PYRAMID OF PAIN

Hazırlayan: Halil İbrahim KORKUDAN

Tarih: 17.02.2025

Giriş

Siber tehditler giderek daha karmaşık hale gelmekte ve saldırganlar sürekli olarak yeni yöntemler geliştirmektedir. Siber güvenlik uzmanlarının bu tehditlere karşı proaktif stratejiler geliştirmesi kritik bir öneme sahiptir. "Pyramid of Pain" (Acı Piramidi) modeli, siber tehdit istihbaratında etkin bir şekilde kullanılabilecek bir çerçeve sunmaktadır. David J. Bianco tarafından geliştirilen bu model, saldırganların operasyonlarını sürdürebilmek için bağımlı oldukları göstergeleri (IoC'ler) analiz ederek, savunma ekiplerinin saldırganları en çok zorlayabilecek noktaları belirlemelerine yardımcı olur.

Pyramid of Pain Nedir?

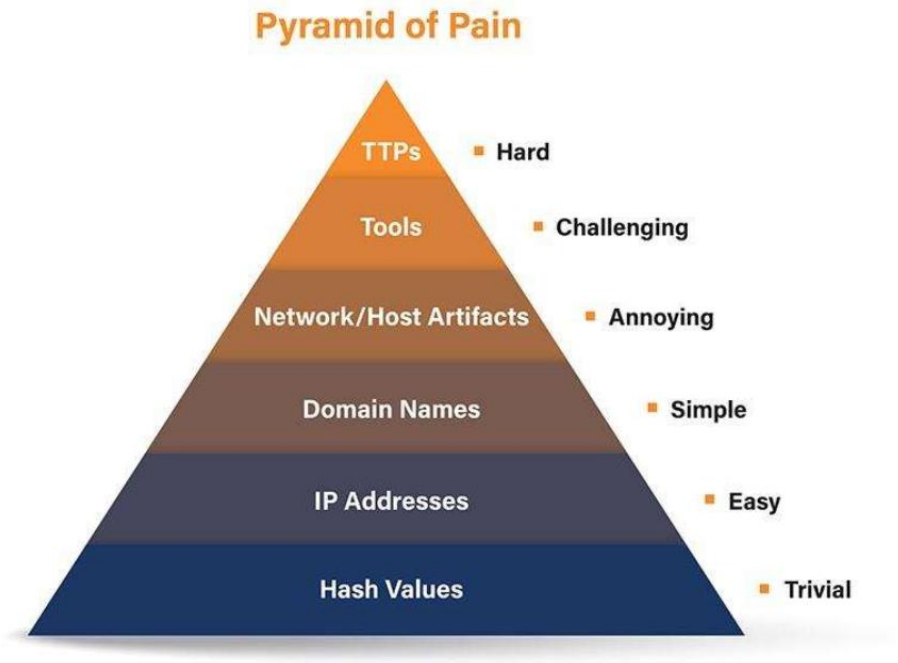
Pyramid of Pain, siber tehdit istihbaratında tehdit göstergelerini (IoC) sınıflandıran bir modeldir. Bu model, saldırganların operasyonlarını sürdürebilmeleri için gerekli olan unsurları analiz eder ve güvenlik ekiplerinin bu unsurları hedef alarak saldırganları etkisiz hale getirmelerini sağlar. Model, tehdit göstergelerini saldırganlar tarafından değiştirilme zorluklarına göre altı farklı seviyede kategorize eder. Bu kategorilendirme, siber güvenlik uzmanlarının hangi IoC seviyesine odaklanarak en büyük etkiyi yaratabileceğini anlamalarına yardımcı olur. Modelin temel amacı, saldırganların operasyonel süreçlerini bozarak onları daha maliyetli ve zorlayıcı değişiklikler yapmaya zorlamaktır.

Pyramid of Pain ve Tehdit Göstergeleri

Acı Piramidi modeli, tehdit göstergelerini (IoC) altı seviyede sınıflandırır:

1. Hash Değerleri
2. IP Adresleri
3. Alan Adları
4. Ağ/Sunucu Artifaktları
5. Araçlar
6. Taktikler, Teknikler ve Prosedürler (TTP)

Bu seviyeler, saldırganların operasyonlarına olan etkileri ve bu göstergelerin değiştirilme zorluklarına göre sıralanmıştır. Model, alt seviyedeki IoC'lerin tespit edilmesinin kolay ancak saldırganlar üzerinde düşük etkiye sahip olduğunu, üst seviyedeki IoC'lerin ise tespit edilmesinin zor ancak saldırganlar için büyük operasyonel maliyet yarattığını vurgular.



Piramidin Seviyeleri ve Etkileri

1. Hash Değerleri

Hash değerleri, bir dosyanın veya verinin benzersiz dijital imzasıdır. Antivirüs yazılımları ve tehdit istihbarat sistemleri, kötü amaçlı yazılımları tespit etmek için genellikle hash değerlerini kullanır. Ancak, saldırganlar bir dosyanın küçük bir bölümünü değiştirerek hash değerini tamamen değiştirebilirler. Bu yüzden, hash tabanlı tespit mekanizmaları genellikle statik ve değiştirilemeyen tehditler için etkilidir.

2. IP Adresleri

IP adresleri, saldırganların ağ üzerindeki varlıklarını tespit etmek için önemli göstergelerdir. Kötü amaçlı trafik analiz edilirken IP adreslerinin engellenmesi, saldırganların belirli kaynaklara erişimini kesebilir. Ancak, VPN, Tor ağı ve dinamik IP kullanımı ile saldırganlar IP adreslerini değiştirebilirler. Bu nedenle, tek başına IP engelleme yöntemi sınırlı bir savunma sağlar.

3. Alan Adları

Saldırganlar, komuta ve kontrol (C2) sunucuları, oltalama saldırıları veya kötü amaçlı yazılım yaymak için belirli alan adları kullanabilirler. Alan adlarının tespit edilerek engellenmesi, saldırganları yeni alan adları kaydetmeye zorlar ve operasyonel maliyetlerini artırır. Ancak, alan adı üretim algoritmaları (DGA) gibi tekniklerle saldırganlar sürekli olarak yeni alan adları oluşturabilirler.

4. Ağ/Sunucu Artifaktları

Bu seviye, saldırganların ağ üzerinde bıraktığı izleri ve belirli yapılandırma değişikliklerini içerir. IDS/IPS sistemleri, bu tür anormallikleri tespit edebilir ve saldırganların erişimini kesebilir. Artifaktların değiştirilmesi saldırganlar için daha karmaşıktır çünkü operasyonel süreçlerini önemli ölçüde değiştirmeleri gerekir.

5. Araçlar

Saldırganlar, saldırılarını gerçekleştirmek için belirli yazılımlar ve araçlar kullanırlar. Bunlar uzaktan erişim araçları (RAT), exploit kitleri veya zararlı yazılım framework'leri olabilir. Eğer savunma ekipleri bu araçları tespit edip etkisiz hale getirirse, saldırganların yeni araçlar geliştirmesi veya mevcut araçlarını değiştirmesi gerekecektir. Bu, onların operasyonel verimliliğini ciddi şekilde sekteye uğratır.

6. Taktikler, Teknikler ve Prosedürler (TTP)

Piramidin en üst seviyesinde bulunan TTP'ler, saldırganların operasyonel stratejilerini ifade eder. Bu seviyede bir IoC tespit edildiğinde, saldırganların saldırı yöntemlerini değiştirmeleri gerekir. TTP'leri analiz etmek, saldırganların alışkanlıklarını anlamaya ve onları daha etkili bir şekilde engellemeye yardımcı olur. MITRE ATT&CK gibi framework'ler, TTP'lerin tanımlanması için kullanılabilir. Bu seviyede yapılan tespitler, saldırganların operasyonel süreçlerini tamamen bozabilir.

Sonuç: Pyramid of Pain Modelinin Önemi

Pyramid of Pain modeli, siber güvenlik operasyon merkezleri (SOC) ve tehdit istihbarat ekipleri için kritik bir yol haritası sunmaktadır. Güvenlik ekipleri, IoC'leri yalnızca tespit etmekle kalmayıp, saldırganları operasyonel olarak zorlayacak önlemler geliştirmelidir. Özellikle TTP seviyesinde yapılan analizler, saldırganların stratejik hamlelerini değiştirmelerini zorunlu kılar ve saldırıların önlenmesinde en etkili yöntemlerden biri olur.

Bu model, güvenlik ekiplerinin tehditleri yönetme ve önleme süreçlerini optimize etmelerine yardımcı olurken, saldırganların faaliyetlerini daha maliyetli ve zor hale getirmek için stratejik bir yaklaşım sunmaktadır.

Kaynakça

https://www.gaissecurity.com/blog/aci-piramidi-siber-tehdit-istihbaratinda-analitik-bir-model

https://cybershieldcommunity.com/pyramid-of-pain/

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

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

https://medium.com/@AbhijeetSingh4/pyramid-of-pain-soc-level-1-tryhackme-walkthrough-15ea4a09b901