Pyramid of Pain

Hazırlayan: Sinan Kocagöz

Tarih: 16.02.2025

İçindekiler Tablosu

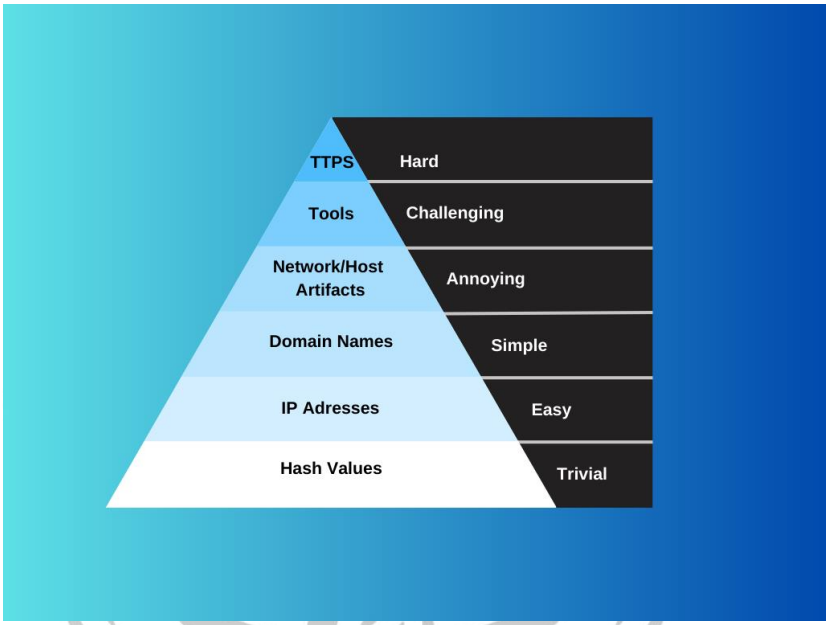
1. Giriş

Siber tehdit istihbaratı, saldırganların yöntemlerini anlamak ve savunma stratejileri geliştirmek için kritik bir rol oynar. David Bianco tarafından geliştirilen Pyramid of Pain (Acı Piramidi), tehdit aktörlerinin saldırı izlerini ve siber savunmaların bu izleri engelleme seviyelerini anlamamıza yardımcı olan bir modeldir. Bu piramit, saldırganların operasyonlarını sürdürebilmesi için ihtiyaç duyduğu göstergeleri (Indicators of Compromise - IoC) farklı seviyelerde sınıflandırır.

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.

2. Pyramid of Pain Nedir?

Bir piramit şeklinde yapılandırılmış olup, siber tehditlerle ilgili farklı göstergeleri ve nitelikleri kategorilere ayırır; bunlar, karma değerler, IP adresleri ve alan adları gibi en altta değişiklik yapılması gereken önemsiz şeylerden, Taktikler, MITRE teknikleri ve Prosedürler (TTP'ler) gibi en üstte değiştirilmesi en maliyetli ve karmaşık olanlara kadar uzanır (MITRE ATT&CK çerçevesinde ifade edildiği gibi).



"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.

3. Pyramid of Pain Katmanları

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

safe.exe	fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066
DefenderControl.exe	a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae
PRETTYOCEANApplicationdrs.bi	6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0
Setup.exe	510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1
WRSA.exe	ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d

Tek bir boşluğun veya tek bir kod satırının eklenmesi veya kaldırılması gibi ince bir değişiklik bile (programın işleyişine müdahale etmediği sürece) kötü amaçlı yazılımın karma değerini tamamen değiştirebilir. Bu özellik, karma değerlerini, göze çarpmayan ve altta yatan programın veya aracın işlevselliğini bozmayan değişikliklere karşı oldukça hassas hale getirir.

2. **IP Adresleri:** Proxy sunucuları ve VPN'ler gibi gerçek IP adreslerini maskeleyen ve kullanıcıların farklı yerlerden bağlanıyormuş gibi görünmesini sağlayan araç ve tekniklerin varlığı nedeniyle, saldırganların IP adreslerini değiştirmesi kolaydır, bu da onları engellemenin nispeten az etki yaratacağı anlamına gelir.

   Tor ağı, trafiği birden fazla sunucu üzerinden yönlendirerek ve orijinal IP'yi gizleyerek başka bir anonimlik katmanı sunar. Dahası, saldırganlar eylemlerini tehlikeye atılmış makineler üzerinden yönlendirerek gerçek IP adreslerini gizleyebilir ve saldırıların bu sistemlerden kaynaklandığı izlenimini verebilir.

3. **Domain İsimleri:** Bir alan adı potansiyel olarak kara listeye alındığında veya yetkililer tarafından kaldırıldığında, kötü niyetli aktörler operasyonlarını hızla yeni kayıtlı bir alana kaydırabilir ve kötü niyetli faaliyetlerinde minimum kesintiyle sürekliliği koruyabilir.

   Bu akışkanlık, alan adlarını uzun vadede kötü niyetli faaliyetleri izlemek için daha az güvenilir bir parametre haline getirir.
   Domain isimlerini engellemek, saldırganın yeni bir domain oluşturmasını gerektirir. Bu, onlara biraz daha maliyet ve zorluk çıkarır.

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

5. **Host Artifacts:** Hedef cihazda bırakılan izler veya dosyalar. Bunları değiştirmek, saldırganın sistemdeki erişimini yeniden yapılandırmasını gerektirir.

6. **Tools**: Acı Piramidi'nde, araçları değiştirmek rakipler için önemli bir zorluk teşkil eder çünkü kapsamlı bilgi, çaba ve kaynak gerektirir. Kötü amaçlı araçlar oluşturmak veya değiştirmek, karmaşık beceriler ve her ikisine ilişkin derin bir anlayış gerektirir.

   Saldırganları, mevcut güvenlik önlemlerini ve savunmalarını başarıyla aşabilen yeni kötü amaçlı araçlar geliştirmek, test etmek ve dağıtmak için önemli miktarda zaman ve enerji harcamaya zorlayarak, bunu külfetli ve kaynak yoğun bir görev haline getirir ve dolayısıyla piramidin üst sıralarına yerleştirir.

7. **Tactics, Techniques, and Procedures (TTPs):** Acı Piramidi göz önüne alındığında, Taktikler, Teknikler ve Prosedürler (TTP'ler) rakiplerin değiştirmesinin oldukça zor olduğu yüksek bir zorluk ve karmaşıklık seviyesini temsil eder.

   TTP'leri değiştirmek, derin bir anlayış, yaratıcı strateji ve ustaca uygulama gerektirir ve bunları bir saldırganın araç setinin temel bir yönü haline getirir ve dolayısıyla bunları değiştirmek, saldırgana önemli bir acı verir ve kötü niyetli çabaları sorunsuz bir şekilde düzenleme yeteneğini engeller. Tespit edilemeyen yeni ve etkili bir saldırı akışı geliştirmek, kapsamlı bilgi ve uyarlanabilirlik gerektirir ve TTP'lerin siber tehdit manzaralarında neden ayrılmaz ve değiştirilmesi zor olduğunu vurgular.

4. Pyramid of Pain ve MITRE ATT&CK Karşılaştırması

- Siber tehdit istihbaratında Pyramid of Pain ve MITRE ATT&CK çerçevesi, saldırganların yöntemlerini anlamak ve etkili savunma stratejileri geliştirmek için kullanılan iki kritik modeldir. Pyramid of Pain, saldırganların operasyonlarını sürdürebilmek için ihtiyaç duydukları tehdit göstergelerini (IoC - Indicators of Compromise) sınıflandırarak, savunma ekiplerinin (Blue Team) tehdit aktörlerine ne kadar "acı" verebileceğini gösterir. MITRE ATT&CK ise siber tehdit gruplarının kullandığı taktikler, teknikler ve prosedürleri (TTP'ler) detaylı bir şekilde analiz eden bir çerçevedir.
  Bu iki model, saldırganları tespit etmek ve engellemek amacıyla kullanılmakla birlikte, odaklandıkları noktalar farklıdır:
  - Pyramid of Pain, saldırganların karşılaşacağı zorluk seviyesini gösterirken, MITRE ATT&CK, bu saldırıların nasıl gerçekleştirildiğini detaylı olarak açıklar.
  - Pyramid of Pain'in üst katmanları (Tools, TTP'ler) doğrudan MITRE ATT&CK teknikleriyle örtüşür ve saldırganların en çok zorlandığı alanları temsil eder.
  - MITRE ATT&CK'teki TTP'ler, Pyramid of Pain'in en üst seviyesindeki göstergelere karşılık gelir. Yani bir saldırganın TTP'lerini değiştirmek, operasyonel devamlılığı açısından en maliyetli olanıdır.

5. Pyramid of Pain ile MITRE ATT&CK Nasıl Birlikte Kullanılabilir?

5.1.IoC'leri MITRE ATT&CK Teknikleri ile Eşleştirme

- Pyramid of Pain'in alt seviyelerindeki IoC'ler (hash değerleri, IP adresleri vb.), MITRE ATT&CK teknikleriyle doğrudan ilişkilendirilebilir. Örneğin, T1071 (Application Layer Protocols) saldırısında kullanılan kötü amaçlı IP adresleri veya domain adları, Pyramid of Pain'in alt seviyelerine denk gelir.

5.2.Saldırganın Operasyonel Esnekliğini Kısıtlama

- Pyramid of Pain, saldırganın adaptasyon yeteneğini aşamalı olarak zorlaştıran bir yapı sunar. MITRE ATT&CK ise saldırganın hangi aşamada olduğu konusunda bir harita sağlar.

5.3.Tehdit Avcılığı (Threat Hunting) Stratejileri Geliştirme

- MITRE ATT&CK çerçevesi, organizasyonların hangi TTP'lerin tehdit oluşturduğunu anlamasına yardımcı olurken, Pyramid of Pain, hangi önlemlerle saldırganın faaliyetlerini daha fazla sekteye uğratabileceğimizi gösterir.

5.4.Savunma Maliyetlerini Azaltma

- Pyramid of Pain'in üst seviyelerindeki göstergeler (TTP'ler) engellenirse, saldırganın yeniden yapılanma maliyeti çok daha fazla olur. MITRE ATT&CK ile bu süreç detaylandırılarak, hangi tekniklere karşı daha iyi önlem alınması gerektiği belirlenebilir.

6. 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.

7. Sonuç

Siber güvenlikte etkili savunma stratejileri oluşturmak için hem Pyramid of Pain hem de MITRE ATT&CK kritik öneme sahiptir. Pyramid of Pain, saldırganların operasyonel sürdürülebilirliğini nasıl zorlaştırabileceğimizi gösterirken, MITRE ATT&CK çerçevesi ise saldırganların taktiklerini ve tekniklerini anlamamıza yardımcı olur.

Bu iki model birlikte kullanıldığında, güvenlik ekipleri tehdit avcılığı, saldırı tespiti ve önleme süreçlerinde daha sistematik ve etkili bir yaklaşım benimseyebilir. Saldırganları yalnızca tespit etmek değil, onların adaptasyon süreçlerini zorlaştırmak ve daha maliyetli hale getirmek uzun vadede daha güçlü bir siber savunma sağlar.

Sonuç olarak, siber tehdit istihbaratının doğru şekilde uygulanması, tehdit aktörlerinin IoC'leri kolayca değiştirebileceği bir oyundan, onları TTP değişikliği yapmaya zorlayan ve maliyetlerini artıran bir mücadeleye dönüşebilir. Bu nedenle, Pyramid of Pain ve MITRE ATT&CK birlikte ele alındığında, siber saldırılara karşı savunma sadece reaktif değil, aynı zamanda proaktif bir hale getirilebilir.

Kaynakça

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