Mitre Att&ck Framework

Hilal ŞAHİN

Şubat 2025

1. Giriş

Siber güvenlik dünyasında saldırıların daha iyi anlaşılması ve etkili bir şekilde tespit edilmesi için MITRE ATT&CK Framework, kritik bir bilgi kaynağı olarak öne çıkmaktadır. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber saldırganların operasyonlarını nasıl yürüttüğünü sistematik bir şekilde analiz eden ve belgeleyen bir çerçevedir. Bu framework, gerçek dünya saldırılarından elde edilen verileri kullanarak tehdit aktörlerinin yöntemlerini, tekniklerini ve prosedürlerini kategorize etmektedir. MITRE ATT&CK, siber tehdit istihbaratı, tehdit avcılığı, saldırı tespiti ve güvenlik analizlerinde yaygın olarak kullanılmaktadır. Bu sistem, organizasyonların siber tehditleri daha iyi anlamalarına ve güvenlik önlemlerini bu bilgilere dayalı olarak geliştirmelerine yardımcı olur. Saldırı yüzeyinin genişlediği günümüz dünyasında, siber güvenlik uzmanlarının savunma stratejilerini oluştururken saldırganların taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) anlamaları büyük önem taşımaktadır.

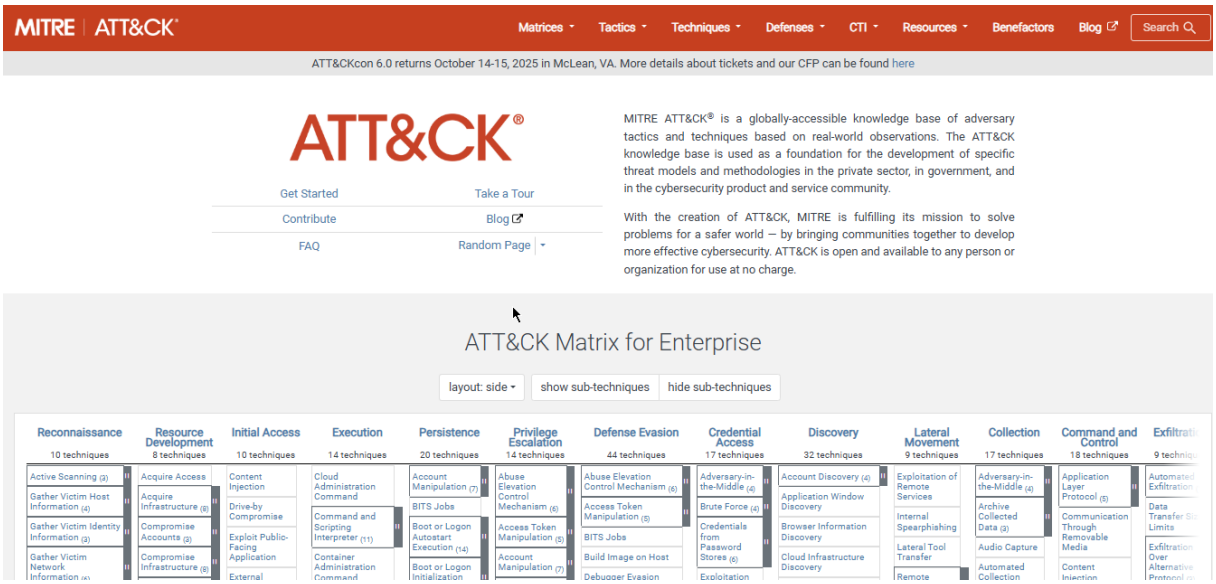
Bu rapor, MITRE ATT&CK Framework'ünün yapısını, önemini ve kullanıldığı temel alanları açıklayarak, güvenlik uzmanlarının tehditlere karşı daha bilinçli ve etkili savunma mekanizmaları geliştirmesine katkı sağlamayı amaçlamaktadır.

2. MITRE ATT&CK tablosu nedir?

MITRE ATT&CK, siber saldırganların taktiklerini, tekniklerini ve prosedürlerini tanımlayan kapsamlı bir bilgi tabanıdır. Bu çerçeve, saldırganların hedeflerine ulaşmak için kullandıkları yöntemleri sistematik bir şekilde sınıflandırır ve güvenlik profesyonellerine savunma stratejilerini geliştirmede yardımcı olur.

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 kullanacağı 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.



Şekil 1. Mittre Attack

3. MITRE ATT&CK tablosu neden önemlidir?

MITRE ATT&CK, siber güvenlik de tehdit aktörlerinin davranışlarını daha iyi anlamayı ve savunma önlemlerini güçlendirmeyi sağlar. Bu çerçeve, saldırıların nasıl gerçekleştirildiğini ve hangi tekniklerin kullanıldığını belirleyerek, güvenlik ekiplerinin tehditleri daha etkili bir şekilde tespit etmelerine ve yanıt vermelerine olanak tanır. Saldırganlarının kullandıkları yöntemleri detaylı bir şekilde saldırılara karşı önlem almasını sağlar. Güvenlik olayların analiz edilmesine ve saldırı sonrası süreçlerin yönetilmesine yardımcı olur. Siber güvenlik uzmanları için eğitim metaryeli olarak kullanılır. Tehdit avcılığı ve saldırı simülasyonları yapılmasını sağlar.

4. MITRE ATT&CK Framework'de bulunan taktik ve tekniklerin önemi nedir?

MITRE ATT&CK Framework, saldırganların sistemlere nasıl sızdığını, hangi yöntemleri kullandığını ve saldırılarını nasıl sürdürebildiğini detaylandıran bir yapı sunar. Bu framework, saldırı yaşam döngüsünü modelleyerek savunma ekiplerinin siber tehditlere karşı daha bilinçli ve proaktif olmasını sağlar.

Bu modelde taktikler, saldırganların belirli bir aşamadaki amaçlarını, teknikler ise bu amaçlara ulaşmak için kullanılan yöntemleri temsil eder.

4.1. Taktiğin Önemi

Taktikler, bir saldırının genel aşamalarını tanımlar. MITRE ATT&CK, saldırganların bir hedefe ulaşmak için izlediği taktikleri şu şekilde kategorize eder:

- **Initial Access (İlk Erişim):** Saldırganın hedef sisteme giriş yapmak için kullandığı yöntemleri içerir (örneğin, kimlik avı saldırıları veya güvenlik açıklarından yararlanma).
- **Execution (Yürütme):** Zararlı kodun sistemde çalıştırılması aşamasıdır (örneğin, PowerShell betikleri veya makrolar).
- **Persistence (Süreklilik):** Saldırganın sistemde uzun süreli varlığını korumasını sağlayan yöntemlerdir (örneğin, arka kapılar veya kayıt defteri değişiklikleri).
- **Privilege Escalation (Yetki Yükseltme):** Saldırganın, sistemde daha yüksek yetkilere sahip olmak için uyguladığı tekniklerdir.
- **Defense Evasion (Savunmadan Kaçış):** Güvenlik önlemlerini atlatmak için kullanılan yöntemleri içerir (örneğin, dosyasız kötü amaçlı yazılım teknikleri).
- **Credential Access (Kimlik Bilgisi Erişimi):** Kullanıcı adı ve parola gibi bilgilerin ele geçirilmesi için kullanılan tekniklerdir (örneğin, Mimikatz aracı ile kimlik bilgisi çalma).
- **Discovery (Keşif):** Hedef ağ veya sistem hakkında bilgi toplama aşamasıdır.
- **Lateral Movement (Yanal Hareket):** Saldırganın bir sistemden diğerine geçiş yaparak saldırıyı genişletmesi.
- **Collection (Toplama):** Hedef sistemden veri toplayarak bunları dışarı sızdırmaya hazırlama sürecidir.
- **Exfiltration (Veri Sızdırma):** Ele geçirilen verilerin saldırganın kontrol ettiği sistemlere aktarılması.
- **Impact (Etkilendirme):** Sisteme zarar verme veya operasyonları sekteye uğratma.

4.2. Tekniklerin Önemi

Her taktik, saldırganların belirli amaçlarını gerçekleştirmek için kullandıkları çeşitli tekniklerle desteklenir. MITRE ATT&CK, yüzlerce farklı saldırı tekniğini sınıflandırarak güvenlik uzmanlarının belirli tehditlere karşı daha iyi önlem almasını sağlar.

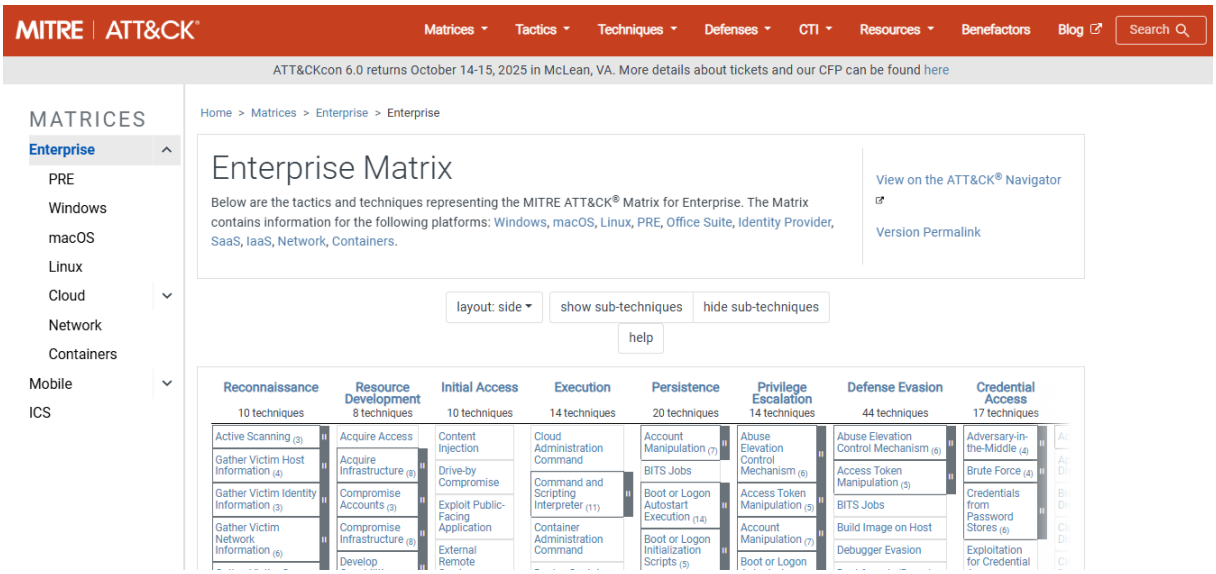
Örneğin:

- **Phishing (Kimlik Avı):** E-posta veya sahte web siteleri kullanılarak kullanıcıların kimlik bilgilerinin çalınması.
- **Process Injection (Süreç Enjeksiyonu):** Kötü amaçlı kodun yasal bir sürecin içine enjekte edilerek çalıştırılması.
- **Pass the Hash:** Kullanıcı parolasının kendisini değil, parola özetini kullanarak kimlik doğrulama gerçekleştirme yöntemi.
- **Living off the Land (LotL) Attacks:** Yasal sistem araçlarının saldırılar için kullanılması.

Bu teknikleri bilip uygulayarak güvenlik ekiplerinin hangi saldırı vektörlerini kullanıldığını anlamalarına ve saldırıların belirlenmesinde yardımcı olacaktır.

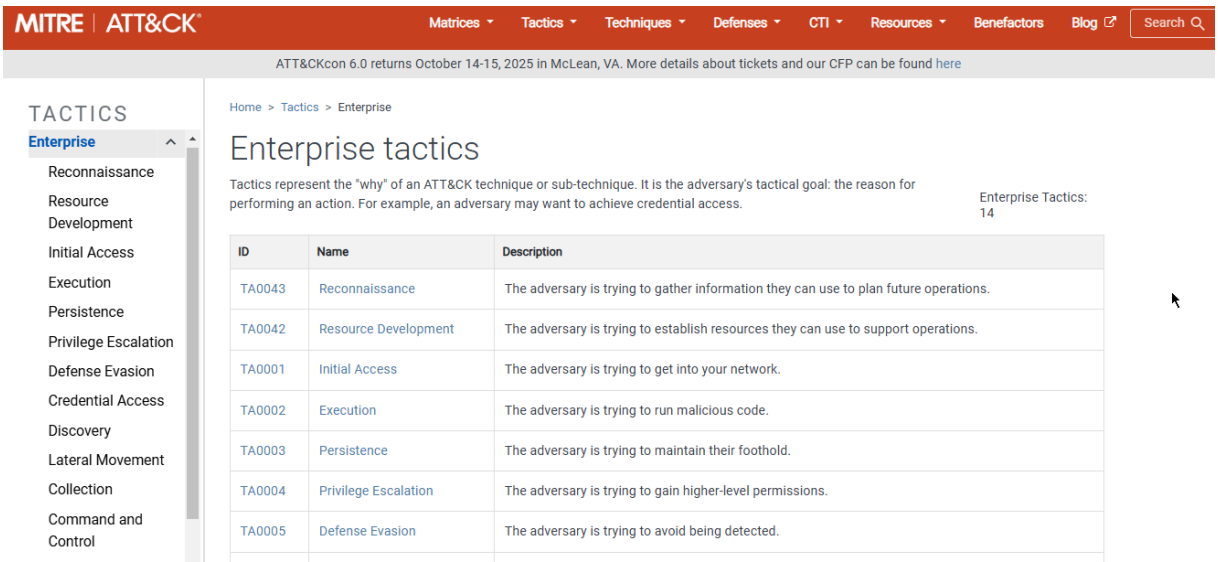
5. MITRE ATT&CK Framework'un içeriği

5.1. **Matris:** Saldırganın siber saldırıları gerçekleştirirken kullandıkları taktik ve teknikleri tablo halinde gösterir. Sütunlar taktik; satırlar ise teknikleri temsil eder.



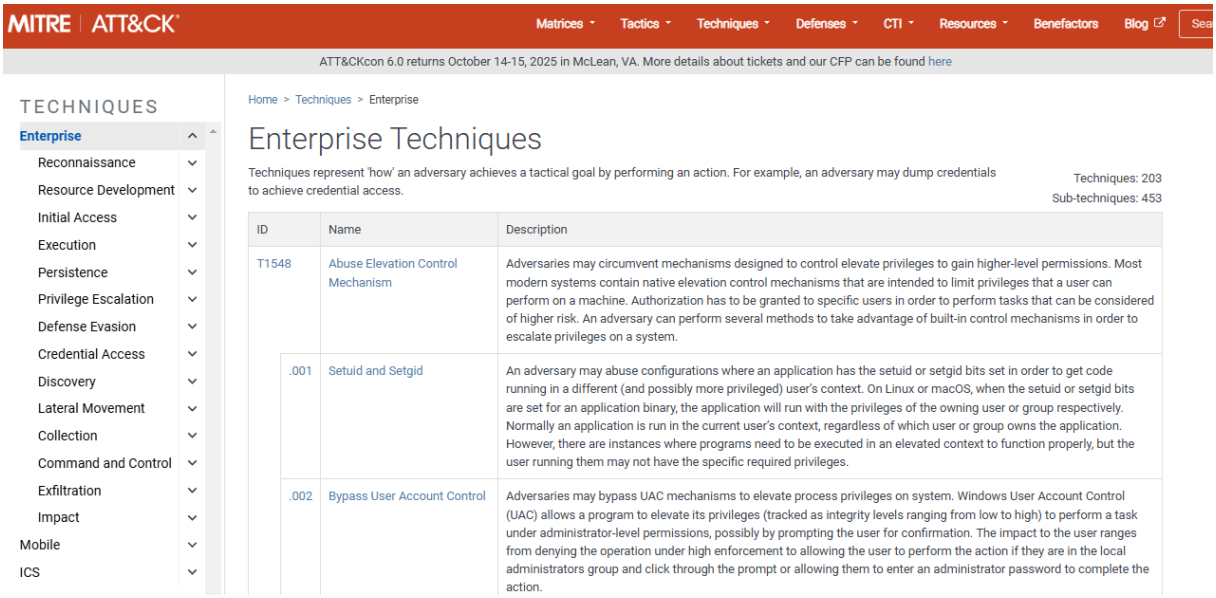
Şekil 2: Matrices

5.2. **Taktikler:** Saldırı esnasında gerçekleştirmek istedikleri genel amacı ifade eder. Taktikler, saldırının farklı aşamalarını temsil eder. Bir saldırganın amacı sisteme erişimi sağlamak istiyorsa Inital Access taktiğini kullanabilir.



Şekil 3: Tactics

5.3. **Teknikler:** Saldırı yöntemleridir. Taktiklerin altında birden fazla taktikler bulunur.



Şekil 4: Techniques

5.4. **Prosedürler:** Prosedürler, belirli bir tehdit aktörünün veya zararlı yazılımın belirli bir teknik ve taktiği nasıl uyguladığını açıklar. Örneğin, bir APT grubu kimlik avı saldırısını özel bir zararlı e-posta ek dosyasıyla gerçekleştiriyorsa, bu bir prosedür olarak adlandırılır.

6. TTP-Based Threat Hunting

TTP tabanlı tehdit avcılığı, saldırganların kullandığı bilinen taktikler, teknikler ve prosedürleri keşfetmeye yönelik aktif bir güvenlik yaklaşımıdır. Burada amaç, saldırganların geçmişte kullandığı yolları ve davranışları belirleyerek, bu davranışları bir tehdit avcılığı sürecinde tespit etmek ve önlem almaktır. Bu, sürekli bir gözlem, analiz ve sistematik araştırma gerektirir.

Proaktif Yaklaşım: TTP tabanlı tehdit avcılığı, yalnızca alarm verildiğinde değil, sistemdeki potansiyel tehditleri önceden tespit etmek amacıyla yapılır.

Veri Toplama ve Analiz: Saldırganların kullandığı tekniklerin izlerini araştırarak, sistemde anormallikleri tespit etmek için log verileri, ağ trafiği ve diğer güvenlik verileri toplanır.

Saldırı Zinciri: Her bir saldırının başlangıcından sona kadar nasıl geliştiği, genellikle bir saldırı zinciri olarak izlenir. TTP tabanlı tehdit avcılığı bu zincirin her aşamasını kontrol etmeye çalışır.

7. Detection Engineering

Detection Engineering (Tespit Mühendisliği), güvenlik olaylarını doğru bir şekilde tanımlamak ve tespit etmek için algoritmalar, sistemler ve araçlar geliştiren bir süreçtir. Bu süreç, tehdit avcılığı için gerekli olan verileri analiz etmek ve tehditleri hızlı bir şekilde tanımak için tespit mekanizmaları oluşturur.

Algoritmalar ve Kural Tabanlı Tespit: Saldırıların erken tespiti için log verileri üzerinde özel algoritmalar veya kurallar geliştirilir.

Anomali Tespiti: Tespit mühendisliği, anomali tespiti yaparak olağan dışı davranışları ortaya çıkarabilir. Bu, TTP'lerin belirli sistemlerde nasıl işlediğini anlamakla mümkündür.

Altyapı İyileştirmeleri: Tespit mühendisliği, tehditlerin etkisini en aza indirmek için güvenlik altyapısını güçlendirmek amacıyla sistem iyileştirmeleri de yapar.

8. 2022 Ukrayna Elektrik Gücü Saldırısı

Sandworm grubunun enerji altyapısını hedef alarak elektrik şebekelerinde kesintiye yol açmaya çalıştığı bir siber saldırı gerçekleşmiştir. Saldırıda kullanılan bazı teknikler:

1. **T1059 (PowerShell)**: PowerShell ile kötü amaçlı yazılımlar dağıtıldı.
2. **T1543 (Systemd Service)**: GOGETTER yazılımı, kalıcılık sağlamak amacıyla kullanıldı.
3. **T1485 (Veri Yok Etme)**: CaddyWiper kullanılarak sistem verileri yok edildi.
4. **T1484.001 (Group Policy Modification)**: Grup politikaları aracılığıyla kötü amaçlı yazılımlar yayıldı.
5. **T1570 (Yanıt Araçlarıyla Geçiş)**: Ağ üzerinden kötü amaçlı yazılım transferi sağlandı.

9. Senaryo

Stars Şirketi, büyük bir finans kuruluşudur. Son zamanlarda artan siber tehditlerle karşı karşıyadır. Tehdit aktörleri, şirketin hassas verilerini ele geçirmek amacıyla sistemlerine sızmayı planlamaktadır. Bu saldırıyı gerçekleştiren tehdit aktörleri arasında APT33 (Elfin) veya OilRig gibi Orta Doğu'da faaliyet gösteren grupların benzer yöntemleri kullandığı bilinmektedir. Aşağıda, saldırganların izlediği adımları içeren detaylı bir senaryo bulunmaktadır.

1. Reconnaissance (Keşif) [TA0043]

Saldırganlar, XYZ Şirketi hakkında bilgi toplamak için çeşitli keşif tekniklerini kullanırlar.

- **Teknik 1:** Harici Bilgi Toplama (T1590)

    - Saldırganlar, şirketin web sitesini, sosyal medya hesaplarını ve çalışanların LinkedIn profillerini inceleyerek organizasyon yapısını, kullanılan teknolojileri ve çalışan e-posta adreslerini belirler.
- **Teknik 2:** Açık Kaynak Araştırması (OSINT) (T1592)
    - Shodan ve Google Dorking gibi araçları kullanarak, şirkete ait açık portlar ve savunmasız sunucular tespit edilir.

2. Initial Access (İlk Erişim) [TA0001]

Saldırganlar, şirketin ağına sızmak için ilk erişim tekniklerini uygular.

- **Teknik 1:** Kimlik Avı (Phishing) (T1566)
    - Şirket çalışanlarına sahte e-postalar gönderilerek kötü amaçlı bağlantılara tıklamaları sağlanır.
- **Teknik 2:** Zafiyet İstismarı (Exploit Public-Facing Application) (T1190)
    - Şirketin dışa açık bir web uygulamasındaki güvenlik açığından yararlanarak uzaktan kod yürütme gerçekleştirilir.

3. Privilege Escalation (Yetki Yükseltme) [TA0004]

İlk erişimi elde eden saldırganlar, sistemde daha yüksek yetkilere ulaşmaya çalışır.

- **Teknik 1:** Erişim Token Çalma (Steal Access Token) (T1134)
    - Çalışanların kimlik doğrulama token'ları ele geçirilerek yönetici hakları elde edilir.
- **Teknik 2:** Zayıf Parola Kullanımı (T1078)
    - Ele geçirilen kimlik bilgileri kullanılarak sistem yöneticisi hesaplarına erişim sağlanır.

4. Lateral Movement (Yanal Hareket) [TA0008]

Yetki yükseltme işlemi başarılı olduktan sonra saldırganlar, şirket içindeki diğer sistemlere yayılmaya başlar.

- **Teknik 1:** Uzak Masaüstü Protokolü (RDP) Kullanımı (T1021)
    - Ele geçirilen kimlik bilgileriyle, RDP kullanılarak diğer sunuculara bağlanılır.
- **Teknik 2:** SMB Üzerinden Komut Yürütme (T1021.002)
    - SMB protokolü üzerinden zararlı yazılım yüklenerek sistemler arasında hareket edilir.

4. Lateral Movement (Yanal Hareket) [TA0008]

Yetki yükseltme işlemi başarılı olduktan sonra saldırganlar, şirket içindeki diğer sistemlere yayılmaya başlar.

- **Teknik 1:** Uzak Masaüstü Protokolü (RDP) Kullanımı (T1021)
    - Ele geçirilen kimlik bilgileriyle, RDP kullanılarak diğer sunuculara bağlanılır.
- **Teknik 2:** SMB Üzerinden Komut Yürütme (T1021.002)
    - SMB protokolü üzerinden zararlı yazılım yüklenerek sistemler arasında hareket edilir.

5. Exfiltration (Veri Sızdırma) [TA0010]

Saldırganlar, ele geçirilen hassas verileri dışarı çıkarmak için veri sızdırma tekniklerini kullanır.

- **Teknik 1:** Şifrelenmiş Kanal Kullanımı (T1048.002)
    - Çalınan veriler, tespit edilmemek için şifrelenmiş VPN veya TOR ağı üzerinden dışarı aktarılır.
- **Teknik 2:** Bulut Depolama Hizmetleri Kullanımı (T1567.002)
    - Google Drive veya Dropbox gibi bulut hizmetlerine yüklenerek veriler çalınır.

Taktik (Tactic)	Teknik (Technique)	TID (Technique ID)
Reconnaissance (Keşif)	Harici Bilgi Toplama	T1590
	Açık Kaynak Araştırması (OSINT)	T1592
Initial Access (İlk Erişim)	Kimlik Avı (Phishing)	T1566
	Zafiyet İstismarı	T1190
Privilege Escalation (Yetki Yükseltme)	Erişim Token Çalma	T1134
	Zayıf Parola Kullanımı	T1078
Lateral Movement (Yanal Hareket)	Uzak Masaüstü Protokolü (RDP) Kullanımı	T1021
	SMB Üzerinden Komut Yürütme	T1021.002
Exfiltration (Veri Sızdırma)	Şifrelenmiş Kanal Kullanımı	T1048.002
	Bulut Depolama Hizmetleri Kullanımı	T1567.002
Command and Control (Komuta ve Kontrol)	Zararlı Yazılımın C2 Sunucusu ile Haberleşmesi	T1105
	Güvenlik Araçlarını Devre Dışı Bırakma	T1562

Tablo 1: Mittre Attack Teknik ve Taktikler

Sonuç olarak senaryoda, saldırgan keşif sırasından başlayarak farklı teknik ve taktikler ile şirkete sızmıştır. C2 altyapısı ile sistemde uzun süre kalmayı başarmıştır. Bunun gibi saldırılara karşı korunmak için güçlü kimlik doğrulama sistemleri, anomali tespiti ve güvenlik farkındalık eğitimleri kritik öneme sahiptir.

10.Kaynakça

https://attack.mitre.org/

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

https://www.exclusive-networks.com/tr/wp-content/uploads/sites/32/2020/12/MITRE-ATTCK-InfoBlox-.pdf