

MITRE ATT&CK FRAMEWORK



HAZIRLAYAN

AD: Ayşe

SOYAD: BALCI

TARİH: 17.02.2025

İçindekiler

GİRİŞ.....	3
MITRE ATT&CK Nedir?	4
MITRE ATT&CK Neden Önemlidir?	6
MITRE ATT&CK Taktik ve Tekniklerinin Önemi?	6
TTP Nedir?	7
TTP-Based Threat Hunting Nedir?.....	7
Detection Engineering Nedir?	8
2022 Ukrayna Elektrik Santral Saldırısı	9
Şirketin Hacklenmesi Senaryosu	14
Saldırının MITRE ATT&CK Tablosu.....	14
SONUÇ	15
KAYNAKÇA	16

GİRİŞ

Siber güvenlik dünyasında tehditleri anlamak ve etkili savunma stratejileri geliştirmek giderek daha önemli hale gelmiştir. MITRE ATT&CK, siber saldırganların kullandığı taktikleri, teknikleri ve prosedürleri (TTP'ler) sistematik bir şekilde belgeleyen kapsamlı bir bilgi tabanıdır. Bu çerçeve, güvenlik ekiplerine saldırıları tespit etme, analiz etme ve önleme konusunda rehberlik eder. Bu çalışmada, MITRE ATT&CK çerçevesinin temel bileşenleri, saldırganların yöntemleri ve güvenlik uzmanlarının bu çerçeveyi nasıl kullanabileceği ele alınacaktır.

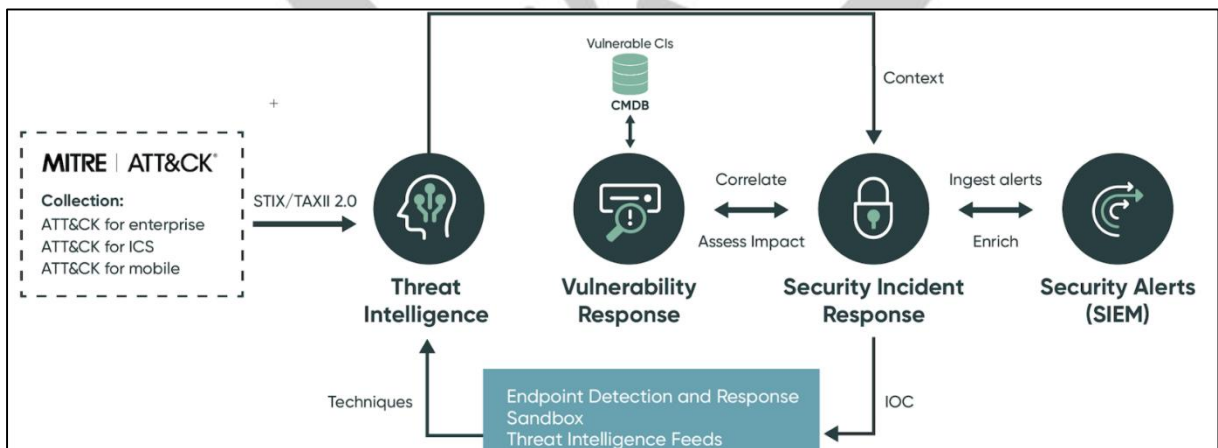


MITRE ATT&CK Nedir?

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber güvenlik alanında kullanılan bir bilgi tabanıdır. Bu bilgi tabanı, siber saldırganların kullandığı taktikleri, teknikleri ve prosedürleri (TTP'ler) sistematik bir şekilde belgelemektedir. MITRE ATT&CK, siber tehditleri anlamak, analiz etmek ve savunma stratejileri geliştirmek için önemli bir kaynak sağlar.

MITRE ATT&CK çerçevesinde, **Enterprise, Mobile ve ICS** terimleri farklı saldırı ve savunma bağlamlarında kullanılır. Her biri, hedef sistemlerin türüne göre farklı taktikler ve tekniklere odaklanır.

- **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 taktikleri**, genellikle kurumsal ağlar ve altyapılarla ilgilidir. Bu, daha geniş bir kullanıcı tabanına sahip, karmaşık sistemlerin güvenliği için taktikler içerir. Saldırganlar, bu tür ağlarda genellikle daha fazla erişim elde etmeye, veri sızdırmaya ve iç sistemleri ele geçirmeye yönelik teknikler kullanır.
- **Mobile taktikleri**, mobil cihazları hedef alan saldırı tekniklerini kapsar. Bu taktikler, akıllı telefonlar ve tabletler gibi taşınabilir cihazlara yönelik uygulama güvenliği, kimlik doğrulama, veri güvenliği ve cihaz yönetimi gibi alanlara odaklanır.
- **ICS taktikleri**, endüstriyel kontrol sistemlerini hedef alan teknikleri kapsar. Bu taktikler, SCADA ve PLC sistemleri gibi kritik altyapılara yönelik siber saldırılara odaklanır. ICS güvenliği, fiziksel dünyayı etkileyebilecek, kritik sistemleri hedef alan tehditleri ele alır.



Şekil 1

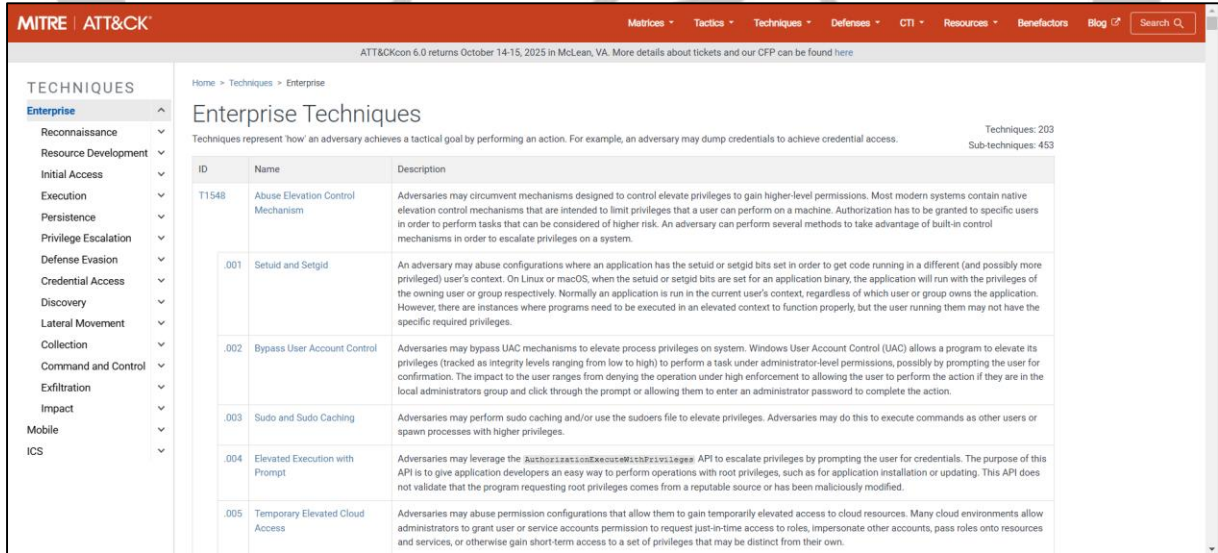
Enterprise altında 14 farklı taktik bulunur. Bunları açıklamak gerekirse:

- **Reconnaissance** (Keşif): Saldırganların hedef sistem veya ağı inceleyerek bilgi toplama sürecidir. Hedefin zayıflıkları ve güvenlik önlemleri hakkında bilgi edinmeyi amaçlar.
- **Resource Development** (Kaynak Geliştirme): Saldırganların saldırı için gerekli araçlar, yazılımlar veya altyapıyı toplama ve geliştirme sürecidir.
- **Initial Access** (Başlangıç Erişimi): Saldırganların hedef sisteme ilk erişimi sağlaması için kullandığı yöntemler. Örnekler: Phishing, Exploit Public-Facing Application.
- **Execution** (Çalıştırma): Kötü amaçlı yazılımların veya komutların hedef sistemde çalıştırılması. Örnekler: Scripting, Command-Line Interface, System Binary Proxy Execution.
- **Persistence** (Süreklilik): Saldırganların sistemde kalıcı erişim sağlamaları. Örnekler: Web Shell, Registry Run Keys/Startup Folder.
- **Privilege Escalation** (Yetki Yükseltme): Saldırganların daha yüksek sistem izinleri elde etmeleri. Örnekler: Exploitation for Privilege Escalation, Abuse Elevation Control Mechanism.
- **Defense Evasion** (Savunma Kaçışı): Saldırganların güvenlik önlemlerinden kaçmalarını sağlamak için kullandıkları yöntemler. Örnekler: Obfuscated Files or Information, Rootkit.
- **Credential Access** (Kimlik Bilgileri Erişimi): Saldırganların kimlik bilgilerine erişim sağlamaları. Örnekler: Brute Force, Credential Dumping.
- **Discovery** (Keşif): Saldırganların hedef sistemi ve ağı keşfetme yöntemleri. Örnekler: Network Service Scanning, File and Directory Discovery.
- **Lateral Movement** (Yanal Hareket): Saldırganların bir sistemden diğerine geçiş yaparak ağda ilerlemeleri. Örnekler: Remote File Copy, Pass the Hash.
- **Collection** (Toplama): Saldırganların hedef sistemden bilgi toplaması. Örnekler: Data Staged, Clipboard Data.
- **Exfiltration** (Veri Çıkartma): Toplanan bilgilerin hedef dışına çıkartılması. Örnekler: Exfiltration Over C2 Channel, Exfiltration Over Web Service.
- **Impact** (Etkileme): Saldırganların hedef sisteme zarar vermek veya sistemi bozmak amacıyla yaptıkları işlemler. Örnekler: Data Destruction, Service Stop.
- **Command and Control** (Komut ve Kontrol): Saldırganların hedef sisteme komut göndermeleri ve kontrol sağlamaları. Örnekler: Protocol Tunneling, Remote Access Software.

TTP Nedir?

MITRE ATT&CK çerçevesinde taktik, teknik ve prosedür kavramları saldırganların izlediği yöntemleri anlamamıza yardımcı olur:

- **Taktik:** Saldırganın ulaşmak istediği genel amaçtır. Örneğin, "Başlangıç (Initial Access)", "Yetki Yükseltme (Privilege Escalation)" veya "Savunmadan Kaçış (Defense Evasion)" gibi taktikler vardır.
- **Teknik:** Belirli bir taktiği gerçekleştirmek için kullanılan yöntemdir. Örneğin, "Kimlik Avı (Phishing)", "Hizmet Kötüye Kullanımı (Service Exploitation)" veya "Yetki Ayrıcalıklarının Kötüye Kullanma (Abuse Elevation Control Mechanism)" gibi teknikler bulunur.
- **Prosedürler:** Belirli bir teknik altında, saldırganların bu teknikleri nasıl uyguladıklarına dair daha ayrıntılı bilgi sağlar. Prosedürler, belirli bir saldırgan grubunun veya kampanyasının kullandığı özel yöntemleri ve araçları içerebilir.



ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.
.002	Bypass User Account Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.
.003	Sudo and Sudo Caching	Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.
.004	Elevated Execution with Prompt	Adversaries may leverage the <code>AuthorizationContextElevationPrivileges</code> API to escalate privileges by prompting the user for credentials. The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.
.005	Temporary Elevated Cloud Access	Adversaries may abuse permission configurations that allow them to gain temporarily elevated access to cloud resources. Many cloud environments allow administrators to grant user or service accounts permission to request just-in-time access to roles, impersonate other accounts, pass roles onto resources and services, or otherwise gain short-term access to a set of privileges that may be distinct from their own.

Şekil 3 Mitre Taktik Teknikler

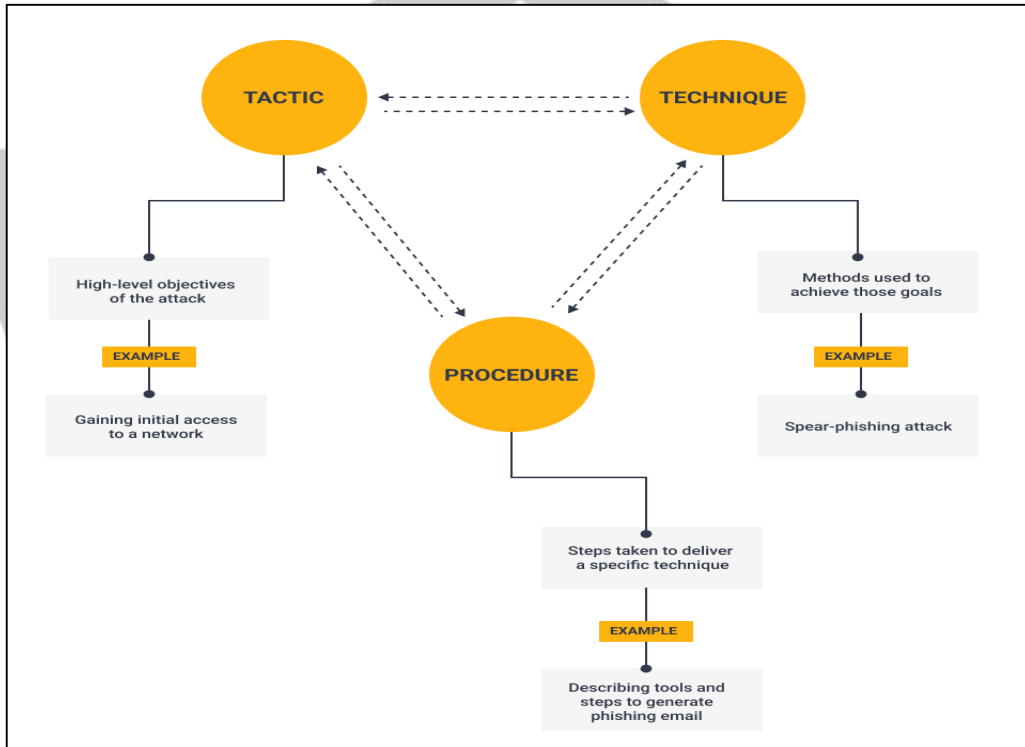
TTP-Based Threat Hunting Nedir?

TTP (Tactics, Techniques, Procedures), siber saldırganların hedeflerine ulaşmak için kullandıkları yöntemler, taktikler ve prosedürleri ifade eder. Bu üç bileşen, MITRE ATT&CK gibi tehdit çerçevelerinde detaylı olarak tanımlanmıştır. **TTP tabanlı tehdit avcılığı (TTP-Based Threat Hunting)**, saldırganların sistemlere nasıl sızmaya çalıştığını proaktif bir yaklaşımla öngörmeyi amaçlar. Bu yöntem yalnızca belirli saldırıları izlemekle kalmaz, aynı zamanda potansiyel tehditleri tahmin etmek ve engellemek için stratejik bir çerçeve sunar.

TTP tabanlı tehdit avcılığı, **aktif bir savunma modeli** olarak saldırganların bilinen tekniklerle ağ içinde ilerlemesini erken tespit etmeye çalışır. Bu yaklaşım, sistemdeki

tehditleri pasif bir şekilde beklemek yerine, sürekli izleme ve analiz yoluyla anormal hareketleri belirleyerek saldırıları engellemeye odaklanır. Böylece güvenlik ekipleri, tehditlere daha hızlı tepki verebilir ve organizasyonlarını saldırılara karşı daha dirençli hale getirebilir.

Bu yöntemde, geçmiş saldırılardan elde edilen tehdit istihbaratı ve bilinen TTP'ler kullanılarak saldırgan davranışları haritalandırılır. Özellikle **Uzlaşma Göstergeleri (Indicators of Compromise - IoC)**, tehditleri belirlemek için kritik rol oynar. IoC'ler, bir saldırının gerçekleştiğini veya gerçekleşme ihtimalini gösteren anormal aktiviteleri ve kanıtları içerir. Siber güvenlik ekipleri, bu göstergeleri analiz ederek saldırganların izlerini takip eder ve sistem zarar görmeden önce gerekli önlemleri alır.



Şekil 4 TTP based hunting

Detection Engineering Nedir?

Detection Engineering, güvenlik tehditlerini etkin bir şekilde tespit etmek için kullanılan bir mühendislik alanıdır. Bu süreç, saldırganların izlerini (TTP'ler) belirleyerek SIEM gibi güvenlik çözümlerini doğru şekilde yapılandırmayı amaçlar. Sürekli olarak yeni tehditleri analiz ederek tespit sistemlerini güncellemek, bu alanın temel bileşenlerinden biridir.

Detection Engineering, MITRE ATT&CK çerçevesiyle yakından ilişkilidir ve saldırganların sistemlere nasıl girebileceği konusunda kapsamlı bir rehber sunar. Güvenlik mühendisleri, belirli saldırı tekniklerine odaklanarak, log analizi ve alarm kuralları oluşturur. Örneğin, bir

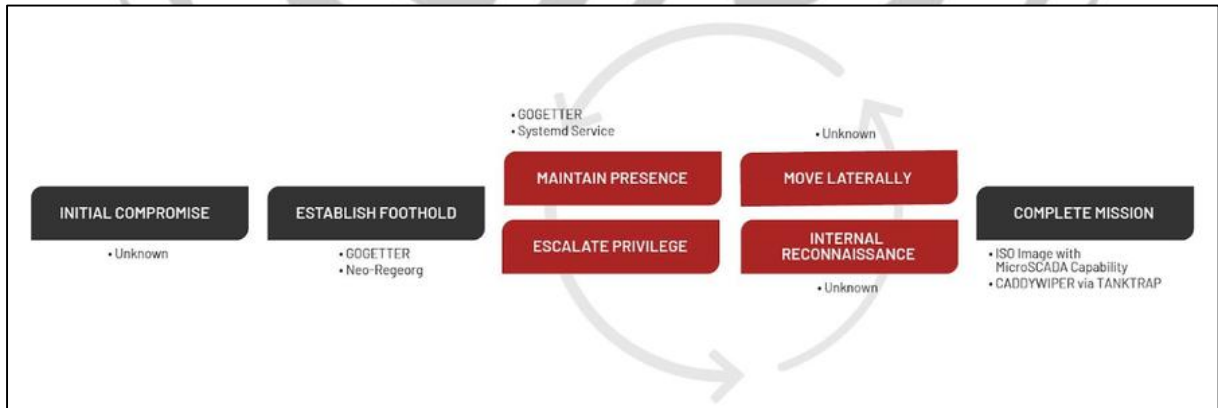
saldırganın "hizmetleri devre dışı bırakma" tekniğini kullanıp kullanmadığını tespit etmek için uygun log kayıtları izlenebilir.

Bu süreç, doğru veri toplama yöntemleriyle anlamlı uyarılar üretmeyi, false positive'leri azaltmayı ve tespit sisteminin sürekli gelişimini sağlamayı hedefler. Proaktif bir savunma yaklaşımı olarak, güvenlik analistlerinin tehditleri daha hızlı ve etkili bir şekilde belirlemesine yardımcı olur.

2022 Ukrayna Elektrik Santral Saldırısı

2022 Ukrayna Elektrik Enerjisi Saldırısı, Sandworm Grubu tarafından gerçekleştirilen bir siber saldırı operasyonudur. Bu saldırıda, GOGETTER, Neo-REGEORG, CaddyWiper ve Living off the Land (LotL) gibi teknikler kullanılarak, Ukrayna'daki bir elektrik şirketinin SCADA sistemlerine yetkisiz erişim sağlanmıştır. Saldırı, MITRE ATT&CK çerçevesinin hem Kurumsal (Enterprise) hem de Endüstriyel Kontrol Sistemleri (ICS) alanlarındaki çeşitli teknikleri kapsamaktadır.

SCADA (Supervisory Control and Data Acquisition – Merkezi Denetim ve Veri Toplama Sistemi), endüstriyel tesislerin, altyapıların ve kritik sistemlerin izlenmesi ve kontrol edilmesi amacıyla kullanılan bir otomasyon platformudur. SCADA, enerji şebekeleri, su temin ve arıtma sistemleri, petrol ve doğalgaz işleme tesisleri, üretim süreçleri ve ulaşım altyapıları gibi önemli sektörlerde yaygın olarak kullanılır. Bu sistemler, uzaktan denetim ve yönetim sağlayarak operasyonel verimliliği artırır ve güvenliği sağlar.



Şekil 5 Ukrayna Saldırısı

Kullanılan Teknikler:

- **T1059.001(Command and Scripting Interpreter: PowerShell):** T1059, MITRE ATT&CK çerçevesinde "Execution" taktiği altında yer alır ve saldırırganların PowerShell, Windows Command Shell, Unix Shell, Visual Basic, Python ve JavaScript gibi yorumlayıcıları kötüye kullanarak hedef sistemde komut çalıştırmasını kapsar.

Sandworm Ekibi, bir wiperi yaymak ve başlatmak için Windows Grup İlkesi'ni kullanarak TANKTRAP adlı bir PowerShell aracını kullandı. Powershell yardımıyla hedef sistemde komut çalıştırdı.

- **T1543.002(Create or Modify System Process:Systemd Service):** T1543.002, MITRE ATT&CK çerçevesinde "Persistence" taktiği altında yer alır ve saldırganların **Systemd Service** oluşturarak veya değiştirerek hedef sistemde kalıcılık sağlamasını kapsar. Bu teknik, Linux sistemlerinde Systemd yapılandırmalarını kötüye kullanarak kötü amaçlı yazılımların veya komutların sistem başlangıcında veya belirli olaylarda otomatik olarak çalıştırılabilmesini sağlar.

Sandworm Ekibi, GOGETTER'in kalıcılığını sağlamak için Systemd'yi yapılandırdı ve GOGETTER'in sistem kullanıcı girişlerini kabul etmeye başladığında çalışması için WantedBy=multi-user.target ayarını belirtti.

- **T1485 (Data Destruction):** T1485, MITRE ATT&CK çerçevesinde "Impact" taktiği altında yer alır ve saldırganların Data Destruction (Veri İmhası) yaparak hedef sistemdeki verileri kalıcı olarak silmesini kapsar. Bu teknik, dosyaları, disk bölümlerini veya tüm depolama aygıtlarını yok ederek sistemlerin çalışmasını bozmayı ve veri kaybına neden olmayı amaçlar.

Sandworm Ekibi, kurbanın BT ortamındaki sistemlere CaddyWiper'ı dağıtarak OT yetenekleriyle ilgili dosyaları, haritalanmış sürücülerini ve fiziksel disk bölümlerini sildi.

- **T1484.001(Domain or Tenant Policy Modification: Group Policy Modification):** T1484.001, MITRE ATT&CK çerçevesinde "**Impact**" (Etkileşim) taktiği altında yer alır. Bu teknik, **Data Destruction** (Veri İmhası) alt kategorisindedir ve saldırganların hedef sistemdeki verileri kalıcı olarak silmelerini amaçlar. Bu, dosyaların, disk bölümlerinin veya tüm depolama aygıtlarının yok edilmesi yoluyla sistemin işlevselliğini bozarak veri kaybına yol açar.

Sandworm Takımı, Group Policy Objects (GPO'lar) kullanarak kötü amaçlı yazılım dağıttı ve çalıştırdı.

- **T1570 (Lateral Tool Transfer): T1570 - Network Denial of Service (Ağ Hizmeti Engelleme),** MITRE ATT&CK çerçevesinde "**Impact**" taktiği altında yer alır. Bu teknik, saldırganların hedef ağın veya sistemin erişilebilirliğini engellemeyi amaçlar. Ağ trafiğini aşırı yükleyerek veya sistem kaynaklarını tükenmesine yol açarak hedef ağın çalışmasını durdururlar. Sonuç olarak, ağ hizmetleri devre dışı kalır ve hedef sistemin işleyişi bozulur.

Sandworm Takımı, bir Group Policy Object (GPO) kullanarak CaddyWiper'ın çalıştırılabilir dosyası msserver.exe'yi bir geçici sunucudan yerel bir sabit diske kopyalayarak dağıtım öncesinde hazırlık yaptı.

- **T1036.004(Masquerading: Masquerade Task or Service): Trusted Developer Utilities,** MITRE ATT&CK çerçevesinde "**Defense Evasion**" taktiği altında yer alır. Saldırganlar, kötü amaçlı yazılımlarını tanınmış ve güvenilir geliştirici araçlarının dosya adlarını taklit ederek gizlerler. Bu, güvenlik yazılımlarının veya kullanıcıların kötü amaçlı dosyaları tespit etmelerini zorlaştırır.

Sandworm Takımı, GOGETTER kötü amaçlı yazılımını meşru veya meşru gibi görünen hizmetler olarak gizlemek için Systemd hizmet birimlerini kullandı.

- **T1095(Non-Application Layer Protocol):** MITRE ATT&CK çerçevesinde "**Command and Control**" taktiği altında yer alır. Bu teknik, saldırganların uygulama katmanı dışındaki protokoller (örneğin, ICMP, DNS, veya raw TCP/UDP gibi) kullanarak komut ve kontrol (C2) iletişimi kurmalarını ifade eder. Bu, genellikle güvenlik çözümlerinden kaçmak ve tespit edilmeden iletişim kurmak amacıyla yapılır.

Sandworm Takımı C2 iletişimlerini TLS tabanlı bir tünel içinde proxy üzerinden iletti.

- **T1572 (Protocol Tunneling): T1572 - Protocol Tunneling,** saldırganların bir protokolü başka bir protokolün içine gizleyerek tespit edilmeden komut ve kontrol (C2) iletişimi sağlamasını ifade eder. Bu, güvenlik önlemlerinden kaçmak için kullanılır.

Sandworm Takımı, dış bir sunucu(lar) ile "Yamux" TLS tabanlı C2 kanalı oluşturmak için GOGETTER tünel yazılımını dağıttı.

- **T1053.005(Scheduled Task/Job: Scheduled Task):** MITRE ATT&CK çerçevesinde "**Persistence**" taktiği altında yer alır. Saldırganlar, WMI kullanarak zamanlanmış görevler oluşturup kötü amaçlı yazılımlarını sürekli çalıştırarak güvenlik yazılımlarından kaçmak ve erişim sağlamak için bu tekniği kullanır.

Sandworm Takımı, CaddyWiper'ı önceden belirlenmiş bir saatte çalıştırmak için Group Policy Object (GPO) aracılığıyla Zamanlanmış Görevleri kullandı.

- **T1505.003(Server Software Component: Web Shell):** MITRE ATT&CK çerçevesinde "**Persistence**" taktiği altında yer alır. Saldırganlar, web shell yükleyerek hedef sunucuyu uzaktan kontrol eder ve sürekli erişim sağlar.

Sandworm Takımı, internet erişimi olan bir sunucuda Neo-REGEORG web shell'ini dağıttı.

- **T0895(Autorun Image): T0895 - Autorun Image,** MITRE ATT&CK çerçevesinde "**Execution**" (Çalıştırma) taktiği altında yer alır. Saldırganların kötü amaçlı yazılımları, otomatik olarak çalışacak şekilde yapılandırılmış bir CD-ROM veya medya aygıtı üzerinden çalıştırmalarını sağlar. Bu, hedef sistemin zayıflıklarından yararlanarak kötü amaçlı dosyaların otomatik olarak çalıştırılmasına neden olur.

Sandworm Takımı, mevcut hypervisor erişimini kullanarak a.iso adlı bir ISO görüntüsünü, bir SCADA sunucusu çalıştıran sanal makineye bağladı. SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik olarak çalışacak şekilde yapılandırılmıştı ve bu nedenle ISO görüntüsündeki kötü amaçlı bir VBS betiği otomatik olarak çalıştırıldı.

- **T0807(Command-Line Interface):** MITRE ATT&CK çerçevesinde "**Execution**" (Çalıştırma) taktiği altında yer alır. Bu teknik, saldırganların komut satırı arayüzü (CLI) kullanarak hedef sistemde komutlar çalıştırarak kötü amaçlı yazılımlarını yürütmelerini sağlar. CLI, saldırganlara doğrudan komutlar girme ve sistemde işlem yapma imkanı sunar.

Sandworm Takımı, scilc.exe ikili dosyasını kullanarak komutları çalıştırmak için MicroSCADA platformundaki SCIL-API'yi kullandı.

- **T0853(Scripting):** MITRE ATT&CK çerçevesinde "**Execution**" taktiği altında yer alır. Saldırganlar, kötü amaçlı yazılımlarını veya komutlarını çalıştırmak için betikler (PowerShell, VBScript, Python vb.) kullanarak hedef sistemde komut çalıştırır.

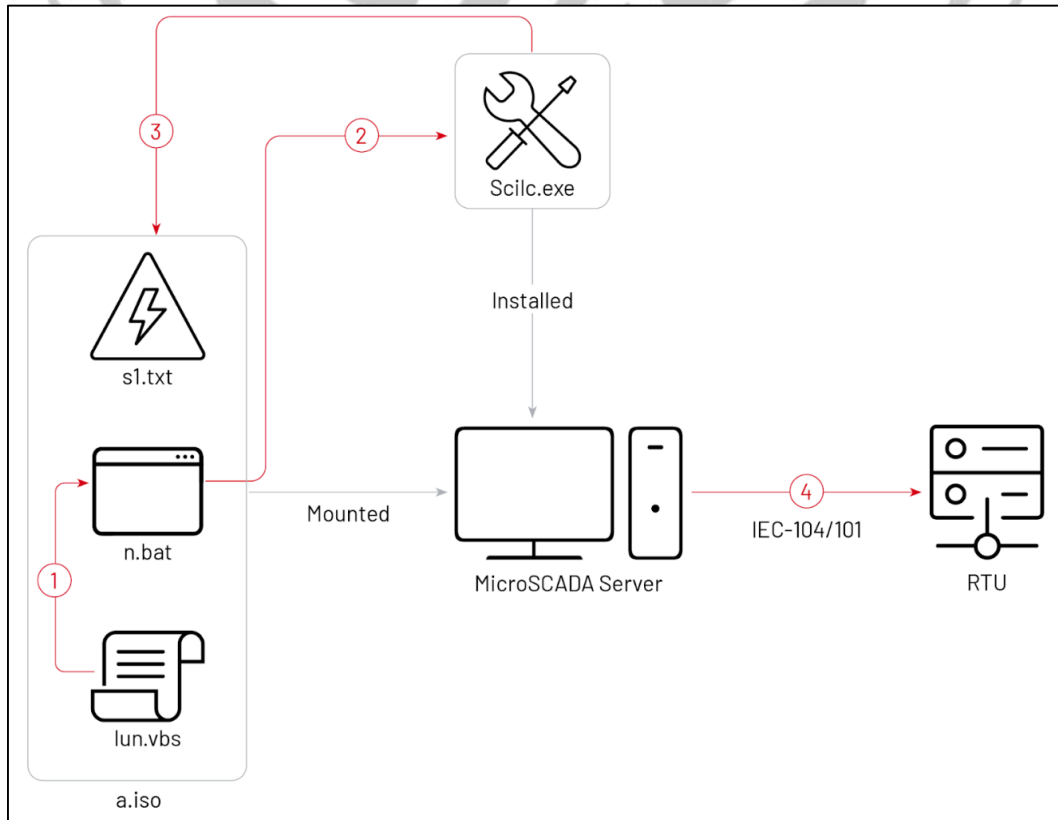
Sandworm Takımı, n.bat dosyasını çalıştırmak için lun.vbs adlı bir Visual Basic betiği kullandı ve ardından MicroSCADA scilc.exe komutunu çalıştırdı.

- **T0894(System Binary Proxy Execution):** MITRE ATT&CK çerçevesinde "**Execution**" taktiği altında yer alır. Saldırganlar, kötü amaçlı yazılımlarını meşru bir sistem dosyasını proxy olarak kullanarak çalıştırır ve güvenlik yazılımlarından kaçabilir.

Sandworm Takımı, bir dosyada belirtilen önceden tanımlanmış SCADA talimatları listesini göndermek için scilc.exe adlı bir MicroSCADA uygulama ikili dosyasını çalıştırdı. Çalıştırılan komut C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt, SCADA yazılımını kullanarak uzak trafolarla yetkisiz komut mesajları gönderdi.

- **T0855(Unauthorized Command Message): T0855 - Unauthorized Command Message,** MITRE ATT&CK çerçevesinde "**Impact**" taktiği altında yer alır. Saldırganlar, hedef sisteme yetkisiz komutlar göndererek işlemleri manipüle eder ve uzak sistemlerdeki servisleri kontrol eder.

Sandworm Takımı, SCADA talimatları seti belirlemek ve trafoların cihazlarına yetkisiz komutlar göndermek için MicroSCADA SCIL-API'yi kullandı.



Şekil 6 Ukrayna Saldırısı Diyagramı

Şirketin Hacklenmesi Senaryosu

Savunma sanayiinde kritik projeler yürüten bir teknoloji şirketine APT grubu tarafından saldırı yapılacaktır. Grup bu şirketin AR-GE çalışmalarını ve askeri sözleşmelerini çalarak rakip bir devlete stratejik avantaj sağlamak amacıyla kapsamlı bir operasyon planlıyor.

Keşif (Reconnaissance)

T1595 - Active Scanning

Şirketin çevrimiçi platformlarına yönelik aktif tarama gerçekleştirilir. Şirketin kullandığı yazılımlar ve güvenlik açıkları hakkında bilgi toplanır.

T1589 - Gather Victim Identity Information

Şirketin sosyal medya hesapları, çevrimiçi forumlar ve sızıntı veritabanları üzerinden çalışan kimlik bilgileri toplanır.

Erişim Kazanma (Initial Access)

T1071.001 - Application Layer Protocol: Web Protocols

Şirketin çalışanlarının sıklıkla kullandığı bir web uygulaması bulunur ve uygulamadaki güvenlik açığı kullanılarak sisteme giriş sağlanır.

T1074.002 - Data Staged: Cloud Storage

Hassas belgeler, şirketin bulut altyapısına aktarılır ve şifrelenir. Veriler dışarıya sızdırılmadan önce burada güvenli bir şekilde saklanır.

Savunmadan Kaçınma (Defense Evasion)

T1564.003 - Impair Defenses: Time-Based Evasion

Saldırganlar, günün belirli saatlerinde ağ trafiğini normal bir hale getirerek tespit edilmeden veri sızdırmaya devam ederler.

T1222 - File and Directory Permissions Modification

Şirket ağındaki kritik sistemlere yönelik güvenlik yazılımlarının devre dışı bırakılması için dosya izinleri değiştirilir.

Yanal Hareket (Lateral Movement)

T1210 - Exploitation of Remote Services

Şirket içindeki AR-GE departmanındaki bilgisayarlarda uzaktan erişim için güvenlik açığı bulunarak, saldırganlar diğer sistemlere geçiş yapar.

T1091 - Replication Through Removable Media

Çalışanlara verilen promosyon USB bellekleri aracılığıyla zararlı yazılım, şirket içi sistemlere yayılır.

Etki (Impact)

T1489 - Service Stop

Şirketin ERP ve üretim yazılımlarını çalıştıran sunucularda hizmet durdurma komutları uygulanır. Bu da üretim süreçlerinin durmasına sebep olur.

T1491.001 - Defacement: Internal Defacement

Şirket içi iletişim platformunda tehditkar mesajlar gösterilerek çalışanlar arasında paniğe yol açılır.

Saldırının MITRE ATT&CK Tablosu

Taktik	Teknik	TID
Keşif (Reconnaissance)	Active Scanning	T1595
	Gather Victim Identity Information	T1589
Erişim Kazanma (Initial Access)	Application Layer Protocol: Web Protocols	T1071.001
	Data Staged: Cloud Storage	T1074.002
Savunmadan Kaçınma (Defense Evasion)	Time-Based Evasion	T1564.003
	File and Directory Permissions Modification	T1222
Yanal Hareket (Lateral Movement)	Exploitation of Remote Services	T1210
	Replication Through Removable Media	T1091
Etki (Impact)	Service Stop	T1489
	Internal Defacement	T1491.001

SONUÇ

MITRE ATT&CK çerçevesi, siber tehditleri anlamada ve savunma stratejileri geliştirmede kritik bir rol oynar. Saldırı yöntemlerinin detaylı bir şekilde sınıflandırılması, güvenlik ekiplerine tehditleri daha hızlı ve etkin bir şekilde tespit etme imkanı sağlar. Ayrıca, TTP tabanlı tehdit avcılığı ve Detection Engineering gibi yöntemlerle saldırıları önceden tahmin etmek ve önlemek mümkün hale gelmektedir. Günümüzde siber güvenlik tehditlerinin sürekli evrildiği düşünüldüğünde, MITRE ATT&CK gibi frameworklerin kullanımı, organizasyonların siber dayanıklılığını artırmak için vazgeçilmez bir araç haline gelmiştir.



KAYNAKÇA

1. <https://berqnet.com/blog/mitre-attck-framework>
2. <https://www.ibm.com/think/topics/mitre-attack>
3. [https://csrc.nist.gov/glossary/term/tactics techniques and procedures#:~:text=A %20tactic%20is%20the%20highest%20level%20description%20of%20the%20 behavior,the%20context%20of%20a%20technique.](https://csrc.nist.gov/glossary/term/tactics%20techniques%20and%20procedures#:~:text=A%20tactic%20is%20the%20highest%20level%20description%20of%20the%20behavior,the%20context%20of%20a%20technique.)
4. <https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf>
5. https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html
6. https://www.google.com/search?q=t1059+ukraine&sc_esv=2879a01ec02bb4c4&ei=J8qsZ4zYHp2C7NYPhML10QM&oq=T1059+ukr&gs_lp=Egxnd3Mtd2l6LXNlcniAICVQxMDU5IHVrcioCCAEyBRAhGKABMgUQIRigAUjvP1D9CViHKXABeAGQAQCYAc8BoAGIB6oBBTAuMy4yuAEDyAEA-AEB-AECmAIGoAKpB6gCCsICEBAAGAMYtAIY6gIYjwHYAQHCAgUQABiABM ICBBAAGB7CAgcQABiABBgTwgIGEAAYExgewgIIEAAYExgKGB7CAgoQA BgTGAUYChgemAMK8QWxWKIQniIqMLoGBAgBGAqSBwUxLjMuMqAH8w4&scient=gws-wiz-serp
7. <https://www.dragos.com/blog/new-details-electrum-ukraine-electric-sector-compromise-2022/>
8. <https://attack.mitre.org/groups/G0034/>
9. <https://cyberartspro.com/en/mitre-attack-framework-nedir/>
10. <https://www.exclusive-networks.com/tr/wp-content/uploads/sites/32/2020/12/MITRE-ATTCK-InfoBlox-.pdf>
11. <https://docs.lumu.io/portal/en/kb/articles/attack-matrix>
12. <https://letsdefend.io/blog/how-to-become-a-detection-engineer>
13. <https://www.feroot.com/education-center/what-are-tactics-techniques-and-procedures-ttps/>
14. https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html
15. <https://socprime.com/blog/what-is-detection-engineering/>