Mitre Att&ck Framework

Hazırlayan: Sinan Kocagöz

Tarih: 13.02.2025

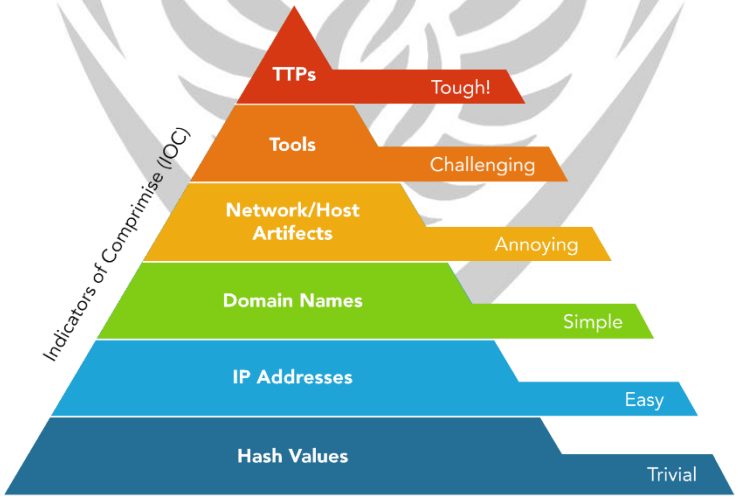
İçindekiler Tablosu

1. Giriş

- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework siber güvenlik uzmanlarına kapsamlı bir rehber sunmaktadır. MITRE ATT&CK, siber tehdit aktörlerinin kullandığı taktikler, teknikler ve prosedürler (TTP – Tactics, Techniques, and Procedures) hakkında ayrıntılı bilgiler içeren bir bilgi tabanıdır. Güvenlik ekipleri, bu framework'ü kullanarak saldırı tekniklerini analiz edebilir, tehdit avcılığı (Threat Hunting) süreçlerini geliştirebilir ve güvenlik sistemlerini daha etkili bir şekilde yapılandırabilirler.

2. MITRE ATT&CK Tablosu Nedir?

- MITRE ATT&CK tablosu, siber saldırganların hedeflerine ulaşmak için kullandığı taktik ve teknikleri sistematik bir şekilde sınıflandıran bir bilgi tabanıdır. Bu tablo, siber tehdit aktörlerinin izleyebileceği yolları ayrıntılı bir şekilde açıklayarak güvenlik ekiplerine tehdit avcılığı (Threat Hunting), risk değerlendirmesi ve savunma stratejileri geliştirme konularında önemli bir avantaj sağlar.
- Her bir teknik, saldırganların kullanabileceği yöntemleri ve bu yöntemlere karşı alınabilecek savunma önlemlerini içerir. Bu sayede kurumlar, bilinen saldırı senaryolarına karşı savunmalarını test edebilir, güvenlik açıklarını belirleyebilir ve sistemlerini iyileştirmek için stratejik önlemler alabilir. Ayrıca, güncel tehdit raporlarından yararlanarak en yaygın kullanılan saldırı vektörlerine karşı proaktif savunma mekanizmaları oluşturabilirler.
- Güvenlik uzmanı David Bianco, tehdit göstergelerini önemlerine göre sınıflandırmak amacıyla 2013 yılında Acı Piramidi kavramını ortaya attı. Bu kavramda piramidin her katmanı hem güvenlik uzmanlarının hem de saldırganların ilgili tehdidi başlatmak veya tespit etmek için katlanmak zorunda kalacakları "acıyı" temsil ediyor. Bu nedenle, örneğin, karma değerlerini toplamak ve anlamak nispeten kolay olsa da saldırıları belirlemek ve azaltmak için TTP (taktik, teknik, prosedür) analizini uygulamak için aynı şey söylenemez.



3. MITRE ATT&CK Matrisleri

3.1.Enterprise ATT&CK Matrisi

- MITRE ATT&CK Enterprise Matrisi, siber güvenlikteki en yaygın kullanılan araçlardan biridir. Özellikle işletmelerde kullanılan Windows, macOS, ve Linux işletim sistemleri üzerine odaklanır. Saldırı tespit edildiğinde, matris saldırının hangi aşamada olduğunu ve hangi tekniklerin kullanıldığını

belirlemeye yardımcı olur, böylece müdahale ekipleri daha hızlı ve etkin hareket edebilir.

- Enterprise matrisi, siber saldırı süreçlerinin farklı aşamalarını temsil eden 14 ana taktik kategorisi içerir. Tüm taktikler aşamalarla birbirini takip eden saldırı zincirinden oluşur. Matrisin hangi yerinde bulunduğunuzu tespit ederek süreci hızla ilerletebilirsiniz.

3.2.Mobile ATT&CK Matrisi

- Mobile matrisi, mobil cihazlara yönelik tehditlerle ilgili Android ve iOS işletim sistemlerine odaklanır. Cihaz bazlı konfigürasyon hatalarından mobil uygulamalara kadar çeşitli açılardan zafiyet verileri bulunur. Mobil cihazlara özgü saldırı vektörlerini inceleyerek özel bilgilerinizin bulunduğu cihazlarınızı koruma altına alabilirsiniz.

3.3.ICS ATT&CK Matrisi

- ICS Matrisi, endüstriyel kontrol sistemlerine yönelik siber tehditleri ele alır. Kritik altyapıların korunmasında önemli rol oynayan matris, enerji santralleri, su arıtma tesisleri gibi yerlerde sıklıkla kullanılır. Potansiyel saldırıları analiz ederek şehirlerin refahını güvende tutar. ICS matrisi, fiziksel proseslerin ve bunların siber dünyayla olan etkileşimlerinin güvenliğine odaklanır. Herhangi bir şüpheli eylem durumunda güvenlik operasyon merkezi (SOC) ile, ICS ATT&CK Matrisini kullanarak tehditleri analiz edebilir, uygun müdahale stratejilerini geliştirebilirsiniz.

4. Mitre Atak Tablosu Neden Önemlidir?

Bu tablo aşağıdaki nedenlerden dolayı kritik öneme sahiptir:

- Ortak bir siber güvenlik dili oluşturur, güvenlik ekiplerinin aynı terminolojiyle çalışmasını sağlayarak bilgi paylaşımını kolaylaştırır.
- Tehdit aktörlerinin davranışlarını anlama ve öngörme imkanı sağlar, saldırganların hangi taktik ve teknikleri kullandığını analiz ederek proaktif savunma stratejileri geliştirmeye yardımcı olur.
- Savunma stratejilerinin geliştirilmesinde sistematik bir yaklaşım sunar, saldırıların her aşamasına yönelik önlemler belirlemeye imkan tanır.
- Güvenlik ekiplerinin tehdit avlama (Threat Hunting) ve tespit mühendisliği (Detection Engineering) çalışmalarına rehberlik eder, potansiyel tehditleri tespit etme ve güvenlik açıklarını kapatma süreçlerini iyileştirir.
- Risk değerlendirmesi ve güvenlik olgunluk seviyesinin belirlenmesinde kullanılır, kurumların mevcut güvenlik duruşlarını analiz etmelerine ve eksik yönlerini tespit etmelerine yardımcı olur.

- Tehdit simülasyonları ve tatbikatlar için temel oluşturur, saldırı senaryolarını canlandırarak güvenlik açıklarını önceden tespit etme imkanı sunar.
- Güvenlik olaylarına müdahale süreçlerini hızlandırır, olay yanıt ekiplerine saldırganın muhtemel bir sonraki adımını tahmin etme ve buna göre aksiyon alma fırsatı verir.

Bu sayede kurumlar, önceden tanımlanmış saldırı senaryolarına karşı savunmalarını ölçebilir, zayıf noktalarını tespit ederek iyileştirmeler yapabilir ve en yaygın kullanılan saldırı vektörlerine karşı önlemler alabilirler.

5. Taktik ve Tekniklerin Önemi

- Taktik ve teknikler, saldırganların hedeflerine ulaşmak için kullandıkları yöntemleri detaylı olarak açıklar. Taktikler, saldırının genel aşamalarını (örn. Initial Access, Execution, Persistence) temsil ederken, teknikler bu aşamalarda kullanılan spesifik yöntemleri tanımlar.
  Bu yapı, güvenlik ekiplerine:
  - Saldırı senaryolarını daha iyi anlama, saldırganların olası yollarını önceden belirleme fırsatı sunar.
  - Savunma mekanizmalarını önceliklendirme, kritik saldırı vektörlerine karşı önleyici önlemler geliştirmeye yardımcı olur.
  - Tespit ve müdahale stratejilerini geliştirme, saldırı gerçekleşmeden önce veya sırasında etkin yanıt verme şansı tanır.
  - Güvenlik operasyonlarını iyileştirme, tehdit avcılığı (Threat Hunting) ve olay müdahalesini daha verimli hale getirir.

6. TTP Nedir?

- TTP (Tactics, Techniques, and Procedures), tehdit aktörlerinin saldırı metodolojilerini tanımlayan üç temel bileşeni ifade eder:

6.1.Taktikler (Tactics)

- Taktikler, bir saldırganın başarmaya çalıştığı hedeflere veya amaçlara atıfta bulunur ve saldırganın operasyonun farklı aşamalarındaki davranışlarıyla karakterize edilir. Bunlara ilk erişim, yürütme, kalıcılık, ayrıcalık yükseltme, savunma kaçınma, kimlik bilgisi erişimi, keşif, yanal hareket, toplama, komuta ve kontrol, sızdırma ve etki dahildir.
  Örnek: TA0002 (Saldırgan kötü amaçlı kod çalıştırmak istiyor).

6.2.Teknikler (Techniques)

- Teknikler, bir saldırganın hedeflerine nasıl ulaştığını açıklar, yani başarılı bir istismar başlatmak için kullanılan araçlar, teknolojiler, kod, istismarlar,

yardımcı programlar vb. Saldırının ayrıntılarının açıklandığı yer burasıdır. Örnek: T1059.001 (PowerShell - bir saldırıda PowerShell kullanımı)

6.3.Prosedürler (Procedures)

- Prosedürler, bir tekniğin nasıl gerçekleştirildiğine dair belirli örnekler sağlar. Bunlar, saldırgan grupları, ilişkili grupların açıklamaları, teknikler, sürümler, oluşturma ve değiştirme tarihleri ve yazılım hakkında bilgiler içerir.
  Örnek: APT19 (Tekniğin nasıl yürütüldüğüne dair detaylı bilgi)

7. TTP-Based Threat Hunting ve Detection Engineering

- TTP (Tactics, Techniques, and Procedures) tabanlı tehdit avcılığı (Threat Hunting) ve tespit mühendisliği (Detection Engineering), güvenlik ekiplerinin siber tehditleri daha etkili bir şekilde tespit edebilmesi ve önlem alabilmesi için kullanılan proaktif yaklaşımlardır. Bu metodoloji, saldırganların geçmişte kullandıkları davranış kalıplarını ve teknikleri analiz ederek gelecekteki saldırılara karşı erken önlem almayı hedefler.

7.1.TTP-Based Threat Hunting (Tehdit Avcılığı)

- Tehdit avcılığı, geleneksel güvenlik çözümlerinin (ör. antivirüs veya IDS/IPS) kaçırabileceği saldırıları tespit etmek amacıyla proaktif olarak gerçekleştirilen bir analiz sürecidir. TTP tabanlı tehdit avcılığı, belirli tehdit aktörlerinin davranış modellerine ve MITRE ATT&CK gibi çerçevelerde tanımlanan tekniklere dayanarak gerçekleştirilir.
  Bu yaklaşım, aşağıdaki süreçleri içerir:
  - **Davranışsal Analiz:** Tehdit aktörlerinin geçmişte uyguladığı saldırı teknikleri ve metodolojileri analiz edilir.
  - **Tehdit Hipotezleri Geliştirme:** Belirli bir ortamda gerçekleşebilecek potansiyel saldırı senaryoları belirlenir.
  - **Sorgular ve Algılama Mekanizmaları Oluşturma:** SIEM (Security Information and Event Management) veya EDR (Endpoint Detection and Response) gibi sistemler üzerinden belirli teknikleri tespit etmek için özel sorgular yazılır.
  - **Anomali Tespiti:** Şüpheli olaylar analiz edilerek olası tehditler belirlenir.

7.2.TTP-Based Detection Engineering (Tespit Mühendisliği)

- Tespit mühendisliği, tehdit avcılığı sürecinde elde edilen bilgiler doğrultusunda tehditleri daha etkili tespit edebilmek için güvenlik sistemlerinde yeni tespit kurallarının geliştirilmesini içerir. TTP tabanlı tespit mühendisliği, belirli saldırı tekniklerine karşı özel algılama yöntemleri geliştirmek için kullanılır.

Bu süreç şu adımları içerir:

- Tehdit Modelleme: Organizasyona yönelik potansiyel saldırı vektörleri belirlenir ve olası tehdit senaryoları oluşturulur.
- Algılama Kuralları Geliştirme: SIEM veya EDR platformlarında belirli TTP'lere dayalı tespit kuralları (YARA, Sigma, Suricata vb.) yazılır.
- False Positive ve False Negative Analizi: Algılama kurallarının etkinliği test edilir ve gereksiz alarmlar minimize edilir.
- Otomatik Müdahale Mekanizmaları: Tespit edilen saldırılara karşı otomatik aksiyon alınmasını sağlayan çözümler uygulanır.

8. 2022 Ukrayna Elektrik Saldırısı (C0034) Analizi

- 2022 yılında Ukrayna'nın elektrik altyapısına yönelik gerçekleştirilen saldırı (Kampanya Kodu: C0034), Sandworm Team adlı tehdit aktörü tarafından düzenlenmiştir. Bu saldırıda, saldırganlar çeşitli taktik ve teknikler kullanarak hedeflerine ulaşmışlardır.

  MITRE ATT&CK Framework'deki TID (Teknik Kimlik) değerleri belirtilmiştir:

  - **T1059 Serisi .001(Komut ve Komut Dosyası Yorumlayıcısı PowerShell):** Saldırganlar, TANKTRAP adlı bir PowerShell aracını kullanarak, Windows Grup İlkesi aracılığıyla bir wiper (silici) yazılımını yaymış ve çalıştırmışlardır.
  - **T1543 Serisi .002(Sistem İşlemi Oluşturun veya Değiştirin Systemd Hizmeti):** GOGETTER adlı kötü amaçlı yazılımın kalıcılığını sağlamak için Systemd yapılandırılmış ve "WantedBy=multi-user.target" ayarıyla sistem kullanıcı girişlerini kabul etmeye başladığında GOGETTER'ın çalışması sağlanmıştır.
  - **T1485 Serisi(Veri İmhası):** Saldırganlar, CaddyWiper adlı silici yazılımı kullanarak, hedef sistemlerde OT (Operasyonel Teknoloji) ile ilgili dosyaları, paylaşılan sürücüleri ve fiziksel disk bölümlerini silmişlerdir.
  - **T1484 Serisi .001(Etki Alanı veya Kiracı İlkesi Değişikliği: Grup İlkesi Değişikliği):** Grup İlkesi Nesneleri (GPO) kullanılarak, kötü amaçlı yazılımın dağıtımı ve çalıştırılması sağlanmıştır.
  - **T1570 Serisi(Yanal Takım Transferi):** CaddyWiper'ın msserver.exe adlı çalıştırılabilir dosyası, bir hazırlık sunucusundan yerel bir sabit diske kopyalanmış ve ardından dağıtımı gerçekleştirilmiştir.
  - **T1036 Serisi .004(Maskeli Balo: Maskeli Balo Görevi veya Hizmeti):** Systemd servis birimleri kullanılarak, GOGETTER kötü amaçlı yazılımı meşru veya meşru görünen servisler olarak gizlenmiştir.
  - **T1095 Serisi(Uygulama Dışı Katman Protokolü):** Komuta ve Kontrol (C2) iletişimleri, TLS tabanlı bir tünel içinde proxy'lenmiştir.
  - **T1572 Serisi(Protokol Tüneli Oluşturma):** GOGETTER tünelleme yazılımı kullanılarak, harici sunucularla "Yamux" adlı TLS tabanlı bir C2 kanalı oluşturulmuştur.

- **T1053 Serisi .005(Zamanlanmış Görev/İş: Zamanlanmış Görev):** Grup İlkesi Nesnesi (GPO) aracılığıyla Zamanlanmış Görevler kullanılarak, CaddyWiper belirli bir zamanda çalışacak şekilde ayarlanmıştır.
- **T1505 Serisi .003(Sunucu Yazılım Bileşeni: Web Kabuğu):** İnternete açık bir sunucuya Neo-REGEORG adlı web shell yerleştirilmiştir.
- **T0895 Serisi(Otomatik Çalıştırma Görüntüsü):** Mevcut hipervizör erişimi kullanılarak, a.iso adlı bir ISO imajı SCADA sunucusu çalıştıran sanal makineye bağlanmıştır. SCADA sunucusunun işletim sistemi, CD-ROM imajlarını otomatik çalıştıracak şekilde yapılandırıldığından, ISO imajındaki kötü amaçlı VBS betiği otomatik olarak çalıştırılmıştır.
- **T0807 Serisi(Komut satırı arayüzü):** Saldırgan ikili dosya aracılığıyla komutları yürütmek için MicroSCADA platformundaki SCIL-API'den yararlandı. "scilc.exe"
- **T0853 Serisi(Komut dosyası):** Saldırıyı yürütmek için bir Visual Basic komut dosyası kullanır ve ardından MicroSCADA komutunu yürütür. "lun.vbsn.batscilc.exe"
- **T0894 Serisi(Sistem İkili Proxy Yürütme):** Saldırgan, düşman tarafından tanımlanan bir dosyada belirtilen önceden tanımlanmış bir SCADA talimatlarının listesini göndermek için bir MicroSCADA uygulama ikili dosyası yürüttü. Yürütülen komut, uzak trafo merkezlerine yetkisiz komut mesajları göndermek için SCADA yazılımını kullanır. "scilc.exes1.txtC:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt"
- **T0855 Serisi(Yetkisiz Komut Mesajı):** Saldırganlar, trafo merkezi cihazlarına yetkisiz komutların gönderilmesi de dahil olmak üzere bir dizi SCADA talimatını belirtmek için MicroSCADA SCIL-API'yi kullandı.

9. Saldırı Senaryosu

- Hastanenin veritabanına sızarak hasta bilgilerini ele geçirmek ve bu bilgileri kullanarak hastaları dolandırmak.
    1. Keşif (Reconnaissance):
        - T1595.002 - Aktif Tarama: Güvenlik Açığı Taraması
          Hedef hastanenin internete açık veritabanlarını Shodan, Censys, ZoomEye gibi araçlarla tarar.
          Özellikle MongoDB, Elasticsearch, MySQL veya PostgreSQL gibi açık portlara sahip sistemleri arar.

        - T1598.002 - Bilgi için Sahtecilik: Spearphishing Eki
          Hastane çalışanlarının LinkedIn, sosyal medya veya sızdırılmış veri setlerinden e-posta adreslerini ve şifrelerini toplar.
          Dark Web'de satılan e-posta şifreleriyle, çalışan hesaplarını denemeye başlar.

2. İlk Erişim (Initial Access):
    - T1078.003 - Geçerli Hesaplar: Yerel Hesaplar
      Sızdırılmış veya tahmin edilen bir yönetici e-postası ile hastanenin VPN veya RDP sistemine giriş yapar.
      Çalınan giriş bilgilerini Hastane Bilgi Yönetim Sistemi (HBYS) veya hasta kayıt sistemlerine erişmek için kullanır.

    - T1566.001 - Kimlik Avı: Spearphishing Eki
      Hastane personeline, sahte bir tıbbi cihaz faturası içeren e-posta gönderir.
      Ek olarak, hastane muhasebesine yönelik sahte bir ödeme talebi belgesi göndererek içeride hareket alanı yaratır.

3. Yetki Yükseltme (Privilege Escalation):
    - T1068 - Ayrıcalık Yükseltmesi İçin Sömürü
      Hastanenin kullandığı HBYS veya hasta kayıt yazılımında eski ve yaması yapılmamış bir güvenlik açığı bulunursa bunu kullanarak veritabanı yönetici yetkileri elde eder.

    - T1055 - Proses Enjeksiyonu
      Hastanenin veritabanı sunucusuna veya HBYS sistemine erişim sağlandıktan sonra, saldırgan, sistemde çalışan bir güvenlik servisine (örneğin Antivirüs veya bir Windows hizmetine) zararlı kod enjekte eder.

4. Yan Hareket (Lateral Movement):
    - T1021.001 - Uzaktan Hizmetler: Uzak Masaüstü Protokolü
      Elde edilen yönetici hesabı ile diğer kritik sunuculara bağlanılır.

    - T1072 - Yazılım Dağıtım Araçlarını Kötüye Kullanma
      Hastanenin SCCM (System Center Configuration Manager) veya benzeri bir merkezi yönetim aracını kullanarak zararlı bir yük dağıtılır.
      Yönetici haklarıyla çalışan bir sistemden, tüm istemcilere kötü amaçlı yazılım bulaştırılır.

5. Savunmadan Kaçınma (Defense Evasion)
    - T1036.004 - Maskeleme: Maskeli Görev veya Hizmet
      Kendi zararlı kodunu, hastanenin HBYS yazılımına sahte bir DLL dosyası olarak enjekte eder.

    - T1202 - Dolaylı Komut Yürütme
      Saldırganlar, komut satırı yorumlayıcılarının kullanımını sınırlayan güvenlik kısıtlamalarını aşmak için komut yürütülmesine izin veren yardımcı programları kötüye kullanabilir.

6. Etki (Impact)
    - T1486 - Etki İçin Şifrelenmiş Veriler
      Veritabanı şifrelenerek erişilemez hale getirilir ve hastaneden belirli bir miktar fidye talep edilir.

    - T1531 - Hesap Erişiminin Kaldırılması
      Saldırganlar, meşru kullanıcılar tarafından kullanılan hesaplara erişimi engelleyerek sistem ve ağ kaynaklarının kullanılabilirliğini kesintiye uğratabilir. Hesaplara erişimi kaldırmak için hesaplar silinebilir, kilitlenebilir veya manipüle edilebilir.

7. Sosyal Mühendislik ile Hastaları Dolandırma
    - T1583.003 - Sahte Web Siteleri ile Dolandırıcılık
      Sahte bir özel klinik veya hayır kurumu web sitesi oluşturulur. Hastalara, "Sizin için özel bir tedavi programı oluşturduk, ödeme yaparak başlayabilirsiniz." şeklinde sahte e-postalar gönderilir.

    - T1566.002 - Hastalara Kimlik Avı Mesajı Gönderme
      Hastalara sahte SMS veya WhatsApp mesajları gönderilir: "Özel bir kanser tedavi programına ücretsiz kayıtlısınız, onay için şu linke tıklayın."
      Bağlantıya tıklayan kişilerden kredi kartı bilgileri veya kişisel bilgileri çalınır.

10. Sonuç

- MITRE ATT&CK çerçevesi, siber güvenlik dünyasında saldırganların kullandığı taktik ve teknikleri sistematik bir şekilde analiz etmek, tehdit avcılığı yapmak ve etkili savunma stratejileri oluşturmak için kritik bir kaynak sağlamaktadır. Kurumlar, bu framework'ü kullanarak tehdit aktörlerinin davranışlarını daha iyi anlayabilir, güvenlik açıklarını tespit edebilir ve proaktif savunma mekanizmaları geliştirebilirler.Hastalara sahte SMS veya WhatsApp mesajları gönderilir: "Özel bir kanser tedavi programına ücretsiz kayıtlısınız, onay için şu linke tıklayın." Bağlantıya tıklayan kişilerden kredi kartı bilgileri veya kişisel bilgileri çalınır.
- TTP tabanlı tehdit avcılığı ve tespit mühendisliği yaklaşımları sayesinde, saldırganların tekniklerine karşı özel algılama kuralları ve savunma stratejileri geliştirilebilir. Bu, siber tehditlere karşı erken uyarı ve müdahale imkanı sağlayarak güvenlik operasyonlarının daha etkili hale gelmesine katkıda bulunur.
- Sonuç olarak, siber güvenlik ekiplerinin MITRE ATT&CK framework'ünü etkin bir şekilde kullanarak tehdit modelleme, tehdit avcılığı ve tespit mühendisliği süreçlerini geliştirmeleri gerekmektedir. Bu sayede, hem mevcut güvenlik açıkları belirlenebilir hem de gelecekteki saldırılar önceden tahmin edilerek riskler minimize edilebilir.

Kaynakça

https://attack.mitre.org/

https://www.ibm.com/think/topics/mitre-attack#Overview

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

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

ATT&CK® Algılama Mühendisliği Eğitimi ve Sertifikasyonu - MAD20

2022 Ukraine Electric Power Attack, Campaign C0034 | MITRE ATT&CK®

ATT&CK Eğitimi | GÖNYE ATT&CK®