PYRAMID OF PAIN

MURAT GÜRSOY

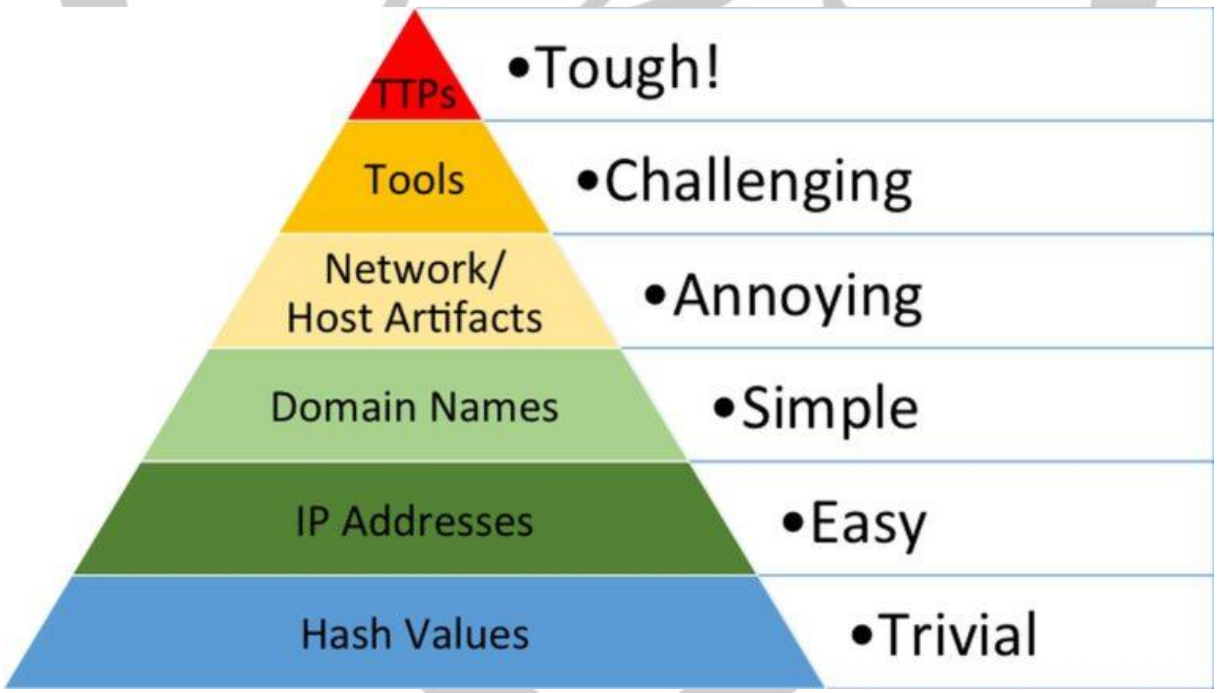
12/02/2025

İçindekiler

Giriş

David J. Bianco tarafından 2013 yılında geliştirilen **Pyramid of Pain** (Acı Piramidi) konsepti, saldırı göstergelerinin (Indicators of Compromise - IoC) etkinliğini değerlendirmek için kullanılan bir modeldir. Bu piramit, saldırganların faaliyetlerini sürdürebilmeleri için ne kadar çaba harcamaları gerektiğini gösterir. Piramidin alt seviyelerinde yer alan unsurlar kolayca değiştirilebilirken, üst seviyelere doğru çıkıldıkça saldırganlar için daha büyük bir zorluk oluşur. Bu model, siber tehdit istihbaratı ve saldırı tespit süreçlerinde önemli bir rol oynar.

Pyramid of Pain



Hash Values(Hash değerleri): Piramidin en alt seviyesinde bulunan hash değerleri, belirli bir dosyanın veya zararlı yazılımın benzersiz kimliğini tanımlamak için kullanılan sabit uzunluktaki dizilerdir. MD5, SHA-1 ve SHA-256 gibi hash algoritmaları, dosya bütünlüğünü doğrulamak için kullanılır. Ancak saldırganlar, zararlı yazılımların hash değerlerini kolayca değiştirebilirler. Örneğin, bir dosyanın içeriğinde küçük bir değişiklik bile hash değerini tamamen farklı hale getirebilir. Bu nedenle, yalnızca hash değerlerine güvenmek etkili bir tespit yöntemi değildir.

IP Addresses(IP adresleri): Saldırganın Tor ya da anonim Proxy sağlayıcıları, VPN'nin kullanılmış olmasına özellikle dikkat edilir. Ayrıca arka planda Threat Intelligence bir yapı kullanılması kolaylık ve daha fazla bilgi içerektir.

Domain Names(Alan Adları): Hedef sistemle bağlantı kuran domain adı veya subdomian'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.

Network/Host Artifacts(Ağ/Ana bilgisayar eserleri): Ağ ve ana bilgisayar seviyesinde tespit edilen zararlı aktiviteler, saldırganların sistemlerde bıraktığı izlerdir. Bunlar arasında şüpheli ağ bağlantıları, olağandışı HTTP istekleri, kayıt defteri değişiklikleri ve sistem dosyalarındaki anormallikler bulunur. Bu izler saldırganların faaliyetlerini ortaya çıkarmak için kullanılabilir. Ancak saldırganlar, ağ trafiklerini şifreleyerek veya sistem değişikliklerini gizleyerek bu tespit yöntemlerini aşmaya çalışırlar.

Tools(Araçlar): Saldırganın amacına ve hedefine yönelik kullandığı yazılımlar olarak tanımlayabiliriz. Saldırganın kendine özel kullandığı ya da hedeflediği sistemde bulunan araçlar da dahil edilebilir. 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

TTP(Teknik, Taktik, Prosedürler): Piramidin en üst seviyesinde yer alan **TTP'ler**, saldırganların kullandıkları yöntemlerin bütününü ifade eder. Bu aşamada saldırganların çalışma biçimi, saldırı süreçleri ve hedefe ulaşmak için izledikleri adımlar analiz edilir, bu aşamalarına bakılarak saldırganın Cyber Kill Chain metodolojisi de denebilir. MITRE ATT&CK çerçevesi, bu tür saldırı tekniklerini sınıflandırarak siber güvenlik uzmanlarına rehberlik eder. Saldırganların TTP seviyesinde analiz edilmesi, en etkili tespit ve savunma yöntemidir çünkü saldırganın davranışlarını değiştirmesi diğer seviyelere göre çok daha zordur.

Sonuç

Pyramid of Pain modeli, tehdit istihbaratı ve saldırı tespiti açısından önemli bir çerçeve sunar. Piramidin alt seviyelerinde bulunan göstergeler hızlıca değiştirilebilirken, üst seviyelere doğru ilerledikçe saldırganlar için değişim daha zor hale gelir. Bu nedenle, siber güvenlik uzmanlarının saldırganları TTP seviyesinde analiz ederek savunma mekanizmalarını buna göre oluşturması kritik öneme sahiptir. Bu yaklaşım, saldırganların etkinliğini azaltırken, savunma mekanizmalarının daha güçlü olmasını sağlar.

Kaynakça:

https://sdogancesur.medium.com/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-nedir-d20f3d86541e

https://hacktorx.com/the-pyramid-of-pain/