Pyramid of Pain

Hazırlayan: Saliha Polat

Tarih: 17.02.2025

İçindekiler

Giriş

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?

Acı Piramidi, David Bianco tarafından geliştirilen, siber güvenlik savunmaları bağlamında bir saldırganın tespit edilmekten kaçınmak ve saldırısına devam etmek için karşılaşacağı zorluk seviyelerini ve maliyeti gösteren kavramsal bir çerçevedir.

Pyramid of Pain (Acı Piramidi), siber saldırıların olası etkilerini hiyerarşik olarak sınıflandırarak, savunma kaynaklarının bu etkilere göre önceliklendirilmesine yardımcı olur.

Acı Piramidi, siber güvenlik düzeyinin beş seviyesini temsil eden bir modeldir. Acı Piramidi, en alt seviyede en temel güvenlik ihtiyaçlarını ve en üst seviyede daha sofistike güvenlik önlemlerini kapsar.

Piramidin alt seviyeleri, temel güvenlik adımlarını içerir. Bu seviyeler, ağa erişim kontrolü, güvenlik duvarları, antivirüs yazılımları, yama yönetimi ve güvenlik politikaları gibi önemli adımları içerir.

Orta seviyeler, ağ güvenliği için daha ileri düzey önlemleri içerir. Bu seviyeler, ağa saldırı tespit ve önleme, trafiği şifreleme, kimlik doğrulama ve yetkilendirme, güvenlik bilgisi ve olay yönetimi gibi çözümleri kapsar.

Piramidin üst seviyeleri, daha sofistike siber güvenlik önlemlerini içerir. Bu seviyeler, yapay zekâ ve makine öğrenimi ile güçlendirilmiş güvenlik, davranışsal analiz ve siber tehdit istihbaratı, uçtan uca şifreleme, güvenli yazılım geliştirme ve veri yönetimi ve güvenliği gibi daha gelişmiş çözümleri içerir.

Acı Piramidi, siber güvenlikte farkındalığı artırmak ve en uygun güvenlik önlemlerini almak için bir çerçeve sunar.

Pyramid of Pain Neden Önemlidir?

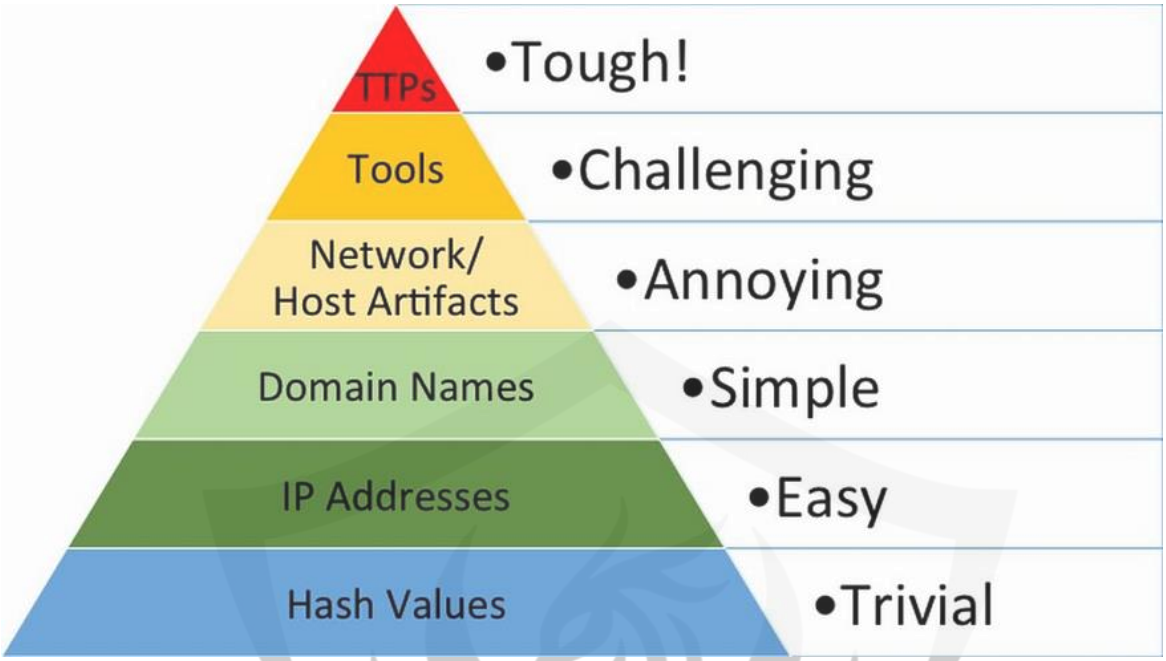
“Pyramid of Pain” modeli, siber güvenlik savunucularının (Blue Team) tehditleri sadece tespit etmekle kalmayıp, saldırganların taktik ve yöntemlerini değiştirmeye zorlayacak stratejiler geliştirmesini sağlar. Bu da siber saldırganlar için maliyeti ve zorluğu artırır, başarılı bir savunma stratejisi oluşturmak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

Acı piramidi modeli, tespit mühendislerinin, saldırganlara maksimum düzeyde zarar verebilecek, onları kötü niyetli faaliyetlerinde başarılı olmak için daha fazla zaman, çaba ve kaynak yatırmaya zorlayacak etkili savunma stratejileri ve analizlerini anlamaları ve geliştirmeleri için bir araç görevi görür.

Savunmacılar piramidin daha yüksek seviyelerine odaklanarak daha sağlam ve dayanıklı güvenlik duruşları oluşturabilir ve saldırganların tespit edilmeden hareket etmesini giderek daha da zorlaştırabilir.

Pyramid of Pain Katmanları



1) Hash Değerleri (Hash Values)

Saldırganın kullandığı zararlı örneklerine bakıldığı piramidin en altındaki seviyedir. Entegrasyonu yapılmış araçlarla MD5, SHA gibi şifrelenmiş verilerle zararlı hakkında referans sağlanır. Burada unutulmaması gereken zararlı yazılımın tek bir biti değiştirildiği takdirde bile şifre özeti değişecektir.

Dosyaların dijital imzaları olan hash'ler, saldırganların değiştirmesi oldukça kolay olan göstergelerdir. Bu yüzden saldırganı ciddi şekilde zorlamaz.

Hash değerlerini aramak için **virustotal** veya **OPSWAT** kullanılabilir.

2) IP Adresleri (IP Addresses)

Saldırganın Tor ya da anonim Proxy sağlayıcıları, VPN'nin kullanılmış olmasına özellikle dikkat edilir. Ayrıca arka planda Threat Intellengence bir yapı kullanılması kolaylık ve daha fazla bilgi içerektir.

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

3) Domain Adları (Domain Names)

Hedef sisteme bağlantı kuran domain adı veya subdomain'ler taranır. Domain adlarının nereden sağlandığına da bakılır. Ücretsiz ve güvensiz birçok alan adı sağlayıcısı mevcuttur. Bu sayede saldırgan domain adlarını IP adresleri kadar kolayca değiştirebilir.

Domain isimlerini engellemek, saldırganın yeni bir domain oluşturmasını gerektirir. Bu, onlara biraz daha maliyet ve zorluk çıkarır.

4) Ağ/Ana Bilgisayar Eserleri (Network/Host Artifacts)

Normal ilerleyen ağ hareketliliği, C&C protokollerini kullanılması, HTTP isteklerinde şüpheli hareketler aranır. Saldırganın normal görünen ağ davranışları araştırılır.

Host tarafında ise dosya izinleri ve erişimleri, registry değerleri, mutex verileri, bellek dizinlerindeki zararlı olabilecek aksiyonlar aranır.

Network Artifacts, saldırganın ağda bıraktığı izler veya yapılandırmalar daha özeldir ve değiştirilmesi daha zordur. Bu seviyede bir müdahale, saldırganı daha fazla zorlar.

Host Artifacts, hedef cihazda bırakılan izler veya dosyalar. Bunları değiştirmek, saldırganın sistemdeki erişimini yeniden yapılandırmasını gerektirir.

5) Araçlar (Tools)

Saldıran tarafın amacına ve hedefine yönelik kullandığı yazılımlar olarak tanımlayabiliriz. Saldırganın kendine özel kullandığı ya da hedeflediği sistemde bulunan araçlarda olabilir. Zararlı dokümanlar oluşturmak, arka kapı bırakmak için ya da parola kırmak için araçlar kullanılabilir. Hedeflenen sistemde bulunan yazılımlara TOR, GCC, Powershell, Windows Task Scheduler örnek verilebilir. Bunlar kötü amaçlı yazılımlar olmasa bile şüphe uyandırmayacağı anlamına gelmez.

Saldırganların kullandığı araçları engellemek, operasyonlarını ciddi anlamda zorlaştırır. Çünkü yeni araçlar bulmak veya mevcut araçları değiştirmek zaman alıcıdır.

6) TTP (Tactics, Techniques and Procedures)

Bu aşamaya saldırganın Cyber Kill Chain metodolojisi demek yanlış olmaz. Saldırganın hedeflediği sisteme keşiften sızmasına kadar her aşamasındaki yöntemleridir. Zararlı kodu enjekte ettiği pdf dosyası, phishing mailleri, ZIP biçimindeki zararlı kodlar vs. kullanan saldırganın her hareketi analiz edilir. MITRE ATT&CK framework'unu kullanmak bu aşamada elzem noktalardan biridir. Saldırganı tamamıyla tanıdığımız en ağrılı aşamadır.

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.

Sonuç

Pyramid of Pain, siber tehdit istihbaratında saldırganlarla mücadelede kritik bir çerçeve sunar. Bu model, tehdit aktörlerinin izlediği izleri ve güvenlik önlemlerine verdikleri tepkileri anlamamıza yardımcı olur. Hash değerleri, IP adresleri ve domain adları gibi düşük seviyeli göstergeler saldırganlar tarafından kolayca değiştirilebilirken, TTP'ler gibi daha üst seviyedeki göstergeleri tespit etmek ve engellemek saldırganlar için çok daha büyük bir maliyet oluşturur.

Bu nedenle, güvenlik ekipleri tehdit istihbaratını yalnızca yüzeysel göstergelerle sınırlamamalı, ağ ve ana bilgisayar eserleri, kullanılan araçlar ve saldırganların taktik, teknik ve prosedürlerini de analiz ederek daha kapsamlı bir savunma stratejisi geliştirmelidir. Pyramid of Pain yaklaşımı, siber tehditlere karşı proaktif bir savunma mekanizması oluşturmanın temel taşlarından biridir ve siber güvenlik uzmanları için vazgeçilmez bir rehber niteliği taşır.

Kaynakça

Medium - Software Development Turkey. *Ağrı Piramidi (Pyramid of Pain)*. Erişim Linki

Picus Security. *What is Pyramid of Pain?*. Erişim Linki

AttackIQ. *Pyramid of Pain*. Erişim Linki

S. Doğan Cesur - Medium. *Ağrı Piramidi (Pyramid of Pain) Nedir?*. Erişim Linki

Cyber Shield Community. *Pyramid of Pain*. Erişim Linki

EC-Council Cybersecurity Exchange. *Pyramid of Pain in Threat Detection*. Erişim Linki