MITRE ATT&CK Framework

Hazırlayan: Berra Söyler
Tarih: 14.02.2025

İçindekiler

1.Giriş

Günümüz dijital dünyasında siber saldırılar giderek daha karmaşık hale gelmekte ve güvenlik ekiplerinin saldırganların yöntemlerini anlamadan etkili savunmalar geliştirmesi neredeyse imkânsız hale gelmektedir. Bu noktada, **MITRE ATT&CK Framework** siber tehdit aktörlerinin kullandığı taktik, teknik ve prosedürleri (TTP) detaylandırarak güvenlik uzmanlarına güçlü bir rehber sunmaktadır.

Bu rapor, **MITRE ATT&CK**'in temel yapısını, neden önemli olduğunu ve siber güvenlik alanında nasıl kullanıldığını ele almaktadır. Özellikle **TTP odaklı tehdit avcılığı (Threat Hunting) ve saldırı tespit mühendisliği (Detection Engineering)** gibi kritik konulara değinilerek, tehditleri daha iyi anlamak ve etkili bir savunma stratejisi oluşturmak için gerekli bilgiler sunulmuştur. Siber güvenlik ekiplerinin saldırılara karşı daha hazırlıklı olması, olay müdahale süreçlerini hızlandırması ve tehditleri proaktif bir şekilde tespit edebilmesi adına MITRE ATT&CK Framework'ün sunduğu fırsatlar detaylı bir şekilde incelenmiştir.

2. MITRE ATT&CK Tablosu

2.1 MITRE ATT&CK Nedir?

MITRE ATT&CK, gerçek dünya gözlemlerine dayalı olarak, siber tehdit aktörlerinin kullandığı taktikleri, teknikleri ve prosedürleri küresel ölçekte erişilebilir hale getiren bir bilgi tabanıdır. Özel sektör, hükümet kurumları ve siber güvenlik alanındaki araştırmacılar tarafından; tehdit modelleri geliştirmek, saldırı metodolojilerini analiz etmek ve güvenlik önlemlerini güçlendirmek amacıyla bir temel olarak kullanılır. MITRE ATT&CK, siber saldırıların aşamalarını sistematik bir şekilde inceleyerek, savunma stratejilerinin geliştirilmesine yardımcı olur.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

2.2 MITRE ATT&CK Neden Önemlidir?

Özel sektör, hükümet kurumları ve siber güvenlik araştırmacıları, gerçek dünyadaki saldırı örneklerini analiz edip taktik, teknik ve prosedürlere (TTP) göre sınıflandırmak için MITRE ATT&CK Framework'ten büyük ölçüde faydalanmaktadır. Bu framework, siber tehditlerin sistematik bir şekilde incelenmesini sağlayarak saldırıların daha iyi anlaşılmasına ve etkili savunma stratejilerinin geliştirilmesine yardımcı olur. Ayrıca, gerçekleşen saldırıların MITRE ATT&CK terminolojisi ve başlıkları doğrultusunda raporlanması, güvenlik uzmanları için ortak bir dil oluşturur. Bu sayede olay müdahale ekipleri ve analistler, tehditleri daha hızlı değerlendirebilir, alınması gereken önlemleri standart bir çerçevede belirleyebilir ve saldırıları anlık olarak analiz ederek etkili bir yanıt süreci yürütebilir.

3. TTP Nedir?

TTP (Taktikler, Teknikler ve Prosedürler), tehdit aktörlerinin saldırı sırasında izlediği yolları tanımlayan bir terimdir.

3.1 Taktikler

Taktikler, saldırganların bir sistemi ele geçirmek veya belirli bir hedefe ulaşmak için izlediği genel stratejilerdir. MITRE ATT&CK çerçevesinde her saldırı belirli bir taktik altında sınıflandırılır ve bu sayede güvenlik analistleri tehditlerin hangi aşamalarda gerçekleştiğini anlayabilir.

Örneğin, bir saldırganın hedef sistemden hassas verileri alıp dışarıya sızdırması, **"Veri Sızdırma (Exfiltration)"** taktiği kapsamında değerlendirilir. Benzer şekilde, bir saldırganın bir sisteme ilk kez erişim sağlamak için çalışanlara kimlik avı (phishing) e-postaları göndermesi **"İlk Erişim (Initial Access)"** taktiğinin bir parçasıdır.

3.2 Teknikler

Teknikler, saldırganların belirli bir taktiği gerçekleştirmek için kullandığı yöntemlerdir. Bir saldırının sadece amacı (taktik) değil, bu amaca ulaşmak için kullanılan yöntemleri(teknikler) de önemlidir. MITRE ATT&CK, her taktiğin altında farklı teknikleri listeleyerek saldırıların nasıl gerçekleştirildiğini detaylandırır.

Örneğin, bir saldırgan sistemden veri çalmak istiyorsa ,ki bu **"Veri Sızdırma (Exfiltration)"** taktiğine girer, bunu gerçekleştirmek için çeşitli teknikler kullanabilir. USB bellekle hassas dosyaları kopyalamak **"Çıkarılabilir Ortam ile Veri Sızdırma (T1052)"**, ağ üzerinden dosyaları bir başka sunucuya göndermek için **"Ağ Üzerinden Veri Sızdırma (T1041)"** tekniğinden faydalanabilir.

Başka bir örnek olarak, saldırgan sisteme ilk erişimi sağlamak için çalışanlara (phishing) kimlik avı e-postaları gönderebilir **"Kimlik Avı (T1566)"**. Ancak, e-posta

içindeki zararlı dosyanın bir makroya sahip olması ve çalıştırıldığında kötü amaçlı bir kod çalıştırması ile gerçekleşiyorsa **"Kötü Amaçlı Makro (T1204.002)"** tekniği kapsamında değerlendirilir.

3.3 Prosedürler

Prosedürler, tehdit aktörlerinin belirli bir tekniği nasıl uyguladığına dair ayrıntılı yöntemleri ifade eder. Bir saldırganın belirli bir tekniği nasıl hayata geçirdiği, saldırının türüne, hedef sisteme ve kullanılan araçlara göre değişebilir. MITRE ATT&CK, prosedürleri inceleyerek güvenlik ekiplerinin saldırıların nasıl gerçekleştirildiğini anlamasına ve önlem almasına yardımcı olur.

Örneğin, saldırganların kimlik bilgilerini ele geçirmek için **"Pass-the-Hash (T1550.002)"** tekniğini kullandığını düşünelim. Bu teknik, bir kullanıcının parolasını kırmaya çalışmak yerine doğrudan hash'lenmiş kimlik doğrulama verisini kullanarak sisteme giriş yapmayı içerir. Ancak saldırganın bu tekniği nasıl uyguladığı, yani prosedürü farklılık gösterebilir:

- Bir saldırgan Mimikatz gibi bir araç kullanarak sistem belleğinden NTLM hash'leri çıkarabilir.
- Başka bir saldırgan, SMB veya RDP protokolleri üzerinden hash'leri kullanarak yanal hareket(Lateral Movement) gerçekleştirebilir.

Başka bir örnek olarak, saldırganın "Kimlik Avı ile İlk Erişim (T1566.001)" tekniğini uygulaması farklı yollarla gerçekleşebilir:

- Hedef kullanıcıya kötü amaçlı bir e-posta göndererek, ekli dosyanın çalıştırılmasıyla zararlı yazılımın yüklenmesini sağlamak.
- E-posta içindeki sahte bir bağlantıya tıklanmasını sağlayarak, hedefin kimlik bilgilerini ele geçirmek.

Bu detaylandırma sayesinde güvenlik uzmanları, saldırganların kullandıkları yöntemleri daha iyi anlayabilir ve belirli prosedürlere karşı savunma stratejileri geliştirebilir. MITRE ATT&CK Çerçevesi, tehdit aktörlerinin bilinen saldırı metotlarını detaylandırıp dokümante ederek gerçek dünyada karşılaşılan saldırıları daha hızlı tespit etmesine ve hangi yöntemlerin kullanıldığına dair derinlemesine analiz yapmasına olanak tanır. Bu sayede savunma mekanizmaları daha güçlü hale getirilebilir.

4. MITRE ATT&CK Framework'de Bulunan Taktik Ve Tekniklerin Önemi

MITRE ATT&CK, siber saldırıların aşamalarını taktikler olarak tanımlar ve her taktik altında saldırı tekniklerini sıralar. Bu yapı, tehdit istihbaratını geliştirmek, saldırı tespit sistemlerini güçlendirmek ve güvenlik ekiplerinin olay müdahale süreçlerini hızlandırmak için büyük önem taşır.

Örneğin, bir şirketin ağına yönelik bir saldırı tespit edildiğinde; saldırganın, "kimlik bilgilerini çalma" yoluyla sisteme erişim sağladığı anlaşılır. Bu durum, MITRE ATT&CK çerçevesinde **"Kimlik Bilgisi Hırsızlığı (Credential Access)"** taktiği altında **"Pass-the-Hash (T1550.002)"** tekniği olarak tanımlanır. Güvenlik analistleri, saldırıyı bu teknik doğrultusunda incelediklerinde, benzer saldırıların hangi diğer yollarla gerçekleşebileceğini ve nasıl tespit edilip engellenebileceğini belirleyebilir.

Bir başka örnek olarak, bir sistemde olağan dışı uzak masaüstü bağlantıları (RDP) tespit edildiğinde, MITRE ATT&CK üzerinden **"Yanal Hareket (Lateral Movement)"** taktiği incelenerek, saldırganların **"Geçerli Hesap Kullanımı (T1078)"** veya **"RDP ile Yanal Hareket (T1021.001)"** tekniklerini kullanıp kullanmadığı analiz edilebilir. Bu bilgiler doğrultusunda, olay müdahale ekipleri tehditlerin kaynağını belirleyerek güvenlik önlemlerini güçlendirebilir.

Bu nedenle MITRE ATT&CK, tehdit aktörlerinin izlediği yolları sistematik bir şekilde belgeleyerek güvenlik uzmanlarının saldırılara karşı daha bilinçli, organize ve hızlı tepki vermesini sağlar.

5. TTP-Based Threat Hunting Ve Detection Engineering

Saldırıları tespit ederken ve threat hunting yaparken signature-based, profile-based, anomaly-based gibi yöntemler mevcuttur. Bir de **TTP-based threat hunting and detection engineering** vardır. Her bir yöntemin kendine özgü avantajları ve dezavantajları bulunmaktadır. Bu raporda TTP-based yöntemi özelinde bir inceleme yapılmıştır. Bu yöntem, önceki yöntemlerin tamamlayıcısı niteliğindedir ve saldırganların belirli imzalardan kaçınmak için sürekli değiştirebileceği göstergeler **(IoC)** yerine, onların değiştirmesi çok daha zor olan davranışsal kalıplara odaklanır.

5.1 TTP-Based Threat Hunting Nedir?

TTP-Based Threat Hunting (Taktik, Teknik ve Prosedürlere Dayalı Tehdit Avcılığı), tehdit avcılığı sürecini tehdit aktörlerinin kullandığı taktikler, teknikler ve prosedürler temelinde yürütmeyi amaçlayan bir yaklaşımdır. MITRE ATT&CK çerçevesinde tanımlanan saldırı modellerini kullanarak, potansiyel tehditleri proaktif olarak tespit etmeyi sağlar. Geleneksel güvenlik yaklaşımlarında tehditler genellikle olay sonrası tespit edilirken, TTP odaklı tehdit avcılığı, saldırıların henüz zarar vermeden önce belirlenmesine yardımcı olur.

Örneğin, bir sistemde şüpheli bir komut dosyası çalıştırıldığında, yalnızca imza tabanlı bir antivirüs yazılımı bu tehdidi tespit edemeyebilir. Ancak TTP-Based Threat Hunting yaklaşımıyla güvenlik analistleri, bu komutun bilinen bir saldırı tekniğiyle (örn. PowerShell üzerinden komut çalıştırma – T1059.001) ilişkili olup olmadığını araştırarak tehdidin kaynağını anlayabilir. Benzer şekilde, bir sistem yöneticisinin normalde kullanmadığı RDP bağlantıları tespit edildiğinde, bu aktivitenin "Geçerli

Hesap Kullanımı (T1078)” veya “RDP ile Yanal Hareket (T1021.001)” teknikleri kapsamında bir saldırının parçası olup olmadığı değerlendirilebilir.

Bu yaklaşım, güvenlik ekiplerinin yalnızca belirli saldırı imzalarına değil, saldırganların davranış modellerine odaklanmasını sağlar. Böylece, daha önce bilinmeyen saldırılar dahi TTP'ler üzerinden analiz edilerek erken aşamada tespit edilebilir ve tehditlere karşı daha güçlü bir savunma mekanizması oluşturulabilir.

5.2 Detection Engineering Nedir?

Detection Engineering (Tespit Mühendisliği), SOC’ta ve tehdit avcılığı süreçlerinde saldırıları tespit etmek, analiz etmek ve önlemek için kullanılan yöntemlerin ve kuralların tasarlanması, geliştirilmesi ve uygulanmasını kapsayan bir disiplindir. Temel amacı, siber tehditlere karşı proaktif bir savunma mekanizması oluşturarak güvenlik sistemlerinin saldırılara karşı daha dirençli hale getirilmesini sağlamaktır.

Bu süreç, log analizi, tehdit istihbaratı, olay yanıtı ve MITRE ATT&CK gibi framework'ler kullanılarak saldırı tekniklerinin anlaşılmasını ve bunlara yönelik tespit kurallarının yazılmasını içerir. Detection Engineering sayesinde, saldırganların kullandığı **Taktik, Teknik ve Prosedürler (TTP'ler)** analiz edilerek güvenlik sistemleri için özel olarak hazırlanmış **SIEM kuralları, imzalar ve algılama mekanizmaları** geliştirilir.

Örneğin; bir saldırgan, sistemde kimlik bilgilerini çalmak için Mimikatz gibi bir araç kullandığında, bu saldırı **MITRE ATT&CK Framework’te "T1003 - Credential Dumping"** tekniği olarak sınıflandırılır. Bu tür saldırıları tespit etmek için **Detection Engineering** kapsamında farklı yöntemler uygulanabilir. PowerShell komutları izlenerek Mimikatz gibi araçların çalıştırdığı komutlar tespit edilebilir. Bellek dökümü analiz edilerek hassas bilgilerin çekilip çekilmediği kontrol edilebilir. Ayrıca, ele geçirilen kimlik bilgileriyle yapılan olağandışı oturum açma girişimleri izlenerek (örneğin, farklı IP'lerden gelen ani yetkili kullanıcı oturumları) saldırılar erkenden belirlenebilir ve önlem alınabilir.

Detection Engineering, saldırganların kullandığı tekniklerin daha çok otomatik olarak tespit edilmesini sağlarken, Tehdit Avcılığı saldırıların daha detaylı araştırılmasını ve henüz keşfedilmemiş tehditlerin bulunmasını sağlar. MITRE ATT&CK framework'ü, her iki alan için de rehberlik sunarak kritik altyapıların korunmasında önemli bir rol oynamaktadır.

6. 2022 Ukraine Electric Power Attack (C0034) İncelemesi

2022 Ukraine Electric Power Attack (C0034), gelişmiş bir siber saldırı olup, özellikle endüstriyel kontrol sistemleri (ICS) ve elektrik altyapısını hedef alarak kritik hizmetleri aksatmayı amaçlamıştır. Bu saldırının MITRE ATT&CK Framework ile analiz edilmesi, kullanılan taktik, teknik ve prosedürleri (TTP'ler) anlamamıza yardımcı olur. Aynı zamanda,

Threat Hunting ve Detection Engineering perspektifinden bu saldırının nasıl tespit edilebileceğini ve önlenebileceğini değerlendirmek mümkündür.

6.1 Saldırının MITRE ATT&CK Analizi

2022 yılında Ukrayna'nın elektrik altyapısına yönelik gerçekleştirilen saldırılar, Rusya bağlantılı Sandworm ve ELECTRUM tehdit grupları tarafından düzenlenmiştir. Bu saldırılar, MITRE ATT&CK framework'ünde tanımlanan çeşitli taktik ve teknikler kullanılarak gerçekleştirilmiştir. Aşağıda bu saldırının genel hatlarını ifade edecek kadarı belirtilmiştir.

Taktik	Teknik	Açıklama
Yürütme (Execution)	PowerShell (T1059.001)	TANKTRAP aracıyla zararlı yazılımların dağıtımı ve çalıştırılması.
Kalıcılık (Persistence)	Systemd Servisi (T1543.002)	GOGETTER'ın kalıcı olarak çalışması için Systemd servislerinin yapılandırılması.
Savunmadan Kaçınma (Defense Evasion)	Maskelemek için Görev veya Servis Kullanımı (T1036.004)	GOGETTER'ın meşru görünen servisler olarak gizlenmesi.
Yanal Hareket (Lateral Movement)	Lateral Araç Transferi (T1570)	CaddyWiper'ın hedef sistemlere taşınması ve dağıtılması.
Veri Silme (Data Destruction)	Veri Silme (T1485)	CaddyWiper kullanılarak kritik dosyaların ve sistemlerin silinmesi.
Komuta ve Kontrol (Command and Control)	Protokol Tünelleme (T1572)	GOGETTER ile TLS tabanlı komuta ve kontrol kanallarının oluşturulması.

İlk Erişim (Initial Access): Açıkta Kalan Uygulamaların Sömürülmesi (Exploit Public-Facing Application) [T1190]: Saldırganlar, internet üzerinden erişilebilen ve güncel olmayan MicroSCADA yazılımını çalıştıran bir sunucuyu hedef alarak sisteme sızmışlardır.

Yanal Hareket (Lateral Movement): Uzak Hizmetler (Remote Services) [T1021]: Sisteme girdikten sonra, saldırganlar ağ içinde yanal hareket ederek farklı sistemlere erişim sağlamışlardır.

Yetki Yükseltme (Privilege Escalation): Geçerli Hesaplar (Valid Accounts) [T1078]: Saldırganlar, geçerli kullanıcı hesaplarını ele geçirerek sistemde daha yüksek yetkiler elde etmişlerdir.

Kalıcılık (Persistence): Sistem Hizmetini Oluşturma veya Değiştirme (Create or Modify System Process) [T1543]: Saldırganlar, GOGETTER adlı kötü amaçlı yazılımın kalıcılığını sağlamak için Systemd yapılandırmasını değiştirmişlerdir.

Komuta ve Kontrol (Command and Control): Proxy Kullanımı (Proxy) [T1090]: GOGETTER yazılımı, TLS tabanlı bir tünel oluşturarak saldırganların komuta ve kontrol sunucularıyla güvenli iletişim kurmasını sağlamıştır.

Etkileme (Impact): Veri İmhası (Data Destruction) [T1485]: Saldırganlar, CaddyWiper adlı kötü amaçlı yazılımı kullanarak hedef sistemlerdeki verileri silmişlerdir.

2022 Ukraine Electric Power Attack (C0034) saldırısı, Ukrayna'daki elektrik altyapısını hedef alarak geniş çaplı kesintilere, endüstriyel kontrol sistemlerinde bozulmalara ve ekonomik kayıplara yol açmıştır. Özetle saldırganlar, SCADA yazılımındaki açıkları kullanarak sistemlere sızmış, geçerli hesapları ele geçirerek yanal hareket etmiş ve CaddyWiper zararlısıyla verileri silmiştir. Bu saldırılar, kritik altyapılara yönelik tehditlerin ciddiyetini ve siber güvenlik önlemlerinin önemini bir kez daha gösterirken, MITRE ATT&CK framework'ü bu tür saldırıların analizinde ve savunma stratejilerinin geliştirilmesinde değerli bir rehberlik sunmaktadır. Bu tür tehditleri önlemek için ağ izleme, güncel yazılım kullanımı, çok faktörlü kimlik doğrulama ve tehdit avcılığı gibi her türlü önlemi uygulamak oldukça önemlidir.

6.2 Bunun Gibi Bir Saldırıda Tehdit Avcıları(Threat Hunters) Ne Yapar?

Tehdit avcıları, saldırıyı tespit edebilmek için belirli odak noktalarına yönelir. Özellikle şu soruların yanıtlarını ararlar:

- Sistem hizmetlerinde beklenmeyen değişiklikler var mı? (*T1543*)
- Ağda TLS tünelleme veya şüpheli bağlantılar tespit ediliyor mu? (*T1090*)
- Yetki yükseltme için olağan dışı girişimler mevcut mu? (*T1078*)

Bu süreçte, sistem günlükleri (logs), ağ trafiği ve uç nokta aktiviteleri detaylı bir şekilde incelenir. Eğer şüpheli bir hareket tespit edilirse, olayın derinlemesine araştırılması ve saldırının etkisini en aza indirmek için hızlı müdahale gerçekleştirilir.

6.3 Bunun Gibi Bir Saldırıda Tespit Mühendisleri(Detection Engineers) Ne Yapar?

Kötü Amaçlı Yazılım Davranışlarını İzleme: GOGETTER ve CaddyWiper gibi zararlı yazılımların tespit edilmesinden sonra bu yazılımların karakteristik davranışları belirlenmeli ve bu hareketler için tespit kuralları yazılmalıdır.

Anormal Trafiği Tespit Etme: Proxy kullanımı ve uzak bağlantılar (T1090) gibi teknikler, normal ağ trafiğinden farklı olduğu için sistemlerine özel bir **anormallik algılama (anomaly detection)** mekanizmasını devreye sokabilir.

Yetki Yükseltme Girişimlerini Engelleme: Sistem günlüklerinde beklenmeyen yönetici yetkisi artışları (T1078) için alarmlar oluşturulmalıdır.

2022 Ukraine Electric Power Attack (C0034) saldırısında, Threat Hunting saldırı izi sürme, anomali analizi ve aktif tehditleri tespit etme sürecini kapsarken Detection Engineering bu tehditlerin proaktif olarak belirlenmesi ve güvenlik kontrollerinin oluşturulmasını sağlamaktadır. Threat Hunting kısmı daha çok log analizi, ağ trafiği izleme ve anormallikleri araştırmaya odaklanırken, Detection Engineering kısmı bu anomalileri otomatik tespit eden kuralların ve izleme sistemlerinin geliştirilmesine odaklanır. Bu kapsamda, saldırının MITRE ATT&CK çerçevesinde incelenmesi, hem avcılar (hunters) hem de mühendisler (engineers) için saldırıyı önleme ve tespit etme noktasında büyük bir avantaj sağlar.

7. Örnek Bir Senaryo Üzerinden İnceleme: X Firmasına Yönelik Siber Saldırının MITRE ATT&CK Çerçevesinde Analizi

Bu raporda, varsayımsal olarak finansal teknoloji alanında faaliyet gösteren **X Firması**'na düzenlenen bir siber saldırı MITRE ATT&CK çerçevesinde analiz edilmiştir. Saldırının aşamaları, kullanılan teknikler ve bu tür tehditlere karşı alınabilecek önlemler detaylandırılmıştır.

7.1 Saldırı Senaryosu Ve Saldırının Amacı

Son dönemde X Firması'nın güvenlik ekibi, artan kimlik avı girişimleri ve anormal ağ trafiği nedeniyle bir güvenlik ihlalinden şüphelenmiştir. Yapılan incelemeler sonucunda saldırganların sistemlere yetkisiz erişim sağladığı tespit edilmiştir. Saldırganların temel hedefleri:

- Kullanıcı kimlik bilgilerini ele geçirmek,
- Ödeme sistemlerini manipüle ederek finansal kazanç sağlamak,
- Hassas şirket verilerine erişim elde etmek.

Bu saldırının tespit edilmesi ve önlenmesi sürecinde birden fazla siber güvenlik ekibi aktif rol oynamıştır:

SOC (Security Operations Center) Birimi: Sürekli izleme yaparak olayları tespit eder ve anormallikleri analiz eder.

Mavi Takım (Blue Team): Savunma güvenlik politikalarını belirler, tehdit avcılığı yapar ve saldırıları önlemeye yönelik güvenlik yapılandırmalarını uygular.

Olay Müdahale Ekibi (Incident Response Team - IRT): Saldırı gerçekleştiğinde müdahale eder, sistemleri temizler ve saldırının yayılmasını engeller.

Sistem ve Ağ Güvenliği Ekibi: Güvenlik duvarları, IDS/IPS sistemleri, ağ segmentasyonu ve erişim kontrollerini yönetir.

Siber Tehdit İstihbarat (Threat Intelligence) Ekibi: Tehdit aktörlerini ve saldırı yöntemlerini analiz ederek önleyici güvenlik önlemleri alınmasını sağlar.

Red Team (Sızma Testi Ekibi): Şirketin güvenlik açıklarını test ederek savunma ekiplerinin zayıflıklarını belirler.

Bu birimlerin koordineli çalışması, saldırının tespit edilip etkili bir şekilde müdahale edilmesini sağlamıştır.

7.2 Saldırı Aşamaları

Keşif (Reconnaissance) – T1595 & T1589

Saldırganlar, X Firması'nın dış dünyaya açık sistemlerini analiz ederek hedeflerine dair bilgi topladı.Ağ keşfi için Shodan, Censys gibi araçlarla açık servisler tarandı. Sosyal mühendislik yapılarak LinkedIn ve GitHub gibi platformlardan çalışanlar hakkında bilgi edinildi. Daha önce veri sızıntısı yapıldıysa, ele geçirilmiş hesap bilgilerinin varlığı araştırıldı.

Alınan Önlemler:

Siber Tehdit İstihbarat Ekibi, Dark Web Monitoring araçlarıyla çalışanların e-posta adreslerine dair veri sızıntılarını takip etti.
Mavi Takım & Ağ Güvenliği Ekibi, gereksiz servisleri kapatarak WAF ve IDS/IPS sistemlerini güçlendirdi.
SOC Ekibi, SIEM loglarını analiz ederek şüpheli IP'leri ve yoğun tarama trafiğini izledi.

İlk Erişim (Initial Access) - T1566

Saldırganlar, çalışanlara güvenilir görünen kimlik avı e-postaları göndererek kullanıcı hesap bilgilerini ele geçirdi. Bu e-postalar, şirketin CEO'su gibi gözüken ve bir ödemenin acil yapılması gerektiğini ifade eden sahte içeriklere sahipti. Bir çalışanın şüpheli bir e-postayı SOC birimine bildirmesiyle olay fark edildi. (Kimlik Avı (Spear Phishing Attachment)) Ancak bazı çalışanlar bu e-postalarda gönderilen bir dosyayı açtı. Ve açtığında, PowerShell üzerinden Cobalt Strike tabanlı bir arka kapı (backdoor) indirildi.

Alınan Önlemler:

SOC Ekibi, SIEM logları üzerinden şüpheli PowerShell komutlarını inceledi ve anormal e-posta aktivitelerini belirledi.
Olay Müdahale Ekibi, Tehdit tespit edilir edilmez etkilenen hesapları kilitleyerek makineleri izole etti.
Mavi Takım, DMARC, DKIM ve SPF ayarlarını güçlendirerek gönderilmeye devam eden sahte e-postaların teslim edilmesini engelledi. Çalışanlara sahte e-postalar hakkında eğitim verilmesi için bir program oluşturuldu.

Yetki Yükseltme (Privilege Escalation) - T1078

Dosyaları çalıştıran çalışanların hesapları ele geçirilmişti. Ele geçirilen hesaplardan biri yönetici yetkilerine sahipti. Saldırganlar, bu hesabı kullanarak sistemde daha geniş erişim elde etti. (T1078.002 - Valid Accounts: Domain Accounts)
SOC birimi kullandıkları SIEM ürünü üzerinden, hesaplara anormal girişleri tespit ettiler. Bazı çalışanların yetkileri düzgün ayarlanmadığı için saldırganların üst düzey çalışanların hesaplarına kadar ilerlemesi zor olmamıştı. Elde edilen hesap bilgileri kullanılarak mimikatz ile kimlik bilgileri ele geçirildi. Ele geçirilen kimlik bilgileri ile kritik sunuculara yetkisiz erişim sağlandı.

Alınan Önlemler:

SOC Ekibi, anormal girişleri tespit etti ve MFA zorunluluğunu denetledi.
Sistem ve Ağ Güvenliği Ekibi, yetkisiz hesap yükseltmelerini önlemek için "Least Privilege" ilkesini uyguladı.
Olay Müdahale Ekibi, ele geçirilen hesapları devre dışı bıraktı.

Yanal Hareket (Lateral Movement) - T1021.001

Yetkilerini artıran saldırganlar, şirket içi diğer sistemlere yayılmak için RDP ve SMB protokollerini kullandı. Böylece daha fazla sisteme erişim sağladılar. (T1021.001 - Remote Desktop Protocol, T1550.002 - Pass-the-Hash)
Ele geçirilen admin hesabı ile uzak masaüstü bağlantıları yapıldı. Pass the Hash saldırısı ile kimlik doğrulama bilgileri kullanılarak sunuculara erişim sağlandı.

Alınan Önlemler:

SOC Ekibi, olağandışı RDP girişimlerini tespit etti.
Sistem ve Ağ Güvenliği Ekibi, ağ segmentasyonu ile saldırganın hareket alanını kısıtladı.
Red Team, saldırı sonrası yanal hareket testleri yaparak güvenlik açıklarını belirledi.

Veri Hırsızlığı (Credential Access & Exfiltration) - T1003 & T1041

Saldırganlar, sistemde Mimikatz gibi araçlar kullanarak ek kimlik bilgilerini çaldı. Daha sonra, hassas müşteri ve şirket verilerini şifreleyerek bir dış sunucuya aktardı. (T1003.001 - OS Credential Dumping, T1041 - Exfiltration Over C2 Channel)

Alınan Önlemler:

LSASS koruması ile kimlik bilgileri hırsızlığı engellendi.
DLP çözümleri ile veri sızıntısı izlendi.
Ağ trafik analizi ile C2 trafiği tespit edildi.

Kalıcılık (Persistence) - T1098

Saldırganlar, gelecekteki erişimlerini sürdürmek amacıyla yeni yönetici hesapları oluşturdu ve sistemde PowerShell komutları çalıştırarak arka kapılar kurdu. (T1098 - Account Manipulation, T1059.001 - PowerShell Execution)

Alınan Önlemler:

SOC Ekibi, Active Directory audit loglarını izleyerek yetkisiz hesap oluşturma girişimlerini belirledi.
PowerShell güvenlik politikaları ile zararlı komutlar engellendi.
EDR çözümleri ile şüpheli aktiviteler izlendi ve otomatik aksiyonlar aldı.

Bu saldırı senaryosu, saldırganların finansal kazanç ve hassas verilere erişim sağlamak için izlediği adımları analiz etmektedir. MITRE ATT&CK çerçevesinin kullanılması, saldırı tekniklerini anlamayı, tehditleri erken tespit etmeyi ve etkili savunma stratejileri geliştirmeyi sağlar.

Anormal aktiviteleri tespit edebilen SIEM, EDR ve XDR sistemleri, saldırgan hareketlerini izleyerek erken müdahale imkânı sunar. Ayrıca, çalışan farkındalık eğitimleri ve güçlü erişim kontrolleri ile saldırı yüzeyi azaltılabilir. MITRE ATT&CK temelli bir olay müdahale planı, saldırıların sistematik olarak analiz edilmesini ve etkili aksiyon alınmasını sağlayarak zararları minimize etmeye yardımcı olur.

Aşama	Taktik	Teknik	TID (Teknik Kimliği)
Keşif (Reconnaissance)	Açık Kaynak Araştırması Sosyal Mühendislik	Açık servisleri tarama (Shodan, Censys) Çalışan bilgilerini toplama	T1595 T1589
İlk Erişim (Initial Access)	Kimlik Avı (Phishing) USB veya Medya Sömürme	Zararlı e-posta ekleri ile erişim sağlama Zararlı yazılım içeren USB cihazları kullanma	T1566.001 T1200
Yetki Yükseltme (Privilege Escalation)	Geçerli Hesapların Ele Geçirilmesi	Ele geçirilen kimlik bilgileriyle sistemde ilerleme	T1078.002
Savunmadan Kaçınma (Defense Evasion)	PowerShell Kullanımı	PowerShell ile zararlı komut çalıştırma	T1059.001
Yanal Hareket (Lateral Movement)	Uzaktan Masaüstü Bağlantısı (RDP). Kimlik Bilgisi Geçişi (Pass-the-Hash)	RDP ile diğer sistemlere sızma Hash değerleri ile sistemlere erişim	T1021.001 T1550.002
Komuta ve Kontrol (C2)	C2 Sunucusu Üzerinden Bağlantı	Dış sunucularla gizli iletişim	T1041
Etkiler (Impact)	ICS Manipülasyonu Hizmet Reddi (Denial of Service)	SCADA sistemlerini devre dışı bırakma Şebekeyi devre dışı bırakma saldırısı	T0869 T1498

8. Sonuç

Siber tehditlerin giderek karmaşıklaştığı bir dünyada, güvenlik ekiplerinin saldırganların yöntemlerini anlaması ve tehditleri erken aşamada tespit etmesi hayati önem taşımaktadır. MITRE ATT&CK, tehdit aktörlerinin kullandığı taktikler, teknikler ve prosedürleri sistematik bir şekilde belgeleyerek güvenlik ekiplerine güçlü bir rehber sunmaktadır.

Bu raporda ele alınan **TTP-Based Threat Hunting ve Detection Engineering** yaklaşımları, saldırıları geleneksel imza tabanlı yöntemlerden daha önce tespit etmeyi ve etkili bir savunma mekanizması geliştirmeyi mümkün kılmaktadır. MITRE ATT&CK'in sunduğu çerçeve sayesinde, tehdit avcılığı süreçleri daha verimli hale gelmekte ve saldırılara karşı daha proaktif güvenlik önlemleri alınabilmektedir.

Sonuç olarak, MITRE ATT&CK yalnızca bir tehdit modeli değil, aynı zamanda siber güvenlik dünyasında ortak bir dil oluşturarak **tehdit istihbaratı, olay müdahale süreçleri ve güvenlik mimarisi açısından kritik bir yapı taşı** haline gelmiştir. Bu framework'ün etkin

bir şekilde kullanılması, saldırganların bir adım önünde olmayı sağlayarak siber güvenlik stratejilerini daha güçlü hale getirecektir.

9. Kaynakça

https://attack.mitre.org/
https://attack.mitre.org/campaigns/C0034/
https://attack.mitre.org/resources/learn-more-about-attack/training/threat-hunting/
https://attack.mitre.org/resources/learn-more-about-attack/training/detection-engineering/
https://www.dragos.com/blog/new-details-electrum-ukraine-electric-sector-compromise-2022/
https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/