Mitre Att&ck Framework

Hazırlayan

Neslihan ASLAN

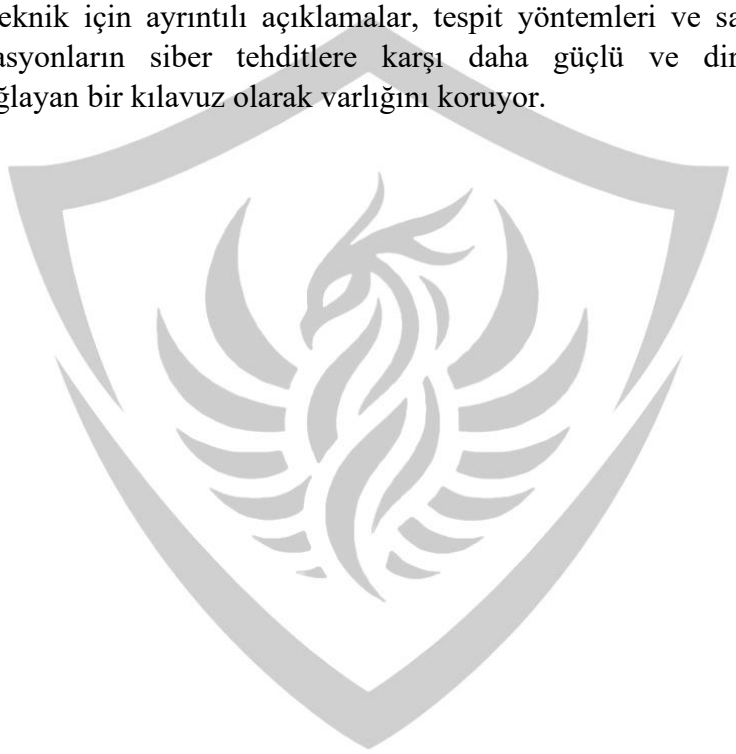
15/02/2025

İçindekiler

Giriş

Günümüz siber dünyasında, tehdit aktörleri sürekli olarak yeni saldırı yöntemleri geliştirmektedir. Bu noktada MITRE ATT&CK Framework, siber güvenlik alanında gelişmiş bir tehdit istihbarat kaynağıdır. Saldırganların siber saldırılarda kullandıkları yöntemleri, taktikleri ve teknikleri detaylı bir şekilde sınıflandırarak, bu saldırıların nasıl işlediğine dair kapsamlı kaynak sunar. Her bir saldırı aşaması, belirli bir amaca yönelik kullanılan taktikler ve teknikler ile açıklanır. Böylece saldırılar daha hızlı tespit edilebilir, etkili savunmalar oluşturulabilir ve olası tehditlere karşı daha hazırlıklı olunabilir.

Siber güvenlik dünyasında hızla gelişen tehditler ve saldırı teknikleri ile mücadele etmek için, MITRE ATT&CK, savunma ekiplerinin doğru bilgi ve araçlarla donatılmasını sağlar. Bu çerçeve, her bir teknik için ayrıntılı açıklamalar, tespit yöntemleri ve savunma stratejileri sunarak, organizasyonların siber tehditlere karşı daha güçlü ve dirençli savunmalar geliştirmelerini sağlayan bir kılavuz olarak varlığını koruyor.



Mitre Att&ck Tablosu ve Önemi

MITRE ATT&CK tablosu, siber saldırıların nasıl gerçekleştirildiğini anlamak ve analiz etmek için oluşturulmuş kapsamlı bir bilgi tabanıdır. Bu tablo, saldırganların kullandığı taktikler, teknikler ve prosedürler (TTP) hakkında detaylı bilgiler içerir ve saldırı sürecini adım adım ele alır.

MITRE ATT&CK, gerçek saldırılardan elde edilen gözlemlerle hazırlanmış bir çerçevedir ve güvenlik ekiplerince bir saldırganmış gibi düşünerek savunma stratejileri geliştirme konusunda güvenlik ekiplerine yardımcı olur. MITRE ATT&CK tablosu, saldırganların hedeflerine ulaşmak için kullandıkları sistemlere sızma, kalıcılık sağlama, hak yükseltme, savunmadan kaçınma, veri sızdırma gibi yöntemleri 14 temel taktik kategorisine ayrılmış ve her taktik altında, saldırganların kullandığı farklı teknikler ile detaylandırılmıştır.

MITRE ATT&CK' in en büyük avantajlarından biri güvenlik ekiplerine risk değerlendirme, tehdit tespiti ve saldırı önleme konularında nesnel ve yapılandırılmış bir yaklaşım sunmasıdır. SIEM, XDR, SOAR gibi güvenlik sistemleri bu bilgileri bütünleştirerek tehditleri daha etkin bir şekilde analiz edebilir. Böylece saldırılara tepki vermek dışında saldırıları önceden tahmin edip önleyici adımlar atılabilir.

Şekil 1

Diğer siber güvenlik çerçeveleriyle (örneğin, Cyber Kill Chain, NIST, ISO 27001) karşılaştırıldığında ise MITRE ATT&CK tablosu diğerlerine kıyasla saldırıları saldırgan perspektifinden ele alarak daha detaylı bir analiz imkânı sunmaktadır.

MITRE ATT&CK Matrisleri

MITRE ATT&CK, farklı sistemler için tehdit analiz edilebilmesi için dört temel matris sunmaktadır:

- **PRE-ATT&CK Matris**: Saldırı başlamadan önceki hazırlık ve keşif aşamalarını kapsar. Saldırganların hedef belirleme, istihbarat toplama, güvenlik açıklarını keşfetme, gerekli uygulamalara erişim ve saldırı altyapısını oluşturma süreçlerini kapsamaktadır.

- **Enterprise Matris:** Kurumsal ağlara yönelik tehditleri ve saldırı yöntemlerini içerir. Yaygın kullanılan bir araçtır. Windows, Linux, macOS, Azure AD, Google Workspace, Kubernetes gibi BT ortamlarındaki saldırıları kapsar.

- **Mobile Matris**: Android ve iOS mobil işletim sistemlerine yönelik mobil tehditleri ve saldırı tekniklerini içermektedir.

- **ICS Matris**: SCADA, PLC ve DCS gibi endüstriyel kontrol sistemlerine yönelik siber saldırıları inceler. Kritik altyapıların korunmasında yaygın kullanılmaktadır.

Mitre Atak Framework'de yer alan Taktik ve Tekniklerin Önemi

MITRE ATT&CK tablosu, saldırganların saldırılar sırasında izlediği taktikleri ve teknikleri ayrıntılı şekilde tanımlamaktadır. Daha etkili bir savunma sistemi için Mitre Attack tablosu, oldukça önemlidir.

- Taktikler, saldırganların seçtikleri hedefe ulaşmak için izledikleri genel stratejilerdir. Örneğin, İlk Erişim bir ağa sızmayı, Yanal Hareket sistemler arasında yayılmayı ve Veri Çıkışı hassas bilgilerin dışarı sızdırılmasını kapsıyor.

- Teknikler ise bu taktiklerin nasıl uygulandığını gösteren spesifik yöntemlerdir. Örneğin, Spear Phishing kimlik avı saldırılarıyla erişim elde etmeyi, Brute Force ile parola tahmin saldırılarını ya da Credential Dumping ile kullanıcı şifrelerini ele geçirmek gibi

Bu çerçeve ile saldırıları daha iyi anlamayı ve tehditlere karşı uygun savunma önlemleri geliştirmek mümkündür. MITRE ATT&CK' in ile gelen bu detaylı bilgilerle, güvenlik ekiplerinin tehditleri tespit etmesini, analiz etmesini ve etkili karşı önlemler almasını kolaylaşır.

TTP nedir?

TTP, Taktikler (Tactics), Teknikler (Techniques) ve Prosedürler (Procedures) kelimelerinin baş harflerinden oluşan bir kısaltmadır ve saldırganların saldırılarını nasıl gerçekleştirdiğini anlamak için kullanılan temel bir kavramdır. MITRE ATT&CK çerçevesi, bu TTP'leri sınıflandırarak güvenlik ekiplerinin tehditleri analiz etmesini ve etkili savunma mekanizmaları oluşturmasını kolaylaştırır**.**

Taktikler

MITRE ATT&CK çerçevesinde taktikler, saldırganların bir sistemi hedef alırken ulaşmak istedikleri amaçları ifade eder. Her siber saldırı belirli bir amaca hizmet eder ve bu amaç doğrultusunda farklı teknikler kullanılır. Taktikler, saldırganların izlediği stratejik hedeflerdir ve saldırının hangi aşamada olduğunu anlamamızı sağlar.

Örneğin, bir saldırganın amacı sisteme ilk erişimi sağlamak olabilir. Bu durumda kimlik avı (phishing) veya kötü amaçlı yazılım yerleştirme gibi teknikler kullanılabilir ya da saldırgan, ağ içinde yanal hareket ederek daha fazla cihaza erişmek isteyebilir ya da verileri dışarıya aktarmak için çeşitli yöntemleri deneyebilir.

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.

Şekil 2 Enterprise Matris

Teknikler

MITRE ATT&CK çerçevesindeki teknikler, bir saldırganın hedef taktiği uygulamak için kullandığı yöntemlerdir. Taktikler, saldırganın ulaşmayı hedeflediği amaçları temsil ederken, teknikler bu hedeflere ulaşmak için kullanılan spesifik eylemleri veya araçları tanımlar. Yani teknikler, "nasıl" bir saldırının gerçekleştiğini açıklar.

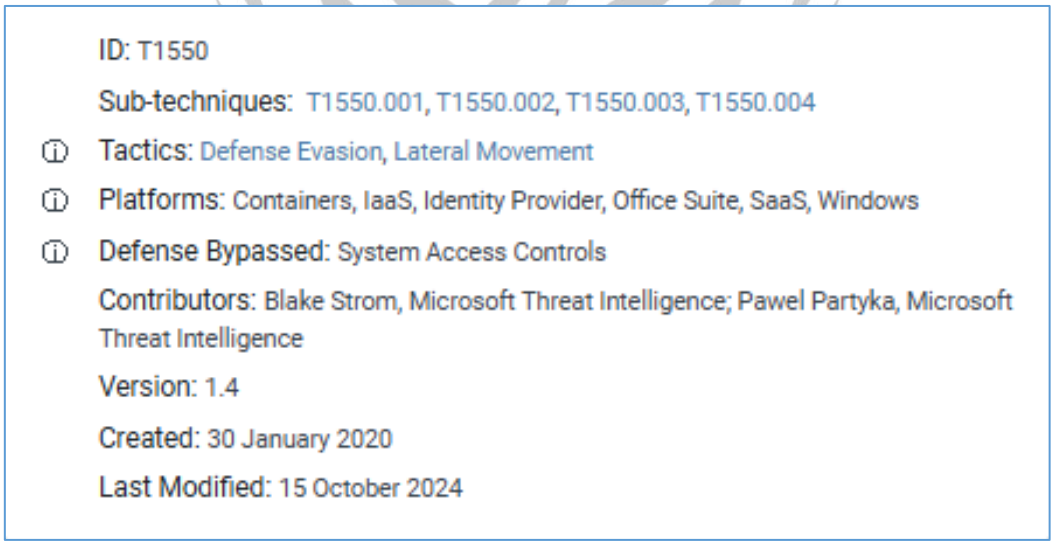
Her taktiğin birden fazla tekniği olabilir ve her teknik, saldırganların farklı yollarla aynı hedefe ulaşmalarını sağlar. Örneğin, keşif taktiği altında, saldırganlar hedef sistem hakkında bilgi toplamak için farklı teknikler (ağ taramaları yapmak, güvenlik açıklarını taramak veya IP blokları üzerinden aktif keşif gibi yöntemler) kullanabilir.

MITRE ATT&CK çerçevesi, her teknik için detaylı bir açıklama sunar ve bu tekniklerin nasıl uygulandığına dair örnekler sağlar. Ayrıca, her teknik için savunma ve algılama stratejileri de sunulmaktadır.

Teknikler, genellikle bir saldırının başlatılması için kullanılan araçlar, teknolojiler, kodlar, istismarlar veya yardımcı programlar gibi detaylı unsurları içermektedir. Örneğin, Pass-the-Hash tekniği, saldırganın NTLM kimlik doğrulama özetlerini kullanarak sistemlere yetkisiz erişim sağlamasını açıklarken, Living off the Land Binaries (LOLBins) tekniği, PowerShell veya CertUtil gibi sistem araçlarının kötü amaçlı işlemler için nasıl kullanılacağını ele alır.

Her tekniğin genellikle bir teknik kimlik numarasın (Txxxx) vardır. Bazı teknikler daha özel ve belirli alt yöntemler içerir. Alt yöntemler alt teknik olarak geçer. Alt teknikler, bir saldırganın genel bir tekniği nasıl uygulayacağını daha ayrıntılı bir şekilde belirtir. Alt teknikler, ATT&CK'ta "Txxxx.xxx" formatında tanımlanır.

Örneğin: alternatif kimlik doğrulama materyali tekniğinin kimlik numarası T1550 iken bu teknik altında olan Windows Komut Kabuğu alt tekniğinin kimlik numarası T1059.003 olarak görünmektedir.



Şekil 3

Her teknik, saldırganların farklı eylemlerle hedeflerine ulaşmalarını sağlayan stratejik adımlar olduğu için birden fazla taktik altında yer alabilir. Teknikler, saldırganların eylemlerini daha iyi anlamamıza ve bu eylemleri tespit etme konusunda savunmalar geliştirmemize yardımcı olur.

Özetle, taktikler bir saldırganın "ne yapmak istediğini", teknikler ise "bunu nasıl gerçekleştirdiğini" açıklamaktadır.

Prosedürler

MITRE ATT&CK çerçevesinde prosedürler, saldırganların belirli teknikleri nasıl uyguladıklarını ve nasıl eyleme geçtiklerini açıklayan ayrıntılı yöntemlerdir. Prosedürler, saldırganların, belirli bir saldırı tekniğini nasıl gerçeğe dönüştürdüğünü gösteren spesifik örneklerdir.

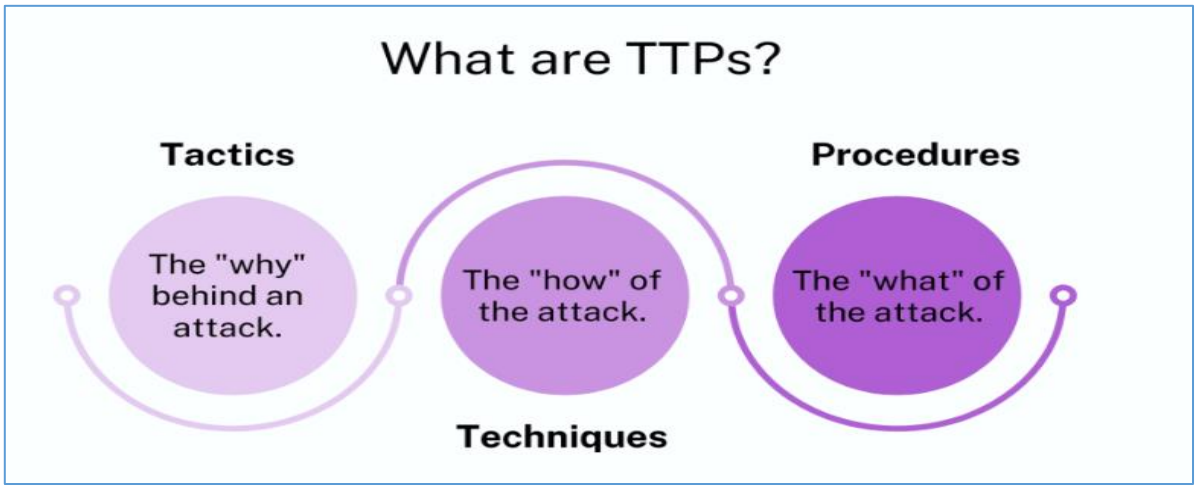
Bu prosedürler genelde tehdit istihbarat raporlarında ve gelişmiş sürekli tehdit (APT) gruplarının analizlerinde yer alır. Örneğin, APT29 (Cozy Bear) grubunun, kimlik avı yöntemi kullanarak kötü amaçlı ek içeren e-postalarla hedefin şifresini ele geçirmesi, bu teknik için bir prosedür örneğidir ya da Lazarus Group tarafından kullanılan Side-Channel saldırıları; bu grup, tedarik zinciri saldırıları aracılığıyla şirket içi ağlara sızmayı tercih etmiştir.

Prosedürler, geçmişteki saldırıları inceleyerek, benzer tehditleri tespit etme ve savunma stratejileri geliştirme konusunda yardımcı olur. Böylece, saldırganların teknikleri nasıl özelleştirip farklı şekillerde uyguladığını gözlemlenebilir. Bu durumu saldırıların hedeflerini ve kullanılan araçların daha doğru bir şekilde analiz edilmesi takip eder.

TTP-Based Threat Hunting ve Detection Engineering

TTP-Based Threat Hunting

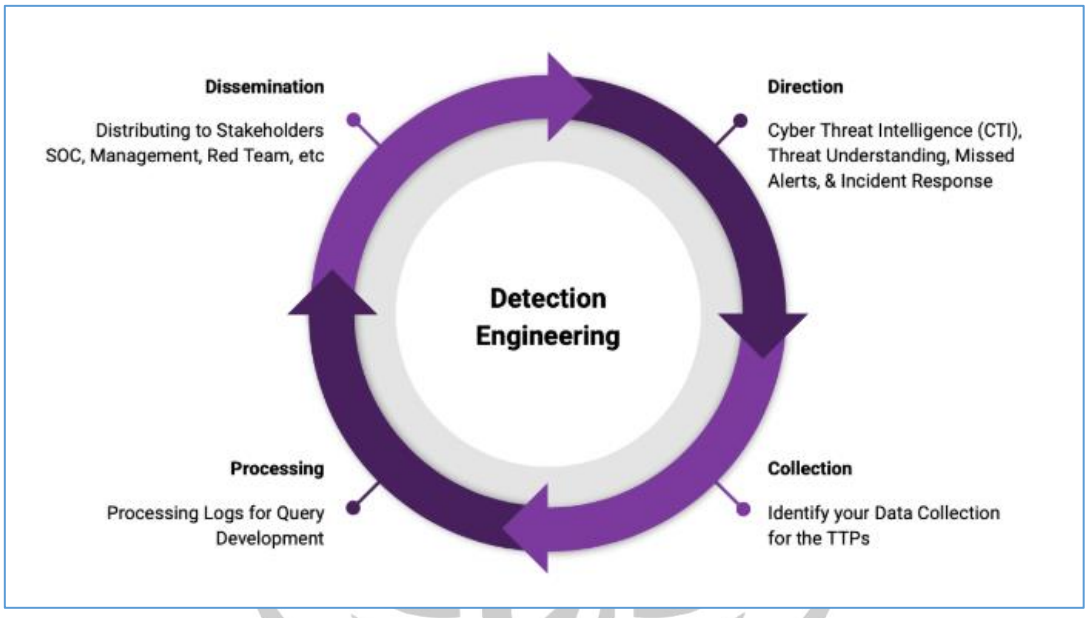
Saldırganların kullandığı belli davranışları, saldırı modellerini ve operasyonel teknikleri tespit etme sürecini kapsamaktadır. TTP-Based Threat Hunting, MITRE ATT&CK çerçevesinde tanımlanan taktik, teknik ve prosedürleri kullanarak, potansiyel saldırıları proaktif bir şekilde belirlemeyi amaçlar. TTP tabanlı tehdit avcılığı, geçmiş siber saldırıları analiz ederek saldırganların kullandığı yöntemleri anlamaya çalışır ve bu bilgilerle yeni saldırıları tahmin eder. Bu yaklaşım aslında saldırganların hangi teknikleri kullandığını anlamaya ve buna göre savunmalar geliştirmeye odaklanır. Böylece, daha sağlam ve stratejik bir tehdit avcılığı uygulanmış olur.



Şekil 4

Detection Engineering

Saldırıları tespit etmek için gerekli olan tespit kurallarını ve algılama mekanizmalarını geliştirir. Detection Engineer (Tespit Mühendisi), güvenlik alarmları üreten yapıları kurar ve gerektiğinde bu sistemleri günceller böylece kötü niyetli etkinliklerin tespit edilebilmesi için tespit sistemlerini tasarlamış olur. Ayrıca, tehdit istihbaratını ve elde ettiği bilgileri kullanarak savunma mekanizmalarını güçlendir. MITRE ATT&CK, tespit edilen olayların saldırı zincirinde nerede olduğunu anlamalarına yardımcı olur.



Şekil 5

2022 Ukraine Electric Power Attack C0034

2022 yılında Ukrayna'da gerçekleşen elektrik kesintisi saldırısı (Ukraine Electric Power Attack), siber saldırganların elektrik altyapısını hedef alarak büyük bir etki yaratan karmaşık bir saldırıydı. Bu saldırıda, özellikle enerji altyapısına yönelik hedefli teknikler kullanıldı. MITRE ATT&CK çerçevesinde, her bir saldırı tekniği belirli bir TID (Technique ID) değeriyle tanımlanır.

Techniques Used

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilized a PowerShell utility called TANKTRAP to spread and launch a wiper using Windows Group Policy.[1]
Enterprise	T1543	.002	Create or Modify System Process: Systemd Service	During the 2022 Ukraine Electric Power Attack, Sandworm Team configured Systemd to maintain persistence of GOGETTER, specifying the `WantedBy=multi-user.target` configuration to run GOGETTER when the system begins accepting user logins.[1]
Enterprise	T1485		Data Destruction	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed CaddyWiper on the victim's IT environment systems to wipe files related to the OT capabilities, along with mapped drives, and physical drive partitions.[1]
Enterprise	T1484	.001	Domain or Tenant Policy Modification: Group Policy Modification	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Group Policy Objects (GPOs) to deploy and execute malware.[1]
Enterprise	T1570		Lateral Tool Transfer	During the 2022 Ukraine Electric Power Attack, Sandworm Team used a Group Policy Object (GPO) to copy CaddyWiper's executable `msserver.exe` from a staging server to a local hard drive before deployment.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Systemd service units to masquerade GOGETTER malware as legitimate or seemingly legitimate services.[1]
Enterprise	T1095		Non-Application Layer Protocol	During the 2022 Ukraine Electric Power Attack, Sandworm Team proxied C2 communications within a TLS-based tunnel.[1]
Enterprise	T1572		Protocol Tunneling	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the GOGETTER tunneler software to establish a "Yamux" TLS-based C2 channel with an external server(s).[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Scheduled Tasks through a Group Policy Object (GPO) to execute CaddyWiper at a predetermined time.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the Neo-REGEORG webshell on an internet-facing server.[1]
ICS	T0895		Autorun Image	During the 2022 Ukraine Electric Power Attack, Sandworm Team used existing hypervisor access to map an ISO image named `a.iso` to a virtual machine running a SCADA server. The SCADA server's operating system was configured to autorun CD-ROM images, and as a result, a malicious VBS script on the ISO image was automatically executed.[1]
ICS	T0807		Command-Line Interface	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged the SCIL-API on the MicroSCADA platform to execute commands through the `scilc.exe` binary.[1]
ICS	T0853		Scripting	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilizes a Visual Basic script `lun.vbs` to execute `n.bat` which then executed the MicroSCADA `scilc.exe` command.[1]
ICS	T0894		System Binary Proxy Execution	During the 2022 Ukraine Electric Power Attack, Sandworm Team executed a MicroSCADA application binary `scilc.exe` to send a predefined list of SCADA instructions specified in a file defined by the adversary, `s1.txt`. The executed command `C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt` leverages the SCADA software to send unauthorized command messages to remote substations.[1]
ICS	T0855		Unauthorized Command Message	During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[1]

Şekil 6 C0034 Teknikleri

Kullanılan Enterprise Matris

- **T1059.001: PowerShell**

T1059 (Command and Scripting Interpreter) tekniğinin alt tekniğidir**.** T1059 tekniği, Saldırganlar, sistemde komut çalıştırmak için betik dilleri (PowerShell, Bash, Python vb.) veya komut satırı araçlarını kullanmasını ifade eder. Bu teknik, zararlı yazılımların yürütülmesi ve sistemlerin kontrol edilmesi için yaygın bir yöntemdir.

C0034 saldırısında kullanılan T1059.001 alt tekniği ise saldırganların Windows PowerShell'i kullanarak komutlar yürütebilmesini ifade eder. PowerShell, sistem yönetimi için güçlü bir araçtır ve saldırganlar tarafından kötüye kullanılabilir.

- **T1543.002: Systemd Service**

T1543 (Create or Modify System Process) tekniğinin alt tekniğidir. T1543 tekniği, saldırganların sistem süreçlerini oluşturarak veya değiştirerek kalıcılık sağlayabilmesidir. Bu teknik, kötü amaçlı servisler veya görevler oluşturarak bir saldırganın sistemde uzun süre aktif kalmasına yardımcı olabilir.

C0034 saldırısında kullanılan T1543.002 alt tekniği ise saldırganların tarafından Linux sistemlerinde kalıcılık sağlamak veya ayrıcalıklarını yükseltmek için systemd servislerini oluşturabilirmesi veya mevcut servisleri değiştirebilmeleridir.

- **T1485: Data Destruction**

Bu teknik ile, saldırganların hedef sistemdeki verileri silerek veya yok ederek zarar vermesini ifade eder. Bu tekniğin kullanıldığı saldırılarda, dosyaların üzerine yazılarak veya yerel ve uzak sürücülerdeki veriler aracılığıyla depolanan veriler geri alınamaz halde yok edilir.

- **T1484.001: Group Policy Modification**

T1484 (Domain or Tenant Policy Modification) tekniğinin alt tekniğidir. T1484 tekniği, Windows Active Directory ortamında, saldırganlar etki alanı politikalarını değiştirerek güvenlik kontrollerini devre dışı bırakabilir veya saldırının yayılmasını kolaylaştırabilir.

C0034 saldırısında kullanılan T1484.001 alt tekniği ise saldırganlar tarafından Active Directory ortamlarında Grup Politikalarını değiştirerek geniş çaplı yapılandırma değişiklikleri yapabilirler.

- **T1570: Lateral Tool Transfer**

Bu teknik, saldırganların bir araç veya dosyayı güvenliği ihlal edilmiş ortamdaki bir sistemden diğerine taşımasını ifade eder.

- **T1036.004: Masquerade Task or Service**

T1036 (Masquerading) tekniğinin alt tekniğidir. T1036 tekniği saldırganların kötü amaçlı işlemleri veya yazılımları meşru sistem bileşenleri gibi göstermesine dayanır. Örneğin, kötü amaçlı bir dosyanın adını yasal bir Windows süreci gibi değiştirmek.

C0034 saldırısında kullanılan T1036.004 alt tekniği ise saldırganların kötü amaçlı görev veya servisleri meşru görünen isimlerle gizleyerek tespit edilmekten kaçınabilirler.

- **T1095: Non-Application Layer Protocol**

Bu teknik, saldırganların komuta ve kontrol (Sunucular, ana bilgisayar ve C2 sunucusu veya bir ağ içindeki virüslü ana bilgisayarlar arasındaki iletişimi olabilir) iletişimi için uygulama katmanı dışındaki protokolleri kullanmasını ifade eder.

- **T1572: Protocol Tunneling**

Saldırganlar, bir protokolü başka bir protokol içinde tünelleyerek (algılama / ağ filtrelemesini önlemek ve / veya başka türlü erişilemeyen sistemlere erişimi sağlamak için) ağ güvenlik kontrollerini atlatabilirler.

- **T1053.005: Scheduled Task**

T1053 (Scheduled Task/Job) tekniğinin alt tekniğidir. T1053 tekniği, saldırganların belirli zamanlarda otomatik çalışacak kötü amaçlı görevler oluşturarak kalıcılığını arttırabilmeleridir. Windows'ta schtasks, Linux'ta cron kullanılarak bu işlem yapılabilir.

C0034 saldırısında kullanılan T1053.005 alt tekniği ise saldırganlar, Windows'ta zamanlanmış görevler oluşturarak belirli zamanlarda veya olaylarda kötü amaçlı kod çalıştırabilmeleridir.

- **T1505.003: Web Shell**

T1505 (Server Software Component) tekniğinin alt tekniğidir. T1505 tekniği, Saldırganların web sunucuları veya veritabanları gibi sunucu bileşenlerine kötü amaçlı kod yerleştirerek saldırılarını sürdürebilmesidir. Örneğin, web shell kullanımı bu teknik kapsamında değerlendirilir.

C0034 saldırısında kullanılan T1053.005 alt tekniği ise saldırganların web sunucularına kötü amaçlı betikler (web shell) yerleştirerek uzaktan komut yürütmesini sağlar.

Kullanılan ICS Matris

- **T0895: Autorun Image**

Kötü amaçlı kod yürütmek için AutoRun işlevlerinden veya komut dosyalarından yararlanılabilir. Saldırganların, çıkarılabilir medyaya (örneğin, USB bellek) otomatik çalıştırma özelliği ekleyerek kötü amaçlı yazılımın otomatik olarak çalıştırabilmeleridir.

- **T0807: Command-Line Interface**

Sistemlerle etkileşim kurmak ve komutları yürütmek için komut satırı arabirimleri (CLI) kullanarak endüstriyel kontrol sistemlerinin manipüle etmesini ifade eder. Bir işlem sırasında kurulabilecek kötü amaçlı araçlar da dahil olmak üzere yeni yazılım yüklemek ve çalıştırmak için CLI' ları kullanabilir.

- **T0853: Scripting**

Saldırganlar, önceden yazılmış bir komut dosyası biçiminde veya bir yorumlayıcıya kullanıcı tarafından sağlanan kod biçiminde rasgele kod yürütmek için komut dosyası dillerini kullanabilir.

- **T0894: System Binary Proxy Execution**

Bu teknik, kötü amaçlı içeriğin imzalanmış veya başka bir şekilde güvenilir ikili dosyalarla yürütülmesini proxy olarak işleyerek ve / veya imza tabanlı savunmaları atlayabilmelerini ifade eder.

- **T0855: Unauthorized Command Message**

Saldırganlar, kontrol sistemi varlıklarına amaçlanan işlevlerinin dışında veya beklenen işlevlerini tetiklemek için mantıksal önkoşullar olmadan işlem yapma talimatı vermek için yetkisiz komut mesajları gönderebilmesidir. Raporlama mesajlarını engelleyerek operatörlerin gerçek sistem durumunu görmesini de engelleyebilirler.

Senaryo: IoT Cihazlarını Kullanarak Şirket Ağına Sızma

Bir teknoloji şirketinin ofislerinde kullanılan akıllı kameralar, saldırganların hedefi haline gelir. Şirketin bir toplantı odasında bulunan IoT kamera cihazı, üretici tarafından varsayılan kullanıcı adı ve şifre ile bırakılmıştır. Saldırganlar, şirketin açık Wi-Fi ağını tarayarak bu cihazı tespit eder ve oturum açmayı başarır. Kameraya sızdıktan sonra, şirketin iç ağına yönlendirme yaparak diğer kritik sistemlere erişmeye çalışırlar. Root yetkilerini ele geçiren saldırganlar, IoT cihazlarının firmware'ini değiştirerek kalıcı bir arka kapı bırakır. Böylece, şirket ağında izlenmeden uzun süre kalabilirler. Son aşamada saldırganlar, IoT cihazları üzerinden önemli iş belgelerini ve sunuculardaki hassas verileri, şifrelenmiş bir kanal kullanarak kendi kontrol ettikleri bir sunucuya aktarırlar.

1. Keşif (Reconnaissance)

Saldırganlar, şirket ağında bulunan IoT cihazlarını tespit etmeye çalışır.

- **Network Sniffing- T1040**
  Şirketin açık Wi-Fi ağlarını ve IoT cihazlarını analiz ederler.

- **Search Open-Source Databases- T1592**
  Şirketin kullandığı ağ cihazlarının üreticileri ve zafiyetleri hakkında bilgi toplarlar.

2. İlk Erişim (Initial Access)

Şirketin IoT cihazlarını ele geçirerek iç ağa sızmaya çalışırlar.

- **Default Credentials- T1078.001**
  IoT cihazlarının değiştirilmemiş yönetici hesaplarını kullanarak giriş yaparlar.

- **Exploit Firmware Vulnerabilities- T1200**
  Güvenlik güncellemeleri yapılmamış eski IoT cihazlarındaki zafiyetlerden faydalanarak sisteme erişirler.

3. Yetki Yükseltme (Privilege Escalation)

Ağa girdikten sonra yetkilerini artırmaya çalışırlar.

- **Boot or Firmware Manipulation- T1542.002**
  IoT cihazlarının firmware'ini değiştirerek kalıcı bir arka kapı oluştururlar.

- **Container Breakout- T1611**
  IoT cihazlarındaki sandbox ortamlarından kaçarak root yetkileri elde ederler.

4. Savunma Kaçışı (Defense Evasion)

Tespit edilmemek için çeşitli teknikler kullanırlar.

- **Rootkit Deployment- T1014**
  IoT cihazlarına rootkit yükleyerek varlıklarını gizlerler.

- **Virtualization/Sandbox Evasion- T1497**
  IoT güvenlik sistemlerinden kaçınmak için özel komutlar kullanırlar.

5. Veri Sızdırma (Exfiltration)

Şirketin IoT cihazları üzerinden veri sızdırırlar.

- **Unsecured Protocol- T1071.001**
  IoT cihazlarını kontrol etmek için telnet veya FTP gibi güvenli olmayan protokolleri kullanırlar.

- **C2 Communication- T1105**
  Saldırganların yönettiği bir sunucuya IoT cihazlarından veri aktarımı yaparlar.

Sonuç

MITRE ATT&CK Framework, siber tehditlere karşı hazırlıklı olmayı sağlayan kapsamlı bir rehberdir. Saldırganların kullandığı teknikleri ve taktikleri daha iyi anlayarak, oluşumlar savunmalarını daha sağlam bir temele oturtabilirler. Bu çerçeve, sadece tespit ve savunma stratejilerini değil, aynı zamanda saldırıların önlenmesi ve etkilerinin en aza indirilmesi konusunda da rehberlik eder.

MITRE ATT&CK, tehdit aktörlerinin izlediği yolları sistematik bir şekilde ele alarak, güvenlik ekiplerinin saldırı zincirini anlamasını ve buna yönelik proaktif önlemler almasını sağlar. Siber güvenlik operasyon merkezleri (SOC), tehdit istihbarat ekipleri ve güvenlik analistleri, bu framework'ü kullanarak saldırıları daha erken aşamada tespit edebilir, olay müdahale süreçlerini hızlandırabilir ve güvenlik açıklarını daha etkili bir şekilde kapatabilirler.

Ayrıca, MITRE ATT&CK'in sürekli güncellenmesi ve iyileştirilmesi, tehdit aktörlerinin gelişen taktiklerini ve tekniklerini takip etmek açısından kritik bir noktadır. Yeni keşfedilen saldırı yöntemleri ve zafiyetler çerçeveye eklenerek, güvenlik stratejilerinin güncel tehditlere karşı dirençli olması sağlanır. Bu sayede, kuruluşlar hem mevcut güvenlik sistemlerini güçlendirebilir hem de gelecekte karşılaşabilecekleri saldırılara karşı daha hazırlıklı hale gelebilirler.

Kaynakça

1. **https://www.ibm.com/think/topics/mitre-attack**
2. **https://www.exclusive-networks.com/tr/wp-content/uploads/sites/32/2020/12/MITRE-ATTCK-InfoBlox-.pdf**
3. **https://en.wikipedia.org/wiki/ATT%26CK**
4. **https://berqnet.com/blog/mitre-attck-framework**
5. **https://www.splunk.com/en_us/blog/learn/mitre-attack.html**
6. **https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-matrix**
7. **https://www.techtarget.com/searchsecurity/definition/MITRE-ATTCK-framework**
8. **https://www.dnssense.com/post/what-is-the-mitre-att-ck-framework**
9. **https://docs.lumu.io/portal/en/kb/articles/attack-matrix**
10. **https://www.cybereason.com/blog/what-is-the-mitre-attck-framework**
11. **https://www.upguard.com/blog/what-is-ttp-hunting**
12. **https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf**
13. **https://letsdefend.io/blog/how-to-become-a-detection-engineer**
14. **https://socprime.com/blog/what-is-detection-engineering/**
15. **https://attack.mitre.org/campaigns/C0034/**
16. **https://www.balbix.com/insights/tactics-techniques-and-procedures-ttps-in-cyber-security/#:~:text=TTPs%20in%20cybersecurity%20describe%20how,understand%20and%20counteract%20potential%20threats.**