"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 tespite 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 gözükmüyor. 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.

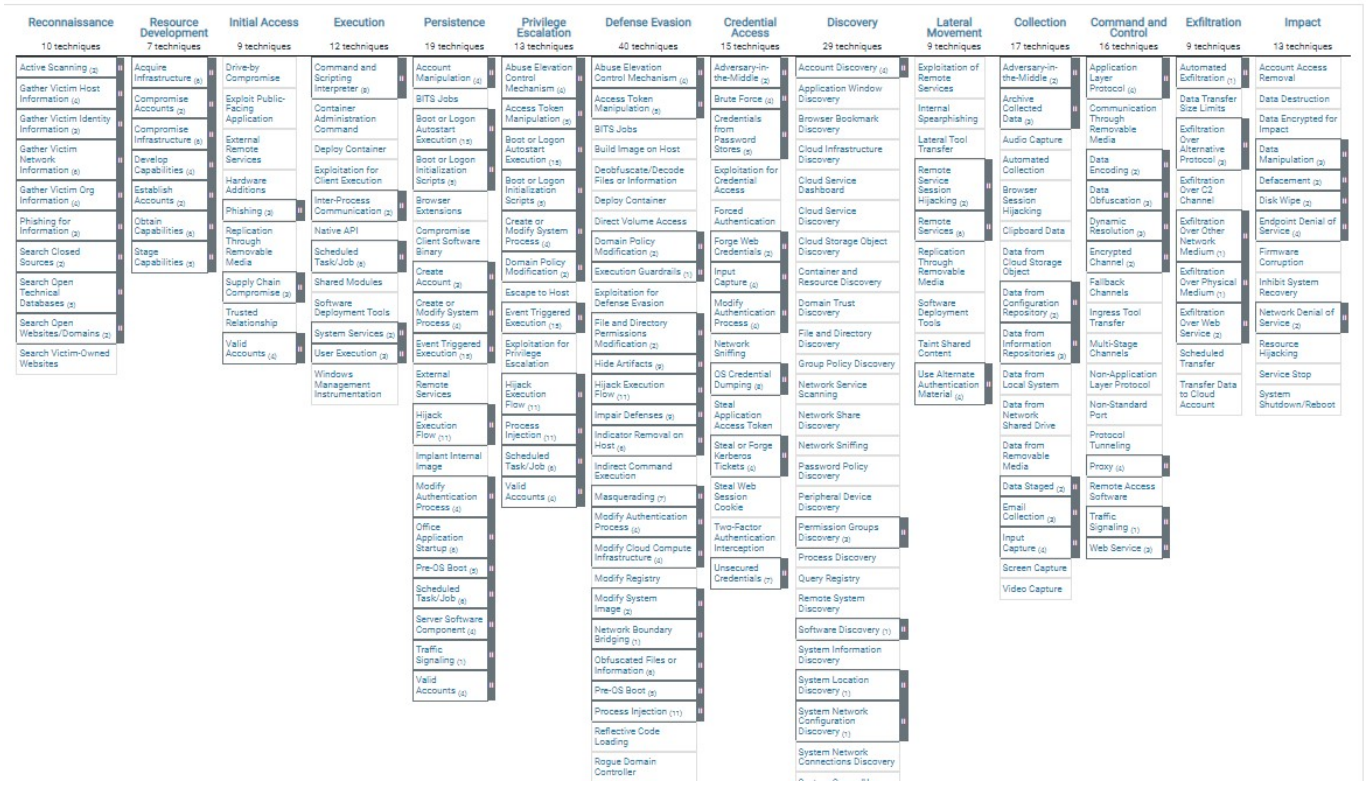
MITRE ATT&CK yapısı içerisinde şu ana kadar 129 grup bu şekilde tasniflenmiş. Bu grupların her birinin kullandığı teknikler, istifade ettikleri yazılımlar, birbirleriyle bağlı veya işbirliği yapan gruplar ve bunların referansları belirtilmiş.

MITRE ATT&CK Ne Sunuyor?

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

Keşif, saldırganın sızmak 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.



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 çözümlemelere önem veriyor, katkı sağlıyor. Örneğin Kaspersky, yıl içerisindeki her çeyrekte o dönem en aktif APT'leri ve faaliyetlerini yayınlayarak 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 çözümleme, 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/

[ii] https://attack.mitre.org/

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

[iv] https://attack.mitre.org/resources/versions/

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

[vi] https://attack.mitre.org/groups/

[vii]
https://www.cizgiotesi.info/bilim-teknoloji/siber-saldiri-asamalari-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/