

**Mitre Att&ck Framework**

**İlayda HÖRGÜŞLÜOĞLU**

**16/02/2025**

**Mitre Att&ck Framework**

1. **Mitre ATT&CK Tablosu Nedir?**

Mitre ATT&CK, (Adversarial Tactics, Techniques, and Common Knowledge tablosu saldırganların kullandığı saldırı taktik ve teknikleri açıklayan, sınıflandıran ve belgeleyen bir veri tabanıdır. Mitre ATT&CK, tehdit istihbaratı, olay müdahalesi, tehdit avcılığı ve güvenlik açığı yönetimi gibi birçok alanda güvenlik ekiplerine yol göstermektedir.

1. **Mitre ATT&CK Tablosu Neden Önemlidir?**

Saldırıların nasıl gerçekleştiğini ve hangi yöntemlerin kullanıldığını detaylı bir şekilde açıklayarak siber güvenlik uzmanlarının tehditleri anlamasına ve savunma mekanizmalarını güçlendirmelerine yardımcı olmaktadır. Siber güvenlik ekipleri bu tabloyu kullanarak tehdit aktörlerinin taktiklerini ve tekniklerini analiz edebilir ve tehdit avcılığı süreçlerini geliştirebilir ve olay müdahale süreçlerini optimize edebilir.

1. **Mitre ATT&CK Framework’de Bulunan Taktik ve Tekniklerin Önemi**

Saldırganların saldırı sürecinde izlediği yöntemleri analiz edebilmek için önemli bir yere sahiptir. Taktikler, saldırının hangi aşamada olduğunu tanımlarken, teknikler saldırının nasıl gerçekleştirildiğini detaylı bir şekilde açıklamaktadır. Bu başlıklar sayesinde, sistemler güçlendirilebilmekte ve tehditlere karşı etkili önlemler alınabilmektedir. Özellikle güvenlik operasyon merkezleri (SOC) ve tehdit istihbarat ekipleri, bu tablodan yararlanarak daha etkili tehdit avcılığı ve tespit mühendisliği gerçekleştirilebilmeleri mümkündür.

1. **TTP Nedir?**

Taktik, teknik, prosedür (Tactics, Techniques, and Procedures) kelimelerinin kısaltılmışıdır. Tehdit aktörlerinin saldırı sürecinde izlediği yöntemleri ifade etmektedir.

* Taktik: Saldırganların, saldırı sürecinde hedeflerine ulaşabilmek için izledikleri yollar veya genel stratejidir.
* Teknik: Taktikleri gerçekleştirmek için kullanılan spesifik yöntemlerdir.
* Prosedür: Saldırganların belirli teknikleri nasıl uyguladığına dair detaylı açıklamalardır.

1. **TTP-Based Threat Hunting ve Detection Engineering nedir?**

* **TTP-Based Threat Hunting (Tehdit Avcılığı)**

Saldırganların belirli taktik, teknik ve prosedürlerini analiz ederek ağ içinde gizlenen tehditleri tespit etmeye yönelik bir yaklaşımdır. Bu yöntem, MITRE ATT&CK tablosunu kullanılarak gerçekleştirilir ve güvenlik uzmanlarının saldırı yöntemlerini belirlemesine yardımcı olur.

* **Detection Engineering (Tespit Mühendisliği)**

Güvenlik olaylarını ve saldırıları tespit etmek için tespit kurallarının ve izleme sistemlerinin geliştirilmesini içerir. Tehdit avcılığı sürecinde belirlenen saldırı teknikleri temel alınarak, özel tespit mekanizmaları oluşturulur.

1. **2022 Ukraine Electric Power Attack C0034**

2022 yılında Ukrayna’nın elektrik altyapısına yönelik gerçekleştirilen bu saldırı, Rusya bağlantılı tehdit aktörleri tarafından gerçekleştirildi. Bu saldırıda amaç Ukraynalı bir elektrik şirketine erişim sağlamaktı. Sandworm Team hacker grubu tarafından gerçekleştirildiği bilinmektedir.

| **İD** | | **İsim** | **Kullanmak** |
| --- | --- | --- | --- |
| Girişim | [T1059](https://attack.mitre.org/techniques/T1059) | [.001](https://attack.mitre.org/techniques/T1059/001) | [Komut ve Komut Dosyası Yorumlayıcısı](https://attack.mitre.org/techniques/T1059) : [PowerShell](https://attack.mitre.org/techniques/T1059/001) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , Windows Grup İlkesi'ni kullanarak bir silme aracını yaymak ve başlatmak için TANKTRAP adlı bir PowerShell yardımcı programını kullandı. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1543](https://attack.mitre.org/techniques/T1543) | [.002](https://attack.mitre.org/techniques/T1543/002) | [Sistem İşlemini Oluştur veya Değiştir](https://attack.mitre.org/techniques/T1543) : [Systemd Hizmeti](https://attack.mitre.org/techniques/T1543/002) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , GOGETTER'ın kalıcılığını korumak için Systemd'yi yapılandırdı ve WantedBy=multi-user.targetsistem kullanıcı oturum açmalarını kabul etmeye başladığında GOGETTER'ı çalıştıracak yapılandırmayı belirtti. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1485](https://attack.mitre.org/techniques/T1485) | | [Veri İmhası](https://attack.mitre.org/techniques/T1485) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , eşlenen sürücüler ve fiziksel sürücü bölümleriyle birlikte OT yetenekleriyle ilgili dosyaları silmek için kurbanın BT ortam sistemlerine [CaddyWiper'ı](https://attack.mitre.org/software/S0693) yerleştirdi . [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1484](https://attack.mitre.org/techniques/T1484) | [.001](https://attack.mitre.org/techniques/T1484/001) | [Alan veya Kiracı Politikası Değişikliği](https://attack.mitre.org/techniques/T1484) : [Grup Politikası Değişikliği](https://attack.mitre.org/techniques/T1484/001) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , kötü amaçlı yazılımları dağıtmak ve yürütmek için Grup İlkesi Nesnelerini (GPO'lar) kullandı. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1570](https://attack.mitre.org/techniques/T1570) | | [Yanal Alet Transferi](https://attack.mitre.org/techniques/T1570) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , dağıtım öncesinde [CaddyWiper'ın](https://attack.mitre.org/software/S0693) yürütülebilir dosyasını msserver.exebir hazırlama sunucusundan yerel bir sabit sürücüye kopyalamak için bir Grup İlkesi Nesnesi (GPO) kullandı . [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1036](https://attack.mitre.org/techniques/T1036) | [.004](https://attack.mitre.org/techniques/T1036/004) | [Maskeleme](https://attack.mitre.org/techniques/T1036) : [Maskeli Görev veya Hizmet](https://attack.mitre.org/techniques/T1036/004) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , GOGETTER kötü amaçlı yazılımını meşru veya meşru görünen hizmetler olarak maskelemek için Systemd hizmet birimlerinden yararlandı. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1095](https://attack.mitre.org/techniques/T1095) | | [Uygulama Dışı Katman Protokolü](https://attack.mitre.org/techniques/T1095) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , TLS tabanlı bir tünel içinde C2 iletişimlerini proxy'ledi. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1572](https://attack.mitre.org/techniques/T1572) | | [Protokol Tünelleme](https://attack.mitre.org/techniques/T1572) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , harici bir sunucu(lar) ile "Yamux" TLS tabanlı bir C2 kanalı kurmak için GOGETTER tünelleme yazılımını konuşlandırdı. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1053](https://attack.mitre.org/techniques/T1053) | [.005](https://attack.mitre.org/techniques/T1053/005) | [Zamanlanmış Görev/İş](https://attack.mitre.org/techniques/T1053) : [Zamanlanmış Görev](https://attack.mitre.org/techniques/T1053/005) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , [CaddyWiper'ı](https://attack.mitre.org/software/S0693) önceden belirlenmiş bir zamanda yürütmek için bir Grup İlkesi Nesnesi (GPO) aracılığıyla Zamanlanmış Görevlerden yararlandı . [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| Girişim | [T1505](https://attack.mitre.org/techniques/T1505) | [.003](https://attack.mitre.org/techniques/T1505/003) | [Sunucu Yazılım Bileşeni](https://attack.mitre.org/techniques/T1505) : [Web Shell](https://attack.mitre.org/techniques/T1505/003) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , Neo-REGEORG web kabuğunu internete bakan bir sunucuya yerleştirdi. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| İKS | [T0895](https://attack.mitre.org/techniques/T0895) | | [Otomatik Çalıştırma Görüntüsü](https://attack.mitre.org/techniques/T0895) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında , [Sandworm Ekibi,](https://attack.mitre.org/groups/G0034) bir SCADA sunucusunu çalıştıran sanal bir makineye adlandırılmış bir ISO görüntüsünü eşlemek için mevcut hipervizör erişimini kullandı a.iso. SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik olarak çalıştıracak şekilde yapılandırıldı ve sonuç olarak, ISO görüntüsünde kötü amaçlı bir VBS betiği otomatik olarak yürütüldü. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| İKS | [T0807](https://attack.mitre.org/techniques/T0807) | | [Komut Satırı Arayüzü](https://attack.mitre.org/techniques/T0807) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , ikili dosya aracılığıyla komutları yürütmek için MicroSCADA platformundaki SCIL-API'yi kullandı scilc.exe. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| İKS | [T0853](https://attack.mitre.org/techniques/T0853) | | [Komut dosyası](https://attack.mitre.org/techniques/T0853) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , MicroSCADA komutunu yürüten lun.vbsbir Visual Basic betiğini kullandı . [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology)n.batscilc.exe |
| İKS | [T0894](https://attack.mitre.org/techniques/T0894) | | [Sistem İkili Proxy Çalıştırma](https://attack.mitre.org/techniques/T0894) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında , [Sandworm Ekibi,](https://attack.mitre.org/groups/G0034)scilc.exe saldırgan tarafından tanımlanan bir dosyada belirtilen önceden tanımlanmış bir SCADA talimatları listesini göndermek için bir MicroSCADA uygulama ikili dosyasını yürüttü s1.txt. Yürütülen komut, C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txtyetkisiz komut mesajlarını uzak trafo merkezlerine göndermek için SCADA yazılımını kullanır. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |
| İKS | [T0855](https://attack.mitre.org/techniques/T0855) | | [Yetkisiz Komut Mesajı](https://attack.mitre.org/techniques/T0855) | [2022 Ukrayna Elektrik Gücü Saldırısı](https://attack.mitre.org/campaigns/C0034) sırasında [Sandworm Ekibi](https://attack.mitre.org/groups/G0034) , trafo merkezlerine yetkisiz komutların gönderilmesi de dahil olmak üzere bir dizi SCADA talimatını belirtmek için MicroSCADA SCIL-API'sini kullandı. [[1]](https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology) |

1. **Senaryo**

Askeri malzemeler üreten bir fabrika olan “HürGüçlü İleri Malzemeler Sanayi ve Teknoloji” şirketi son zamanlarda hızla büyüyen bir firma haline gelmiştir. Rakip firmalardan biri bu büyüyüşten rahatsız olarak HürGüçlü şirketinin verilerini sızdırarak kötü bir algı yaratıp şirketin büyüyüşünü engellemek hatta ekonomik olarak çıkmaza sürüklemek istemektedir. Bunun için siber bir saldırı başlatmayı hedeflemektedir. Gerçekleştirdiği aşamalar aşağıdaki gibidir:

1. Kimlik bilgisi toplama (Credential Dumping) (T1003)

Şirketin ip bilgisini elde etmek için çeşitli yöntemler denenmiştir ve ip bilgileri elde edilmiştir.

1. Ağ Keşfi (Active Scanning) (T1595)

Nmap ve çeşitli toollar kullanılarak trafik akışı incelenmiş, açık port taraması gerçekleştirilmiştir.

1. Kimlik Avı (Spearphishing Link) (T1566.002)

Şirket çalışanlarına çeşitli yanıltıcı mailler göndererek phishing saldırısı gerçekleştirilmiştir.

1. Geçerli Hesap Kullanımı (Valid Accounts) (T1078)

Phishing saldırısında edinilen bilgiler ile ayrıcalık yükseltme gibi işlemlerin yapılabilmesi için phishing saldırısına yakalanan bir çalışanın hesabına giriş yapılır.

1. LPE Sömürüsü (Exploitation for Privilege Escalation) (T1068)

Girilen hesapta çeşitli yöntemler kullanılarak yetki yükseltme aşaması yapılır.

1. Hizmetler Aracılığıyla Yetki Yükseltme (Service Execution) (T1569)

Diğer aşamada yapılanlar sayesinde root olarak şirket yöneticisinin yetkilerine ulaşılarak verilere daha kolay bir şekilde erişilebilmiştir.

1. Zamanlanmış Görevler (Scheduled Task/Job) (T1053)

Saldırgan yüklediği kodu şirket çalışanlarının mesailerinin dışında bir saatte çalıştırılmak üzere planlamıştır.

1. Arka Kapı (Backdoor) Kullanımı (T1574)

Sistemde gezinerek bütün bilgiler toplanır.

1. Şifreli Kanal Üzerinden C2 İletişimi (Encrypted Channel) (T1573)

Verileri aktarabilmek için kanal iletişimi kurulurmuştur.

1. Uzaktan Dosya Transferi (Ingress Tool Transfer) (T1105)

Veri transferi gerçekleştirilmiştir.