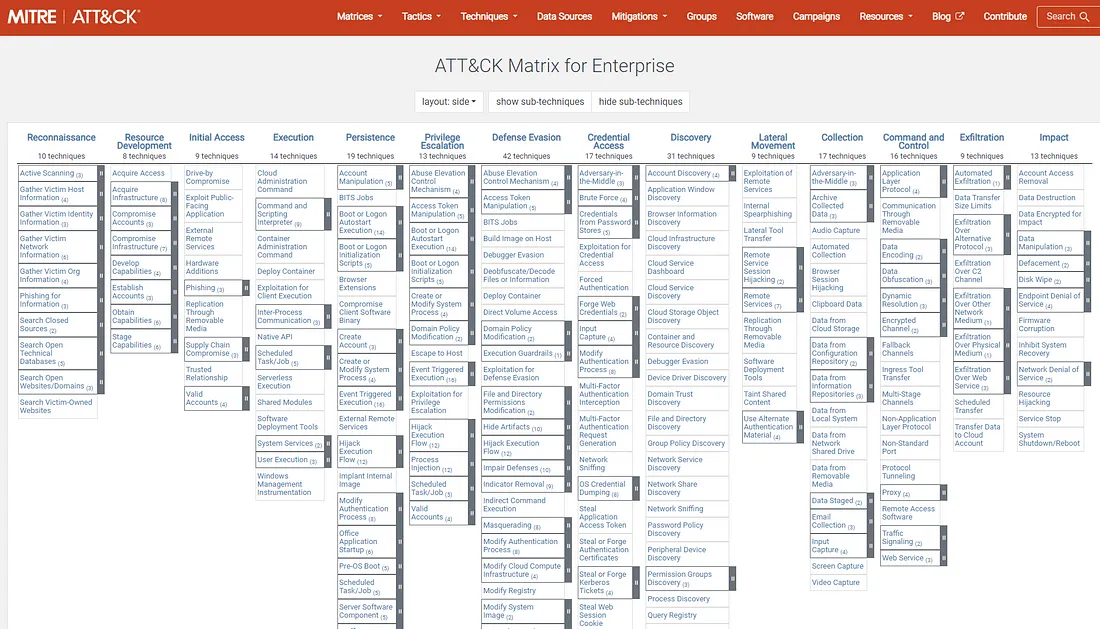
17.02.2025



**Mitre ATT&CK**  
  
  
Şerif GÜL

Altay Takımı

****

**Giriş**

**MITRE ATT&CK Tarihçesi**

MITRE, Bedford, Massachusetts ve McLean, Virginia'da bulunan tarafsız, kar amacı gütmeyen bir kuruluştur. Federal hükümete mühendislik ve teknik rehberlik sağlamak üzere kurulmuştur.

MITRE ATT&CK çerçevesi, gelişmiş kalıcı tehdit (APT) gruplarının kurumsal işletmelere karşı kullandığı TTP'leri belgelemek için 2013 yılında bir MITRE araştırma projesinin parçası olarak geliştirilmiştir. FMX adlı bir MITRE araştırma projesi tarafından kullanılacak düşman TTP'lerini tanımlama ihtiyacından doğmuştur.

FMX'in amacı, uç nokta telemetri verilerinin ve analizlerinin, kurumsal ağlarda faaliyet gösteren saldırganların saldırı sonrası tespitini iyileştirmeye nasıl yardımcı olabileceğini araştırmaktı. ATT&CK çerçevesi, FMX kapsamındaki sensörlerin ve analitiklerin etkinliğini test etmek için kullanıldı ve hem hücum hem de savunmanın zaman içinde gelişmek için kullanabileceği ortak bir dil olarak hizmet etti.

MITRE ATT&CK, 2015 yılı itibariyle ücretsiz olarak kullanıma sunulmuş ve tüm dünyadan indirilebilmektedir. Bugün, tüm sektörlerdeki kuruluşların güvenlik ekiplerinin mevcut tehditleri daha iyi anlamalarına ve sistemlerini bunlara karşı güvence altına almalarına yardımcı olmaktadır.

MITRE ATT&CK çerçevesi, yeni siber güvenlik kullanım durumları için tehdit istihbaratı ihtiyaçlarına ayak uyduracak şekilde değişerek gelişmeye devam etmiştir. MITRE ATT&CK başlangıçta tek bir hedef ortama (örneğin, Windows kurumsal sistemleri) yönelik tehditleri ele almak için geliştirilmiş olsa da, Linux, macOS, mobil, bulut, ağ, konteynerler ve endüstriyel kontrol sistemleri (ICS) dahil olmak üzere diğerlerine yönelik siber saldırıları da içerecek şekilde genişletilmiştir.

**MITRE ATT&CK Tablosunun Önemi**

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.

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.

MITRE ATT&CK'yi entegre etmenin başlıca faydalarından biri tehdit istihbaratının ve güvenlik operasyonlarının geliştirilmesidir. Ekipler, gerçek dünya saldırılarını simüle etmek için çerçeveden yararlanabilir ve sistemlerindeki güvenlik açıklarını istismar etmeden önce belirleyebilir. Bu proaktif yaklaşım güvenlik duruşlarını güçlendirir ve güvenlik ekiplerini gelişen siber tehditler konusunda eğitir.

Dahası, çerçeve siber güvenlik uzmanları için ortak bir dil oluşturmayı kolaylaştırır. Tehditleri standart bir şekilde kategorize ederek ve tanımlayarak, ekipler arasında ve dış paydaşlarla iletişimi kolaylaştırır, olaylar sırasında işbirliğini ve yanıt sürelerini iyileştirir.

Kuruluşlar ayrıca MITRE ATT&CK veri tabanına yapılan sürekli güncellemelerden ve topluluk katkılarından da faydalanmaktadır. Yeni teknikler ve taktikler gözlemlendikçe ve belgelendikçe, çerçeve gelişir ve mevcut tehdit ortamını yansıtan güncel bir kaynak sunar.

MITRE ATT&CK Teknikleri ve Önemi

MITRE ATT&CK teknikleri, siber saldırganlar tarafından kullanılan taktik ve tekniklerin kapsamlı ve sürekli gelişen bir listesidir. Teknikler, bir siber saldırının farklı aşamalarını temsil eden 11 kategori veya taktik şeklinde düzenlenmiştir.

Bu taktikler, kuruluşların saldırganların ağlarını veya sistemlerini tehlikeye atabilecekleri farklı yolları daha iyi anlamalarına yardımcı olmak için tasarlanmıştır. Teknikler, tehdit istihbaratını tanımlamak ve paylaşmak için ortak bir dil sağlar ve bir kuruluşun savunmasındaki güvenlik açıklarını belirleyerek ve ele alarak güvenliği artırmak için kullanılabilir.

Aşağıda her bir taktiğe kısa bir genel bakış yer almaktadır:

İlk Erişim, kimlik avı veya güvenlik açıklarından yararlanma gibi bir hedef sistem veya ağ üzerinde ilk dayanağı elde etmek için kullanılır.

Yürütme, bir kötü amaçlı yazılım yükü çalıştırmak veya kod yürütmek için bir güvenlik açığından yararlanmak gibi hedef sistemde kötü amaçlı kod çalıştırmak için kullanılır.

Kalıcılık, yeni bir kullanıcı hesabı oluşturmak veya bir arka kapı yüklemek gibi bir sistemde yer edinmek için kullanılır.

Ayrıcalık Yükseltme, bir güvenlik açığından yararlanmak veya kimlik bilgilerini çalmak gibi bir sisteme daha yüksek düzeyde erişim elde etmek için kullanılır.

Savunma Kaçırma, kodu gizlemek veya antivirüs atlatma teknikleri kullanmak gibi güvenlik araçları veya savunucular tarafından tespit edilmekten kaçınmak için kullanılır.

Kimlik Bilgilerine Erişim, parolaları çalmak veya kaba kuvvet saldırıları kullanmak gibi geçerli kullanıcı kimlik bilgilerini elde etmek için kullanılır.

Keşif, açık bağlantı noktalarının taranması veya kullanıcı hesaplarının numaralandırılması gibi hedef sistem veya ağ hakkında bilgi toplamak için kullanılır.

Yanal Hareket, güvenlik açıklarından yararlanmak veya diğer sistemlere erişmek için çalınan kimlik bilgilerini kullanmak gibi bir ağ içinde yanal olarak hareket etmek için kullanılır.

Toplama, keylogging veya ekran görüntüsü alma gibi bir hedef sistem veya ağdan veri veya bilgi toplamak için kullanılır.

Sızma, bir hedef sistem veya ağdaki veri veya bilgileri bir dış kaynağa kopyalamak için kullanılır. Sızdırılan bu veriler daha sonra istismar kanıtı olarak veya şantaj için kullanılabilir.

Komuta ve Kontrol, bir uzaktan erişim aracı veya komuta ve kontrol sunucusu kullanmak gibi bir bağlantıyı sürdürmek ve güvenliği ihlal edilmiş bir sistem veya ağ ile iletişim kurmak için kullanılır.

**Teknik ,Taktik ve prosedür (TTP)**

Toplu olarak ele alındığında, TTP'ler insanların, genellikle güvenlik uzmanlarının, gerçekten gözlemlediği sistem yapılarının veya davranışsal özelliklerin göstergeleridir. TTP'ler, yetkisiz bir varlığın engellenen veya izin verilmeyen bir faaliyette bulunmaya çalıştığını gösterir veya gösterir, örneğin:

Ağın değiştirilmesi.

Hassas bilgi işlem kaynaklarına erişim.

Harici bir komuta ve kontrol sunucusuna veri gönderme.

Bu göstergeler genellikle tutarlı bir çerçeve izler. Bu davranışsal göstergeler, yakın bir siber güvenlik riskinin devam etmekte olduğunu göstermektedir. Etkili bir şekilde kullanıldığında, TTP'ler siber tehdit istihbaratını ve proaktif tehdit avcılığı gibi diğer güvenlik kullanım durumlarını bilgilendirebilir.

Bir güvenlik çerçevesi olan MIRE ATT&CK, saldırganların gerçek dünyada kullandıkları TTP'lerin kapsamlı bir koleksiyonudur.

TTP üçgeninin her bir parçasını tanımlayalım:

Taktikler: Bir tehdit aktörünün davranış ve stratejisinin üst düzey tanımı. Taktik, belirli bir hedefe ulaşmak için düşman tarafından kullanılan bir dizi davranış ve eylemi içerir.

Teknikler: Bunlar bir taktik eylemin nasıl gerçekleştirilebileceğini açıklayan spesifik olmayan kılavuzlar ve ara yöntemlerdir.

Prosedürler: Bunlar, bir saldırı taktiğini uygulamak için bir teknik kullanılarak gerçekleştirilen eylemler dizisini ifade eder. Prosedür, bir tehdit aktörünün hedeflerine başarıyla ulaşmasını sağlayan özel faaliyetlere ilişkin ayrıntılı açıklamaları içerir.

Şimdi Taktik, Teknik ve Prosedürleri ayrıntılı olarak gözden geçirelim.

(TTP'ler iş başında: tehdit araştırmacıları APT29 tarafından WINELOADER kampanyasında ve arka kapısında kullanılan TTP'leri analiz ediyor)

Taktikler

Bir tehdit aktörünün taktikleri, siber saldırı ölüm zincirinin farklı aşamalarında nasıl davrandıklarını açıklar. Bu aşamalar şunları içerir:

Keşif

Teslimat ve kullanım

Hedefler doğrultusunda hareket etmek

Bir kampanyaya potansiyel tehdit atfetmenin zorluğu, saldırının yeniliğine ve karmaşıklığına bağlıdır. Tehdit göstergeleri DDoS saldırıları gibi yaygın saldırı modellerini gösteriyorsa, aşağıdaki gibi konularda veri toplayarak kampanya taktiklerinin sonraki aşamaları tahmin edilebilir:

İlk giriş noktası(ları)

Güvenliği ihlal edilmiş düğümler veya kimlik bilgileri

Sofistike bir saldırı taktiği, radarın altında kalmaya ve kötü amaçlı bir yük teslim edilene veya veri varlıkları harici bir komuta ve kontrol sunucusuna sızana kadar tehlikeye atılan ağda yalnızca ince değişiklikler yapmaya odaklanır.

Taktikler nasıl ortaya çıkarılır

Bu tür saldırıları keşfetmenin yollarından biri, herhangi bir anormal ağ olayına yol açan eserleri, araçları ve altyapı değişikliklerini yakından analiz etmektir:

zeroday güvenlik açıklarından yararlanan sofistike bir siber saldırı, yüksek oranda gizlenmiş veya katmanlı özel araçlara dayanabilir.

Buna karşılık, sıradan bir bilgisayar korsanı yalnızca açık kaynaklı veya herkesin erişebileceği araçlar kullanabilir.

Düşmanla bir profil ilişkilendirmek ve savunma için karşı önlemleri proaktif olarak yetkilendirmek için aktörün taktiksel davranışının (giriş noktaları, saldırı araçları, altyapı değişiklikleri ve ağ trafiği davranışı) parmak izini kullanabilirsiniz.

Teknikler

Teknikler, tehdit aktörlerinin her türlü kötü soruna neden olmak için yaptıkları şeylerdir:

Bir ağa sızmak.

Komuta ve kontrol merkezleri kurmak.

İz bırakmadan ağ içinde yanal olarak hareket edin.

Kötü amaçlı yazılım bulaşmasını dağıtılmış ağ konumlarına yaymak.

İzi sürülemeyen altyapı değişiklikleri ve veri transferleri için kontrol sağlamak.

Bu teknikler geneldir ve her türlü siber saldırı kampanyasına uygulanabilir. Bu nedenle, tehdit aktörlerinin sistemlerinizi tehlikeye atmak için kullanabilecekleri yöntemleri ve araçları anlamak çok önemlidir.

Önemli bir ayrım. Teknikler teknolojiyi belirtmeyebilir, ancak yalnızca kampanyanın metodolojisine odaklanır ve ilgili eylemler dizisine rehberlik eder.

Örneğin, sosyal mühendislik amaçlı bir oltalama taktiği, şüphelenmeyen bir kullanıcıyı kandırarak yerel makineye kötü amaçlı bir yük indiren ve oturum açma kimlik bilgilerini çalan bir bağlantıya tıklamasını sağlamak için kullanılabilir. Bu teknik, sosyal mühendislik saldırısını daha inandırıcı kılmak amacıyla sınırlı sayıda kullanıcıyı hedef alacak şekilde özel olarak tasarlanmış olabilir.

teknikleri

Saldırının ilerleyen aşamalarında, özellikle de yük teslimi, ağ üzerinde hareket, yapılandırma değişiklikleri ve güvenlik açığı keşfinin söz konusu olduğu durumlarda, araç seçimi önemli bir rol oynar.

Bu aşamada, düşman zaten savunmasız bir sistem bileşenine özel bir kod yüklemiş olabilir. Kurulumun izi bulunamazsa, InfoSec ekiplerinin sistemi aşağıdakiler için analiz etmesi gerekebilir:

Yapılandırma suistimali

Altyapı değişiklikleri

Ayrıcalık yükseltmeleri

Sistemde yapılan diğer yetkisiz değişiklikler

Siber saldırı tekniğinin son aşaması, metodoloji ve araçların bir kombinasyonunu içerebilir: örneğin, ele geçirilen veri varlıklarının, önce aktörün ağ protokolleri ve şifreleme şemaları seçimini kullanarak gizlenmesi yoluyla dışarı sızdırılması.

Prosedürler

Prosedürler, tekniklerin seçimi ve bir dizi eyleme geçirilebilir, dikkatle hazırlanmış ve kesin eylemler (yani prosedürler) kullanılarak taktiklerin nasıl yürütüldüğünün ayrıntılı açıklamasıdır.

Bu eylemler son derece özelleştirilmiştir ve süreç, tehdit aktörlerinin şartnamelere göre tam olarak takip etmesi için belgelenmiştir. Bu eylemler kapsamlı olma eğilimindedir ancak sıklıkla tekrarlanır.

Kötü amaçlı bir kod teslim edilebilir ve otomatik veri toplama için savunmasız yazılıma yamalanabilir. Böyle bir kod otomatik olarak şifreyi çözer ve ilgili hizmetler ve araçlarla etkileşime girer.

Prosedürlerin öğrenilmesi

Güvenlik analitiği, ağ ve olay günlüklerini analiz ederek bu prosedürleri yeniden yapılandırabilir.Bu bilgileri analiz eden bir siber adli tıp ekibi, tehdit aktörü tarafından kullanılan genişletilmiş öldürme zinciri sürecine, tekniklere ve taktiklere de odaklanacaktır.

TTP siber tehdit istihbaratının temelini oluşturur

TTP bilgileri, güvenlik izleme sırasında keşfedilen tehdit göstergeleri ve izleri hakkında bağlamsal bilgi edinmek için önemli bir kılavuz görevi görür. TTP aynı zamanda Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından önerilen açık ve topluluk tabanlı siber güvenlik programlarının bir parçasıdır ve işletmelerin güvenlik duruşlarını geliştirmelerine yardımcı olmak için TTP bilgi tabanını paylaşma konusunda yönergeler sağlar.

EDR sistemleri, uç noktalarda (bilgisayarlar, sunucular vb.) şüpheli aktiviteleri tespit etmek ve tehditleri önlemek için kullanılır. Antivirüs çözümlerinin ötesine geçerek gelişmiş saldırıları analiz eder ve tehdit istihbaratı ile ilişkilendirir.

**Özellikleri:**

* Gerçek zamanlı tehdit tespiti ve analizi.
* Uç noktalar arasında bağlantılı olay incelemesi.
* Otomatik tehdit yanıt mekanizmaları (kötü amaçlı yazılımı karantinaya alma, süreçleri sonlandırma vb.).
* Siber tehdit avcılığı (Threat Hunting).

**2022 Ukraine Electric Power Attack C0034**

[T1059](https://attack.mitre.org/techniques/T1059).001 [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059): [PowerShell](https://attack.mitre.org/techniques/T1059/001): Saldırganlar komutları, komut dosyalarını veya ikili dosyaları çalıştırmak için komut ve komut dosyası yorumlayıcılarını kötüye kullanabilir

[T1543](https://attack.mitre.org/techniques/T1543).002 [Create or Modify System Process](https://attack.mitre.org/techniques/T1543): [Systemd Service](https://attack.mitre.org/techniques/T1543/002): Saldırganlar, kalıcılığın bir parçası olarak kötü amaçlı yükleri tekrar tekrar çalıştırmak için sistem düzeyinde service oluşturabilir veya bunları değiştirebilir.

[T1485](https://attack.mitre.org/techniques/T1485): [Data Destruction](https://attack.mitre.org/techniques/T1485): Saldırganlar, sistemlerin, hizmetlerin ve ağ kaynaklarının kullanılabilirliğini kesintiye uğratmak için belirli sistemlerdeki veya bir ağdaki çok sayıda veriyi ve dosyayı yok edebilir.

[T1484](https://attack.mitre.org/techniques/T1484) [.001](https://attack.mitre.org/techniques/T1484/001) [Domain or Tenant Policy Modification](https://attack.mitre.org/techniques/T1484): [Group Policy Modification](https://attack.mitre.org/techniques/T1484/001): Saldırganlar, merkezi olarak yönetilen ortamlarda savunmaları atlatmak ve/veya ayrıcalıkları artırmak için bir etki alanının veya kimlik kullanıcısının yapılandırma ayarlarını değiştirebilir.

[T1570](https://attack.mitre.org/techniques/T1570) [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) Saldırganlar, tehlikeye atılmış bir ortamda sistemler arasında araçlar veya diğer dosyaları transfer edebilir. Kurban ortamına getirildikten sonra (yani, [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) ) dosyalar, bir operasyon boyunca saldırgan araçları veya diğer dosyaları sahnelemek için bir sistemden diğerine kopyalanabilir.

[T1036](https://attack.mitre.org/techniques/T1036) [.004](https://attack.mitre.org/techniques/T1036/004) [Masquerading](https://attack.mitre.org/techniques/T1036): [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) Saldırganlar, meşru veya zararsız görünmesini sağlamak için bir görevin veya hizmetin adını değiştirmeye çalışabilir

[T1095](https://attack.mitre.org/techniques/T1095) [Non-Application Layer Protocol](https://attack.mitre.org/techniques/T1095) Saldırganlar, ana bilgisayar ile C2 sunucusu veya bir ağ içindeki enfekte ana bilgisayarlar arasında iletişim için bir OSI uygulama dışı katman protokolü kullanabilir.

[T1572](https://attack.mitre.org/techniques/T1572) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) Saldırganlar, tespit/ağ filtrelemesinden kaçınmak ve/veya aksi takdirde erişilemeyen sistemlere erişimi etkinleştirmek için ayrı bir protokol içinde bir kurban sistemine ve bu sistemden ağ iletişimlerini tünelleyebilir

[T1053](https://attack.mitre.org/techniques/T1053) [.005](https://attack.mitre.org/techniques/T1053/005) [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053): [Scheduled Task](https://attack.mitre.org/techniques/T1053/005) Saldırganlar, kötü amaçlı kodun ilk veya tekrarlayan yürütülmesi için görev zamanlaması yapmak üzere Windows Görev Zamanlayıcısını kötüye kullanabilir

[T1505](https://attack.mitre.org/techniques/T1505) [.003](https://attack.mitre.org/techniques/T1505/003) [Server Software Component](https://attack.mitre.org/techniques/T1505): [Web Shell](https://attack.mitre.org/techniques/T1505/003)

Saldırganlar, sistemlere kalıcı erişim sağlamak için sunucuların meşru genişletilebilir geliştirme özelliklerini kötüye kullanabilir

[T0895](https://attack.mitre.org/techniques/T0895) [Autorun Image](https://attack.mitre.org/techniques/T0895) Saldırganlar kötü amaçlı kod yürütmek için AutoRun işlevselliğini veya betiklerini kullanabilir.

[T0807](https://attack.mitre.org/techniques/T0807) [Command-Line Interface](https://attack.mitre.org/techniques/T0807) Saldırganlar sistemlerle etkileşim kurmak ve komutları yürütmek için komut satırı arayüzlerini (CLI'ler) kullanabilir.

[T0853](https://attack.mitre.org/techniques/T0853) [Scripting](https://attack.mitre.org/techniques/T0853) önceden yazılmış bir betik biçiminde veya bir yorumlayıcıya kullanıcı tarafından sağlanan kod biçiminde keyfi kodu yürütmek için betik dillerini kullanabilirler

[T0894](https://attack.mitre.org/techniques/T0894) [System Binary Proxy Execution](https://attack.mitre.org/techniques/T0894) Saldırganlar, imzalı veya başka şekilde güvenilir ikili dosyalarla kötü amaçlı içeriğin yürütülmesini proxy ederek işlem ve/veya imza tabanlı savunmaları aşabilir.

[T0855](https://attack.mitre.org/techniques/T0855) [Unauthorized Command Message](https://attack.mitre.org/techniques/T0855) Saldırganlar, kontrol sistemi varlıklarına amaçlanan işlevselliklerinin dışında veya beklenen işlevlerini tetiklemek için mantıksal ön koşullar olmadan eylemler gerçekleştirmeleri talimatını vermek için yetkisiz komut mesajları gönderebilir.

Siber Saldırı Senaryosu:

1. Keşif (Reconnaissance)

Tehdit aktörleri, A Şirketi hakkında bilgi toplamak için çeşitli keşif yöntemleri kullanır:

* Açık kaynak istihbaratı (OSINT): Şirketin çalışanlarının LinkedIn profillerini, sosyal medya hesaplarını ve şirketin internet üzerindeki varlığını analiz ederler.
* Hedefleme (T1593.002 - Search Open Technical Databases): Shodan gibi araçlar kullanarak şirketin açık servislerini ve IP adreslerini keşfederler.

2. İlk Erişim (Initial Access)

Saldırganlar şirket ağına sızmak için çeşitli yöntemler kullanır:

* Kimlik avı (T1566.001 - Spearphishing Attachment): Çalışanlara sahte e-postalar göndererek zararlı dosya eklerini açmalarını sağlarlar.
* Geçerli hesapların ele geçirilmesi (T1078.002 - Domain Accounts): Çalınmış veya tahmin edilen zayıf parolaları kullanarak iç ağa erişim elde ederler.

3. Yetki Yükseltme (Privilege Escalation)

İlk erişim sağlandıktan sonra, saldırganlar yönetici yetkilerini elde etmeye çalışır:

* Yerel güvenlik açıklarının istismarı (T1068 - Exploitation for Privilege Escalation): Windows veya Linux sistemlerindeki bilinen zafiyetleri kullanarak daha yüksek yetkilere ulaşırlar.
* Kimlik bilgisi dökümü (T1003.001 - LSASS Memory): Mimikatz gibi araçlarla RAM üzerinden kimlik bilgilerini çalarlar.

4. Savunmadan Kaçınma (Defense Evasion)

Saldırganlar, tespit edilmemek için aşağıdaki teknikleri kullanır:

* Gizli yürütme (T1202 - Indirect Command Execution): PowerShell ve LOLBins (Living off the Land Binaries) kullanarak zararlı komutları çalıştırırlar.
* Antivirüs atlatma (T1036.005 - Match Legitimate Name or Location): Zararlı dosyaları, sistemdeki yasal dosyalarla aynı isimde kaydederek fark edilmeden çalıştırırlar.

5. Etki ve Çıkış (Impact & Exfiltration)

Son aşamada saldırganlar verileri çalar ve sistemlere zarar verir:

* Veri sızdırma (T1567.002 - Exfiltration Over Web Service): Ele geçirilen hassas verileri, anonim bulut depolama hizmetlerine aktarırlar.
* Şifreleme ve fidye yazılımı (T1486 - Data Encrypted for Impact): Şirketin kritik dosyalarını şifreleyerek fidye talep ederler.

MITRE ATT&CK Tablosu

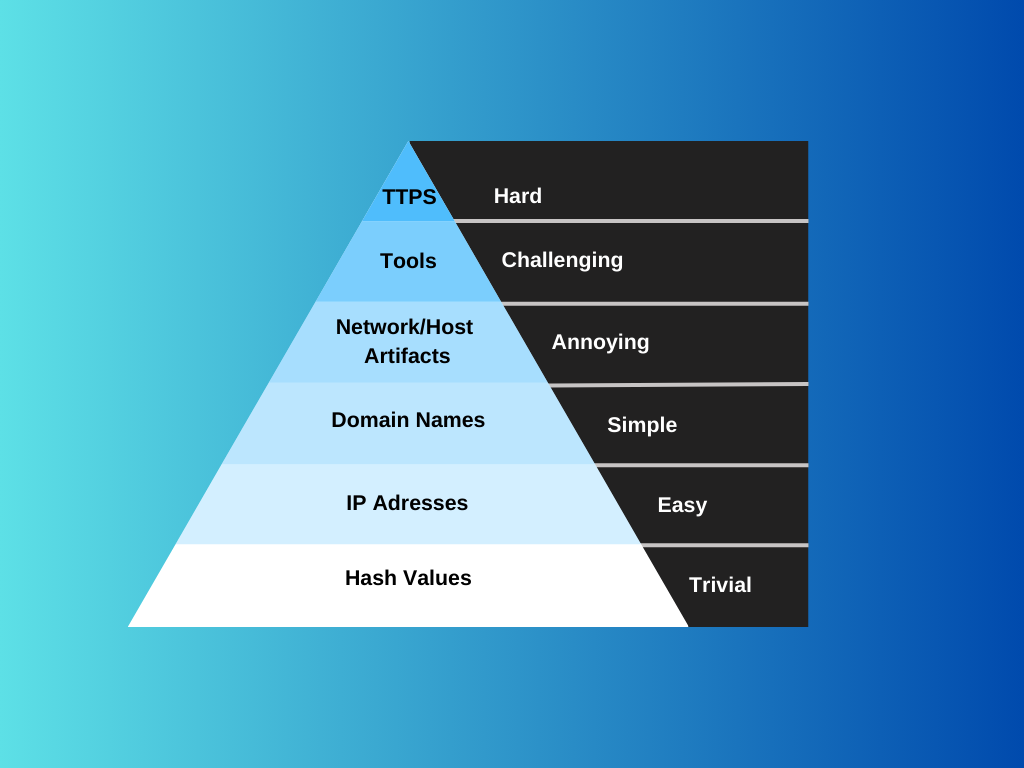
|  |  |  |
| --- | --- | --- |
| Taktik | Teknik | TID |
| Keşif (Reconnaissance) | Search Open Technical Databases | T1593.002 |
| İlk Erişim (Initial Access) | Spearphishing Attachment | T1566.001 |
| İlk Erişim (Initial Access) | Domain Accounts | T1078.002 |
| Yetki Yükseltme (Privilege Escalation) | Exploitation for Privilege Escalation | T1068 |
| Yetki Yükseltme (Privilege Escalation) | LSASS Memory | T1003.001 |
| Savunmadan Kaçınma (Defense Evasion) |  | T1202 |
| Savunmadan Kaçınma (Defense Evasion) | Match Legitimate Name or Location | T1036.005 |
| Etki ve Çıkış (Impact & Exfiltration) | Exfiltration Over Web Service | T1567.002 |
| Etki ve Çıkış (Impact & Exfiltration) | Data Encrypted for Impact | T1486 |

**“Pyramid of Pain” Nedir ve Neden Önemlidir?**

Siber güvenlik dünyasında savunma mekanizmaları geliştikçe, saldırganlar da daha sofistike hale geliyor. Bu durumda tehditleri tespit etmek ve saldırganları durdurmak için etkili bir stratejiye sahip olmak kritik hale geliyor. “Pyramid of Pain” (Acı Piramidi) modeli, tehdit istihbaratı alanında güvenlik uzmanlarına rehberlik eden önemli bir araçtır. David J. Bianco tarafından geliştirilen bu model, saldırganların davranışlarını izlemek ve onlara karşı stratejik adımlar atmak için kullanılıyor.

Siber güvenlik dünyasında “Pyramid of Pain” modeli, Cyber Kill Chain modeline benzer bir yaklaşımla tehditlerin tespit edilmesine ve saldırganların faaliyetlerinin engellenmesine odaklanır. Ancak temel fark şudur ki, Cyber Kill Chain daha çok saldırganların adımlarını tanımlayan bir modelken, Pyramid of Pain özellikle Blue Team (savunma ekipleri) için bir rehberdir. Blue Team, saldırılara karşı koyma stratejileri geliştirirken, bu model üzerinden saldırganın operasyonlarını ne kadar zorlaştırabileceklerine odaklanır.

Pyramid of Pain Nedir?

“Pyramid of Pain”, bir siber saldırganın operasyonel etkinliğini sekteye uğratmak için farklı tehdit göstergelerini (IOC – Indicators of Compromise) kullanır. Piramidin her katmanı, saldırgana ne kadar “acı” vereceğinizi ve onların faaliyetlerini ne derece zorlaştıracağınızı gösterir. 

**Piramidin Katmanları**

1. Hash Değerleri: Dosyaların dijital imzaları olan hash’ler, saldırganların değiştirmesi oldukça kolay olan göstergelerdir. Bu yüzden saldırganı ciddi şekilde zorlamaz.
2. IP Adresleri: Saldırganlar IP adreslerini kolayca değiştirebilir, bu da onları engellemenin nispeten az etki yaratacağı anlamına gelir.
3. Domain İsimleri: Domain isimlerini engellemek, saldırganın yeni bir domain oluşturmasını gerektirir. Bu, onlara biraz daha maliyet ve zorluk çıkarır.
4. Network Artifacts: Saldırganın ağda bıraktığı izler veya yapılandırmalar daha özeldir ve değiştirilmesi daha zordur. Bu seviyede bir müdahale, saldırganı daha fazla zorlar.
5. Host Artifacts: Hedef cihazda bırakılan izler veya dosyalar. Bunları değiştirmek, saldırganın sistemdeki erişimini yeniden yapılandırmasını gerektirir.
6. Tools: Saldırganların kullandığı araçları engellemek, operasyonlarını ciddi anlamda zorlaştırır. Çünkü yeni araçlar bulmak veya mevcut araçları değiştirmek zaman alıcıdır.
7. Tactics, Techniques, and Procedures (TTPs): Piramidin en üstünde yer alan TTP’ler, saldırganın genel stratejileridir. Bu seviyede yapılan müdahale, saldırganın tüm operasyon tarzını değiştirmesini gerektirir ve ona en fazla acıyı verir.

Neden Önemlidir?

“Pyramid of Pain” modeli, siber güvenlik savunucularının (Blue Team) tehditleri sadece tespit etmekle kalmayıp, saldırganların taktik ve yöntemlerini değiştirmeye zorlayacak stratejiler geliştirmesini sağlar. Bu da siber saldırganlar için maliyeti ve zorluğu artırır, başarılı bir savunma stratejisi oluşturmak için önemli bir yapı taşıdır.

Bu modelle, saldırganları ne kadar zorlayabileceğinizi ve hangi noktada en çok “acı” verebileceğinizi anlamak, güçlü bir savunma inşa etmek için kritik önem taşır.

**KAYNAKÇA**

[**https://cybershieldcommunity.com/**](https://cybershieldcommunity.com/)

[**https://www.splunk.com/**](https://www.splunk.com/)

[**https://www.paloaltonetworks.com/**](https://www.paloaltonetworks.com/)

[**https://infosecwriteups.com/**](https://infosecwriteups.com/)

[**https://cyberartspro.com/**](https://cyberartspro.com/)

