ALTAY TAKIMI

CYBER KILL CHAIN RAPORU

HAZIRLAYAN:GÜRKAN PARLAK
17.02.2025

İÇİNDEKİLER

Giriş 3
MITRE ATT&CK Nedir? 4
Enterprise ATT&CK 4
1-Reconnaissance (Keşif) 4
2-Resource Development (Kaynak geliştirme) 5
3-Initial Access (İlk Erişim) 5
4-Execution (Yürütme) 5
5-Persistence (Kalıcılık) 5
6-Privilege Escalation (Ayrıcalık Arttırma) 5
7-Defense Evasion (Savunmadan Kaçınma) 5
8-Credential Access (Kimlik Bilgileri Erişimi) 5
9-Discovery (Keşif) 5
10-Lateral Movement (Yanal Hareket) 6
11-Collection (Toplama) 6
12-Command and Control (Komut ve Kontrol) 6
13-Exfiltration (Sızma) 6
14-Impact (Etki) 6
MITRE ATT&CK Neden Önemlidir? 6
MITRE ATT&CK Framework Taktik ve Tekniklerin Önemi 7
TTP Nedir? 8
TTP-Based Threat Hunting 8
TTP-Based Detection Engineering (TTP Tabanlı Tespit Mühendisliği) 8
TTP Tabanlı Tehdit Avcılığı ve Tespit Mühendisliğinin Önemi 9
Ukrayna Electric Power Attack 9
Senaryo 10
Sonuç 11
Kaynakça 12

Giriş

Bu rapor, Mitre ATT&CK Framework'ün siber güvenlik alanındaki önemini, saldırganların davranışlarını analiz etmek ve tespit etmek için nasıl kullanıldığını açıklamaktadır. Bu raporda, Mitre ATT&CK Tablosu'nun ne olduğunu, önemini, taktik ve tekniklerin nasıl kullanıldığını, TTP (Taktikler, Teknikler ve Prosedürler) kavramını ve bunların tehdit avcılığı ve tespit mühendisliği süreçlerindeki rolünü detaylandırmaktadır.

Ayrıca, 2022 Ukrayna Elektrik Gücü Saldırısı örneği üzerinden Mitre ATT&CK Framework'ün nasıl uygulandığı ve hangi tekniklerin kullanıldığı TID değerleriyle açıklanmaktadır.

Son olarak, bu raporda, bir şirketin hacklenmesi üzerine oluşturulacak senaryo ile saldırganların keşif aşamasından itibaren nasıl ilerlediği anlatılacak ve bu saldırı süreci boyunca kullanılan taktikler ve teknikler Mitre ATT&CK Tablosu üzerinden analiz edilmektedir.

Bu rapor, Mitre ATT&CK çerçevesini derinlemesine inceleyerek, siber güvenlik analistlerinin saldırıları tespit etme ve önleme stratejileri geliştirme konusunda bilgi sahibi olmalarını amaçlamaktadır.

MITRE ATT&CK Nedir?

Mitre ATT&CK Framework, siber dünyada saldırganların sisteme yapabileceği eylemleri gösteren teknik, taktik ve prosedürleri gösteren bir bilgi tabanıdır. 2013 yılından itibaren Mitre firması tarafından geliştirilmekte olan Mitre ATT&CK (Adversarial Tacticks, Techniques and Common Knowledge) saldırganların davranışlarını sistematik olarak kategorize etme ihtiyacından doğmuştur.

Söz konusu siber güvenlik olayını çözüme kavuşturmak için, saldırganların mevcut sistemdeki faaliyetlerinin sınıflandırılması gerekmektedir. Saldırganlar, mevcut güvenlik önlemleriyle tespit edilmemesi için saldırı yöntemlerini değiştireceklerdir. Siber vakanın çözüme kavuşturulmasında görev alan güvenlik ekiplerinin de olaya yaklaşımlarını geliştirmeleri gerekecektir.

Saldırganın, hedefi doğrultusunda alabileceği aksiyonlara karşı risklerin belirlenmesi, gerekli iyileştirme ve planlamaların yapılması, alınan güvenlik önlemlerinin doğruluğunu kontrol etmek için kullanılmaktadır.

MITRE ATT&CK, birkaç farklı matristen oluşmaktadır.

Enterprise ATT&CK: Windows, Linux veya MacOS sistemlerine uygulanan teknik ve taktiklerden oluşur.
Mobile ATT&CK: Mobil cihazlara uygulanan taktikleri ve teknikleri içerir.
Pre-ATT&CK: Saldırganların sisteme girmeden önceki çalışmalarını içeren taktik ve teknikleri içerir.

Enterprise ATT&CK

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. Matrisin hangi yerinde bulunduğunuzu tespit ederek süreci hızla ilerletebilmek mümkündür.

1-Reconnaissance (Keşif)

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. Aktif bilgi toplanan sistem bilgilerine; bilişim sisteminin altyapı ve personel bilgileri gibi hassas verilerini içerebilmektedir.

2-Resource Development (Kaynak geliştirme)
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.

3-Initial Access (İlk Erişim)
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 sağlar.

4-Execution (Yürütme)
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.

5-Persistence (Kalıcılık)
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.

6-Privilege Escalation (Ayrıcalık Arttırma)
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.

7-Defense Evasion (Savunmadan Kaçınma)
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.

8-Credential Access (Kimlik Bilgileri Erişimi)
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.

9-Discovery (Keşif)

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.

10-Lateral Movement (Yanal Hareket)

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.

11-Collection (Toplama)

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.

12-Command and Control (Komut ve Kontrol)

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.

13-Exfiltration (Sızma)

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

14-Impact (Etki)

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.

MITRE ATT&CK Neden Önemlidir?

MITRE ATT&CK için en iyi kullanım örnekleri arasında Red Team Sızma testi, tehdit istihbaratı, Blue Team için son derece önemlidir.

Red Team Sızma (Penetrasyon) Testi

Red Team taktikleri ve teknikleri yıllar içinde gelişmiş, ancak kullanılması gereken en iyi uygulamalar konusunda fikir birliğine varamamıştır. MITRE ATT&CK, Red Team'lerin standart bir sözlük kullanmalarına ve çalışmalarını planlamada onları

destekleyen taktikleri ve temel teknikleri seçme konusunda düzenli, oldukça organize bir yaklaşım kullanmalarına olanak tanır. MITRE ATT&CK ayrıca Red Team'lerin hem kullandıkları tekniklerle hem de bu teknikleri dağıtma sıralarıyla ve ayrıca dağıttıkları belirli yazılım araçlarıyla gerçek dünyadaki saldırganları modellemelerine de olanak tanır.

Tehdit İstihbaratı
Günümüzde bir güvenlik operasyon merkezinin ve Blue Team'in tehdit istihbarat raporlarına zamanında yanıt vermesi çok zor. Verdikleri ilk tepki genellikle "Bu konuda ne yapmamızı önerirsiniz?" oluyor. Siber saldırganlar daha hızlı hareket ediyor. Siber savunucuların, saldırganlara karşı avantaj elde etmek ve bu avantajı sürdürmek için, güvenlik ihlali olaylarına, imza ve IP adresi gibi metriklere bağımlı olmaktan uzaklaşarak daha davranışsal bir yaklaşıma geçmeleri gerekir.
MITRE ATT&CK, tehdit istihbaratını yapılandırmanın bir yolunu sağlar. IP adresleri ve etki alanları gibi göstergelere odaklanmak yerine belirli davranışlara odaklanırsınız. Daha sonra bunu saldırı tekniğiyle eşleştirebilir ve savunucuların güvenlik açıklarını daha doğru bir şekilde belirlemek, riskleri değerlendirmek ve hafifletme planı yapmak için kullanabileceği çok daha iyi ve tutarlı bir şekilde organize edilmiş veriler sunulabilir.

Blue Team
Blue Team, potansiyel bir siber saldırganın anatomisini daha iyi anlayabilirler. Bu anlayış, mevcut bir saldırıda kullanılan tekniklerin hızlı bir şekilde sınıflandırılmasını, saldırganın kimliğine ilişkin olası bilgileri, kuruma yönelik en olası tehditlerin gelişmiş risk değerlendirmesini ve sonrasında bu tehditlerin objektif olarak ayrıştırılarak siber güvenlik altyapınızın neresinde güvenlik açıkları olabileceğinin anlaşılmasını içerir. Daha sonra bu güvenlik açıkları önceliklendirilebilir ve engellenir.

MITRE ATT&CK Framework Taktik ve Tekniklerin Önemi

1. Saldırı Aşamalarını Anlama
MITRE ATT&CK, saldırıların başlangıcından veri sızdırma aşamasına kadar olan tüm süreçleri adım adım açıklar. Bu sayede, saldırının hangi aşamada olduğunu tespit etmek ve buna göre önlem almak daha kolay olur.

2. Savunma Stratejilerini Güçlendirme
Her taktik altında belirtilen teknikler, güvenlik önlemlerinin nereye odaklanması gerektiğini gösterir.
Bu durumda güvenlik analistleri atak vektörlerine uygun güvenlik önlemleri alabilir ve süreci daha iyi yönetebilir.

3. Güvenlik Çözümlerinin Daha İyi Kullanımı
SIEM,SOAR,EDR gibi güvenlik çözümleri için MITRE tekniklerine göre kurallar oluşturulabilir. Bu sayede bu ürünlerin daha verimli kullanımı sağlanmış olur.

4. Olay Müdahale Süreçlerini İyileştirme
Her taktik, bir saldırının hangi aşamada durdurulabileceğine dair rehberlik eder. Bu sayede saldırıyı en kısa süre içerisinde tespit ve müdahele şansı artar.

5. Red Team ve Blue Team İşbirliğini Güçlendirme

Red Team, MITRE tekniklerini kullanarak saldırılar düzenler. Blue Team, bu saldırıları MITRE taktiklerine göre izler ve savunma stratejilerini geliştirir.

TTP Nedir?

TTP (Tactics, Techniques, and Procedures), siber tehdit aktörlerinin (saldırganların) kullandığı taktikler, teknikler ve prosedürler anlamına gelir. Bu üç bileşen, bir saldırının nasıl yapıldığını ve saldırganların hedeflerine ulaşmak için kullandıkları yöntemleri anlamamıza yardımcı olur.

Tactic (Taktik): Bir saldırganın elde etmeyi amaçladığı hedef veya stratejidir. Bu, bir saldırının genel amacıdır. Örneğin, "ilk erişim" (Initial Access) veya "yetki yükseltme" (Privilege Escalation) gibi amaçlar olabilir.

Technique (Teknik): Saldırganın taktiği gerçekleştirmek için kullandığı belirli yöntemdir. Örneğin, "kimlik avı" (Phishing) veya "sosyal mühendislik" gibi teknikler, saldırganların "ilk erişim" sağlamak için kullandıkları araçlardır.

Procedure (Prosedür): Tekniklerin ve taktiklerin uygulanma biçimidir. Bu, saldırganın kullandığı özel araçlar, komutlar veya süreçler olabilir. Örneğin, bir saldırganın "kimlik avı" yapmak için kullandığı belirli e-posta şablonları veya otomatikleştirilmiş araçlar.

TTP-Based Threat Hunting

TTP-Based Threat Hunting, TTP-Based Detection Engineering ve genel olarak TTP tabanlı tehdit avcılığı ve algılama mühendisliği kavramları, MITRE ATT&CK framework ve benzeri framework'ler üzerinden, saldırganların saldırı yöntemlerini anlamak ve bu yöntemlere karşı savunma stratejileri geliştirmek için kullanılan bir yaklaşımdır.

TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı)
TTP tabanlı tehdit avcılığı, saldırganların kullandığı taktikler, teknikler ve prosedürler hakkında önceden bilgi sahibi olarak, bu saldırı yöntemlerine karşı aktif bir şekilde avlanmayı ifade eder.

Örnek:
Bir tehdit avcısı, ağ trafiğini ve işlem günlüklerini inceleyerek, Lateral Movement (yanal hareket) ve Credential Dumping gibi saldırı tekniklerine dair izler arar. Bu, ağda yapılan şüpheli aktiviteleri tespit etmek için kullanılabilecek bir yöntemdir.

TTP-Based Detection Engineering (TTP Tabanlı Tespit Mühendisliği)

TTP tabanlı algılama mühendisliği, belirli saldırı tekniklerini, taktiklerini ve prosedürlerini tespit etmek için kuralların oluşturulması ve sistemlerin yapılandırılması sürecidir. Burada amaç, saldırganların kullandığı yöntemlere dair belirli işaretler ve izler aracılığıyla güvenlik sistemlerinde alarmlar oluşturmak ve anomali tespiti yapmaktır.

Örnek:

Bir tespit mühendisi, şüpheli PowerShell etkinliği tekniğine karşı, PowerShell komutlarının doğruluğunu ve amacını analiz eden bir kural oluşturur. Bu, şüpheli komutların anında tespit edilmesini sağlar.

TTP Tabanlı Tehdit Avcılığı ve Tespit Mühendisliğinin Önemi

Proaktif Savunma Sağlar: TTP tabanlı tehdit avcılığı, yalnızca geçmişteki olayları incelemekle kalmaz, aynı zamanda gelecekteki saldırıları tahmin etmeye ve bu saldırılara karşı önlem almayı hedefler.

Gelişmiş Tespit Yetenekleri: Algılama mühendisliği, yalnızca mevcut tehditlere karşı değil, gelecekteki saldırılara karşı da etkin bir savunma sağlar. Buna göre güvenlik önlemleri geliştirir.

Zamanında Müdahale: Saldırıların erken tespiti, hızlı olay müdahele süreci izlenir bu sayede daha güvenli bir yapı oluşturulur.

Sürekli İyileştirme: Bu süreçler, organizasyonların sürekli olarak siber güvenlik önlemlerini güçlendirmesine yardımcı olur, çünkü her yeni saldırı tipi ve tekniği ile daha iyi mücadele etmek için gelişmiş algılama kuralları oluşturulabilir.

TTP tabanlı tehdit avcılığı ve algılama mühendisliği, siber güvenlikte savunma mekanizmalarının daha hedeflenmiş ve etkili olmasını sağlar. Bu yaklaşım, tehditlerin tespiti ve engellenmesi konusunda önemli bir stratejidir ve organizasyonların sürekli değişen siber tehdit ortamında daha hazırlıklı olmasına yardımcı olur.

Ukrayna Electric Power Attack

2022 Ukrayna Electric Power Attack, Rusya bağlantılı Sandworm grubu tarafından Ukrayna'nın enerji altyapısını hedef alan çok katmanlı bir siber saldırıdır. Bu saldırıda hem bilgi teknolojileri (IT) hem de endüstriyel kontrol sistemleri etkilenmiştir. Sandworm ekibi, PowerShell üzerinden zararlı yazılımlar dağıtmış, Group Policy Objects kullanarak ağ içinde yanal hareket etmiş ve Systemd servislerini kullanarak kalıcılık sağlamıştır. Ayrıca, SCADA sistemlerine ISO dosyaları üzerinden otomatik çalıştırmalar yoluyla yetkisiz komutlar gönderilmiştir. Saldırı sonucunda enerji dağıtımında aksaklıklar yaşanmış, Ukrayna'nın kritik altyapısı ciddi zarar görmüştür.

TID Değeri	Adı	Kullanımı
T1059.001	Command and Scripting Interpreter: PowerShell	Sandworm ekibi, TANKTRAP adlı bir PowerShell aracını kullanarak wiper yazılımını Windows Group Policy üzerinden yaydı ve çalıştırdı.
T1543.002	Create or Modify System Process: Systemd Service	Sandworm ekibi, GOGETTER adlı zararlı yazılımın oturum açma sırasında çalıştırılması için Systemd üzerinde persistence sağladı.
T1485	Data Destruction	CaddyWiper yazılımı kullanılarak OT sistemleriyle ilişkili dosyalar, harici sürücüler ve fiziksel disk bölümleri silindi.
T1484.001	Domain or Tenant Policy Modification:	Açıklama: Malware dağıtımı ve çalıştırılması için Group Policy Objects (GPO) kullanıldı.Açıklama:

	Group Policy Modification	Malware dağıtımı ve çalıştırılması için Group Policy Objects (GPO) kullanıldı.
T1570	Lateral Tool Transfer	GPO aracılığıyla msserver.exe adlı CaddyWiper dosyası, bir hazırlık sunucusundan yerel diske taşındı.
T1036.004	Masquerading: Masquerade Task or Service	GOGETTER zararlı yazılımı, Systemd servis birimlerinde yasal görünümlü bir hizmet gibi gizlendi.
T1095	Non-Application Layer Protocol	C2 (Komuta ve Kontrol) iletişimleri TLS-tabanlı bir tünel üzerinden proxylenerek gerçekleştirildi.
T1572	Protocol Tunneling	Yamux tabanlı TLS tüneli kullanılarak GOGETTER yazılımı ile dış sunucular arasında C2 kanalı kuruldu.
T1053.005	Scheduled Task/Job: Scheduled Task	CaddyWiper, belirli bir zamanda çalıştırılmak üzere GPO ile zamanlanmış görev olarak ayarlandı.
T1505.003	Server Software Component: Web Shell	Neo-REGEORG web shell, internet üzerinden erişilebilen bir sunucuya yerleştirildi.
T0895	Autorun Image	Bir ISO dosyası, SCADA sunucusuna otomatik çalıştırılacak şekilde bağlanarak kötü amaçlı bir VBS scripti çalıştırıldı.
T0807	Command-Line Interface	MicroSCADA platformunda SCIL-API kullanılarak komutlar doğrudan scilc.exe ile çalıştırıldı.
T0853	Scripting	lun.vbs adlı bir Visual Basic scripti kullanılarak n.bat çalıştırıldı ve ardından SCADA komutları icra edildi.
T0894	System Binary Proxy Execution	scilc.exe kullanılarak SCADA yazılımı üzerinden yetkisiz komutlar uzak alt istasyonlara gönderildi.
T0855	Unauthorized Command Message	SCIL-API üzerinden SCADA alt istasyon cihazlarına yetkisiz komut mesajları iletildi.

Senaryo

Oğuzlar Siber Güvenlik beklenmedik bir sistem kesintisi ile karşı karşıya kalır. Şirketin güvenlik ekibi, olayın bir siber saldırıdan kaynaklandığını tespit eder. Yapılan incelemeler sonucunda, saldırganların sosyal mühendislik ile başlayan ve kritik sistemlere sızılmaya kadar giden bir süreç olduğunu tespit eder.

Taktik	**Teknik**	**TID**
1. Keşif (Reconnaissance)	Phishing üzerinden bilgi toplama	T1598
	OSINT kullanarak çalışan bilgilerini toplama	T1593
2. İlk Erişim (Initial Access)	Hedefli phishing (Spearphishing) e-postası	T1566.001
	Kötü amaçlı makrolar içeren belge kullanımı	T1203
3. Yetki Yükseltme (Privilege Escalation)	Exploit kullanarak sistem açıklarından faydalanma	T1068
	Credential Dumping (Kimlik bilgisi çıkarma)	T1003
4. Yanal Hareket (Lateral Movement)	SMB üzerinden ağ içinde hareket etme	T1021.002
	Uzak Masaüstü Protokolü (RDP) kullanımı	T1021.001
5. Etki (Impact)	Verileri şifreleyerek fidye talebi (Data Encryption)	T1486
	Kritik servisleri durdurarak hizmet kesintisi oluşturma	T1499

Sonuç

Mitre ATT&CK Framework, siber tehdit aktörlerinin saldırı süreçlerini anlamak, tespit etmek ve önlemek için geliştirilmiş son derece verimli bir veritabanıdır. Bu framework, siber güvenlik analistlerinin saldırganların taktiklerini, tekniklerini ve prosedürlerini analiz etmelerine yardımcı olur.
TTP (Taktikler, Teknikler ve Prosedürler), saldırıların nasıl yapıldığını anlamak ve önceden tahmin etmek için önemli bir yapı taşır. TTP tabanlı tehdit avcılığı ve tespit mühendisliği, saldırıların hızlı bir şekilde tespit edilmesini ve engellenmesini sağlar.
Genel olarak, Mitre ATT&CK Framework, siber savunma stratejilerinin gelişmesini ve siber güvenlik ekiplerinin atak vektörlerine karşı daha dirençli hale gelmesini sağlamak için hayati bir rol oynamaktadır.

Kaynakça

https://attack.mitre.org

https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/

https://kaleileriteknoloji.medium.com/tehdit-avcılığı-f58d7003e0f9

https://bilisimevreni.com.tr/mitre-attack-framework/

https://cybershieldcommunity.com/mitre-attck-framework/

https://www.securefors.com/mitre-attack-framework-nedir/

https://medium.com/@demezmurat1/mitre-att-ck-nedir-nasil-kullanilir-3c6762c55a74

https://www.exclusive-networks.com/tr/wp-content/uploads/sites/32/2020/12/MITRE-ATTCK-InfoBlox-.pdf