MİTRE ATT&CK
PYRAMIT OF PAIN

Hazırlayan
Burak Ali DÜZÜN

23.02.2025

İÇİNDEKİLER

MITRE ATT&CK 1
Giriş 1
MITRE ATT&CK Nedir? 1 1
MITRE ATT&CK Enterprise: 2
1. Enterprise ATT&CK Yapısı: 2
2. Enterprise ATT&CK Matrisinde Yer Alan Taktikler: 2
1) Initial Access (Başlangıç Erişimi): 2 2
2) Execution (Çalıştırma): 5 5
3) Persistence (Kalıcılık Sağlama) – MITRE ATT&CK 6 6
4) Privilege Escalation (Ayrıcalık Yükseltme) – MITRE ATT&CK 7 7
5) Defense Evasion (Savunmadan Kaçınma) – MITRE ATT&CK 10 10
6) Credential Access (Kimlik Bilgisi Erişimi) – MITRE ATT&CK 14 14
6) Discovery (Keşif) – MITRE ATT&CK 16 16
7) Lateral Movement (Yanal Hareket) – MITRE ATT&CK 19 19
8) Collection (Veri Toplama) – MITRE ATT&CK 21 21
9) Command and Control (Komuta ve Kontrol) – MITRE ATT&CK 24 24
10) Exfiltration (Veri Sızdırma) – MITRE ATT&CK 26 26
11) Impact (Etkilendirme) – MITRE ATT&CK 28 28
3. Enterprise ATT&CK Kullanım Alanları: 31 31
4. ATT&CK Enterprise ve MITRE Engenuity Evaluations: 31 31
5. Sonuç: 31 31

Pyramit of Pain 33
Giriş: 33
Pyramid of Pain (Acı Piramidi) Nedir? 33
1. Piramidin Yapısı: 33
1.1. Hash Değerleri: 33
1.2. IP Adresleri: 33 33
1.3. Domain Adresleri: 34
1.4. URL'ler: 34
1.5. Araçlar (Tools) ve Teknikler: 34
2. Piramidin Anlamı ve Kullanımı: 34
3. Kullanım Alanları: 34 34
Pyramid of Pain Nasıl Çalışır? 35
1. Katmanlar Arasındaki İlişki: 35
2. Tehdit İstihbaratı ve Analiz: 35
3. Savunma Stratejilerinin Geliştirilmesi: 35 35
4. Sürekli İyileştirme ve Güncelleme: 36
Sonuç 36 36

MITRE ATT&CK

Giriş

Siber güvenlik tehditleri her geçen gün daha karmaşık hale gelirken, bu tehditlere karşı etkili bir savunma mekanizması oluşturmak kritik bir gereklilik haline gelmiştir. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber tehdit aktörlerinin saldırı yöntemlerini, tekniklerini ve taktiklerini sistematik bir şekilde belgeleyen kapsamlı bir çerçevedir.

Bu çerçeve, saldırganların sistemlere sızmak, kalıcılık sağlamak, ayrıcalıklarını yükseltmek ve nihayetinde hedeflerine ulaşmak için kullandıkları yöntemleri detaylı bir şekilde kategorize eder. MITRE ATT&CK, güvenlik uzmanlarına saldırıları analiz etme, tehdit istihbaratı oluşturma ve savunma stratejilerini geliştirme konusunda rehberlik eder. Özellikle kurumsal ağlardan bulut ortamlarına kadar geniş bir saldırı yüzeyini kapsayan bu model, hem proaktif hem de reaktif güvenlik stratejilerinde temel bir referans kaynağı olarak kullanılmaktadır.

Bu raporda, MITRE ATT&CK çerçevesinin yapısı, kullanım alanları ve siber güvenlik dünyasındaki önemi ele alınacaktır. Ayrıca, çerçevenin tehdit tespitinde nasıl kullanıldığı ve savunma stratejilerine nasıl entegre edilebileceği incelenecektir.

MITRE ATT&CK Nedir?

Siber güvenlik alanında, tehdit aktörlerinin kullandığı saldırı tekniklerini ve taktiklerini anlamak, etkili bir savunma stratejisi geliştirmek için kritik öneme sahiptir. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber saldırıların nasıl gerçekleştirildiğini sistematik bir şekilde belgeleyen bir bilgi tabanıdır. MITRE tarafından geliştirilen bu çerçeve, saldırganların hedef sistemlere sızmak, kalıcılık sağlamak, kimlik bilgilerini çalmak ve sistemleri manipüle etmek için kullandıkları yöntemleri detaylı bir şekilde kategorize eder.

MITRE ATT&CK, gerçek dünyadaki siber saldırılardan elde edilen veriler kullanılarak oluşturulmuş olup, güvenlik uzmanlarına tehditleri analiz etme, tespit etme ve bunlara karşı savunma geliştirme konusunda rehberlik eder. Günümüzde siber güvenlik ekipleri, tehdit avcılığı (*threat hunting*), olay müdahalesi (*incident response*), saldırı simülasyonları (*red teaming*) ve tehdit istihbaratı (*threat intelligence*) gibi birçok alanda MITRE ATT&CK çerçevesini kullanmaktadır.

MITRE ATT&CK çerçevesi, farklı saldırı ortamlarına göre üç ana kategoriye ayrılmıştır:

1. Enterprise ATT&CK – Kurumsal BT altyapılarını hedef alan saldırıları içerir.
2. Mobile ATT&CK – Mobil cihazlara yönelik tehditleri kapsar.
3. ICS ATT&CK – Endüstriyel kontrol sistemlerine (ICS/SCADA) yönelik saldırıları analiz eder.

Bu raporda, özellikle kurumsal sistemleri hedef alan Enterprise ATT&CK çerçevesi detaylandırılacaktır.

MITRE ATT&CK Enterprise:

MITRE ATT&CK çerçevesi, farklı saldırı ortamlarına uygun olarak çeşitli matrisler içerir. Bunlar arasında Enterprise ATT&CK, özellikle kurumsal BT altyapılarını hedef alan saldırı tekniklerini ve taktiklerini kapsayan en kapsamlı modeldir. Bu model, modern işletim sistemleri, bulut hizmetleri ve sanallaştırma platformları gibi kurumsal ortamlarda kullanılan sistemlere yönelik tehditleri analiz etmek için tasarlanmıştır.

1. Enterprise ATT&CK Yapısı:

Enterprise ATT&CK matrisi, saldırganların gerçekleştirdiği eylemleri Taktikler (Tactics), Teknikler (Techniques) ve Alt Teknikler (Sub-techniques) olarak sınıflandırır:

• Taktikler (*Why? – Neden?*): Saldırganın hedef sistemde gerçekleştirmeye çalıştığı yüksek seviyeli amaçları tanımlar. Örneğin, başlangıç erişimi elde etmek, veri sızdırmak veya savunmadan kaçmak gibi.

• Teknikler (*How? – Nasıl?*): Saldırganların belirli bir taktiği gerçekleştirmek için kullandıkları yöntemlerdir. Örneğin, kimlik bilgisi hırsızlığı (Credential Dumping) veya DLL enjeksiyonu (DLL Injection) gibi.

• Alt Teknikler: Tekniklerin daha spesifik alt yöntemlerini açıklar. Örneğin, kimlik bilgisi hırsızlığı kapsamında LSASS dump, Mimikatz kullanımı, SAM dosyası okuma gibi farklı yöntemler bulunabilir.

2. Enterprise ATT&CK Matrisinde Yer Alan Taktikler:

Enterprise ATT&CK, saldırganların hedef sistemlere yönelik gerçekleştirdiği saldırı yaşam döngüsünü tanımlamak için 14 ana taktik içerir:

1) Initial Access (Başlangıç Erişimi):

1. Initial Access Nedir?

Başlangıç erişimi, saldırganların hedef sisteme giriş yapabilmek için kullandıkları yöntemleri içerir. Bu aşama, bir saldırının başarılı olup olmayacağını belirleyebilir. Erişim sağlandıktan sonra saldırgan, ayrıcalık yükseltme (Privilege Escalation), kalıcılık sağlama (Persistence) ve yanal hareket (Lateral Movement) gibi taktiklerle sistemde daha fazla ilerleyebilir.

Saldırganlar, sistemlere erişim kazanmak için sosyal mühendislikten ağ güvenlik açıklarına kadar birçok farklı yöntemi kullanabilir. Bu süreç genellikle şu adımlardan oluşur:

1. Hedef sistem veya kullanıcı belirleme.

2. Sisteme giriş yapmak için kullanılabilecek açıkları veya zayıflıkları belirleme.

3. Kötü amaçlı yazılım veya güvenlik açıklarını kullanarak sisteme erişim sağlama.

2. Initial Access Teknikleri:

MITRE ATT&CK çerçevesinde Initial Access taktiği altında çeşitli teknikler ve alt teknikler bulunur. İşte en yaygın kullanılan saldırı teknikleri:

2.1. Phishing (Kimlik Avı) [T1566]

Açıklama:

Saldırganlar, hedefleri kandırarak kötü amaçlı bağlantılara tıklamalarını veya ekleri açmalarını sağlamak için kimlik avı (phishing) tekniklerini kullanır.

Alt Teknikler:

• T1566.001 – Spear Phishing Attachment: Hedefe kötü amaçlı ek içeren bir e-posta gönderilir.

• T1566.002 – Spear Phishing Link: Kötü amaçlı bir web sitesine yönlendiren bağlantı içeren e-posta veya mesaj gönderilir.

• T1566.003 – Spear Phishing via Service: Sosyal medya, mesajlaşma uygulamaları veya diğer hizmetler aracılığıyla yapılan kimlik avı saldırılarıdır.

2.2. Exploit Public-Facing Application (İnternete Açık Uygulamalardaki Zafiyetlerin Kullanılması) [T1190]

Açıklama:

Saldırganlar, doğrudan internete açık olan web sunucuları, e-posta sunucuları veya diğer hizmetlerde bulunan güvenlik açıklarını kullanarak sisteme erişim sağlarlar.

2.3. External Remote Services (Dış Uzaktan Erişim Hizmetleri) [T1133]

Açıklama:

Saldırganlar, VPN, RDP (Remote Desktop Protocol), SSH veya diğer uzaktan erişim hizmetlerine erişim sağlayarak sisteme giriş yapabilir.

2.4. Valid Accounts (Geçerli Hesapları Kullanma) [T1078]

Açıklama:

Saldırganlar, ele geçirilen veya çalınmış kullanıcı hesaplarını kullanarak sisteme erişim sağlar.

Alt Teknikler:

• T1078.001 – Local Accounts: Yerel sistem hesaplarını ele geçirme.

• T1078.002 – Domain Accounts: Şirket içi Active Directory hesaplarını ele geçirme.

• T1078.003 – Cloud Accounts: Bulut hizmetlerine ait hesap bilgilerini kullanma.

2.5. Supply Chain Compromise (Tedarik Zinciri Saldırısı) [T1195]

Açıklama:

Saldırganlar, bir yazılımın veya hizmetin tedarik zincirine sızarak hedef sistemlere zararlı yazılım bulaştırır.

2.6. Drive-by Compromise (Web Siteleri Üzerinden Bulaşma) [T1189]

Açıklama:

Kötü amaçlı kod içeren bir web sitesine giren kullanıcının, farkında olmadan zararlı yazılımı çalıştırmasını sağlar.

3. Initial Access Önleme Yöntemleri:

Siber güvenlik uzmanları, Initial Access aşamasını engellemek için aşağıdaki önlemleri alabilir:

🔷 Kimlik Avı Koruması

• Çalışanlara sosyal mühendislik saldırıları hakkında farkındalık eğitimi verilmeli.

• Şüpheli e-postalar ve bağlantılar otomatik olarak taranmalı.

• Multi-Factor Authentication (MFA) etkinleştirilmeli.

🔷 Ağ ve Sistem Güvenliği

• İnternete açık uygulamalar düzenli olarak güvenlik testlerinden geçirilmelidir.

• RDP ve SSH gibi hizmetler varsayılan portlarda çalıştırılmamalı, erişimleri sınırlandırılmalıdır.

• Güçlü parola politikaları ve kimlik doğrulama mekanizmaları uygulanmalıdır.

🔷 Güncellemeler ve Yama Yönetimi

• Tüm sistemler, işletim sistemleri ve yazılımlar düzenli olarak güncellenmeli.

• Bilinen güvenlik açıkları için hızlı bir şekilde yamalar uygulanmalıdır.

🔷 Gelişmiş Tehdit Tespit Yöntemleri

• SIEM ve IDS/IPS sistemleri kullanılarak ağ trafiği analiz edilmeli.

• Tehdit avcılığı (*Threat Hunting*) faaliyetleri düzenli olarak yürütülmelidir.

Initial Access, saldırı zincirindeki en kritik adımlardan biridir. Bir saldırgan sistemlere giriş yaptıktan sonra, saldırıyı ilerletmek için farklı teknikler kullanabilir. Bu yüzden, giriş noktalarının güvence altına alınması ve saldırıları tespit edecek mekanizmaların geliştirilmesi hayati önem taşımaktadır.

2) Execution (Çalıştırma):

1. Execution Nedir?

Execution, saldırganın hedef sistemde kötü amaçlı yazılım, betikler veya komutları çalıştırdığı aşamadır. Çalıştırılan kod, saldırının ilerleyen aşamalarını yönetmek, yetkileri yükseltmek veya sistemde kalıcılık sağlamak için kullanılabilir.

Bu aşama genellikle Initial Access sonrası gelir ve şu amaçlarla gerçekleştirilir:

✔ Sistemi ele geçirmek ve yönetmek

✔ Bilgi toplamak veya kötü amaçlı işlemler başlatmak

✔ Zafiyetleri tetiklemek ve saldırıyı ilerletmek

✔ Diğer aşamalara geçiş yapmak (örneğin, Persistence veya Privilege Escalation)

Bu aşamada saldırganlar, yerel veya uzaktan kod çalıştırabilir ve sistem üzerinde tam kontrol sağlamaya çalışabilir.

2. Execution Teknikleri:

MITRE ATT&CK çerçevesinde Execution aşamasında kullanılan çeşitli teknikler vardır. İşte en yaygın kullanılan yöntemler:

2.1. Command and Scripting Interpreter (Komut ve Betik Yorumlayıcıları) [T1059]

Açıklama:

Saldırganlar, komut satırı veya betik dillerini kullanarak sistemde kötü amaçlı kod çalıştırabilir.

Alt Teknikler:

• T1059.001 – PowerShell: Windows'un güçlü otomasyon aracı PowerShell kullanılarak kod çalıştırılır.

• T1059.002 – AppleScript: macOS ve iOS cihazlarında kullanılan AppleScript üzerinden saldırılar düzenlenir.

• T1059.003 – Windows Command Shell: cmd.exe kullanılarak zararlı komutlar yürütülür.

• T1059.004 – Unix Shell: bash, sh, zsh gibi Unix/Linux komut satırları üzerinden saldırılar gerçekleştirilir.

• T1059.005 – Visual Basic: Windows ortamında VBScript veya Makrolar kullanılarak kod çalıştırılır.

• T1059.006 – Python: Python betikleri çalıştırılarak sistem ele geçirilir.

• T1059.007 – JavaScript/JScript: Web tarayıcıları veya sistem komutları aracılığıyla JavaScript çalıştırılır.

Sonuç:

Execution (Çalıştırma), saldırının en kritik aşamalarından biridir çünkü saldırgan, hedef sistem üzerinde doğrudan kötü amaçlı komutları yürütmeye başlar. Bu aşamada kullanılan tekniklerin çoğu, sistem yönetim araçlarını suistimal ederek tespit edilmekten kaçınmayı amaçlar. Bu yüzden, ağ güvenliği, olay izleme ve güvenlik farkındalığı eğitimleri kritik önem taşır.

3) Persistence (Kalıcılık Sağlama) – MITRE ATT&CK

1. Persistence Nedir?

Persistence (Kalıcılık Sağlama), saldırganın hedef sistemde uzun süre erişimini korumasını sağlayan teknikleri ifade eder. Bir saldırgan, başlangıç erişimini (Initial Access) elde ettikten sonra, sistem yöneticisi fark etmeden veya bir güvenlik yazılımı tarafından temizlenmeden varlığını sürdürmek ister.

Persistence, saldırganın:

✔ Sistemin yeniden başlatılması durumunda erişimini kaybetmemesini,

✔ Kullanıcı oturumu kapansa bile kötü amaçlı yazılımın çalışmaya devam etmesini,

✔ Güvenlik güncellemelerine veya saldırının tespit edilmesine karşı direnç göstermesini sağlar.

Persistence sağlandığında, saldırgan sistem üzerinde uzun süre fark edilmeden faaliyet gösterebilir.

2. Persistence Teknikleri:

MITRE ATT&CK çerçevesinde saldırganların kalıcılık sağlamak için kullandığı çeşitli teknikler bulunmaktadır. İşte en yaygın yöntemler:

2.1. Account Manipulation (Hesap Manipülasyonu) [T1098]

Açıklama:

Saldırganlar, mevcut kullanıcı hesaplarını ele geçirerek veya yeni hesaplar oluşturarak sistemde kalıcılık sağlayabilir.

Alt Teknikler:

- T1098.001 – Yeni Kullanıcı Hesabı Açma
- T1098.002 – Yetki Seviyesini Değiştirme (Privilege Escalation)
- T1098.003 – Kullanıcı Parolasını Değiştirme

Sonuç:

Persistence (Kalıcılık Sağlama), saldırganın sistemde uzun süre kalmasını sağladığı kritik bir aşamadır. Saldırganlar, kullanıcı hesaplarını manipüle etmekten zamanlanmış görevler oluşturmaya kadar birçok teknik kullanabilir.

Bu nedenle, sistem yöneticileri ve güvenlik ekipleri, başlangıç programlarını izleyerek, olay günlüklerini inceleyerek ve güçlü kimlik doğrulama önlemleri alarak saldırıları önleyebilir.

4) Privilege Escalation (Ayrıcalık Yükseltme) – MITRE ATT&CK

1. Privilege Escalation Nedir?

Privilege Escalation (Ayrıcalık Yükseltme), saldırganın bir sistemde mevcut yetkilerini artırarak daha fazla kontrol elde etmesini sağlayan tekniktir. Başlangıç erişimini (Initial Access) sağladıktan sonra, saldırgan genellikle standart kullanıcı veya misafir hesabı gibi düşük ayrıcalıklara sahip bir erişim elde eder. Ancak saldırgan, daha fazla yetki kazanarak:

- ✓ Sistem yöneticisi (Administrator) veya root yetkileri elde edebilir,
- ✓ Kullanıcı hesaplarını yönetebilir,
- ✓ Dosya sistemine tam erişim sağlayabilir,
- ✓ Kötü amaçlı yazılımları gizlemek veya güvenlik önlemlerini devre dışı bırakmak için sistem ayarlarını değiştirebilir.

Ayrıcalık yükseltme genellikle Persistence (Kalıcılık Sağlama) ile birlikte kullanılır, çünkü saldırganın sistemde uzun süre fark edilmeden kalmasına olanak tanır.

2. Privilege Escalation Teknikleri:

MITRE ATT&CK çerçevesinde saldırganların ayrıcalık yükseltmek için kullandığı birçok teknik bulunmaktadır. İşte en yaygın yöntemler:

2.1. Exploiting Vulnerabilities (Zafiyetleri Kullanma) [T1068]

Açıklama:

Saldırganlar, işletim sistemindeki veya yüklü yazılımlardaki güvenlik açıklarını kullanarak sistemde ayrıcalıklarını yükseltebilir.

Önleme Yöntemleri:

✔ İşletim sistemleri ve yazılımlar düzenli olarak güncellenmelidir.

✔ Güvenlik açıklarını taramak için Vulnerability Scanner (Nessus, OpenVAS, etc.) kullanılmalıdır.

2.2. Credential Dumping (Kimlik Bilgilerini Ele Geçirme) [T1003]

Açıklama:

Saldırganlar, sistemde depolanan kimlik bilgilerini ele geçirerek yönetici yetkisine sahip hesapları ele geçirebilir.

Alt Teknikler:

• T1003.001 – LSASS Bellek Dökümü

• T1003.002 – SAM (Security Account Manager) Veritabanı Çıkartma

• T1003.003 – NTDS.dit Dosyasını Ele Geçirme

Önleme Yöntemleri:

✔ Windows'ta LSASS koruması (Credential Guard) etkinleştirilmelidir.

✔ Hassas bilgiler RAM'de tutulmamalı, kullanıcı oturumları düzenli olarak kapatılmalıdır.

2.3. Access Token Manipulation (Erişim Jetonu Manipülasyonu) [T1134]

Açıklama:

Windows sistemlerinde, erişim jetonları (Access Tokens), bir kullanıcının yetkilerini tanımlamak için kullanılır. Saldırgan, başka bir kullanıcının (özellikle yönetici) erişim jetonunu çalarak yetkilerini yükseltebilir.

Önleme Yöntemleri:

✔ LSA Protection (Local Security Authority Protection) etkinleştirilmelidir.

✔ Yüksek ayrıcalıklı hesaplar, düşük güvenlikli sistemlere giriş yapmamalıdır.

2.4. Scheduled Task/Job (Zamanlanmış Görevleri Kötüye Kullanma) [T1053]

Açıklama:

Saldırganlar, zamanlanmış görevleri kullanarak kötü amaçlı yazılımları yönetici yetkileriyle çalıştırabilir.

Önleme Yöntemleri:

✔ Windows'ta Task Scheduler ve Event Viewer logları düzenli olarak incelenmelidir.

✔ Linux'ta /etc/crontab dosyası ve systemctl servisleri izlenmelidir.

2.5. Kernel Exploits (Çekirdek Zafiyetleri) [T1068]

Açıklama:

Saldırganlar, işletim sisteminin çekirdeğinde bulunan güvenlik açıklarını kullanarak en yüksek yetkilere (root/SYSTEM) sahip olabilirler.

Önleme Yöntemleri:

✔ Çekirdek ve sürücüler düzenli olarak güncellenmelidir.

✔ Kernel Exploit'leri engellemek için AppArmor, SELinux gibi güvenlik modülleri etkinleştirilmelidir.

3. Privilege Escalation Önleme Yöntemleri:

Ayrıcalık yükseltme saldırılarına karşı alınabilecek güvenlik önlemleri şunlardır:

🔷 Sistem Güncellemelerini Yapın

• İşletim sistemlerini ve yazılımları güncel tutarak güvenlik açıkları kapatılmalıdır.

🔷 Minimum Yetki İlkesi (Least Privilege Principle) Uygulayın

• Kullanıcılar yalnızca gerekli yetkilere sahip olmalıdır. Yönetici hakları gereksiz kişilere verilmemelidir.

🔷 Log ve Anomali İzleme Yapın

• Windows Event Viewer, Linux syslog ve SIEM araçları (Splunk, ELK, Wazuh) ile sistem aktiviteleri izlenmelidir.

🔷 Çekirdek Güvenliğini Artırın

• Linux'ta SELinux ve AppArmor gibi güvenlik modülleri etkinleştirilmelidir.

• Windows'ta LSA Protection ve Credential Guard gibi özellikler etkinleştirilmelidir.

🔷 Kimlik Bilgilerini Koruyun

• LSASS koruması, MFA (Çok Faktörlü Kimlik Doğrulama) ve Parola Politikaları sıkılaştırılmalıdır.

Sonuç:

Privilege Escalation, saldırganların sistemde daha fazla kontrol elde etmek için kullandıkları kritik bir tekniktir. Exploit'ler, kimlik bilgisi ele geçirme yöntemleri ve erişim jetonları gibi tekniklerle yönetici yetkileri elde edebilirler.

Güvenlik önlemleri alınarak, bu tür saldırılar tespit edilebilir ve engellenebilir.

5) Defense Evasion (Savunmadan Kaçınma) – MITRE ATT&CK

1. Defense Evasion Nedir?

Defense Evasion (Savunmadan Kaçınma), saldırganların güvenlik çözümlerinden (antivirüs, EDR, IDS/IPS, güvenlik duvarları vb.) kaçınmak için uyguladığı tekniklerin genel adıdır. Saldırganlar, sistemde keşfedilmeden kalabilmek için zararlı aktivitelerini gizlemek ve güvenlik önlemlerini atlatmak zorundadır.

Bu teknikler saldırı sürecinin farklı aşamalarında kullanılabilir ve çoğu zaman Persistence (Kalıcılık Sağlama) ve Privilege Escalation (Ayrıcalık Yükseltme) ile birlikte uygulanır.

2. Defense Evasion Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların savunma mekanizmalarını aşmak için kullandığı birçok teknik bulunmaktadır. En yaygın teknikler aşağıda açıklanmıştır.

2.1. Obfuscated Files or Information (Bulanıklaştırılmış Dosyalar veya Bilgiler) [T1027]

Açıklama:

Saldırganlar, zararlı yazılımlarının veya komutlarının güvenlik yazılımları tarafından algılanmasını zorlaştırmak için çeşitli şifreleme, kodlama veya karartma (obfuscation) yöntemleri kullanır.

Önleme Yöntemleri:

✔ Dosyaların şifrelenmiş olup olmadığını tespit etmek için antivirüs ve EDR çözümleri kullanılmalıdır.

✔ SIEM ve log analiz sistemleri, şüpheli PowerShell komutlarını takip etmelidir.

2.2. Disable or Modify Security Software (Güvenlik Yazılımlarını Devre Dışı Bırakma veya Değiştirme) [T1562]

Açıklama:

Saldırganlar, sistemdeki güvenlik yazılımlarını (antivirüs, Windows Defender, EDR gibi) devre dışı bırakarak kötü amaçlı faaliyetlerinin tespit edilmesini engeller.

Önleme Yöntemleri:

✔ Yönetici hakları olmadan bu tür değişikliklerin yapılmasını önlemek için UAC ve Grup İlkesi (GPO) yapılandırılmalıdır.

✔ Antivirüs ve güvenlik duvarı logları izlenerek anormal aktiviteler tespit edilmelidir.

2.3. Process Injection (Süreç Enjeksiyonu) [T1055]

Açıklama:

Bu teknik, saldırganların kötü amaçlı kodlarını başka bir sürecin içine enjekte ederek çalıştırmasını sağlar. Böylece kötü amaçlı işlemler yasal sistem süreçleri gibi görünür ve güvenlik yazılımlarının radarından kaçabilir.

Örnek Teknikler:

• DLL Injection – Zararlı bir DLL dosyasını yasal bir süreç içinde çalıştırma.

• Process Hollowing – Mevcut bir süreci boşaltarak kendi kodunu içine enjekte etme.

• Portable Executable (PE) Injection – Zararlı bir yürütülebilir dosyanın RAM üzerinde başka bir süreç içerisine yüklenmesi.

Önleme Yöntemleri:

✔ Windows Defender Exploit Guard gibi sistem güvenlik çözümleri devreye alınmalıdır.

✔ Bellek içi analiz ve olay izleme araçları kullanılmalıdır (Sysmon, Volatility).

2.4. Rootkits Kullanımı [T1014]

Açıklama:

Rootkit'ler, sistemde düşük seviyeli (çekirdek modu) kötü amaçlı yazılımlardır. Bunlar tespit edilmesi zor olacak şekilde tasarlanmıştır ve genellikle işletim sistemi bileşenlerini değiştirerek kendilerini gizlerler.

Önleme Yöntemleri:

✔ Kernel modüllerinin yüklenmesini sınırlandırmak için Secure Boot ve Kernel Module Signing etkinleştirilmelidir.

✔ Rootkit tarayıcıları (Chkrootkit, rkhunter) düzenli olarak çalıştırılmalıdır.

2.5. Masquerading (Kılık Değiştirme) [T1036]

Açıklama:

Saldırganlar, zararlı dosya veya işlemlerini yasal sistem bileşenleri gibi göstererek tespit edilmekten kaçınırlar.

Önleme Yöntemleri:

✔ Dosya imza doğrulama (Code Signing) kullanılarak sahte sistem dosyaları tespit edilmelidir.

✔ Yasal süreçlerin imza kontrolleri düzenli olarak yapılmalıdır.

2.6. Bypass User Account Control (UAC'yi Atlatma) [T1548]

Açıklama:

Windows'ta, yüksek ayrıcalıklı işlemleri engelleyen UAC (User Account Control) mekanizması vardır. Ancak saldırganlar çeşitli yollarla bu güvenlik önlemini aşabilir.

Önleme Yöntemleri:

✔ Yalnızca yetkili kullanıcılara yönetici hakları verilmelidir.

✔ Grup İlkesi (GPO) ile UAC zorunlu hale getirilmelidir.

3. Defense Evasion Önleme Yöntemleri:

Savunmadan kaçınma tekniklerine karşı alınabilecek önlemler şunlardır:

🔷 Güvenlik Güncellemelerini Yapın

• Sistemler, güvenlik yazılımları ve sürücüler düzenli olarak güncellenmelidir.

🔷 Gelişmiş Algılama ve İzleme Kullanın

• EDR (Endpoint Detection and Response) çözümleri kullanılmalıdır.

• PowerShell logları ve işlem izleme araçları (Sysmon, SIEM) devreye alınmalıdır.

🔷 Kod İmzalama Politikaları Uygulayın

• Yalnızca imzalı ve güvenilir kodların çalışmasına izin verilmelidir.

🔷 Gizlenmiş veya Şifrelenmiş Kötü Amaçlı Kodları Analiz Edin

• Dosya analizi için VirusTotal, Any.Run, Hybrid Analysis gibi araçlar kullanılmalıdır.

Sonuç:

Defense Evasion, saldırganların tespit edilmeden sistemde kalmak için kullandıkları temel bir tekniktir. Antivirüs atlatma, rootkit kullanımı, süreç enjeksiyonu ve UAC bypass gibi çeşitli yöntemler kullanılmaktadır.

6) Credential Access (Kimlik Bilgisi Erişimi) – MITRE ATT&CK

1. Credential Access Nedir?

Credential Access (Kimlik Bilgisi Erişimi), saldırganların sistemdeki kimlik bilgilerini (kullanıcı adı, parola, erişim anahtarları, hash'ler vb.) ele geçirmek için kullandıkları teknikleri kapsar. Bu bilgiler, saldırganlara yetkili kullanıcı hesaplarını taklit etme, yetkilerini yükseltme ve ağda yanal hareket etme imkanı sağlar.

Saldırganlar, RAM, disk, kimlik doğrulama protokolleri ve yapılandırma dosyaları gibi farklı kaynaklardan kimlik bilgilerini toplayabilir.

2. Credential Access Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların kimlik bilgilerini ele geçirmek için kullandıkları tekniklerden bazıları şunlardır:

2.1. OS Credential Dumping (İşletim Sistemi Kimlik Bilgilerini Dökme) [T1003]

Açıklama:

Saldırganlar, sistemdeki parolaları veya hash'leri ele geçirmek için LSASS (Local Security Authority Subsystem Service) veya SAM (Security Account Manager) gibi bileşenlerden bilgi çekebilir.

Önleme Yöntemleri:

✔ LSASS erişimini kısıtlayın:

• Credential Guard ve LSASS Protection etkinleştirilmelidir.

✔ SAM dosyasına erişimi sınırlandırın:

• Yalnızca SYSTEM kullanıcısı bu dosyalara erişebilmelidir.

2.2. Keylogging (Tuş Kaydediciler) [T1056.001]

Açıklama:

Saldırganlar, tuş vuruşlarını kaydederek kullanıcıların yazdığı şifreleri, hassas verileri ve komutları ele geçirebilir.

Önleme Yöntemleri:

✔ Antivirüs ve EDR çözümleri ile keylogger'ları tespit edin.

✔ Sanal klavye veya iki faktörlü kimlik doğrulama (2FA) kullanarak riskleri azaltın.

2.3. Credential Stuffing (Kimlik Bilgisi Doldurma) [T1110.004]

Açıklama:

Saldırganlar, ele geçirilen kimlik bilgilerini (kullanıcı adı ve parola kombinasyonları) farklı platformlarda denemek için otomatik araçlar kullanır.

Önleme Yöntemleri:

- ✓ MFA (Multi-Factor Authentication) kullanarak ek güvenlik katmanı oluşturun.
- ✓ Şüpheli oturum açma denemelerini SIEM ile izleyin.

2.4. LLMNR & NBT-NS Poisoning (Ağ Üzerinden Kimlik Bilgilerini Ele Geçirme) [T1557.001]

Açıklama:

Windows sistemlerinde Link-Local Multicast Name Resolution (LLMNR) ve NetBIOS Name Service (NBT-NS) saldırıları, yanlış yönlendirme yaparak kullanıcıların kimlik bilgilerini ele geçirmeye yönelik saldırılardır.

Önleme Yöntemleri:

- ✓ LLMNR ve NetBIOS'u devre dışı bırakın
- ✓ NTLM kimlik doğrulamasını Kerberos ile değiştirin

2.5. Password Spraying (Şifre Spreyleme) [T1110.003]

Açıklama:

Saldırganlar, belirli bir kullanıcı hesabına sürekli farklı şifreler denemek yerine, birden fazla kullanıcı hesabına yaygın kullanılan bir şifre ile giriş yapmaya çalışır.

Önleme Yöntemleri:

- ✓ Hesap kilitleme politikaları belirleyerek başarısız giriş denemelerini sınırlayın.
- ✓ Güçlü parolalar ve 2FA kullanarak güvenliği artırın.

2.6. Browser Credential Theft (Tarayıcıdan Kimlik Bilgisi Çalma) [T1555.003]

Açıklama:

Saldırganlar, tarayıcılarda saklanan şifreleri çekerek kullanıcı hesaplarına erişim sağlamaya çalışır.

Önleme Yöntemleri:

- ✓ Tarayıcıda şifre kaydetmek yerine bir şifre yöneticisi kullanın
- ✓ Disk şifreleme ile saklanan şifreleri koruyun.

3. Credential Access Önleme Yöntemleri:

Savunma önlemlerini artırarak bu saldırıları minimize edebilirsiniz:

✅ MFA (Çok Faktörlü Kimlik Doğrulama) Kullanın

• Tek başına şifre güvenli değildir. OTP, biyometrik doğrulama gibi ek katmanlar eklenmelidir.

✅ İşletim Sistemi Güvenlik Özelliklerini Etkinleştirin

• Windows Credential Guard, Linux PAM yapılandırmaları gibi güvenlik önlemleri alınmalıdır.

✅ Şüpheli Davranışları İzleyin

• SIEM araçları ile başarısız giriş denemeleri, oturum açma saatleri ve kimlik bilgisi erişim olayları izlenmelidir.

✅ Güçlü Şifre Politikaları Uygulayın

• Kullanıcıların zayıf veya tekrar eden parolalar kullanmasını engelleyin.

✅ Antivirüs ve EDR Kullanarak Kötü Amaçlı Araçları Engelleyin

• Mimikatz, Responder, Hydra gibi araçlar tespit edilmelidir.

Sonuç:

Credential Access, saldırganların sistemde kalıcı olmasını sağlayan ve diğer saldırı tekniklerini besleyen kritik bir adımdır. Kimlik bilgisi dökme, şifre çalma, brute-force saldırıları ve tarayıcı şifreleri çalma gibi yöntemlerle gerçekleştirilebilir.

7) Discovery (Keşif) – MITRE ATT&CK

1. Discovery Nedir?

Discovery (Keşif), saldırganların bir sistem veya ağ hakkında bilgi toplamak için gerçekleştirdiği aktiviteleri kapsar. Keşif aşaması, saldırganlara hassas verilere erişme, zayıf noktaları tespit etme ve saldırıyı planlama imkanı sunar.

Bu aşama, genellikle ilk erişim (Initial Access) veya ayrıcalık yükseltme (Privilege Escalation) sonrası gerçekleşir. Saldırgan, ağdaki makineleri, kullanıcıları, güvenlik çözümlerini ve sistem yapılandırmalarını anlamaya çalışır.

2. Discovery Teknikleri:

MITRE ATT&CK çerçevesinde saldırganların keşif aşamasında kullandığı bazı teknikler şunlardır:

2.1. Account Discovery (Hesap Keşfi) [T1087]

Açıklama:

Saldırgan, sistemde hangi kullanıcı hesaplarının mevcut olduğunu belirlemeye çalışır. Bu bilgi, ayrıcalık yükseltme veya yanal hareket (Lateral Movement) için kullanılabilir.

Önleme Yöntemleri:

✔ Minimum ayrıcalık prensibi ile kullanıcıların gereksiz hesap bilgilerine erişimini kısıtlayın.

✔ SIEM (Security Information and Event Management) ile yetkisiz erişim denemelerini izleyin.

2.2. System Information Discovery (Sistem Bilgisi Keşfi) [T1082]

Açıklama:

Saldırgan, hedef sistemin işletim sistemi, donanım bilgileri ve yüklü yamalar hakkında bilgi toplar.

Önleme Yöntemleri:

✔ Gereksiz komut çalıştırma izinlerini kısıtlayın.

✔ Endpoint Detection and Response (EDR) çözümleri ile sistem bilgi toplama aktivitelerini izleyin.

2.3. Network Service Discovery (Ağ Servislerini Keşfetme) [T1046]

Açıklama:

Saldırgan, sistemde çalışan servisleri ve açık portları belirleyerek ağın güvenlik durumunu analiz eder.

Önleme Yöntemleri:

✔ Güçlü bir güvenlik duvarı yapılandırması oluşturun.

✔ Ağ trafiğini izleyerek şüpheli taramaları tespit edin.

2.4. Software Discovery (Yüklü Yazılımları Keşfetme) [T1518]

Açıklama:

Saldırgan, hedef sistemde yüklü olan yazılımları belirleyerek, potansiyel güvenlik açıklarını tespit eder.

Önleme Yöntemleri:

✔ Güncellenmemiş veya gereksiz yazılımları kaldırın.

✔ Yazılım envanterini düzenli olarak kontrol edin.

2.5. Remote System Discovery (Uzak Sistemleri Keşfetme) [T1018]

Açıklama:

Saldırgan, bir ağdaki diğer makineleri keşfetmeye çalışır. Bu bilgi, yanal hareket (Lateral Movement) için kullanılabilir.

Önleme Yöntemleri:

✔ Ağ segmentasyonu kullanarak erişimi sınırlayın.

✔ İzinsiz ağ keşif denemelerini tespit etmek için IDS/IPS kullanın.

2.6. Process Discovery (Çalışan Süreçleri Keşfetme) [T1057]

Açıklama:

Saldırgan, hedef sistemde çalışan işlemleri inceleyerek, güvenlik çözümlerini ve diğer kritik süreçleri belirler.

Önleme Yöntemleri:

✔ Sistem kaynaklarına erişimi sınırlayın.

✔ Davranışsal analiz ile şüpheli aktiviteleri tespit edin.

3. Discovery Önleme Yöntemleri:

Discovery aşamasını engellemek için aşağıdaki güvenlik önlemleri uygulanmalıdır:

✅ Minimum Yetki İlkesi

• Kullanıcıların yalnızca ihtiyaç duyduğu bilgilere erişimini sağlayarak keşif saldırılarını zorlaştırın.

✅ Ağ Segmentasyonu

• Sistemleri farklı güvenlik bölgelerine ayırarak saldırganların tüm ağa erişimini engelleyin.

✅ Loglama ve İzleme

• SIEM ve EDR çözümleri ile sistemde keşif aşamasında kullanılan komutları ve aktiviteleri izleyin.

✅ IDS/IPS Kullanımı

• Ağ tabanlı izleme sistemleri (Snort, Suricata) ile yetkisiz tarama ve keşif girişimlerini tespit edin.

Sonuç:

Discovery (Keşif), saldırganların hedef sistem veya ağ hakkında bilgi edinerek, saldırının sonraki aşamalarını planlamasına olanak tanır. Kullanıcı hesapları, ağ servisleri, çalışan süreçler ve yüklü yazılımlar gibi birçok bileşen saldırganların ilgisini çeker.

Güçlü erişim denetimleri, güvenlik izleme araçları ve ağ segmentasyonu gibi önlemler ile keşif aşamasındaki saldırıları tespit edip engellemek mümkündür.

8) Lateral Movement (Yanal Hareket) – MITRE ATT&CK

1. Lateral Movement Nedir?

Lateral Movement (Yanal Hareket), saldırganların bir ağ içinde hareket ederek, ilk erişim sağladıkları sistemden diğer sistemlere geçiş yapma süreçlerini ifade eder. Bu aşama, saldırganın ağda daha fazla yetki elde etme, hassas verilere erişme veya daha kritik sistemlere saldırma amacını taşır.

Yanal hareket, genellikle ilk erişim (Initial Access) ve ayrıcalık yükseltme (Privilege Escalation) aşamalarından sonra gerçekleşir ve saldırganlar tarafından sistemler arası geçiş yapmak için kullanılır.

2. Lateral Movement Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların yanal hareket aşamasında kullandığı bazı teknikler şunlardır:

2.1. Pass the Hash (Hash Kullanarak Kimlik Doğrulama) [T1075]

Açıklama:

Saldırgan, bir kullanıcı hesabının parolasını elde etmeden, ilgili hesapla ilişkili hash değerlerini kullanarak başka bir sisteme erişim sağlar. Bu, genellikle Windows ortamlarında yaygın bir tekniktir.

Önleme Yöntemleri:

✔ Lokal Yönetici Parola Yönetimi uygulayarak parolaları düzenli olarak değiştirin.

✔ Hesap erişimlerini sınırlandırarak parola hash’lerinin kullanılmasını zorlaştırın.

2.2. Remote Services (Uzak Servisler) [T1021]

Açıklama:

Saldırgan, uzaktan erişim sağlayarak diğer sistemlere bağlanır. Bu, genellikle RDP (Remote Desktop Protocol), SSH (Secure Shell) veya benzeri protokollerle yapılır.

Önleme Yöntemleri:

✔ Uzak erişim protokollerinin güvenliğini sağlamak için çok faktörlü kimlik doğrulama (MFA) kullanın.

✔ Güvenlik duvarı kuralları ile uzaktan erişimi sınırlayın.

2.3. Windows Admin Shares (Windows Yönetici Paylaşımları) [T1077]

Açıklama:

Saldırgan, yönetici paylaşımlarını kullanarak dosyalara erişim sağlar. Bu paylaşımlar, genellikle C$ gibi varsayılan paylaşımlardır ve yalnızca yönetici yetkisine sahip kullanıcılar tarafından erişilebilir.

Önleme Yöntemleri:

✔ Yönetici paylaşımlarını devre dışı bırakmayı ve yalnızca ihtiyaç duyulan paylaşımları açmayı düşünün.

✔ Güvenlik denetimleri ile paylaşımlara erişimi izleyin.

2.4. Credential Dumping (Kimlik Bilgisi Dökme) [T1003]

Açıklama:

Saldırgan, hedef sistemdeki kimlik bilgilerini (parolalar, hashler vb.) toplamak için çeşitli yöntemler kullanır. Bu bilgiler, yanal hareket için diğer sistemlerde kullanılabilir.

Önleme Yöntemleri:

✔ Antivirüs ve EDR çözümleri ile bu tür araçları tespit edin.

✔ Sistem güncellemeleri ve yamalar ile zayıf noktaları kapatın.

2.5. Exploitation of Remote Services (Uzak Servislerin Sömürülmesi) [T1210]

Açıklama:

Saldırgan, ağdaki zayıf hizmetleri veya açık portları kullanarak diğer sistemlere saldırır. Bu, genellikle yazılım zafiyetlerini kullanarak yapılır.

Önleme Yöntemleri:

✔ Düzenli zafiyet taramaları yaparak sistemdeki açıkları kapatın.

✔ Güvenlik duvarı ile yalnızca gerekli portların açık olmasını sağlayın.

3. Lateral Movement Önleme Yöntemleri:

Yanal hareketi engellemek için aşağıdaki güvenlik önlemleri uygulanmalıdır:

✅ Ağ Segmentasyonu

• Ağınızı farklı segmentlere ayırarak saldırganların kolayca geçiş yapmasını zorlaştırın.

✅ Güçlü Kimlik Doğrulama

• MFA gibi ek güvenlik önlemleri ile kimlik doğrulama sürecini güçlendirin.

✅ Erişim Kontrolleri

• Kullanıcıların yalnızca görevleri için gerekli sistemlere erişimi olmasını sağlayın.

✅ Loglama ve İzleme

• SIEM sistemleri ile yanal hareket girişimlerini izleyin ve loglayın.

Sonuç:

Lateral Movement (Yanal Hareket), saldırganların hedef sistemlerde daha fazla yetki elde etmek ve hassas verilere erişim sağlamak için gerçekleştirdiği kritik bir aşamadır. Pass the Hash, Uzak Servisler ve Kimlik Bilgisi Dökme gibi teknikler, bu aşamada sıkça kullanılmaktadır.

Güçlü güvenlik önlemleri, düzenli izleme ve eğitim ile yanal hareket girişimlerini engellemek mümkündür.

9) Collection (Veri Toplama) – MITRE ATT&CK

1. Collection Nedir?

Collection (Veri Toplama) aşaması, bir saldırganın hedef sistemlerdeki önemli verileri toplama sürecini ifade eder. Bu aşama, saldırganın hedef sistemlerde elde ettiği verilere erişim sağlamak amacıyla çeşitli teknikler kullanmasını içerir. Veri toplama, genellikle kimlik bilgileri, hassas dosyalar, konfigürasyon dosyaları ve gizli bilgiler gibi önemli verilerin hedef alındığı bir süreçtir.

2. Collection Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların veri toplama aşamasında kullandığı bazı teknikler şunlardır:

2.1. Data from Information Repositories (Bilgi Depolarından Veri) [T1213]

Açıklama:

Saldırganlar, sistemlerdeki dosya sistemleri veya veri tabanları gibi bilgi depolarından veri toplar. Bu, genellikle kullanıcı belgeleri, e-postalar veya diğer hassas bilgileri içerir.

Önleme Yöntemleri:

- ✔ Erişim kontrollerini sıkı tutarak sadece yetkili kullanıcıların verilere erişmesini sağlayın.
- ✔ Veri sınıflandırma ve etiketleme politikaları uygulayın.

2.2. Screen Capture (Ekran Yakalama) [T1113]

Açıklama:

Saldırgan, hedef sistemin ekran görüntülerini alarak hassas bilgileri toplar. Bu, kullanıcıların şifrelerini veya diğer gizli bilgilerini görüntülemek için kullanılabilir.

Önleme Yöntemleri:

- ✔ Ekran paylaşımını ve uzaktan erişimi sınırlayın.
- ✔ Antivirüs yazılımlarıyla ekran yakalama araçlarını tespit edin.

2.3. Clipboard Data (Panoya Erişim) [T1115]

Açıklama:

Saldırgan, kullanıcının panosunda bulunan verileri toplamak için panoya erişim sağlar. Bu, genellikle kullanıcıların kopyaladığı kimlik bilgileri veya hassas bilgiler için kullanılır.

Önleme Yöntemleri:

- ✔ Panoya erişimi kontrol eden güvenlik çözümleri kullanarak olası sızıntıları önleyin.
- ✔ Eğitimlerle kullanıcıları bilinçlendirin.

2.4. Data Staged (Veri Hazırlama) [T1074]

Açıklama:

Saldırgan, topladığı verileri daha sonraki aşamalar için saklar. Bu, verilerin hedef sistemlerden dışarı çıkarılmadan önce düzenlenmesi ve depolanması sürecidir.

Önleme Yöntemleri:

✔ Düzenli sistem denetimleri ile veri toplama ve hazırlama süreçlerini izleyin.

✔ Güvenlik duvarları ve veri kaybı önleme (DLP) çözümleri ile dışa veri akışını izleyin.

2.5. Data from Local System (Yerel Sistemden Veri) [T1005]

Açıklama:

Saldırgan, doğrudan hedef sistemdeki dosyalardan veri toplar. Bu, genellikle kritik sistem konfigürasyonları veya kullanıcı verileri gibi yerel dosyalara erişimi içerir.

Önleme Yöntemleri:

✔ Dosya erişim izinlerini sıkı tutarak hassas verilere erişimi kısıtlayın.

✔ Antivirüs yazılımlarıyla bu tür davranışları izleyin.

3. Collection Önleme Yöntemleri:

Veri toplama sürecini engellemek için aşağıdaki güvenlik önlemleri uygulanmalıdır:

✅ Erişim Kontrolü

• Verilere erişim izinlerini sıkı bir şekilde yönetin ve kullanıcıların yalnızca ihtiyaç duyduğu bilgilere erişim sağlamasını garanti edin.

✅ Veri Şifreleme

• Hassas verileri şifreleyerek, bu verilere izinsiz erişimi engelleyin.

✅ Loglama ve İzleme

• SIEM sistemleri ile veri toplama girişimlerini izleyin ve loglayın.

✅ Eğitim ve Farkındalık

• Kullanıcıları veri güvenliği ve kimlik avı saldırıları hakkında eğitin.

Sonuç:

Collection (Veri Toplama) aşaması, saldırganların hedef sistemlerden kritik bilgileri toplama sürecidir. Bilgi depolarından veri toplama, ekran yakalama ve panoya erişim gibi teknikler, bu aşamada sıkça kullanılmaktadır.

Güçlü güvenlik önlemleri ve kullanıcı eğitimi ile veri toplama girişimlerini etkili bir şekilde engellemek mümkündür.

10) Command and Control (Komuta ve Kontrol) – MITRE ATT&CK

1. Command and Control Nedir?

Command and Control (C2 veya C&C), saldırganların hedef sistemler üzerinde uzaktan kontrol sağlamasına olanak tanıyan bir aşamadır. Bu aşama, saldırganın kurban sistemlerle iletişim kurarak çeşitli komutlar göndermesine ve hedef sistemden veri almasına olanak tanır. Genellikle, bu aşama zararlı yazılımın yüklenmesinden sonra başlar ve saldırganın hedef sistem üzerinde kontrol sahibi olmasına olanak tanır.

2. Command and Control Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların C2 aşamasında kullandığı bazı teknikler şunlardır:

2.1. Application Layer Protocol (Uygulama Katmanı Protokolü) [T1071]

Açıklama:

Saldırgan, hedef sistemle iletişim kurmak için standart uygulama katmanı protokollerini (HTTP, HTTPS, DNS gibi) kullanır. Bu teknik, zararlı yazılımın tespit edilmesini zorlaştırır çünkü meşru trafik ile aynı protokoller üzerinden iletişim kurulur.

Önleme Yöntemleri:

✔ Ağ trafiğini izleyerek anormal davranışları tespit edin.

✔ Uygulama katmanı güvenlik duvarları kullanarak potansiyel tehditleri engelleyin.

2.2. Domain Generation Algorithms (Domain Üretim Algoritmaları) [T1483]

Açıklama:

Saldırgan, zararlı yazılımın kontrol sunucusuna bağlanmak için rastgele veya algoritmik olarak oluşturulan alan adlarını kullanır. Bu yöntem, C2 sunucularının tespit edilmesini zorlaştırır ve saldırganın erişimini sürdürebilir.

Önleme Yöntemleri:

✔ Alan adlarını izleyerek olağan dışı ve şüpheli alan adlarını tespit edin.

✔ Domain blacklist (yasaklı alan adı listeleri) kullanarak bilinen kötü niyetli alan adlarını engelleyin.

2.3. Non-Standard Port (Standart Olmayan Portlar) [T1571]

Açıklama:

Saldırgan, C2 iletişimini sağlamak için standart olmayan portlar kullanır. Bu, zararlı yazılımlarının ağ güvenlik cihazları tarafından tespit edilmesini zorlaştırır.

Önleme Yöntemleri:

✔ Ağ güvenlik cihazlarını kullanarak yalnızca gerekli portların açık olmasını sağlayın.

✔ Ağ trafiğini izleyerek anormal port kullanımlarını tespit edin.

2.4. Remote File Copy (Uzak Dosya Kopyalama) [T1105]

Açıklama:

Saldırgan, hedef sistemlere dosyalar kopyalamak veya zararlı yazılımlar yüklemek için uzak bağlantılar kullanır. Bu, genellikle dosya transfer protokolleri (FTP, SCP) ile gerçekleştirilir.

Önleme Yöntemleri:

✔ Dosya transferini izleyin ve yalnızca gerekli dosya transferlerine izin verin.

✔ Uzak bağlantıları sınırlayın ve gereksiz protokolleri engelleyin.

2.5. Command and Control over Web Service (Web Servisi Üzerinden Komuta ve Kontrol) [T1132]

Açıklama:

Saldırgan, meşru web servisleri kullanarak hedef sistemle iletişim kurar. Bu, saldırganın zararlı yazılımı kontrol etmesine olanak tanırken, aynı zamanda tespit edilmesini de zorlaştırır.

Önleme Yöntemleri:

✔ Web servislerine yapılan istekleri izleyin ve anormal davranışları tespit edin.

✔ Güvenlik duvarlarını kullanarak şüpheli web trafiğini engelleyin.

3. Command and Control Önleme Yöntemleri

C2 aşamasını engellemek için aşağıdaki güvenlik önlemleri uygulanmalıdır:

✅ Ağ Segmentasyonu

• Ağı bölerek zararlı yazılımların yayılmasını ve kontrolünü zorlaştırın.

✅ Güvenlik Duvarları ve IPS

• Güvenlik duvarları ve saldırı önleme sistemleri ile şüpheli trafiği engelleyin.

✅ Düzenli Güncellemeler

• Yazılım ve sistem güncellemelerini düzenli olarak yaparak bilinen güvenlik açıklarını kapatın.

✅ Eğitim ve Farkındalık

• Kullanıcılara kimlik avı saldırıları ve diğer sosyal mühendislik teknikleri hakkında eğitim verin.

Sonuç:

Command and Control (C2) aşaması, saldırganların hedef sistemler üzerinde uzaktan kontrol sağlamasını mümkün kılar. Uygulama katmanı protokolleri, domain üretim algoritmaları ve uzak dosya kopyalama gibi teknikler, bu aşamada sıkça kullanılır.

Güçlü güvenlik önlemleri ve eğitim, C2 iletişimini etkili bir şekilde engellemek için kritik öneme sahiptir.

11) Exfiltration (Veri Sızdırma) – MITRE ATT&CK

1. Exfiltration Nedir?

Exfiltration, bir saldırganın hedef sistemlerden veya ağlardan veri çalma sürecidir. Bu aşama, saldırganın hassas bilgileri ele geçirdikten sonra bunları sistemden dışarı çıkarmak için kullandığı teknikleri içerir. Veri sızdırma, genellikle kimlik bilgileri, finansal bilgiler, kişisel veriler veya şirket sırları gibi değerli bilgilerin hedef alındığı bir aşamadır.

2. Exfiltration Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların veri sızdırma aşamasında kullandığı bazı teknikler şunlardır:

2.1. Exfiltration Over Command and Control Channel (Komut ve Kontrol Kanalı Üzerinden Veri Sızdırma) [T1041]

Açıklama:

Saldırgan, komut ve kontrol (C2) kanalı üzerinden hedef sistemden veri sızdırır. Bu yöntem, zararlı yazılımın kontrolünü sürdürürken, veri transferini de gerçekleştirmeyi sağlar.

Önleme Yöntemleri:

✔ Ağ trafiğini izleyerek C2 iletişimlerini tespit edin.

✔ Şüpheli bağlantıları engellemek için güvenlik duvarları kullanın.

2.2. Exfiltration Over Alternative Protocol (Alternatif Protokol Üzerinden Veri Sızdırma) [T1048]

Açıklama:

Saldırgan, veri sızdırmak için alternatif veya alışılmadık protokoller kullanır. Bu, zararlı yazılımın standart güvenlik önlemlerinden kaçmasını sağlar.

Önleme Yöntemleri:

- ✔ Ağ trafiğini izleyerek olağandışı protokol kullanımını tespit edin.
- ✔ Güvenlik duvarlarında yalnızca gerekli olan protokollere izin verin.

2.3. Data Transfer Size Limits (Veri Transferi Boyut Sınırlamaları) [T1030]

Açıklama:

Saldırgan, veri sızdırma işlemlerini gizlemek için küçük veri parçaları halinde bilgi aktarır. Bu, normal ağ trafiği ile aynı boyutta veri transferleri gerçekleştirilerek tespit edilme olasılığını azaltır.

Önleme Yöntemleri:

- ✔ Veri transferlerini izleyin ve büyük veri transferlerini tespit edin.
- ✔ Şüpheli trafik için alarm oluşturun ve analiz yapın.

2.4. Data Staged for Exfiltration (Veri Sızdırma için Hazırlama) [T1074]

Açıklama:

Saldırgan, hedef sistemden çalınan verileri bir yere toplar ve daha sonra bu verileri sızdırmak için hazır hale getirir. Bu, verilerin birleştirilmesi veya sıkıştırılması gibi işlemleri içerebilir.

Önleme Yöntemleri:

- ✔ Dosya sistemini izleyin ve olağandışı dosya değişikliklerini tespit edin.
- ✔ Veri yedekleme ve koruma önlemleri ile önemli verilerinizi koruyun.

2.5. Scheduled Transfer (Planlı Transfer) [T1026]

Açıklama:

Saldırgan, veri sızdırma işlemlerini belirli bir zaman diliminde planlar. Bu, tespit edilme olasılığını azaltmak için zamanlama stratejileri içerir.

Önleme Yöntemleri:

✔ Ağ trafiğini izleyin ve olağan dışı zamanlarda veri transferlerini tespit edin.

✔ İzleme sistemleri kullanarak belirli zaman dilimlerinde anormal aktiviteleri takip edin.

3. Exfiltration Önleme Yöntemleri:

Veri sızdırma işlemlerini engellemek için aşağıdaki güvenlik önlemleri uygulanmalıdır:

✅ Veri Sınıflandırma ve Koruma

• Hassas verileri tanımlayın ve uygun güvenlik önlemleri ile koruyun.

✅ Ağ Segmentasyonu

• Ağı bölerek hassas verilere erişimi sınırlayın.

✅ İzleme ve Analiz

• Ağ ve sistem aktivitelerini düzenli olarak izleyin ve anormal davranışları analiz edin.

✅ Eğitim ve Farkındalık

• Kullanıcıları veri güvenliği ve sosyal mühendislik saldırıları hakkında eğitin.

Sonuç:

Exfiltration (Veri Sızdırma) aşaması, bir saldırganın hedef sistemlerden bilgi çalmak için kullandığı çeşitli teknikleri içerir. Komut ve kontrol kanalı üzerinden veri sızdırma, alternatif protokoller ve veri hazırlama gibi yöntemler, bu aşamada sıkça kullanılır.

Güçlü güvenlik önlemleri ve eğitim, veri sızdırma girişimlerini etkili bir şekilde engellemek için kritik öneme sahiptir.

12) Impact (Etkilendirme) – MITRE ATT&CK

1. Impact Nedir?

Impact (Etkilendirme), bir saldırganın hedef sistem veya ağa gerçekleştirdiği faaliyetlerin sonuçlarını ifade eder. Bu aşama, saldırganın hedefteki verileri, hizmetleri veya sistemleri manipüle etme veya yok etme niyetini içerir. Amaç, genellikle finansal kayıplar, itibarsal zararlar veya operasyonel kesintiler gibi olumsuz etkiler yaratmaktır.

2. Impact Teknikleri:

MITRE ATT&CK çerçevesinde, saldırganların etkili bir şekilde hedeflerini etkilediği bazı teknikler şunlardır:

2.1. Data Destruction (Veri Yok Etme) [T1485]

Açıklama:

Saldırgan, hedef sistemdeki verileri kalıcı olarak silerek yok eder. Bu, işletmelerin kritik verilerini kaybetmesine yol açabilir.

Önleme Yöntemleri:

- ✓ Veri yedekleme stratejileri geliştirin ve düzenli olarak yedek alın.
- ✓ Erişim kontrolleri ile kritik verilere yetkisiz erişimi engelleyin.

2.2. Data Manipulation (Veri Manipülasyonu) [T1491]

Açıklama:

Saldırgan, verileri değiştirmek veya manipüle etmek suretiyle hedef sistemin işleyişini etkiler. Bu, yanlış bilgi yayma veya sistemin doğru çalışmasını engelleme amacı taşır.

Önleme Yöntemleri:

- ✓ Veri bütünlüğü kontrolleri uygulayın.
- ✓ Erişim kontrolleri ile veri değişikliklerini izleyin.

2.3. Service Stop (Hizmet Durdurma) [T1489]

Açıklama:

Saldırgan, hedef sistemlerdeki hizmetleri durdurur veya devre dışı bırakır. Bu, işletmelerin operasyonlarını aksatabilir ve mali kayıplara yol açabilir.

Önleme Yöntemleri:

- ✓ Ağ izleme ve güvenlik sistemleri ile hizmet durdurma girişimlerini tespit edin.
- ✓ Hizmetleri yedekleme ve yeniden başlatma stratejileri oluşturun.

2.4. Account Access Removal (Hesap Erişiminin Kaldırılması) [T1531]

Açıklama:

Saldırgan, hedef sistemdeki kullanıcı hesaplarına erişimi kaldırarak kullanıcıların sisteme erişimini engeller.

Önleme Yöntemleri:

- ✓ Kullanıcı erişimlerini düzenli olarak gözden geçirin ve gereksiz hesapları silin.
- ✓ Hesap yönetim sistemlerini kullanarak erişim kontrolü sağlayın.

2.5. Resource Hijacking (Kaynak Kaçırma) [T1496]

Açıklama:

Saldırgan, hedef sistemin kaynaklarını (CPU, ağ bant genişliği vb.) kaçırarak kendi amaçları için kullanır. Bu, hedef sistemin performansını olumsuz etkileyebilir.

Önleme Yöntemleri:

✔ Ağ trafiğini izleyin ve olağandışı kaynak kullanımını tespit edin.

✔ Kaynak yönetimi ile sistem kaynaklarını optimize edin.

3. Impact Önleme Yöntemleri:

Etkilendirme girişimlerini engellemek için aşağıdaki güvenlik önlemleri uygulanmalıdır:

✅ Ağ Güvenliği

• Güçlü güvenlik duvarları ve saldırı tespit sistemleri kurarak, ağ trafiğini izleyin.

✅ Veri Yedekleme

• Verileri düzenli olarak yedekleyin ve yedeklerin güvenli bir ortamda saklanmasını sağlayın.

✅ Erişim Kontrolleri

• Kullanıcı erişimlerini sıkı bir şekilde yönetin ve gereksiz hesapları kaldırın.

✅ Eğitim ve Farkındalık

• Çalışanları, veri güvenliği ve potansiyel tehditler hakkında eğitin.

Sonuç:

Impact (Etkilendirme) aşaması, saldırganların hedef sistemlere zarar verme veya etkileme niyetlerini içerir. Veri yok etme, veri manipülasyonu ve hizmet durdurma gibi teknikler, bu aşamada yaygın olarak kullanılan yöntemlerdir.

Güçlü güvenlik önlemleri ve farkındalık eğitimi, etkilenmeyi önlemek için kritik öneme sahiptir.

3. Enterprise ATT&CK Kullanım Alanları:

MITRE ATT&CK Enterprise matrisi, birçok farklı alanda siber güvenlik uzmanları tarafından kullanılmaktadır:

• Tehdit Avcılığı (Threat Hunting): Güvenlik analistleri, mevcut tehditleri tespit etmek için ATT&CK çerçevesini kullanarak sistemlerini proaktif olarak analiz edebilirler.

• Saldırı Simülasyonları (Red Team & Blue Team): Red Team (saldırgan simülasyonları) ve Blue Team (savunma ekipleri) ATT&CK çerçevesini kullanarak sistemlerinin güvenliğini test edebilirler.

• Güvenlik Farkındalığı ve Eğitim: Siber güvenlik ekipleri, tehditleri daha iyi anlamak ve savunma stratejileri geliştirmek için bu matrisi kullanabilir.

• Tehdit İstihbaratı (Threat Intelligence): Gerçek dünya saldırılarına dayalı olarak saldırganların kullandığı teknikleri analiz etmek ve bu bilgileri güvenlik politikalarına entegre etmek.

4. ATT&CK Enterprise ve MITRE Engenuity Evaluations:

MITRE, farklı güvenlik çözümlerinin saldırıları nasıl tespit edip engelleyebildiğini ölçmek için MITRE Engenuity ATT&CK Evaluations adlı testler yapmaktadır. Bu testlerde güvenlik araçları, gerçek dünya tehditlerine karşı nasıl performans gösterdikleri açısından değerlendirilir.

5. Sonuç:

MITRE ATT&CK çerçevesi, siber tehditleri anlamak ve karşı koymak için kapsamlı bir kaynak sunmaktadır. Bu raporda, başlangıç erişiminden etkilendirmeye kadar uzanan çeşitli aşamalar ve teknikler ele alınmıştır. Her aşama, saldırganların hedef sistemlere sızma, kontrol sağlama ve nihayetinde hedefe zarar verme amacına ulaşmak için izlediği yolları ortaya koymaktadır.

1. Initial Access (Başlangıç Erişimi): Saldırganlar, hedef ağa girmek için çeşitli yöntemler kullanır; bu aşama, etkili siber saldırıların temelini oluşturur.

2. Execution (Çalıştırma): Elde edilen erişim, saldırganın kötü amaçlı yazılımlar veya komutlar çalıştırarak sistem üzerinde kontrol sağlamasını mümkün kılar.

3. Persistence (Kalıcılık Sağlama): Saldırganlar, sistemde kalabilmek için arka kapılar açar veya hizmetleri değiştirir.

4. Privilege Escalation (Ayrıcalık Yükseltme): Hedef sistemdeki yetkilerini artırarak daha fazla kontrol elde etmeye çalışırlar.

5. Defense Evasion (Savunmadan Kaçınma): Saldırganlar, tespit edilmeden kalabilmek için çeşitli teknikler kullanır.

6. Credential Access (Kimlik Bilgisi Erişimi): Hedef sistemdeki kullanıcıların kimlik bilgilerine erişim sağlamaya çalışırlar.

7. Discovery (Keşif): Hedef ağ ve sistemler hakkında bilgi toplamak amacıyla keşif faaliyetleri yürütürler.

8. Lateral Movement (Yanal Hareket): Saldırganlar, bir sistemden diğerine geçerek ağ üzerinde daha fazla kontrol sağlamaya çalışırlar.

9. Collection (Veri Toplama): Hedef sistemlerdeki kritik verileri toplamak için çeşitli yöntemler kullanırlar.

10. Command and Control (Komuta ve Kontrol): Topladıkları verileri yönetmek ve sistem üzerinde kontrol sağlamak amacıyla komuta ve kontrol altyapısı kurarlar.

11. Exfiltration (Veri Sızdırma): Hedef sistemden verileri dışarı sızdırmak için çeşitli teknikler kullanırlar.

12. Impact (Etkilendirme): Son olarak, hedef sistemlerde kalıcı zarar vermek veya sistemleri etkisiz hale getirmek için çeşitli yollar denerler.

Bu aşamalar, siber saldırganların hedeflerini etkili bir şekilde nasıl etkilediğini anlamak için kritik öneme sahiptir. Organizasyonlar, bu teknikleri ve aşamaları dikkate alarak güvenlik politikalarını güçlendirmeli, çalışanlarını eğitmeli ve olası tehditlere karşı hazırlıklı olmalıdır. Güçlü güvenlik önlemleri, veri yedekleme stratejileri ve sürekli eğitim, siber saldırılara karşı koruma sağlamak için gereklidir.

Siber güvenlik dünyası sürekli değişmektedir; bu nedenle, organizasyonların güncel kalması ve yeni tehditlere karşı adaptasyon göstermesi önemlidir. MITRE ATT&CK çerçevesi, bu değişimi takip etmek ve etkili savunmalar geliştirmek için önemli bir araçtır.

Pyramit of Pain

Giriş:

Pyramid of Pain (Acı Piramidi), siber güvenlikteki tehdit aktörlerinin tespit edilmesi ve izlenmesi konusundaki zorlukları vurgulayan bir kavramdır. David J. Bianco tarafından geliştirilen bu model, siber saldırılara karşı savunma stratejilerinin etkinliğini değerlendirmeye yardımcı olurken, tehdit aktörlerinin kullandığı tekniklerin, taktiklerin ve araçların tespit edilmesi açısından yaşanan zorlukları da açıkça ortaya koyar. Acı Piramidi, saldırganların kullandığı araçların ve tekniklerin seviyelerini farklı bir perspektiften ele alarak, daha derin ve etkili bir anlayış geliştirmeyi amaçlar. Piramidin alt kısımlarında daha genel ve yaygın tespit edilen tehditler yer alırken, üst kısımlarda daha özel ve zorlayıcı tehditler bulunmaktadır. Bu model, güvenlik analistlerine, organizasyonlarının siber güvenlik duruşunu güçlendirmek ve karşılaştıkları tehditleri daha iyi anlamak için stratejiler geliştirmelerinde rehberlik eder. Bu rapor, Pyramid of Pain kavramını derinlemesine inceleyerek, siber tehditlerin doğasını, saldırganların taktiklerini ve etkili savunma yöntemlerini ele almayı amaçlamaktadır.

Pyramid of Pain (Acı Piramidi) Nedir?

Pyramid of Pain (Acı Piramidi), siber güvenlik alanında kullanılan bir kavram olup, siber saldırganların tespit edilmesi ve analiz edilmesi açısından zorlukları anlamak için geliştirilmiş bir modeldir. Bu model, David J. Bianco tarafından ortaya konmuş ve siber tehditlerin doğasına yönelik daha derin bir anlayış geliştirmek için kullanılmıştır.

1. Piramidin Yapısı:

Pyramid of Pain, beş katmandan oluşan bir piramit şeklinde tasarlanmıştır. Bu katmanlar, saldırganların kullandığı tekniklerin ve araçların tespit edilmesinin zorluğunu ifade eder. Piramidin her bir katmanı, belirli bir tehdit türünü temsil eder:

1.1. Hash Değerleri:

• Tanım: Dosyaların kriptografik özetleri (hash) ile temsil edildiği en alt katmandır. Örneğin, bir dosyanın MD5 veya SHA256 hash değeri.

• Zorluk: Bu katmandaki tehditlerin tespiti genellikle kolaydır çünkü hash değerleri, bilinen kötü amaçlı yazılımlarla karşılaştırılarak hızlıca tanımlanabilir.

1.2. IP Adresleri:

• Tanım: Saldırganların kullandığı kötü niyetli IP adresleri bu katmanda yer alır.

• Zorluk: IP adresleri ile tehditlerin tespiti, dinamik IP kullanımı nedeniyle daha zordur; çünkü saldırganlar sıkça IP adreslerini değiştirir.

1.3. Domain Adresleri:

• Tanım: Saldırganların kontrol ettiği alan adları. Kötü niyetli yazılımlar genellikle belirli domainlere bağlanır.

• Zorluk: Alan adları da sıkça değişebilir; bu nedenle tespit edilmesi hash veya IP adreslerine göre daha karmaşık hale gelir.

1.4. URL'ler:

• Tanım: Kötü niyetli aktivitelerin gerçekleştiği belirli URL'ler.

• Zorluk: URL'ler sürekli değişir ve saldırganlar farklı teknikler kullanarak güvenlik sistemlerini atlatmaya çalışabilir. Bu da tespit sürecini zorlaştırır.

1.5. Araçlar (Tools) ve Teknikler:

• Tanım: Saldırganların kullandığı yazılımlar ve teknikler. Örneğin, belirli bir fidye yazılımı veya exploit kit.

• Zorluk: Bu katmandaki tehditlerin tespiti, daha fazla bilgi ve deneyim gerektirir. Çünkü saldırganlar özel araçlar geliştirerek tespit edilmeyi zorlaştırabilirler.

2. Piramidin Anlamı ve Kullanımı:

Pyramid of Pain, siber güvenlik profesyonellerine, tehditlerin ne kadar derin ve karmaşık olabileceğini gösterir. Piramidin alt katmanlarındaki tehditler daha kolay tespit edilebilirken, üst katmanlar daha sofistike ve gizli tehditleri temsil eder. Bu modelin ana amacı, organizasyonların tehdit istihbaratı ve savunma stratejilerini geliştirmelerine yardımcı olmaktır.

3. Kullanım Alanları:

• Tehdit İstihbaratı: Tehditleri anlamak ve analiz etmek için kullanılabilir.

• Güvenlik Politikaları: Organizasyonlar, hangi seviyedeki tehditlere daha fazla odaklanmaları gerektiğini belirleyebilir.

• Savunma Stratejileri: Savunma mekanizmaları geliştirirken, organizasyonlar piramidin üst katmanlarına odaklanarak daha etkili önlemler alabilir.

Sonuç:

Pyramid of Pain, siber tehditlerin doğasını ve saldırganların tespit edilme zorluklarını anlamak için kritik bir araçtır. Bu model, güvenlik analistlerine hangi tehditlerin daha fazla dikkat gerektirdiğini anlamalarına yardımcı olur ve organizasyonların savunma stratejilerini güçlendirmelerine katkıda bulunur.

Pyramid of Pain Nasıl Çalışır?

Pyramid of Pain (Acı Piramidi), siber güvenlikteki tehditlerin tespit edilmesi ve izlenmesi açısından önemli bir modeldir. Bu model, siber saldırganların kullandığı tekniklerin ve araçların zorluk seviyelerini anlamaya yardımcı olur. Pyramid of Pain'ın nasıl çalıştığını anlamak için aşağıdaki bileşenleri inceleyebiliriz:

1. Katmanlar Arasındaki İlişki:

Pyramid of Pain, beş katmandan oluşur: hash değerleri, IP adresleri, domain adresleri, URL'ler ve araçlar/teknikler. Bu katmanlar, tespit edilme zorluklarına göre sıralanmıştır.

• Alt Katmanlar (Hash Değerleri ve IP Adresleri): Bu katmanlar, tespit edilmesi en kolay olanlardır. Kötü amaçlı yazılımların hash değerleri veri tabanlarıyla karşılaştırılarak hızla tanımlanabilirken, IP adresleri de belirli filtreleme ve izleme yöntemleriyle tespit edilebilir.

• Üst Katmanlar (Araçlar ve Teknikler): Bu katmanlar, daha karmaşık ve gelişmiş tehditleri temsil eder. Saldırganlar, belirli bir teknik veya araç kullanarak sistemlere sızdıklarında, bu tür tehditlerin tespit edilmesi daha zordur. Genellikle, bu katmandaki tehditler daha fazla bilgi ve deneyim gerektirir.

2. Tehdit İstihbaratı ve Analiz:

Pyramid of Pain, güvenlik analistlerine tehdit istihbaratını daha etkili bir şekilde analiz etme olanağı sunar. Analistler, belirli bir katmanda yer alan tehditleri inceleyerek, hangi tehditlerin daha acil ve önemli olduğunu belirleyebilirler.

• Zaman ve Kaynak Yönetimi: Bu model, güvenlik ekiplerinin hangi tehditlere daha fazla kaynak ayırmaları gerektiğini belirlemelerine yardımcı olur. Daha zorlayıcı üst katmanlardaki tehditler, daha fazla dikkat ve kaynak gerektirdiğinden, analistler bu alana odaklanabilirler.

3. Savunma Stratejilerinin Geliştirilmesi:

Pyramid of Pain, organizasyonların savunma stratejilerini geliştirmelerine yardımcı olur. Model, hangi tür tehditlerin en yaygın olduğunu ve hangi tekniklerin kullanılabileceğini gösterir.

• Güvenlik Prosedürleri: Organizasyonlar, bu model üzerinden güvenlik politikalarını oluşturabilir. Örneğin, daha düşük katmanlardaki tehditleri düzenli olarak takip ederken, üst katmanlardaki tehditleri belirlemek için daha sofistike yöntemler geliştirebilirler.

4. Sürekli İyileştirme ve Güncelleme:

Siber tehditler sürekli olarak evrim geçirdiğinden, Pyramid of Pain modeli de güncellenmeli ve geliştirilmelidir. Güvenlik ekipleri, yeni tehditleri ve teknikleri düzenli olarak analiz ederek modelin etkinliğini artırabilir.

• Yeni Tehditlere Yanıt: Organizasyonlar, yeni ortaya çıkan tehditleri ve saldırganların kullandığı yeni araçları takip ederek, modelin üst katmanlarını güncel tutabilirler.

Pyramid of Pain, siber güvenlik alanında tehditlerin tespit edilmesi ve izlenmesi için etkili bir çerçeve sunar. Katmanlar arası ilişki, tehdit istihbaratının analizi, savunma stratejilerinin geliştirilmesi ve sürekli iyileştirme, modelin nasıl çalıştığını anlamak için kritik unsurlardır. Bu model, güvenlik analistlerine daha derin bir anlayış ve etkili savunma yöntemleri geliştirme olanağı sağlar.

Sonuç:

Pyramid of Pain (Acı Piramidi), siber güvenlik alanında önemli bir çerçeve sunarak, güvenlik analistlerine ve organizasyonlara tehditlerin tespit edilmesi ve yönetilmesi konusunda derin bir anlayış kazandırır. Model, beş katmandan oluşur: hash değerleri, IP adresleri, domain adresleri, URL'ler ve araçlar/teknikler. Bu katmanlar, saldırganların kullandığı yöntemlerin zorluk seviyelerine göre sıralandığından, güvenlik ekiplerinin hangi tehditlere odaklanmaları gerektiği konusunda net bir rehberlik sağlar.

Pyramid of Pain, siber tehditlerin dinamik doğasıyla başa çıkabilmek için gerekli stratejilerin geliştirilmesine yardımcı olur. Alt katmanlardaki tehditlerin tespiti ve analizi, genellikle daha kolayken, üst katmanlardaki tehditler daha karmaşık ve gelişmiş olduğundan, bu alanlara daha fazla dikkat ve kaynak ayrılması gerekmektedir. Bu model, organizasyonların, tehdit istihbaratı toplama ve analiz etme süreçlerini iyileştirmelerine olanak tanır. Tehditlerin zaman içinde evrim geçirdiği göz önüne alındığında, sürekli güncelleme ve iyileştirme, siber güvenlik stratejilerinin etkinliğini artırmak için kritik öneme sahiptir.

Sonuç olarak, Pyramid of Pain, siber güvenlikte etkili bir savunma ve saldırı öncesi hazırlık için vazgeçilmez bir araçtır. Bu model, sadece tehditlerin tespit edilmesine yardımcı olmakla kalmaz, aynı zamanda güvenlik ekiplerine stratejik bir perspektif kazandırarak, riskleri daha iyi anlamalarını ve bunlarla başa çıkmalarını sağlar. Organizasyonlar, bu modeli kullanarak, siber güvenlik duruşlarını güçlendirebilir ve siber tehditlerle daha etkili bir şekilde mücadele edebilirler. Bu bağlamda, Pyramid of Pain, modern siber güvenlik stratejilerinin önemli bir bileşeni haline gelmiştir ve gelecekte de bu rolünü sürdürmesi beklenmektedir.