ALTAY TAKIMI

PYRAMID OF PAIN RAPORU

HAZIRLAYAN:GÜRKAN PARLAK
17.02.2025

İçindekiler

Giriş

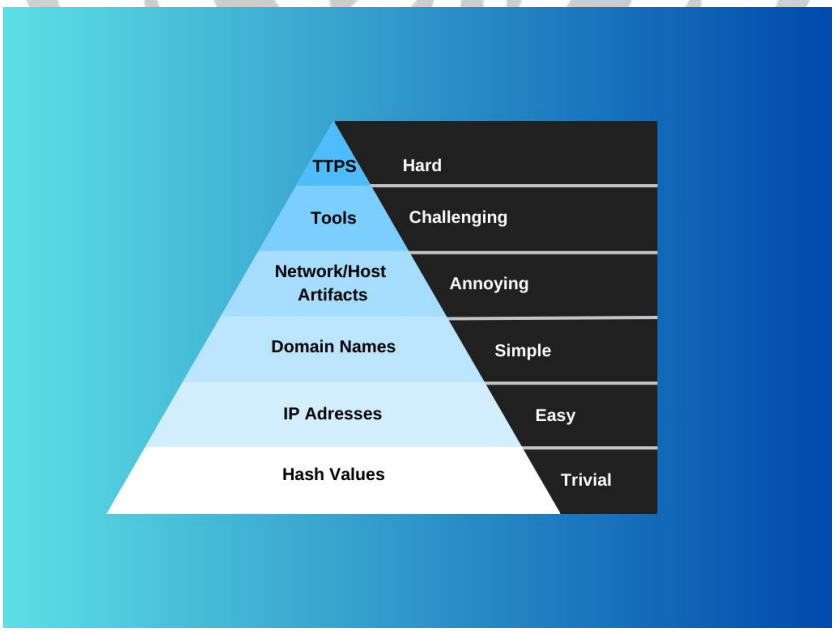
Bu rapor, siber güvenlikte tehdit avcılığı ve savunma stratejilerinin etkinliğini değerlendiren Pyramid of Pain modelini incelemeyi amaçlamaktadır.İlk olarak, Pyramid of Pain kavramı ve nasıl çalıştığı ele alınacak, ardından modelin farklı katmanları detaylandırılacaktır.

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.

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, 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.



Pyramid of Pain Nasıl Çalışır?

Acı Piramidi, kurumsal ağ savunucuları için değerli bir referans sağlar.
Örneğin, bir saldırgan saldırı zincirinde kötü amaçlı yazılım (malware) kullanarak bir uç noktayı enfekte ediyorsa, savunmacı yalnızca dosya hash değerleriyle bu davranışı tespit etmenin yeterli olmayacağını bilir. Bunun nedeni, saldırganların bu yöntemi kolayca atlatabilmesidir. Saldırganlar, kötü amaçlı yazılım örneğini yeniden derleyerek analistin kullandığı dosya hash değerini geçersiz hale getirebilir.

Bu nedenle, Acı Piramidi, saldırı göstergelerinin (Indicators of Compromise - IoC) önemini ve saldırganların hangi teknikleri daha zor veya kolay aşabileceğini vurgular.

Pyramid of Pain Katmanları

1-Hash Değerleri

Güvenlik analistleri, genellikle kötü amaçlı veya şüpheli bir dosyayı benzersiz şekilde tanımlamak ve incelemek amacıyla hash değerlerini kullanır. Hash değerleri, belirli bir kötü amaçlı yazılım örneği hakkında bilgi edinmek ve ilgili dosyaya referans vermek için önemli bir araçtır..

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.

Örnek: **e98a58a428cb48d5f220858678127e03** (MD5 Hash)

2-IP Adresleri

Bir ağa bağlı herhangi bir cihazı tanımlamak için IP adresi kullanılır. Savunma açısından, bir saldırganın kullandığı IP adreslerinin bilinmesi önemli bir avantaj sağlar. Yaygın bir savunma yöntemi, iç veya dış güvenlik duvarlarında belirli IP adreslerinden gelen istekleri engellemek, bırakmak veya reddetmektir. Ancak deneyimli bir saldırgan, yalnızca yeni bir genel IP adresi kullanarak bu önlemi kolayca aşabilir. Bu nedenle, bu tür bir savunma yöntemi tek başına yeterli değildir.

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-Domain Names

DNS adlarını değiştirmek, saldırganlar için genellikle daha zahmetlidir çünkü bir alan adı satın almayı, kaydetmeyi ve DNS kayıtlarını güncellemeyi gerektirir. Ancak savunucular açısından, birçok DNS sağlayıcısının gevşek güvenlik standartlarına sahip olması ve saldırganların API'ler aracılığıyla hızlı ve kolay bir şekilde alan adı değiştirmesine olanak tanıması önemli bir risk oluşturur.

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

4-Host/Networks Artifacts

Bu seviyede saldırıyı tespit edebilirseniz, saldırgan daha fazla rahatsızlık ve hayal kırıklığı yaşayacaktır. Tespitten kaçınmak için saldırganın araçlarını ve yöntemlerini değiştirmesi gerekecek, bu da ona hem zaman hem de ek kaynak maliyeti yaratacaktır.

Ana bilgisayar yapılandırmaları, kayıt defteri değerleri, şüpheli işlem yürütmeleri, saldırı kalıpları veya IoC'ler (Güvenlik İhlali Göstergeleri) gibi izler, saldırganların sistemde bıraktığı gözlemlenebilir belirtilerdir. Bunlar; kötü amaçlı yazılımlar tarafından bırakılan dosyalar veya mevcut tehdide özgü diğer davranışsal işaretler olabilir.

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.

5-Tools

Saldıran tarafın amacına ve hedefine(amaç ve hedef aynı şey değildir) 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

6-TTP(Teknik,Taktik,Prosedürler)

Bu aşamaya saldırganın Cyber Kill Chain metodolojisi demek yanlış olmaz kanımca. 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.

Sonuç

Pyramid of Pain saldırganların etkisini anlamak için önemli bir çerçevedir. Bu model basit teknik göstergelerden karmaşık atak vektörlerine kadar çeşitli seviyelerde bakış açısı sağlar.
Piramidin üst seviyelerine odaklanmak ve önlemler almak saldırganların başarısız olmasını arttırır. Ayrıca yöntemlerini değiştirmek zorunda kalan saldırganlar daha fazla zaman, çaba ve kaynak harcamaya zorlar. Bu nedenle, etkili bir tehdit avı (threat hunting) ve savunma stratejisi oluştururken, özellikle saldırganların taktik, teknik ve prosedürlerini (TTP) anlamak ve izlemek kritik öneme sahiptir.

Kaynaklar

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

https://www.attackiq.com/glossary/pyramid-of-pain/

https://medium.com/software-development-turkey/ağrı-piramidi-pyramid-of-pain-91554269b9b6

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

https://sdogancesur.medium.com/ağrı-piramidi-pyramid-of-pain-nedir-d20f3d86541e