


PYRAMID OF PAIN



HAZIRLAYAN:

ADI: Ayşe

SOYADI: BALCI

TARİH: 17.02.2025

İçindekiler Tablosu

Giriş	2
PYRAMID OF PAIN NEDİR?.....	3
ACI PİRAMİDİ BASAMAKLARI.....	4
Hash Değerleri	4
IP Adresleri	4
Alan Adları.....	4
Host/Networks Artifacts	4
Araçlar	5
TTP	5
Sonuç	6
KAYNAKÇA	7

Giriş:

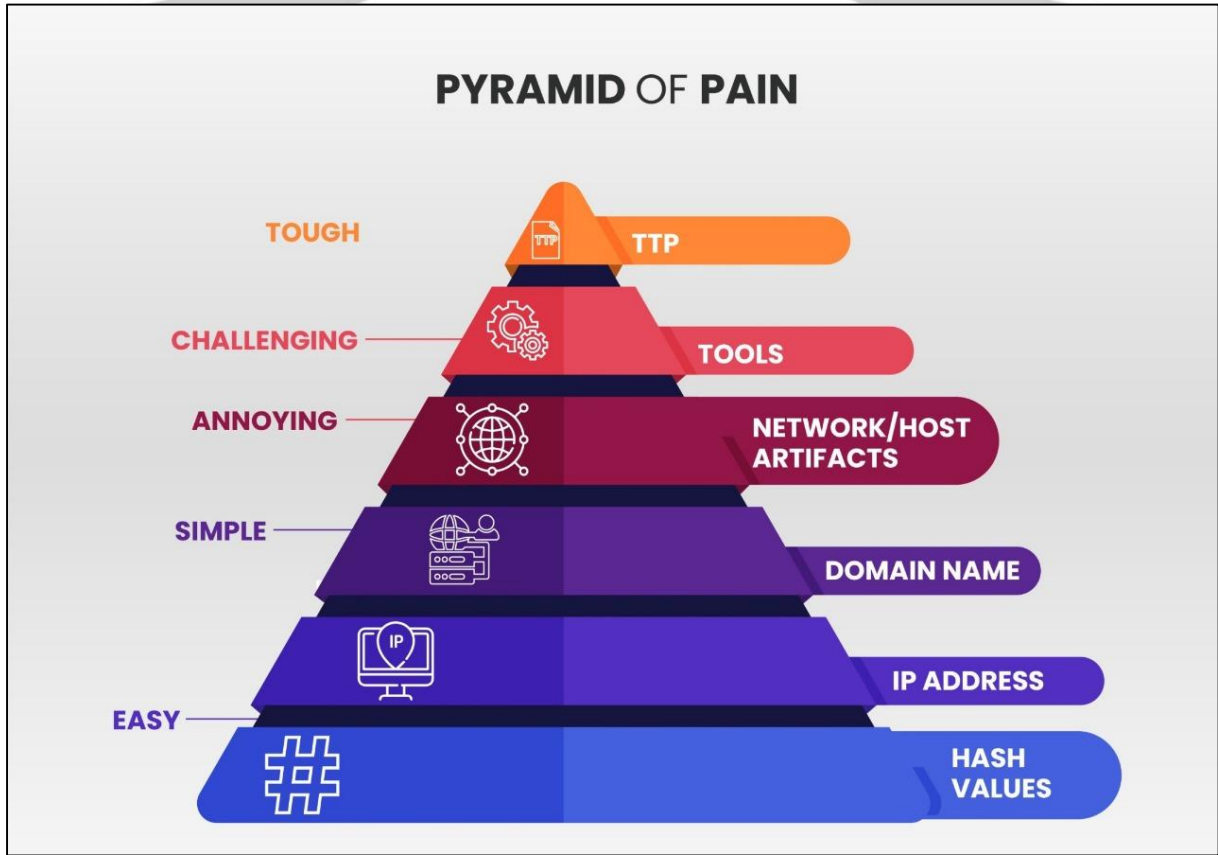
Siber güvenlik tehditleri, günümüzde giderek daha karmaşık hale gelmekte ve güvenlik ekiplerinin saldırıları tespit edip engelleme süreçlerini daha stratejik bir yaklaşımla ele almasını gerektirmektedir. Bu noktada, **Acı Piramidi (Pyramid of Pain)**, tehdit aktörlerinin davranışlarını anlamak ve etkili savunma stratejileri oluşturmak için kritik rehberler sunar. Acı Piramidi, saldırganların kullandığı göstergeleri değiştirmenin ne kadar zor olduğunu hiyerarşik bir yapıyla açıklar. Bu çalışmada, bu modelin temel bileşenleri incelenerek, siber güvenlik operasyon merkezleri (SOC) için nasıl bir savunma çerçevesi sunduğu ele alınacaktır.



PYRAMID OF PAIN NEDİR?

Acı Piramidi (Pyramid of Pain), siber saldırıların etkilerini hiyerarşik olarak sınıflandırarak, savunma kaynaklarını önceliklendirmeye yardımcı olan bir siber güvenlik modelidir. Beş seviyeden oluşan bu model, en alt seviyede temel güvenlik ihtiyaçlarını, en üst seviyede ise daha sofistike güvenlik önlemlerini kapsar. Alt seviyelerde erişim kontrolü, güvenlik duvarları ve antivirüs gibi temel önlemler bulunurken, orta seviyelerde ağ saldırı tespiti, şifreleme ve kimlik doğrulama gibi gelişmiş çözümler yer alır. Üst seviyelerde ise yapay zeka destekli güvenlik, tehdit istihbaratı ve uçtan uca şifreleme gibi ileri düzey önlemler bulunur. Acı Piramidi, güvenlik önlemlerini stratejik bir şekilde belirlemeye yardımcı olur.

Acı Piramidi, siber güvenlikte farkındalığı artırmak ve en uygun güvenlik önlemlerini almak için bir çerçeve sunar.



Şekil 1 Pyramif of Pain

ACI PİRAMİDİ BASAMAKLARI

Hash Değerleri

Hash değeri, veriyi benzersiz şekilde tanımlayan sabit uzunlukta sayısal bir değerdir ve bir hashing algoritmasının sonucudur. Yaygın olarak kullanılan bazı hashing algoritmaları şunlardır

Siber güvenlik uzmanları, hash değerlerini kötü amaçlı yazılımları tanımlamak, şüpheli dosyaları analiz etmek ve zararlı bileşenleri benzersiz şekilde referans almak için kullanır.

Hash değerlerini aramak ve analiz etmek için yaygın olarak VirusTotal ve OPSWAT kullanılabilir.

IP Adresleri

Acı Piramidi'nde IP adresleri, saldırganlar için değiştirilmesi en kolay göstergelerden biri olduğu için en alt seviyede yer alır. Kötü niyetli etkinliklerde kullanılan IP adreslerini bilmek ve güvenlik duvarlarında engellemek savunmada önemlidir, ancak bu yöntem saldırganlara çok az "acı" verir çünkü farklı bir genel IP adresi kullanarak kolayca yeniden bağlanabilirler. Bu nedenle, IP adreslerine dayalı savunma yöntemleri tek başına yeterli olmayıp, piramidin üst seviyelerindeki daha zor değiştirilebilir göstergelerle desteklenmelidir.

Alan Adları

Acı Piramidi'nde alan adları, IP adreslerinin bir üst seviyesinde yer alır çünkü değiştirilmesi daha zor ve maliyetlidir. Saldırganlar, kötü amaçlı faaliyetlerde özel olarak kaydedilmiş alan adlarını kullanır ve bunları engellemek, zararlı trafiği durdurmak için etkili olabilir. Ancak, deneyimli bir saldırgan yeni bir alan adı kaydederek veya dinamik DNS hizmetleri kullanarak bunu kolayca aşabilir. Bu yüzden, alan adlarına dayalı savunma yöntemleri, daha zor değiştirilebilir ağ izleri, araçlar ve TTP'ler gibi göstergelerle desteklenmelidir.

Host/Networks Artifacts

Bu seviyede saldırıyı tespit edebilirsiniz, saldırgan araçlarını ve yöntemlerini değiştirmek zorunda kalacağı için daha fazla zaman ve kaynak harcaması gerekecektir. Bu da saldırganı hüsrana uğratar ve saldırıyı sürdürmesini zorlaştırır.

Ana bilgisayar yapıları, kayıt defteri değerleri, şüpheli işlem yürütmeleri, saldırı modelleri ve IOC'ler gibi izler, saldırganın sistemde bıraktığı gözlemlenebilir öğelerdir. Ayrıca, kötü amaçlı yazılımların bıraktığı dosyalar veya mevcut tehdide özgü diğer izler de bu kategoriye girer. Bu izleri tespit etmek, saldırganın ilerlemesini ciddi şekilde zorlaştırabilir.

Araçlar

Bu aşama koyu sarı renkle gösterilmektedir çünkü burada tehdit aktörünün kullandığı araçlar ve zararlılar tespit edilebilir. Bu süreçte, saldırganın kullandığı zararlı yazılımlar ve benzeri araçların analizi yapılabilir ve buna göre etkili önlemler alınabilir. Saldırganın kullandığı araç setlerinin etkisiz hale gelmesi, saldırganın motivasyonunu önemli ölçüde düşürür çünkü yeni araçlar geliştirebilmek için ciddi bir araştırma ve çaba sarf etmesi gerekir.

Bu aşamada, antivirüs yazılımları ve YARA kuralları gibi yöntemler, saldırganları tespit etmek için etkili araçlar olarak kullanılabilir.

TTP

Bu aşama kırmızı renkle işaretlenmiştir çünkü burada saldırganın davranışları analiz edilerek kimliği hakkında önemli çıkarımlar yapılabilir. Bu tür bir bilgi, saldırganın gelecekteki hareketlerini önceden tahmin etmeyi ve buna göre karşı stratejiler geliştirmeyi mümkün kılar, bu da saldırganın etkisiz hale getirilmesini kolaylaştırır. Bu durum, saldırgan için oldukça olumsuzdur çünkü iki seçeneği vardır: ya tamamen vazgeçecek ya da her şeyini yeniden başlatmak zorunda kalacaktır.

Hacker gruplarının TTP'lerini (Teknikler, Taktikler ve Prosedürler) öğrenmek ve analiz etmek için MITRE ATT&CK çerçevesi oldukça faydalı bir araçtır.

Sonuç:

Acı Piramidi (Pyramid of Pain), siber güvenlik tehditlerine karşı mücadelede, saldırganların kullandığı göstergeleri hiyerarşik bir yapıda ele alarak güvenlik önlemlerinin etkinliğini artırmayı hedefler. Bu model, en alt seviyelerde kolay değiştirilebilir göstergelerden başlayarak, en üst seviyede saldırganın taktik, teknik ve prosedürlerine (TTP) kadar uzanır. Piramidin üst kademelerine odaklanıldığında, saldırganların faaliyetlerini sürdürmesi daha maliyetli ve zor hale gelir, bu da onları caydırıcı bir etki yaratır. Bu nedenle, siber güvenlik ekipleri yalnızca IP adresleri ve hash değerleri gibi kolay değiştirilebilir göstergelerle değil, aynı zamanda saldırganın araçlarını ve yöntemlerini analiz ederek daha stratejik bir savunma mekanizması oluşturmalıdır. Acı Piramidi'nin doğru bir şekilde uygulanması, saldırganların operasyonlarını aksatmada ve uzun vadeli güvenlik önlemleri geliştirmede kritik bir rol oynar.



KAYNAKÇA

1. <https://medium.com/software-development-turkey/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-91554269b9b6>
2. <https://medium.com/@AbhijeetSingh4/pyramid-of-pain-soc-level-1-tryhackme-walkthrough-15ea4a09b901>
3. <https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain>
4. https://www.google.com/imgres?q=pyramid%20of%20pain&imgurl=https%3A%2F%2Fwww.terrabytegroup.com%2Fwp-content%2Fuploads%2F2024%2F06%2Fpyramid-of-pain-image-terrabytegroup.com_.jpg&imgrefurl=https%3A%2F%2Fwww.terrabytegroup.com%2Fpyramid-of-pain-in-cyber-security%2F&docid=MJVIL03axDHdUM&tbnid=tVZwzS-QqYpCgM&vet=12ahUKEwiBgY3FqsqLAXXIQPEDHbhSPHQM3oECFIQAA..i&w=1280&h=898&hcb=2&ved=2ahUKEwiBgY3FqsqLAXXIQPEDHbhSPHQM3oECFIQAA