



# MİTRE ATT&CK

İREM GÜZEL  
17.02.2025

## İçindekiler

Giriş.....	3
Mitre Att&ck Tablosu Nedir? .....	3
Enterprise (İşletme) Matrisi.....	3
Mobile (Mobil) Matrisi .....	4
ICS Matrisi.....	5
Mitre Att&ck Tablosu Neden Önemlidir ?.....	5
Mitre Atak Framework'te Bulunan Taktik&Tekniklerin Önemi .....	5
1. Taktik .....	5
2. Teknik.....	7
3. Prosedür .....	9
Mitigations (Azaltma önlemleri ) .....	9
TTP nedir?.....	10
TTP-Based Threat Hunting .....	10
Detection Engineering .....	10
2022 Ukrayna Elektrik Şebekesi Saldırısı .....	11
Mitre Att&ck Senaryo .....	14
1. Keşif (Reconnaissance): .....	14
2. İlk Erişim (Initial Access) .....	14
3. Uygulamak (Execution).....	14
4. Ayrıcalık Yükseltme Aşaması (Privilege Escalation) .....	15
5. Veri Sızdırma (Exfiltration).....	15
6. Defense Evasion(Savunma Kaçınma).....	16
Sonuç.....	16
KAYNAKÇA.....	17

## Giriş

Mitre ATT&CK çerçevesi, kuruluşların siber güvenlik stratejilerini güçlendirmelerine yardımcı olmak için siber saldırganların en son davranışlarını ve taktiklerini tanımlayan ücretsiz, küresel olarak erişilebilir bir bilgi tabanıdır .

Tehdit avcılarını, MITRE ATT&CK çerçevesini kullanarak sistemlerinde gizli tehditleri proaktif bir şekilde araştırabilir ve olası saldırı izlerini daha etkin bir şekilde ortaya çıkarabilir. Bu tabloyu kullanarak güvenlik bilginizi derinleştirebilir, tehdit algılama süreçlerinizi iyileştirebilir ve daha güçlü bir siber savunma oluşturabilirsiniz.

## Mitre Att&ck Tablosu Nedir?

MITRE ATT&CK (Rakip Taktikler, Teknikler ve Genel Bilgi), MITRE Corporation tarafından kuruluşların güvenlik hazırlıklarını anlamalarına ve savunmalarındaki zaafırları ortaya çıkarmalarına yardımcı olmak için geliştirilen bir çerçeve, veri matrisleri seti ve değerlendirme aracıdır.

2013 yılında geliştirilen MITRE ATT&CK Çerçevesi, belirli saldırı yöntemlerini, taktiklerini ve tekniklerini belgelemek için gerçek dünya gözlemlerini kullanır. Yeni güvenlik açıkları ve saldırı yüzeyleri ortaya çıktıkça, bunlar sürekli olarak gelişen ATT&CK çerçevesine eklenir. Geçtiğimiz birkaç yıl içinde, MITRE ATT&CK çerçevesi ve matrisleri, saldırgan davranışına ilişkin hem bilgi hem de düzeltme araçları için bir endüstri standardı haline geldi.

MITRE ATT&CK Çerçevesi içerisinde platform tiplerine göre 3 farklı matris oluşturulmuştur:

- İşletme Matrisi
- Mobil Matris
- ICS (Endüstriyel Kontrol Sistemleri) Matrisi

## Enterprise (İşletme) Matrisi

MITRE ATT&CK Enterprise Matrisi, saldırganların kurumsal ağlara nasıl sızdığını, nasıl hareket ettiğini ve hedeflerine nasıl ulaştığını detaylandırır.

Alt Kümesi:

- PRE
- Windows
- macOS
- Linux
- Cloud
- Network
- Containers

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
15 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	23 techniques	8 techniques	17 techniques	10 techniques	9 techniques	14 techniques
Active Scanning (2)	Acquire Access (2)	Current Injection (2)	Cloud Administration Command (2)	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services (2)	Adversary-in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (2)	Account Access Removal (2)
Gather Victim Host Information (2)	Acquire Infrastructure (2)	Drive-by Compromise (2)	Command and Scripting Interpreter (2)	BITS Jobs (2)	Access Token Manipulation (2)	Access Token Manipulation (2)	Broken Force (2)	Application Window Discovery (2)	Internal Reconnaissance (2)	Active Collected Data (2)	Communication Through Removable Media (2)	Data Transfer Size Limits (2)	Data Destruction (2)
Gather Victim Identity Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application (2)	Container Administration Command (2)	BITS Jobs (2)	Account Manipulation (2)	Account Manipulation (2)	Credentials from Password Store (2)	Browser Information Discovery (2)	Lateral Tool Transfer (2)	Audio Capture (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact (2)	Data Encrypted for Impact (2)
Gather Victim Network Information (2)	Compromise Infrastructure (2)	External Remote Services (2)	Deploy Container (2)	Boot or Logon Initialization Scripts (2)	Build Image on Host (2)	Build Image on Host (2)	Debugger Execution (2)	Cloud Infrastructure Discovery (2)	Remote Service Session Hijacking (2)	Automated Collection (2)	Content Injection (2)	Data Manipulation (2)	Data Manipulation (2)
Gather Victim Org Information (2)	Develop Capabilities (2)	Hardware Additions (2)	Exploitation for Client Execution (2)	Browser Extensions (2)	Desktop/Local/Decade Files or Information (2)	Desktop/Local/Decade Files or Information (2)	Forceful Authentication (2)	Cloud Service Dashboard (2)	Remote Services (2)	Browser Session Hijacking (2)	Data Encoding (2)	Defacement (2)	Defacement (2)
Phishing for Information (2)	Establish Accounts (2)	Replication Through Removable Media (2)	Inter-Process Communication (2)	Browser Extensions (2)	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Forge Web Credentials (2)	Cloud Service Discovery (2)	Remote Services (2)	Clipboard Data (2)	Dynamic Resolution (2)	Exfiltration Over C2 Channel (2)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (2)	Supply Chain Compromise (2)	Native API (2)	Create Account (2)	Create or Modify System Process (2)	Create or Modify System Process (2)	Inject Capture (2)	Cloud Storage Object Discovery (2)	Application Through Removable Media (2)	Data from Cloud Storage (2)	Encrypted Channel (2)	Exfiltration Over Other Network Medium (2)	Endpoint Denial of Service (2)
Search Open Technical Databases (2)	Stage Capabilities (2)	Trusted Relationship (2)	Scheduled Task/Job (2)	Create or Modify System Process (2)	Domain or Token Policy Modification (2)	Domain or Token Policy Modification (2)	Multi-Factor Authentication Request Generation (2)	Container and Resource Discovery (2)	Software Deployment Tools (2)	Data from Configuration Repository (2)	Fullback Channels (2)	Exfiltration Over Physical Medium (2)	Financial Theft (2)
Search Open Websites/Domains (2)		Valid Accounts (2)	Shared Modules (2)	Event Triggered Execution (2)	Execution Guardrails (2)	Execution Guardrails (2)	Multi-Factor Authentication Request Generation (2)	Debugger Snippet (2)	Telemetry Shared Content (2)	Device Driver Discovery (2)	Ingress Tool Transfer (2)	Exfiltration Over Web Service (2)	Inhibit System Recovery (2)
Search Victim-Owned Websites (2)			Software Deployment Tools (2)	External Remote Services (2)	Escape to Host (2)	Escape to Host (2)	Multi-Factor Authentication Request Generation (2)	File and Directory Discovery (2)	Use Alternate Authentication Material (2)	File and Directory Discovery (2)	Multi-Stage Channels (2)	Scheduled Transfer (2)	Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (2)	Exploitation for Privilege Escalation (2)	Exploitation for Privilege Escalation (2)	File and Directory Permissions Modification (2)	Log Enumeration (2)		Data from Local System (2)	Non-Application Layer Protocol (2)	Transfer Data to Cloud Account (2)	Resource Hijacking (2)
			User Execution (2)	Impair Internal Image (2)	Hide Artifacts (2)	Hide Artifacts (2)	Hide Artifacts (2)	Network Sniffing (2)		Data from Network Shared Drive (2)	Non-Standard Port (2)	Service Step (2)	System Shutdown/Reboot (2)
			Windows Management Instrumentation (2)	Impair Internal Image (2)	Hijack Execution Flow (2)	Hijack Execution Flow (2)	Impair Defenses (2)	OS Credential Dumping (2)		Data from Removable Media (2)	Protocol Tunneling (2)		
				Modify Authentication Process (2)	Process Injection (2)	Process Injection (2)	Indicator Termination (2)	OS Credential Dumping (2)		Data Staged (2)	Reverse Access Software (2)		
				Office Application Hijack (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Indicator Termination (2)	OS Credential Dumping (2)		Email Collection (2)	Traffic Signaling (2)		
				Power Settings (2)	Valid Accounts (2)	Valid Accounts (2)	Indicator Termination (2)	OS Credential Dumping (2)		Input Capture (2)	Web Service (2)		
				Pre-OS Boot (2)			Indicator Termination (2)	OS Credential Dumping (2)		Screen Capture (2)			
				Scheduled Task/Job (2)			Indicator Termination (2)	OS Credential Dumping (2)		Video Capture (2)			
				Server Software Component (2)			Indicator Termination (2)	OS Credential Dumping (2)					
				Traffic Signaling (2)			Indicator Termination (2)	OS Credential Dumping (2)					
				Valid Accounts (2)			Indicator Termination (2)	OS Credential Dumping (2)					

## Enterprise Matrisi

## Mobile (Mobil) Matrisi

Mobil matris, mobil cihazlar için hazırlanmış ve mobil cihazların siber güvenliği hakkında bilgi içeren matristir. Bu matris, bireysel ve kurumsal mobil cihazların güvenliğini sağlamak için kullanılabilir. Kurumsal Matris ile karşılaştırıldığında, daha az bilgi içerir.

## Alt kümesi:

- Android
- iOS

layout slide ▾											
show sub-techniques											
hide sub-techniques											
help											
Initial Access 7 techniques	Execution 4 techniques	Persistence 7 techniques	Privilege Escalation 2 techniques	Defense Evasion 14 techniques	Credential Access 5 techniques	Discovery 8 techniques	Lateral Movement 2 techniques	Collection 12 techniques	Command and Control 9 techniques	Exfiltration 2 techniques	Impact 10 techniques
Application Versioning (2)	Command and Scripting Interpreter (2)	Boot or Logon Initialization Scripts (2)	Abuse Elevation Control Mechanism (2)	Application Versioning (2)	Access Notifications (2)	File and Directory Discovery (2)	Exploitation of Remote Services (2)	Access Notifications (2)	Application Layer Protocol (2)	Exfiltration Over Alternative Protocol (2)	Account Access Removal (2)
Drive-by Compromise (2)	Exploitation for Client Execution (2)	Compromise Application Executable (2)	Exploitation for Privilege Escalation (2)	Download New Code at Runtime (2)	Clipboard Data (2)	Location Tracking (2)	Replication Through Removable Media (2)	Adversary-in-the-Middle (2)	Call Control (2)	Exfiltration Over C2 Channel (2)	Call Control (2)
Exploitation for Initial Access (2)	Native API (2)	Compromise Client Software Binary (2)	Process Injection (2)	Execution Guardrails (2)	Credentials from Password Store (2)	Network Service Scanning (2)	Audio Capture (2)	Dynamic Resolution (2)	Dynamic Resolution (2)	Encrypted Channel (2)	Data Destruction (2)
Lockscreen Bypass (2)	Scheduled Task/Job (2)	Event Triggered Execution (2)	Hide Artifacts (2)	Foreground Persistence (2)	Input Capture (2)	Process Discovery (2)	Cell Control (2)	Encrypted Channel (2)	Ingress Tool Transfer (2)	Exfiltration Over C2 Channel (2)	Data Encrypted for Impact (2)
Phishing (2)		Client Triggered Execution (2)	Hooking (2)	Indicator Defenses (2)	Steal Application Access Token (2)	Software Discovery (2)	Clipboard Data (2)	Encrypted Channel (2)	Non-standard Port (2)	Out of Band Data (2)	Data Manipulation (2)
Replication Through Removable Media (2)		Foreground Persistence (2)	Indicator Removal on Host (2)	Input Injection (2)		System Network Configuration Discovery (2)	Data from Local System (2)	Encrypted Channel (2)	Remote Access Software (2)	Input Injection (2)	Endpoint Denial of Service (2)
Supply Chain Compromise (2)		Hijack Execution Flow (2)	Input Injection (2)	Input Injection (2)		System Network Connections Discovery (2)	Protected User Data (2)	Encrypted Channel (2)	Web Service (2)	Generate Traffic from Victim (2)	Network Denial of Service (2)
		Scheduled Task/Job (2)		Obfuscated Files or Information (2)			Screen Capture (2)	Encrypted Channel (2)		SMS Control (2)	
				Process Injection (2)			Stored Application Data (2)	Encrypted Channel (2)			
				Privacy Through Victim (2)			Video Capture (2)	Encrypted Channel (2)			
				Subvert Trust Controls (2)				Encrypted Channel (2)			
				Virtualization/Sandbox Evasion (2)				Encrypted Channel (2)			

## ICS Matrisi

ICS Matrisi, endüstriyel kontrol sistemlerindeki cihazların siber güvenliği için toplanan bilgileri içeren matristir. Bu matris, bir ICS'nin siber güvenliğini ve analizlerini sağlamak için kullanılabilir.

Initial Access 12 techniques	Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 8 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 9 techniques	Inhibit Response Function 14 techniques	Impair Process Control 6 techniques	Impact 12 techniques
Unlink Compromise Exploit Public-Facing Application Exploitation of Remote Services External Remote Services Internet Accessible Device Remote Services Replication Through Removable Media Rogue Master Spearghishing Attachment Supply Chain Compromise Transient Cyber Asset Wireless Compromise	Automate Image Change Operating Mode Command-Line Interface Execution through API Graphical User Interface Hooking Modify Controller Testing Native API Scripting User Execution	Hardcoded Credentials Modify Program Module Firmware Project File Infection System Firmware Valid Accounts	Exploitation for Privilege Escalation Hooking	Change Operating Mode Exploitation for Session Indicator Removal on Host Masquerading Rootkit Spoof Reporting Message System Binary Proxy Execution	Network Connection Enumeration Network Sniffing Remote System Discovery Remote System Information Discovery Wireless Sniffing	Default Credentials Exploitation of Remote Services Hardcoded Credentials Lateral Tool Transfer Program Download Remote Services Valid Accounts	Adversary-on-the-Side Automated Collection Data from Information Repositories Data from Local System Detect Operating Mode I/O Image Monitor Process State Point & Tag Identification Program Upload Screen Capture Wireless Sniffing	Commonly Used Port Connection Proxy Standard Application Layer Protocol	Activate Firmware Update Mode Alarm Suppression Block Command Message Block Reporting Message Block Serial COM Change Credential Data Destruction Denial of Service Device Restart/Shutdown Manipulate I/O Image Modify Alarm Settings Reboot Service Stop System Firmware	Block Sock I/O Modify Parameter Module Firmware Spoof Reporting Message Unauthorized Command Message	Denial of Property Denial of Control Denial of User Loss of Availability Loss of Control Loss of Productivity and Warhead Loss of Protection Loss of Safety Loss of View Manipulation of Control Manipulation of View Theft of Operational Information

ICS Matrisi

## Mire Att&ck Tablosu Neden Önemlidir ?

### • Ortak Bir Dil ve Sınıflandırma

MITRE ATT&CK, siber saldırganların hedeflerine ulaşmak için kullandıkları taktik ve teknikleri ortak bir sınıflandırma altında toplayarak, siber güvenlik uzmanları ve kurumlar arasında net ve anlaşılır bir iletişim sağlar.

### • Olmaz ise ne olur ?

- Tehdit Analizi ve Savunma Stratejileri Zorluğu
- Güvenilir Bilgi Kaynağı Eksikliği
- Kırmızı Takım ve Mavi Takım İş birliği Zorluğu
- Sürekli Gelişim ve Güncellik Eksikliği

## Mitre Atak Framework'te Bulunan Taktik&Tekniklerin Önemi

### 1. Taktik

Taktikler, saldırganların hedeflerine ulaşmak için kullandıkları yüksek seviyeli stratejilerdir. Saldırganın genel amacını ve yaklaşımını belirler. Örneğin, bir saldırganın taktığı, hedef sistemlere sızmak ve hassas verileri çalmak olabilir. Taktikler matrisin en üst sırasındadır.





### **Mobil Taktikleri :**

- Initial Access ( İlk Eriřim )
- Execution ( Uygulamak )
- Persistence ( Azim )
- Privilege Escalation ( Ayrıcalık Yükseltmesi )
- Defense Evasion (Savunma Kaçınma)
- Credential Access ( Kimlik Bilgisi Eriřimi )
- Discovery ( Keřif )
- Lateral Movement ( Yanal Hareket )
- Collection ( Koleksiyon )
- Command and Control ( Komuta ve Kontrol )
- Exfiltration ( Sızdırma )
- Impact ( Darbe )
- Network Effects ( Ağ Etkileri )
- Remote Service Effects ( Uzaktan Hizmetin Etkileri )

### **ICS Taktikleri**

- Initial Access ( İlk Eriřim )
- Execution ( Uygulamak )
- Persistence ( Azim )
- Privilege Escalation ( Ayrıcalık Yükseltmesi )
- Evasion ( Kaçınma )
- Discovery ( Keřif )
- Lateral Movement ( Yanal Hareket )
- Collection ( Koleksiyon )
- Command and Control ( Komuta ve Kontrol )
- Inhibit Response Function ( Tepki Fonksiyonunu Engelle )
- Impair Process Control ( Süreç Kontrolünü Bozmak )
- Impact ( Darbe )

## **2. Teknik**

MITRE ATT&CK teknikleri, taktikleri nasıl başarmaya çalıştıklarını temsil eder. Bunlar, phishing ve brute force saldırıları gibi temel yöntemlerden, DLL arama sırası ele geçirme ve process enjeksiyonu gibi daha karmařık yöntemlere kadar geniş bir yelpazeye yayılır.

Siber güvenlik uzmanlarının bu teknikleri anlaması, tehditleri daha hızlı tespit etmelerine, güvenlik önlemlerini güçlendirmelerine ve olaylara daha etkili bir şekilde müdahale etmelerine yardımcı olur. Bu nedenle, MITRE ATT&CK gibi tehdit istihbaratı çerçeveleri, güvenlik ekipleri için kritik bir rehber niteliğindedir





### 3. Prosedür

Prosedür, tekniklerin/alt tekniklerin kullanım örneklerinden oluşur. Basitçe, tekniğin uygulanması sırasında hangi araç/yazılımın kullanıldığını gösterir. Başka bir deyişle, tekniğin kullanımıyla ilgili pratik bilgilerin açıklamasıdır.

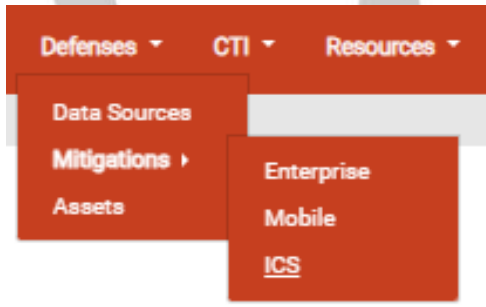
#### Procedure Examples

ID	Name	Description
G0001	Axiom	Axiom has used spear phishing to initially compromise victims. <sup>[9][10]</sup>

Mitre Att&ck Prosedür

### Mitigations (Azaltma önlemleri )

Mitigations, Mitre Att&ck matrisindeki tekniklere yanıt olarak alınabilecek önlemler ve eylemleri açıklar.



Mitre Att&ck Mitigations

Azaltmalar için de matrisler 3'e ayrılmıştır. Raporun yazıldığı zaman dilimi için güncel Azaltma sayısı :

- Enterprise Mitigations : 44
- Mobile Mitigations : 13
- ICS Mitigations : 52

#### Techniques Addressed by Mitigation

Domain	ID	Name	Use
ICS	T0830	Adversary-in-the-Middle	Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.
ICS	T0811	Data from Information Repositories	Consider periodic reviews of accounts and privileges for critical and sensitive repositories.

ICS için örnek Mitigations



### TTP nedir?

TTP'ler, siber saldırganların hedeflerine ulaşmak için kullandıkları yöntemlerin üç boyutunu ifade eder:

**T** : Tactics

**T** : Techniques

**P** : Procedures

### TTP-Based Threat Hunting

**Tehdit**, bir kuruluşun bilgi varlıklarına zarar verme potansiyeli taşıyan her türlü zararlı aktivite veya saldırgandır. Bilgisayar sistemlerine, ağlara, veri tabanlarına ve kritik altyapılara zarar verebilirler.

**Tehdit avlama** ise, siber güvenlik uzmanlarının ağlarda ve sistemlerde gizlenmiş tehditleri aktif olarak aradığı proaktif bir süreçtir. Otomatik güvenlik çözümlerinin tespit edemediği saldırıları belirlemek için kullanılır ve siber saldırıların erken aşamalarında tespit edilmesini sağlar.

**TTP Tabanlı Tehdit Avcılığı** ise tehdit aktörlerinin kullandığı belirli davranışları, saldırı kalıplarını ve operasyonel teknikleri (Taktikler, Teknikler, Prosedürler - TTP) inceleyen bir siber tehdit avcılığı yaklaşımıdır. Bu yöntem, geçmiş siber saldırıları analiz ederek, saldırganların gelecekteki hareketlerini tahmin etmeye ve proaktif bir şekilde tehditleri tespit etmeye olanak sağlar. TTP'lerin analizi, güvenlik ekiplerine daha hedeflenmiş ve etkili savunmalar geliştirme imkanı sunar.

### Detection Engineering

Tespit mühendisliği, siber saldırıları tespit etmek ve bunlara karşı uyarılar oluşturmak için güvenlik araçları ve sistemlerinin (SIEM, IDS/IPS vb.) yapılandırılması ve yönetilmesi sürecidir. Tespit mühendisleri, tehdit istihbaratı, log analizi ve diğer kaynaklardan elde ettikleri bilgileri kullanarak, saldırıların belirtilerini ve kalıplarını tanımlayan kurallar ve algoritmalar geliştirirler. Bu sayede, güvenlik ekipleri saldırıları gerçek zamanlı olarak tespit edebilir ve müdahale edebilirler.

## 2022 Ukrayna Elektrik Şebekesi Saldırısı

Rusya-Ukrayna savaşı sırasında gerçekleşen 2022 Ukrayna Elektrik Şebekesi Saldırısı, siber saldırıların kritik altyapılar üzerindeki etkisini gözler önüne seren önemli bir olaydır. Saldırı, Ukraynalı bir elektrik dağıtım şirketini hedef alarak, yetkisiz komutların SCADA sistemleri üzerinden iletilmesiyle elektrik kesintilerine neden olmuştur.

Saldırıyı gerçekleştiren Sandworm grubu, hedefe ulaşmak için çeşitli kötü amaçlı yazılımlar ve teknikler kullanmıştır:

- GOGETTER: İlk erişimi sağlamak için kullanılan kötü amaçlı yazılım.
- Neo-REGEORG: Saldırganların ağ içinde yan hareket etmesini ve diğer sistemlere erişimini sağlayan araç.
- CaddyWiper: Hedef sistemlerdeki verileri silerek yıkıcı hasar veren kötü amaçlı yazılım.
- Living off the Land (LotL) Teknikleri: Saldırganların, tespit edilmemek için hedef sistemlerde halihazırda bulunan mevcut araçları ve kaynakları kötüye kullanması.

Bu saldırıda kullanılan teknikler ve bunların MITRE ATT&CK çerçevesindeki TID değerleri aşağıdaki gibidir:

DOMAIN	ID		NAME	DESCRIPTION
Enterprise	<u>T1059</u>	.001	<u>Komut ve Komut Dosyası Yorumlayıcısı : PowerShell</u>	Saldırganlar, PowerShell'i kullanarak sistem üzerinde komut çalıştırabilir, kötü amaçlı yazılımlar indirebilir ve çalıştırabilir.
Enterprise	<u>T1543</u>	.002	<u>Sistem İşlemini Oluştur veya Değiştir : Systemd Hizmeti</u>	Systemd, Linux sistemlerde hizmetleri yönetmek için kullanılan bir init sistemidir. Saldırganlar, root yetkileriyle yeni bir systemd servisi oluşturup

				zararlı bir dosyayı sistem başlangıcında çalıştırabilir.
Enterprise	<u>T1485</u>		<u>Veri İmhası</u>	Saldırganlar, sistemdeki kritik verileri silebilir veya şifreleyerek işlevsiz hale getirebilir.
Enterprise	<u>T1484</u>	.001	<u>Alan veya Kiracı Politikası Değişikliği : Grup Politikası Değişikliği</u>	Saldırganlar, Active Directory ortamında <b>Group Policy Objects</b> üzerinde değişiklik yaparak kullanıcı politikalarını değiştirebilir ve sistem kontrolünü ele geçirebilir.
Enterprise	<u>T1570</u>		<u>Yanal Alet Transferi</u>	Saldırganların bir sistemden diğerine kötü amaçlı dosya aktarmasını ifade eder.
Enterprise	<u>T1036</u>	.004	<u>Maskleme : Maskeli Görev veya Hizmet</u>	Saldırganlar, kötü amaçlı işlemleri ve servisleri <b>meşru görünen isimlerle saklayarak</b> tespit edilmelerini zorlaştırabilir.
Enterprise	<u>T1095</u>		<u>Uygulama Dışı Katman Protokolü</u>	Saldırganlar, ağ üzerinden güvenli şekilde çalışmayan protokolleri kullanarak verileri sızdırabilir veya komut kontrol sunucularına bağlanabilir.
Enterprise	<u>T1572</u>		<u>Protokol Tünelleme</u>	Saldırganlar, güvenlik duvarlarından kaçmak için şifreli tünel bağlantıları (VPN, SSH, Tor) oluşturabilir.
Enterprise	<u>T1053</u>	.005	<u>Zamanlanmış Görev/İş : Zamanlanmış Görev</u>	Saldırganlar kötü amaçlı yazılımları belirli bir zaman diliminde çalıştırabilir.
Enterprise	<u>T1505</u>	.003	<u>Sunucu Yazılım Bileşeni : Web Shell</u>	Saldırganların ele geçirdiği bir web sunucusu üzerinde uzaktan komut çalıştırmasına izin veren bir araçtır.

ICS	<u>T0895</u>	<u>Otomatik Çalıştırma Görüntüsü</u>	Bu teknik, saldırganların kötü amaçlı yazılımları veya kodları, sistem açılışında otomatik olarak çalışacak şekilde ayarlamasını ifade eder. Bu sayede, sistem yeniden başlatıldığında veya kullanıcı oturum açıldığında saldırganın kontrolü yeniden sağlanır.
ICS	<u>T0807</u>	<u>Komut Satırı Arayüzü</u>	Saldırganlar, CLI'yi kullanarak sistem üzerinde çeşitli işlemler gerçekleştirebilir, kötü amaçlı yazılımlar çalıştırabilir ve hassas verilere erişebilirler.
ICS	<u>T0853</u>	<u>Komut dosyası</u>	komut dosyaları, belirli bir görevi otomatikleştirmek için yazılan kodlardır. Saldırganlar, komut dosyalarını kullanarak sistem üzerinde çeşitli işlemler gerçekleştirebilir, kötü amaçlı yazılımlar yükleyebilir ve hatta sistemin kontrolünü ele geçirebilirler.
ICS	<u>T0894</u>	<u>Sistem İkili Proxy Çalıştırma</u>	Bu teknik, saldırganların hedef sistemde bir proxy sunucusu çalıştırarak, ağ trafiğini bu sunucu üzerinden yönlendirmesini ifade eder. Bu sayede, saldırganlar izlerini gizleyebilir, ağdaki diğer sistemlere erişebilir ve hatta hassas verileri ele geçirebilirler.
ICS	<u>T0855</u>	<u>Yetkisiz Komut Mesajı</u>	Bu teknik, saldırganların hedef sistemlere yetkisiz komutlar göndermesini ve bu komutların işlenmesini sağlamasını ifade eder.

## Mitre Att&ck Senaryo

Bir tehdit aktörü, X Şirketi'ni hedef alarak siber saldırı planı yapmaktadır. İlk olarak, internette şirket hakkında bilgi toplamak için çeşitli yöntemler kullanır.

### 1. Keşif (Reconnaissance):

- **Gather Victim Identity Information - T1589.004 (Şirket Web Siteleri, Sosyal Medya)**

Saldırgan şirketin "Hakkımızda" veya "İletişim" gibi bölümlerini inceleyerek çalışanlar hakkında bilgi sahibi olmuştur. Aynı zamanda Facebook, Twitter, LinkedIn, Instagram gibi platformlar ile şirket çalışanlarının profillerini daha detaylı analiz edebilmiştir.

- **Gather Victim Host Information - T1592**

Bu teknik, saldırganların hedef sistem veya ağdaki güvenlik açıklarını belirlemek için hedefe tarama yapmasını içerir. Nmap, Shodan, Nessus, vb.

### 2. İlk Erişim (Initial Access)

- **Replication Through Removable Media – T1091 (Çıkarılabilir Medya Aracılığıyla Çoğaltma)**

Saldırgan ,USB cihazını çalışanların bilgisayarlarına fiziksel erişim sağlamak amacıyla kötü amaçlı yazılım taşıyan bir cihaz olarak kullanılır.

Bir süre sonra şirket çalışanlarıyla temasa geçen saldırgan, ilk erişimini USB cihazı ile kurmayı dener. Hedef çalışanların kişisel eşyalarına kendi USB cihazını bırakır. Saldırgan, çalışanların bu USB'yi bilgisayarına takarak oluşturduğu kötü amaçlı yazılımı bulaştırmayı hedefler.

USB'yi kendi bilgisayarlarına takan çalışanlar, kötü amaçlı yazılımı bilgisayarına bulaştırır ve saldırıya ilk erişimi sağlarlar.

### 3. Uygulamak (Execution)

Saldırgan, kalıcı erişim elde etmek ve zamanlanmış görevler aracılığıyla sürekli olarak sisteme erişebilmek için adımlar atar.



- **Scheduled Task/Job - T1053 (Zamanlanmış Görev/İş)**

Zamanlanmış görevler, işletim sistemlerinde belirli zamanlarda veya olaylarda otomatik olarak çalıştırılan komutlar, programlar veya betiklerdir. Sistem yeniden başlatılsa veya kullanıcı oturumu kapatılsa bile, zamanlanmış görevler veya işler sayesinde kötü amaçlı yazılımlar veya komutlar otomatik olarak çalışmaya devam edebilir.

Saldırgan bu sayede sistemde belirli periyotlarla kötü amaçlı yazılımı tekrar çalıştıracaktır.

- **Command and Scripting Interpreter - T1059 (Komut ve Komut Dosyası Yorumlayıcısı)**

Saldırgan, PowerShell, Bash ve diğer komut yorumlayıcıları aracılığıyla zararlı komutlarını yürütür.

#### 4. Ayrıcalık Yükseltme Aşaması (Privilege Escalation)

- **Account Manipulation - T1098 (Hesap Manipülasyonu)**

Bu teknik, saldırganların sistemdeki kullanıcı hesaplarını manipüle ederek yetkilerini artırmasına veya kalıcılık sağlamasına olanak tanır. Bu senaryoda saldırgan düşük ayrıcalıklı bir hesaba erişim sağladıktan sonra bu hesabın yetkilerini yükseltmiştir.

- **Process Injection - T1055 (Süreç Enjeksiyonu)**

Bu teknik, saldırganların kötü amaçlı kodlarını meşru bir sürecin adres alanına enjekte ederek çalıştırmasını ifade eder.

#### 5. Veri Sızdırma (Exfiltration)

Senaryonun bu aşamasına kadar saldırgan artık sistemde tam yetkiye sahiptir. Geriye sistem kaynaklarını sömürmesi ve ele geçirmesi kalmıştır.

- **Automated Exfiltration - T1020 (Otomatik Veri Sızdırma)**

Saldırgan, elde ettiği verileri belirli zaman aralıklarıyla otomatik olarak dışarı çıkaracak bir komut veya script kullanır.

- **Data Transfer Size Limits - T1030 (Veriyi Parçalar Halinde Gönderme)**

Saldırgan büyük hacimli verilerin güvenlik sistemlerine takılmasını önlemek için veriyi daha küçük parçalara bölünerek dışarı sızdırır. Bu teknik ile anormal ağ trafiği analizlerinden ve DLP sistemlerinden kaçınmayı hedefler.

## 6. Defense Evasion(Savunma Kaçınma)

### • Indicator Removal - T1070 (Sistemdeki İzleri Silme)

Saldırgan, arkada iz bırakmamak ve adli analiz süreçlerini zorlaştırmak için logları silme, komut geçmişlerini temizleme gibi sistemdeki izlerini yok etme yöntemlerini kullanır.

- T1070.001 - Clear Windows Event Logs : Windows olay günlüklerini temizler
- T1070.002 - Clear Linux Logs : Linux sistem günlüklerini temizler
- T1070.003 - Clear Command History : Komut geçmişlerini temizler
- T1070.004 - File Deletion : Oluşturduğu dosyaları temizler

## Sonuç

Tüm bu rapordan anlayacağımız gibi Mitre Att&ck framework'ün taktik ve tekniklerini benimsemek; saldırı çeşitlerinin daraltılmasını, tehditlerin erken aşamada tespit edilmesini ve olay müdahale süreçlerinin hızlandırılmasını sağlar. Her geçen zaman diliminde saldırganların kullandıkları bu stratejiler daha da genişlemekte ve çoğalmaktadır. Bu yüzden kuruluşların, sürekli güncellenen Mitre Att&cK yapısını takip ederek güvenlik stratejilerini güçlendirmesi, farkındalığı artırması ve siber tehditlere karşı daha dirençli hale gelmesi kritik öneme sahiptir.

## KAYNAKÇA

<https://app.letsdefend.io/training/lessons/mitre-attck-framework>

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

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

<https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/>

<https://www.upguard.com/blog/what-is-ttp-hunting>

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

<https://attack.mitre.org/>

<https://chatgpt.com/>

