MITRE ATTACK FRAMEWORK VE PYRAMID OF PAIN

MELİKE TAŞDELEN

17.02.2025

GİRİŞ

Günümüzde siber güvenlik tehditleri giderek daha karmaşık hale gelmekte ve geleneksel güvenlik önlemleri, gelişmiş saldırı tekniklerine karşı yetersiz kalmaktadır. Bu noktada, tehdit istihbaratı ve tehdit avcılığı süreçlerini destekleyen MITRE ATT&CK Framework ve Pyramid of Pain gibi modeller, güvenlik uzmanlarının tehditleri daha iyi anlamasına ve etkili savunma stratejileri geliştirmesine yardımcı olmaktadır.

MITRE ATT&CK Framework, saldırganların kullandığı taktikler, teknikler ve prosedürler (TTP'ler) hakkında bilgi sunarak, güvenlik ekiplerinin tehditleri sınıflandırmasını, analiz etmesini ve önlem almasını sağlar. Aynı zamanda, TTP tabanlı tehdit avcılığı (Threat Hunting) ve algılama mühendisliği (Detection Engineering) gibi proaktif güvenlik yaklaşımlarını destekleyerek, kuruluşların siber tehditleri saldırı zincirinin erken aşamalarında tespit etmesine olanak tanır.

Bununla birlikte, Pyramid of Pain modeli, tehdit göstergelerinin (IoC) saldırganlar üzerindeki etkisini değerlendirerek, savunma stratejilerinin ne ölçüde saldırganları zorlayabileceğini gösterir

İÇİNDEKİLER

Mitre Atak Tablosu Nedir?

Kar amacı gütmeyen bir kuruluş olan MITRE Corporation tarafından geliştirilen, saldırgan davranışının fiilen gözlemlenmesiyle toplanan siber saldırgan taktikleri ve tekniklerinden oluşan kapsamlı bir bilgi tabanıdır. Evrensel olarak erişilebilir ve sürekli olarak güncellenir böylece güvenlik ekiplerine yardımcı olabilir. Ayrıca, MITRE ATT&CK'nin saldırgan taktikleri, teknikleri ve alt tekniklerine ilişkin sınıflandırması güvenlik uzmanlarının siber tehditler hakkında bilgi paylaşmak ve tehdit önleme konusunda iş birliği yapmak için kullanabilecekleri ortak bir dil oluşturur.

Mitre Atak Tablosu Neden Önemlidir?

Anlık güvenlik önlemleri sağlamanın yanı sıra uzun vadeli stratejik planlama ve sürekli iyileştirme için de temel oluşturur. Ortak dil kullanımı, işbirliğiyle birlikte bilgi paylaşımını teşvik eder, bu da daha etkili tehdit koordinasyonu sağlar.

Siber saldırıları daha iyi anlamaya yardımcı olur, böylece olası saldırılar gerçekleşmeden önce savunma stratejileri geliştirilebilir. Sürekli güncellenen bir framework olması sebebiyle en yeni tehdit senaryolarının saldırı teknikleri hakkında dahi bilgiler sunar.

TTP Nedir?

Taktik, teknikler ve prosedürler(TTP'ler), siber güvenlik,tehdit istihbaratı ve olay müdahalesi alanında kullanılan temel bileşenlerdir ve siber saldırganların nasıl çalıştığını ve saldırıları nasıl gerçekleştirdiğini açıklar. Bu üç unsur, bir tehdit grubunun ve belirli bir tehdit aktörünün yöntemlerini ve davranışlarını anlamak için yapılandırılmış bir yol sağlar.

TTP'ler, siber güvenlik uzmanlarının siber tehditleri ve saldırıları anlamaları, kategorize etmeleri ve bunlara yanıt vermeleri için bir bilgi tabanı, çerçeve ve metodoloji olan Mitre Atak'ın temel bileşenleridir . Taktikler, bir saldırının üst düzey hedeflerini tanımlamasına, Teknikler ise saldırganların hedeflere ulaşmak için kullandıkları yöntemleri açıklamasına , Prosedürler de tekniklerin somut örneklerini ve uygulama ayrıntılarını sağlamasına yardımcı olur. Mitre Ataktaki bu yapı, güvenlik uzmanlarının siber tehditleri etkili bir şekilde anlamalarına ve bunlara yanıt vermelerine yardımcı olur.

Taktikler

Saldırganların amaçlarına ulaşmak için kullandığı geniş stratejilerdir. Güvenlik uzmanları ve tehdit avcıları, rakiplerin genel hedeflerini anlamak için taktikleri kullanabilir ve bu da onların olası saldırı vektörlerini tahmin etmelerine yardımcı olur .

Teknikler

Taktiklerin altında yer alan daha spesifik saldırı yöntemleridir. Her bir taktik altında birden fazla teknik bulunabilir. Güvenlik ekipleri, özel algılama kuralları ve uyarılar oluşturmak için bilinen düşman tekniklerini ortamlarının günlüklerine ve veri kaynaklarına eşleyebilir.

Prosedürler

Güvenlik analistleri, tekniklerin pratik uygulamasına ilişkin içgörüler elde etmek için prosedürleri kullanabilir. Prosedürler bazen bir saldırı sırasında geride bırakılan benzersiz özelliklere veya eserlere dayanarak kötü niyetli bir aktörün kimliği veya kökeni hakkında ipuçları da sağlayabilir.

TTP analizi, siber saldırganlara karşı savunma için değerli bir yaklaşımdır. Siber suçlular ve tehdit aktörleri tarafından kullanılan davranışları ve yöntemleri incelemeyi ve anlamayı içerir.

Siber güvenlikte TTP-Based Threat Hunting ve Detection Engineering, saldırganların TTP yani taktik, teknik ve prosedürlerine dayalı olarak tehdit avcılığı yapmayı ve tespit mekanizmaları geliştirmeyi amaçlayan iki kritik yaklaşımdır.

Threat Hunting

Threat Hunting, tehditlerin belirlenmesi, analiz edilmesi ve ortadan kaldırılması için geliştirilmiş tekniklerden oluşur. Tehdit avcılığı proaktif bir siber savunma faaliyetidir. Tehdit avcılığı, tehditleri tespit etmek için yalnızca güvenlik çözümlerine veya hizmetlerine güvenmek yerine, sistematik bir güvenlik stratejileri için öngörücü bir güvensiz ve kuruluşlara tehditlere devam etme yetkisi verir. Siber güvenlik uzmanlarının ağlarda ve sistemlerde gizlenmiş tehditleri aktif olarak aradığı bir süreçtir.

Indicators of Compromise (IOC)

Bir sistemde kötü niyetli bir etkinliğin veya güvenlik ihlalinin meydana geldiğine dair işaretlerdir.

Indicators of Attack (IOA)

Saldırının başlangıcını veya devam ettiğini gösteren işaretlerdir.

Tactics, Techniques, and Procedures (TTP)

Saldırganların bir saldırıyı gerçekleştirmek için kullandıkları yöntemler, teknikler ve prosedürlerdir.

Cyber Threat Intelligence (CTI)

Tehdit istihbaratı, siber tehditler hakkında toplanan, değerlendirilen ve analiz edilen bilgileri ifade eder.

Threat Hunting Teknikleri

Geleneksel güvenlik önlemlerinin ötesine geçerek siber saldırıları erken aşamalarda belirlemeye yardımcı olur. Yaygın olarak kullanılan bazı tehdit avlama teknikleri :

Hipotez Tabanlı Avlama (Hypothesis Hunting)

Hipotezler, mevcut tehdit istihbaratı, güvenlik olayları ve ağ trafiği verilerine dayanarak geliştirilir. Hipotezler test edilerek doğrulanır veya çürütülür.

Davranışsal Analiz (Behavior Analysis)

Kullanıcı ve sistem davranışlarının normalden sapmalarını tespit etmeye odaklanır. Bu teknik, sistemler ve kullanıcılar arasındaki tipik etkileşim modellerini belirler ve anormal davranışları tespit eder.

Anomali Tespiti (Anomaly Detection)

Ağ trafiği, sistem olayları gibi çeşitli veri kaynaklarında normal davranıştan sapmaları belirlemeyi amaçlar. Anomali tespiti, makine öğrenimi ile veri analizi araçlarını kullanarak normal davranış modellerini öğrenip bu modellerden sapmaları tespit eder.

IOC Tabanlı Avlama (IOC Threat Hunting)

IOC tabanlı avlama, göstergeleri izleyip tespit ederek tehditleri belirlemeyi amaçlar.

Detection Engineering

Algılama Mühendisliği, kötü amaçlı faaliyetleri gösterebilecek belirli kalıpları, davranışları ve Tehlikeye Atma Göstergelerini (IoC'ler) tanımlayan tehdit algılama kuralları kümelerinin oluşturulmasıdır. Tespit Mühendisliği, kuruluşlardaki güvenlik ihlallerini tespit etmede ve sonrasında engellemede önemli bir rol oynar ve sıklıkla Ürün Güvenliği ve Kurumsal Güvenlik gibi ekiplerle ortaklık kurar.

Tespit mühendisliği hiçbir şekilde olayların (aktivitenin) tespiti ile sınırlı değildir. Ayrıca, dijital adli tıpta veya olay müdahalesinde sıklıkla kullanılan koşulların (durumların) tespitini de içerir.

Neden Önemlidir?

- Tehditleri saldırı zincirinin erken aşamalarında tespit ederek kuruluşlar, olası ihlalleri büyümeden önleyebilirler.
- Etkili tespit, güvenlik olaylarıyla ilişkili mali etkiyi azaltır.
- Şüpheli davranışları yakalayabilir.
- Gelişmiş tespit mekanizmaları kullanarak yanlış alarmları azaltır.
- İçerideki anormal aktiviteleri de analiz ederek iç tehditleri engelleyebilir.
- Sürekli güncellenerek en yeni saldırılara karşı korunmayı sağlar.

2022 UKRANIE ELECTRİC POWER ATTACK

2022 yılında Ukrayna'nın elektrik altyapısına yönelik gerçekleştirilen saldırı Sandworm Team adlı tehdit aktörü tarafından düzenlenmiştir. Bu saldırıda, saldırganlar çeşitli kötü amaçlı yazılımlar ve teknikler kullanarak SCADA sistemleri üzerinden yetkisiz komutlar göndermişlerdir.

Komut ve Betik Yorumlayıcısı: PowerShell (T1059.001)

Saldırganlar, TANKTRAP adlı bir PowerShell aracını kullanarak, Windows Group Policy üzerinden bir wiper (silici) yazılımını yaymış ve çalıştırmışlardır. Bu teknik, sistemde komutların yürütülmesi ve kötü amaçlı yazılımların dağıtılması için kullanılmıştır.

Sistem Süreci Oluşturma veya Değiştirme: Systemd Servisi (T1543.002)

GOGETTER adlı kötü amaçlı yazılımın kalıcılığını sağlamak için saldırganlar, Systemd yapılandırmasını değiştirmişlerdir. Sistem kullanıcı girişlerini kabul etmeye başladığında GOGETTER'ın otomatik olarak çalışmasını sağlamışlardır.

Veri İmhası (T1485)

Saldırganlar, CaddyWiper adlı zararlı yazılımı kullanarak, hedef sistemlerdeki OT (Operasyonel Teknoloji) ile ilgili dosyaları, haritalanmış sürücüleri ve fiziksel disk bölümlerini silmişlerdir. Bu teknik, sistemlerin işlevselliğini bozmak ve veri kaybına neden olmak amacıyla uygulanmıştır.

Etki Alanı veya Kiracı Politikası Değiştirme: Grup Politikası Değişikliği (T1484.001)

Saldırganlar, kötü amaçlı yazılımları dağıtmak ve çalıştırmak için **Group Policy Objects (GPO)** kullanmışlardır. Bu yöntemle, zararlı yazılımların hedef sistemlere yayılması ve yürütülmesi sağlanmıştır.

Yanal Araç Transferi (T1570)

CaddyWiper'ın çalıştırılabilir dosyası, saldırganlar tarafından bir GPO aracılığıyla bir hazırlık sunucusundan yerel diske kopyalanmıştır. Bu teknik, zararlı yazılımın hedef sistemlere taşınması ve dağıtılması için kullanılmıştır.

Gizleme: Görev veya Servis Maskelenmesi (T1036.004)

Saldırganlar, Systemd servis birimlerini kullanarak, GOGETTER kötü amaçlı yazılımını yasal veya meşru görünen servisler olarak gizlemişlerdir. Bu sayede, zararlı yazılımın tespit edilmesi zorlaştırılmıştır.

Uygulama Katmanı Dışı Protokol (T1095)

Komuta ve Kontrol (C2) iletişimlerini gizlemek için saldırganlar, TLS tabanlı tünelleme kullanarak C2 trafiğini şifrelemişlerdir. Bu yöntem, ağ trafiğinin izlenmesini ve tespit edilmesini zorlaştırmıştır.

Protokol Tünelleme (T1572)

Saldırganlar, GOGETTER tünelleme yazılımını kullanarak, harici sunucularla TLS tabanlı bir C2 kanalı oluşturmuşlardır. Bu teknik, güvenlik kontrollerini atlatmak ve gizli iletişim kanalları kurmak için uygulanmıştır.

Zamanlanmış Görev/İş: Zamanlanmış Görev (T1053.005)

CaddyWiper'ı belirli bir zamanda çalıştırmak için saldırganlar, bir GPO aracılığıyla Zamanlanmış Görevler oluşturmuşlardır. Bu yöntem, zararlı yazılımın önceden belirlenmiş bir zamanda otomatik olarak yürütülmesini sağlamıştır.

Sunucu Yazılım Bileşeni: Web Shell (T1505.003)

Saldırganlar, internet üzerinden erişilebilen bir sunucuya web shell yerleştirmişlerdir. Bu araç, saldırganlara hedef sistem üzerinde uzaktan kontrol imkânı sağlamıştır.

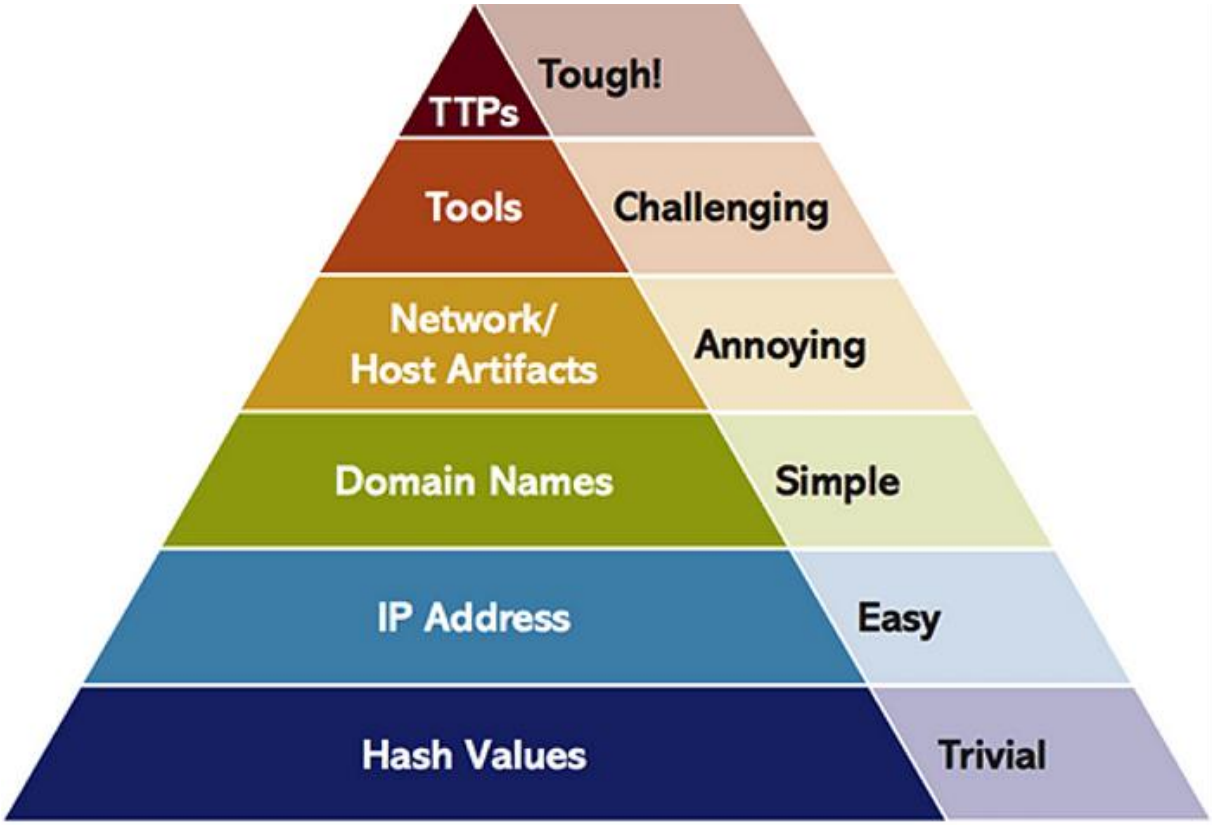
Otomatik Çalışan Görüntü (T0895)

Saldırganlar, mevcut hiper yönetici erişimini kullanarak, bir ISO görüntüsünü SCADA sunucusu çalıştıran sanal makineye bağlamışlardır. SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik çalıştıracak şekilde yapılandırılmış olduğundan, ISO görüntüsündeki kötü amaçlı VBS betiği otomatik olarak çalıştırılmıştır.

PYRAMID OF PAIN

Siber güvenlikte tehdit istihbaratı ve tehdit avcılığı süreçlerinde kullanılan bir modeldir. 2013 yılında ortaya çıkan güvenlik uzmanı David J Bianco'nun icadıdır. Bu pramit , saldırganların izlediği teknikleri ve güvenlik analistlerinin bu izleri tespit ettiğinde saldırganlar üzerinde oluşturduğu etkiyi gösterir.

Pyramid of Pain Katmanları



Piramit, alt seviyeden üst seviyeye doğru gittikçe saldırganlar için daha fazla "acı" veren (yani onların operasyonlarını daha fazla zorlaştıran) göstergelerden oluşur.

Hash Values

Dosyaların dijital imzaları olan hash'ler, saldırganların değiştirmesi oldukça kolay olan göstergelerdir.

IP Address

Saldırganlar IP adreslerini kolayca değiştirebilir, bu da onları engellemenin nispeten az etki yaratacağı anlamına gelir.

Domain Names

Domain isimlerini engellemek, saldırganın yeni bir domain oluşturmasını gerektirir.

Network/Host Artifacts

Saldırganın ağda bıraktığı izler veya yapılandırmalar daha özeldir ve değiştirilmesi daha zordur.

Tools

Saldırganların kullandığı araçları engellemek, operasyonlarını ciddi anlamda zorlaştırır.

TTPS

Piramidin en üstünde yer alan TTP'ler, saldırganın genel stratejileridir.

SONUÇ

Geleneksel güvenlik önlemlerinin yanı sıra proaktif tehdit avcılığı ve istihbarat odaklı güvenlik yaklaşımlarının önemi artmaktadır. MITRE ATT&CK Framework ve Pyramid of Pain gibi modeller, güvenlik ekiplerine saldırganların davranışlarını anlama, tehditleri önceden tespit etme ve saldırganları etkisiz hale getirme konusunda kritik avantajlar sağlar.

MITRE ATT&CK, siber saldırganların kullandığı taktikler, teknikler ve prosedürler (TTP'ler) hakkında derinlemesine bilgi sunarak, güvenlik uzmanlarının tehditleri daha sistematik bir şekilde analiz etmesine ve önleyici tedbirler almasına yardımcı olur. Pyramid of Pain ise saldırganların operasyonlarını ne ölçüde zorlaştırabileceğimizi anlamamıza yardımcı olarak, daha etkili savunma stratejileri geliştirmemizi sağlar.

Bu iki modelin birlikte kullanılması, tehdit istihbaratı, tehdit avcılığı ve güvenlik olaylarına müdahale süreçlerini daha etkili hale getirir. Özellikle TTP tabanlı tehdit avcılığı ve davranışsal analiz yöntemleri, saldırganların basit değişikliklerle güvenlik önlemlerini aşmasını engelleyerek, uzun vadeli bir güvenlik stratejisi oluşturulmasına katkı sağlar.

Sonuç olarak, kuruluşların siber tehditlere karşı daha dirençli olabilmesi için yalnızca geleneksel güvenlik önlemlerine değil, MITRE ATT&CK ve Pyramid of Pain gibi kapsamlı tehdit istihbaratı modellerine dayalı savunma mekanizmalarına yönelmesi gerekmektedir. Böylece, saldırganların yalnızca izlerini değil, saldırı yöntemlerini de engelleyerek, daha sürdürülebilir bir siber güvenlik yaklaşımı benimsenebilir.

KAYNAKÇA

https://medium.com/software-development-turkey/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-91554269b9b6

https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/pyramid-pain-threat-detection/

https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain

https://sdogancesur.medium.com/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-nedir-d20f3d86541e

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

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

https://medium.com/@dusiber/mitre-att-ck-9c8a66d9b46f

https://www.broadcom.com/topics/mitre-attack

https://www.mitre.org/focus-areas/cybersecurity/mitre-attack