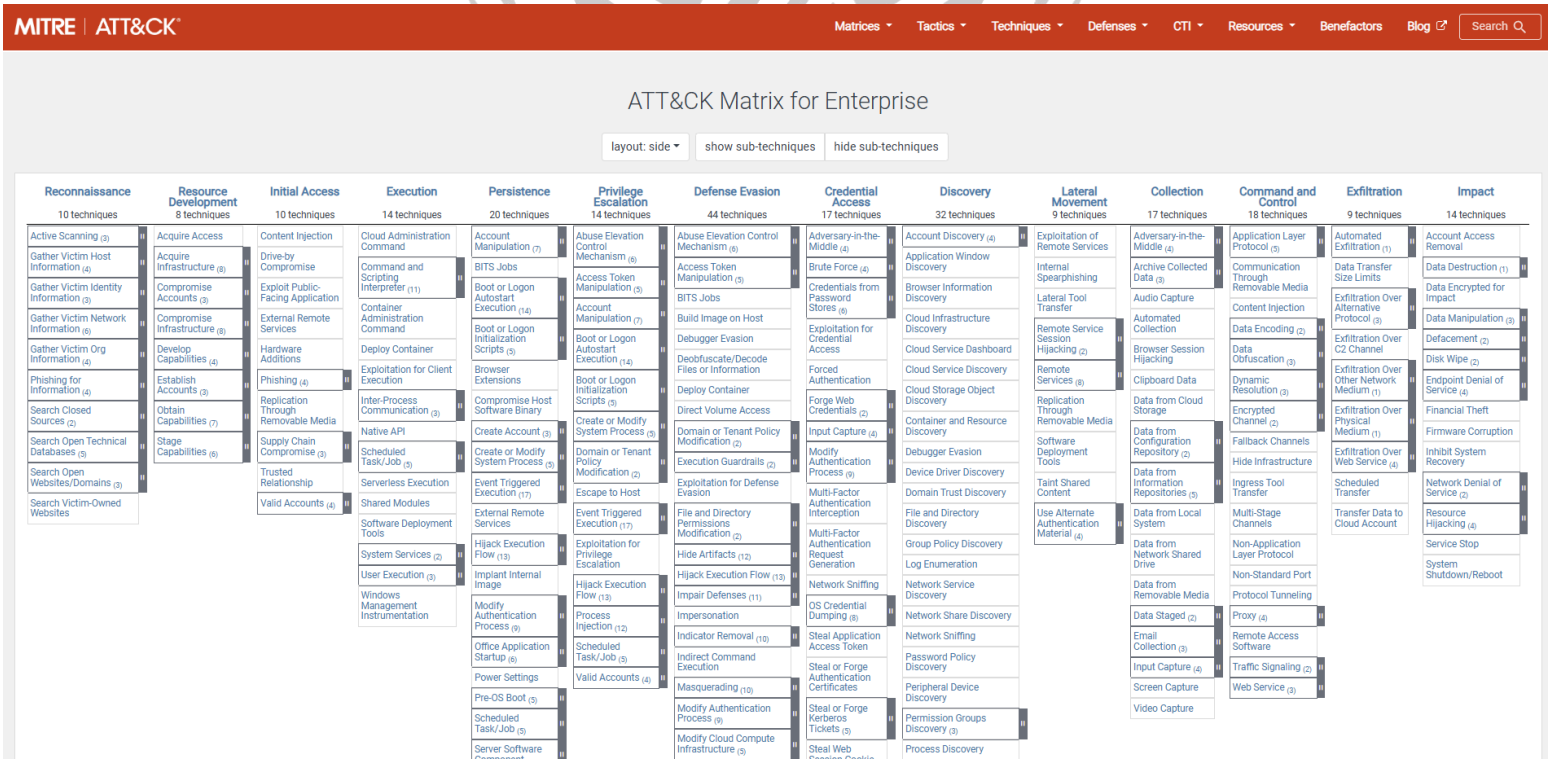
2. ***TEKNİK (*Techniques)**

   Taktiklerin altında yer alan daha spesifik saldırı yöntemleridir. Taktiklerin gerçekleştirilmesi için kullanılan yöntemleri ayrıntılarıyla açıklar. Her bir taktik altında birden fazla teknik bulunabilir. Örnek teknikler arasında “Hesap Gizleme,” “Kod İmzalarını Değiştirme,” “E-posta Eklerini Kullanma” gibi başlıklar yer alır.

Tekniklerin altında bulunan **Alt Tekniklerde (**Sub-techniques**)** mevcuttur. Bir teknikten daha düşük seviyede davranışı tanımlar ve güvenlik ekiplerinin belirli riskleri azaltmak için ayrıntılı siber güvenlik taktikleri oluşturmasına yardımcı olur. Örneğin, bir kimlik avı saldırısında kötü amaçlı bir ek kullanma.

3. ***Prosedür (*Procedures)**
   Saldırganların bir tekniği veya alt tekniği yürütmek için kullandıkları belirli uygulamalardır. Bir tekniğin nasıl uygulandığını ayrıntılı bir şekilde gösterir. Saldırganlar, belirli bir hedefe ulaşmak için belirli bir prosedürü izleyebilirler. Örneğin, bir saldırının başlaması, saldırganın hedef ağa sızması, veri toplaması ve hedef ağdan çıkış yapması gibi adımlar prosedürler olarak adlandırılabilir.

Teknik, Taktik ve Prosedürler (TTP), siber güvenlik alanında temel bir kavramdır ve saldırganların siber saldırıları nasıl planladığını ve uyguladığını anlamak için önemlidir. Siber güvenlik uzmanları, TTP analizi yaparak saldırganların hareketlerini izleyebilir ve savunma stratejilerini buna göre güçlendirebilirler.



TTP - Based Threat Hunting Nedir?

TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı), saldırganların Tactics, Techniques, and Procedures (TTP) modellerini analiz ederek, ağda gizlenmiş tehditleri proaktif olarak tespit etmeye yönelik bir siber güvenlik stratejisidir.TTP tabanlı tehdit avcılığı, saldırganların belirli araçlar, teknikler ve prosedürler kullanarak hedef sistemlerde nasıl hareket ettiğini anlamaya yönelik derinlemesine bir analiz sürecidir.

Bu yöntem, MITRE ATT&CK çerçevesi gibi tehdit istihbaratı kaynaklarını kullanarak, saldırıların taktik, teknik ve prosedürler düzeyinde analiz edilmesine olanak tanır. Tehdit avcıları, belirli bir saldırgan grubunun geçmiş saldırılarını ve kullandıkları teknikleri inceleyerek, mevcut ortamlarında bu tür aktivitelerin izlerini araştırır.

TTP tabanlı tehdit avcılığı, yalnızca mevcut tehditleri tespit etmekle kalmaz, aynı zamanda saldırganların kullandığı tekniklerin daha erken aşamalarda fark edilmesini sağlayarak güvenlik ekiplerinin daha proaktif bir savunma stratejisi geliştirmesine yardımcı olur. Böylece, henüz güvenlik çözümlerinin tespit edemediği gelişmiş saldırıları belirlemek ve hızlıca müdahale etmek mümkün hale gelir.

Detection Engineering Nedir?

Detection Engineering, siber güvenlikte tehditleri erken aşamada tespit etmek, analiz etmek ve otomatikleştirilmiş savunma mekanizmaları oluşturmak için kullanılan stratejik bir yaklaşımdır. Bu mühendislik alanı, siber güvenlik operasyon merkezlerinde, tehdit avcıları, olay müdahale ekipleri ve siber tehdit istihbaratı uzmanları tarafından geliştirilir ve yönetilir.
Tespit mühendisliği, bir kültürün yanı sıra mevcut tehditlere karşı savunmak için tespit geliştirme, geliştirme ve ayarlama süreciyle ilgilidir. Tehdit aktörlerinin saldırılarını ve tekniklerini geliştirmeleri gibi, güvenlik ekipleri de tespit içeriklerini geliştirmelidir. Bu nedenle tespit mühendisliği, sürekli çaba gerektiren bir yaşam döngüsüdür. Bununla birlikte, iyi yapıldığında, tespit mühendisliği bir tehdidi tespit etmek ve bunlara yanıt vermek için ortalama süreyi azaltabilir ve bir tehditten kurtulabilir.

Bu yaklaşım, saldırganların kullandığı teknikler, taktikler ve prosedürlerin üzerine yoğunlaşarak, tehditlerin henüz belirli bir imza oluşturmadan tespit edilmesini amaçlar. Bu süreçte, MITRE ATT&CK, Cyber Kill Chain, gibi saldırı analiz çerçeveleri kullanılarak, saldırıların hangi aşamalarda gerçekleştiği, hangi tekniklerin kullanıldığı ve nasıl tespit edilebileceği incelenir.

2022 Ukraine Electric Power Attack C0034

2022 yılında Ukrayna'nın enerji altyapısını hedef alan siber saldırı, Sandworm Team tarafından gerçekleştirildi. Bu grup, Rusya ile bağlantılı APT gruplarından biri olarak bilinir ve geçmişte de Ukrayna'nın kritik altyapısına yönelik saldırılar düzenlemiştir.

Bu saldırının temel amacı, Ukrayna'nın elektrik dağıtım sistemlerini devre dışı bırakmak, ülkenin kritik altyapısını felç etmek ve halkın günlük yaşamını olumsuz etkilemekti. Özellikle, endüstriyel kontrol sistemleri altyapısını hedef alarak enerji santrallerinin ve elektrik iletim hatlarının çalışmasını durdurmaya yönelik bir plan uygulanmıştır.

Saldırganlar, sistemlere sızarak SCADA sistemlerini manipüle etmiş ve Industroyer2 adlı gelişmiş bir zararlı yazılımı kullanarak elektrik şebekesi üzerinde kontrol sağlamaya çalışmıştır. Bunun yanında, CaddyWiper adlı veri silme yazılımı kullanılarak, sistemlerdeki kritik veriler hedef alınmış ve sistemlerin tekrar çalışmasını engellemek için dosyalar silinmiştir.

Saldırıda Kullanılan Teknikler

- **Komut ve Betik Yorumlayıcısı: PowerShell (T1059.001):** Saldırganlar, TANKTRAP adlı bir PowerShell aracını kullanarak Windows Grup İlkesi üzerinden bir silici yazılımı yaymış ve çalıştırmıştır.

- **Veri İmhası (T1485):** CaddyWiper adlı zararlı yazılım, hedef sistemlerde OT ile ilgili dosyaları, bağlı sürücüleri ve fiziksel disk bölümlerini silmek için kullanılmıştır.

- **Etki Alanı veya Kiracı İlkesi Değiştirme: Grup İlkesi Değiştirme (T1484.001):** Saldırganlar, kötü amaçlı yazılımları dağıtmak ve çalıştırmak için Grup İlkesi Nesneleri'nden faydalanmıştır.

- **Yanal Araç Transferi (T1570):** CaddyWiper'ın çalıştırılabilir dosyası olan msserver.exe, dağıtımdan önce bir hazırlık sunucusundan yerel diske kopyalanmıştır.

- **Gizleme: Görev veya Hizmeti Gizleme (T1036.004):** GOGETTER zararlı yazılımı, meşru veya meşru görünen hizmetler olarak gizlenmiştir.

- **Uygulama Katmanı Dışı Protokol (T1095):** Komuta ve Kontrol iletişimleri, TLS tabanlı bir tünel içinde yönlendirilmiştir.

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

- **Zamanlanmış Görev/İş: Zamanlanmış Görev (T1053.005):** CaddyWiper'ın belirli bir zamanda çalıştırılması için Grup İlkesi Nesneleri aracılığıyla Zamanlanmış Görevler kullanılmıştır.

- **Sunucu Yazılım Bileşeni: Web Kabuk (T1505.003):** Neo-REGEORG web kabuğu, internet üzerinden erişilebilen bir sunucuya yerleştirilmiştir.

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

ÖRNEK SENARYO

1. Keşif Aşaması

Tehdit aktörleri, şirketin internet sitesini ve sosyal medya hesaplarını inceleyerek açıklar ve zayıf noktalar aramaktadır. Aynı zamanda, şirket çalışanlarına ait e-posta adresleri ve kişisel bilgileri bulmaya çalışır.

- **Taktik**: *Reconnaissance* (T1071)
    - **Teknik 1**: *Gather Victim Identity Information* (T1071.001)
      Aktör, şirket çalışanlarının e-posta adreslerini ve diğer kişisel bilgilerini toplar.
    - **Teknik 2**: *Search Open Websites/Domains* (T1071.002)
      Aktör, şirketin web sitesinde açıkça paylaşılan bilgileri ve veritabanlarını tarar.

2. Erişim Sağlama

Tehdit aktörü, şirketin çalışanlarından birinin e-posta adresini bulur ve phishing saldırısı başlatır. Saldırıya uğrayan çalışan, kötü amaçlı bir bağlantıyı tıklayarak bilgisayarına zararlı yazılımı indirir.

- **Taktik**: *Initial Access* (T1071)
    - **Teknik 1**: *Phishing* (T1566)
      E-posta yoluyla zararlı bağlantı içeren phishing kampanyası.
    - **Teknik 2**: *Spearphishing Attachment* (T1193)
      Çalışanlara zararlı e-posta ekleri gönderilir.

3. Çalışan Sistemi Üzerinden Hareket Etme

Zararlı yazılım çalışan bilgisayarına sızdıktan sonra, ağda daha fazla bilgi toplamak ve ağda ilerlemek amacıyla oturum açma bilgilerini çalar. Elde edilen kimlik bilgileriyle şirket içindeki diğer sistemlere erişmeye başlar.

- **Taktik**: *Lateral Movement* (T1071)
    - **Teknik 1**: *Credential Dumping* (T1003)
      Çalışanların oturum açma bilgileri ele geçirilir.
    - **Teknik 2**: *Remote Desktop Protocol (RDP)* (T1076)
      Kötü amaçlı yazılım, şirketin iç ağına RDP kullanarak erişir.

4. Veri Toplama ve Eski Verilerin Çalınması

Aktör, şirketin veri tabanlarına erişim sağladıktan sonra önemli bilgileri toplar. Özellikle finansal veriler ve müşteri bilgileri hedeflenir.

- **Taktik**: *Collection* (T1071)
    - **Teknik 1**: *Data from Information Repositories* (T1213)
      Şirketin veritabanları ve dosya depolama sistemleri hedef alınır.
    - **Teknik 2**: *Automated Collection* (T1119)
      Veriler otomatik olarak toplanır ve dışa aktarılır.

5. Veri Çıkışı

Veri toplandıktan sonra, tehdit aktörü, çalınan verileri şirketin dışına çıkarmak için şifreli bir bağlantı kurar. Bu, şirketin veri sızıntılarını fark etmeden verileri çıkarmalarına olanak sağlar.

- **Taktik**: *Exfiltration* (T1071)
    - **Teknik 1**: *Exfiltration Over C2 Channel* (T1041)
      Çalınan veriler, komut ve kontrol kanalına yönlendirilerek dışarıya sızdırılır.
    - **Teknik 2**: *Exfiltration Over Web Service* (T1071.001)
      Veriler, web hizmetleri aracılığıyla dışa aktarılır.

SONUÇ

Bu rapor, MITRE ATT&CK tablosunun siber güvenlikteki rolünü ve önemini, tehdit aktörlerinin saldırı metodolojilerinin analizini, ve bu metodolojilerin nasıl tespit edilebileceğine dair bir bakış açısı sunmuştur. MITRE ATT&CK Framework'ü, siber tehdit avcıları ve güvenlik mühendisleri için saldırganların hareketlerini daha iyi anlamalarına ve savunma stratejilerini bu tehditler doğrultusunda şekillendirmelerine olanak tanır.

TTP (Tactics, Techniques, and Procedures) kavramı, tehdit aktörlerinin saldırılarını gerçekleştirmek için kullandıkları yöntemleri tanımlayarak, bu tekniklerin savunma ve tespit mühendisliğinde nasıl kullanılabileceğini açıklar. Bu raporda, TTP-Based Threat Hunting ve Detection Engineering stratejileriyle tehdit avcılığının nasıl daha etkin hale getirilebileceği de tartışılmıştır.

Özellikle 2022 yılında gerçekleşen Ukraine Electric Power Attack (C0034) örneği, bir siber saldırının farklı aşamalarında hangi MITRE ATT&CK tekniklerinin kullanıldığını göstererek, savunma tarafının bu tür saldırıları nasıl tespit edebileceği ve engelleyebileceği hakkında önemli bilgiler sunmuştur. Bu tür saldırıların analizi, saldırıların hangi aşamalarında hangi tekniklerin kullanıldığını belirleyerek, bu tekniklerin TID değerleriyle haritalandırılmasını sağlar.

Örnek bir şirket hacklenme senaryosunda, MITRE ATT&CK tablosu üzerinden yapılan analiz, saldırganların keşif aşamasından itibaren nasıl ilerlediklerini ve hangi teknikleri kullandıklarını göstererek, güvenlik ekiplerinin bu tür saldırılara karşı savunmalarını geliştirmeleri için yol gösterici olmuştur. Tactic ve Technique bazında yapılan bu analizler, her adımda hangi güvenlik önlemlerinin alındığını belirleyerek, etkili bir tehdit algılama ve müdahale süreci oluşturulmasını sağlayacaktır.

Sonuç olarak, MITRE ATT&CK tablosu, güvenlik profesyonellerine kapsamlı bir saldırı analizi, tehdit avcılığı ve tespit mühendisliği yaklaşımı sunarak, güvenlik ekiplerinin modern tehditlerle daha etkili bir şekilde mücadele etmelerini sağlar. Siber güvenlik savunmalarının güçlendirilmesi için MITRE ATT&CK'in sürekli olarak güncellenmesi ve uygulanması kritik öneme sahiptir.

KAYNAKÇA

MITRE ATT&CK®
ATT&CK - Wikipedia
https://attack.mitre.org/groups/G0034/
https://attack.mitre.org/campaigns/C0034/
https://www.serdarsargin.com.tr/article-title2/
https://berqnet.com/blog/mitre-attck-framework#
https://cyberartspro.com/mitre-attack-framework-nedir/
https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e
https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/detection-engineering/