

"MITRE ATT&CK" Nedir? DİKKİD'le Alakası Ne?

Serdar Gülsoy

DİKKİD'i Hatırlamak

Askerliğin ve güvenlik bürokrasisinin temel esaslarından biri, Sun Tzu'nun çağlar öncesinden belirttiği gibi, "düşmanını tanı" prensibidir. Terörle mücadelede ya da bir tehditle karşı karşıya kalındığında, kendi imkân ve kabiliyetlerimizin bilinmesi kadar, karşı tarafın stratejisi, doktrini, taktik ve tekniklerinin bilinmesi de önem kazanmaktadır. Bunun için yıllarca karşı tarafın imkân ve kabiliyetleri araştırılır, incelenir, casusluk filmlerine senaryo olur. Karşı tarafın bu kabiliyeti, Düşman İmkân ve Kabiliyetleri-DİK olarak adlandırılır. Ve bunlardan en kuvvetli ihtimal içerisinde olanı da DİKKİD-Düşman İmkân ve Kabiliyetleri Kabul İhtimal Derecesi olarak ifade edilir.

Peki bunun siber güvenlik alanıyla ilgisi nedir?

Siber güvenlik birimleri de, yıllardır saldırı düzenleyen ve bu maksatla gruplar oluşturan aktörleri, kullandıkları kodlardan, istismar taktik ve tekniklerine kadar çeşitli incelemelere tabi tutup sınıflandırmaya, bir sonraki saldırılarını öngörmeye ya da saldırı anında etkin mücadeleyi gerçekleştirmeye çalışıyorlar.

Yani önce, bu saldıran kimdir, daha önce bir sisteme sızabilmek için hangi yazılımları ve istismar araçlarını denemiştir, saldırganın imkân ve kabiliyetlerini ve bunlardan uygulanması en muhtemel olanı tespitte çalışıyorlar. Çünkü bu grupların da birer şirket ya da küçük ordu gibi olduğunu/çalıştığını düşünecek olursak, çalıştırdıkları kişilerden (hacker) kullandıkları teçhizata kadar belirli bir profesyonel bilgi birikimine sahip olmaları gerekmekte ve bunu sürdürülebilir kılmak durumundalar. Bu da onların o edindikleri yazılım dili ve araçlarıyla belirli bir patern izlemelerini gerekli kılıyor.

Burada devreye ABD merkezli MITRE Kuruluşu (non profit organisation-kar amacı gütmeyen kuruluş) giriyor. MITRE Corporation'ın 2020 yılı geliri 1.9 milyar dolar.[\[i\]](#) Virginia - Tysons Corner bölgesindeki iki ana merkezden biri olan bir binasını ilk gördüğümde büyük apartman komplekslerine verilen devasa isimler gibi büyük bir yerleşke sandığım MITRE'nin, siber güvenliğe ilişkin çalışmalara başladığımda ilk karşıma çıkan konseptin merkezi olduğunu anladım.

MITRE ATT&CK Nedir?[\[ii\]](#)

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge - Düşman Taktiği, Tekniği ve Ortak Bilgileri) gerçek olay gözlemlerine dayalı, düşman taktikleri ve teknikleri hakkında, küresel olarak erişilebilir halde bulunan bir bilgi tabanıdır. ATT&CK bilgi tabanı, özel sektörde, devlet kurumlarında ve siber güvenlik ürünleri ve hizmeti sunan kuruluşlarda, belirli tehdit modellerinin ve metodolojilerinin geliştirilmesi için bir temel olarak kullanılır.

2015 yılında hizmete sunulan MITRE ATT&CK yapısı, "kapsamlı ve güncel siber güvenlik tehdidi bilgileri sunan, ücretsiz, küresel olarak erişilebilir hizmet" ve "tehdit etkinliği, teknikleri ve modellerinin küresel bilgi tabanı" olarak olarak tanımlanmıştır.

MITRE ATT&CK yapısı, ABD federal kurumu olan CISA (Cybersecurity and Infrastructure Security Agency - Siber Güvenlik ve Altyapı Güvenliği Ajansı) ve FBI tarafından da kullanılmaktadır. Ayrıca, California Üniversitesi (Berkeley) ve McAfee (ünlü güvenlik yazılımı şirketi) tarafından 2020'de yayınlanan bir araştırmaya göre, şirketlerin yüzde 80'i MITRE ATT&CK siber güvenlik yapısını kullanmaktadır.[\[iii\]](#) **Yapının son versiyonu "ATT&CK v12", 25 Ekim 2022'de piyasaya sürülmüştür.**[\[iv\]](#)

ATT&CK'nin oluşturulmasıyla, daha güvenli bir siber dünya için, siber güvenlik topluluklarının bir araya getirilmesiyle sorunları çözme misyonu amaçlanıyor. ATT&CK, herhangi bir kişi veya kuruluşun ücretsiz olarak kullanımına açık şekilde hizmet veriyor.

APT (Advanced Persistent Threat) Nedir?

MITRE ATT&CK olarak adlandırılan yapıda, bugüne kadar yapılan binlerce siber atak incelenmiş, hacker'ların kullandıkları yazılım uygulamaları ve sızma teknikleri tespit edilmiş. Bunlardan kendisine isim veren hacker grupları kendi isimleriyle bilinirken (Dragonfly, Cozy Bear vb) henüz isimlendirilmemiş gruplar da numaralarla APT29, APT35 (APT-Advanced Persistent Threat - Gelişmiş Kalıcı/Sürekli Tehdit) tasnif edilmiş. APT'ler bir kişi veya grubun bir ağa yetkisiz erişim sağladığı ve uzun bir süre boyunca algılanamadığı bilgisayar ağı saldırısıdır.[\[v\]](#) APT'lerin bu imkân ve kabiliyete kavuşabilmesi ve bunu sürdürülebilmesi için (mesela yerleri veya grup üyelerinin tespit edilememesi için) devlet veya istihbarat birimleri tarafından desteklenmeden yaşamaları mümkün gözüküyor. Bu nedenle APT'ler çoğunlukla, devlet destekli olarak, Çin, Kuzey Kore, İran ve Rusya'dan çıkıyor.*

Lazarus Group (APT38), Cozy Bear (APT29), Leviathan, CopyKittens, Deep Panda, Oilrig, Sandworm gibi ünlü grupların sıralandığı[\[vi\]](#) MITRE ATT&CK APT Gruplar listesindeki "Sandworm"un Rusya Genelkurmay İstihbarat Dairesi (GRU) Özel Teknolojiler için Ana Merkezi tarafından yürütülen bir grup olduğunu da görüyoruz.

MITRE ATT&CK yapısı içerisinde şu ana kadar 129 grup bu şekilde tasniflenmiş. Bu grupların her birinin kullandığı teknikler, istifade ettikleri yazılımlar, birbirleriyle bağlı veya işbirliği yapan gruplar ve bunların referansları belirtilmiş.

MITRE ATT&CK Ne Sunuyor?

Matriste "Taktikler ve Teknikler", hem kurumsal (enterprise) sistemler hem de mobil sistemler için ayrı ayrı belirlenmiş.

Keşif, saldırganın sızma istediği sisteme ilk erişimi, kimlik bilgilerine erişim, saldırganın ilk erişimi sağladıktan sonra ağın derinliklerine ilerlemek için kullandığı sonraki hareketler (lateral movement), kalıcılık, komuta ve kontrol, sisteme sızma gibi daha birçok teknik teker teker incelenmiş ve şablonlaştırılmaya çalışılmış.

Kurumsal ve mobil kullanıcılar için taktik ve teknikler matrisi yayınlayan MITRE, saldırganın keşifte kullandığı taktik ve tekniklerden, saldırganın arzu ettiği nihai son duruma kadar, tüm saldırı aşamalarında (burada Cyber Kill Chain'den [\[vii\]](#) daha ayrıntılı bir kademelendirme görüyoruz) neler yapabileceğini ve bunu nasıl yapabileceğini anlatıyor. Bu bize askerî eğitimlerde üzerinde hassasiyetle ve en detaylı biçimde çalıştığımız 'Olay Matrisi'ni hatırlatıyor.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (3)	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	Adversary-in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (2)	Account Access Removal
Gather Victim Host Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (2)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Data Transfer Size Limits	Data Destruction	Data Encrypted for Impact
Gather Victim Identity Information (2)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	Credentials from Password Stores (2)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Communication Through Removable Media	Exfiltration Over Alternative Protocol (2)	Data Manipulation (2)
Gather Victim Network Information (3)	Develop Capabilities (2)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Gather Victim Org Information (2)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Browser Extensions	Browser Extensions	Browser Extensions	Forced Authentication	Cloud Service Dashboard	Remote Service Hijacking (2)	Browser Session Hijacking (2)	Data Obfuscation (2)	Disk Wipe (2)	Endpoint Denial of Service (2)
Phishing for Information (2)	Obtain Capabilities (2)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (2)	Create or Modify System Process (2)	Forge Web Credentials (2)	Cloud Service Discovery	Remote Services (3)	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Other Network Medium (1)	Firmware Corruption
Search Closed Sources (2)	Stage Capabilities (2)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create Account (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Encrypted Channel (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Inhibit System Recovery
Search Open Technical Databases (2)	Trusted Relationship	Software Deployment Tools	Shared Modules	Event Triggered Execution (1)	Event Triggered Execution (1)	Event Triggered Execution (1)	Modify Authentication Process (2)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Network Medium (1)	Network Denial of Service (2)
Search Open Websites/Domains (2)	Valid Accounts (2)	System Services (2)	System Services (2)	Event Triggered Execution (1)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Sniffing	Domain Trust Discovery	Tam Shared Content	Data from Information Repositories (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Resource Hijacking
Search Victim-Owned Websites	Windows Management Instrumentation	User Execution (2)	User Execution (2)	External Remote Services	Hijack Execution Flow (1)	Hijack Execution Flow (1)	OS Credential Dumping (2)	File and Directory Discovery	Use Alternate Authentication Material (2)	Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Service Stop
				Hijack Execution Flow (1)	Impair Defenses (2)	Impair Defenses (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	System Shutdown/Reboot
				Process Injection (1)	Indicator Removal on Host (2)	Indicator Removal on Host (2)	Steal or Forge Harbored Tickets (2)	Network Share Discovery		Data from Removable Media	Protocol Tunneling		
				Scheduled Task/Job (2)	Indirect Command Execution	Indirect Command Execution	Steal Web Session Cookie	Network Sniffing		Data Staged (2)	Proxy (2)		
				Valid Accounts (2)	Masquerading (1)	Masquerading (1)	Two-Factor Authentication Interception	Password Policy Discovery		Email Collection (2)	Remote Access Software		
				Office Application Startup (2)	Modify Authentication Process (2)	Modify Authentication Process (2)	Unsecured Credentials (1)	Peripheral Device Discovery		Input Capture (2)	Traffic Signaling (1)		
				Pre-OS Boot (2)	Modify Cloud Compute Infrastructure (2)	Modify Cloud Compute Infrastructure (2)	Query Registry	Permission Groups Discovery (2)		Screen Capture	Web Service (2)		
				Scheduled Task/Job (2)	Modify Registry	Modify Registry	Remote System Discovery	Process Discovery		Video Capture			
				Server Software Component (2)	Modify System Image (2)	Modify System Image (2)	Software Discovery (1)	System Information Discovery					
				Traffic Signaling (1)	Network Boundary Bridging (1)	Network Boundary Bridging (1)	System Location Discovery (1)	System Location Discovery (1)					
				Valid Accounts (2)	Obfuscated Files or Information (2)	Obfuscated Files or Information (2)	System Network Configuration Discovery (1)	System Network Configuration Discovery (1)					
					Pre-OS Boot (2)	Pre-OS Boot (2)	System Network Connections Discovery	System Network Connections Discovery					
					Process Injection (1)	Process Injection (1)							
					Reflective Code Loading	Reflective Code Loading							
					Rogue Domain Controller	Rogue Domain Controller							

MITRE ayrıca tüm bu taktik ve tekniklerle yapılacak saldırı çeşitlerine yönelik çözümler öneriyor.[\[viii\]](#) Hesap Kullanım politikaları, Anti-virüs/Kötü Amaçlı Yazılımdan Koruma, Kimlik Bilgileri Erişim Koruması, Veri yedekleme, Veri kaybını önleme vb. daha birçok başlık altında güvenlik maksatlı neler yapılması gerektiği yayınlanıyor.

Sadece MITRE değil, CrowdStrike, Fireeye, Kaspersky gibi diğer siber güvenlik çözümleri sunan şirketler de benzeri sınıflandırma ve çözümlere önem veriyor, katkı sağlıyor. Örneğin Kaspersky, yıl içerisinde her çeyrekte o dönem en aktif APT'leri ve faaliyetlerini yayınlarken bilişim sistemlerini kullanan tüm kullanıcılara ikazlarda bulunuyor.[\[ix\]](#)

Mesela 2021'in sonuna doğru Çin merkezli HoneyMyte saldırı grubunun tekrar aktifleştiği ifade ediliyor. Aynı grubun 2019 yılında Myanmar, Moğolistan, Etiyopya, Vietnam ve Bangladeş'teki hükümetlerinin yanı sıra; Pakistan, Güney Kore, ABD, İngiltere, Belçika, Nepal, Avustralya ve Singapur'da bulunan yabancı elçilikleri de hedef aldığı belirtiliyor. Grubun 2019'da doğal kaynak yönetimi ile ilgili Myanmar'daki devlet kuruluşlarını ve Afrika'daki büyük organizasyonları hedef aldığı belirtiliyor. HoneyMyte'nin ana motivasyonlarından birinin jeopolitik ve ekonomik istihbarat toplamak olduğu iddia ediliyor.[\[x\]](#) Çin'in son dönemdeki Afrika açılımlarını, demek ki siber güvenlik ve saldırılar bağlamında da okumak gerekiyor.

WORLD TERROR ATT&CK - Dünya Terör Örgütleri Taktik ve Teknikleri Ortak Yapısı Mümkün mü?

MITRE ATT&CK** platformu, tüm illegal hacker gruplarının siber saldırı teknik ve taktiklerini, grupların iş birliği içinde olduğu diğer saldırı gruplarını, kullandıkları yazılımları ve bu yazılımlarla ülkelerin ya da organizasyonların hangi bilişim sistemlerini/zafiyetlerini hangi metotlar ve kodlarla istismar ettiğini gözümüzün önüne seriyor. Diğer kurum ve kuruluşlarla iş birliği yaparak çözüm önerileri öneriyor.

Siber saldırılar için kullanılan bu kodifikasyon ve çözümlene, acaba silahlı terör grupları için de mümkün mü? Dünya barışına katkı sağlamak isteyen ülkeler ve orduları, acaba terör örgütlerinin teknik ve taktiklerini birbirleriyle paylaşacakları ve bunların her birine ortak çözüm önerileri getirecekleri bir organizasyon ya da mekanizmayı bir gün kurabilir mi?

Neden olmasın!?

* Gereksiz Bilgi Dipnotu: Nedense "kitten" ismi çokça APT tarafından kullanılırken, "dog-puppy" isimli grup yok denecek kadar az!?

** MITRE 2016 ve 2017'de, ABD'de en çok çalışılmak istenen 10 şirketin arasında gösterilmiş.[\[xi\]](#)

[\[i\]](https://impact.mitre.org/) <https://impact.mitre.org/>

[\[ii\]](https://attack.mitre.org/) <https://attack.mitre.org/>

[\[iii\]](https://en.wikipedia.org/wiki/Mitre_Corporation) https://en.wikipedia.org/wiki/Mitre_Corporation

[\[iv\]](https://attack.mitre.org/resources/versions/) <https://attack.mitre.org/resources/versions/>

[\[v\]](https://tr.wikipedia.org/wiki/Gelişmiş_Sürekli_Tehdit) https://tr.wikipedia.org/wiki/Gelişmiş_Sürekli_Tehdit

[\[vi\]](https://attack.mitre.org/groups/) <https://attack.mitre.org/groups/>

[\[vii\]](#)

<https://www.cizgiotesi.info/bilim-teknoloji/siber-saldiri-asamaları-siber-olum-zinciri-cyber-kill>

-chain/

[viii] <https://attack.mitre.org/mitigations/enterprise/>

[ix] <https://securelist.com/apt-trends-report-q3-2021/104708/>

[x] <https://securelist.com/ksb-2019-review-of-the-year/95394/>

[xi] <https://www.washingtonpost.com/graphics/2017/business/top-workplaces/>