Mitre Att&ck Framework

Hazırlayan: Saliha Polat

Tarih: 17.02.2025

İçindekiler

Giriş

Siber güvenlik, her geçen gün daha kritik bir hale gelen bir alan ve dijital dünyanın gelişmesiyle birlikte bu alandaki tehditler de hızla evrim geçiriyor. Bugün, bir şirketin ya da ülkenin altyapısının hedef alınması sadece veri hırsızlığı ya da mali kayıplar anlamına gelmiyor, aynı zamanda ulusal güvenlik ve toplumsal düzen üzerinde ciddi tehditler oluşturabiliyor. Bu bağlamda, siber güvenlik uzmanlarının kullandığı araçlar ve metodolojiler büyük önem taşıyor. MITRE ATT&CK framework de bu alandaki en önemli araçlardan biri olarak öne çıkıyor. Saldırıların nasıl gerçekleştiğini ve saldırganların hangi teknikleri kullandığını anlamak, savunma mekanizmalarının etkinliğini artırmak için kritik bir adımdır.

Bu yazıda, MITRE ATT&CK framework' ünün ne olduğunu, içinde yer alan Taktik, Teknik ve Prosedürlerin (TTP) ne anlama geldiğini ve bu yapının nasıl kullanılarak daha etkili bir siber tehdit avı gerçekleştirilebileceğini ele alacağız. Ayrıca, siber tehdit avı (Threat Hunting) ve tespit mühendisliği (detection engineering) gibi konulara da değinilecek ve gelişmiş saldırılara karşı nasıl daha iyi bir savunma stratejisi oluşturulabileceği üzerinde durulacaktır. 2022 yılında Ukrayna'nın elektrik altyapısına yapılan saldırı gibi büyük ölçekli olaylar, bu tür saldırılara karşı ne kadar hazırlıklı olmamız gerektiğini gösteriyor. Sonuç olarak, bu yazı hem siber güvenlikteki en son gelişmeleri hem de etkili saldırı tespit tekniklerini tartışarak, dijital dünyada daha güvenli bir ortam yaratmaya yönelik önemli ipuçları sunmaktadır.

MITRE ATT&CK

MITRE ATT&CK Tablosu Nedir?

Mitre Attack 1958'de kurulan tarafsız bir kuruluş olan MITRE Corporation, ABD'nin çeşitli alanlarda faaliyet gösteren devlet kurumları için çalışmaktadır. 2015 yılında MITRE Corp tarafından geliştirilmiş ve piyasaya sürülmüştür. Mitre Attack tablosu, saldırgan davranışının fiilen gözlemlenmesiyle toplanan siber saldırgan taktikleri ve tekniklerinden oluşan kapsamlı bir bilgi tabanıdır. Bu sistem ücretsiz ve herkese açıktır.

MITRE ATT&CK Tablosu Neden Önemlidir?

MITRE atak, bir suistimal gerçekleştikten sonra bir saldırganın davranışını daha iyi anlamak için kapsamlı bir sınıflandırma sağlar. Başka bir deyişle, çerçeve, bir saldırgan gibi düşünmenizi sağlar ve savunma önlemlerinizi bir saldırganın atması muhtemel adımlara karşı dengelemenize yardımcı olur. MITRE atak kullanmaktaki amaç, riskleri değerlendirme, yeni güvenlik kontrollerini devreye alma ve ağınızı savunma konusunda daha iyi kararlar vermektir.

MITRE ATT&CK, saldırıları çok tutarlı bir şekilde bölümlere ayırmıştır; bu da saldırıları karşılaştırmayı ve saldırganların ağınızdan nasıl yararlanmış olabileceğini belirlemeyi kolaylaştırır. Tipik saldırı analizinin aksine, mitre atak, saldırganları içeri girdikten sonra çok daha yakından inceler. Saldırı sonrası davranışın anlaşılması, ağ çevrelerinin hızla değiştiği için, günümüzde çok önemlidir. Bulut ağ iletişimi ve mobil kullanımlara geçiş arttıkça ve sürekli değişen saldırılar statik imzalardan kaçmaya devam ettikçe, bir noktada bir saldırganın ağınıza başarıyla sızması olasıdır. Mitre atak'ın saldırgan davranışına ayrıntılı bir şekilde odaklanması, devam eden bir saldırıyı veri hırsızlığı veya yıkıcı davranış gerçekleşmeden önce bulmanın ve durdurmanın en iyi yoludur.

MITRE ATT&CK, tek siber güvenlik çerçevesi değildir. Lockheed Martin Cyber Kill Chain, ISO/IEC 270011, NIST siber güvenlik çerçevesi2 ve COBIT3 gibi birkaç önemli güvenlik çerçevesi daha bulunmaktadır. MITRE ATT&CK, gerçek dünya testi ve süreci için son derece ayrıntılı yetenekler sağlar; MITRE ATT&CK'ı diğer güvenlik çerçevelerinden ayıran en önemli özelliği, saldırganın bakış açısından saldırının nasıl göründüğüne dair derin ve ayrıntılı veriler sunmasıdır. MITRE ATT&CK ayrıca bir saldırganın güvenlik ihlali sonrası davranışının en son ayrıntısına kadar odaklanır. Kavramsal olarak, MITRE ATT&CK, Cyber Kill Chain 'in bir alt kümesini kapsar, ancak çok daha fazla derinlik ve ayrıntıya girer. Enterprise ATT&CK; Windows, Linux, MacOS ve Android ve iOS kullanan mobil cihazları kapsar.

TTP Nedir?

TTP'ler taktikler, teknikler ve prosedürler anlamına gelir. Bu, siber güvenlik uzmanları tarafından bir tehdit aktörünün tehditler geliştirmek ve siber saldırılarda bulunmak için kullandığı davranışları, süreçleri, eylemleri ve stratejileri tanımlamak için kullanılan terimdir.

Taktikler: Saldırının ardındaki genel hedefler ve tehdit aktörünün saldırıyı uygulamak için izlediği genel stratejiler. Örneğin, tehdit aktörünün hedefi, müşteri kredi kartı bilgilerini çalmak için bir web sitesine sızmak olabilir.

Teknikler: Tehdit aktörünün saldırıya katılmak için kullandığı yöntem, örneğin e-skimming , magecart , javascript enjeksiyon saldırıları veya siteler arası betik çalıştırma (XSS) .

Prosedürler: Saldırının adım adım açıklaması, onu düzenlemek için kullanılan araçlar ve yöntemler dahil. Siber güvenlik analistleri genellikle bir tehdit aktörü veya tehdit grubu için bir profil veya parmak izi oluşturmaya yardımcı olmak için bir saldırının prosedürlerini kullanır.

Mitre Attack Framework' de Bulunan Taktik ve Tekniklerin Önemi?

Taktikler ve teknikler, Mitre'nin düşmanca davranışları kategorize etmesinin iki farklı yoludur. Mitre'nin tanımına göre, bir atak tekniği, düşmanların hedeflerine nasıl ulaştıklarını ve bazı durumlarda bu hedefe ulaşmaktan ne elde ettiklerini açıklar. Bir atak taktiği , saldırıyı gerçekleştirmenin amacını veya nedenini açıklar. Teknikler, saldırganların peşinde olduğu bilgileri ve bunları nasıl elde ettiklerini gösterir. Taktikler, bunu neden istediklerini açıklar. Taktiksel bir hedefe ulaşmak için birden fazla teknik kullanılabilir.

Güvenlik uzmanları, karşı istihbarat çabalarında kendilerine yardımcı olmak için bir tehdit aktörünün taktiklerini, tekniklerini ve prosedürlerini tanımlar ve analiz eder. TTP'ler, güvenlik araştırmacılarının bir saldırıyı bilinen bir bilgisayar korsanı veya tehdit grubuyla ilişkilendirmelerine ve bir saldırı çerçevesini daha iyi anlamalarına yardımcı olabilir. TTP'ler, araştırmacıların araştırma yollarını odaklamalarına, tehdit kaynağını veya saldırı vektörlerini belirlemelerine, tehdidin ciddiyetini tanımlamalarına ve olay yanıtını ve tehdit azaltmayı desteklemelerine yardımcı olur. Güvenlik uzmanları ayrıca tehdit modelleme faaliyetlerinde TTP' leri kullanır.

Güvenlik araştırmacıları tehdit aktörlerini ve gruplarını belirleyerek diğer saldırganlarla var olabilecek ilişkileri tespit edebilir. TTP'ler ayrıca ortaya çıkan tehditleri belirlemede ve tehdit ve saldırı önlemleri geliştirmede yardımcı olabilir.

Based Threat Hunting Nedir?

Siber Tehdit Avcılığı, bir ağ (network) ya da veri seti (data set) içerisinde var olan güvenlik çözümlerinden kaçan tehditleri proaktif ve tekrarlı olarak; arama, tespit etme ve izole etme sürecidir. Siber tehdit avcılığının proaktif bir yaklaşım ile uygulanması, sisteme zarar verecek herhangi bir olay gerçekleşmeden "önlem alma süreci" haline getirmektedir.

Geleneksel siber güvenlik çözümlerinin kullanıldığı bir kurum ağı içerisinde siber güvenlik amaçlı alarm değerlendirme sistemleri, sorgu tabanlı log yönetim sistemleri, ağ güvenliği için IDS/IPS (Intrusion Detection System) sistemleri, merkezi log toplama ve korelasyon işlemleri için SIEM (Security Information and Event Management) çözümleri ve bunların dışında farklı yazılım ve teknikler kullanılmaktadır. Tehdit avcılığı, güvenlik analistleri tarafından kullanılan aktif bir bilgi güvenliği süreci ve stratejisidir. Ağ, bulut ve uç nokta sistem günlüklerinde yinelemeli arama yaparak tehlike göstergelerini (IoC'ler); tehdit aktörü taktiklerini, tekniklerini ve prosedürlerini (TTP'ler); ve mevcut güvenlik sisteminizden kaçan gelişmiş kalıcı tehditler (APT'ler) gibi tehditleri tespit etmekten oluşur.

Siber Tehdit Avı ile Gelişmiş Saldırılar Nasıl Tespit Edilir?

Tehdit avcılığı kullanılarak gelişmiş saldırıların tespiti üç aşamadan oluşur: tetikleme, soruşturma ve çözüm.

Tetiklemek Anormal bir etkinlik algılanırsa, bir uyarı tetiklenir. Tehdit algılama araçları tehdidin tam olarak nerede bulunduğunu göstereceğinden, siber güvenlik ekipleri ağın hangi belirli alanını inceleyeceklerini bilirler. Güvenlik ekipleri daha sonra tehdidin sistem içindeki faaliyetleri hakkında bir hipotez geliştirebilir. Soruşturma Bir sonraki adım, toplanan verilerde yeni tehdit davranışları ve kalıpları bulmak için çeşitli taktiklere, tekniklere ve prosedürlere (TTP'ler) bakmaktır. Veri incelemesi, önceki adımda geliştirilen hipotez desteklenene veya çürütülene kadar devam eder. Çözünürlük Tehdidin doğası belirlendikten sonra, güvenlik uzmanları saldırıyı derhal etkisiz hale getirmeli, ardından ilk etapta hangi güvenlik açığının buna neden olduğunu anlamak için adımlar atmalıdır. Bu, güvenliği iyileştirmeye ve gelecekteki saldırıları önlemeye yardımcı olur.

En İyi 4 Etkili Tehdit Avlama Aracı Yönetilen tespit ve yanıt

(MDR): Güvenlik sağlayıcıları, kuruluşları tehditlerden korumak için MDR hizmetlerini dış kaynaklı bir hizmet olarak sunar. Uzaktaki bir tehdit avcıları ekibi, hizmetlerini kullanan kuruluş adına tehditleri belirler, analiz eder, araştırır ve bunlara yanıt verir.

SIEM: Güvenlik bilgisi ve olay yönetimi (SIEM), farklı kaynaklardan gelen güvenlik bilgilerini ve olay yönetimi verilerini bir araya getirir. Ağınızdaki çeşitli donanım ve yazılım bileşenleri tarafından üretilen güvenlik uyarılarının gerçek zamanlı analizini sağlayan yazılım ürünleri ve hizmetlerini kullanır.

Güvenlik Analitiği: BT sistemlerindeki olası güvenlik açıklarını bulmak için yazılım, algoritmalar ve analitik teknikleri bir araya getirir. Güvenlik analitiği araçları tehdit verileri hakkında anlaşılması kolay grafikler ve çizelgeler sağladığından, korelasyonları ve kalıpları tespit etmek daha hızlı ve çok daha kolaydır.

(EDR) Uç nokta tespiti ve yanıt Siber avlanma aracı olarak uç nokta tespit ve müdahale (EDR) sistemi aşağıdaki işlevleri yerine getirir:

- Bir tehdit belirtisi olabilecek uç nokta etkinlik verilerini gözlemleyin ve toplayın
- Herhangi bir tehdit modelini tespit etmek için bu bilgileri inceleyin
- Tehditler tespit edildiğinde otomatik olarak ortadan kaldırın veya kontrol altına alın ve ardından güvenlik personelini uyarın
- Tespit edilen riskleri araştırmak ve anormal aktiviteyi aramak için adli tıp ve analiz kullanın

Detection Engineering Nedir?

Tespit mühendisliği, bilgisayar ağlarında, yazılım sistemlerinde ve diğer dijital ortamlarda güvenlik tehditlerini tespit etmek ve ayrıca önemli zararlara yol açmadan önce olaylara müdahale etmek için sistemleri, araçları ve süreçleri (örneğin , güvenlik bilgisi ve olay

yönetimi (SIEM) sistemleri, ağ tespit ve yanıt (NDR) sistemleri, davranış analitiği ve makine öğrenimi algoritmaları) tasarlama ve uygulama sürecidir.

Detection Engineering Ne Yapar?

Detection Engineering, siber güvenlikte, bir organizasyonun güvenlik savunmalarını güçlendirmek için tehditleri tespit etmek ve izlemek amacıyla çeşitli alarmlar ve dedektörler geliştiren bir disiplindir. Bu alandaki profesyonellerin temel görevleri, güvenlik olaylarını erken tespit edebilmek için çeşitli veri kaynaklarını analiz etmek ve etkin algılama çözümleri tasarlamaktır. Detection Engineering'in görevleri:

Alarm ve Kural Geliştirme: Ağ trafiği, loglar, dosya değişiklikleri ve diğer veri kaynaklarını inceleyerek anormal etkinlikleri ve saldırı göstergelerini tanımlayan alarmlar ve kurallar oluşturur.

Algılama Sistemlerinin Yönetimi: Güvenlik araçları ve sistemleri (örneğin, SIEM, IDS/IPS, EDR) üzerinde çalışan tespit algoritmalarını optimize eder.

Saldırı Taktikleri, Teknikleri ve Prosedürlerinin (TTPs) İzlenmesi: Saldırganların kullanabileceği yöntemleri belirleyerek, bu tehditleri erken aşamada tespit edebilmek için algılama kuralları geliştirir.

Veri Analizi ve Olay Tespiti: Toplanan güvenlik verilerini analiz eder ve olası tehditleri belirler. Bu, örneğin ağ trafiği, kullanıcı etkinlikleri veya sistem loglarının incelenmesini içerebilir.

False Positive Azaltılması: Yanlış alarm oranlarını (False Positive) en aza indirgemek için kuralları ve algoritmaları iyileştirir, böylece yalnızca gerçek tehditler tespit edilir.

Gelişmiş Analitik ve Makine Öğrenmesi: Daha karmaşık tehditleri tespit edebilmek için makine öğrenmesi ve yapay zeka tabanlı yöntemler kullanabilir.

Güvenlik İstihbaratı ve İleri Tespit: Tehdit istihbaratını kullanarak yeni saldırı vektörlerine karşı tespit yöntemleri geliştirebilir.

Detection Engineering, güvenlik ekiplerinin daha hızlı ve etkili bir şekilde tehditleri anlamalarına ve müdahale etmelerine olanak tanır. Bu alanda çalışan kişiler, siber güvenlik tehditlerini anlayan, analitik ve teknik becerilere sahip olmalıdır.

2022 Ukraine Electric Power Attack C0034 İncelemesi

2022 Ukraine Electric Power Attack (C0034), Ukrayna'nın elektrik altyapısını hedef alan çok aşamalı bir siber saldırı kampanyasıdır. Saldırganlar, enerji şirketlerinin sistemlerine sızarak operasyonlarını aksatmayı ve büyük ölçekli elektrik kesintileri oluşturmayı amaçlamıştır. Bu saldırıda saldırganlar Ukrayna'nın enerji şebekelerini hedef alarak kritik altyapı sistemlerini bozup büyük çapta elektrik kesintilerine ve altyapı bozulmalarına neden olmuştur. Saldırı, Sandworm Team tarafından gerçekleştirilmiş olup, MITRE ATT&CK framework'üne göre çeşitli teknikler kullanılmıştır.

Bu saldırıda saldırganlar Ukrayna elektrik şirketlerini, enerji iletim sistemlerini ve kritik altyapı sistemlerini hedef almıştır. Amaçları elektrik kesintileri oluşturarak Ukrayna'nın enerji altyapısına zarar vermek, SCADA sistemlerine zarar vermek, endüstriyel süreçleri sabote etmek ve kamu hizmetlerini sekteye uğratmaktı. Bunun için zararlı yazılım kullanarak sistemlere sızma, kimlik avı teknikleriyle yetkilendirilmiş hesapları ele geçirme, uzak erişimle ağ içinde yayılma ve şebeke operasyonlarını sabote etme, yanal hareket, uzaktan erişim ve SCADA sistemlerine yetkisiz komut gönderme gibi yöntemler kullandılar.

Kullanılan Mitre Attack Teknikleri ve TID Değerleri

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilized a PowerShell utility called TANKTRAP to spread and launch a wiper using Windows Group Policy.[1]
Enterprise	T1543	.002	Create or Modify System Process: Systemd Service	During the 2022 Ukraine Electric Power Attack, Sandworm Team configured Systemd to maintain persistence of GOGETTER, specifying the `WantedBy=multi-user.target` configuration to run GOGETTER when the system begins accepting user logins.[1]
Enterprise	T1485		Data Destruction	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed CaddyWiper on the victim's IT environment systems to wipe files related to the OT capabilities, along with mapped drives, and physical drive partitions.[1]
Enterprise	T1484	.001	Domain or Tenant Policy Modification: Group Policy Modification	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Group Policy Objects (GPOs) to deploy and execute malware.[1]
Enterprise	T1570		Lateral Tool Transfer	During the 2022 Ukraine Electric Power Attack, Sandworm Team used a Group Policy Object (GPO) to copy CaddyWiper's executable `msserver.exe` from a staging server to a local hard drive before deployment.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Systemd service units to masquerade GOGETTER malware as legitimate or seemingly legitimate services.[1]
Enterprise	T1095		Non-Application Layer Protocol	During the 2022 Ukraine Electric Power Attack, Sandworm Team proxied C2 communications within a TLS-based tunnel.[1]
Enterprise	T1572		Protocol Tunneling	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the GOGETTER tunneler software to establish a "Yamux" TLS-based C2 channel with an external server(s).[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Scheduled Tasks through a Group Policy Object (GPO) to execute CaddyWiper at a predetermined time.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the Neo-REGEORG webshell on an internet-facing server.[1]
ICS	T0895		Autorun Image	During the 2022 Ukraine Electric Power Attack, Sandworm Team used existing hypervisor access to map an ISO image named `a.iso` to a virtual machine running a SCADA server. The SCADA server's operating system was configured to autorun CD-ROM images, and as a result, a malicious VBS script on the ISO image was automatically executed.[1]
ICS	T0807		Command-Line Interface	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged the SCIL-API on the MicroSCADA platform to execute commands through the `scilc.exe` binary.[1]
ICS	T0853		Scripting	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilizes a Visual Basic script `lun.vbs` to execute `n.bat` which then executed the MicroSCADA `scilc.exe` command.[1]
ICS	T0894		System Binary Proxy Execution	During the 2022 Ukraine Electric Power Attack, Sandworm Team executed a MicroSCADA application binary `scilc.exe` to send a predefined list of SCADA instructions specified in a file defined by the adversary, `s1.txt`. The executed command `C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt` leverages the SCADA software to send unauthorized command messages to remote substations.[1]
ICS	T0855		Unauthorized Command Message	During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[1]

Saldırı Aşamaları

1. Initial Access (Başlangıç Erişimi)

Sandworm Team, hedef elektrik şirketlerinde çalışan kişilere yönelik **spear-phishing** saldırıları düzenledi.

Zararlı ekler içeren e-postalar ile çalışanların cihazlarına erişim sağlandı.

PowerShell tabanlı bir zararlı yazılım (TANKTRAP) kullanılarak ilk erişim elde edildi.

2. Privilege Escalation & Lateral Movement (Yetki Yükseltme ve Yanal Hareket)

Ele geçirilen sistemlerde Systemd Service (T1543.002) ile kalıcılık sağlandı.

Group Policy Objects (GPO) değişiklikleri (T1484.001) yapılarak kötü amaçlı yazılım dağıtıldı.

Ele geçirilen hesaplar ile sistemde yanal hareket (T1570) gerçekleştirilerek SCADA bileşenlerine erişim sağlandı.

3. Defense Evasion &Discovery)

SCADA sistemlerine ulaşmak için ağ keşfi yapıldı (T1018 – Remote System Discovery).

Yetkisiz erişimi gizlemek için Non- Application Layer Protocol (T1095) ve Protocol Tunneling (T1572) teknikleri kullanıldı.

4. ICS Attack Techniques (SCADA Sistemlerinin Ele Geçirilmesi ve Manipülasyonu)

SCADA kontrol sistemlerine yönelik komutlar Unauthorized Command Message (T0855) yöntemiyle çalıştırıldı.

Command – Line Interface (T0807) ve Script (T0853) teknikleri kullanılarak otomatik komut dosyaları çalıştırıldı.

Enerji yönetim süreçlerine zarar vermek amacıyla MicroSCADA bileşenlerine yetkisiz erişim sağlandı.

5. Impact (Sisteme Zarar verme ve Son Aşama)

CaddyWiper zararlısı kullanılarak sistemdeki kritik dosyalar silindi. (T1485 – Data Destuction).

SCADA sistemleri tamamen işlevsiz hale getirildi.

Network Denial of Service (T1498) saldırısı ile enerji iletim sistemleri çökertildi.

Saldırıda kullanılan teknikler, MITRE ATT&CK framework'üne dayalı olarak tespit edilen birçok farklı aşamadan oluşmuştur. Bu, sadece elektrik altyapısına zarar vermekle kalmamış, aynı zamanda ülkenin kritik endüstriyel süreçlerini de sekteye uğratmıştır.

Sonuç olarak, bu tür saldırılar, kritik altyapıları hedef alan siber tehditlerin artan tehdit ortamını yansıtmaktadır. Enerji altyapıları ve SCADA sistemleri gibi kritik bileşenlere yönelik tehditlerin önlenmesi, sadece teknik önlemlerle değil, aynı zamanda iyi bir farkındalık ve siber savunma stratejisi ile mümkün olacaktır. Bu saldırı, ulusal güvenliği tehdit eden siber saldırıların daha geniş çapta etki yaratabileceğini ve uluslararası iş birliklerinin bu tür tehditlere karşı daha güçlü bir şekilde organize edilmesi gerektiğini bir kez daha göstermektedir.

Olası Senaryo Örneği

Senaryo: Bir E-Ticaret Sitesinin Hacklenmesi

1. **Adım : Reconnaissance (Keşif)**

Saldırganlar siteyi hacklemek için öncelikle hedef hakkında bilgi toplamalılar. Sitenin web uygulamasındaki açıkları bulmak için Google Dorking, Whois sorguları ve Shodan taramaları yapabilirler. Çalışanların kişisel bilgilerine ulaşmak için sosyal medya taramaları yapabilirler.

Kullanılan Mitre Attack Tekniklerinin TID Değerleri :

- T1595 – Active Scanning (Aktif Keşif)
- T1593 – OSINT (Açık Kaynak İstihbaratı)

2. **Adım : Initial Access (Başlangıç Erişimi)**

Saldırganlar şirketin müşteri destek ekibinde çalışan bir kişiye özel hazırlanmış phishing e-postası gönderir. E-posta, müşteri şikayetlerini içeren sahte bir PDF içerir ve ekipte çalışan kişinin açmasıyla giriş bilgilerini çalan bir keylogger yükler.

Kullanılan Mitre Attack Tekniklerinin TID Değerleri :

- T1566.001 – Spear Phishing
- T1056.001 – Keylogger

3. **Adım : Privilege Escalation (Yetki Yükseltme)**

Saldırganlar, ele geçirilen bilgileri kullanarak şirketin içerisindeki sistemlerine sızar. Daha yüksek yetkilere sahip bir hesabı ele geçirmek için şirketin eski bir web uygulamasındaki SQL Injection açığını kullanarak veri tabanındaki parolaları çalar ve hashlerini kırar.

Kullanılan Mitre Attack Tekniklerinin TID Değerleri :

- T1078 – Geçerli Kimlik Bilgilerinin Kullanımı
- T1190 – SQL Injection (Web Uygulama Açıkları)

4. **Adım : Defense Evasion (Savunmadan Kaçınma)**

Saldırganlar, tespit edilmemek için kötü amaçlı davranışların sistem yöneticileri tarafından fark edilmemesi için Proxy araçları kullanarak yönlendirirler. Ayrıca, güvenlik yazılımlarının takibini zorlaştırmak için log dosyalarını temizler.

Kullanılan Mitre Attack Tekniklerinin TID Değerleri :

- T1070.002 – Log dosyalarının Manipülasyonu

- T1090 – Proxy Kullanımı

5. Adım : Exfiltration & Impact (Veri Çalma ve Sistemleri Kapatma)

Saldırganlar, şirketin müşteri ödeme bilgilerini ele geçirerek dark web' de satışa çıkarır. Ayrıca, saldırıyı gizlemek için e-ticaret sitesine Web Shell yerleştirerek uzun süreli erişim sağlarlar ve şirkete büyük ölçekte maddi ve manevi zarar verirler.

Kullanılan Mitre Attack Tekniklerinin TID Değerleri :

- T1041 – Exfiltration Over C2 Channel (Veri Dışarı Sızdırma)
- T1005.003 – Web Shell Kullanımı

Sonuç olarak saldırı sonunda, şirket müşteri ödeme bilgilerini kaybeder ve güvenilirliği büyük ölçüde zarar görür. Bu tür saldırılara karşı şirketin güçlü parola politikaları, phishing farkındalık eğitimleri, web uygulama güvenlik testleri (WAF) ve olay müdahale planları gibi önlemler alması gerekir.

Sonuç

Sonuç olarak, MITRE ATT&CK'in sunduğu kapsamlı yaklaşım, siber güvenlikteki en güncel tehditlere karşı savunmayı güçlendirmenin yanı sıra, tüm sektörlerde daha dayanıklı ve güvenli dijital altyapıların oluşturulmasına büyük katkı sağlar. Bu framework, saldırganların kullandığı yöntemleri ve teknikleri anlamamıza olanak tanır, böylece savunma stratejilerimizi daha etkili hale getirebiliriz. Saldırıların nasıl gerçekleştiğini bilmek, bunlara karşı hazırlıklı olmak ve erken tespitler yapabilmek, dijital güvenliği sağlamada en önemli faktörlerden biridir. Teknolojinin hızla geliştiği ve dijital dünyada her geçen gün daha fazla tehdit ortaya çıktığı bu dönemde, saldırganların stratejilerini anlamak, doğru araçlar ve metodolojilerle onlara karşı koymak büyük önem taşır. Bu yazıda ele alınan bilgiler ve öneriler, siber güvenlik profesyonellerinin daha hazırlıklı ve bilinçli bir yaklaşım benimsemelerine yardımcı olacak, aynı zamanda organizasyonların karşılaşabileceği yeni tehditlere karşı daha sağlam bir savunma inşa etmelerini sağlayacaktır. Dijital dünyada güvenliği sağlamak, sadece teknik çözümlerle değil, doğru strateji ve iş birlikleriyle mümkün olacaktır.

Kaynakça

CrowdStrike. (t.y.). *Detection Engineering*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/detection-engineering/

Exabeam. (t.y.). *Threat Hunting: Tips and Tools*. Exabeam. https://www.exabeam.com/explainers/information-security/threat-hunting-tips-and-tools/

Exclusive Networks. (2020). *MITRE ATT&CK InfoBlox*. Exclusive Networks. https://www.exclusive-networks.com/tr/wp-content/uploads/sites/32/2020/12/MITRE-ATTCK-InfoBlox-.pdf

Feroot. (t.y.). *What Are Tactics, Techniques, and Procedures (TTPs)?* Feroot. https://www.feroot.com/education-center/what-are-tactics-techniques-and-procedures-ttps/

Fortinet. (t.y.). *Threat Hunting*. Fortinet. https://www.fortinet.com/resources/cyberglossary/threat-hunting

MITRE. (t.y.). *MITRE ATT&CK Enterprise Matrix*. MITRE ATT&CK. https://attack.mitre.org/matrices/enterprise/

Netenrich. (t.y.). *What Is Detection Engineering?* Netenrich. https://netenrich.com/blog/what-is-detection-engineering

Onur Oktay. (2022). *Detection Engineer Ne Yapar? Günlük Görevleri & Rutinleri*. Medium. https://medium.com/@onuroktay/detection-engineer-ne-yapar-g%C3%BCnl%C3%BCk-g%C3%B6revleri-rutinleri-nelerdir-1d6a23a4fee4

Picus Security. (t.y.). *The Top Ten MITRE ATT&CK Techniques*. Picus Security. https://www.picussecurity.com/resource/the-top-ten-mitre-attck-techniques

Siber Tehdit Avcılığı. (2018). *Siber Tehdit Avcılığı Nedir? (Cyber Threat Hunting)*. BGA Security. https://www.bgasecurity.com/2018/02/siber-tehdit-avciligi-nedir-cyber-threat-hunting/

SOC Prime. (t.y.). *What Is Detection Engineering?* SOC Prime. https://socprime.com/blog/what-is-detection-engineering/

Splunk. (t.y.). *TTP: Tactics, Techniques, and Procedures*. Splunk. https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html

Splunk. (t.y.). *Threat Actors*. Splunk. https://www.splunk.com/en_us/blog/learn/threat-actors.html

TechTarget. (t.y.). *MITRE ATT&CK Framework*. TechTarget. https://www.techtarget.com/searchsecurity/definition/MITRE-ATTCK-framework

Bilişim Hareketi. (2023). *Cyber Threat Hunting Nedir?* Medium. https://medium.com/bili%C5%9Fim-hareketi/cyber-threat-hunting-nedir-cabfdf01e06b

Xcitium. (t.y.). *Detection Engineering*. Xcitium. https://www.xcitium.com/detection-engineering/

"Russian Strikes Against Ukrainian Infrastructure (2022–present)." *Wikipedia*. Erişim: https://en.wikipedia.org/wiki/Russian_strikes_against_Ukrainian_infrastructure_(2022%E2%80%93present).

"The Economic Toll of Attacks on Ukraine's Power Grid." *Centre for Economic Policy Research (CEPR)*, 2023. Erişim: https://cepr.org/voxeu/columns/economic-toll-attacks-ukraines-power-grid.

"Russian Spies Behind Cyberattack on Ukrainian Power Grid – 2022: Researchers." *Reuters*, 9 Kasım 2023. Erişim: https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/.

"Ukraine: Russian Attacks on Energy Grid Threaten Civilians." *Human Rights Watch*, 6 Aralık 2022. Erişim: https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians.

"Campaign: C0034." *MITRE ATT&CK*. Erişim: https://attack.mitre.org/campaigns/C0034/.