ALTAY TAKIM GÖREVİ

Hazırlayan: Alperen Buğra AKCA

Tarih :17.02.2025

GİRİŞ

Siber tehditler günümüzde hızla gelişmekte ve saldırganlar giderek daha sofistike teknikler kullanmaktadır. Bu bağlamda, siber güvenlik uzmanlarının saldırganların yöntemlerini anlaması ve savunma stratejilerini buna göre şekillendirmesi büyük önem taşımaktadır.

Bu rapor, MITRE ATT&CK çerçevesini temel alarak siber saldırganların kullandığı taktikleri, teknikleri ve prosedürleri (TTP'ler) detaylı bir şekilde incelemektedir. MITRE ATT&CK, tehdit aktörlerinin saldırı süreçlerini analiz etmek, güvenlik açıklarını belirlemek ve saldırılara karşı daha etkili savunma mekanizmaları geliştirmek için kullanılan bir referans kaynağıdır.

Raporun amacı, MITRE ATT&CK tablosunun yapısını, önemini ve kullanım alanlarını açıklayarak siber güvenlik profesyonellerine rehberlik etmektir. Ayrıca, gerçek dünya saldırı senaryoları ve tehdit avcılığı süreçleri ele alınarak, siber güvenlik operasyonlarında nasıl daha etkin bir yaklaşım benimsenebileceği üzerinde durulacaktır.

1.MITRE ATT & CK tablosu nedir?

MITRE ATT & CK (Adversarial Taktikler, Teknikler ve Ortak Bilgi), kuruluşların güvenlik hazır olduklarını anlamalarına ve savunmalarındaki güvenlik açıklarını ortaya çıkarmalarına yardımcı olmak için MITRE Corporation tarafından geliştirilen bir çerçeve, veri matrisleri seti ve değerlendirme aracıdır.

2013 yılında geliştirilen MITRE ATT & CK Framework, belirli saldırı yöntemlerini, taktiklerini ve tekniklerini belgelemek için gerçek dünya gözlemlerini kullanır. Yeni güvenlik açıkları ve saldırı yüzeyleri ortaya çıktıkça, ATT & CK çerçevesine eklenirler, bu da sürekli olarak gelişir. Son birkaç yılda, MITRE ATT & CK çerçevesi ve matrisleri, saldırgan davranışıyla ilgili hem bilgi hem de iyileştirme araçları için bir endüstri standardı haline gelmiştir.

2. Mitre ATT&CK Tablosu Neden Önemlidir?

- Tehdit Tespiti ve Analizi: SOC analistleri ve tehdit avcıları için saldırganların davranışlarını anlamak ve izlemek kolaylaşır.
- Standart Referans: Farklı güvenlik ekipleri arasında ortak bir dil oluşturur.
- Zafiyet Tespiti: Saldırganların kullandığı tekniklere karşı savunmasız noktaları belirlemeye yardımcı olur.
- Saldırı Simülasyonu: Kırmızı takım ve mavi takım simülasyonları için ideal bir rehberdir.

3.MITRE ATT & CK Teknikleri

Teknikler, bir siber saldırının farklı aşamalarını temsil eden 11 kategori veya taktik halinde düzenlenmiştir.

Bu taktikler, kuruluşların saldırganların ağlarını veya sistemlerini tehlikeye atabilecekleri farklı yolları daha iyi anlamalarına yardımcı olmak için tasarlanmıştır. Teknikler, tehdit istihbaratını tanımlamak ve paylaşmak için ortak bir dil sağlar ve bir kuruluşun savunmasındaki güvenlik açıklarını belirleyerek ve ele alarak güvenliği artırmak için kullanılabilir.

Bu teknikler şunlardır;

- İlk Erişim(Initial Access) kimlik avı veya güvenlik açıklarından yararlanma gibi bir hedef sistem veya ağdaki ilk dayanağı elde etmek için kullanılır.
- Infaz(Execution) kötü amaçlı yazılım yükünü çalıştırmak veya kodu yürütmek için bir güvenlik açığından yararlanmak gibi bir hedef sistemde kötü amaçlı kod çalıştırmak için kullanılır.
- Kalıcılık(Persistence) yeni bir kullanıcı hesabı oluşturmak veya bir arka kapı kurmak gibi bir sistemdeki bir dayanağı korumak için kullanılır.
- Ayrıcalıklı Tırmanma(Privilege Escalation) bir güvenlik açığından yararlanma veya kimlik bilgilerini çalma gibi bir sisteme daha yüksek düzeyde erişim elde etmek için kullanılır.
- Savunma Kaçakçılığı(Defense Evasion) kod gizleme veya antivirüs kaçırma teknikleri kullanma gibi güvenlik araçları veya savunucuları tarafından tespit edilmesini önlemek için kullanılır.
- Kimlik Bilgisi Erişimi(Credential Access) parola çalmak veya kaba kuvvet saldırıları kullanmak gibi geçerli kullanıcı kimlik bilgilerini almak için kullanılır.
- Keşif(Discovery) açık bağlantı noktalarını tarama veya kullanıcı hesaplarını numaralandırma gibi bir hedef sistem veya ağ hakkında bilgi toplamak için kullanılır.
- Yanal Hareket(Lateral Movement) güvenlik açıklarından yararlanmak veya diğer sistemlere erişmek için çalıntı kimlik bilgilerini kullanmak gibi bir ağ içinde yanal olarak hareket etmek için kullanılır.
- Koleksiyon(Collection) keylogging veya ekran görüntüsü gibi bir hedef sistemden veya ağdan veri veya bilgi toplamak için kullanılır.
- Sızma(Exfiltration) hedef sistemden veya ağdan veri veya bilgileri dış kaynağa kopyalamak için kullanılır. Bu sızan veriler daha sonra istismar kanıtı veya çalmak için kullanılabilir.
- Komut ve Kontrol(Command and Control) bir bağlantıyı korumak ve uzaktan erişim aracı veya komut ve kontrol sunucusu kullanmak gibi güvenliği ihlal edilmiş bir sistem veya ağla iletişim kurmak için kullanılır.

4. TTP Nedir?

TTP, Tactics, Techniques, and Procedures (Taktikler, Teknikler ve Prosedürler) ifadesinin kısaltmasıdır:

- Taktikler: Saldırının yüksek seviyede hedefi.
- Teknikler: Bu hedeflere ulaşmak için kullanılan yöntemler.
- Prosedürler: Saldırganların teknikleri uygularken kullandığı adımlar.

TTP'ler, tehdit aktörlerinin davranışlarını anlamak ve belirlemek için kritik öneme sahiptir.

5. TTP-Based Threat Hunting ve Detection Engineering Nedir?

- TTP-Based Threat Hunting: Tehdit avcılarının, saldırganların davranış kalıplarını analiz ederek daha önce tespit edilmemiş tehditleri proaktif olarak aramasıdır. TTP odaklı tehdit avı, geleneksel imza tabanlı tespit yöntemlerinden daha gelişmiştir.
- Detection Engineering: Güvenlik ekiplerinin TTP'lere dayanarak özel tespit kuralları ve analizler geliştirmesi işlemidir. Bu süreç, sürekli iyileştirme ve saldırılara karşı daha güçlü savunma mekanizmaları oluşturmayı içerir.

6. 2022 Ukraine Electric Power Attack

Bu saldırı kampanyası, Rusya tarafından Ukrayna'ya yönelik bir elektrik şebekesi saldırısıdır.kullanılan teknikler şunlardır;

Groups --> G0034 sandworm team (Rusyanın Askeri İstihbarat Servisi)

TID

T1059: 2022 Ukrayna Elektrik Gücü Saldırısı sırasında Sandworm Ekibi, Windows Grup İlkesi'ni kullanarak bir siliciyi yaymak ve başlatmak için TANKTRAP adlı bir PowerShell yardımcı programından yararlandı.

T1543: sistem kullanıcı oturum açma bilgilerini kabul etmeye başladığında GOGETTER'ı çalıştıracak WantedBy=multi-user.target yapılandırmasını belirterek Systemd'yi GOGETTER'in kalıcılığını koruyacak şekilde yapılandırdı.

T1485: Sandworm Ekibi, eşlenen sürücüler ve fiziksel sürücü bölümlerinin yanı sıra OT yetenekleriyle ilgili dosyaları silmek için kurbanın IT ortam sistemlerine CaddyWiper'ı kurdu.

T1484: kötü amaçlı yazılımları dağıtmak ve yürütmek için Grup İlkesi Nesnelerinden (GPO'lar) yararlandı.

T1570: Sandworm Ekibi, dağıtımdan önce CaddyWiper'ın yürütülebilir msserver.exe dosyasını bir hazırlama sunucusundan yerel bir sabit sürücüye kopyalamak için bir Grup İlkesi Nesnesi (GPO) kullandı.

T1036: Sandworm Ekibi, GOGETTER kötü amaçlı yazılımını meşru veya görünüşte meşru hizmetler olarak maskelemek için Systemd hizmet birimlerinden yararlandı

T1095: Sandworm Ekibi, TLS tabanlı bir tünel içerisinde C2 iletişimlerine proxy sağladı.

T1572: Sandworm Ekibi, harici bir sunucuyla "Yamux" TLS tabanlı bir C2 kanalı oluşturmak için GOGETTER tünel açma yazılımını kullandı

T1053: Sandworm Ekibi, CaddyWiper'ı önceden belirlenen bir zamanda çalıştırmak için bir Grup İlkesi Nesnesi (GPO) aracılığıyla Zamanlanmış Görevlerden yararlandı

T1505: Sandworm Ekibi, Neo-REGEORGwebshell'i internete bakan bir sunucuya yerleştirdi.

T0895: Sandworm Ekibi, a.iso adlı bir ISO görüntüsünü SCADA sunucusu çalıştıran bir sanal makineye eşlemek için mevcut hipervizör erişimini kullandı. SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik olarak çalıştıracak şekilde yapılandırıldı ve bunun sonucunda, ISO görüntüsü üzerinde kötü amaçlı bir VBS betiği otomatik olarak yürütüldü.

T0807: Sandworm Ekibi, scilc.exe ikili dosyası aracılığıyla komutları yürütmek için MicroSCADA platformundaki SCIL-API'den yararlandı.

T0853: Sandworm Ekibi, n.bat'ı yürütmek için bir Visual Basic komut dosyası lun.vbs'yi kullanır ve ardından MicroSCADA scilc.exe komutunu çalıştırır.

T0894: Sandworm Ekibi, düşman tarafından tanımlanan bir dosya olan s1.txt'de belirtilen SCADA talimatlarının önceden tanımlanmış bir listesini göndermek için bir MicroSCADA uygulaması ikili programı scirc.exe'yi çalıştırdı. Yürütülen C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt komutu, uzak trafo merkezlerine yetkisiz komut mesajları göndermek için SCADA yazılımından yararlandı.

T0855: Sandworm Ekibi, trafo merkezlerine yetkisiz komutların gönderilmesi de dahil olmak üzere bir dizi SCADA talimatını belirlemek için MicroSCADA SCIL-API'yi kullandı.

8. Senaryo: Şirket Hacklenme Senaryosu

Adım 1: Keşif (Reconnaissance)

- Technique: Active Scanning (T1595)
- Technique: Gather Victim Network Information (T1590)

Saldırgan, şirketin ağ yapısını ve açık portları belirlemek için ağ taraması gerçekleştirir.

Adım 2: Başlangıç Erişimi (Initial Access)

- Technique: Spear Phishing Attachment (T1566.001)
- Technique: Drive-by Compromise (T1189)

Saldırgan, bir e-posta ile zararlı ek göndererek çalışanların kimlik bilgilerini ele geçirir.

Adım 3: Yanal Hareket (Lateral Movement)

- Technique: Remote Services (T1021)
- Technique: Pass the Hash (T1550.002)

Saldırgan, ele geçirdiği kimlik bilgilerini kullanarak ağdaki diğer sistemlere erişir.

Adım 4: Hak Yükseltme (Privilege Escalation)

- Technique: Exploitation for Privilege Escalation (T1068)
- Technique: Abuse Elevation Control Mechanism (T1548)

Saldırgan, yönetici haklarına erişmek için zafiyetleri kullanır.

Adım 5: Etki (Impact)

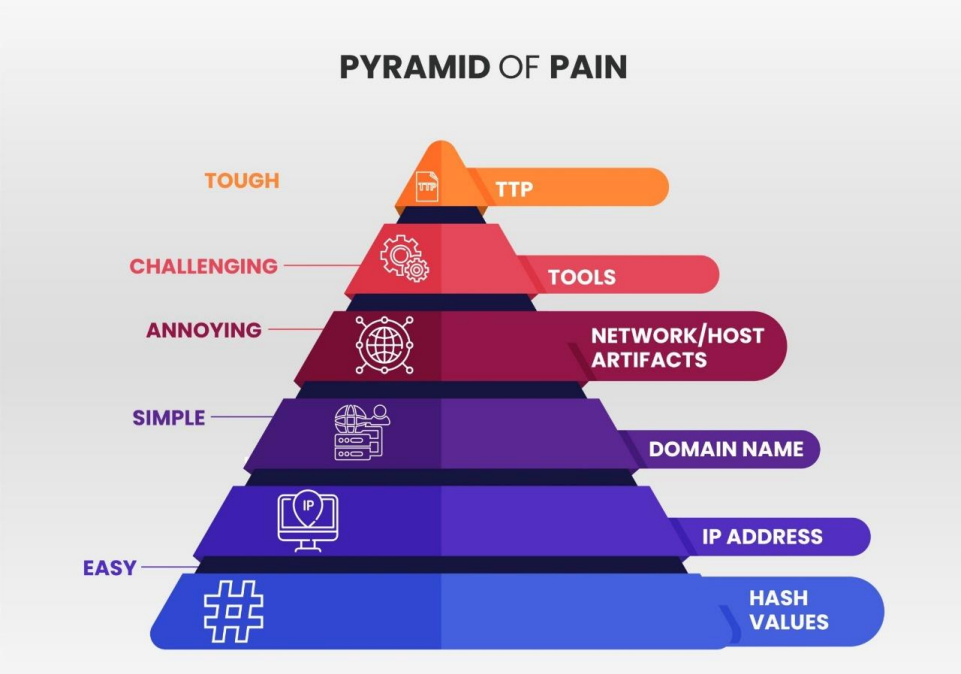
- Technique: Data Encrypted for Impact (T1486)
- Technique: Inhibit System Recovery (T1490)

Saldırgan, şirket verilerini şifreleyerek fidye talep eder ve sistem kurtarma mekanizmalarını devre dışı bırakır.

Reconnaissance	Active Scanning	T1595
	Gather Victim Network Information	T1590
Initial Access	Spear Phishing Attachment	T1566
	Drive-by Compromise	T1189
Lateral Movement	Remote Services	T1021

	Pass the Hash	T1550
Privilege Escalation	Exploitation for Privilege Escalation	T1068
	Abuse Elevation Control Mechanism	T1548
Impact	Data Encrypted for Impact	T1486
	Inhibit System Recovery	T1490

9. Pyramid of Pain Modeli Nedir?



Pyramid of Pain (Acı Piramidi), saldırganların siber saldırılar sırasında kullandıkları farklı tehdit göstergelerinin (IoC - Indicators of Compromise) önemini ve saldırıya müdahale eden ekiplere (SOC analistleri, tehdit avcıları) sağladığı zorluk derecesini gösteren bir modeldir.

Bu model, David J. Bianco tarafından geliştirilmiştir ve bir saldırıya yanıt verirken belirli göstergelere odaklanmanın saldırgan üzerindeki etkisini gösterir. Piramit, farklı katmanlardan oluşur ve her bir katman, daha üst seviyelere çıktıkça saldırgana daha fazla zarar verme potansiyeli taşır.

Hash Values(Hash değerleri): Saldırganın kullandığı zararlı örneklerine bakıldığı piramidin en altındaki seviyedir. Entegrasyonu yapılmış araçlarla MD5, SHA gibi şifrelenmiş verilerle zararlı hakkında referans sağlanır. Burada unutulmaması gereken zararlı yazılımın tek bir biti değiştirildiği takdirde bile şifre özeti değişecektir.

IP Addresses(IP adresleri): Saldırganın Tor ya da anonim Proxy sağlayıcıları, VPN'nin kullanılmış olmasına özellikle dikkat edilir. Ayrıca arka planda Threat Intellengece bir yapı kullanılması kolaylık ve daha fazla bilgi içerektir.

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

Network/Host Artifacts(Ağ/Ana bilgisayar eserleri): Normal ilerleyen ağ hareketliliği, C&C protokollerini kullanılması, HTTP isteklerinde şüpheli hareketler aranır. Saldırganın normal görünen ağ davranışları araştırılır.

Host tarafında ise dosya izinleri ve erişimleri, registry değerleri, mutex verileri, bellek dizinlerindeki zararlı olabilecek aksiyonlar aranır.

Tools(Araçlar): Saldıran tarafın amacına ve hedefine(amaç ve hedef aynı şey değildir) yönelik kullandığı yazılımlar olarak tanımlayabiliriz. Saldırganın kendine özel kullandığı ya da hedeflediği sistemde bulunan araçlarda olabilir. Zararlı dokümanlar oluşturmak, arka kapı bırakmak için ya da parola kırmak için araçlar kullanılabilir. Hedeflenen sistemde bulunan yazılımlara TOR, GCC, Powershell, Windows Task Scheduler örnek verilebilir. Bunlar kötü amaçlı yazılımlar olmasa bile şüphe uyandırmayacağı anlamına gelmez

TTP(Teknik, Taktik, Prosedürler): Bu aşamaya saldırganın Cyber Kill Chain metodolojisi demek yanlış olmaz kanımca. Saldırganın hedeflediği sisteme keşiften sızmasına kadar her aşamasındaki yöntemleridir. Zararlı kodu enjekte ettiği pdf dosyası, phishing mailleri, ZIP biçimindeki zararlı kodlar vs. kullanan saldırganın her hareketi analiz edilir. MITRE ATT&CK framework'unu kullanmak bu aşamada elzem noktalardan biridir. Saldırganı tamamıyla tanıdığımız en ağrılı aşamadır.

Sonuç

Mitre ATT&CK Framework siber güvenlik ekipleri için saldırganların davranışlarını anlamada ve tehditlere karşı daha etkili stratejiler geliştirmede kritik öneme sahiptir.

Mitre ATT&CK Framework: Taktik, teknik ve prosedürlerin (TTP'ler) sistematik olarak sınıflandırılması sayesinde tehdit aktörlerinin tüm saldırı yaşam döngüsü boyunca izlenmesine olanak tanır. Bu çerçeve, tehdit avcılığı ve saldırı tespiti süreçlerinde bir standart oluşturur.

Pyramid of Pain: Bu model, saldırılara yanıt verirken hangi tehdit göstergelerine odaklanmanın saldırganlar üzerinde daha fazla acı yaratacağını net bir şekilde ortaya koyar. Özellikle TTP'lere odaklanmak, saldırganların operasyonel yapısını bozarak saldırıları zorlaştırır.

Sonuç olarak, siber güvenlik ekiplerinin tehditleri tespit etmek ve saldırganları engellemek için TTP odaklı bir yaklaşıma geçmeleri hayati önem taşımaktadır. Bu yaklaşım, saldırıların etkili bir şekilde durdurulmasını ve gelecekteki saldırılara karşı daha güçlü bir savunma mekanizması oluşturulmasını sağlar. Siber güvenlik operasyonlarında bu iki modelin bir arada kullanılması, kurumsal güvenliğin en üst seviyeye çıkarılmasına yardımcı olacaktır.

Kaynakça:

https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e

https://www.terrabytegroup.com/pyramid-of-pain-in-cyber-security/

https://attack.mitre.org/campaigns/C0034/

https://www.broadcom.com/topics/mitre-attack

https://www.paloaltonetworks.com/cyberpedia/what-are-mitre-attack-techniques

https://sdogancesur.medium.com/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-nedir-d20f3d86541e

https://chatgpt.com/