Pyramid of Pain

Hazırlayan

Neslihan ASLAN

17/02/2025

İçindekiler

Giriş

Siber güvenlikte tehdit aktörlerini tespit etmek ve engellemek için çeşitli teknikler kullanılır. Bu süreçte, tehdit göstergeleri (IoC – Indicator of Compromise) saldırganların izlerini belirlemede önemli bir rol oynar ve tehdit istihbaratının kritik bir unsur olduğunu ortaya koyar.

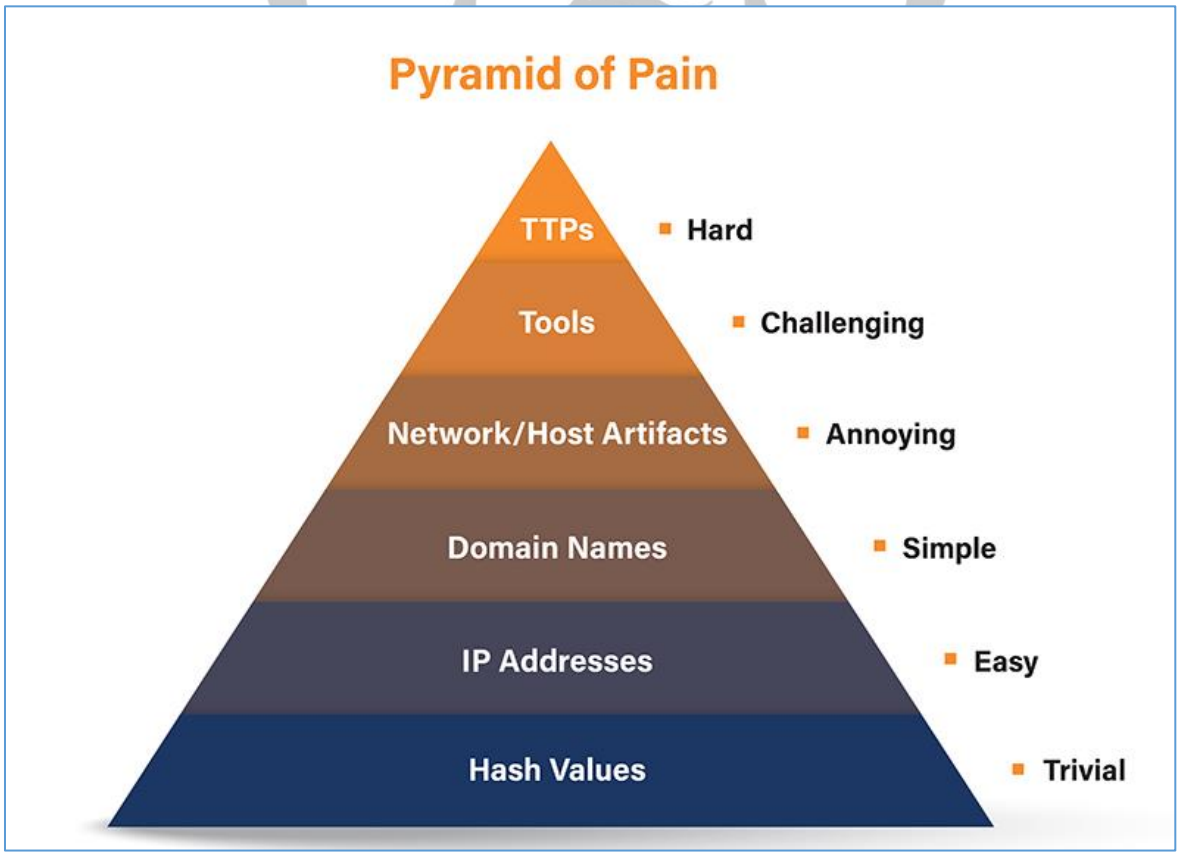
David Bianco tarafından geliştirilen Pyramid of Pain (Acı Piramidi) modeli, farklı IoC türlerinin saldırganlar üzerindeki etkisini açıklar. Bu model, tehdit göstergelerini seviyelere ayırarak her birinin saldırganlar için oluşturduğu zorluk derecesini gösterir.

Güvenlik ekipleri, bu piramit sayesinde hangi göstergelerin saldırganlar üzerinde daha büyük bir etkiye sahip olduğunu anlayarak daha stratejik güvenlik önlemleri alabilir. Böylece saldırılar daha etkili bir şekilde önlenebilir ve tehdit aktörlerinin hareket alanı kısıtlanabilir.

Pyramid of Pain Nedir?

Pyramid of Pain, siber tehditleri tespit etmek ve saldırganların faaliyetlerini zorlaştırmak amacıyla kullanılan bir modeldir. Bu model, farklı tehdit göstergelerini (IoC – Indicator of Compromise) altı seviyede sınıflandırarak, her seviyenin saldırganlar üzerindeki etkisini belirlermektedir. IoC, bir siber saldırının gerçekleştiğine dair geride kalan kanıt veya işarettir ve genellikle saldırının izlerini takip etmek ve kaynağını tespit etmek için kullanılmaktadır. Alt seviyelerde yer alan göstergeler, örneğin IP adresleri veya hash değerleri, hızlıca değiştirilebilirken, üst seviyelerde bulunan stratejik unsurlar daha zor değiştirilir ve saldırganlar üzerinde daha büyük bir etki yaratmaktadır. Stratejik unsurlar, saldırganların kullandığı taktikler, teknikler ve prosedürler (TTP'ler) gibi daha karmaşık göstergeleri ifade etmektedir. Bu göstergeler, saldırganların yöntemlerini değiştirmelerini gerektirir ve böylece bu durum onları daha fazla zorlamış olur.

Pyramid of Pain, güvenlik ekiplerine saldırıları daha etkili bir şekilde engelleme ve savunma stratejilerini geliştirme konusunda yol gösteren önemli bir yaklaşımdır.



Şekil 1 Pyramid Of Pain

Hash Değerleri

Dosya hash değerleri (MD5, SHA-1, SHA-256), saldırganlar tarafından kolayca değiştirilebilen göstergelerdir. Hash, bir veri kümesinin sabit uzunlukta ve genellikle benzersiz bir temsilidir. Verinin içeriğine göre oluşturulan bu değer, verinin, dosyanın "parmak izi" gibi düşünülebilir. Hash değeri, veri güvenliğinde sıklıkla kullanılır ve verilerin doğruluğunu, bütünlüğünü kontrol etmek için kullanılmaktadır.

Hash, belirli kötü amaçlı dosyalara benzersiz referanslar sağlamak için de kullanılır. Saldırganlar, dosya bütünlüğünü koruyarak hash değerlerini değiştirebilir, bu da tespit etme süreçlerini zorlaştırır. Ancak, hash değerleri tespit edilip engellendiğinde, saldırganlar tekrar bu tür değişiklikleri yapmak zorunda kalır ve bu da onlar için biraz zaman kaybı olur.

IP Adresleri

IP adresleri, saldırganların kolayca değiştirebileceği bir diğer göstergedir. Eğer bir IP adresi engellenirse, saldırganlar farklı bir IP adresi kullanarak devam edebilir. Ancak, sürekli olarak IP değiştirmek, saldırgan için pratikte bazı zorluklar yaratabilmektedir. Örneğin zamanla daha fazla kaynak tüketir ve etkisi olarak saldırganın operasyonel verimliliğini azaltır.

Domain Adları

Domain adları, saldırganlar tarafından kullanılarak zararlı aktiviteler gerçekleştirebilir. Engellenmiş bir domain adı, saldırganın yeni bir domain adresi bulmasını gerektirir, ancak bu işlem biraz daha fazla zaman ve kaynak harcayarak yapılır. Domainlerin değiştirilmesi, genellikle saldırganın operasyonel sürecinde bir kesintiye neden olur ve saldırganın izlerini gizleme çabalarını zorlaştırır**.**

Network/Host Artifacts

Bu katman, saldırganların kötü amaçlı yazılım faaliyetlerine dair belirli izleri içerir. Örneğin özel dosya yolları, kayıt defteri anahtarları veya ağ trafiği desenleri gibi göstergeler olabilir. Bu tür izler, genellikle saldırganın kullandığı zararlı yazılımlar veya sistemin kötüye kullanımına dair belirli izler bırakır. Bu göstergeleri tespit etmek, saldırganın saldırı planını bozarak engel olur, ancak bu tür izler de saldırgan tarafından değiştirilebilir.

Tools

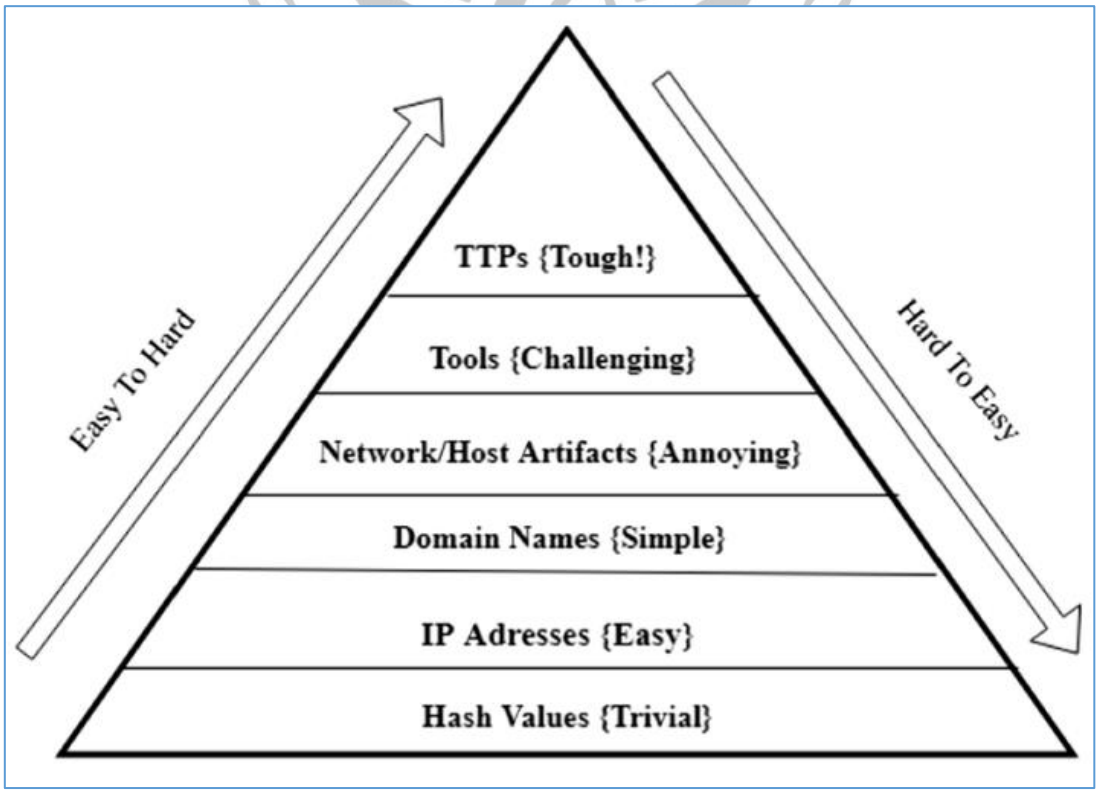
Saldırganların kullandığı araçlar (örneğin, Metasploit, Cobalt Strike) engellendiğinde, saldırganların alternatif araçlar araması gerekir. Bu tür araçlar, saldırıların uygulanmasında kritik bir rol oynar ve engellendiğinde saldırganlar yeni araçlar bulmak zorunda bırakır. Sonuçları arasında saldırganların operasyonlarını bir ölçüde aksaması ve sürekli bir araç değişimi yapmalarından kaynaklı olarak onlara zaman kaybettirir.

TTPs

Bu katman, saldırganların uyguladığı taktikler, teknikler ve prosedürleri (TTP'ler) ifade eder. TTP'ler, saldırganların saldırılarını gerçekleştirme yöntemlerini kapsar ve saldırganların en zor değiştirilebilen davranışlarıdır. Bu göstergeler engellendiğinde, saldırganların yeni yöntemler geliştirmesi gerekir. Bu ise, siber tehdit aktörleri için oldukça zor ve pyramid of pain modelinde en maliyetli bir süreçtir. Saldırganların TTP'lerini değiştirmeleri, onların stratejik yaklaşımlarını yeniden yapılandırmalarını gerektirir ve bu da onları önemli ölçüde zorlar.

Pyramid Of Pain Modelinde Aşağıdan Yukarıya Doğru;

Bu modele göre, piramidin alt katmanlarından üst katmanlarına doğru ilerledikçe, saldırganların göstergelerinde değişlik yapması maliyetini, zaman harcama süresini ve çabasını arttırır. Alt katmanlarda, hash değerleri veya IP adresleri gibi göstergeler kolayca değiştirilebilir olduğundan saldırganın düşük maliyetle hareket etmesine olanak tanır. Ama, piramidin üst katmanlarına çıkıldıkça, saldırganlar daha karmaşık stratejiler geliştirmek zorunda kalır ve bu çok daha fazla kaynak gerektirir. Taktik ve tekniklerin değiştirilmesi, saldırganın hedefi için planladığı operasyonları zorlaştırır ve değiştirmesi gereken göstergelerin zorluğuna bağlı olarak daha uzun süreli etkiler yaratır. Ayrıca, üst katmanlardaki göstergeler daha karmaşık olduğu için tespit edilmesi daha zor hale getirilir, çünkü saldırganlar bu düzeydeki değişikliklerle daha dikkatli ve gizli bir şekilde hareket ederler.



Şekil 2

Sonuç

Pyramid of Pain, tehdit istihbaratında saldırganları engellemenin ne kadar zor veya ne kadar kolay olacağını görselleştiren önemli bir modeldir. Özellikle üst seviyelerdeki göstergeleri hedef alarak yapılan savunma stratejileri ile saldırganları daha fazla zorlayarak tehditlere karşı daha güçlü bir koruma sağlanabilir. Bu model rehberliğinde hareket edilerek, saldırganların operasyonel süreçlerini aksatılaabilir ve tehdit aktörlerine daha büyük zararlar verilebilir. Dolayısıyla bu yaklaşım, saldırı vektörlerini anlamayı, daha derinlemesine analiz yapmayı ve olay müdahale süreçlerini iyileştirmeyi mümkün kılmaktadır. Aynı zamanda, sürekli gelişen tehdit ortamına uyum sağlamak için proaktif savunma stratejileri geliştirilmesine de olanak tanır. Bu nedenle, Pyramid of Pain modeli sadece mevcut tehditleri engellemekle kalmaz, aynı zamanda gelecekteki saldırılara karşı organizasyonel dayanıklılığı da artırır.

Kaynakça

1. **https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain**
2. **https://cybershieldcommunity.com/pyramid-of-pain/**
3. **https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/pyramid-pain-threat-detection/**
4. **https://www.netsurion.com/articles/the-pyramid-of-pain**
5. **https://www.selimozis.com/taktikler-ve-teknikler/**
6. **https://www.researchgate.net/figure/Pyramid-of-pain-Adapted-from-5_fig1_338735931**