MITRE ATT&CK

Hazırlayan: Şevval Kömeç

16.02.2024

İÇİNDEKİLER

GİRİŞ

Bu rapor, siber güvenlikte kritik bir yere sahip olan **MITRE ATT&CK Çerçevesi**'ni ele almaktadır. MITRE ATT&CK, saldırganların siber saldırılar sırasında kullandıkları taktikler, teknikler ve prosedürleri (TTP) sistematik bir şekilde sınıflandırarak, güvenlik uzmanlarına saldırı süreçlerini anlamada ve önlem geliştirmede rehberlik eden bir bilgi tabanıdır. Raporun amacı, MITRE ATT&CK çerçevesinin bileşenlerini, önemi ve kullanım alanlarını detaylı bir şekilde açıklayarak, siber tehditlerin tespiti ve önlenmesinde nasıl bir yol gösterici olduğunu ortaya koymaktır. Ayrıca, gerçek dünya saldırı örnekleri üzerinden MITRE ATT&CK tekniklerinin nasıl kullanıldığını göstererek, siber güvenlik farkındalığını artırmak hedeflenmiştir.

MITRE ATT&CK Çerçevesi Nedir?

MITRE ATT&CK çerçevesi (MITRE ATT&CK), siber suçluların bilinen düşmanca davranışlarına dayalı siber güvenlik tehditlerini modellemek, tespit etmek, önlemek ve bunlarla mücadele etmek için evrensel olarak erişilebilir, sürekli güncellenen bir bilgi tabanıdır.

MITRE: ABD merkezli, kâr amacı gütmeyen bir kuruluş olan *MITRE Corporation* tarafından geliştirilmiştir. MITRE, savunma, siber güvenlik, sağlık ve diğer kritik alanlarda araştırmalar yapan bir kuruluştur.

ATT&CK: "*Adversarial Tactics, Techniques, and Common Knowledge*" ifadesinin kısaltmasıdır. Türkçeye çevirecek olursak:

- **A**dversarial (**Saldırganla ilgili**)
- **T**actics (**Taktikler**)
- **T**echniques (**Teknikler**)
- **C**ommon **K**nowledge (**Ortak Bilgi**)

Bu isim, saldırganların gerçek dünyada siber saldırılar sırasında kullandığı taktikler, teknikler ve prosedürleri (TTP'ler) sistematik bir şekilde belgeleyen bir bilgi tabanı olmasından gelir. İlk olarak 2013 yılında MITRE tarafından, siber tehditleri anlamak ve simüle etmek amacıyla oluşturulmuş ve zamanla endüstri standardı haline gelmiştir.

Mitre Atak Tablosu Neden Önemlidir?

MITRE ATT&CK tablosu, siber güvenlik alanında büyük bir öneme sahiptir. Bu çerçeve, siber saldırganların taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) sistematik bir şekilde sınıflandırarak, güvenlik profesyonellerine saldırıların nasıl gerçekleştirildiğini ve bu saldırılara karşı nasıl savunma yapılabileceğini anlamada yardımcı olur.

MITRE ATT&CK'in önemi şu noktalarda öne çıkar:

1. **Görselleştirme ve Analiz:** Saldırıların nasıl gerçekleştiğini ve hangi yöntemlerin kullanıldığını görselleştirerek, güvenlik ekiplerinin saldırı yaşam döngüsünü anlamalarını ve etkili savunma stratejileri geliştirmelerini sağlar.
2. **Standartlaştırma:** Siber saldırılar için ortak bir dil sağlayarak, farklı güvenlik ekipleri ve kuruluşlar arasında daha etkili bir iletişim ve işbirliği ortamı oluşturur.
3. **Eğitim ve Farkındalık:** Siber güvenlik uzmanlarının eğitiminde ve farkındalığın artırılmasında kullanılarak, saldırganların nasıl çalıştığını ve bu saldırılara karşı nasıl savunma yapılabileceğini anlamalarına yardımcı olur.
4. **Tehdit İstihbaratı:** Tehdit istihbaratı sağlayıcıları ve kullanıcıları için kritik bir araç olarak, gerçek dünyada karşılaşılan saldırılar hakkında detaylı bilgi sunar ve bu bilgilerin etkin bir şekilde kullanılmasını mümkün kılar.

MITRE ATT&CK tablosu, siber güvenlik profesyonelleri için vazgeçilmez bir kaynak olup, saldırıların nasıl gerçekleştiğini anlamak ve bu saldırılara karşı etkili savunma stratejileri geliştirmek isteyen herkes için başvurulması gereken bir bilgi tabanıdır.

MITRE ATT&CK Matrisleri ve Kapsamları

1. İşletme (Enterprise) Matrisi
Kurumsal Matris, kurumsal altyapıya yönelik saldırılarda kullanılan tüm saldırgan tekniklerini içerir. Bu matris, Windows, MacOS ve Linux platformları için alt matrislerin yanı sıra ağ altyapısı, bulut platformları ve kapsayıcı teknolojilerini içerir.

2.Mobil Matris
Mobil Matris, mobil cihazlara doğrudan saldırılarda ve mobil cihaza erişim gerektirmeyen ağ tabanlı mobil saldırılarda kullanılan teknikleri içerir. Bu matris, iOS ve Android mobil platformları için alt matrisler içerir.

3.ICS Matrisi
ICS (Industrial Control Systems-Endüstriyel Kontrol Sistemleri) Matrisi, endüstriyel kontrol sistemlerine yönelik saldırılarda kullanılan teknikleri içerir; özellikle fabrikalar, kamu hizmetleri, ulaşım sistemleri ve diğer kritik hizmet sağlayıcılarının operasyonlarını kontrol etmek veya otomatikleştirmek için kullanılan makineler, cihazlar, sensörler ve ağlar.

TTP nedir?

TTP, siber güvenlikte "Taktikler, Teknikler ve Prosedürler" (Tactics, Techniques, and Procedures) teriminin kısaltmasıdır. Bu terim, saldırganların belirli bir hedefe ulaşmak için kullandığı genel strateji, yöntem ve süreçleri tanımlar.

- **Taktikler (Tactics):** Saldırganların genel hedeflerine ulaşmak için kullandıkları stratejilerdir. Her taktik, bir saldırı aşamasını temsil eder (örneğin, İlk Erişim, Yükseltilmiş Yetkiler, Veri Hırsızlığı).
- **Teknikler (Techniques):** Saldırganların belirli bir taktiği gerçekleştirmek için kullandığı yöntemlerdir. Örneğin, kimlik avı veya zayıf parola kullanımı gibi yöntemler, bir taktiğe ulaşmak için kullanılan tekniklerdir.
- **Prosedürler (Procedures):** Tekniklerin daha spesifik ve ayrıntılı uygulamalarıdır. Bu, saldırganların teknikleri nasıl kullandığına dair spesifik davranışları ve araçları tanımlar (örneğin, belirli bir kimlik avı e-posta şablonunun kullanılması veya belirli bir zararlı yazılım türünün yüklenmesi).

TTP'ler, saldırganların nasıl hareket ettiğini, hangi araçları kullandığını ve hangi yollarla hedeflerine ulaşmaya çalıştığını anlamak için çok önemlidir. Bu kavramlar, saldırıların analiz edilmesi ve savunma stratejilerinin geliştirilmesi için kritik bilgiler sunar.

MITRE ATT&CK Framework'de Bulunan Taktik ve Tekniklerin Önemi.

MITRE ATT&CK Framework'deki taktik ve teknikler, siber tehdit aktörlerinin saldırı süreçlerini detaylı bir şekilde ortaya koyar ve bu da güvenlik ekiplerinin hangi alanlara odaklanacağını netleştirir. Güvenlik operasyonları, bu bilgileri kullanarak hem şüpheli aktiviteleri daha hızlı tespit edebilir hem de kaynaklarını en etkili şekilde yönlendirerek proaktif savunma stratejileri geliştirebilir. Örneğin, belirli teknikleri engellemek için denetimleri artırabilir veya saldırıların ilerlemesini durduracak önlemler alabilir. Bu

framework, saldırı yüzeyini daraltmayı ve potansiyel zararları minimize etmeyi sağlayarak siber güvenlik süreçlerinde kritik bir rol oynar.

MITRE ATT&CK Tablosu

MITRE ATT&CK tablosu, siber saldırganların gerçekleştirdiği saldırıları aşamalara ayırarak her aşamada kullanılan teknikleri detaylı bir şekilde listeleyen bir matrise (tabloya) sahiptir. Bu tablo, güvenlik uzmanlarının ve mavi takım (defansif güvenlik) ekiplerinin saldırıları anlamalarına ve önlem almalarına yardımcı olur.
Ayrıca, MITRE ATT&CK çerçevesini kullanarak saldırı tekniklerini analiz etmek ve logları incelemek, güvenlik operasyonları merkezleri (SOC) için kritik öneme sahiptir. Özellikle, PowerShell logları ve diğer güvenlik olayları izlenerek potansiyel tehditler tespit edilebilir.

MITRE ATT&CK tablosunda:
🔻 Yatay eksende (Sütunlar): Taktikler (Tactics) → Saldırının genel aşamalarını gösterir.
🔻 Dikey eksende (Satırlar): Teknikler (Techniques) ve Alt Teknikler (Sub-Techniques) → Teknikler, saldırganların bir taktiği gerçekleştirmek için "nasıl" hareket ettiğini açıklar.
Alt Teknikler (Sub-techniques): Bazı teknikler, daha spesifik alt tekniklere ayrılır. Bu alt teknikler, ana tekniğin belirli bir varyasyonunu veya daha detaylı bir uygulamasını gösterir. Örneğin, "PowerShell" tekniğinin altında, belirli modüllerin kötüye kullanılması gibi alt teknikler bulunabilir.

MITRE ATT&CK Tablosunda Bulunan 14 Taktik

Keşif (Reconnaissance)
Saldırganların hedef hakkında bilgi toplama aşaması.

Kaynak Geliştirme (Resource Development)
Saldırganların saldırı için gerekli kaynakları edinme süreci.

İlk Erişim (Initial Access)
Saldırganların hedef sisteme ilk kez erişim sağlama yöntemleri.

Çalıştırma (Execution)
Saldırganların kötü amaçlı kodları çalıştırma teknikleri.

Kalıcılık (Persistence)
Saldırganların sistemde kalıcı erişim sağlama yöntemleri.

Yetki Yükseltme (Privilege Escalation)
Saldırganların daha yüksek yetkiler elde etme teknikleri.

Savunma Kaçışı (Defense Evasion)
Saldırganların güvenlik önlemlerini atlatma yöntemleri.

Kimlik Bilgisi Erişimi (Credential Access)
Saldırganların kimlik bilgilerini elde etme teknikleri.

Keşif (Discovery)
Saldırganların ağ ve sistem hakkında bilgi toplama yöntemleri.

Yanal Hareket (Lateral Movement)
Saldırganların ağ içinde hareket ederek diğer sistemlere erişim sağlama teknikleri.

Toplama (Collection)
Saldırganların hedef sistemlerden veri toplama yöntemleri.

Veri Sızdırma (Exfiltration)
Saldırganların topladıkları verileri dışarıya aktarma teknikleri.

Etkileşim (Impact)
Saldırganların hedef sistem üzerinde zarar verme veya işlevselliği bozma yöntemleri.

TTP-Based Threat Hunting ve Detection Engineering nedir?

Siber güvenlikte tehdit avcılığı ve tespit mühendisliği, kuruluşların güvenlik sistemlerini güçlendirmek ve saldırganları etkili bir şekilde tespit etmek için kullanılan iki temel yaklaşımdır. Her iki yaklaşım da tehditleri belirlemeye odaklanır, ancak yöntemleri ve amaçları farklıdır.

TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı)

TTP tabanlı tehdit avcılığı, saldırganların taktik, teknik ve prosedürlerine (TTP'ler) odaklanarak, henüz tespit edilmemiş tehditleri proaktif olarak arama sürecidir. Geleneksel güvenlik çözümleri tarafından algılanamayan tehditleri bulmak için hipotez geliştirme, veri analizi ve saldırgan davranışlarını inceleme gibi yöntemler kullanılır.

Bu süreçte öncelikle potansiyel saldırı yöntemleri ve hedefler hakkında hipotezler geliştirilir. Ardından, şüpheli aktiviteleri belirlemek için sistem günlükleri, ağ trafiği ve olay verileri analiz edilir. Saldırganların teknikleri ile eşleşen anormallikler değerlendirilerek, tespit edilen tehditlere karşı önlem alınır ve güvenlik açıkları kapatılır. TTP tabanlı avcılık, tehditleri keşfetme konusunda daha esnek ve saldırganların uzun vadeli stratejilerine odaklanan bir yaklaşımdır.

Detection Engineering (Tespit Mühendisliği)

Tespit mühendisliği, saldırı tekniklerini belirlemek ve bunlara karşı otomatik tespit mekanizmaları geliştirmek için kullanılan bir yöntemdir. SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response) ve NDR (Network Detection and Response) gibi araçlarla tehditlerin erken aşamada algılanmasını sağlar.

Bu yöntemde belirli saldırı yöntemlerine karşı özel tespit kuralları geliştirilir. Yanıltıcı alarmların önüne geçmek için tespit mekanizmaları optimize edilir ve tehditlere otomatik yanıt verilmesi sağlanır. Tespit mühendisliği, güvenlik sistemlerinin sürekli iyileştirilmesini ve tehditlerin daha hızlı algılanmasını amaçlar.

TTP-Based Threat Hunting ve Detection Engineering Arasındaki Farklar

TTP tabanlı tehdit avcılığı proaktif bir yaklaşımdır ve bilinmeyen tehditleri keşfetmeye odaklanırken, tespit mühendisliği reaktif ve önleyici bir yaklaşımla bilinen tehditleri tespit

etmeye çalışır. Tehdit avcılığı hipotez geliştirme ve davranışsal analiz gibi yöntemleri kullanırken, tespit mühendisliği SIEM, EDR ve kural tabanlı tespit sistemleriyle tehditleri otomatik olarak belirler. Tehdit avcılığı sürekli araştırmaya dayalı bir süreçken, tespit mühendisliği anlık ve sürekli çalışarak tehditleri algılar. Sonuç olarak, TTP tabanlı tehdit avcılığı yeni saldırı yöntemlerini keşfetmeye odaklanırken, tespit mühendisliği mevcut tehditleri otomatik olarak algılamaya yöneliktir. Her iki yöntem de siber güvenlik stratejilerinde tamamlayıcı bir rol oynar ve birlikte kullanıldığında daha güçlü bir savunma sağlar.

2022 Ukrayna Elektrik Gücü Saldırısı

2022 Ukrayna Elektrik Enerjisi Saldırısı, Sandworm Ekibi tarafından gerçekleştirilen bir siber saldırı kampanyasıdır. Bu saldırıda, GOGETTER, Neo-REGEORG, CaddyWiper ve living of the land (LotL) teknikleri kullanılarak Ukraynalı bir elektrik şirketinin SCADA sistemlerine yetkisiz erişim sağlandı. Saldırı, MITRE ATT&CK framework'ünün hem Enterprise hem de ICS alanlarındaki çeşitli teknikleri içeriyordu.

SCADA (Supervisory Control and Data Acquisition) Nedir?

SCADA (Supervisory Control and Data Acquisition – Merkezi Denetleme ve Veri Toplama Sistemi), endüstriyel süreçleri, altyapıları ve tesisleri uzaktan izlemek ve kontrol etmek için kullanılan bir otomasyon sistemidir.
SCADA, elektrik şebekeleri, su arıtma tesisleri, petrol rafinerileri, üretim hatları, ulaşım sistemleri gibi kritik altyapıları yönetmek için kullanılır.

Saldırının Enterprise Alanındaki Kullanılan Teknikleri:

T1059: Komut ve Komut Dosyası Yorumlayıcısı

Saldırganlar, sistemlerle etkileşim kurmak için komut ve betik yorumlayıcılarını kötüye kullanır. Bu yorumlayıcılar, Unix Shell, Windows Command Shell, PowerShell gibi yerleşik özelliklerdir. Ayrıca Python, JavaScript ve Visual Basic gibi platformlar arası yorumlayıcılar da kullanılabilir. Saldırganlar, bu yorumlayıcıları keyfi komutlar çalıştırmak için kullanır. Komutlar, kurbanlara yem belgeleri olarak veya mevcut bir komuta ve kontrol (C2) sunucusundan indirilen yükler olarak teslim edilebilir. Bu teknik, saldırganların sistemlerde yetkisiz erişim sağlamasına ve kötü amaçlı faaliyetler gerçekleştirmesine olanak tanır.

- **T1059.001: PowerShell**

  Saldırganlar, PowerShell'i kötüye kullanarak bilgi keşfi, kod yürütme ve yürütülebilir dosyaları indirip çalıştırma gibi işlemler gerçekleştirebilir. PowerShell, diske dokunmadan bellekten çalıştırılabilen dosyaları indirip çalıştırabilir. Empire, PowerSploit, PoshC2 ve PSAttack gibi PowerShell tabanlı saldırı araçları mevcuttur.

PowerShell komutları, `powershell.exe` ikili dosyası veya .NET çerçevesi aracılığıyla doğrudan yürütülebilir.

T1543: Sistem İşlemini Oluştur veya Değiştir

Saldırganlar, kalıcılık sağlamak için sistem düzeyinde süreçler oluşturabilir veya değiştirebilir. Windows ve Linux'ta hizmetler, macOS'ta ise Launch Daemon ve Launch Agent olarak bilinen süreçler kullanılır. Saldırganlar, yeni hizmetler oluşturarak veya mevcut hizmetleri değiştirerek kötü amaçlı yüklerin otomatik olarak çalıştırılmasını sağlayabilir. Bu teknik, ayrıcalık yükseltme ve kalıcılık sağlamak için kullanılır.

- **T1543.002: Systemd Hizmeti**

  Saldırganlar, Linux sistemlerinde systemd hizmetlerini kötüye kullanarak kötü amaçlı yüklerin kalıcılığını sağlayabilir. Systemd, hizmetleri yönetmek için .service uzantılı birim yapılandırma dosyalarını kullanır. Saldırganlar, bu dosyaları değiştirerek veya yeni hizmet dosyaları oluşturarak kötü amaçlı komutların otomatik olarak çalıştırılmasını sağlayabilir. Ayrıca, sembolik bağlantılar kullanarak kötü amaçlı yüklerin bulunmasını zorlaştırabilirler.

T1485: Veri İmhası

Saldırganlar, sistemlere ve ağlara zarar vermek için büyük miktarda veri ve dosyayı imha edebilir. Veriler, rastgele oluşturulmuş içeriklerle üzerine yazılarak kurtarılamaz hale getirilebilir. Bu tür saldırılar, ağ genelinde veri kaybını maksimize etmek için kötü amaçlı yazılımlar aracılığıyla yayılabilir. Bulut ortamlarında ise kritik depolama nesneleri, makine görüntüleri ve veritabanları silinebilir.

T1484: Alan veya Kiracı Politikası Değişikliği

Saldırganlar, etki alanı veya kimlik kiracısının yapılandırma ayarlarını değiştirerek savunmaları atlatabilir ve ayrıcalıkları artırabilir. Bu değişiklikler, etki alanları veya kiracılar arasındaki güven ilişkilerini manipüle edebilir. Saldırganlar, GPO'ları değiştirerek kötü amaçlı zamanlanmış görevler gönderebilir veya etki alanı güven ilişkilerini manipüle edebilir.

- **T1484.001: Grup Politikası Değişikliği**

  Saldırganlar, Active Directory (AD) ortamında Grup İlkesi Nesnelerini (GPO'lar) kötüye kullanarak ayrıcalıkları artırabilir. GPO'lar, kullanıcı ve bilgisayar ayarlarını merkezi olarak yönetmek için kullanılır. Saldırganlar, GPO ayarlarını değiştirerek kötü

amaçlı zamanlanmış görevler ekleyebilir veya belirli kullanıcı haklarını değiştirerek etki alanının tam kontrolünü ele geçirebilir.

T1570: Yanal Alet Transferi

Saldırganlar, tehlikeye atılmış bir ortamda sistemler arasında araçlar veya dosyalar transfer edebilir. SMB/Windows Yönetici Paylaşımları, Uzak Masaüstü Protokolü veya scp, rsync gibi araçlar kullanılarak dosyalar kopyalanabilir. Ayrıca, Dropbox veya OneDrive gibi Web Servisleri kullanılarak dosyalar paylaşılabilir.

T1036: Maskeli

Saldırganlar, kullanıcıların ve güvenlik araçlarının gözünde meşru görünmek için eserlerinin özelliklerini manipüle edebilir. Bu, dosya meta verilerini değiştirmeyi, kullanıcıları dosya türünü yanlış tanımlamaya kandırmayı veya meşru görev veya hizmet adları vermeyi içerebilir.

- **T1036.004: Maskeli Görev veya Hizmet**

  Saldırganlar, meşru görünmesini sağlamak için bir görevin veya hizmetin adını değiştirebilir. Görev Zamanlayıcı veya systemd tarafından yürütülen görevler/hizmetler genellikle bir ad ve açıklama alır. Saldırganlar, meşru olanlarınkine benzer adlar vererek kötü amaçlı faaliyetlerini gizleyebilir.

T1095: Uygulama Dışı Katman Protokolü

Saldırganlar, ana bilgisayar ile C2 sunucusu arasında iletişim için OSI uygulama dışı katman protokolleri kullanabilir. ICMP, UDP, SOCKS gibi protokoller kullanılarak iletişim gizlenebilir. ICMP, TCP veya UDP kadar yaygın olarak izlenmez ve saldırganlar tarafından iletişimleri gizlemek için kullanılabilir.

T1572: Protokol Tünelleme

Saldırganlar, ağ iletişimlerini tünelleme yöntemiyle gizleyebilir. Tünelleme, bir protokolün başka bir protokol içinde kapsüllenmesini içerir. SSH tünelleme veya HTTPS üzerinden DNS (DoH) gibi yöntemler kullanılarak C2 iletişimleri gizlenebilir.

T1053: Zamanlanmış Görev/İş

Saldırganlar, kötü amaçlı kodun ilk veya tekrarlayan yürütülmesini sağlamak için görev planlama işlevselliğini kötüye kullanabilir. Windows Görev Zamanlayıcısı, saldırganlar

tarafından programları sistem başlangıcında veya belirli aralıklarla çalıştırmak için kullanılabilir.

- **T1053.005: Zamanlanmış Görev**

  Saldırganlar, Windows Görev Zamanlayıcısını kötüye kullanarak kötü amaçlı kodun yürütülmesini sağlayabilir. `schtasks` komut satırı aracı veya PowerShell cmdlet'leri kullanılarak zamanlanmış görevler oluşturulabilir. Saldırganlar, savunma araçları tarafından tespit edilmeyen "gizli" görevler oluşturabilir.

T1505: Sunucu Yazılım Bileşeni

Saldırganlar, sunucuların meşru genişletilebilir geliştirme özelliklerini kötüye kullanarak kalıcı erişim sağlayabilir. Kurumsal sunucu uygulamaları, geliştiricilerin ana uygulamanın işlevselliğini genişletmek için yazılım veya betikler yazmalarına olanak tanır.

- **T1505.003: Web Kabuğu**

  Saldırganlar, web sunucularına web kabukları yerleştirerek sistemlere kalıcı erişim sağlayabilir. Web kabukları, saldırganın web sunucusu üzerinden komutlar çalıştırmasına olanak tanır. China Chopper gibi web kabuğu istemcileri, saldırganların web sunucusuyla iletişim kurmasını sağlar.

Saldırının ICS Alanındaki Kullanılan Teknikleri:

T0895: Otomatik Çalıştırma Görüntüsü

Saldırganlar, AutoRun işlevselliğini kullanarak kötü amaçlı kod yürütebilir. Bu özellik, özellikle çıkarılabilir medya üzerinde depolanan kötü amaçlı yazılımları çalıştırmak için kullanılabilir. Sanal makine ortamlarında, saldırganlar disk görüntülerine kötü amaçlı AutoRun betikleri ekleyebilir.

T0807: Komut Satırı Arayüzü

Saldırganlar, sistemlerle etkileşim kurmak ve komutları yürütmek için komut satırı arayüzlerini (CLI'ler) kullanabilir. CLI'ler, kontrol sistemleri ortamlarındaki birçok platform ve cihaz türünde ortak bir özelliktir. Saldırganlar, SSH, Telnet ve RDP gibi hizmetler aracılığıyla CLI'lara erişebilir.

T0853: Komut Dosyası

Saldırganlar, betik dillerini kullanarak keyfi kod yürütebilir. Betik dilleri, derlenmiş dillerden farklı olarak bir yorumlayıcı kullanır. Python gibi betik dilleri, saldırganlar tarafından hedef ortamda kod yürütmek için kötüye kullanılabilir.

T0894: Sistem İkili Proxy Çalıştırma

Saldırganlar, imzalanmış veya güvenilir ikili dosyaları kötü amaçlı içerik yürütmek için proxy olarak kullanarak savunma mekanizmalarını aşabilir. Bu dosyalar genellikle Microsoft tarafından imzalanmış olup, işletim sisteminde yerel olarak bulunur veya güvenilir kaynaklardan indirilmiştir. Windows ve Linux sistemlerinde çeşitli güvenilir ikili dosyalar kötüye kullanılabilir. Ayrıca, saldırganlar belirli uygulama ikili dosyalarını kötü amaçlı kod yürütmek veya ağ cihazlarını hedeflemek için kullanabilir. Bu teknik, özel kötü amaçlı yazılım geliştirmeden saldırı gerçekleştirmeye olanak tanırken, bazen özel araçların kullanılmasını gerektirebilir.

T0855: Yetkisiz Komut Mesajı

Saldırganlar, kontrol sistemi varlıklarına yetkisiz komut mesajları gönderebilir. Bu mesajlar, cihazların normal sınırlarının dışında eylemler gerçekleştirmesine neden olabilir. Saldırganlar, kontrol sistemi cihazlarına zarar verici eylemler gerçekleştirmesi talimatını verebilir.

Bir Şirketin Hacklenme Senaryosu

Bir orta ölçekli teknoloji şirketi, siber güvenlik altyapısını aşmak ve hassas verilerini ele geçirmek amacıyla organize bir siber saldırı grubu tarafından hedef alınmıştır. Saldırganlar, şirketin dijital varlıklarını ve çalışanlarını hedef alan karmaşık bir saldırı kampanyası başlatmıştır. Saldırganlar, ilk olarak şirketin internete açık sistemlerini ve çalışanların dijital ayak izlerini detaylı bir şekilde analiz ederek zafiyetlerini belirlemişlerdir. Daha sonra bu bilgileri kullanarak sisteme sızmış, yetkilerini artırmış ve güvenlik önlemlerini atlayarak şirketin kritik verilerini uzak bir sunucuya sızdırmışlardır.

1. Keşif (Reconnaissance)

Saldırganlar, şirketin internete açık varlıklarını ve çalışanlarını keşfetmek için başlangıçta bilgi toplama faaliyetlerinde bulunurlar.

- Active Scanning (Aktif Tarama) - T1595
  Saldırganlar, şirketin web sunucuları ve ağ altyapısına yönelik aktif taramalar gerçekleştirerek açık portlar ve zafiyetler bulurlar.
- Social Media Harvesting (Sosyal Medya Bilgi Toplama) - T1594
  Şirket çalışanlarının sosyal medya hesaplarını inceleyerek e-posta adresleri ve kişisel

bilgiler toplayarak sosyal mühendislik saldırıları için hazırlık yaparlar.

2. İlk Erişim (Initial Access)

Saldırganlar, topladıkları bilgileri kullanarak sisteme girmek için bir giriş noktası oluştururlar.

- Spearphishing Attachment (Hedefli Phishing Eki) - T1566.001
  Çalışanlara zararlı bir dosya eklenmiş hedefli bir phishing e-postası gönderirler. Bir çalışan dosyayı açtığında, saldırganlar sisteme ilk erişimi elde ederler.
- Exploit Public-Facing Application (İnternete Açık Uygulamayı Açıklardan Yararlanma) - T1190
  Daha önce keşfettikleri zafiyeti kullanarak, şirketin internete açık bir uygulamasını ele geçirirler ve bu yolla da sisteme erişim sağlarlar.

3. Yetki Yükseltme (Privilege Escalation)

Sisteme girdikten sonra, saldırganlar daha fazla kontrol sağlamak için ayrıcalıklarını yükseltirler.

- Valid Accounts (Geçerli Hesaplar) - T1078
  Ele geçirdikleri bir kullanıcının kimlik bilgilerini kullanarak yetkili bir hesap üzerinden hareket ederler.
- Process Injection (İşlem Enjeksiyonu) - T1055
  Mevcut bir işleme kötü amaçlı kod enjekte ederek yönetici yetkilerini ele geçirirler.

4. Savunma Kaçışı (Defense Evasion)

Saldırganlar, güvenlik mekanizmalarını atlamak ve faaliyetlerini gizlemek için çeşitli yöntemler kullanırlar.

- Disable or Modify Tools (Araçları Devre Dışı Bırakma veya Değiştirme) - T1562.001
  Güvenlik yazılımlarını devre dışı bırakarak tespit edilmelerini engellerler.
- File and Directory Permissions Modification (Dosya ve Dizin İzinlerini Değiştirme) - T1222
  Kritik dosya ve dizinlerin izinlerini değiştirerek erişimlerini kolaylaştırırlar.

5. Veri Sızdırma (Exfiltration)

Son olarak, saldırganlar şirketin hassas verilerini toplar ve dışarıya aktarır.

- Exfiltration Over C2 Channel (C2 Kanalı Üzerinden Veri Kaçırma) - T1041
  Topladıkları verileri komuta ve kontrol (C2) sunucusuna aktararak uzak bir konuma kaydederler.
- Automated Exfiltration (Otomatikleştirilmiş Veri Kaçırma) - T1020
  Otomatikleştirilmiş araçlar kullanarak düzenli aralıklarla veri aktarımı gerçekleştirirler.

Raporun Değerlendirilmesi ve Kazanımlar

Bu rapor, MITRE ATT&CK çerçevesinin siber güvenlikteki önemini, içerdiği taktik, teknik ve prosedürlerin (TTP) nasıl kullanıldığını detaylı bir şekilde ortaya koymuştur. Araştırma sonucunda, MITRE ATT&CK'in sadece saldırıları tespit etmede değil, aynı zamanda savunma stratejileri geliştirme, tehdit avcılığı (TTP-Based Threat Hunting) ve tespit mühendisliği (Detection Engineering) gibi kritik güvenlik süreçlerinde önemli bir rehber olduğu görülmüştür. Ayrıca, 2022 Ukrayna Elektrik Gücü Saldırısı gibi örnekler üzerinden, gerçek dünyada saldırganların hangi teknikleri nasıl kullandıkları ve bu saldırılara karşı alınabilecek önlemler anlaşılmıştır. Sonuç olarak, bu çalışma, güvenlik profesyonellerinin saldırgan davranışlarını daha iyi anlamalarına, proaktif savunma önlemleri geliştirmelerine ve siber tehditlere karşı daha hazırlıklı olmalarına katkı sağlamıştır.

KAYNAKÇA

https://attack.mitre.org/

https://www.ibm.com/think/topics/mitre-attack

https://cyberartspro.com/mitre-attack-framework-nedir/?utm_source=chatgpt.com

https://www.cozumpark.com/mitre-attck-ile-guvenlik-sikilastirmasi-bolum-1/?utm_source=chatgpt.com

https://cyberwebeyeos.com/siber-guvenlik/mitre-attck/mitre-attck-nedir?utm_source=chatgpt.com

https://www.feroot.com/education-center/what-are-tactics-techniques-and-procedures-ttps/

https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html

https://www.splunk.com/en_us/blog/learn/detection-engineering.html

https://netenrich.com/blog/what-is-detection-engineering?utm_source=chatgpt.com

https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf

https://chatgpt.com/

https://chat.qwenlm.ai/

https://chat.deepseek.com/