Mitre Att&ck Framework

Hasan Karaca

16.02.2025

İÇİNDEKİLER

Giriş

Siber güvenlik tehditlerinin giderek artmasıyla birlikte kuruluşlar, tehdit aktörlerinin saldırı yöntemlerini daha iyi anlamak ve etkili savunma stratejileri geliştirmek için çeşitli güvenlik çerçevelerine başvurmaktadır. MITRE ATT&CK Framework, saldırganların kullandığı taktikleri, teknikleri ve prosedürleri (TTP) detaylı bir şekilde açıklayan, dünya çapında kabul gören bir bilgi tabanıdır. Bu rapor, framework'ün yapısını ve önemini ele alarak, tehdit avcılığı ve tespit mühendisliği bağlamında nasıl uygulanabileceğini incelemektedir. Ayrıca, **Ukraine Electric Power Attack (C0034)** analiz edilerek kullanılan teknikler incelenecek ve bir şirketin siber saldırıya uğrama süreci senaryolaştırılarak saldırganların ilerleyişi MITRE ATT&CK tablosu ile gösterilecektir.

Mitre Att&ck Framework Nedir

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework, siber güvenlik alanında saldırganların kullandığı taktikleri, teknikleri ve ortak bilgiyi tanımlamak için kullanılan bir bilgi tabanıdır. MITRE Corporation tarafından geliştirilmiştir. Framework, savunma ve saldırı taraflarına, güvenlik uzmanlarına ve siber güvenlik araştırmacılarına yardımcı olmak için tasarlanmıştır.

MITRE ATT&CK Framework'un temel amacı, savunma taraflarının saldırganların kullanabileceği taktikleri ve teknikleri anlamalarına ve siber saldırılarla mücadele ederken daha etkili olmalarına yardımcı olmaktır. Bu şekilde, güvenlik uzmanları ve kurumlar, siber saldırılara karşı daha iyi savunma stratejileri geliştirebilir ve olası saldırıları tespit ve önleme konusunda daha proaktif bir tutum alabilirler.

TTP (Tactics, Techniques, and Procedures) Nedir?

TTP, Tactics (Taktikler), Techniques (Teknikler) ve Procedures (Prosedürler) kelimelerinin baş harflerinden oluşan bir siber güvenlik terimidir. Saldırganların bir siber saldırı sırasında kullandıkları yöntemleri, araçları ve stratejileri tanımlamak için kullanılır.

1. Tactics (Taktikler):

- Saldırganların nihai amacını ifade eder.
- Örneğin, bir saldırganın amacı sistemlere yetkisiz erişim sağlamak, verileri çalmak veya fidye yazılımı yaymak olabilir.
- MITRE ATT&CK Framework'te bu taktikler "Initial Access (İlk Erişim)", "Privilege Escalation (Yetki Yükseltme)", "Exfiltration (Veri Çalma)" gibi kategorilere ayrılır.

2. Techniques (Teknikler):

- Saldırganların belirli bir taktiği gerçekleştirmek için kullandıkları yöntemlerdir.
- Örneğin, "Credential Dumping" (Kimlik Bilgisi Toplama) bir Privilege Escalation (Yetki Yükseltme) tekniğidir.

- MITRE ATT&CK'te her teknik, belirli bir saldırı türünü tanımlayan benzersiz bir kodla belirtilir.

3. Procedures (Prosedürler):

- Belirli saldırı gruplarının veya tehdit aktörlerinin teknikleri nasıl uyguladığına dair detaylı süreçleri içerir.
- Örneğin, APT29 grubu Spear Phishing Attachment (Kimlik Avı Eki) tekniğini kullanarak hedef sistemlere zararlı yazılım bulaştırabilir.
- Bu aşamada kullanılan özel araçlar, kötü amaçlı yazılım türleri ve saldırı zincirindeki adımlar belirlenir.

Kurumsal Taktikler Matrisi	
İlk Erişim (Initial Access)	Saldırgan ağınıza girmeye çalışıyor.
Çalıştırma (Execution)	Saldırgan kötü amaçlı kodu sisteme sızdırmaya çalışıyor.
Kalıcılık (Persistence)	Saldırgan, edindiği yeri korumaya çalışıyor.
Ayrıcalık Yükseltme (Privilege Escalation)	Saldırgan daha üst düzey izinler elde etmeye çalışıyor.
Savunmayı Atlatma (Defense Evasion)	Saldırgan, tespit edilmekten kaçınmaya çalışıyor.
Kimlik Bilgilerine Erişim (Credential Access)	Saldırgan hesap adlarını ve parolaları çalmaya çalışıyor.
Keşif (Discovery)	Saldırgan ortamınızı anlamaya çalışıyor.
Yanal Hareket (Lateral Movement)	Saldırgan ortamınızda gezinmeye çalışıyor.
Toplama (Collection)	Saldırgan, kendi amacına uygun verileri toplamaya çalışıyor.
Komuta ve Kontrol (Command& Control)	Saldırgan, güvenliği ihlal edilmiş sistemleri kontrol etmek için onlarla iletişim kurmaya çalışıyor.
Sızma (Exfiltration)	Saldırgan veri çalmaya çalışıyor.
Etki (Impact)	Saldırgan, sistemlerinizi ve verilerinizi manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalışıyor.

TTP Neden Önemlidir?

TTP'ler, güvenlik araştırmacıları ve tehdit avcıları için saldırgan davranışlarını anlamada kritik bir rol oynar. Siber tehdit istihbaratında TTP'lerin analiz edilmesi, saldırıların nasıl gerçekleştiğini ve nasıl önlenebileceğini belirlemeye yardımcı olur. Özellikle MITRE ATT&CK gibi tehdit modelleri, TTP'leri standartlaştırarak siber güvenlik ekiplerinin saldırılara karşı proaktif savunmalar geliştirmesine olanak tanır.

TTP-Based Threat Hunting ve Detection Engineering nedir

TTP-Based Threat Hunting ve Detection Engineering, modern siber güvenlik stratejilerinin temel bileşenlerindendir ve saldırganların taktik, teknik ve prosedürlerini (TTP) analiz ederek tehditleri tespit etmeyi amaçlar. TTP-Based Threat Hunting, geleneksel güvenlik çözümleriyle tespit edilemeyen saldırıları belirlemek için proaktif bir yaklaşım sunar. Bu yöntemde, MITRE ATT&CK Framework gibi tehdit istihbaratı kaynakları kullanılarak saldırganların izlediği yöntemler incelenir ve sistemde anomali olup olmadığı araştırılır. Tehdit avcılığı süreci, belirli bir hipotez oluşturulmasıyla başlar, ardından sistemlerden toplanan verilerin analiz edilmesiyle devam eder ve anormal aktivitelerin tespit edilmesiyle sonuca ulaşır. Elde edilen bulgular doğrultusunda, güvenlik ekipleri tehditleri etkisiz hale getirmek için hızlıca aksiyon alır.

Öte yandan, Detection Engineering, güvenlik sistemlerinin tehditleri daha etkin bir şekilde algılayabilmesi için özel tespit kuralları ve mekanizmaları geliştirme sürecidir. Bu süreçte, saldırganların MITRE ATT&CK'te tanımlanan TTP'leri analiz edilerek, SIEM, EDR ve XDR gibi güvenlik sistemlerinde özel algılama kuralları oluşturulur. Geliştirilen bu kuralların doğruluğu, saldırı simülasyonları ve testlerle değerlendirilerek optimize edilir. Detection Engineering, tehditlerin erken aşamada tespit edilmesini sağlayarak güvenlik operasyonlarının etkinliğini artırırken, yanlış pozitifleri minimize etmeye de yardımcı olur. Sonuç olarak, TTP-Based Threat Hunting ve Detection Engineering birlikte kullanıldığında, organizasyonların siber tehditlere karşı daha dayanıklı hale gelmesini sağlayan güçlü bir güvenlik yaklaşımı sunar.

MITRE ATT&CK Framework'u kimler kullanır?

- **Siber Güvenlik Uzmanları:** Siber güvenlik uzmanları, ATT&CK Framework'u kullanarak savunma stratejilerini iyileştirmek ve güvenlik açıklarını kapatmak için saldırganların kullanabileceği teknikleri ve taktikleri anlamak için kullanır.
- **Siber Güvenlik Analistleri:** Siber güvenlik analistleri, güvenlik olaylarını analiz ederken Framework'u kullanarak saldırganların iz bırakabileceği belirli tekniklerin izlerini arayabilirler.
- **Kırmızı ve Mavi Takım Uzmanları:** Kırmızı takım, kurum içindeki güvenlik açıklarını test etmek için saldırı senaryoları oluştururken ATT&CK Framework'ü kullanabilir. Mavi takım ise saldırıları tespit etmek ve müdahale etmek için Framework'den yararlanabilir.
- **Siber Tehdit İstihbaratı Analistleri:** Siber tehdit istihbaratı analistleri, saldırgan grupların belirli taktik ve tekniklerini anlamak ve izlemek için ATT&CK Framework'ü kullanabilirler.

2022 Ukraine Electric Power Attack C0034

2022 Ukrayna Elektrik Gücü Saldırısı (C0034), Sandworm Team tarafından gerçekleştirilen ve Ukrayna'daki bir elektrik hizmet sağlayıcısına yönelik bir kampanyadır. Bu saldırıda, saldırganlar GOGETTER, Neo-REGEORG, CaddyWiper gibi araçların yanı sıra sistemde mevcut araçları kullanarak (Living off the Land - LotL) SCADA sistemleri üzerinden yetkisiz komutlar göndermişlerdir.

1. Komut ve Betik Yorumlayıcısı: PowerShell (T1059.001)

Saldırganlar, TANKTRAP adlı bir PowerShell aracını kullanarak Windows Group Policy üzerinden bir wiper (silici) yaymış ve çalıştırmışlardır.

2. Sistem Süreci Oluşturma veya Değiştirme: Systemd Servisi (T1543.002)

GOGETTER'ın kalıcılığını sağlamak için Systemd yapılandırılmış ve WantedBy=multi-user.target ayarıyla sistem kullanıcı girişlerini kabul etmeye başladığında GOGETTER'ın çalışması sağlanmıştır.

3. Veri İmhası (T1485)

Saldırganlar, CaddyWiper'ı kullanarak OT (Operasyonel Teknoloji) ile ilgili dosyaları, eşlenmiş sürücüleri ve fiziksel disk bölümlerini silmişlerdir.

4. Etki Alanı veya Kiracı Politikası Değiştirme: Grup Politikası Değişikliği (T1484.001)

Grup Politikası Nesneleri (GPO) kullanılarak kötü amaçlı yazılım dağıtımı ve çalıştırılması gerçekleştirilmiştir.

5. Yanal Araç Transferi (T1570)

CaddyWiper'ın msserver.exe adlı çalıştırılabilir dosyası, bir GPO aracılığıyla bir hazırlık sunucusundan yerel diske kopyalanmıştır.

6. Kılık Değiştirme: Görev veya Servis Maskesi (T1036.004)

Systemd servis birimleri kullanılarak GOGETTER kötü amaçlı yazılımı, meşru veya meşru görünen servisler olarak gizlenmiştir.

7. Uygulama Katmanı Dışı Protokol (T1095)

Komuta ve Kontrol (C2) iletişimleri, TLS tabanlı bir tünel içinde yönlendirilmiştir.

8. Protokol Tünelleme (T1572)

GOGETTER tünelleme yazılımı kullanılarak, harici sunucularla "Yamux" TLS tabanlı C2 kanalı oluşturulmuştur.

9. Zamanlanmış Görev/İş: Zamanlanmış Görev (T1053.005)

CaddyWiper'ın belirli bir zamanda çalıştırılması için GPO aracılığıyla Zamanlanmış Görevler kullanılmıştır.

10. Sunucu Yazılım Bileşeni: Web Shell (T1505.003)

İnternete açık bir sunucuya Neo-REGEORG web shell'i yerleştirilmiştir.

11. Otomatik Çalıştırma İmajı (T0895)

Mevcut hypervisor erişimi kullanılarak, a.iso adlı bir ISO imajı SCADA sunucusu çalıştıran sanal makineye bağlanmıştır. SCADA sunucusunun işletim sistemi, CD-ROM imajlarını otomatik çalıştıracak şekilde yapılandırılmış olduğundan, ISO imajındaki kötü amaçlı VBS betiği çalıştırılmıştır.

Senaryo

1. Keşif Aşaması (Reconnaissance)

Web Sitesi Üzerinden Aktif Tarama (T1595.002)

Saldırganlar, kargo şirketine ait bir üçüncü taraf lojistik firmasının web sitesine sızarak, buradan hedef şirketin iç sistemlerine yönelik aktif taramalar gerçekleştirmiştir. Açık portlar, güvenlik duvarı yapılandırmaları ve şirketin dahili sunucuları hakkında bilgi toplanmıştır.

Çalışan Bilgilerinin Toplanması (T1589.002)

Hedef şirkette çalışan yöneticiler ve BT personeli, sosyal medya ve sızdırılmış veritabanları üzerinden araştırılmıştır. LinkedIn, GitHub ve diğer profesyonel ağlardan elde edilen bilgiler kullanılarak kimlik avı saldırısında kullanılacak hedefler belirlenmiştir.

2. İlk Erişim (Initial Access)

Kimlik Avı: Kötü Amaçlı Makro İçeren E-posta (T1566.001)

Saldırganlar, şirket çalışanlarına resmi bir gönderi bildirimine benzeyen sahte e-postalar göndermiştir. E-postada "Güncellenmiş Gönderi Listesi" başlıklı bir Excel dosyası eklenmiş ve açılması istenmiştir.

Makro Kötü Amaçlı Yazılım Yürütme (T1204.002)

Çalışan, Excel dosyasını açtığında, içindeki makrolar otomatik olarak çalışarak saldırganın uzaktan erişim sağlayabileceği bir PowerShell komutu çalıştırmıştır. Bu komut, zararlı bir yükü indirerek sistemde çalıştırmıştır.

3. Hak Yükseltme ve Kalıcılık Sağlama (Privilege Escalation & Persistence)

Yetki Yükseltme: Token Taklit Etme/Çalma (T1134)

Saldırganlar, sistemde yüksek ayrıcalıklarla işlem yapabilmek için mevcut oturum belirteçlerini ele geçirmiş ve taklit etmiştir.

Sistem Süreci Oluşturma veya Değiştirme: Zamanlanmış Görev (T1053.005)

Kötü amaçlı yazılımın her sistem açılışında çalışmasını sağlamak için Windows Zamanlanmış Görevler kullanılmıştır.

4. Komuta ve Kontrol (Command and Control)

Uygulama Katmanı Dışı Protokol (T1095)

Saldırganlar, güvenlik sistemlerinden kaçınmak için TLS tabanlı tünelleme kullanarak Komuta ve Kontrol (C2) iletişimini sürdürmüştür.

Protokol Tünelleme (T1572)

GOGETTER benzeri tünelleme yazılımları ile, şirketin güvenlik duvarını aşarak veriler saldırganlara iletilmiştir.

Etki Alanı Politikası Değiştirme: Grup Politikası Değişikliği (T1484.001)

Saldırganlar, şirket sistemlerinde kötü amaçlı yazılım yaymak için Grup Politikası Nesneleri (GPO) değiştirmiştir.

5. Son Aşama: Veri Çalma ve Sistem Manipülasyonu

Veri Manipülasyonu: Kullanıcı Bilgilerinin Değiştirilmesi (T1565.001)

Saldırganlar, sistemde kayıtlı kullanıcıların adres ve telefon numaralarını değiştirerek yanlış bilgiler eklemiş ve veri bütünlüğünü bozmuştur.

Ransomware: Veritabanı Şifreleme (T1486)

Saldırganlar, fidye yazılımı kullanarak şirketin veritabanındaki tüm bilgileri şifrelemiş ve sistemlerin kullanımını engellemiştir.

Rapor Kazanımları

Bu rapor, siber tehdit aktörlerinin saldırı süreçlerini anlamak ve savunma stratejilerini geliştirmek için MITRE ATT&CK Framework çerçevesinde gerçekleştirilen bir analiz sunmaktadır. Çalışmada, saldırganların kullandığı taktikler, teknikler ve prosedürler (TTP) detaylandırılarak, tehdit avcılığı (Threat Hunting) ve tespit mühendisliği (Detection Engineering) açısından değerlendirilmiştir. Ayrıca, Ukraine Electric Power Attack (C0034) vakası üzerinden somut bir saldırı senaryosu incelenmiş ve bir şirketin siber saldırıya uğrama süreci adım adım modellenmiştir. Senaryoda, keşif aşamasından başlayarak kimlik avı saldırıları, hak yükseltme, yanal hareket, veri çalma ve fidye yazılımı dağıtımı gibi saldırı aşamaları MITRE ATT&CK teknikleri ve TID değerleriyle ilişkilendirilmiştir. Rapor, siber güvenlik ekiplerine tehdit aktörlerinin saldırı yöntemlerini daha iyi anlama, saldırı tespit süreçlerini güçlendirme ve proaktif savunma mekanizmaları geliştirme konusunda rehberlik etmektedir.

Kaynakça

- https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e
- https://www.securefors.com/mitre-attack-framework-nedir/
- https://attack.mitre.org/campaigns/C0034/
- https://www.exclusive-networks.com/tr/wp-content/uploads/sites/32/2020/12/MITRE-ATTCK-InfoBlox-.pdf
- ChatGPT