EXCLUSIVE NETWORKS

Infoblox
NEXT-LEVEL NETWORKING

MITRE ATT&CK'e Giriş

Bu Eşsiz Güvenlik Kaynağını Kullanarak Siber Savunmanızı Nasıl Desteklersiniz?

İçindekiler Tablosu

Yönetici Özeti

MITRE ATT&CK, siber güvenlik ekipleri için paha biçilmez bir kaynaktır. Güvenlik uygulayıcılarınız, gerçek gözlemlere dayanan atak taktikleri ve tekniklerine ilişkin bu etkileşimli veri tabanını kullanarak, siber saldırıların nasıl çalıştığını daha iyi anlayabilir ve bu siber saldırıları önceden tahmin etmek ve engellemek gerektiğinde daha hızlı ve daha sonuç odaklı kararlar verebilir.

MITRE ATT&CK Nedir?

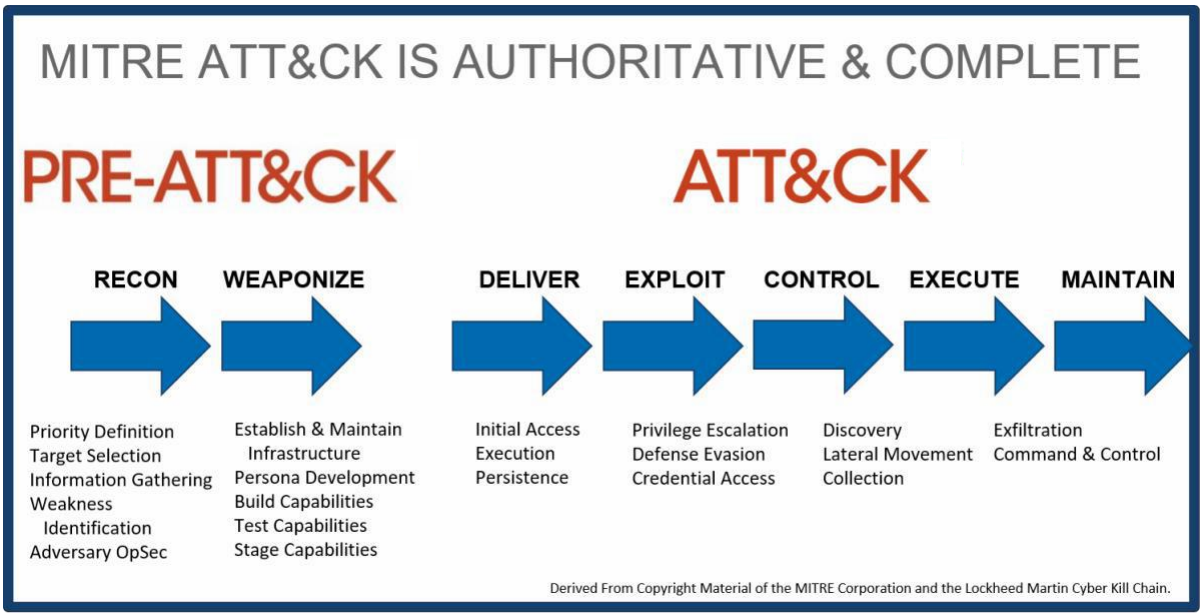
1958'de kurulan tarafsız bir kuruluş olan MITRE Corporation, ABD'nin çeşitli alanlarda faaliyet gösteren devlet kurumları için çalışmaktadır. MITRE ATT&CK (Saldırgan Taktikleri, Teknikleri Ve Ortak Bilgileri [*Adversarial Tactics, Techniques, And Common Knowledge*]), MITRE Corp tarafından 2015 yılında geliştirilmiş ve piyasaya sürülmüştür. MITRE ATT&CK çerçevesi, saldırgan davranışının fiilen gözlemlenmesiyle toplanan siber saldırgan taktikleri ve tekniklerinden oluşan kapsamlı bir bilgi tabanıdır. Siber savunma ekibinizde yer alan herkes, MITRE ATT&CK bilgi tabanında bulunan verileri kullanarak, saldırgan faaliyetlerini inceleyebilir ve karşılaştırabilir ve ardından savunma için en iyi seçenekleri anlayabilir. Bu sistem, ücretsiz olup herkese açıktır.

MITRE ATT&CK, siber güvenlik riskini değerlendirmek ve potansiyel güvenlik açıklarını belirlemek için nesnel bir ortam sağlar. Bu güvenlik açıkları anlaşıldıktan sonra, kurumunuz bu risklerin ele alınması konusunda objektif kararlar alabilir. Kurumunuz daha sonra güvenlik kontrollerinin ve diğer kaynakların dağıtımı açısından öncelikleri belirleyebilir ve en iyi süreç kararlarını verebilir.

MITRE ATT&CK, bir suiistimal gerçekleştikten sonra bir saldırganın davranışını daha iyi anlamak için kapsamlı bir sınıflandırma sağlar. Başka bir deyişle, çerçeve, bir saldırgan gibi düşünmenizi sağlar ve savunma önlemlerinizi bir saldırganın atması muhtemel adımlara karşı dengelemenize yardımcı olur. MITRE ATT&CK'i kullanmaktaki amaç, riskleri değerlendirme, yeni güvenlik kontrollerini devreye alma ve ağınızı savunma konusunda daha iyi kararlar vermektir.

MITRE ATT&CK, saldırıları çok tutarlı bir şekilde bölümlere ayırmıştır; bu da saldırıları karşılaştırmayı ve saldırganların ağınızdan nasıl yararlanmış olabileceğini belirlemeyi kolaylaştırır. Ek olarak, öncelikle çevre savunmalarına odaklanma eğiliminde olan tipik saldırı analizinin çok daha ötesindedir. Tipik saldırı analizinin aksine, MITRE ATT&CK, saldırganları içeri girdikten sonra çok daha yakından inceler. Saldırı sonrası davranışın anlaşılması, ağ çevrelerinin hızla değiştiği için, günümüzde çok önemlidir. Gerçek şu ki, bulut ağ iletişimi ve mobil kullanımlara geçiş arttıkça ve sürekli değişen saldırılar statik imzalardan kaçmaya devam ettikçe, bir noktada bir saldırganın ağınıza başarıyla sızması olasıdır. MITRE ATT&CK'in saldırgan davranışına ayrıntılı bir şekilde odaklanması, devam eden bir saldırıyı veri hırsızlığı veya yıkıcı davranış gerçekleşmeden önce bulmanın ve durdurmanın en iyi yoludur.

MITRE ATT&CK, tek siber güvenlik çerçevesi değildir. Lockheed Martin Cyber Kill Chain, ISO/IEC 270011, NIST siber güvenlik çerçevesi[2] ve COBIT[3] gibi birkaç önemli güvenlik çerçevesi daha bulunmaktadır. MITRE ATT&CK, gerçek dünya testi ve süreci için son derece ayrıntılı yetenekler sağlar; MITRE ATT&CK'i diğer güvenlik çerçevelerinden ayıran en önemli özelliği, saldırganın bakış açısından saldırının nasıl göründüğüne dair derin ve ayrıntılı veriler sunmasıdır. MITRE ATT&CK ayrıca bir saldırganın güvenlik ihlali sonrası davranışının en son ayrıntısına kadar odaklanır. Kavramsal olarak, MITRE ATT&CK, Cyber Kill Chain 'in bir alt kümesini kapsar, ancak çok daha fazla derinlik ve ayrıntıya girer. Enterprise ATT&CK; Windows, Linux, macOS ve Android ve iOS kullanan mobil cihazları kapsar.



Şekil 1: MITRE PRE-ATT&CK ve ATT&CK ile eşleştirilen Siber Öldürme Zinciri

Ayrıca, siber savunucuların bir saldırıyı saldırgan ağa erişmeden önce önlemesine yardımcı olan MITRE PRE-ATT&CK bulunmaktadır. Özünde, PRE-ATT&CK için üst düzey taktik kategorileri, Siber Öldürme Zincirinin ilk iki aşamasıyla ilişkilidir. PRE-ATT&CK, bir siber saldırganın hedefleri tanımlamak, bilgi toplamak ve ardından bir saldırı başlatmak için kullanacağı taktikleri, temel teknikleri ve prosedürleri sunar. MITRE PRE-ATT&CK, riski daha doğru bir şekilde değerlendirebilmeleri ve hafifletme eylemlerini daha iyi planlayabilmeleri için siber savunuculara olası saldırgan faaliyetlerine ilişkin daha kapsamlı bir görünüm sağlar.

ATT&CK Siber Savunuculara Ortak Bir Dil Getiriyor

MITRE ATT&CK, siber saldırganların hedeflerine ve adım adım kullanacakları taktik ve tekniklere ortak bir sınıflandırma getiriyor. Bu paylaşılan dil, bir tehdidin tam ayrıntıları hakkında siber savunma topluluğundaki diğer kişilerle net bir şekilde iletişim kurmanızı sağlar. Ayrıca, mevcut güvenlik kontrollerinizi ve süreçlerinizi açıklamaya yönelik kullanışlı bir yöntem de4 sağlar.

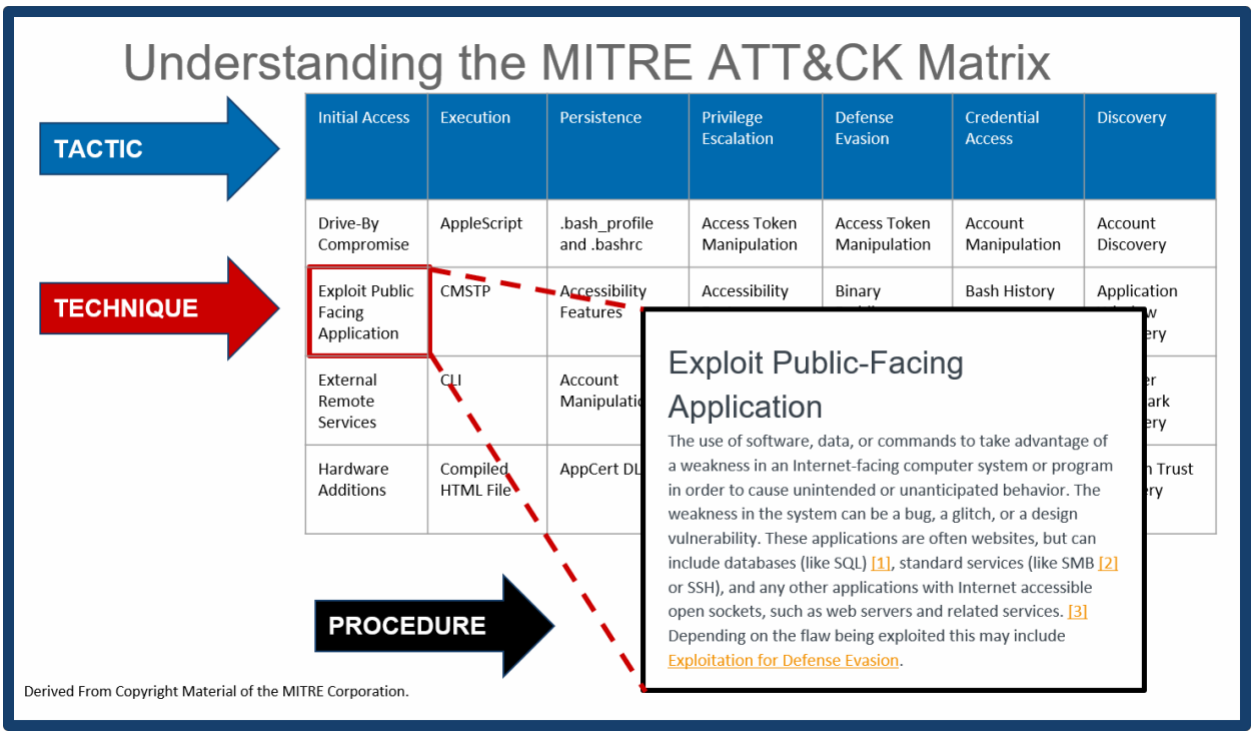
Çok temel bir düzeyde, MITRE ATT&CK, güvenlik uygulayıcılarının bir tehdidin doğasını net bir şekilde tanımlamasına, bu tehdidi, bu tehdide karşı koruma sağlaması gereken kontrollerle eşleştirilmesine ve daha sonra bu kontrollerin etkili olup olmadığına karar vermesine olanak sağlar.

MITRE'nin bilgi tabanını geliştirmek için kullandığı güvenilir veri kaynakları şunları içermektedir: kötü amaçlı yazılım örnekleri; güvenlik sunumları, tehdit istihbaratı raporlaması ve sosyal medya, bloglar ve web seminerleri dahil olmak üzere çeşitli diğer kamu ve özel kaynaklar. MITRE'nin güvendiği bir başka mükemmel bilgi tabanı kaynağı da güvenlik açıklarını bulmak amacıyla bir kuruluşun ağına saldırmaları için işe alınan, bir nevi sızma testçisi görevi gören güvenlik "Red Team" tarafından kullanılan tekniklerdir.

MITRE ATT&CK Nasıl Organize Ediliyor?

MITRE ATT&CK Enterprise Matrix; Windows, Mac ve Linux sistemlerini ilgilendirebilecek tüm saldırı teknikleri için gezilebilir bir sınıflandırma sağlar. MITRE organizasyonunun[4] çevrimiçi bir araç olarak sunduğu matris, her biri 9 ila 67 farklı tekniğe dayanan 12 taktiği kapsamaktadır. Bazı durumlarda, farklı taktikler aynı teknikleri kullanabilmektedir.

Şekil 2, bazı taktik ve tekniklere dair kısmi bir görünüm sunmaktadır. Taktikler, her birinin altında görünen ilişkili tekniklerle birlikte en üstte listelenmiştir. Saldırganların izlediği prosedürlerle ilgili ayrıntılar her teknik için mevcuttur.



Şekil 2: Çevrimiçi MITRE ATT&CK Enterprise Matrix'ten örnekler

Taktikler

Taktikler, bir saldırganın ulaşmaya çalıştığı hedefleri temsil eder. Örneğin, başlıca taktiklerden biri sızdırmadır. MITRE ATT&CK sınıflandırmasında, sızdırma, saldırganların sistemlerinizden veri çalmak için kullanabilecekleri tüm teknikleri içermektedir. Saldırganlar verileri sızdırırken, yazılım kontrolleriniz tarafından algılanmamak için genellikle varlıklarını dikkatli bir şekilde paketler ve kamufle ederler. Bu kamuflaj, sıkıştırma veya şifreleme kullanımını, aktarım boyutunu sınırlamayı, komuta ve kontrol kanallarında ve diğer faaliyetlerinde kullandıklarından farklı bir protokol kullanmayı içerebilir.

Aşağıda, MITRE ATT&CK Enterprise çerçevesindeki taktiklerin temel bir özeti yer almaktadır:

Kurumsal Taktikler Matrisi	
İlk Erişim (Initial Access)	Saldırgan ağınıza girmeye çalışıyor.
Çalıştırma (Execution)	Saldırgan kötü amaçlı kodu sisteme sızdırmaya çalışıyor.
Kalıcılık (Persistence)	Saldırgan, edindiği yeri korumaya çalışıyor.
Ayrıcalık Yükseltme (Privilege Escalation)	Saldırgan daha üst düzey izinler elde etmeye çalışıyor.
Savunmayı Atlatma (Defense Evasion)	Saldırgan, tespit edilmekten kaçınmaya çalışıyor.
Kimlik Bilgilerine Erişim (Credential Access)	Saldırgan hesap adlarını ve parolaları çalmaya çalışıyor.
Keşif (Discovery)	Saldırgan ortamınızı anlamaya çalışıyor.
Yanal Hareket (Lateral Movement)	Saldırgan ortamınızda gezinmeye çalışıyor.
Toplama (Collection)	Saldırgan, kendi amacına uygun verileri toplamaya çalışıyor.
Komuta ve Kontrol (Command& Control)	Saldırgan, güvenliği ihlal edilmiş sistemleri kontrol etmek için onlarla iletişim kurmaya çalışıyor.
Sızma (Exfiltration)	Saldırgan veri çalmaya çalışıyor.
Etki (Impact)	Saldırgan, sistemlerinizi ve verilerinizi manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalışıyor.

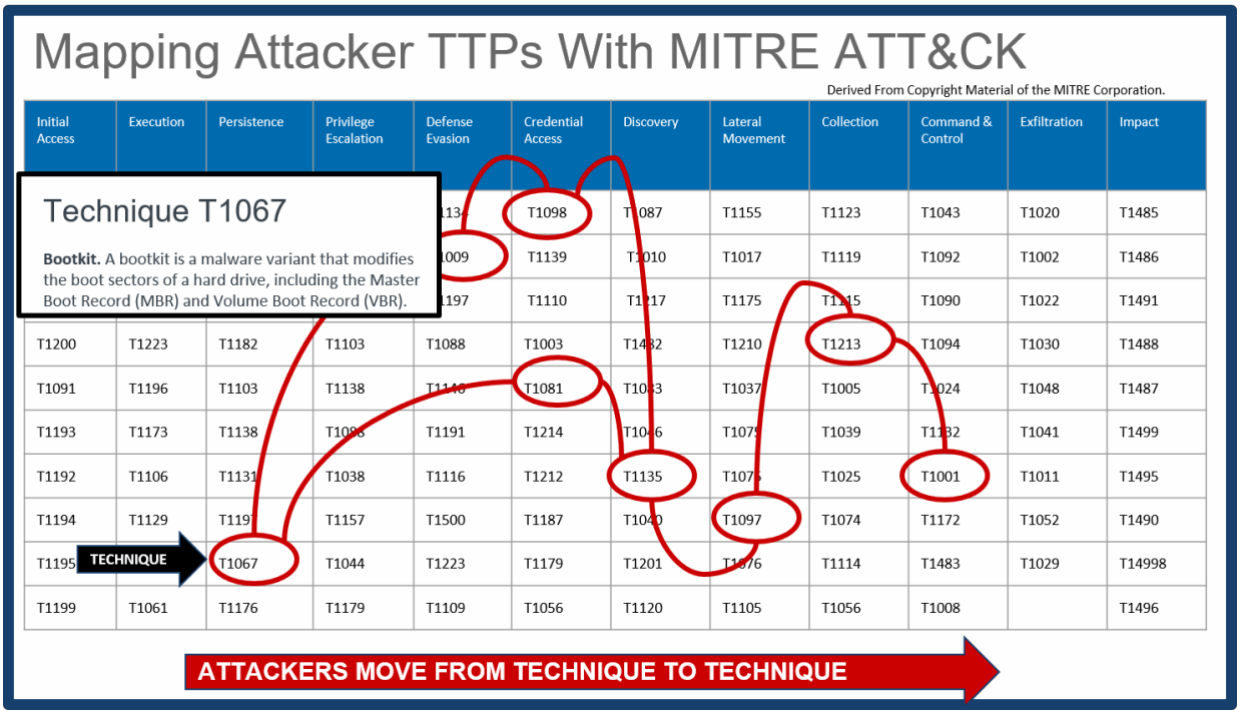
Tablo 1: MITRE ATT&CK taktiklerinin açıklamaları

Teknikler

Teknikler, siber saldırganların taktiklerinin amaç ve hedeflerine ulaşabilecekleri farklı yolları tanımlar. Çevrimiçi matris aracını kullanarak, teknik kimliğine veya adına çift tıklayarak teknikleri ayrıntılı olarak inceleyebilirsiniz. Açılan kısımda tekniğin daha ayrıntılı açıklamalarını, olası hafifletmeleri ve bu tekniğin kullanımıyla ilişkili kötü amaçlı yazılım örneklerini göreceksiniz.

> “Saldırganlar genellikle kendilerine başarı getiren aynı taktik, teknik ve prosedürlere bağlı kalırlar. Sonuç olarak, faaliyetleri, kim olduklarını gösteren dijital parmak izleri bırakıyor. Teknikten tekniğe geçerken kimliklerine, atacakları olası adımlara ve onları verileri sızdırmadan ve operasyonlarınızı etkilemeden önce durdurmanın en iyi yollarına dair ipuçları ve püf noktaları sağlarlar.”
>
> *Anthony James, Ürün Pazarlamadan Sorumlu Başkan Yardımcısı, Infoblox*

Açıklamalar ayrıca, algılama için rehberliğin yanı sıra belirli tekniklerle ilişkili genel kullanıma açık veri referanslarının tamamını sunmaktadır. Şekil 3, aktif bir tehditte tespit edilen bir tehdit grubu tarafından kullanılan farklı tekniklere dair bir örnektir. Saldırganların taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) ATT&CK Matrisi ile eşleştirerek, kim oldukları, daha sonra ne yapabilecekleri ve onları durdurmanın en iyi yolu hakkında bir fikir oluşturabilirsiniz. Bu modelleri, güvenlik kontrollerinizin yeteneklerini ölçmek amacıyla benzetilmiş senaryolar çalıştırmak için, Red Team'i kullanarak ya da MITRE ATT&CK çerçevesinden faydalanan bir ihlal ve saldırı simülasyon sistemi kullanarak oluşturabilirsiniz.



Şekil 3: Saldırgan etkinliklerini tekniğe göre eşleştirme

ATT&CK Grupları

MITRE ATT&CK ayrıca saldırgan adlarının netleştirilmesine yardımcı olur ve farklı saldırgan grupları tarafından düzenlenen tekniklerin ve yazılım araçlarının kullanımı için iyi belgelenmiş bir veri tabanı geliştirmiştir. MITRE ATT&CK'in[5] Gruplar bölümünde şu anda tanımlanmış 91 grup bulunmaktadır. MITRE, grupları, herkese açık olarak bildirilen teknik kullanımıyla eşleştirerek bir noktaya kadar sıralamaktadır. Bunlar gruplar tarafından kullanılan tekniklerin tamamı olmayabilmektedir; yalnızca MITRE'nin düzenli olarak denetlediği açık kaynaklı raporlama yoluyla mevcut olanlardır.

MITRE ATT&CK Grupları, kurumunuza yönelik tehditleri temsil etmesi en muhtemel grupların haritasını çıkarabilmeniz ve ardından bilinen tekniklerini gözden geçirebilmeniz açısından oldukça faydalıdır. Bu yaklaşım, en olası saldırı vektörlerinin risk değerlendirmesine dayalı olarak siber savunmanızda aşamalı iyileştirme için öncelikleri daha iyi belirlemenizi sağlar.

Örnek: APT3'ü derinlemesine incelemek

APT3 grubunu (gelişmiş kalıcı tehditlerle ilişkili bir saldırgan grubu) derinlemesine incelemek için MITRE ATT&CK kullanırsak, gruba genel olarak bir göz atabilir ve MITRE'nin ayrıca bir APT3 Rakip Öykünme Planı sunduğunu görebiliriz. Tehdit istihbaratı kaynağına veya herkese açık olarak bildirilen verilere bağlı olarak APT3, oldukça kesin bir şekilde MITRE ATT&CK kapsamındaki aynı APT3 grubu olarak tanımlanan birçok ilişkili grup tanımından oluşmaktadır.

APT3 için grup tanımları 6 farklı ad içermekte olup hepsinin aynı örgüt olduğu düşünülmektedir.

APT3: İlişkili Grup Açıklamaları
Gothic Panda
Pripi
UPS Team
Buckeye
Threat Group – 0110
TG – 0110

Tablo 2: APT3 ilişkili grup açıklamaları (adlar)

Ayrıca, herkese açık olarak belgelendikleri için kullandıkları teknikleri görebilirsiniz. Tablo 3, tekniği, teknik kimliğini, adı ve tekniğin saldırganlar tarafından kullanımını gösteren MITRE ATT&CK içindeki tablodan bir alıntıdır. Şu anda, APT3 saldırı etkinliğiyle ilişkili 40 kurumsal teknik bulunmaktadır.

Tablo 3 ayrıca, MITRE yazılım kimliğini, yazılımın adını ve yazılımın ilişkilendirildiği teknikleri içeren, APT3 saldırganları tarafından kullanıldığı belgelenen yazılım araçlarını da listelemektedir.

APT3: Kullanılan Yazılım Araçları		
Kimlik	**Ad**	**Teknikler**
S0349	LaZagne	Kimlik Bilgileri Dökümü, Dosyalardaki Kimlik Bilgileri
S0165	OSInfo	Hesap Bulma, Ağ Paylaşımı Bulma, İzin Grupları Bulma, Sorgu Kaydı, Uzak Sistem Bulma, Sistem Bilgisi Bulma, Sistem Ağ Yapılandırması, Sistem Ağ Bağlantıları Bulma
S0013	PlugX	Ve dahası…….
S0166	RemoteCMD	Ve dahası…….
S0111	Schtasks	Ve dahası…….
S0063	SHOTPUT	Ve dahası…….

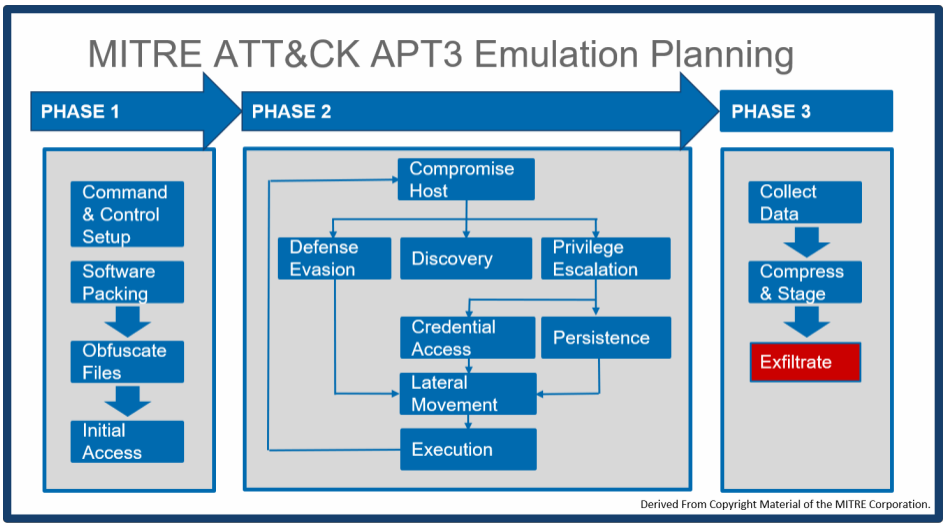
Tablo 3: Saldırganlar tarafından kullanılan APT3 yazılım araçları

MITRE ATT&CK Saldırgan Öykünme Planları (AEP'ler) Nelerdir?

AEP'ler, güvenlik operasyonları ekiplerinin ve tehdit avcılarının ağlarını test etmelerini sağlayan belirli saldırgan etkinliğinin ayrıntılı modelleridir. Herkese açık verilerden derlenmiştir ve tamamını içermeyebilir; ancak bilinen geçmiş performansa dayalı olarak sergilenmesi beklenen davranış açısından genel olarak muhtemelen kuralcıdırlar. Şimdiye kadar, bu planların kullanılabilirliği, tespit edilmiş ve kategorize edilmiş saldırganların çok azıyla sınırlıdır.

AEP'ler, saldırganların teknikleri nasıl sırayla bağladıklarını gösterir; bu, sızma testçilerinin aynı davranışı sergilemelerini ve bir dereceye kadar aynı veya benzer araçları kullanmalarını sağlar. Bu modeller ayrıca güvenlik analistlerine saldırganları anlamanın, güvenlik kontrollerini ve prosedürlerini objektif olarak değerlendirmenin ve savunmalarındaki boşlukları belirlemenin daha iyi bir yolunu sunar. Ayrıca, AEP'ler bir saldırıyı teşhis etmeye ve şüpheli grupları belirlemeye yardımcı olarak, saldırganlardan atmaları beklenebilecek sonraki adımlar konusunda sizi daha hızlı uyarabilir.

APT3 gibi belirli bir APT grubu için akış, veri hırsızlığında amaçlanan aynı nihai hedefe ulaşacak farklı taktik yürütme yolları içerebilir. APT3 AEP'de kullanılan tekniklerin akışını görebilir ve bunu bir akış şemasında kavramsal olarak görselleştirebilirsiniz (Şekil 4).



Şekil 4: Bir APT3 öykünme planlama modelinde saldırı akışına örnek

APT3 akışının herhangi bir bölümünü ağ yayılımı için ayrıntılı olarak incelerseniz, saldırganın hedeflenen saldırıyı yürütmesindeki belirli bir adımla ilişkilendirilebilecek ayrı teknikler görürsünüz.

Örneğin, ana bilgisayar işlemleri sırasında, keşif altında, Tablo 4, APT3'ün çeşitli teknikler kullanılarak belgelendiğini göstermektedir. Daha fazla bilgi için her bir tekniği ayrıntılı olarak inceleyebilirsiniz.

APT3 KEŞİF: ANA İŞLEMLER	
Yerel Sistemi Keşfetme	ATT&CK T1083
Etki Alanı ve Yerel Hesap Grubu Üyeliğini Keşfetme	ATT&CK T1087 ATT&CK T1082 ATT&CK T1069
Diğer Sistemlerle Bağlantıları Keşfetme	ATT&CK T1016 ATT&CK T1049 ATT&CK T1135 ATT&CK T1018
Süreçleri Keşfetme	ATT&CK T1057

Tablo 4: MITRE ATT&CK çevrimiçi aracında APT3 için tanımlanan çeşitli keşif teknikleri için örnek liste

MITRE ATT&CK'e Nasıl Başlayabilirsiniz?

Başlangıçta, mevcut ortamınızda sahip olduğunuz güvenlik kontrollerini seçebilir ve ardından bunları MITRE ATT&CK ile eşleştirebilirsiniz. Taktik ve tekniklere karşı uygulanan kontrollerinizin bu taktik ve tekniklerle karşılaştırılarak yapılan bu temel değerlendirmesi sayesinde, güvenlik açıklarını hemen belirleyebilir, ortamınızdaki olası tehditlerle karşılaştırarak riski değerlendirebilir ve ardından savunmanızı geliştirmek için harekete geçebilirsiniz. Bu değerlendirme potansiyel olarak yazılım geliştirme yaşam döngünüzün (SDLC) bir parçası olabilir ve sonrasında rutin haline gelir. Tekrar edildikçe, savunma duruşunuzu geliştirir, risk alanlarını daha doğrudan ele alır ve tanımladığınız potansiyel saldırılar karşısında başarılı bir ihlale ilişkin genel riskinizi azaltırsınız.

Red Team, saldırganın dış görünümünü alır. MITRE ATT&CK, teknikleri bu görünümle eşleştirmenize ve olasılık ve riski anlamanıza yardımcı olacaktır. Örneğin, kurumunuz APT3'ün ilgili bir tehdit olabileceğini düşünüyorsa, Red Team buna karşı önlem alıp alamayacağınızı görmeye çalışacaktır.

Blue Team, güvenlik denetimi işlevini, beklediğiniz olası taktikler ve tekniklerle eşleştirebilir. Daha sonra bu kontrollerin etkinliğini karşılaştırmaya başlayabilir ve savunma duruşunuzu iyileştirebilirsiniz. Kıyaslama, hiçbir şekilde korunmadığınız taktikler ve ilgili teknikler hakkında anında bir görüş sağlar. Bunlar, ele alınması gereken büyük açıklarınızdır.

MITRE ATT&CK, karşı karşıya kalacağınız olası tehditlere karşı savunmanızı daha iyi hizalayabilmeniz için daha büyük resmin ortaya çıkmasına olanak tanır. Üst yönetime stratejinizin ne olması gerektiğini ve nedenini açıklamanın net ve objektif bir yolunu sunar. Örneğin, kurumunuzu en çok hangi tehditler ilgilendirmelidir? Kurumunuzun hangi güvenlik kontrollerini edinmesi gerekiyor? Hangi güvenlik kontrolleri gerekli korumayı sağlar? MITRE ATT&CK, bu kararları objektif ve ölçülebilir verilere dayalı olarak optimize etmenize yardımcı olur.

MITRE ATT&CK için Önemli Kullanım Durumları Nelerdir?

MITRE ATT&CK için en iyi kullanım örnekleri arasında Red Team Sızma testi, tehdit istihbaratı, Blue Team, üretici analizi, ihlal ve saldırı simülasyonu yer almaktadır.

Red Team Sızma (Penetrasyon) Testi

Red Team taktikleri ve teknikleri yıllar içinde gelişmiş, ancak kullanılması gereken en iyi uygulamalar konusunda fikir birliğine varamamıştır. MITRE ATT&CK, Red Team'lerin standart bir sözlük kullanmalarına ve çalışmalarını planlamada onları destekleyen taktikleri ve temel teknikleri seçme konusunda düzenli, oldukça organize bir yaklaşım kullanmalarına olanak tanır. MITRE ATT&CK ayrıca Red Team'lerin hem kullandıkları tekniklerle hem de bu teknikleri dağıtma sıralarıyla ve ayrıca dağıttıkları belirli yazılım araçlarıyla gerçek dünyadaki saldırganları modellemelerine de olanak tanır.

Tehdit İstihbaratı

Günümüzde bir güvenlik operasyon merkezinin ve Blue Team'in tehdit istihbarat raporlarına zamanında yanıt vermesi çok zor. Verdikleri ilk tepki genellikle "Bu konuda ne yapmamızı önerirsiniz?" oluyor. Siber saldırganlar daha hızlı hareket ediyor. Siber savunucuların, saldırganlara karşı avantaj elde etmek ve bu avantajı sürdürmek için, güvenlik ihlali olaylarına, imza ve IP adresi gibi metriklere bağımlı olmaktan uzaklaşarak daha davranışsal bir yaklaşıma geçmeleri gerekir.

MITRE ATT&CK, tehdit istihbaratını yapılandırmanın bir yolunu sağlar. IP adresleri ve etki alanları gibi göstergelere odaklanmak yerine belirli davranışlara odaklanırsınız. Daha sonra bunu saldırı tekniğiyle eşleştirebilir ve savunucuların güvenlik açıklarını daha doğru bir şekilde belirlemek, riskleri değerlendirmek ve hafifletme planı yapmak için kullanabileceği çok daha iyi ve tutarlı bir şekilde organize edilmiş veriler sunabilirsiniz.

Blue Team

Blue Team, potansiyel bir siber saldırganın anatomisini daha iyi anlayabilirler. Bu anlayış, mevcut bir saldırıda kullanılan tekniklerin hızlı bir şekilde sınıflandırılmasını, saldırganın kimliğine ilişkin olası bilgileri, kuruma yönelik en olası tehditlerin gelişmiş risk değerlendirmesini ve sonrasında bu tehditlerin objektif olarak ayrıştırılarak siber güvenlik altyapınızın neresinde güvenlik açıkları olabileceğinin anlaşılmasını içerir. Daha sonra bu güvenlik açıkları önceliklendirilebilir ve engellenir.

Üretici Analizi

Üretici ürünleri, faaliyet açısından büyük ölçüde değişiklik gösterebilir. MITRE ATT&CK, kurumunuzun karşı karşıya olduğu riskleri nasıl ele aldıklarını görmek için üretici ürünlerini karşılaştırma potansiyeli sağlar. Güvenlik kontrollerinizi, üreticilerden yapmaları beklenen şeylere göre sınıflandırabilir ve ardından bunları yapıp yapmadıklarını objektif olarak belirleyebilirsiniz. Potansiyel risklere ve siber savunmanızda kapatmanız gereken güvenlik açıklarına göre hangisinin ihtiyaçlarınızı daha iyi karşıladığını görmek için üreticiler arasında karşılaştırma yapabilirsiniz.

İhlal ve Saldırı Simülasyonu

MITRE ATT&CK ayrıca, kullanıcıların açık MITRE ATT&CK yapısına dayalı olarak sürekli güvenlik doğrulama testlerini (ihlal ve saldırı simülasyonu olarak da adlandırılır) tamamen otomatikleştirmelerine olanak tanıyan, gelişmekte olan dış parti ekosistemini de desteklemektedir. Otomatik test, üretim ortamınızdaki test edilmiş güvenlik kontrollerinin performansının sürekli olarak objektif bir değerlendirmesini sağlayan çok güçlü bir kavramdır. Kuruluşunuz daha sonra belgeler ve ayrıntılı raporlamayla, “Güvenlik kontrollerimiz şimdi doğru çalışıyor mu?” sorusuna objektif olarak cevap verebilir. Bu değerlendirmeler, yönetici ve yönetim kurulu sorgulamalarını, uygunluk yönetimini ve bütçe gerekçesini desteklemek açısından faydalıdır. Ayrıca, MITRE ATT&CK tarafından doğru bir şekilde modellenebilen APT3 gibi bilinen bir tehdidin sergilediği davranışa karşı güvenlik kontrollerinizi test etmek için de kullanılabilir.

Özet

MITRE ATT&CK, siber saldırgan taktiklerini, tekniklerini ve prosedürlerini anlamaya ve sınıflandırmaya yönelik son derece güçlü açık kaynaklı bir araçtır. MITRE, saldırganları ve davranışlarını tutarlı ve kolay iletilebilen bir şekilde gruplandırmak için ortak bir sınıflandırma sağlayarak siber savunmanın iyileştirilmesini kolaylaştırır. Siber savunma ekipleri, olası tehditlere ve saldırganların sergileyecekleri taktik ve tekniklere karşı güvenlik kontrolleri için kapsamlı bir strateji tasarlayabilir, riskleri değerlendirebilir ve ardından siber savunmalarındaki boşlukları önceleyebilir ve düzeltebilirler.

Daha fazla bilgi edinmek için, lütfen info.tr@exclusive-networks.com adresinden bizimle iletişime geçin.

REFERANSLAR

1. https://www.iso.org/isoiec-27001-information-security.html
2. https://www.nist.gov/cyberframework
3. http://www.isaca.org/cobit/pages/default.aspx
4. https://attack.mitre.org/matrices/enterprise/
5. https://attack.mitre.org/groups/

Infoblox, Güvenli Bulut Yönetimli Ağ Hizmetleri ile bir sonraki seviye ağ deneyimlerini sağlar. Dünyanın en güvenilir, güvenli ve otomatik ağlarını sağlamanın öncüsü olarak, ağ basitliği arayışımızda amansızız. Endüstride tanınmış bir lider olan Infoblox, Fortune 500'ün 350'si dahil olmak üzere 8.000 müşteriden oluşan yüzde 50'lik bir pazar payına sahiptir.