Pyramid of Pain

Hilal ŞAHİN

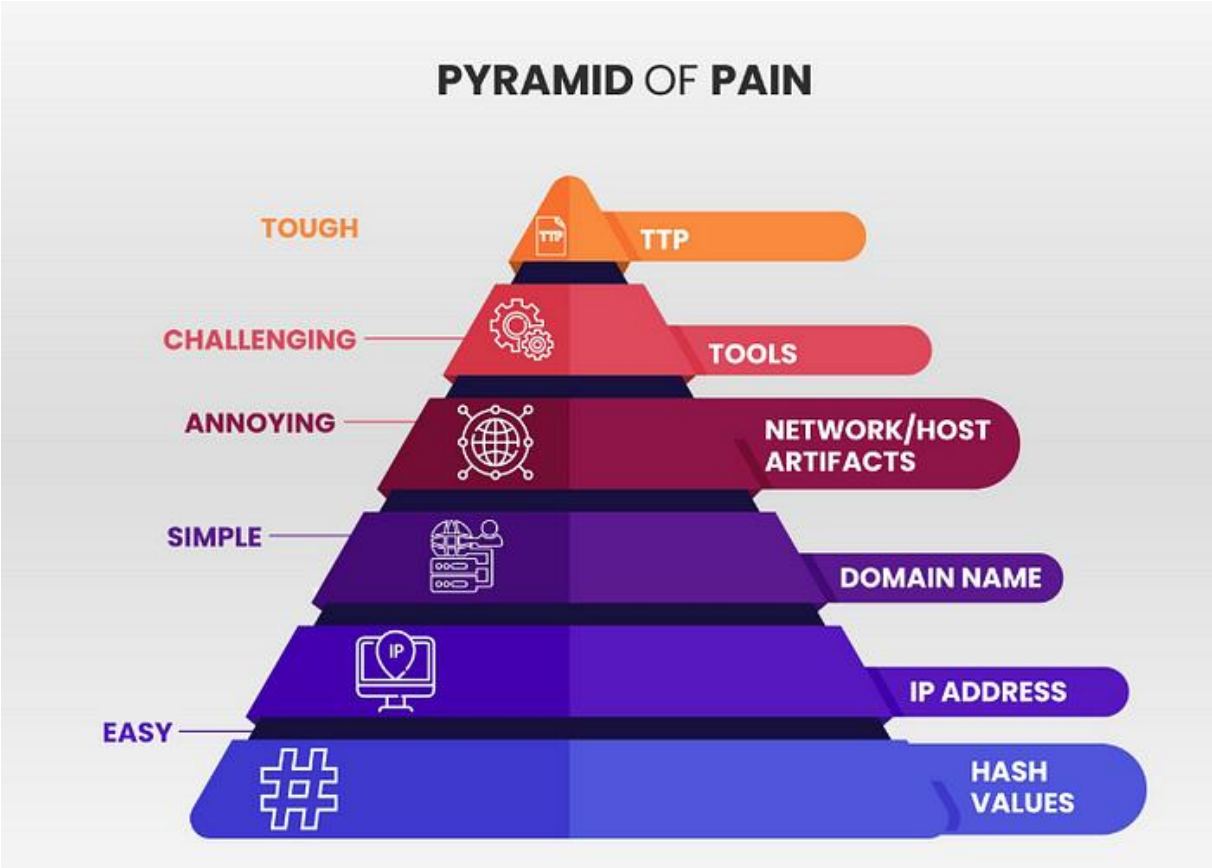
Şubat 2025

1. Giriş

Bu rapor, siber güvenlik alanında önemli bir yer tutan Pyramid of Pain modelini incelemeyi amaçlamaktadır. Pyramid of Pain, bir saldırganın siber güvenlik savunmalarına karşı vereceği tepkilerin zorluk seviyesini ve etkisini değerlendiren bir çerçeve sunar. Model, farklı tespit yöntemlerini beş ana katmanda sıralayarak, her katmanın savunma stratejilerine ne kadar "ağrı" yaratabileceğini gösterir. Raporda, bu modelin temel kavramları açıklanacak, her bir katman detaylı bir şekilde ele alınacak ve siber güvenlik alanında nasıl uygulanabileceği üzerinde durulacaktır. Amacımız, Pyramid of Pain'in siber güvenlik savunmalarındaki etkinliğini anlamak ve bu modelin nasıl daha etkili savunmalar oluşturulmasına yardımcı olabileceğini ortaya koymaktır.

2. 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.



Şekil 1: Pyramid of Pain

3. Piramidin Katmanları

3.1 Hash Değerleri: Saldırganın kullandığı zararlı örneklerine bakıldığı piramidin en altındaki seviyedir. Dosyaların dijital imzaları olan hash'ler, saldırganların değiştirmesi oldukça kolay olan göstergelerdir. Bu yüzden saldırganı ciddi şekilde zorlamaz. Zararlı yazılımın tek bir biti değiştirildiği takdirde bile şifre özeti değişecektir.

3.2 IP Adresleri: Saldırganlar IP adreslerini kolayca değiştirebilir, bu da onları engellemenin nispeten az etki yaratacağı anlamına gelir. Saldırganın Tor ya da anonim Proxy sağlayıcıları, VPN'nin kullanılmış olmasına özellikle dikkat edilir. Ayrıca arka planda Threat Intellengece bir yapı kullanılması kolaylık ve daha fazla bilgi içerektir.

3.3 Domain İsimleri: Hedef sisteme bağlantı kuran damain adı 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.

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

3.5 Host Artifacts: Hedef cihazda bırakılan izler veya dosyalar. Bunları değiştirmek, saldırganın sistemdeki erişimini yeniden yapılandırmasını gerektirir. Dosya izinleri ve erişimleri, registry değerleri, mutex verileri, bellek dizinlerindeki zararlı olabilecek aksiyonlar aranır.

3.6 Tools: Saldırgan tarafından amacına yönelik kullandığı yazılımlardır. Zararlı dokümanlar oluşturmak, arka kapı bırakmak için ya da parola kırmak için araçlar kullanılabilir.

3.7 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.

4. Sonuç

Pyramid of Pain modeli, siber güvenlik uzmanlarına, saldırganların savunmalarla karşılaştığında ne kadar "ağrı" hissedeceklerini ve bu ağrıyı artırarak savunmaların ne kadar etkili olabileceğini gösteren bir araçtır. Modellerin en alt katmanlarından en üst katmanlarına doğru ilerledikçe, savunmaların etkinliği artar ve saldırganların saldırılarını gizleme çabaları daha zorlu hale gelir. Bu model, siber güvenlik stratejilerini geliştirirken dikkate alınması gereken önemli bir çerçeve sunar.

Araştırmada Kazanılan Bilgiler:
Pyramid of Pain, bir saldırganın kullandığı tekniklerin tespit edilmesi ve engellenmesi sürecinde, savunma sistemlerinin nasıl daha etkili hale getirilebileceğine dair stratejik bilgiler sunar. Özellikle dosya davranışları ve özellikleri gibi üst katmanlarda yapılan analizler, savunmaların daha derinlemesine olmasını sağlar ve saldırganları sürekli yeni teknikler denemeye zorlar.

5. Kaynakça

https://cybershieldcommunity.com/pyramid-of-pain/#:~:text=%E2%80%9CPyramid%20of%20Pain%E2%80%9D%20(Ac%C4%B1,stratejik%20ad%C4%B1mlar%20atmak%20i%C3%A7in%20kullan%C4%B1l%C4%B1yor.

https://medium.com/@shunxianou/tryhackme-the-pyramid-of-pain-write-up-33e1494d353