PYRAMID OF PAIN

HAZIRLAYAN: UMUT EMRE KARACAER
TARİH: 17.02.2025

İÇERİK:

GİRİŞ:

Siber güvenlik dünyası, sürekli olarak gelişen tehditlerle başa çıkmak için dinamik bir yaklaşım gerektiren bir alan olarak öne çıkmaktadır. Saldırganlar yeni teknikler geliştirirken, savunma ekipleri de bu tehditlere karşı etkili stratejiler oluşturmak zorundadır. Geleneksel tehdit tespit yöntemleri genellikle belirli göstergeler üzerine yoğunlaşsa da, bunların tespit edilmesi ve engellenmesi her zaman saldırganların faaliyetlerini sonlandırmak için yeterli olmayabilir.

Bu noktada, **David J. Bianco** tarafından geliştirilen **Pyramid of Pain** modeli devreye girerek, siber tehditleri engelleme konusunda daha derin bir anlayış sunmaktadır. Bu model, tehdit göstergelerini farklı seviyelere ayırarak, savunma ekiplerinin sadece tespit etmekle kalmayıp, saldırganların operasyonel etkinliğini en can sıkıcı şekilde azaltmalarını hedefler.

Bu rapor, Pyramid of Pain modelini detaylı bir şekilde inceleyerek, her seviyedeki tehdit göstergelerinin savunma stratejileri açısından nasıl ele alınması gerektiğini açıklamaktadır.

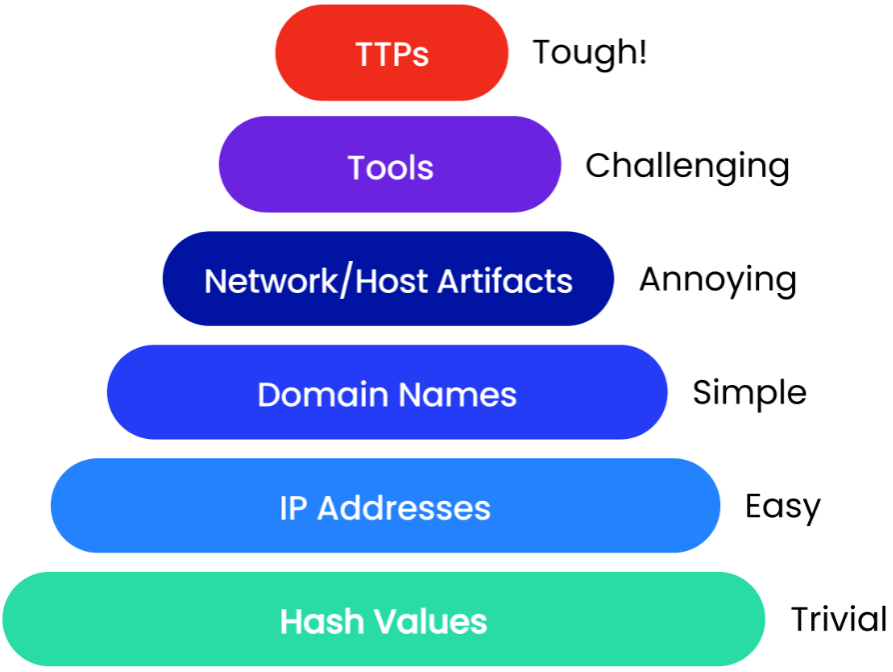
PYRAMID OF PAIN NEDİR?:

Siber güvenlikte saldırganlar ve savunmacılar arasındaki mücadele, sürekli gelişen bir satranç oyunu gibidir. Güvenlik önlemleri güçlendikçe, saldırganlar da yeni yöntemler geliştirerek bu engelleri aşmaya çalışır. İşte tam bu noktada **Pyramid of Pain** devreye girer.

David J. Bianco tarafından ortaya konan bu model, siber tehditleri yalnızca tespit etmekle kalmayıp, saldırganları gerçekten zor duruma sokacak stratejiler geliştirmeye odaklanır. **Pyramid of Pain**, tehdit göstergelerini **(IoC - Indicators of Compromise)** katmanlara ayırarak, saldırganların operasyonlarını ne ölçüde sekteye uğratabileceğimizi anlamamıza yardımcı olur. Piramidin alt seviyelerinde yer alan göstergeleri engellemek saldırgan için küçük bir rahatsızlık yaratırken, üst seviyelere doğru çıkıldıkça tehdit aktörünün gerçekten **"acı"** çekmesine neden olacak engeller koymak mümkündür.

Bu modelin en önemli özelliği, savunma ekiplerinin **(Blue Team)** saldırılara pasif bir şekilde tepki vermek yerine, saldırganları caydıracak ve onların işlerini zorlaştıracak adımlar atmalarını sağlamasıdır. Cyber Kill Chain modeline benzer bir mantıkla çalışsa da, **Pyramid of Pain** doğrudan saldırganın hareket alanını kısıtlamaya odaklanır.

Sonuç olarak, **Pyramid of Pain** güvenlik ekiplerine sadece saldırıları tespit etmekle yetinmemeleri gerektiğini, aynı zamanda saldırganların motivasyonlarını kırarak onları etkisiz hale getirmenin yollarını aramaları gerektiğini hatırlatan güçlü bir yaklaşımdır.



NEDEN ÖNEMLİDİR?:

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.

PİRAMİDİN KATMANLARI:

Seviye 1: Hash Değerleri (Hash Values) – Önemsiz (Trivial):

Kötü amaçlı yazılım dosyalarının veya saldırı araçlarının hash değerleri tespit edilip paylaşıldığında, saldırganlar açısından değiştirilmesi oldukça kolaydır. Bunun sebebi, hash değerlerinin son derece hassas olmasıdır yani en ufak bir değişiklik bile tamamen farklı bir hash değeri üretir.

Örneğin, bir programın koduna boşluk eklemek veya bir satır ekleyip çıkarmak bile hash değerinin tamamen değişmesine neden olur. Bu yüzden, saldırganlar hash tabanlı tespit sistemlerini kolayca atlatabilir.

```
SHA3-256(1111111111111111111111111111111111111111) =
bf8d60cfc6654a2cd4dbf63e5a85cf8c34674c3f41f1bf38312ce88012536d69

SHA3-256(1111111111111111111111111111111111111110) =
b45d95d47b00d9fcdb9af0437bbaa5101a51f55ebcc2163bb731cee7761d6d80
```

SHA3-256 hash fonksiyonu kullanılarak yapılan bir test, yalnızca bir bitlik değişikliğin bile tamamen farklı bir hash ürettiğini göstermektedir. Bu, kriptografik hash fonksiyonlarının belirleyici (deterministik) ancak son derece hassas olduğunu kanıtlar.

Seviye 2: IP Adresleri (IP Addresses) – Kolay (Easy):

Saldırganlar için IP adreslerini değiştirmek oldukça kolaydır çünkü çeşitli araçlar ve teknikler sayesinde gerçek IP adreslerini gizleyebilirler.

Kullanılan yöntemler:

- **Proxy sunucuları ve VPN'ler:** Gerçek IP adresini maskeleyerek farklı bir konumdan bağlanıyormuş gibi görünmesini sağlar.
- **Dinamik IP adresleri:** İnternet Servis Sağlayıcıları (ISP'ler) tarafından atanan IP adresleri sık sık değişebilir.
- **Tor ağı:** Trafiği birçok farklı sunucu üzerinden yönlendirerek orijinal IP adresini gizler.
- **Zombi bilgisayarlar (botnetler):** Saldırganlar, saldırılarını ele geçirilmiş makineler üzerinden gerçekleştirerek gerçek IP adreslerini saklar.

Bu nedenle, dinamik ve anonimleştirici IP kullanımına dayalı bir saldırı modeline karşı savunma yapmak yerine, daha kalıcı ve geniş kapsamlı güvenlik önlemleri almak gerekmektedir.

Seviye 3: Alan Adları (Domain Names) – Basit (Simple):

Alan adlarını engellemek, saldırganın yeni bir domain oluşturmasını gerektirir. Alan adlarını değiştirmek oldukça basittir çünkü yeni bir alan adı kaydetmek kolay ve ucuzdur.

- Eğer bir alan adı kara listeye alınır veya yetkililer tarafından kapatılırsa, saldırganlar yeni bir alan adı alarak saldırılarına devam edebilir.
- Bazı saldırganlar, meşru hizmetleri (örn. e-posta sağlayıcılarını) kötüye kullanarak tespit edilmekten kaçınır.

Seviye 4: Ağ/Host İzleri (Network/Host Artifacts) – Can Sıkıcı (Annoying):

Ağ ve ana bilgisayar seviyesindeki izler (artifacts) saldırganlar için can sıkıcıdır çünkü bunları değiştirmek veya gizlemek daha zordur. Bu izler, kötü amaçlı etkinlikleri tespit etmek için kullanılan ayırt edici unsurlardır ve şunları içerebilir:

- URL kalıpları
- Sistem günlükleri (log mesajları)
- Komuta ve Kontrol (C2) bilgileri
- Kayıt defteri (Registry) anahtarları
- Dosya ve klasör izleri

Bu izleri takip ederek saldırıları tespit etmek mümkündür, ancak saldırganlar da bu izleri gizlemek veya değiştirmek için çeşitli teknikler kullanabilirler.

Seviye 5: Araçlar (Tools) – Zor (Challenging):

Saldırganların hedeflerine ulaşmak için kullandıkları yazılımlardır. Buna, hedefli oltalama (spear phishing) için kötü amaçlı belgeler oluşturmak amacıyla tasarlanmış araçlar, Komuta ve Kontrol (C2) bağlantısı kurmak için kullanılan arka kapılar (backdoors), parola kırıcılar veya diğer ana bilgisayar tabanlı araçlar dahildir. Savunma ekipleri, saldırganların araçlarını hedef alarak büyük bir caydırıcılık sağlayabilirler. Saldırganlar için yeni saldırı araçları oluşturmak veya mevcut olanları değiştirmek zordur çünkü:

- Gelişmiş bilgi ve beceri gerektirir.
- Ciddi zaman ve kaynak harcamalarını gerektirir.
- Saldırı aracının etkin ve tespit edilemez kalmasını sağlamak zordur.

Seviye 6: Taktikler, Teknikler ve Prosedürler (TTP) – Çok Zor (Tough!):

Piramidin en üstünde yer alan TTP'ler, saldırganların kapsamlı saldırı stratejilerini içerir. Tehdit Avcılığı açısından bakıldığı zaman en güvenilir veriler TTP'lerdir. Bu seviyede yapılan müdahale, saldırganın tüm operasyon tarzını değiştirmesini gerektirir ve ona en fazla acıyı verir çünkü bir saldırı grubunun TTP'sinin çıkartılması saldırı grubunu yakalanma şansını arttırmaktadır.

- Saldırı yaşam döngüsünün tüm aşamalarını kapsar.
- Değiştirilmesi son derece zor ve zahmetlidir.
- Savunma ekipleri için en güçlü saldırı tespit noktalarından biridir.

TTP'leri değiştirmek saldırganlar için oldukça maliyetlidir, bu nedenle savunma ekipleri TTP odaklı algılama mekanizmaları geliştirmelidir.

SONUÇ:

Pyramid of Pain modeli, siber güvenlik dünyasında saldırganları gerçekten zor duruma sokmak ve onların hareket alanlarını kısıtlamak için güçlü bir çerçeve sunar. Geleneksel tehdit istihbaratı yaklaşımlarından farklı olarak, yalnızca saldırıları tespit etmek yerine saldırganların taktik, teknik ve prosedürlerini (TTP) değiştirmeye zorlayarak savunma mekanizmalarını daha etkili hale getirmeyi amaçlar.

Piramidin alt seviyelerinde yer alan IoC'lerin (Hash değerleri, IP adresleri, Alan adları) engellenmesi, saldırganlar açısından kolayca aşılabilecek engeller oluştururken, üst seviyelerdeki unsurları hedef almak (Araçlar ve TTP'ler) saldırganlar için büyük maliyet ve zaman kaybına yol açar. Bu nedenle, güçlü bir siber savunma stratejisi geliştirmek isteyen güvenlik ekipleri, tehdit istihbaratı ve tehdit avcılığı süreçlerinde Pyramid of Pain modelini etkin bir şekilde kullanmalıdır.

Sonuç olarak, siber güvenlik savunucuları için saldırganları pasif bir şekilde izlemek yerine onların faaliyetlerini doğrudan zorlaştıran önlemler almak kritik öneme sahiptir. Pyramid of Pain, güvenlik ekiplerine saldırganları engellemek için daha stratejik bir bakış açısı sunarak siber tehditlerle mücadelede etkili bir araç olmayı sürdürmektedir.

KAYNAKÇA:

https://www.attackiq.com/glossary/pyramid-of-pain/
https://cybershieldcommunity.com/pyramid-of-pain/
https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain
https://www.kadircirik.com/cyber-threat-hunting-and-hunt-the-ioc/
https://cymulate.com/cybersecurity-glossary/pyramid-of-pain/
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html