MİTRE ATT&CK

İREM GÜZEL
17.02.2025

İçindekiler

Giriş

Mitre ATT&CK çerçevesi, kuruluşların siber güvenlik stratejilerini güçlendirmelerine yardımcı olmak için siber saldırganların en son davranışlarını ve taktiklerini tanımlayan ücretsiz, küresel olarak erişilebilir bir bilgi tabanıdır .

Tehdit avcıları, MITRE ATT&CK çerçevesini kullanarak sistemlerinde gizli tehditleri proaktif bir şekilde araştırabilir ve olası saldırı izlerini daha etkin bir şekilde ortaya çıkarabilir. Bu tabloyu kullanarak güvenlik bilginizi derinleştirebilir, tehdit algılama süreçlerinizi iyileştirebilir ve daha güçlü bir siber savunma oluşturabilirsiniz.

Mitre Att&ck Tablosu Nedir?

MITRE ATT&CK (Rakip Taktikler, Teknikler ve Genel Bilgi), MITRE Corporation tarafından kuruluşların güvenlik hazırlıklarını anlamalarına ve savunmalarındaki zaafları ortaya çıkarmalarına yardımcı olmak için geliştirilen bir çerçeve, veri matrisleri seti ve değerlendirme aracıdır.

2013 yılında geliştirilen MITRE ATT&CK Çerçevesi, belirli saldırı yöntemlerini, taktiklerini ve tekniklerini belgelemek için gerçek dünya gözlemlerini kullanır. Yeni güvenlik açıkları ve saldırı yüzeyleri ortaya çıktıkça, bunlar sürekli olarak gelişen ATT&CK çerçevesine eklenir. Geçtiğimiz birkaç yıl içinde, MITRE ATT&CK çerçevesi ve matrisleri, saldırgan davranışına ilişkin hem bilgi hem de düzeltme araçları için bir endüstri standardı haline geldi.

MITRE ATT&CK Çerçevesi içerisinde platform tiplerine göre 3 farklı matris oluşturulmuştur:

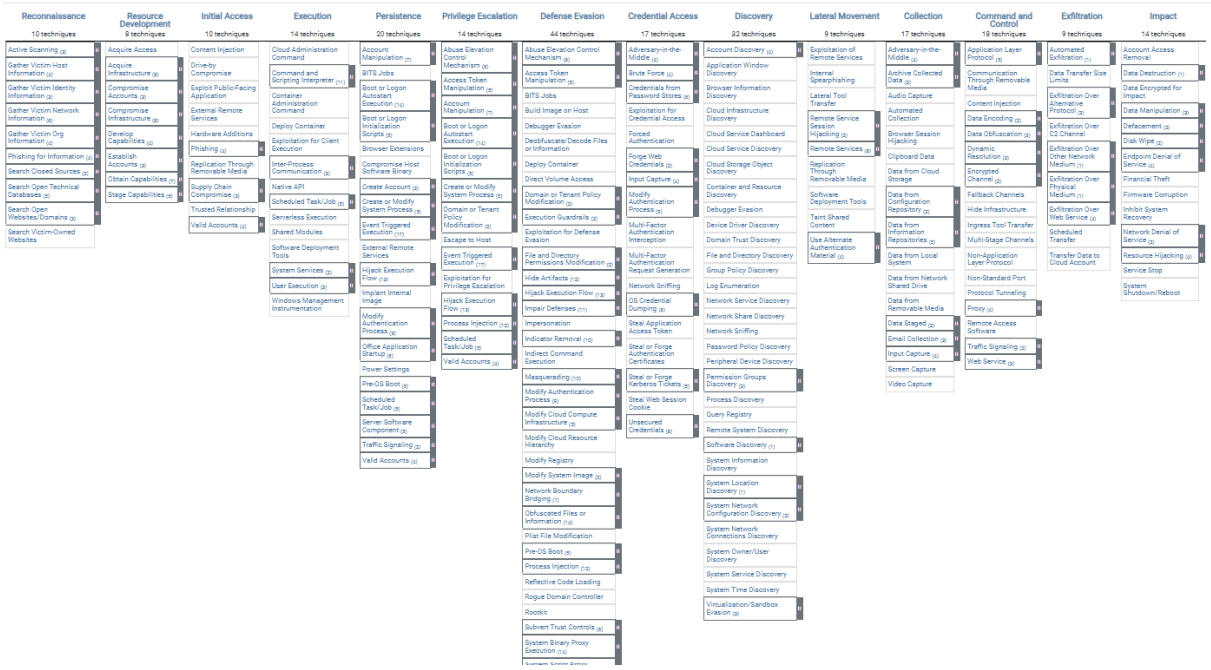
- İşletme Matrisi
- Mobil Matris
- ICS (Endüstriyel Kontrol Sistemleri) Matrisi

Enterprise (İşletme) Matrisi

MITRE ATT&CK Enterprise Matrisi, saldırganların kurumsal ağlara nasıl sızdığını, nasıl hareket ettiğini ve hedeflerine nasıl ulaştığını detaylandırır.

Alt Kümesi:

- PRE
- Windows
- macOS
- Linux
- Cloud
- Network
- Containers



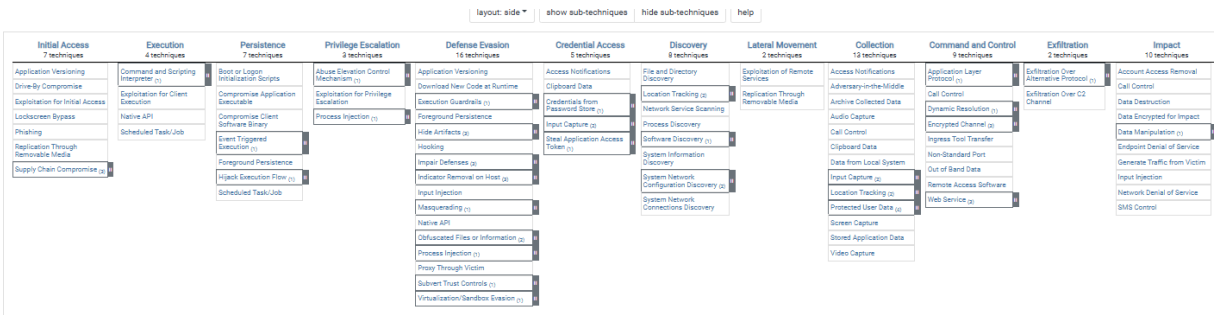
Enterprise Matrisi

Mobile (Mobil) Matrisi

Mobil matris, mobil cihazlar için hazırlanmış ve mobil cihazların siber güvenliği hakkında bilgi içeren matristir. Bu matris, bireysel ve kurumsal mobil cihazların güvenliğini sağlamak için kullanılabilir. Kurumsal Matris ile karşılaştırıldığında, daha az bilgi içerir.

Alt kümesi:

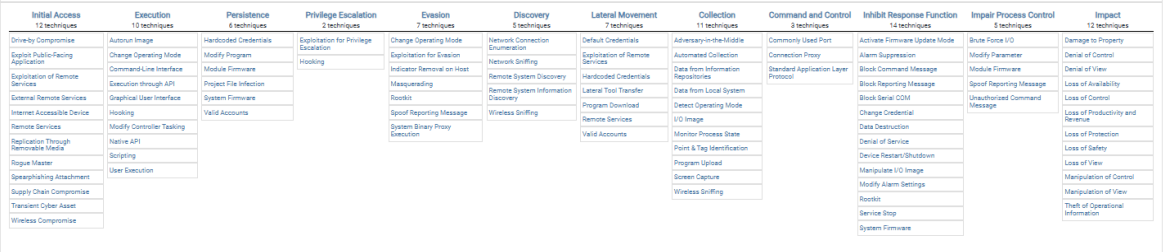
- Android
- İOS



Mobile Matrisi

ICS Matrisi

ICS Matrisi, endüstriyel kontrol sistemlerindeki cihazların siber güvenliği için toplanan bilgileri içeren matristir. Bu matris, bir ICS'nin siber güvenliğini ve analizlerini sağlamak için kullanılabilir.



ICS Matrisi

Mire Att&ck Tablosu Neden Önemlidir ?

- **Ortak Bir Dil ve Sınıflandırma**

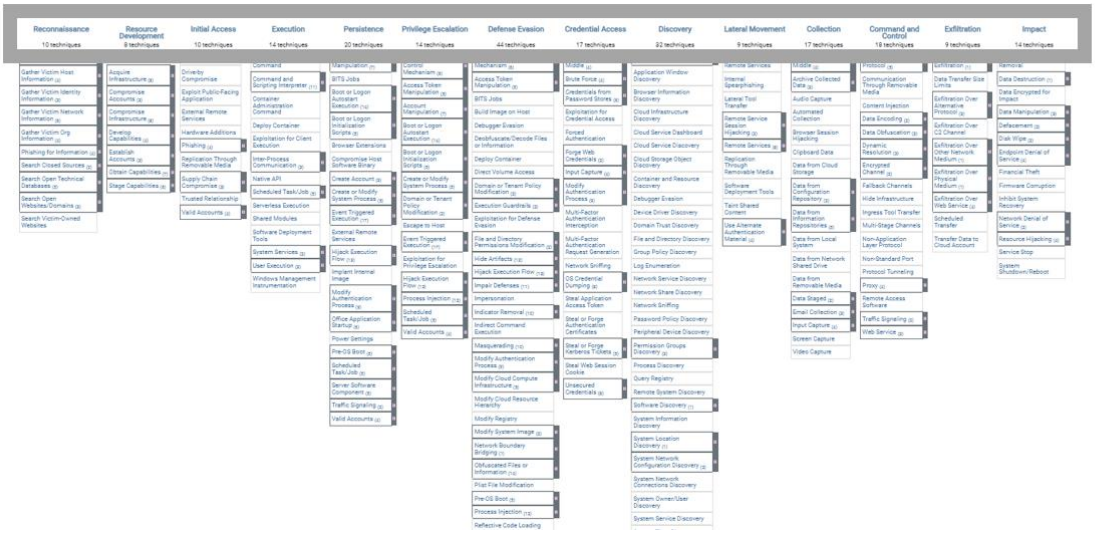
MITRE ATT&CK, siber saldırganların hedeflerine ulaşmak için kullandıkları taktik ve teknikleri ortak bir sınıflandırma altında toplayarak, siber güvenlik uzmanları ve kurumlar arasında net ve anlaşılır bir iletişim sağlar.

- **Olmaz ise ne olur ?**
  - Tehdit Analizi ve Savunma Stratejileri Zorluğu
  - Güvenilir Bilgi Kaynağı Eksikliği
  - Kırmızı Takım ve Mavi Takım İş birliği Zorluğu
  - Sürekli Gelişim ve Güncellik Eksikliği

Mitre Atak Framework'te Bulunan Taktik&Tekniklerin Önemi

1. Taktik

Taktikler, saldırganların hedeflerine ulaşmak için kullandıkları yüksek seviyeli stratejilerdir. Saldırganın genel amacını ve yaklaşımını belirler. Örneğin, bir saldırganın taktiği, hedef sistemlere sızmak ve hassas verileri çalmak olabilir. Taktikler matrisin en üst sırasındadır.



Mitre Att&ck Taktikleri

Enterprise Taktikleri:

- Reconnaissance (Keşif)
- Resource Development (Kaynak Geliştirme)
- Initial Access (İlk Erişim)
- Execution (Uygulamak)
- Persistence (Azim)
- Privilege Escalation (Ayrıcalık Yükseltmesi)
- Defense Evasion (Savunma Kaçınma)
- Credential Access (Kimlik Bilgisi Erişimi)
- Discovery (Keşif)
- Lateral Movement (Yanal Hareket)
- Command and Control (Komuta ve Kontrol)
- Collection (Koleksiyon)
- Exfiltration (Sızdırma)
- Impact (Darbe)

Mobil Taktikleri :

- Initial Access (İlk Erişim)
- Execution (Uygulamak)
- Persistence (Azim)
- Privilege Escalation (Ayrıcalık Yükseltmesi)
- Defense Evasion (Savunma Kaçınma)
- Credential Access (Kimlik Bilgisi Erişimi)
- Discovery (Keşif)
- Lateral Movement (Yanal Hareket)
- Collection (Koleksiyon)
- Command and Control (Komuta ve Kontrol)
- Exfiltration (Sızdırma)
- Impact (Darbe)
- Network Effects (Ağ Etkileri)
- Remote Service Effects (Uzaktan Hizmetin Etkileri)

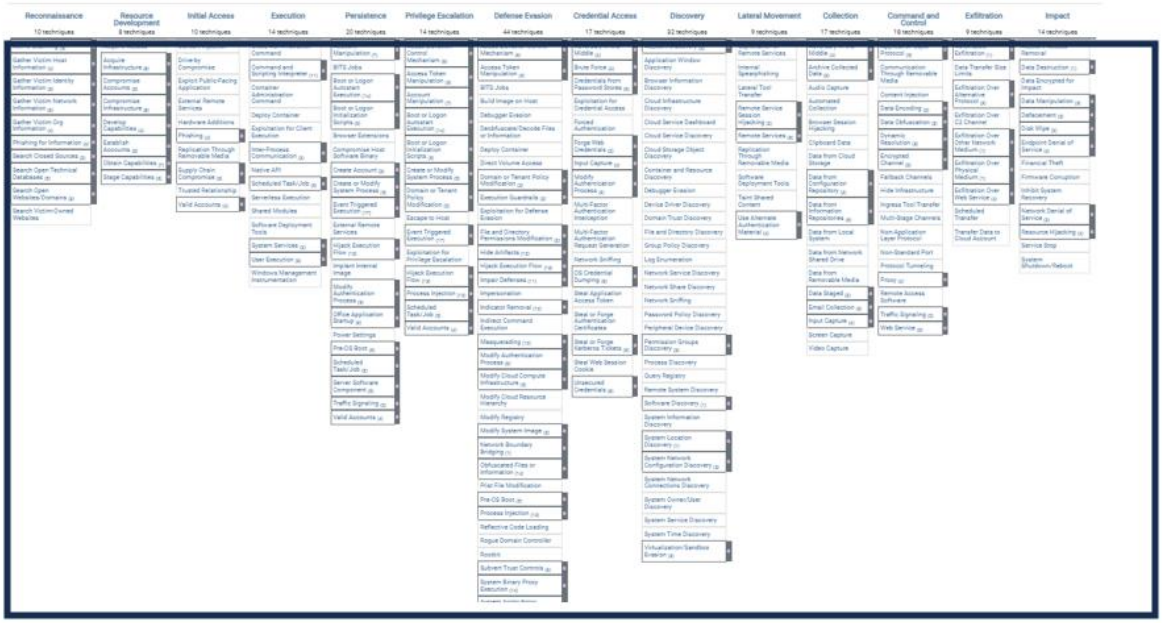
ICS Taktikleri

- Initial Access (İlk Erişim)
- Execution (Uygulamak)
- Persistence (Azim)
- Privilege Escalation (Ayrıcalık Yükseltmesi)
- Evasion (Kaçınma)
- Discovery (Keşif)
- Lateral Movement (Yanal Hareket)
- Collection (Koleksiyon)
- Command and Control (Komuta ve Kontrol)
- Inhibit Response Function (Tepki Fonksiyonunu Engelle)
- Impair Process Control (Süreç Kontrolünü Bozmak)
- Impact (Darbe)

2. Teknik

MITRE ATT&CK teknikleri, taktikleri nasıl başarmaya çalıştıklarını temsil eder. Bunlar, phishing ve brute force saldırıları gibi temel yöntemlerden, DLL arama sırası ele geçirme ve process enjeksiyonu gibi daha karmaşık yöntemlere kadar geniş bir yelpazeye yayılır.

Siber güvenlik uzmanlarının bu teknikleri anlaması, tehditleri daha hızlı tespit etmelerine, güvenlik önlemlerini güçlendirmelerine ve olaylara daha etkili bir şekilde müdahale etmelerine yardımcı olur. Bu nedenle, MITRE ATT&CK gibi tehdit istihbaratı çerçeveleri, güvenlik ekipleri için kritik bir rehber niteliğindedir



Mitre Att&ck Teknikleri

Mitre Att&ck Sub-Teknik

Sub-Teknik

MITRE ATT&CK çerçevesinde Sub-Teknikler, geniş kapsamlı Tekniklerin daha spesifik varyasyonlarıdır. Bir saldırı tekniğinin farklı yöntemlerle nasıl uygulanabileceğini göstermek için kullanılır.

3. Prosedür

Prosedür, tekniklerin/alt tekniklerin kullanım örneklerinden oluşur. Basitçe, tekniğin uygulanması sırasında hangi araç/yazılımın kullanıldığını gösterir. Başka bir deyişle, tekniğin kullanımıyla ilgili pratik bilgilerin açıklamasıdır.

Procedure Examples

ID	Name	Description
G0001	Axiom	Axiom has used spear phishing to initially compromise victims.[9][10]

Mitre Att&ck Prosedür

Mitigations (Azaltma önlemleri)

Mitigations, Mitre Att&ck matrisindeki tekniklere yanıt olarak alınabilecek önlemler ve eylemleri açıklar.

Mitre Att&ck Mitigations

Azaltmalar için de matrisler 3'e ayrılmıştır. Raporun yazıldığı zaman dilimi için güncel Azaltma sayısı :

- Enterprise Mitigations : 44
- Mobile Mitigations : 13
- ICS Mitigations : 52

Techniques Addressed by Mitigation

Domain	ID	Name	Use
ICS	T0830	Adversary-in-the-Middle	Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.
ICS	T0811	Data from Information Repositories	Consider periodic reviews of accounts and privileges for critical and sensitive repositories.

ICS için örnek Mitigations

TTP

TTP nedir?

TTP'ler, siber saldırganların hedeflerine ulaşmak için kullandıkları yöntemlerin üç boyutunu ifade eder:

T : Tactics

T : Techniques

P : Procedures

TTP-Based Threat Hunting

Tehdit, bir kuruluşun bilgi varlıklarına zarar verme potansiyeli taşıyan her türlü zararlı aktivite veya saldırgandır. Bilgisayar sistemlerine, ağlara, veri tabanlarına ve kritik altyapılara zarar verebilirler.

Tehdit avlama ise, siber güvenlik uzmanlarının ağlarda ve sistemlerde gizlenmiş tehditleri aktif olarak aradığı proaktif bir süreçtir. Otomatik güvenlik çözümlerinin tespit edemediği saldırıları belirlemek için kullanılır ve siber saldırıların erken aşamalarında tespit edilmesini sağlar.

TTP Tabanlı Tehdit Avcılığı ise tehdit aktörlerinin kullandığı belirli davranışları, saldırı kalıplarını ve operasyonel teknikleri (Taktikler, Teknikler, Prosedürler - TTP) inceleyen bir siber tehdit avcılığı yaklaşımıdır. Bu yöntem, geçmiş siber saldırıları analiz ederek, saldırganların gelecekteki hareketlerini tahmin etmeye ve proaktif bir şekilde tehditleri tespit etmeye olanak sağlar. TTP'lerin analizi, güvenlik ekiplerine daha hedeflenmiş ve etkili savunmalar geliştirme imkanı sunar.

Detection Engineering

Tespit mühendisliği, siber saldırıları tespit etmek ve bunlara karşı uyarılar oluşturmak için güvenlik araçları ve sistemlerinin (SIEM, IDS/IPS vb.) yapılandırılması ve yönetilmesi sürecidir. Tespit mühendisleri, tehdit istihbaratı, log analizi ve diğer kaynaklardan elde ettikleri bilgileri kullanarak, saldırıların belirtilerini ve kalıplarını tanımlayan kurallar ve algoritmalar geliştirirler. Bu sayede, güvenlik ekipleri saldırıları gerçek zamanlı olarak tespit edebilir ve müdahale edebilirler.

2022 Ukrayna Elektrik Şebekesi Saldırısı

Rusya-Ukrayna savaşı sırasında gerçekleşen 2022 Ukrayna Elektrik Şebekesi Saldırısı, siber saldırıların kritik altyapılar üzerindeki etkisini gözler önüne seren önemli bir olaydır. Saldırı, Ukraynalı bir elektrik dağıtım şirketini hedef alarak, yetkisiz komutların SCADA sistemleri üzerinden iletilmesiyle elektrik kesintilerine neden olmuştur.

Saldırıyı gerçekleştiren Sandworm grubu, hedefe ulaşmak için çeşitli kötü amaçlı yazılımlar ve teknikler kullanmıştır:

- GOGETTER: İlk erişimi sağlamak için kullanılan kötü amaçlı yazılım.
- Neo-REGEORG: Saldırganların ağ içinde yan hareket etmesini ve diğer sistemlere erişimini sağlayan araç.
- CaddyWiper: Hedef sistemlerdeki verileri silerek yıkıcı hasar veren kötü amaçlı yazılım.
- Living off the Land (LotL) Teknikleri: Saldırganların, tespit edilmemek için hedef sistemlerde halihazırda bulunan mevcut araçları ve kaynakları kötüye kullanması.

Bu saldırıda kullanılan teknikler ve bunların MITRE ATT&CK çerçevesindeki TID değerleri aşağıdaki gibidir:

DOMAİN	ID		NAME	DESCRİPTİON
Enterprise	T1059	.001	Komut ve Komut Dosyası Yorumlayıcısı : PowerShell	Saldırganlar, PowerShell'i kullanarak sistem üzerinde komut çalıştırabilir, kötü amaçlı yazılımlar indirebilir ve çalıştırabilir.
Enterprise	T1543	.002	Sistem İşlemini Oluştur veya Değiştir : Systemd Hizmeti	Systemd, Linux sistemlerde hizmetleri yönetmek için kullanılan bir init sistemidir. Saldırganlar, root yetkileriyle yeni bir systemd servisi oluşturup

				zararlı bir dosyayı sistem başlangıcında çalıştırabilir.
Enterprise	T1485		Veri İmhası	Saldırganlar, sistemdeki kritik verileri silebilir veya şifreleyerek işlevsiz hale getirebilir.
Enterprise	T1484	.001	Alan veya Kiracı Politikası Değişikliği : Grup Politikası Değişikliği	Saldırganlar, Active Directory ortamında **Group Policy Objects** üzerinde değişiklik yaparak kullanıcı politikalarını değiştirebilir ve sistem kontrolünü ele geçirebilir.
Enterprise	T1570		Yanal Alet Transferi	Saldırganların bir sistemden diğerine kötü amaçlı dosya aktarmasını ifade eder.
Enterprise	T1036	.004	Maskeleme : Maskeli Görev veya Hizmet	Saldırganlar, kötü amaçlı işlemleri ve servisleri **meşru görünen isimlerle saklayarak** tespit edilmelerini zorlaştırabilir.
Enterprise	T1095		Uygulama Dışı Katman Protokolü	Saldırganlar, ağ üzerinden güvenli şekilde çalışmayan protokolleri kullanarak verileri sızdırabilir veya komut kontrol sunucularına bağlanabilir.
Enterprise	T1572		Protokol Tünelleme	Saldırganlar, güvenlik duvarlarından kaçmak için şifreli tünel bağlantıları (VPN, SSH, Tor) oluşturabilir.
Enterprise	T1053	.005	Zamanlanmış Görev/İş : Zamanlanmış Görev	Saldırganlar kötü amaçlı yazılımları belirli bir zaman diliminde çalıştırılabilir.
Enterprise	T1505	.003	Sunucu Yazılım Bileşeni : Web Shell	Saldırganların ele geçirdiği bir web sunucusu üzerinde uzaktan komut çalıştırmasına izin veren bir araçtır.

ICS	T0895	Otomatik Çalıştırma Görüntüsü	Bu teknik, saldırganların kötü amaçlı yazılımları veya kodları, sistem açılışında otomatik olarak çalışacak şekilde ayarlamasını ifade eder. Bu sayede, sistem yeniden başlatıldığında veya kullanıcı oturum açtığında saldırganın kontrolü yeniden sağlanır.
ICS	T0807	Komut Satırı Arayüzü	Saldırganlar, CLI'yi kullanarak sistem üzerinde çeşitli işlemler gerçekleştirebilir, kötü amaçlı yazılımlar çalıştırabilir ve hassas verilere erişebilirler.
ICS	T0853	Komut dosyası	komut dosyaları, belirli bir görevi otomatikleştirmek için yazılan kodlardır. Saldırganlar, komut dosyalarını kullanarak sistem üzerinde çeşitli işlemler gerçekleştirebilir, kötü amaçlı yazılımlar yükleyebilir ve hatta sistemin kontrolünü ele geçirebilirler.
ICS	T0894	Sistem İkili Proxy Çalıştırma	Bu teknik, saldırganların hedef sistemde bir proxy sunucusu çalıştırarak, ağ trafiğini bu sunucu üzerinden yönlendirmesini ifade eder. Bu sayede, saldırganlar izlerini gizleyebilir, ağdaki diğer sistemlere erişebilir ve hatta hassas verileri ele geçirebilirler.
ICS	T0855	Yetkisiz Komut Mesajı	Bu teknik, saldırganların hedef sistemlere yetkisiz komutlar göndermesini ve bu komutların işlenmesini sağlamasını ifade eder.

Mitre Att&ck Senaryo

Bir tehdit aktörü, X Şirketi'ni hedef alarak siber saldırı planı yapmaktadır. İlk olarak, internette şirket hakkında bilgi toplamak için çeşitli yöntemler kullanır.

1. Keşif (Reconnaissance):

- **Gather Victim Identity Information - T1589.004 (Şirket Web Siteleri, Sosyal Medya)**

Saldırgan şirketin "Hakkımızda" veya "İletişim" gibi bölümlerini inceleyerek çalışanlar hakkında bilgi sahibi olmuştur. Aynı zamanda Facebook, Twitter, LinkedIn, Instagram gibi platformlar ile şirket çalışanlarının profillerini daha detaylı analiz edebilmiştir.

- **Gather Victim Host Information - T1592**

Bu teknik, saldırganların hedef sistem veya ağdaki güvenlik açıklarını belirlemek için hedefe tarama yapmasını içerir. Nmap, Shodan, Nessus, vb.

2. İlk Erişim (Initial Access)

- **Replication Through Removable Media – T1091 (Çıkarılabilir Medya Aracılığıyla Çoğaltma)**

Saldırgan ,USB cihazını çalışanların bilgisayarlarına fiziksel erişim sağlamak amacıyla kötü amaçlı yazılım taşıyan bir cihaz olarak kullanılır.

Bir süre sonra şirket çalışanlarıyla temasa geçen saldırgan, ilk erişimini USB cihazı ile kurmayı dener. Hedef çalışanların kişisel eşyalarına kendi USB cihazını bırakır. Saldırgan, çalışanların bu USB'yi bilgisayarına takarak oluşturduğu kötü amaçlı yazılımı bulaştırmayı hedefler.

USB'yi kendi bilgisayarlarına takan çalışanlar, kötü amaçlı yazılımı bilgisayarına bulaştırır ve saldırgana ilk erişimi sağlarlar.

3. Uygulamak (Execution)

Saldırgan, kalıcı erişim elde etmek ve zamanlanmış görevler aracılığıyla sürekli olarak sisteme erişebilmek için adımlar atar.

- **Scheduled Task/Job - T1053 (Zamanlanmış Görev/İş)**

Zamanlanmış görevler, işletim sistemlerinde belirli zamanlarda veya olaylarda otomatik olarak çalıştırılan komutlar, programlar veya betiklerdir. Sistem yeniden başlatılsa veya kullanıcı oturumu kapatılsa bile, zamanlanmış görevler veya işler sayesinde kötü amaçlı yazılımlar veya komutlar otomatik olarak çalışmaya devam edebilir.

Saldırgan bu sayede sistemde belirli periyotlarla kötü amaçlı yazılımı tekrar çalıştıracaktır.

- **Command and Scripting Interpreter - T1059 (Komut ve Komut Dosyası Yorumlayıcısı)**

Saldırgan, PowerShell, Bash ve diğer komut yorumlayıcıları aracılığıyla zararlı komutlarını yürütür.

4. Ayrıcalık Yükseltme Aşaması (Privilege Escalation)

- **Account Manipulation - T1098 (Hesap Manipülasyonu)**

Bu teknik, saldırganların sistemdeki kullanıcı hesaplarını manipüle ederek yetkilerini artırmasına veya kalıcılık sağlamasına olanak tanır. Bu senoryada saldırgan düşük ayrıcalıklı bir hesaba erişim sağladıktan sonra bu hesabın yetkilerini yükseltmiştir.

- **Process Injection - T1055 (Süreç Enjeksiyonu)**

Bu teknik, saldırganların kötü amaçlı kodlarını meşru bir sürecin adres alanına enjekte ederek çalıştırmasını ifade eder.

5. Veri Sızdırma (Exfiltration)

Senaryonun bu aşamasına kadar saldırgan artık sistemde tam yetkiye sahiptir. Geriye sistem kaynaklarını sömürmesi ve ele geçirmesi kalmıştır.

- **Automated Exfiltration - T1020 (Otomatik Veri Sızdırma)**

Saldırgan, elde ettiği verileri belirli zaman aralıklarıyla otomatik olarak dışarı çıkaracak bir komut veya script kullanır.

- **Data Transfer Size Limits - T1030 (Veriyi Parçalar Halinde Gönderme)**

  Saldırgan büyük hacimli verilerin güvenlik sistemlerine takılmasını önlemek için veriyi daha küçük parçalara bölünerek dışarı sızdırır.Bu teknik ile anormal ağ trafiği analizlerinden ve DLP sistemlerinden kaçınmayı hedefler.

6. Defense Evasion(Savunma Kaçınma)

- **Indicator Removal - T1070 (Sistemdeki İzleri Silme)**

Saldırgan, arkada iz bırakmamak ve adli analiz süreçlerini zorlaştırmak için logları silme, komut geçmişlerini temizleme gibi sistemdeki izlerini yok etme yöntemlerini kullanır.

  - T1070.001 - Clear Windows Event Logs : Windows olay günlüklerini temizler
  - T1070.002 - Clear Linux Logs : Linux sistem günlüklerini temizler
  - T1070.003 - Clear Command History : Komut geçmişlerini temizler
  - T1070.004 - File Deletion : Oluşturduğu dosyaları temizler

Sonuç

Tüm bu rapordan anlayacağımız gibi Mitre Att&ck framework'ün taktik ve tekniklerini benimsemek; saldırı çeşitlerinin daraltılmasını, tehditlerin erken aşamada tespit edilmesini ve olay müdahale süreçlerinin hızlandırılmasını sağlar. Her geçen zaman diliminde saldırganların kullandıkları bu stratejiler daha da genişlemekte ve çoğalmaktadır. Bu yüzden kuruluşların, sürekli güncellenen Mitre Att&cK yapısını takip ederek güvenlik stratejilerini güçlendirmesi, farkındalığı artırması ve siber tehditlere karşı daha dirençli hale gelmesi kritik öneme sahiptir.

KAYNAKÇA

https://app.letsdefend.io/training/lessons/mitre-attck-framework

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

https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e

https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/

https://www.upguard.com/blog/what-is-ttp-hunting

https://attack.mitre.org/campaigns/C0034/

https://attack.mitre.org/

https://chatgpt.com/