ALTAY TAKIMI

PYRAMID OF PAIN RAPORU

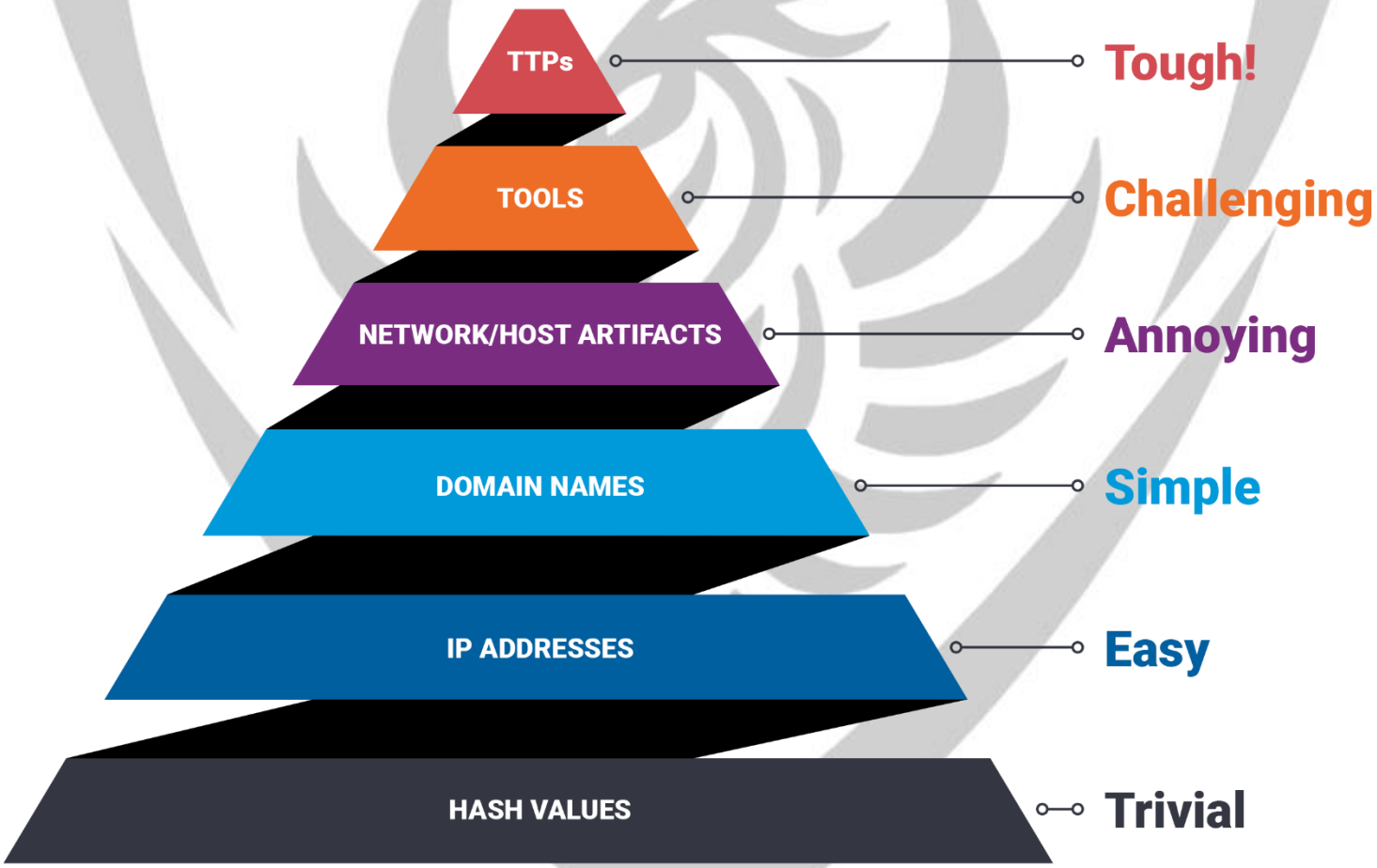
Hazırlayan : Efe Körün

Tarih : 07.02.2025

1. GİRİŞ

Siber güvenlikte tehdit tespiti ve saldırganlarla mücadele, sürekli gelişen bir süreçtir. 2013 yılında David Bianco tarafından geliştirilen *Pyramid of Pain* modeli, saldırganların izlerini sürme ve onları caydırma konusunda siber güvenlik ekiplerine rehberlik eden önemli bir yapıdır. Bu model, saldırı izlerini tespit etmenin zorluk seviyelerini bir piramit şeklinde sıralayarak, güvenlik ekiplerinin hangi seviyelerde etkili önlemler alabileceğini göstermektedir.

Pyramid of Pain, özellikle SOC (Security Operations Center) ekipleri için, tehdit avcılığı ve saldırıların engellenmesi açısından kritik bir araçtır. Bu raporda, modelin farklı seviyeleri, her seviyedeki tehditlerin nasıl tespit edilebileceği ve savunma mekanizmalarının nasıl güçlendirilebileceği ele alınmaktadır.

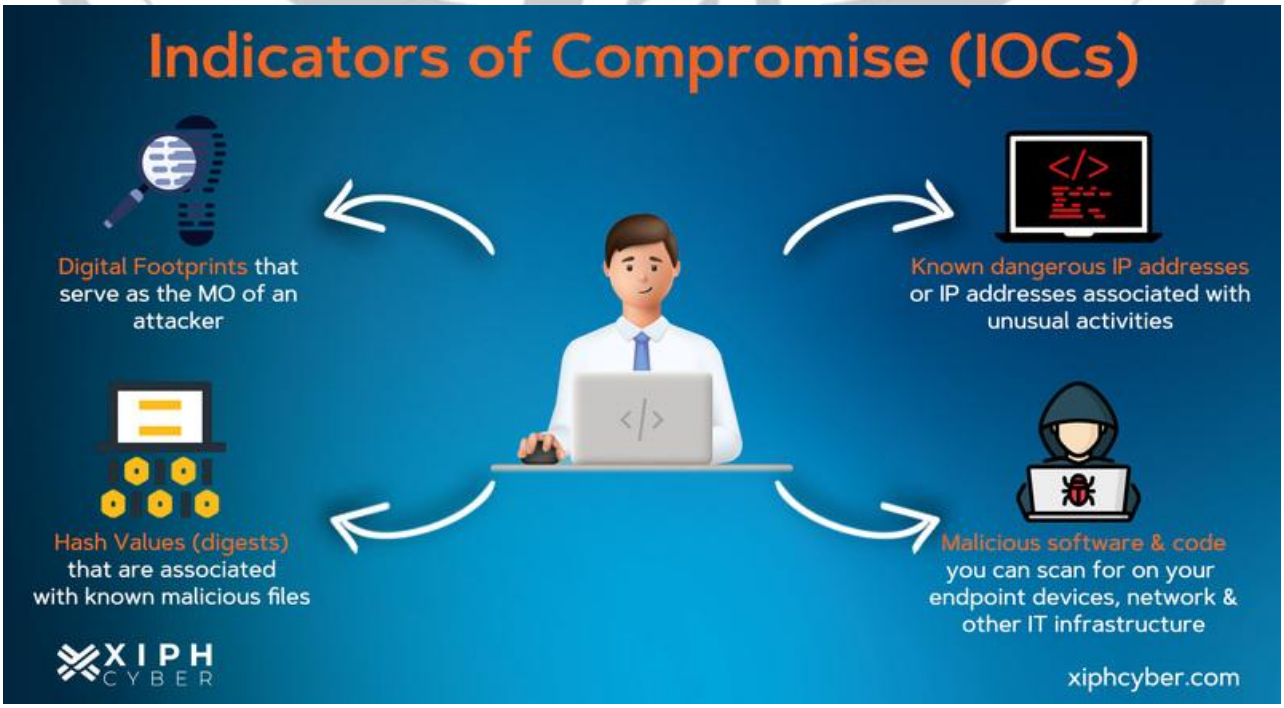


Pyramid of Pain Nedir?

Pyramid of Pain, 2013 yılında David Bianco tarafından geliştirilmiş bir modeldir ve siber güvenlik tehditlerinin tespit edilmesindeki zorluk seviyelerini anlamada rehberlik eder. Özellikle blue team ekipleri tarafından kullanılan bu model, tehditlerin tespit edilebilirliğini bir piramit şeklinde sıralar. Piramidin alt kısmında kolayca tespit edilebilen IOC'ler bulunurken, piramidin üst seviyelerine doğru ilerledikçe, tespit edilmesi daha güç ve karmaşık tehditler yer alır. Model, savunma ekiplerinin tehditleri etkili bir şekilde tespit etme ve bunlarla başa çıkma süreçlerini daha verimli hale getirmeyi amaçlar Üst seviyedeki tehditler, saldırganların gizlenmesini kolaylaştırarak savunma ekiplerinin işini daha karmaşık hale getirir.

IOC Nedir?

IOC (Indicators of Compromise), bir siber saldırının izlerini veya etkilerini tespit etmek için kullanılan göstergelerdir. Bu göstergeler, sistemlerdeki anormal aktiviteler veya kötü amaçlı yazılımların varlığını belirlemek için analiz edilir. IOC'ler, saldırıların erken tespiti ve etkilerinin minimize edilmesi adına savunma ekiplerine önemli bilgiler sağlar.



Pyramid of Pain Aşamaları

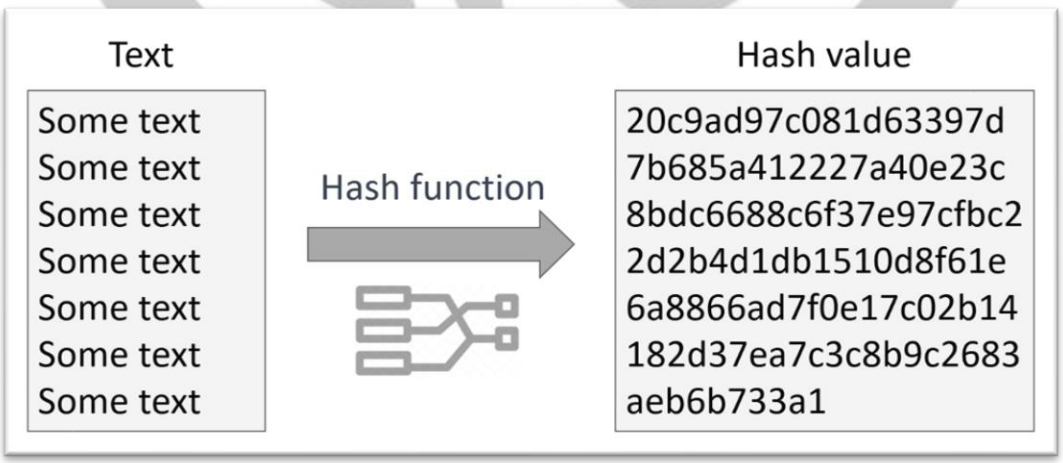
Pyramid of Pain, en alt seviyede dosya hash'leri, daha sonra ikinci seviyede IP adresleri üçüncü seviyede domainler, dördüncü seviyede URL'ler ve registry anahtarları, beşinci seviyede saldırganın kullandığı araçlar ve teknikler, en üst seviyede ise saldırganın davranışlarını ve stratejilerini(TTP) içeren toplam 6 aşamadan oluşmaktadır.

1. Hash Değerleri

Hash değerleri, bir dosyanın benzersiz kimliği gibidir ve dijital parmak izi olarak düşünülebilir. Ancak hash değerleri, oldukça hassastır ve küçük bir değişiklik bile hash değerini tamamen değiştirebilir. Örneğin, bir dosya içeriğine tek bir boşluk eklemek ya da bir satır kodu silmek, programın işleyişini etkilemeden hash değerini değiştirebilir. Bu yüzden hash değerleri kolayca manipüle edilebilir.

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

Örneğin, bir zararlı yazılım dosyası "trojan.dll" adıyla tanımlanmış olsun ve bu dosyanın hash değeri güvenlik yazılımları tarafından bilinsin. Ağda bu dosya tekrar karşılaşıldığında, hash değeri sayesinde hemen tespit edilebilir. Ancak, saldırgan dosyanın içeriğini değiştirmeden sadece boyutunu artırarak bir veri eklerse, hash değeri de değişir. Bu durumda dosya, önceki hash değeriyle tespit edilemez hale gelir çünkü hash değeri farklılaşmıştır.



2. IP Adresleri

IP adresleri, bir ağa bağlı cihazları tanımlamak için kullanılmaktadır ancak saldırganlar IP adreslerini taktikler ve toollar ile hem değiştirip hem de gizleyebilirler.

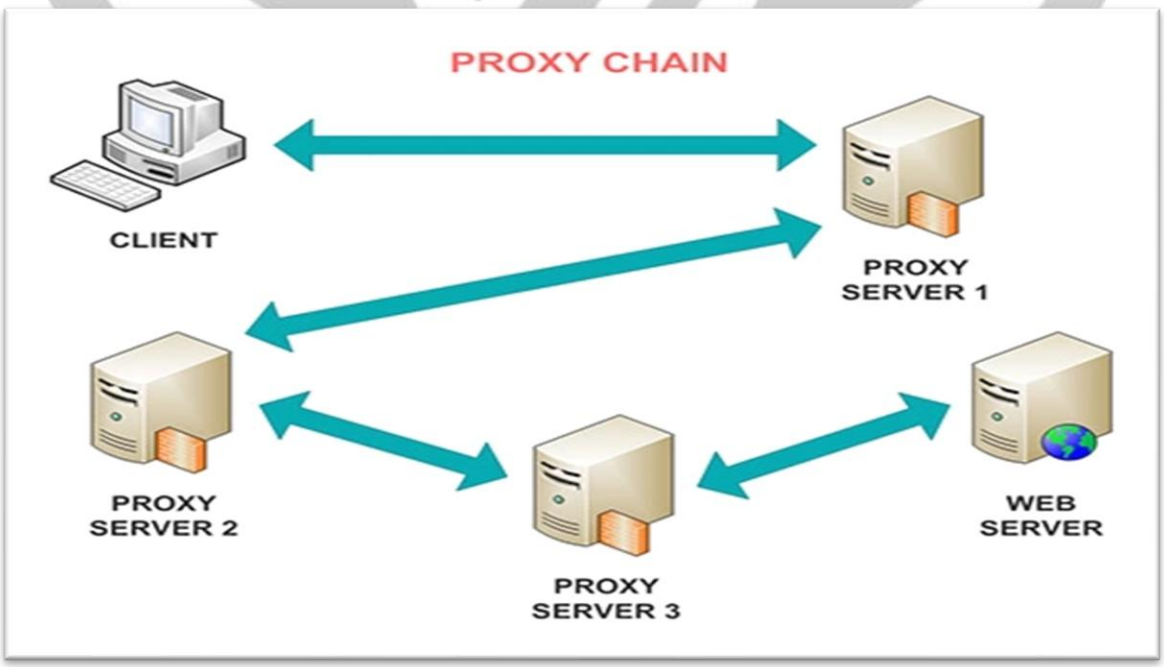
➤ Proxy sunucuları, VPN'ler gibi araçlar sayesinde gerçek IP adresleri gizlenebilir, bu da kullanıcıların farklı konumlardan bağlanıyormuş gibi görünmelerini sağlar.

➤ Tor ağı da anonimlik sağlamak için kullanılır; trafik birden fazla sunucu üzerinden yönlendirilerek orijinal IP adresi gizlenir.

➤ Bunun yanı sıra, saldırganlar ele geçirilmiş makineler üzerinden saldırı yaparak gerçek IP adreslerini gizleyebilir ve saldırıların o makinelerden geliyormuş gibi görünmesini sağlayabilirler.

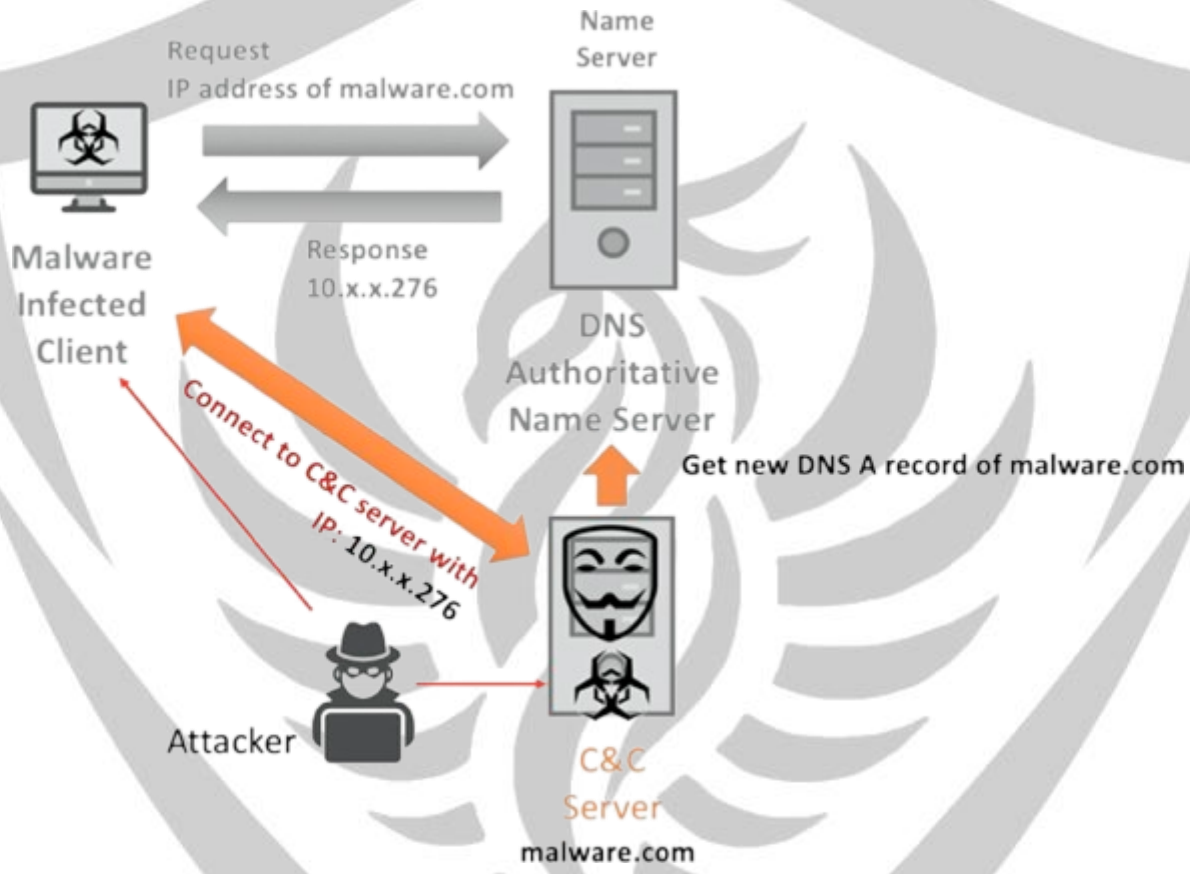
IP Address	First Seen	Description
170.130.165[.]73	October 14, 2024	Likely Cobalt Strike infrastructure
45.11.181[.]44	October 24, 2024	Likely Cobalt Strike infrastructure
66.42.118[.]54	October 15, 2024	Exfiltration server
79.132.130[.]211	October 24, 2024	Likely Cobalt Strike infrastructure

Örneğin, Bir saldırgan, bir siber saldırı gerçekleştirirken Proxychains aracını kullanarak trafiği birden fazla proxy sunucu üzerinden yönlendirerek gerçek IP adresini gizler ve farklı lokasyonlardan saldırıyormuş gibi görünmesini sağlar. böylece saldırganın tespit edilmesi zorlaşır. Bu da, IP adreslerinin güvenlik savunmalarında geçici ve güvenilmez bir unsur olduğunu göstermektedir.



3. Alan Adları (Domain Names)

Alan adları, saldırganların altyapılarının önemli bir parçasıdır ve genellikle saldırılarında kullandıkları komuta ve kontrol (C2) sunucularına bağlantı sağlamak için kullanılmaktadır. Saldırganlar, belirli bir alan kara listeye alındığında veya kapatıldığında, alan adlarının değiştirilmesi oldukça kolay ve düşük maliyetli olduğu için hızla yeni bir alan adı alarak operasyonlarına kesintisiz devam edebilirler. Ayrıca kötü amaçlı alan adlarını yasal hizmetlerle harmanlayarak tespitten kaçınır ve C2 sunucularını sıkça değiştirerek savunma mekanizmalarından kaçarlar.



Örneğin, Blackbasta Grubunun CobaltStrike Saldırısını yaparken kullandığı Domainler

Domain	First Seen
Moereng[.]com	October 9, 2024
Exckicks[.]com	October 2, 2024

4. Network & Host İzleri

Network & Host Artifact'leri, bir saldırganın ağda veya host ortamında gerçekleştirdiği eylemler sırasında bıraktığı izlerdir ve bu izler, zararlı faaliyetlerin tespit edilmesinde önemli bir rol oynar. Bu izler, saldırının ne zaman yapıldığını ve hangi tekniklerin kullanıldığını anlamamıza yardımcı olur ve saldırı izlerini gizlemeye çalışırken saldırganın zaman kaybetmesine yol açar. Ayrıca, bu izler saldırganın gizliliğini bozar ve tespit edilmesini kolaylaştırarak onların işlerini zorlaştırır

Ağda ve host ortamında bırakılan izler, genellikle saldırganın komut ve kontrol (C2) bilgileri, URL pathleri, dosyalar ve registery key gibi öğeleri içerir. Bu izler, kötü niyetli hareketlerle normal işlemleri ayırt etmemize olanak tanır.

Bazı Network & Host İzleri:

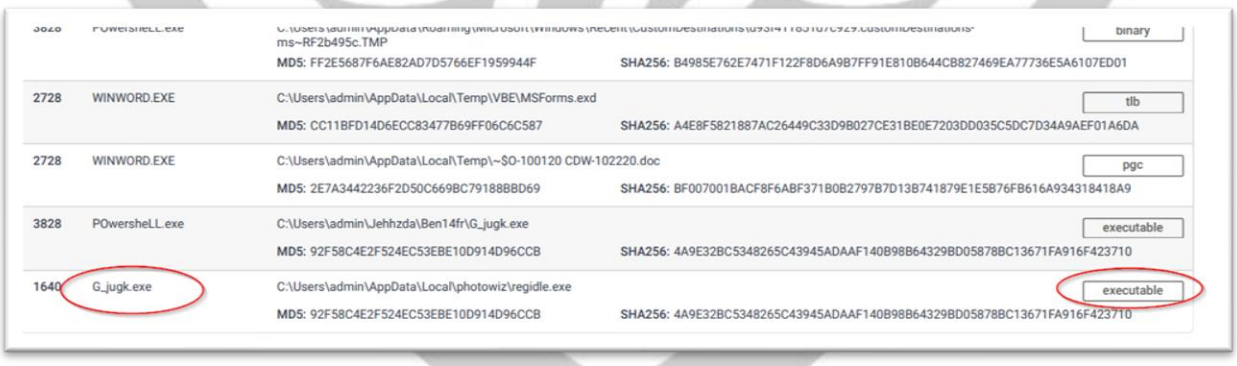
Komut ve Kontrol (C2) Bilgileri: Saldırganın C2 sunucusuna bağlantı kurmak için kullandığı IP adresleri veya bağlantı bilgileri.

Erişim Yapılan URL'ler: Saldırganın ağ üzerinden yaptığı isteklerdeki belirgin URL'ler.

Log Kayıtları: Sistem loglarında görülen anormal değişiklikler. Örneğin, Windows Defender Firewall ayarlarının değiştirilmesi.

Registry Key Değişiklikleri: Zararlı yazılımlar tarafından eklenen özel kayıt defteri anahtarları.
Örneğin
"HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SuperBackupMan:Default:Service"

Dosya ve Klasörler: Saldırganın oluşturduğu veya değiştirdiği dosya ve klasörler.

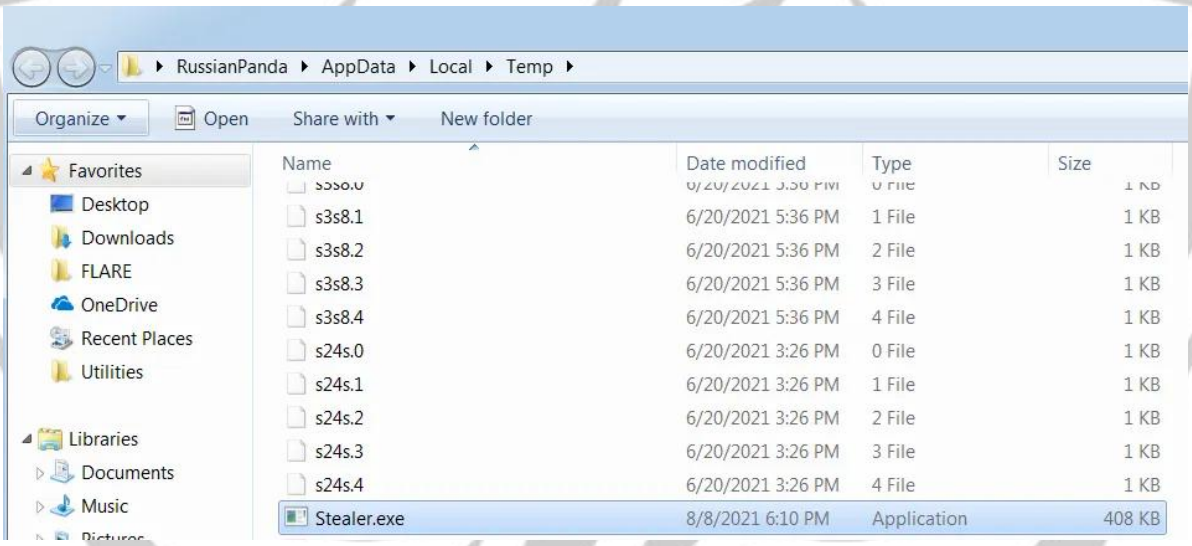


5. Tools

Pyramid of Pain'in Tools aşaması, saldırganlar için oldukça zorlayıcı bir aşamadır. Bu seviyede, saldırganların kullandığı belirli yazılım ve araçları tespit edip engellemek hedeflenir. Çünkü saldırganların başarılı bir saldırı gerçekleştirebilmesi için özel olarak geliştirilmiş veya modifiye edilmiş araçlara ihtiyacı vardır.

Eğer güvenlik ekipleri bu araçları etkili bir şekilde tespit eder ve kullanımını önlerse, saldırganlar ciddi bir sorunla karşılaşır. Mevcut bir aracı değiştirmek veya yeni bir araç geliştirmek sadece zaman kaybına yol açmakla kalmaz, aynı zamanda teknik bilgi ve test süreçleri gerektirir. Bu da saldırganın işini oldukça zorlaştırır.

Örneğin, bir saldırganın uzaktan erişim sağlamak için kullandığı bir RAT tespit edilip engellendiğinde, saldırgan ya yeni bir RAT geliştirmek zorunda kalır ya da piyasada bulunan başka bir yazılımı uyarlamak durumundadır. Ancak siber güvenlik ekipleri benzer araçları tanıyıp engelleme yeteneğine sahipse, saldırganın süreci sürekli kesintiye uğrar ve ilerlemesi giderek zorlaşır.

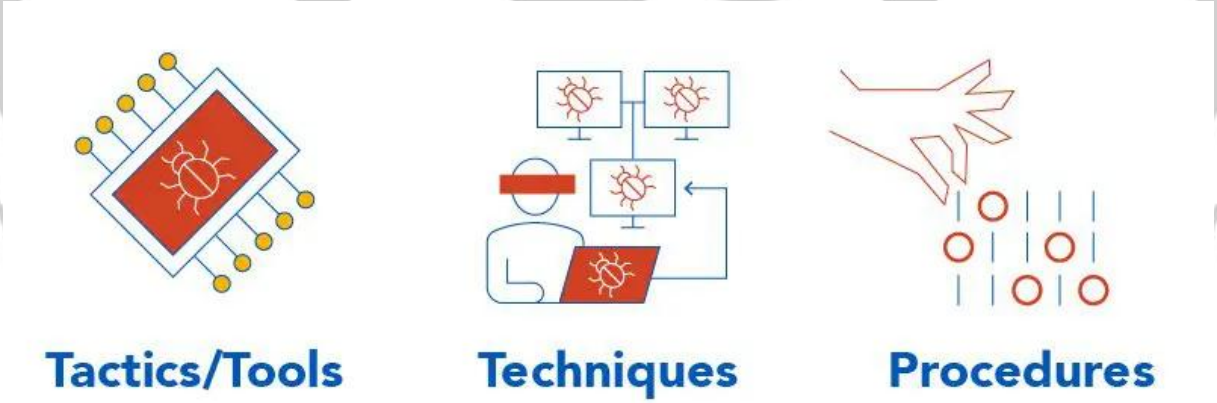


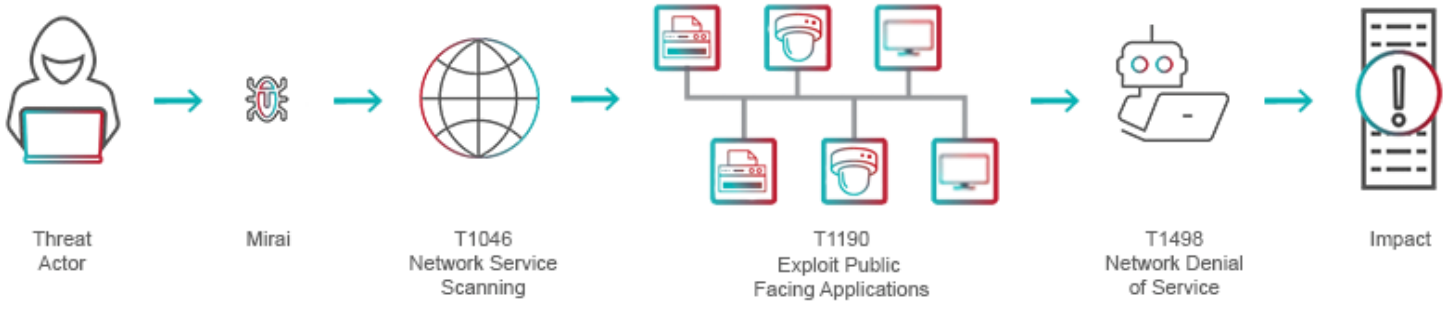
6. Taktikler, Teknikler ve Prosedürler (TTPs)

Pyramid of Pain'in en tepe noktasında, saldırganların en zor değiştireceği unsurlar olan Taktikler, Teknikler ve Prosedürler (TTPs) yer alır. Bu seviyede, saldırganların kullandığı belirli araçları veya indikatörleri değil, saldırılarını nasıl gerçekleştirdiklerini hedef alarak güvenlik önlemleri geliştirilir. Yani, saldırganların yöntemlerini ve stratejilerini tespit edip bozmak, onların tüm operasyon modelini yeniden düşünmeye zorlar.

Örneğin, bir saldırganın "Pass-the-Hash" tekniğini kullandığını tespit ederseniz, bu saldırıyı doğrudan engelleyerek onun araçlarını değiştirmesini değil, tamamen yeni bir saldırı yöntemi öğrenmesini sağlarsınız. Bu, saldırgan açısından en maliyetli ve zaman alıcı süreçtir. Çünkü yeni teknikler geliştirmek, test etmek ve uygulamak her yönden zor bir süreçtir.

Eğer güvenlik ekipleri geniş bir yelpazedeki TTP'leri tespit edip etkisiz hale getirebilirse, saldırganların iki seçeneği olur: Ya tamamen yeni teknikler geliştirmek zorunda kalırlar ya da saldırı girişimlerinden vazgeçerler. Bu nedenle, TTP seviyesinde savunma yapmak, saldırganlar için en büyük zorluklardan birini oluşturur ve en etkili siber güvenlik stratejilerinden biri olarak kabul edilir.





SOC Ekipleri İçin Pyramid Of Pain'in Önemi

Pyramid Of Pain, SOC ekipleri için oldukça önemli bir kavramdır. Temel olarak, saldırganların kullandığı teknikleri hangi seviyede tespit edip engellediğinizin, onların işlerini ne kadar zorlaştıracağını anlatır. SOC ekipleri için bu modelin önemi birkaç başlık altında ele alınabilir:

Tespit ve Müdahale Önceliklerini Belirleme

Pyramid Of Pain, SOC ekiplerinin önceliklerini doğru belirlemesine yardımcı olur. Piramidin en alt seviyesinde yer alan dosya hash'leri veya IP adresleri gibi basit izler kolayca tespit edilip engellenebilir. Ancak saldırganlar da bunları çok hızlı bir şekilde değiştirebilir. Bu yüzden, üst seviyelere odaklanmak (örneğin, saldırganların kullandığı araçlar ve teknikler) onları gerçekten zor durumda bırakır.

Daha Güçlü Tespit Mekanizmaları Kurma

Geleneksel tehdit istihbaratı çoğu zaman IP adresleri veya domainler gibi kısa ömürlü izlere odaklanır. Ancak saldırganlar bunları kolayca saptırabilir. SOC ekipleri, ağda ve sistemlerde bırakılan izleri, kullanılan araçları ve saldırı yöntemlerini analiz ederek çok daha etkili bir savunma hattı oluşturabilir.

Stratejik Tehdit Avcılığı

Pyramid Of Pain, tehdit avcılığı çalışmalarına da rehberlik eder. SOC analistleri, yalnızca belirli IP'leri veya hash'leri aramak yerine, saldırganların davranış kalıplarını ve izledikleri yöntemleri inceleyerek daha derinlemesine analizler yapabilir. Bu da saldırganları henüz zarar vermeden tespit etmeye yardımcı olur.

Kaynakları Daha Verimli Kullanmak

Siber güvenlikte kaynak yönetimi çok kritiktir. Pyramid Of Pain, en çok zarar verici indikatörlere odaklanarak daha etkili bir savunma stratejisi oluşturmayı sağlar. Böylece ekipler zamanlarını ve enerjilerini en doğru yerlere harcar.

Saldırganları Gerçekten Zor Duruma Düşürmek

Siber güvenliğin nihai hedeflerinden biri saldırganları caydırmak ve hareket alanlarını daraltmaktır. Eğer bir saldırganın yalnızca IP adresi engellenirse, bu onun için büyük bir sorun olmaz. Ancak kullandığı saldırı araçları veya yöntemleri engellenirse, tüm operasyonlarını yeniden planlamak zorunda kalır. Bu da zaman ve maliyet açısından ciddi bir yük oluşturur.

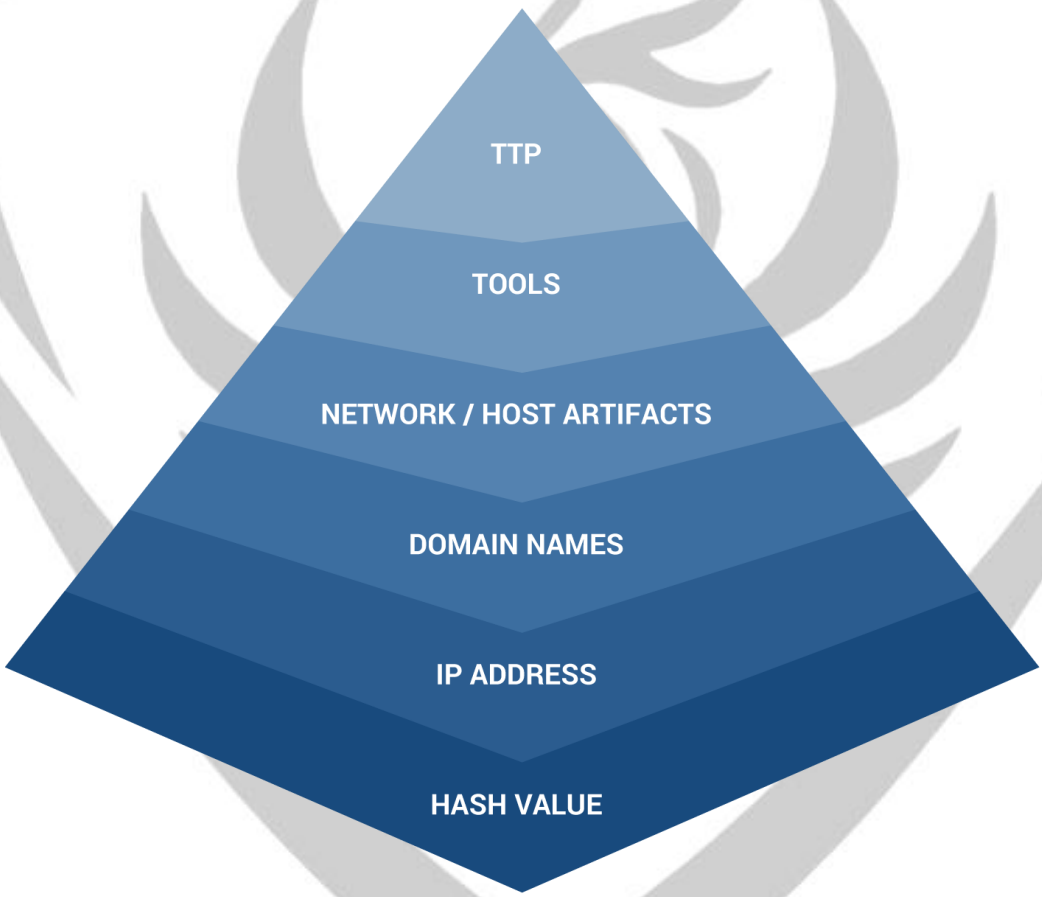
Sürekli Gelişim ve Adaptasyon

Tehditler her geçen gün evrildiği için, savunma stratejilerinin de buna ayak uydurması gerekir. Pyramid Of Pain, SOC ekiplerine sürekli kendilerini geliştirme ve saldırganların en çok canını yakacak yöntemlere odaklanma imkânı tanır.

SONUÇ:

Pyramid Of Pain modeli, siber güvenlik ekiplerine tehditleri yalnızca tespit etmekle kalmayıp, saldırganların operasyonlarını zorlaştırma konusunda da stratejik bir yaklaşım sunar. Hash değerleri, IP adresleri ve alan adları gibi temel göstergelerden, saldırganların araçlarına ve taktiklerine kadar uzanan bu model, etkili bir tehdit istihbaratı ve savunma stratejisi oluşturmanın temel taşlarından biridir.

SOC ekipleri, bu modeli kullanarak daha güçlü tespit mekanizmaları kurabilir, saldırganların yöntemlerini analiz edebilir ve sürekli gelişen tehditlere karşı kendilerini adapte edebilir. Sonuç olarak, Pyramid Of Pain, modern siber güvenlik dünyasında hem saldırıları engellemek hem de saldırganları gerçek anlamda zor durumda bırakmak için vazgeçilmez bir modeldir.



KAYNAKÇA:

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

https://www.vectra.ai/topics/pyramid-of-pain

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

https://cymulate.com/cybersecurity-glossary/pyramid-of-pain/

https://blackcell.io/the-pyramid-of-pain-infographic/#:~:text=Network%2FHost%20Artifacts%3A%20Artifacts%20within,between%20legitimate%20and%20malicious%20actions

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

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a