Pyramid of Pain

Hasan Karaca

15.02.2025

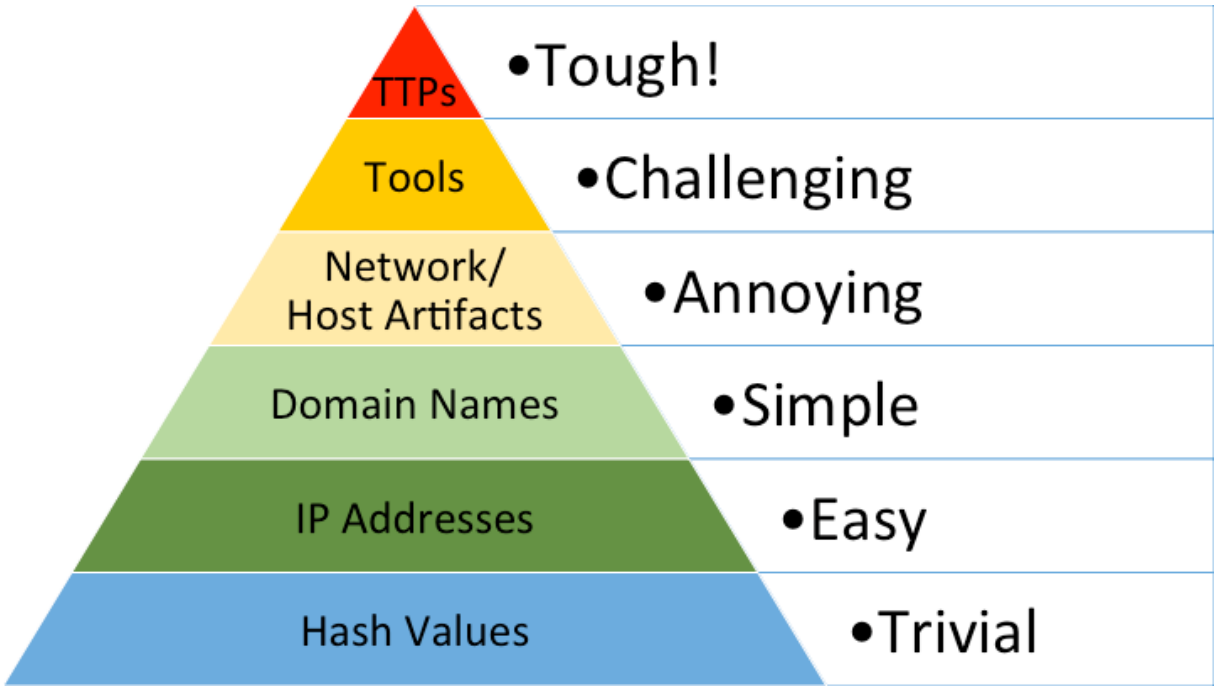
İÇİNDEKİLER

Pyramid of Pain Nedir

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.

Bu rapor, **Pyramid of Pain** modelinin temel bileşenlerini, işlevlerini ve organizasyonlar için önemini açıklamayı amaçlamaktadır

Pyramid of Pain Aşamaları



Hash Values(Hash değerleri):

Saldırganın kullandığı zararlı örneklerine bakıldığı piramidin en altındaki seviyedir. Entegre araçlarla MD5, SHA gibi şifrelenmiş veriler kullanılarak zararlı yazılımlar hakkında referans sağlanır. Hash algoritmaları, verilen girişin bir mesaj özeti (hash) hesaplayarak sabit uzunlukta bir hash değeri üretir ve bu değer tamamen girişe özgüdür. Örneğin, iki dosyanın içeriği bir bit kadar değişse bile, hash değerleri tamamen farklı olur. Bu, hash göstergelerinin doğru ve güvenilir olmasını sağlar. Ancak, dosyadaki herhangi bir küçük değişiklik bile hash değerinin tamamen farklı olmasına yol açar. Bu nedenle, hash değerlerinin sayısı çok fazla olduğu için bu değerleri takip etmek her zaman anlamlı olmayabilir.

IP Addresses(IP adresleri):

IP adresleri, kelimenin tam anlamıyla en temel gösterge türüdür. Yerel sabit diske kopyalanan veriler ve bir USB anahtarıyla kapıdan çıkartılmadığı sürece, bir saldırı gerçekleştirmek için neredeyse her zaman bir ağ bağlantısına ihtiyaç duyarsınız ve bu da IP adresleri anlamına gelir. Piramidin en geniş kısmında yer alırlar çünkü o kadar çok IP adresi vardır. İleri düzey bir saldırgan, IP adreslerini ihtiyaç duyduğu her an çok az çaba ile değiştirebilir. Bazı durumlarda, Tor gibi anonim proxy hizmetleri kullanıyorsa, IP adreslerini oldukça sık değiştirebilir ve bunun farkına bile varmaz ya da umursamazlar. Bu yüzden IP adresleri piramitte yeşil renkte gösterilir. Bir saldırgana bir IP adresinin kullanımını engellerseniz, genellikle adımlarını kesintiye uğratmadan hızla başka bir IP adresi ile devam edebilirler.

Domain Names(Domain Adları):

Piramidin bir üst seviyesinde, Domain Adları (hala yeşil ama daha açık tonlarda) bulunur. Bunları değiştirmek biraz daha zahmetlidir çünkü çalışabilmeleri için kaydedilmeleri, ödeme yapılmaları (çalıntı paralarla bile olsa) ve bir yerde barındırılmaları gerekir. Ancak, kaydetme standartları gevşek olan (birçoğu ücretsiz) birçok DNS sağlayıcısı bulunduğundan, pratikte domain değiştirmek çok da zor değildir. Yeni domainlerin ise İnternet genelinde görünmesi bir ila iki gün sürebilir, bu nedenle domainler, sadece IP adreslerinden biraz daha zor değiştirilir

Network/Host Artifacts(Ağ/Ana bilgisayar eserleri):

Piramidin tam ortasında ve sarı bölgeye girmeye başladığımızda, Ağ ve Ana Bilgisayar Artifaktları (Network and Host Artifacts) yer alır. Bu seviye, nihayetinde saldırgana olumsuz bir etki yaratmaya başladığınız seviyedir. Bu seviyedeki göstergeleri tespit edip yanıt verdiğinizde, saldırganın tekrar laboratuvarına dönüp araçlarını yeniden yapılandırması ve/veya yeniden derlemesi gerekir. Harika bir örnek, saldırganın HTTP keşif aracının, web içeriğinizi ararken belirgin bir User-Agent dizesi kullanmasıdır (örneğin, bir boşluk veya noktalı virgül farkı ile). Belki de sadece adını yazmıştır. Buna gülmeyin, çünkü böyle şeyler gerçekten oluyor! Eğer bu User-Agent ile yapılan talepleri engellerseniz, saldırgana a) keşif aracını nasıl tespit ettiğinizi ve b) bunu nasıl düzelteceğini düşünme zamanı tanımış olursunuz. Elbette, çözüm basit olabilir, ama en azından önlerine bir engel koyduğunuzda bunu tespit edip aşmak için bir çaba harcamak zorunda kalacaklardır.

Tools(Araçlar):

Bir sonraki seviye "Araçlar" (Tools) olarak etiketlenmiştir ve kesinlikle sarıdır. Bu seviyede, saldırganın ok çantasındaki bir veya daha fazla özel oku kullanma yeteneğini elinden alıyoruz. Bu genellikle, aracın artifaktlarını çok çeşitli yollarla tespit etme konusunda o kadar başarılı olduk ki, saldırgan vazgeçip aynı amaç için yeni bir araç bulmak veya oluşturmak zorunda kaldı. Bu senaryo sizin için büyük bir kazançtır çünkü saldırganın araştırma (mevcut bir aracı bulmak), geliştirme (yeni bir araç oluşturmak) ve eğitim (aracı nasıl kullanacağını öğrenmek ve buna hakim olmak) için zaman harcaması gerekir. Eğer bunu birden fazla aracına karşı yapabiliyorsanız, onlara gerçek zaman kaybettirdiniz demektir.

Araç göstergelerine örnekler arasında, aynı dosyaların modere değişikliklerle bile varyasyonlarını bulabilen AV veya Yara imzaları olabilir. Ayrıca, belirgin bir iletişim protokolüyle ağ odaklı araçlar da bu seviyeye girebilir; çünkü protokolü değiştirmek, orijinal aracı önemli ölçüde yeniden yazmayı gerektirir. Ayrıca, yukarıda tartışıldığı gibi, fuzzy hash'ler de büyük olasılıkla bu seviyeye girer.

TTP(Teknik, Taktik, Prosedürler):

Son olarak, zirvede TTP'ler (Tactics, Techniques, and Procedures) bulunur. Bu seviyede tespit ve yanıt verdiğinizde, doğrudan saldırganın davranışlarıyla ilgileniyorsunuz, araçlarıyla değil. Örneğin, saldırganların bu saldırıları gerçekleştirmek için kullandığı araçları değil, Pass-the-Hash saldırılarını kendilerini tespit ediyorsunuz (belki Windows günlüklerini inceleyerek). Saf verimlilik açısından, bu seviye ideal seviyenizdir. Eğer saldırganın TTP'lerine hızlı bir şekilde yanıt verebiliyorsanız, onlara mümkün olan en zaman alıcı şeyi yapmak zorunda bırakıyorsunuz

Pyramid of Pain Modelinin Güvenlik Ekiplerine Katkısı ve Önemi

Pyramid of Pain Modeli, güvenlik ekipleri için büyük bir öneme sahiptir çünkü saldırıların tespit edilmesinden müdahaleye kadar olan süreçlerde stratejik bir yaklaşım sunar. Bu model, saldırganların kullandığı göstergelere odaklanarak, savunma ekiplerine tehditlerin hangi seviyede olduğuna dair derinlemesine bir anlayış kazandırır. IP adresi ve domain gibi düşük seviyedeki göstergelerden, daha karmaşık ve zaman alıcı TTP'lere (Taktikler, Teknikler ve Prosedürler) kadar uzanan bu model, güvenlik ekiplerine saldırganların davranışlarını analiz etme ve müdahale etme imkânı sağlar. TTP'lere odaklanmak, saldırganların araçlarını değiştirmelerini gerektirecek kadar etkili bir savunma stratejisi sunar. Bu süreç, saldırganları yalnızca geçici çözüm arayışına yönlendirmekle kalmaz, aynı zamanda uzun vadede onlara zaman kaybettirir ve savunma stratejilerinin daha kalıcı hale gelmesini sağlar. Sonuç olarak, Pyramid of Pain Modeli, güvenlik ekiplerinin daha etkin, proaktif ve uzun vadeli çözümler geliştirmelerine katkı sağlar.

Rapor Kazanımları

Bu rapor, Pyramid of Pain modelinin siber güvenlikteki rolünü ve saldırı göstergelerinin tespit edilerek engellenme yöntemlerini açıklamaktadır. Modelin farklı seviyeleri incelenerek, IP adresleri, domain adları, ağ eserleri, kullanılan araçlar ve saldırganların teknik, taktik ve prosedürleri (TTP) gibi unsurların savunma stratejilerine etkisi değerlendirilmiştir. Güvenlik ekiplerinin tehditlere karşı daha etkili ve sistematik bir yaklaşım benimsemesi gerektiği ortaya konmuştur. Ayrıca, saldırganların araçlarını değiştirmelerini engellemek yerine doğrudan davranışlarına odaklanmanın, uzun vadede daha güçlü bir savunma sağladığı belirlenmiştir. Çalışma, siber güvenlikte tehdit tespiti ve müdahale yöntemleri konusunda kapsamlı bir analiz sunmaktadır.

Kaynakça

- https://cybershieldcommunity.com/pyramid-of-pain/
- https://sdogancesur.medium.com/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-nedir-d20f3d86541e
- https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html