**Mitre Att&ck Framework**

* **HAZIRLAYAN:**Sude SARIÇ
* **TARİH:**15.02.2024

1

**GİRİŞ**

Bu raporda, siber güvenlik alanında kritik bir çerçeve olan MITRE ATT&CK Framework ele alınacaktır. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), saldırganların kullandığı taktikler, teknikler ve prosedürler hakkında geniş bir bilgi tabanı sunan bir sistemdir. MITRE Corporation tarafından geliştirilen bu çerçeve, siber tehditleri anlamak, analiz etmek ve savunma stratejilerini güçlendirmek amacıyla güvenlik uzmanları, araştırmacılar ve kurumlar tarafından yaygın olarak kullanılmaktadır.

MITRE ATT&CK Framework, saldırganların nasıl hareket ettiğini anlamaya yardımcı olarak, güvenlik ekiplerinin daha etkili önlemler almasını sağlar. Çerçevenin sunduğu yapı sayesinde, olası saldırıların aşamaları detaylı bir şekilde analiz edilerek, siber savunma mekanizmaları geliştirilebilir. Bu bağlamda, raporda MITRE ATT&CK Framework’ün içeriği, önemi ve kullanımı hakkında detaylı bilgiler sunulacaktır.

**Mitre Att&ck Framework Nedir?**

MITRE ATT&CK (Rekabetçi Taktikler, Teknikler ve Ortak Bilgi) Çerçevesi, siber güvenlik alanında saldırganların kullanım taktikleri, teknikleri ve ortak özellikler için kullanılan bir bilgi tabanıdır. MITRE Corporation tarafından kullanılmaktadır. Çerçeve, savunma ve saldırı yazılımları, güvenlik sistemlerine ve siber güvenlik araştırmacılara yardımcı olmak için tasarlanmıştır.

**Mitre Att&ck Tablosu Neden Önemlidir?**

Mıtre atttack tablosunun siber dünyadaki en büyük yeri oluşabilecek saldırılara daha etkin bir taktik ve teknik kullanarak oluşabilecek tehditlere etkin bir savuma olmasına yardımcı olmaktadır.

**MITRE ATT&CK Framework'ün İçeriği**

Mıtre attack fromworkün içeriği pekçok bölüme ayrılır.Bu Bölümleri detaylı incelersek

* **Matris**:Framework'ün ana bölümüdür ve Saldırganların kullandığı taktikler ve bu taktikler altında yer alan stratejiler tablolar halinde gösterilir.
* **Taktikler**: Saldırganların stratejilerina ulaşmak için kullandıkları geniş stratejilerdir
* **Teknikler**: Taktiklerin altında yer alan daha spesifik saldırı modelleridir
* **Yazılım**: Framework, belirli zararlı yazılımlar ve bunların nasıl barındırılacağı.
* **Gruplar**: Framework, özel saldırgan gruplar (APT'ler) ve bunların taktikleri ve teknik örnekleriyle oluşturulur.

2

* **Veri Kaynakları**: ATT&CK Framework, taktik ve tekniklerin tespit edilmesi ve depolanması için çeşitli veri kaynakları belirtilir.

Sonuç olarak, MITRE ATT&CK Framework, siber güvenlik alanında savunma stratejilerini yaygınlaştırıyor, saldırganların taktiklerini ve tekniklerini geliştiriyor ve siber tehditlerle daha etkili bir şekilde mücadele etmek için çok değerli bir araç.

**TTP Nedir?**

Siber güvenlikteki TTP'ler, siber suçluların saldırıları nasıl planlayıp gerçekleştirdiğini açıklar. Taktikler , teknikler ve prosedürler olarak adlandırılan her bileşen, bir saldırının farklı katmanlarına ilişkin içgörü sunarak güvenlik ekiplerinin olası tehditleri anlamalarına ve bunlara karşı koymalarına yardımcı olur.

* **Taktikler** : Bir saldırganın genel hedefleri ve amaçları. Bunlar saldırının ardındaki "neden"dir.
* **Teknikler** : Saldırganların hedeflerine ulaşmak için kullandıkları yöntemler. Bunlar bir saldırının "nasıl"ıdır.
* **Prosedürler** : Teknikleri uygulamak için gerçekleştirilen belirli eylemler. Bunlar, saldırının ayrıntılı düzeyde "ne" olduğudur.

**TTP-Based Threat Hunting nedir?**

TTP-Based Threat Hunting, tehdit aktörlerinin Tactics (Taktikler), Techniques (Teknikler) ve Procedures (Prosedürler) (TTP'ler) üzerinden izlenmesi ve analiz edilmesi yaklaşımıdır. Bu yöntem, geleneksel tehdit avcılığı (threat hunting) yöntemlerinden farklı olarak belirli araçlara veya kötü amaçlı yazılımlara odaklanmak yerine, saldırganların gerçekleştirmek zorunda olduğu teknikleri anlamaya çalışır.

**Detection Engineering Nedir?**

Detection Engineering (Tespit Mühendisliği), siber tehditlerin tespit edilmesini ve analiz edilmesini iyileştirmek için özel algılama kuralları, imzalar, davranış bazlı analizler ve tehdit avcılığı tekniklerinin tasarlanması, geliştirilmesi ve uygulanması sürecidir.

**TTP-Based Threat Hunting ve Detaction Engineering ?**

TTP avcılığı ile detaction engineering, siber güvenlik stratejilerinin vazgeçilmez iki bileşenidir. TTP avcılığı, analistlerin tehdit aktörlerinin davranışlarına, saldırı kalıplarına ve

3

kullanılan tekniklere odaklanarak geçmiş saldırı eğilimlerini değerlendirip gelecekteki saldırıları öngörmelerini sağlar. Öte yandan, detaction engineering , hem dahili hem de harici verileri toplayarak saldırganların amaçlarını ve hedeflerini belirlemeye yardımcı olur. Bu zengin veri tabanı, analistlerin güncel siber tehdit ortamını anlamalarını ve buna göre etkili tespit kuralları oluşturabilmelerini mümkün kılar. İkisinin entegrasyonu sayesinde, organizasyonlar proaktif savunma stratejileri geliştirerek, saldırıların erken aşamada tespit edilmesi ve önlenmesi konusunda daha donanımlı hale gelir.

**2022 Ukraine Electric Power Attack C0034**

10 Ekim 2022'de Rusya, Kiev'deki de dahil olmak üzere Ukrayna genelindeki elektrik şebekesine 84 seyir füzesi ve 24 intihar uçağından oluşan bir dalgayla saldırısıydı. Yetkisiz komutları SCADA sistemlerinden göndermek için Ukraynalı bir elektrik şirketine erişim sağlamak amacıyla **GOGETTER**, **Neo-REGEORG**, **CaddyWiper** ve **living of the land (LotL**) tekniklerinin bir kombinasyonunu kullanan bir Sandworm Ekibi saldırısıydı. **Sandworm Ekibi**, Rusya Genelkurmay Başkanlığı Ana İstihbarat Müdürlüğü (GRU) Özel Teknolojiler Ana Merkezi (GTsST) askeri birimi 74455'e atfedilen yıkıcı bir tehdit grubudur. Bu grup en az 2009'dan beri aktiftir.

**GOGETTER**: GOGETTER, siber saldırganlar tarafından kullanılan bir özel arka kapı (backdoor) aracıdır. İlk olarak Rus devlet destekli tehdit aktörleri tarafından kullanıldığı tespit edilmiştir.

* **Amaç**: Komuta ve Kontrol (C2) altyapısına bağlantı kurarak, tehdit aktörlerinin hedef sistemleri uzaktan yönetmesini sağlar.
* **Çalışma Prensibi**: HTTP ve HTTPS üzerinden saldırganların kontrol ettiği sunuculara bağlanarak zararlı yükleri indirir ve çalıştırır.

**Neo-REGEORG:** Neo-REGEORG, siber saldırganların iç ağlara sızmak ve bunlar üzerinde proxy (vekil sunucu) tünelleri oluşturmak için kullandıkları bir web shell ve tünelleme aracıdır.

* **Amaç:** HTTP ve HTTPS üzerinden tünelleme yaparak saldırganların iç ağlara erişmesini sağlar.
* **Çalışma Prensibi:** Genellikle web sunucularına gizlenmiş ASP, JSP veya PHP tabanlı bir web shell olarak yüklenir.

**CaddyWiper:** CaddyWiper, veri silme (wiper) amacı taşıyan kötü amaçlı bir yazılımdır. İlk olarak Rusya-Ukrayna savaşında kullanıldığı tespit edilmiştir.

* **Amaç:** Bulaştığı sistemlerde dosya ve disk üzerindeki verileri silmek.
* **Çalışma Prensibi:** Windows sistemlerinde çalışır ve dosyaları hedef alarak onları kullanılamaz hale getirir ,Active Directory (AD) ortamlarına yayılabilir ve büyük ölçekli yıkıcı saldırılar düzenlemek için kullanılabilir.

**Living Off The Land (LotL) Teknikleri:** Living off the Land (LotL), saldırganların mevcut sistem araçlarını kötüye kullanarak zararlı işlemler yürütmesini ifade eder**.**

4

* **Amaç:** Kendi kötü amaçlı yazılımlarını bulaştırmak yerine, sistemde zaten var olan yasal araçları kullanarak tespit edilmeden saldırılar gerçekleştirmek**.**

**Ukraine Electric Power Attack C0034’de Kullanılan TID’ler**

1. **T1059.001 – Komut ve Komut Dosyası Yorumlayıcısı: PowerShell**  
   **Kullanım:**
   * Sandworm Ekibi, Windows Grup İlkesi’ni kullanarak TANKTRAP adlı bir PowerShell yardımcı programı vasıtasıyla bir silme aracını yaydı ve çalıştırdı.  
     **Açıklama:**
   * Bu yöntem, saldırı zincirinin erken aşamasında zararlı kodun yayılmasını sağlamak amacıyla kullanılmıştır.
2. **T1543.002 – Sistem İşlemini Oluştur veya Değiştir: Systemd Hizmeti**  
   **Kullanım:**
   * GOGETTER adlı kötü amaçlı yazılımın kalıcılığını sağlamak için Systemd yapılandırıldı.
   * “WantedBy=multi-user.target” yapılandırması, sistem kullanıcılarının oturum açmasıyla GOGETTER’ın otomatik olarak çalışmasını tetikledi.  
     **Açıklama:**
   * Bu teknik, saldırganın sistemde uzun süreli erişim elde etmesi için kalıcılık mekanizması oluşturdu.
3. **T1485 – Veri İmhası**  
   **Kullanım:**
   * Sandworm Ekibi, kurbanın BT ortam sistemlerinde eşlenen sürücüler ve fiziksel sürücü bölümleriyle birlikte OT yetenekleriyle ilgili dosyaları silmek amacıyla CaddyWiper aracını yerleştirdi.  
     **Açıklama:**
   * Veri imhası, saldırı sonrası iz bırakmamak veya hedef sistemin operasyonunu kesintiye uğratmak için kritik dosyaların yok edilmesinde kullanılır.
4. **T1484.001 – Alan veya Kiracı Politikası Değişikliği: Grup Politikası Değişikliği**  
   **Kullanım:**
   * Kötü amaçlı yazılımların dağıtımını ve yürütülmesini desteklemek amacıyla, Grup İlkesi Nesneleri (GPO’lar) kullanıldı.  
     **Açıklama:**

5

* + Bu yöntem, saldırının yaygınlaştırılmasında ve meşru işlemler arasında gizlenerek gerçekleştirilmesinde rol oynadı.

1. **T1570 – Yanal Alet Transferi**  
   **Kullanım:**
   * CaddyWiper’ın yürütülebilir dosyası, msserver.exe adlı hazırlama sunucusundan yerel bir sabit sürücüye, Grup İlkesi Nesnesi (GPO) kullanılarak kopyalandı.  
     **Açıklama:**
   * Bu teknik, zararlı araçların saldırı öncesi transferiyle, sonraki aşamalarda kullanılmak üzere hazır hale getirilmesini sağladı.
2. **T1036.004 – Maskeleme: Maskeli Görev veya Hizmet**  
   **Kullanım:**
   * GOGETTER kötü amaçlı yazılımı, meşru veya meşru görünebilecek hizmetler olarak maskelemek amacıyla Systemd hizmet birimlerinden yararlandı.  
     **Açıklama:**
   * Maskeleme, saldırı araçlarının normal sistem faaliyetleri arasında gizlenerek tespit edilmesini zorlaştırır.
3. **T1095 – Uygulama Dışı Katman Protokolü**  
   **Kullanım:**
   * TLS tabanlı bir tünel içinde, C2 (Komuta ve Kontrol) iletişimleri proxy’lenerek yürütüldü.  
     **Açıklama:**
   * Bu yöntem, saldırgan ile kontrol sunucusu arasındaki iletişimin şifrelenmiş ve gizli tutulmasını sağlar.
4. **T1572 – Protokol Tünelleme**  
   **Kullanım:**
   * GOGETTER tünelleme yazılımı kullanılarak, “Yamux” adı verilen TLS tabanlı bir C2 kanalı oluşturuldu; böylece harici sunucu(lar) ile bağlantı kuruldu.  
     **Açıklama:**
   * Protokol tünelleme, standart trafiğe karışarak saldırı iletişimlerinin tespit edilmesini zorlaştırır.

6

1. **T1053.005 – Zamanlanmış Görev/İş: Zamanlanmış Görev**  
   **Kullanım:**
   * CaddyWiper’ın belirli zamanlarda yürütülmesi için, bir Grup İlkesi Nesnesi (GPO) aracılığıyla Zamanlanmış Görevlerden yararlanıldı.  
     **Açıklama:**
   * Zamanlanmış görevler, saldırı işlemlerinin otomatikleştirilmesi ve önceden belirlenmiş zamanlarda yürütülmesi için kullanılır.
2. **T1505.003 – Sunucu Yazılım Bileşeni: Web Shell**  
   **Kullanım:**
   * Neo-REGEORG web kabuğu, internete bakan bir sunucuya yerleştirilerek uzaktan erişim ve kontrol sağlandı.  
     **Açıklama:**
   * Web shell, saldırganın sisteme erişim sağlaması ve komut çalıştırabilmesi için bir arka kapı görevi görür.
3. **T0895 – Otomatik Çalıştırma Görüntüsü**  
   **Kullanım:**
   * Mevcut hipervizör erişimi kullanılarak, bir SCADA sunucusunu çalıştıran sanal makineye adlandırılmış ISO görüntüsü (a.iso) eşlendi.
   * SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik çalıştıracak şekilde yapılandırılmıştı; bu sayede ISO içindeki kötü amaçlı VBS betiği otomatik olarak yürütüldü.  
     **Açıklama:**
   * Bu teknik, saldırganın SCADA ortamında hedef sistemlere ulaşması ve kötü amaçlı kodu otomatik olarak çalıştırması için kullanılmıştır.
4. **T0807 – Komut Satırı Arayüzü**  
   **Kullanım:**
   * MicroSCADA platformundaki SCIL-API (scilc.exe) kullanılarak, ikili dosya aracılığıyla komutlar yürütüldü.  
     **Açıklama:**
   * Komut satırı arayüzleri, saldırganın sistemde doğrudan komut çalıştırmasını sağlayarak operasyonel faaliyetleri hızlandırır.

7

1. **T0853 – Komut Dosyası**  
   **Kullanım:**
   * MicroSCADA komutunun yürütülmesi için Visual Basic betiği (lun.vbs) kullanıldı.  
     **Açıklama**
   * Komut dosyaları, saldırının belirli aşamalarını otomatikleştirmek ve tekrarlanabilir hale getirmek amacıyla kullanılır.
2. **T0894 – Sistem İkili Proxy Çalıştırma**  
   **Kullanım:**
   * Saldırgan tarafından tanımlanan bir dosyada (örneğin, s1.txt) belirtilen önceden tanımlı SCADA talimatları, scilc.exe adlı MicroSCADA uygulama ikili dosyası aracılığıyla yürütüldü.
   * Örneğin, “C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt” komutu ile yetkisiz komut mesajları uzak trafo merkezlerine gönderildi.  
     **Açıklama:**
   * Bu teknik, SCADA yazılımını kullanarak uzaktaki sistemlere zararlı komutlar iletilmesini sağlar.
3. **T0855 – Yetkisiz Komut Mesajı**  
   **Kullanım:**
   * MicroSCADA SCIL-API’si kullanılarak, trafo merkezlerine yetkisiz komutlar gönderildi.  
     **Açıklama:**
   * Bu yöntem, saldırganın SCADA sistemleri üzerinden kontrol komutları ileterek operasyonu yönlendirmesine olanak tanır.

**Örnek Bir Senaryoyla Mitre Att&ck Tablosunun Kullanımı**

**Senaryo:** X firiması , yatırım sektörüne yönelik yazılım çözümleri geliştiren henüz gelişmekte olan bir şirkettir.HackerX adında bir hacker grubu, şirketin sahip olduğu müşteri verilerini ele geçirmek ve fidye talep etmek amacıyla bir saldırı düzenler. Saldırı süreci, keşif aşamasından veri sızdırma aşamasına kadar sistematik olarak ilerler.

Saldırı Süreci:

Saldırı süreci ilk olarak keşif aşamasıyla başlar HackerX gurubu X firimasına ait öncelikle sosyal mühendislik ,Açık servis taraması yaparak şirketin müşterilerine ait bilgi toplarlar.

8

**Keşif [TA0043]**

**T1598.002 -** Reconnaissance bu tatikle HackerX gurubu , Xfirimasında çalışan bir çalışana bir e-posta hesabı üzerinden satın aldığı bir ürün varmış gibi kulallnıcının biliglerinin olduğu bir mail gönderir.ve çalışan bu biligleri doldurur böylece X firimasında çalışan bir çalışanın biligilerine de erişilmiş olunur.ve bu epostadayı gizli bir şekilde düzenleye saldıgamlar exe çalıştırarak asıl amacına saldırganlar ulaşır.

**T1595.002-**Güvenlik Açığı Taraması,HackerX gurubu shodan gibi araçları kullanarak intarnet üzerindeki açık servisleri tarar.Bu taramaların sonucunda Açık bir RDP ve web sunucu bulurlar.

**İlk Erişim [TA0001]**

**T1133 -** Uzaktan Servisler Üzerinden Yetkisiz Giriş **(**External Remote Services),Açık RDP servisini kullanarak, zayıf parolalara karşı brute-force saldırısı yaparlar ve yönetici ayrıcalıkları olan bir hesabın şifresini kırarlar.

**T1566.001** - Kimlik Avı E-Postası ile Zararlı Dosya Gönderme ,Sosyal mühendislik saldırısı sonucunda, hedeflenen çalışan bir Excel makrosu içeren bir dosya açar. Makro çalıştırıldığında, sistemde PowerShell ile bir ters kabuk (reverse shell) açılır.

**Ayrıcalık Yükseltme [TA0004]**

Sistemdeki kısıtlamaları aşarak daha fazla kontrol elde ederler.

**T1548.002 -** Yetkili Komut Satırına Erişim (Bypass User Account Control - UAC Bypass)

PowerShell üzerinden fodhelper.exe istismar edilerek yönetici hakları yükseltilir.

**T1055.012** - Thread Injection ile Kötü Amaçlı Kod Enjekte Etme (Process Injection - Thread Execution Hijacking)

Saldırganlar, tespit edilmemek için lsass.exe gibi bir sürece zararlı kod enjekte ederler.ve böylece kendi yetkilerini yükseltirler.

**Savunmadan Kaçınma [TA0005]**

Tespit edilmemek için çeşitli teknikler uygulanır.

**T1027.002** - PowerShell Komutlarını Şifreleme (Obfuscated Files or Information - Encoding PowerShell Commands)

9

PowerShell komutları Base64 ile şifrelenerek yürütülür, böylece güvenlik çözümleri tarafından tespit edilmesi zorlaşır.

**T1562.001** - Windows Defender ve Günlükleme Servislerini Devre Dışı Bırakma (Impair Defenses - Disable or Modify Tools)

Windows Defender hizmetleri durdurulur ve güvenlik günlükleri silinir.

**Etki Alanı Haklarının Ele Geçirilmesi [TA0006]**

**Saldırganlar, sistemdeki kimlik bilgilerini ele geçirir.**

**T1003.001 -** LSASS Bellek Dökümleme (OS Credential Dumping: LSASS Memory Dumping)

Mimikatz kullanılarak LSASS bellek dökümü alınır ve sistemdeki şifreler elde edilir.

**T1555.003 -** Tarayıcıdan Kaydedilmiş Şifreleri Çekme (Credentials from Password Stores: Credentials from Web Browsers)

Çalışanların tarayıcılarında kaydedilmiş şifreler çekilir.

**Lateral Movement [TA0008]**

Saldırganlar, şirket ağı içinde yayılır.

**T1075 -** Windows Management Instrumentation (WMI) Kullanarak Uzaktan Komut Çalıştırma

Ele geçirilen sistemlerden diğer sunuculara WMI ile uzaktan kod yürütülerek erişim sağlanır**.**

**T1021.001** - RDP Kullanarak Yanal Hareket (Remote Services: Remote Desktop Protocol - RDP)

Ele geçirilen RDP kimlik bilgileri kullanılarak, şirketin kritik veritabanı sunucusuna erişim sağlanır.

**Veri Hırsızlığı ve Sızdırma (Exfiltration) [TA0010]**

Şirketin kritik verileri çalınır ve dışarı sızdırılır**.**

**T1041 -** Komuta ve Kontrol Sunucusuna Veri Gönderme (Exfiltration Over C2 Channel)

Çalınan veriler, saldırganların Tor ağı üzerinden yönlendirilmiş bir C2 (Command & Control) sunucusuna gönderilir.

**10**

**T1567.002 -** Bulut Depolama Kullanarak Veri Sızdırma (Exfiltration to Cloud Storage - Exfiltration to Dropbox)

Büyük boyutlu dosyalar, Dropbox ve Google Drive API’ları kullanılarak saldırganların kontrolündeki hesaplara yüklenir.

**Etki ve Fidye Talebi (Impact) [TA0040]**

Saldırganlar, şirketin operasyonlarını aksatarak fidye talep eder**.**

**T1486** - Dosya Şifreleme ve Fidye Notu Bırakma (Data Encrypted for Impact - Ransomware Attack)

Sunuculardaki veriler şifrelenir ve çalışan bilgisayarlarına fidye notu bırakılır.

**T1490** - Yedekleme Silme (Inhibit System Recovery)

Windows Shadow Copies ve SQL veritabanı yedekleri saldırganlar tarafından silinir.

**SONUÇ:**

Bu raporda, MITRE ATT&CK Framework’ün yapısı, işleyişi ve siber güvenlik alanındaki önemi detaylı bir şekilde ele alınmıştır. Öncelikle, çerçevenin saldırganların kullandığı taktikler, teknikler ve prosedürleri (TTP’ler) nasıl sınıflandırdığı incelenmiş, ardından bu bilginin siber tehdit istihbaratında nasıl kullanıldığı açıklanmıştır. Rapor boyunca, MITRE ATT&CK Framework’ün temel bileşenleri olan **Taktikler, Teknikler ve Prosedürler (TTP’ler)** detaylı bir şekilde analiz edilmiştir. Bu sayede, bir saldırganın sistemlere nasıl sızdığı, yetkisini nasıl yükselttiği, verileri nasıl ele geçirdiği ve saldırısını nasıl sürdürdüğü gibi kritik aşamalar açıklığa kavuşturulmuştur.

Bu rapor sayesinde, MITRE ATT&CK’ün sadece bir tehdit sınıflandırma sistemi olmadığı, aynı zamanda siber güvenlik stratejilerini geliştiren ve güvenlik ekiplerine rehberlik eden önemli bir kaynak olduğu görülmüştür. Kurumların, bu framework’ü aktif bir şekilde kullanarak saldırılara karşı daha dirençli hale gelebileceği ve güvenlik açıklarını daha iyi analiz edebileceği sonucuna ulaşılmıştır.

**KAYNAKÇA:**

* [**https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e**](https://aslikuzucuu.medium.com/mitre-att-ck-5e465f1920e)
* [**https://www.broadcom.com/topics/mitre-attack**](https://www.broadcom.com/topics/mitre-attack)
* [**https://www.balbix.com/insights/tactics-techniques-and-procedures-ttps-in-cyber-security/**](https://www.balbix.com/insights/tactics-techniques-and-procedures-ttps-in-cyber-security/)
* [**https://kaleileriteknoloji.medium.com/tehdit-avc%C4%B1l%C4%B1%C4%9F%C4%B1-f58d7003e0f9**](https://kaleileriteknoloji.medium.com/tehdit-avc%C4%B1l%C4%B1%C4%9F%C4%B1-f58d7003e0f9)

**11**

* [**https://medium.com/@onuroktay/detection-engineer-ne-yapar-g%C3%BCnl%C3%BCk-g%C3%B6revleri-rutinleri-nelerdir-1d6a23a4fee4#:~:text=Detection%20Engineering%20arkada%C5%9Flar%20g%C3%BCvenlik%20sistemlerini,ba%C4%9Fl%C4%B1%20kalmadan%20monitoring%20yapmalar%C4%B1%20beklenir**](https://medium.com/@onuroktay/detection-engineer-ne-yapar-g%C3%BCnl%C3%BCk-g%C3%B6revleri-rutinleri-nelerdir-1d6a23a4fee4#:~:text=Detection%20Engineering%20arkada%C5%9Flar%20g%C3%BCvenlik%20sistemlerini,ba%C4%9Fl%C4%B1%20kalmadan%20monitoring%20yapmalar%C4%B1%20beklenir)**.**
* [**https://en.wikipedia.org/wiki/Russian\_strikes\_against\_Ukrainian\_infrastructure\_(2022%E2%80%93present)**](https://en.wikipedia.org/wiki/Russian_strikes_against_Ukrainian_infrastructure_(2022%E2%80%93present))

12