Mitre Att&ck Framework

Hazırlayan: Esra Akteke

Tarih: 17.02.2025

İçindekiler

Giriş

Siber güvenlik, günümüz dijital dünyasında her geçen gün daha kritik bir hale gelmektedir. Hem kişisel hem de kurumsal düzeyde bilgi güvenliğini sağlamanın zorlukları arttıkça siber tehditlere karşı koyabilmek için güçlü verimli ve yenilikçi çözümler gereklidir. Bu bağlamda aslında siber tehditlerin daha iyi anlaşılması ve etkin bir şekilde savunulması için kullanılan çeşitli metodolojiler önemli bir rol oynamaktadır. Bunlardan biri de Mitre ATT&CK Framework'tür diyebiliriz.

Siber tehdit ortamının giderek karmaşıklaştığı günümüzde, kuruluşlar tehdit aktörlerinin taktiklerini, tekniklerini ve prosedürlerini anlamak zorundadır. MITRE ATT&CK, bu ihtiyacı karşılamak amacıyla geliştirilmiş, tehdit odaklı bir bilgi tabanıdır. Bu çerçeve güvenlik profesyonellerine tehdit aktörlerinin davranışlarını analiz etme ve buna dayanarak savunma stratejileri geliştirme imkanı tanır. Ayrıca güvenlik ekiplerinin saldırganların sistemlere nasıl sızdığına dair daha derin bir anlayış kazanmasını ve buna uygun tehdit avcılığı süreçlerini oluşturmasını sağlamaktadır.

Mitre ATT&CK dediğimiz şey yalnızca bir saldırı haritası değil aynı zamanda güvenlik ekiplerine tehditleri tespit etmek ve etkili bir şekilde engellemek için gerekli olan bilgileri sunan güçlü bir araçtır. Yazılan bu rapor aslında bu çerçevenin içeriğini ve önemini derinlemesine inceleyerek siber güvenlik dünyasında hem teorik hem de pratik anlamda daha sağlam bir temele sahip olunmasını sağlamayı amaçlamaktadır.

Mitre ATT&CK Tablosu Nedir?

MITRE ATT&CK Tablosu, siber güvenlikte saldırganların uyguladığı teknik ve taktiklerin derlendiği ve sistematik olarak sınıflandırıldığı bir bilgi tabanıdır.
Her bir taktik saldırganların siber saldırı sırasında gerçekleştirmeyi amaçladıkları hedefleri tanımlar. Oysa teknikler bu hedeflere ulaşmak için kullandıkları yöntemleri gösterir. Siber güvenlik profesyonellerine saldırganların saldırı yollarını anlamaları ve bu yolları önlemek için savunma stratejileri geliştirmeleri için güçlü bir referans sunar.

Sistemin, saldırganların kullandığı her türlü teknik ve prosedürü içeren detaylı bir yapısı vardır. Bu yapı sadece saldırıların analiz edilmesini değil, aynı zamanda savunma önlemlerinin daha proaktif bir şekilde geliştirilmesini sağlar. Güvenlik uzmanları, geçmişteki saldırı vakalarını kullanarak potansiyel tehditleri belirleyebilir ve bu tehditlere karşı daha etkili savunma stratejileri geliştirebilirler. Bu şekilde saldırganların savunma sistemlerinden kaçınmak için uyguladığı yöntemler hakkında derinlemesine bir bilgi sahibi olunur ve kurumlar güvenlik açıklarını belirleyerek güçlü bir savunma mekanizması kurabilirler.

MITRE ATT&CK aynı zamanda dünya genelindeki tehdit gruplarının kullanmış olduğu stratejilerin analiz edilerek derlendiği ve sürekli güncellenen dinamik bir yapıya sahiptir. Bu sayede yeni ortaya çıkan saldırı tekniklerine ve taktiklerine hızla adapte olabilir. Bu sürekli gelişim; güvenlik ekiplerine daha bilinçli ve güncel kalma imkanı verir.

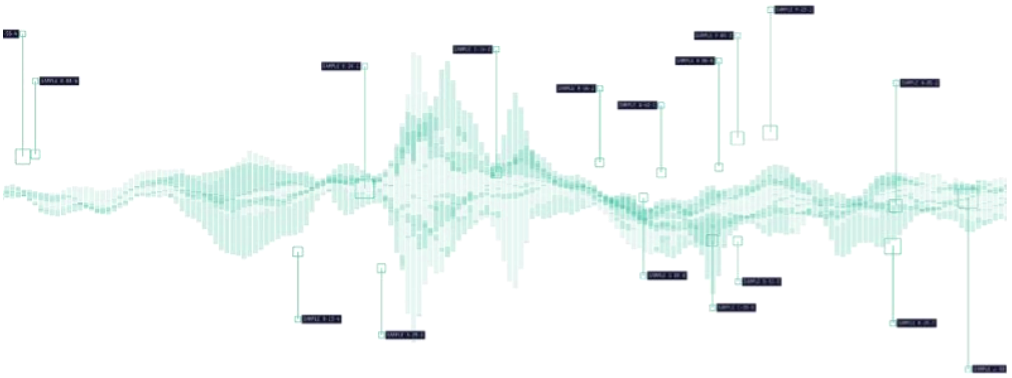
MITRE ATT&CK, farklı kullanım senaryolarına yönelik çeşitli matrislerden oluşur:

Enterprise ATT&CK: Windows, Linux ve macOS gibi işletim sistemlerinde gerçekleştirilen saldırı tekniklerini ve taktiklerini kapsar. Kurumsal ağlara yönelik tehdit aktörlerinin izlediği adımları detaylandırır.

Mobile ATT&CK: Mobil cihazları hedef alan saldırı yöntemlerini ele alır. iOS ve Android sistemlerine yönelik siber tehditlerin nasıl gerçekleştiğini, saldırganların hangi teknikleri kullandığını açıklar.

Pre-ATT&CK: Saldırganların hedef sistemlere erişim sağlamadan önce yürüttükleri keşif ve hazırlık aşamalarını içerir. Bilgi toplama, altyapı oluşturma ve hedef belirleme gibi faaliyetlere odaklanır.

Mitre ATT&CK Tablosu Neden Önemlidir?



MITRE ATT&CK Tablosu siber güvenlik alanında önemli bir referans kaynağıdır çünkü saldırganların davranışlarını detaylı bir şekilde sınıflandırarak, güvenlik ekiplerinin savunmalarını daha hedeflenmiş ve etkili bir şekilde geliştirmelerine yardımcı olur. Bu tablo saldırıların ne şekilde gerçekleşebileceğini, hangi yöntemlerin kullanıldığını ve saldırganların hangi yolları tercih ettiğini analiz etme fırsatı sunar. Sadece teorik değil, gerçek dünyada gözlemlenen saldırılara dayalı bilgiler sunduğundan, uygulamalı bir strateji geliştirilmesine olanak tanır.

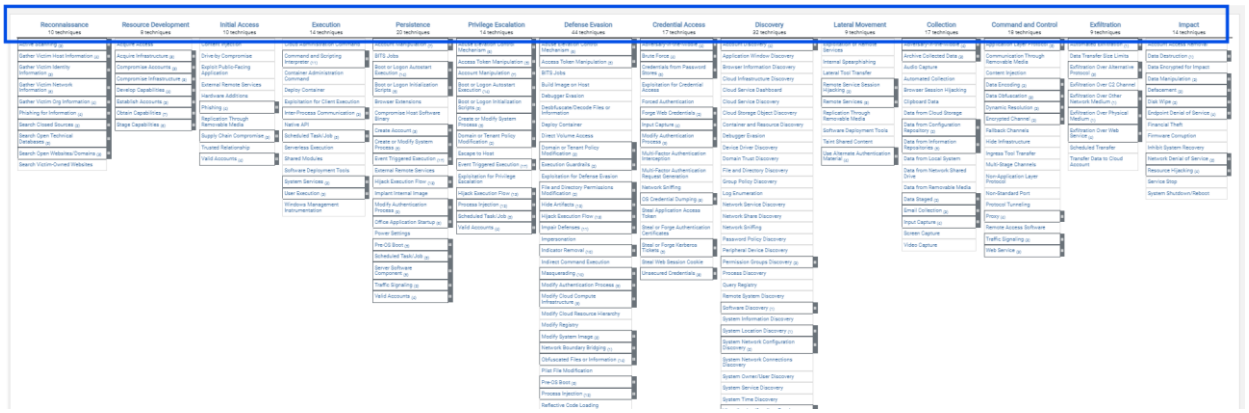
Sürekli güncellenen dinamik yapısı sayesinde tehditleri daha hızlı ve doğru bir şekilde tespit etmeyi mümkün kılması, MITRE ATT&CK'in her geçen gün daha fazla saldırgan davranışını içerecek şekilde genişlemesi, güvenlik ekiplerinin yeni tehditlere karşı hazırlıklı olmalarını sağlar. Bu sayede savunma ekipleri sadece geçmiş saldırılara karşı değil gelecekteki potansiyel tehditlere karşı da proaktif önlemler alabilir.

TTP Nedir?

Taktikler, Teknikler ve Prosedürler (TTP), siber güvenlikte saldırganların hedeflerine ulaşmak için izlediği adımları tanımlayan bir kavramdır. Bu kavramlar saldırganların operasyonlarının her aşamasındaki davranışlarını ve yöntemlerini anlamak için kritik öneme sahiptir. Her biri saldırganın eylemlerinin farklı yönlerini anlamamıza yardımcı olur ve siber güvenlik profesyonellerinin savunma stratejilerini şekillendirmelerinde önemli bir rol oynar.

Taktik Nedir?

MITRE ATT&CK çerçevesinde Taktikler, saldırganların belirli bir hedefe ulaşmak için gerçekleştirdiği geniş kapsamlı adımları temsil eder. Bir saldırının ne amaçla yapıldığını ortaya koyan bu taktikler, saldırının temel yapı taşlarını oluşturur diyebiliriz. Yani saldırganın gerçekleştirdiği her eylem rastgele değil, belirli bir amaca hizmet eden bir stratejinin parçasıdır.



MITRE ATT&CK içindeki taktikleri anlamak, güvenlik uzmanlarına saldırıların genel akışını kavrama ve savunma önlemlerini buna göre şekillendirme konusunda kritik bir avantaj sağlar. Taktikler, saldırı yaşam döngüsünün farklı aşamalarını kapsayarak bir saldırganın sistemde nasıl ilerlediğini gösterir.

MITRE ATT&CK'te Bulunan Taktikler

İlk Erişim (Initial Access) ID:TA0001

Saldırganın hedef sisteme girmesi için kullandığı yöntemleri ifade eder. Bu aşama saldırının ilk adımıdır ve genellikle oltalama saldırıları, kötü amaçlı yazılımlar veya güvenlik açıklarından faydalanma gibi yöntemlerle gerçekleştirilir. Örneğin bir saldırgan, bir çalışana phishing e-postası göndererek, zararlı bir dosyayı açmasını sağladığında başlangıç erişimi elde etmiş oluyor.

Yürütme (Execution) ID:TA0002

Sistemde zararlı bir kodun veya komutun çalıştırıldığı aşamadır. Başlangıç erişimi sağlandıktan sonra, saldırganın sistem üzerinde daha fazla kontrol elde etmesini sağlar. PowerShell veya CMD üzerinden kötü amaçlı komutların çalıştırılması buna örnek verilebilir.

Kalıcılık (Persistance) ID:TA0003

Saldırganın sistemdeki erişimini koruması için yaptığı işlemleri içerir. Buradaki Amaç, sistem kapatılsa veya yeniden başlatılsa bile saldırganın erişiminin devam etmesini sağlamaktır. Windows Registry anahtarlarını değiştirerek kötü amaçlı bir programın her açılışta çalışmasını sağlamak buna örnek verilebilir.

Yükseltilmiş Yetkiler (Privilege Escalation) ID:TA0004

Saldırganın daha yüksek yetkilere sahip bir hesaba erişerek sistemdeki kontrolünü artırmasıdır. Genellikle normal bir kullanıcı hesabı üzerinden sisteme giriş yapan saldırganlar, yönetici yetkilerini ele geçirmeye çalışırlar ve bu sayede elde edilen yüksek yetkili kullanıcı ile sistem üzerinde aktivite gerçekleştirebilirler. Sistem hatalarından yararlanarak bir kullanıcı hesabını yönetici seviyesine yükseltmek buna örnek verilebilir.

Savunmadan Kaçınma (Defense Evasion) ID:TA0005

Saldırganların antivirüs, güvenlik duvarı ve diğer güvenlik çözümlerini atlatmak için uyguladığı tekniklerdir. Bu taktik, saldırının fark edilmeden ilerlemesini sağlamak için kritik bir adımdır diyebiliriz. Kötü amaçlı kodu şifreleyerek antivirüs yazılımlarının tespit etmesini engellemek bu taktiğe örnek olarak verilebilir.

Kimlik Bilgileri Elde Etme (Credential Access) ID:TA0006

Hedef sistemdeki kullanıcı adı, şifre ve diğer kimlik doğrulama bilgilerini ele geçirmek için kullanılan yöntemleri kapsamaktadır. Keylogger yazılımı ile kullanıcının klavyede yazdığı şifreleri kaydetmek buna örnek olarak verilebilir.

Keşif (Discovery) ID:TA0007

Saldırganın hedef sistem hakkında bilgi toplamak için yaptığı çalışmaları içerir. Burada amaç ağ yapısını, kullanıcı haklarını, dosya sistemlerini ve çalıştırılabilir hizmetleri öğrenerek saldırıyı daha etkili hale getirmektir diyebiliriz. Windows'ta net user /domain komutunu kullanarak sistemde hangi kullanıcıların olduğunu keşfetmek örnek olarak verilebilir.

Yanal Hareket (Lateral Movement) ID:TA0008

Saldırganın bir sistemden diğerine geçerek ağ içinde yayılmasını ifade eder. Burada saldırgan, bir kullanıcı hesabı veya açığı kullanarak başka sistemlere erişmeye çalışır.

Çalınan bir hesap bilgisiyle şirketin farklı sunucularına bağlanmak buna örnek olarak verilebilir.

Hedefleme (Collection) ID:TA0009

Saldırganın belirli bir hedef doğrultusunda veri toplaması aşamasıdır. Bu aşama genellikle gizli belgeleri, finansal bilgileri veya oturum açma bilgilerini toplamak için kullanılır. Örneğin belirli bir klasördeki belgeleri sıkıştırıp saldırganın kontrol ettiği bir sunucuya Göndermek veri toplama aşamasında yapılabilecek işlemlerden birisidir.

Etkileşim (Command and Control – C2) ID:TA0011

Saldırganın sistemle uzaktan iletişim kurmasını sağlayan taktikleri kapsar. Burada saldırgan sistem üzerinde komut çalıştırabilir, zararlı yazılımları güncelleyebilir veya veri sızdırabilir. Örnek vermek gerekirse, bir virüsün saldırganın sunucusuna düzenli olarak veri göndermesi iletişim kapsamında yapılabilecek işlemlerden birisidir.

Hedefe Ulaşma (Exfiltration) ID:TA0010

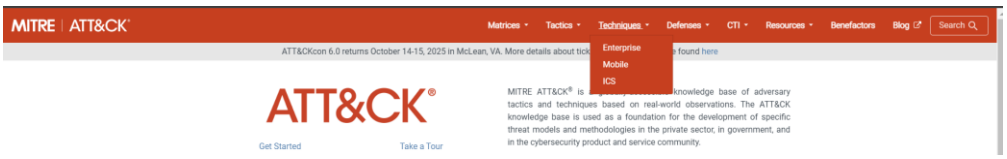
Saldırganın hedef sistemden verileri dışarı çıkardığı aşamadır. Bu aşamada çalınan bilgiler, saldırganın kontrol ettiği sistemlere gönderilir. Hassas verileri şifreleyerek bir bulut hizmetine yüklemek bu aşamaya örnek verilebilir.

Etkiler (Impact) ID:TA0040

Saldırganın, sistemlere zarar verme veya veri bütünlüğünü bozma amacıyla gerçekleştirdiği eylemlerin bütünüdür diyebiliriz. Örnek vermek gerekirse en yaygın olan fidye yazılımı kullanarak, sistemdeki dosyaları şifrelemek ve fidye talep etmek bu aşamada yapılabilecek işlemlerden birisidir.

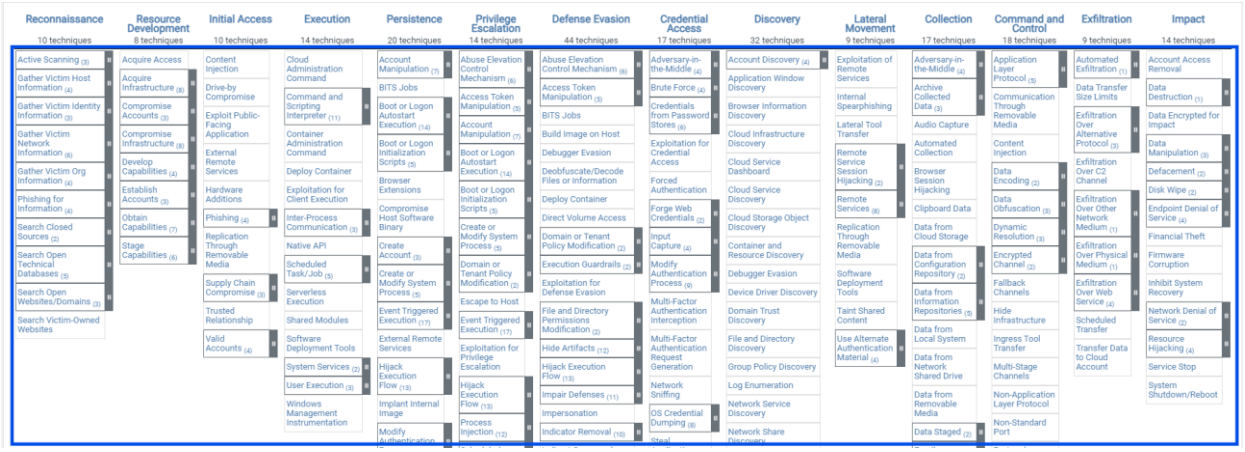
Teknikler

Teknik, bir saldırganın belirli bir hedefe ulaşmak için kullandığı yöntemdir. Yani saldırganın amacına ulaşmak için seçtiği yolları, araçları ve saldırı biçimlerini tanımlar. Her taktiğin altında, bu hedefe ulaşmak için kullanılan bir dizi teknik bulunur.



Örneğin bir saldırganın "ilk erişim" sağlamak için kullandığı yöntemler arasında kimlik

avı, uzaktan erişim araçları kullanma ya da tedarik zincirini hedef alma gibi teknikler yer alabilir.



Prosedürler

Prosedürler, bir tekniğin nasıl uygulandığına dair belirli örnekler sunar. Yani bir teknik kullanılarak gerçekleştirilen pratik eylemleri ve bu eylemleri uygulamak için kullanılan araçları içerir. Belirli bir saldırı grubunun veya tehdit aktörünün kullandığı yöntemlerin ayrıntılarını ve bu yöntemlerin tarihçesini gösterir.

Örneğin, bir grup belirli bir teknik için belirli yazılımlar veya araçlar kullanarak saldırıyı gerçekleştirmişse bu bilgiler prosedürler olarak adlandırılır.

MITRE ATT&CK Framework'de Bulunan Taktik ve Tekniklerin SOC Açısından Önemi

MITRE ATT&CK çerçevesindeki taktik ve teknikler, saldırganların hedeflerine ulaşmak için izlediği adımları anlamamızı sağlayarak güvenlik ekiplerine olayları daha iyi analiz etme imkanı sunar. Bu sayede bir saldırının hangi aşamada olduğu belirlenebilir ve buna uygun savunma stratejileri geliştirilebilir. Özellikle güvenlik duvarları, antivirüs yazılımları ve SIEM sistemleri, bu taktikleri baz alarak tehditleri daha hızlı algılayıp önlem alabilir.

Bununla birlikte güvenlik ekipleri saldırıları önceden öngörerek proaktif tedbirler geliştirebilir ve tehditlere karşı daha hazırlıklı hale gelebilir. Şirketler bu taktikleri ve teknikleri inceleyerek saldırıların farklı aşamalarına yönelik güvenlik politikaları oluşturabilir, sistemlerini daha dayanıklı hale getirebilir ve olay müdahale süreçlerini güçlendirebilir.

TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı)

TTP, saldırganların izlediği adımları tanımlayan bir çerçevedir. TTP-Based Threat Hunting ise saldırganların geçmişte nasıl hareket ettiğini analiz ederek ağda veya sistemde benzer izlerin olup olmadığını proaktif bir şekilde araştırma sürecidir.

Saldırganların izlediği yöntemleri anlamak, tehditleri daha saldırı gerçekleşmeden önce yakalamaya yardımcı olur. Bu yaklaşımda tehdit avcıları MITRE ATT&CK gibi çerçeveleri kullanarak saldırıların belirli aşamalarını inceler ve bir saldırının sistemde iz bırakıp bırakmadığını araştırır.

Örneğin bir saldırganın uzaktan yönetim araçları kullandığı biliniyorsa, güvenlik analistleri ağda veya uç noktalarda benzer bağlantıların izlerini arar. Böylece bilinen saldırı tekniklerine dayalı bir avlanma stratejisi oluşturulmuş olur.

Detection Engineering (Tespit Mühendisliği)

Siber güvenlik sistemlerinin saldırıları daha hızlı ve doğru bir şekilde tespit etmesini sağlamak için kullanılan tekniklerin tasarlanması ve uygulanması sürecidir. Detection Engineering, saldırganın kullandığı teknikleri ve taktikleri anlamak ve bu bilgiyi kullanarak güvenlik araçlarını geliştirmek ve optimize etmek anlamına gelir. Burada ki amaç gerçek zamanlı tehditleri tespit etmek, yanlış alarmları azaltmak ve güvenlik analistlerinin doğru ve zamanında yanıtlar vermelerini sağlayacak sistemler oluşturmaktır.

Detection Engineering genellikle bir güvenlik bilgi ve olay yönetim sistemi veya güvenlik analiz araçlarıyla ilişkilidir. Bu mühendislik dalında tehdit avcıları ve güvenlik analistleri, farklı saldırı tekniklerini ve TTP'lerini tanıyan, bu tekniklere duyarlı algılama kuralları ve algoritmalarını oluşturur.

2022 Ukraine Electric Power Attack C0034

Ukrayna Elektrik Gücü Saldırısı, önemli bir siber saldırı örneği olup enerji altyapısına yönelik ciddi tehditleri göstermektedir. Bu saldırı enerji sektöründeki sistemleri hedef alarak, kritik elektrik güç altyapısını etkisiz hale getirmeyi amaçlamıştır. Saldırganlar, çeşitli siber teknikleri kullanarak hedeflenen bölgedeki elektrik şebekelerini geçici olarak devre dışı bırakmışlardır.

Saldırının detayları incelendiğinde kullanılan tekniklerin MITRE ATT&CK Framework'ün çeşitli taktikleri ve teknikleriyle örtüştüğü görülmektedir. Bu tür bir saldırı, Initial Access, Remote Access, Credential Dumping ve Impact gibi bir dizi taktik ve teknik içeriyor. Bu taktiklerin ve tekniklerin her birinin, saldırganların sistemlere nasıl erişim sağladığını, kimlik bilgilerini nasıl ele geçirdiğini ve nihayetinde enerji altyapısını nasıl hedef aldığını anlamaya yardımcı olacak birçok detay barındırmaktadır.

Kullanılan Teknikler ve TID Değerleri

TID: T1059.001
Taktik: Execution (Yürütme)
Teknik: Powershell Kullanımı

2022 Ukrayna Elektrik Gücü Saldırısı sırasında Sandworm Ekibi, TANKTRAP adlı bir PowerShell yardımcı programı kullanarak Windows Grup İlkesi aracılığıyla bir silme aracı yaydı ve çalıştırdı. PowerShell, komut satırından güçlü bir kontrol sağlamayı mümkün kılarak, saldırganların sistem üzerinde daha fazla yetki elde etmelerini sağlar.

TID: T1543.002
Taktik: Persistence (Kalıcılık)
Teknik: Systemd Service

2022 Ukrayna Elektrik Gücü Saldırısı sırasında Sandworm Ekibi, GOGETTER'ı kalıcı hale getirebilmek için Systemd'yi yapılandırarak, sistem kullanıcı oturumları açıldığında GOGETTER'ın otomatik olarak çalışmasını sağladı. Systemd, Linux tabanlı sistemlerde servislerin yönetilmesini sağlayan bir araçtır ve bu yapılandırma kötü amaçlı yazılımın sürekli olarak çalışmasını mümkün kıldı.

TID: T1485
Taktik: Impact (Etkileşim)
Teknik: Data Destruction

Sandworm Ekibi, kurbanın BT ortamındaki dosyaları silmek için CaddyWiper'ı dağıtarak, Operasyonel Teknoloji (OT) sistemlerine zarar verdi. Bu süreçte eşlenen sürücüler ve fiziksel sürücü bölümleri de silindi.

TID: T1484.001
Taktik: Defense Evasion (Savunma Kaçma)
Teknik: Group Policy Modification

Sandworm Ekibi, kötü amaçlı yazılımları dağıtmak ve çalıştırmak için Grup İlkesi Nesnelerini (GPO) kullanarak savunma önlemlerini atlatmayı başardı. Grup İlkesi değiştirildi ve böylece kötü amaçlı yazılımların etkili bir şekilde yayılması sağlandı.

TID: T1570
Taktik: Lateral Movement (Yanal Hareket)
Teknik: Lateral Tool Transfer

Sandworm Ekibi, CaddyWiper'ın msserver.exe dosyasını dağıtmadan önce bir Grup İlkesi Nesnesi kullanarak, dosyayı hazırlama sunucusundan yerel sabit diske kopyalayarak ağda hareket etmeyi sağladı.

TID: T1036.004
Taktik: Defense Evasion (Savunma Kaçma)
Teknik: Masquerade Task or Service

Sandworm Ekibi, GOGETTER kötü amaçlı yazılımını meşru veya gerçek bir hizmet olarak maskelemek için Systemd hizmet birimlerini kullandı. Bu durum kötü amaçlı yazılımın tespit edilmesini zorlaştırdı.

TID: T1095
Taktik: Command and Control (Komut ve Kontrol)
Teknik: Non-Application Layer Protocol

Sandworm Ekibi, C2 iletişimlerini TLS tabanlı bir tünel aracılığıyla proxy'leyerek, saldırganların iletişimlerini gizli tutmalarına yardımcı oldu.

TID: T1572
Taktik: Command and Control (Komut ve Kontrol)
Teknik: Protocol Tunneling

Sandworm Ekibi, GOGETTER tünelleme yazılımını kullanarak dış sunucularla güvenli bir TLS tabanlı C2 kanalı oluşturdu. Bu tünelleme, saldırganların ağda gizlilik içinde hareket etmelerini sağladı.

TID: T1053.005
Taktik: Persistence (Kalıcılık)
Teknik: Scheduled Task

Sandworm Ekibi, CaddyWiper'ı belirli bir zamanda çalıştırmak için Grup İlkesi Nesnesi (GPO) aracılığıyla Zamanlanmış Görevlerden yararlandı. Bu yöntem, kötü amaçlı yazılımın sistemde kalıcı olmasını sağladı.

TID: T1505.003
Taktik: Impact (Etkileşim)
Teknik: Web Shell

Sandworm Ekibi, Neo-REGEORG web kabuğunu internet üzerinden erişilebilen bir sunucuya yerleştirerek uzaktan kontrol sağladı. Bu web kabuğu, saldırganların hedefi uzaktan denetlemelerine olanak tanıdı.

TID: T0895
Taktik: Initial Access (İlk Erişim)
Teknik: Autorun Image

Sandworm Ekibi, mevcut hipervizör erişimini kullanarak a.iso adlı bir ISO görüntüsünü sanal bir makineye eşledi. SCADA sunucusu, CD-ROM görüntülerini otomatik olarak çalıştıracak şekilde yapılandırılmıştı, bu da ISO içindeki kötü amaçlı VBS betiğinin otomatik olarak çalışmasına neden olmuştur.

TID: T0807
Taktik: Command and Control (Komut ve Kontrol)
Teknik: Command-Line Interface

Sandworm Ekibi, MicroSCADA platformunda komutları yürütmek için SCIL-API'yi kullanarak scilc.exe dosyasını çalıştırdı. Bu, saldırganların SCADA sistemlerine komut göndermelerini sağladı.

TID: T0853
Taktik: Impact (Etkileşim)
Teknik: Scripting

Sandworm Ekibi, MicroSCADA komutunu yürütmek için Visual Basic betiği lun.vbs'yi kullandı. Bu betik, n.bat dosyasını çalıştırarak SCADA platformuna komutlar göndermeyi sağladı.

TID: T0894
Taktik: Command and Control (Komut ve Kontrol)
Teknik: System Binary Proxy Execution

Sandworm Ekibi, MicroSCADA uygulama ikilisini kullanarak, C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt komutunu çalıştırarak SCADA sistemine yetkisiz komut mesajları gönderdi. Bu

işlem, uzaktaki trafo merkezlerine yetkisiz komutlar iletmelerini sağladı.

TID: T0855
Taktik: Impact (Etkileşim)
Teknik: Unauthorized Command Message

Sandworm Ekibi, MicroSCADA SCIL-API'yi kullanarak, trafo merkezlerine yetkisiz komutlar göndermeyi içeren bir dizi SCADA talimatı belirledi ve uyguladı.

Senaryo

Bir tehdit aktörü grubu, Lilith şirketini hedef almıştır. Lilith şirketi, finansal verilerini saklayan ve tıbbi bilgileri işleyen büyük bir sağlık hizmetleri sağlayıcısıdır. Şirketin altyapısında bazı zayıf noktalar ve güncellenmemiş yazılımlar bulunmaktadır. Tehdit aktörleri keşif aşamasına odaklanarak hedefin ağını dikkatlice izlemeye başlar.

1. Keşif (Reconnaissance) Aşaması

Tehdit aktörleri hedefin dış sistemlerini ve çalışanlarını keşfetmek için çeşitli yöntemler kullanır. Çalışanlardan biri şirketin dahili sistemlerine erişebileceği bir şifreyi içeren zayıf bir e-posta şifresiyle Phishing saldırısına uğrar. Bu aşama aktörlerin şirketin ağında ilerlemeye başlamaları için ilk fırsatı sağlar. Şifreyi ele geçiren aktör ağda ilerlemek için gerekli bilgiyi elde etmiş olur.

E-posta Temelli Phishing (T1071) = Tehdit aktörleri çalışanları hedef alarak sahte e-posta gönderir. Bu e-postalar, bir bağlantıyı tıklamaları için onları kandırır. Bağlantıda ki linkler, saldırganların hazırladığı zararlı yazılımı içerir. Çalışan, e-postadaki zararlı bağlantıya tıklayarak kötü amaçlı yazılımı indirir.

Sosyal Mühendislik ile Erişim Sağlama (T1086) = Çalışanlardan birinin sosyal mühendislik yoluyla ağ şifresi çalınır. Saldırganlar çalışanı manipüle ederek ağda yüksek yetkilere sahip şifreyi elde ederler. Bu, aktörlerin ağda ilerlemesini sağlayacak bir giriş noktası oluşturur.

2. Giriş (Initial Access) Aşaması

E-posta phishing saldırısıyla şirkete sızan tehdit aktörleri, kötü amaçlı yazılımı yükleyerek ağda daha fazla sistem üzerinde ilerleme sağlamayı hedefler. Çalışanın bilgisayarına yüklenen yazılım, şirketin merkezi sunucularına bağlanarak ağdaki verileri izlemeye başlar.

Phishing (T1566) = Çalışanlar, sahte bir e-posta yoluyla kötü amaçlı yazılımı bilgisayarlarına indirir. E-posta ile gelen link, zararlı yazılımı çalıştırmak için kullanılan bir dosyadır.

Sürükle ve Bırak (T1075) = Tehdit aktörü, kötü amaçlı yazılımı çalıştırmak için sahte bir dosya üzerinden çalışanı kandırır. Bu dosya görünüşte zararsızdır ancak içeriği çalıştırıldığında sistemin daha fazla kontrol edilmesini sağlar.

3. Yükseltilmiş Yetkiler (Privilege Escalation) Aşaması

Tehdit aktörleri ağda daha fazla yetki elde etmek için çeşitli teknikler kullanır. Bu aşamada aktörler sistem yöneticisi haklarını elde etmek için "Privilege Escalation" yöntemlerine başvurur. Çalışan ağdaki şifreleri sızdırarak yönetici seviyesindeki erişimi sağlar.

Çift Yönlü Saldırılar (T1070) = Tehdit aktörü yetkisini artırmak için ağda başka bir saldırı başlatır. Bu saldırı aktörün ağdaki erişimini ve kontrolünü pekiştirmeye yöneliktir.

Şifre Çalma (T1003) = Yönetici şifreleri ağdaki şifre yönetim yazılımından çalınır. Bu şifrelerin ele geçirilmesi aktörlere ağdaki en yüksek seviyedeki erişimi sağlar ve daha fazla sistemde yetki elde etmelerini mümkün kılar.

4. İç Ağda Hareket Etme (Lateral Movement) Aşaması

Tehdit aktörleri ağda daha fazla sistemde hareket etmeye başlar. Sistem yöneticisi şifresi ele geçirildikten sonra aktörler şirketin kritik sunucularına geçiş yapar. Bu süreçte ağ üzerinde daha fazla veri toplamayı hedeflerler.

Web Shell (T1100) = Tehdit aktörü bir web sunucusunda yerel bir zararlı yazılım kullanarak uzak bir sisteme bağlanır. Web shell, ağda hareket etmeyi ve kritik sistemlere sızmayı sağlar.

Remote Desktop Protocol (T1076) = Aktörler uzaktan masaüstü protokolü kullanarak ağdaki başka bir bilgisayara bağlanırlar. Bu protokol sayesinde ağda daha fazla sisteme erişim sağlanır ve tehdit aktörleri, şirketin iç ağında ilerlemeye devam eder.

5. Veri Çalma (Exfiltration) Aşaması

Tehdit aktörleri şirketin verilerini çalmaya başlar. Şirketin kullanıcı hesaplarının detayları ve tıbbi veriler hedeflenen veriler arasındadır. Aktörler verileri şifreli olarak dışarıya çıkarmak için birkaç farklı yol kullanır.

Veri Sıkıştırma (T1010) = Veriler şifrelenip sıkıştırılarak dışarıya gönderilir. Bu işlem verilerin gizliliğini korur ve aktörlerin veri sızdırma sırasında tespit edilme riskini azaltır.

HTTPS ile Veri Çıkartma (T1071) = Aktörler HTTPS bağlantısı üzerinden verileri şifreli bir şekilde dışarıya sızdırırlar. Bu yöntem verilerin güvenli bir şekilde dışarıya aktarılmasını sağlar ve ağ trafiğini şifreleyerek güvenlik açığına karşı korur.

Günün sonunda bir tehdit aktörü grubu görüldüğü üzere Lilith şirketini hedef almak için siber saldırı sürecine başlar. Şirketin dış ağını keşfeden aktörler, sosyal mühendislik teknikleri ile çalışanları hedef alır. Bir çalışan sahte bir e-posta ile kandırılır ve e-posta içindeki zararlı bağlantıya tıklayarak kötü amaçlı yazılımı bilgisayarına indirir. Bu aşama, tehdit aktörlerinin ilk adımını atmalarını sağlar. İndirilen yazılım aktörlerin şirketin ağında daha fazla sisteme erişmesini mümkün kılar. Artık şirketin ağında bir noktada bulunan aktörler ilerlemek için daha fazla yetki kazanma yoluna giderler. Ele geçirilen bilgisayar üzerinden şifreleri çalarak sistem yöneticisi seviyesinde erişim sağlarlar ve ağda daha derinlemesine ilerlemek için gerekli olan araçları edinirler.

Yüksek yetkilerle hareket etmeye başlayan aktörler, ağdaki diğer bilgisayarlara geçiş yaparak şirketin iç sistemlerinde yayılmaya başlarlar. Bu aşamada yerel bir web sunucusunda kötü amaçlı yazılım kullanarak başka makinelerde de kontrol sağlamayı başarırlar. Ayrıca uzaktan masaüstü protokolleri ile daha fazla sisteme erişim sağlamak için ağdaki başka bilgisayarlara bağlanırlar. Ağdaki yayılmaları ilerledikçe şirketin kritik sunucuları ve veritabanlarına da ulaşırlar. Şirketin veritabanlarında saklanan sağlık ve finansal bilgileri hedef alarak çalınması gereken verileri seçerler. Bu veriler şifreli bağlantılar üzerinden dışarıya aktarılır. Aktörler verileri sıkıştırarak ve şifreli bir şekilde dışarıya çıkartır, böylece tespit edilmeden veri çalma işlemini gerçekleştirirler.

Sonuç olarak tehdit aktörleri şirketin ağında derinlemesine bir sızma gerçekleştirmiş ve kritik verileri çalmayı başarmıştır. Bu süreçte şirketin güvenlik zafiyetleri ve zayıf farkındalık eğitimi nedeniyle saldırganlar siber saldırıyı uzun bir süre boyunca sürdürebilmiş ve büyük miktarda veri çalmıştır. Şirketin siber güvenlik ekibi saldırıyı fark ettiğinde çok geç kalınmış ve aktörler verileri dışarıya sızdırarak hedeflerine ulaşmışlardır. Bu saldırı yalnızca şirketin finansal ve operasyonel verilerine değil, aynı zamanda itibarına da ciddi zararlar vermiştir.

Sonuç

MITRE ATT&CK framework'ü ve bu framework'teki taktik ve tekniklerin siber güvenlikteki önemine odaklanıldı. MITRE ATT&CK, siber tehditlerin ve saldırı tekniklerinin sistematik bir şekilde sınıflandırılması ve modellenmesi açısından kritik bir araçtır. Bu tablo güvenlik ekiplerinin saldırıların nasıl gerçekleştiğini anlamalarına yardımcı olurken aynı zamanda tehdit avcılığı ve saldırı tespit mühendisliği için temel bir referans kaynağı olarak kullanılmaktadır.

Taktikler ve teknikler siber saldırılara karşı etkili savunmalar geliştirilebilmesi için büyük öneme sahiptir. TTP kavramı saldırganların davranışlarını anlamak ve tahmin etmek için oldukça değerli bir model sunar. Bu anlayış savunma stratejilerinin doğruluğunu artırırken, tehditleri daha hızlı tespit etme ve müdahale etme imkanı sağlar.

MITRE ATT&CK framework'ü, siber güvenlik alanında her seviyedeki profesyonelin kullanabileceği kapsamlı ve dinamik bir kaynaktır. Bu framework sadece savunma değil, aynı zamanda saldırganları anlamak ve onlara karşı önleyici stratejiler geliştirmek açısından da vazgeçilmezdir. Gelecekte bu çerçevede yapılan araştırmaların siber güvenlik alanındaki tehditlere daha etkin ve hızlı yanıt verilmesine olanak tanıyacağı aşikardır.

Kaynakça

https://attack.mitre.org/resources/faq/

https://cyberartspro.com/mitre-attack-framework-nedir/

https://www.fortinet.com/resources/cyberglossary/mitre-attck

https://www.dnssense.com/post/what-is-the-mitre-att-ck-framework

https://www.cybereason.com/blog/what-is-the-mitre-attck-framework

https://berqnet.com/blog/mitre-attck-framework

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

https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack