STM Cyber


NİSAN-HAZİRAN 2024

# SİBER TEHDİT DURUM RAPORU

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi


SORUMSUZLUK VE FİKRİ MÜLKİYET HAKKI BEYANI

İşbu eserde/internet sitesinde yer alan veriler/bilgiler ticari amaçlı olmayıp tamamen kamuyu bilgilendirmek amacıyla yayımlanan içeriklerdir. Bu eser/internet sitesinde bulunan veriler/bilgiler tavsiye, reklam ya da iş geliştirme amacına yönelik değildir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. işbu eserde/internet sitesinde sunulan verilerin/bilgilerin içeriği, güncelliği ya da doğruluğu konusunda herhangi bir taahhüde girmemekte, kullanıcı veya üçüncü kişilerin bu eserde/internet sitesinde yer alan verilere/bilgilere dayanarak gerçekleştirecekleri eylemlerden ötürü sorumluluk kabul etmemektedir.


# İÇİNDEKİLER

Sorumsuzluk ve Fikri Mülkiyet Hakkı Beyanı ..... 2
**İÇİNDEKİLER** ..... 3
**ŞEKİLLER** ..... 4
**GİRİŞ** ..... 5
**TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK** ..... 5
**1. Deniz Platformlarında Siber Güvenlik** ..... 5
**2. Polyfill.io Tedarik Zinciri Saldırısı** ..... 6
Benzer Geçmiş Olaylar ..... 6
Örnek Kod: Polyfill.io Kullanımı ..... 7
**3. QR Kod Tabanlı Saldırılar ve Güvenlik Önlemleri** ..... 7
QR Kod Nedir? ..... 7
QR Kodlarının Güvenlik Tehditleri ..... 7
Alınabilecek Güvenlik Önlemleri ..... 7
**4. Yeni Saldırı Tekniği "Sleepy Pickle" Makine Öğrenmesi Modellerini Hedef Alıyor** ..... 8
Makine Ögrenmesi Modellerinde Serialization ve Deserialization ..... 8
Saldırı Süreci ..... 8
Saldırı Sonrası ..... 8
Sleepy Pickle'dan Sticky Pickle'a ..... 8
Saldırıdan Sakınma Yolları ..... 8
Sonuç ..... 9
**5. Memory Tagging Extension (MTE) - Tiktag Saldırıları** ..... 9
Memory Tagging Extension (MTE) Nedir ve Neden Kullanılır ..... 9
Branch Prediction ..... 9
Tiktag-v1 Nedir, Nasıl Çalışır ..... 9
Tiktag-v2 Nedir, Nasıl Çalışır ..... 9
Etkilenen Ürünler Nelerdir ..... 10
**DÖNEM KONUSU** ..... 10
**6. Silah Sistemlerinin Siber Dayanıklılığını Artırmak** ..... 10
**7. Honeypot Verileri** ..... 12
**KAYNAKÇA** ..... 15

# ŞEKİLLER

Şekil 1. Emsal Bir Silah Sistemi Bileşenleri ..... 10
Şekil 2. Silah Sistemleri Siber Güvenliği için Uygulanabilecek Kontrol Gruplar ..... 12
Şekil 3. Gelen saldırıların ülkelere göre dağılımı ..... 13
Şekil 4: Parola etiket bulutu ..... 14
Şekil 5: Kullanıcı adı etiket bulutu ..... 14

# GİRİŞ

2024 yılının ikinci çeyreğinde Siber Güvenlik Müdürlüğü tarafından hazırlanan raporumuzda yine birbirinden ilginç konularla karşınızdayız. İlk olarak, özellikle ülkemizin önemli bir konuma sahip olduğu denizcilik sektöründeki deniz platformlarının siber güvenliği üzerinde duruyoruz.

Ardından, eski tarayıcılar için modern JavaScript desteği sağlayan ve popüler bir açık kaynak kütüphane olan Polfill.io'ya Haziran ayında yerleştirilen kötü niyetli bir kod sayesinde yüz binlerce web sitesinin hack'lenmesi olayını ve bu saldırının detaylarını açıklıyoruz.

Gündelik hayatta insanlara kolaylık sağlayan QR kod teknolojisinin kullanımının özellikle pandemi sonrası önemli derecede yaygınlaşmasından dolayı, QR kod tabanlı saldırıların sayısı hızla artmıştır. Tam da bu sebeple "QR Kod Tabanlı Saldırılar ve Güvenlik Önlemleri" başlığı altında bu saldırıları ve saldırılara dair alınabilecek önlemleri paylaşıyoruz.

Hemen sonrasında, makine öğrenmesi modellerinde kullanılan Pickle formatının, modelleri kullanan kişilerin bilgisayarlarında nasıl rasgele kod yürütme saldırılarına sebebiyet verdiğini inceliyoruz.

Tiktag-v1 ve Tiktag-v2, ARM işlemcilerdeki MTE özelliğini atlatmak için spekülatif yürütmeyi manipüle eden saldırı yöntemleridir. Bu saldırıların, mobil cihazlar, router'lar ve gömülü sistemler gibi ARM işlemcili ürünleri nasıl etkileyebileceğini açıklıyoruz.

Bu çeyrekte dönem konusu olarak belirlediğimiz başlıkta ise silah sistemlerinin siber dayanıklılığını artırma konusunu sizlerle paylaşıyoruz.

Son olarak her raporumuzda güncellediğimiz honeypot verilerimize yer ayırdık.

Bu rapor, bilişim dünyasındaki güvenlik tehditlerini ve koruma stratejilerini anlamak isteyen herkes için önemli bir kaynak olacak. Güvenlik bilincinizi artırmak ve siber tehditlere karşı daha iyi hazırlıklı olmanız için bu raporu incelemenizi tavsiye ederiz. Güvende kalın!

# TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

## 1. Deniz Platformlarında Siber Güvenlik

Denizcilik sektörü, dünya ticaretinin yaklaşık yüzde 90'ını taşımakla küresel ekonominin bel kemiğini oluşturmaktadır[1]. Yüz milyonlarca ton mal, her yıl deniz yoluyla taşınarak dünya pazarlarına ulaşmakta ve bu süreçte denizcilik sektörü, ülkeler arası ticaretin, enerji arzının ve global tedarik zincirinin sorunsuz işleyişinde merkezi bir rol oynamaktadır. Deniz platformları yük taşımacılığının yanı sıra milli güvenlik ve insan taşımacılığı için de büyük önem arz etmektedir.

Dijital dönüşümün getirdiği yenilikler, gemi otomasyon sistemlerinden, yük yönetim yazılımlarına ve navigasyon cihazlarına kadar geniş bir yelpazede karşımıza çıkmaktadır. Gemiler, üzerinde IT ve OT sistemleri barındıran ve bu sistemlere doğrudan bağımlı mega yapılar hâline gelmiştir. Bu teknolojiler, operasyonel verimliliği artırmakta, maliyetleri düşürmekte ve güvenliği sağlamaktadır. Ancak, bu dijitalleşme süreci, siber güvenlik tehditlerinin artmasına da imkân tanımıştır. Gemi platformlarına düzenlenen siber saldırılar, büyük finansal kayıplar getirmenin yanı sıra devletlerin milli güvenliklerini tehdit eden bir unsura dönüşmüştür. Sektörde geçerli bazı tehditler aşağıdaki gibi ele alınabilir:

- Gemi Sistemlerine Yönelik Saldırılar
  - Otomasyon Sistemlerine Müdahale
  - Navigasyon Sistemlerine Müdahale
  - İletişim Sistemlerine Müdahale
- Liman ve Lojistik Sistemlerine Yönelik Saldırılar
  - Liman Yönetim Sistemlerine Müdahale
  - Tedarik Zinciri ve Lojistik Ağına Müdahale
- Veri İhlalleri ve Casusluk
- Zararlı Yazılımlar
- İç Tehditler
  - Çalışan Kaynaklı Tehditler
  - Eğitim Eksiklikleri

Elimizde en yakın kara parçasından millerce uzakta, güvenlik gereksinimleri yüksek, yer yer kritik milli görevler üstlenen bir mega yapı var. Peki bu mega yapı olası siber saldırılardan nasıl korunacak? Açıktır ki bu denli kritik bir unsurda sistematik bir savunmaya sahip olmak elzemdir.

Sistematik güvenlik yaklaşımı için faydalı olabilecek bazı güvenlik çerçeveleri aşağıda belirtilmiştir. İlk iki sırada bulunan ISO27001 ve NIST Cybersecurity Framework (CSF) birçok denizcilik güvenlik standardında ana çerçeveyi oluşturmaktadır. Diğer standart ve uygulamalar da bu iki kıymetli çalışmanın üzerine yerleştirilmiştir.

- NIST Cybersecurity Framework (CSF)[2]
- ISO27001: Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems - Requirements[3]
- BIMCO: The Guidelines on Cyber Security Onboard Ships[4]

- IACS Rec 166: Recommendation on Cyber Resilience[5]
- IACS E26: Cyber Resilience of Ships[6]
- IACS E27: Cyber Resilience of On-Board Systems And Equipment[7]
- IMO "Guidelines on Maritime Cyber Risk Management"[8]
- Cyber Safe for Marine[9]
- IACS E22: Computer-based systems[10]

Siber güvenlik önlemlerinin önemli bölümü gemi henüz tasarım aşamasındayken planlanmaya başlanmalıdır. Olası tedbirler belirlenirken üretim, devreye alma ve operasyon sürecinde yapılması gerekenlerin ayrı ayrı ele alınması güvenliği bir üst seviyeye çıkartır. Temel tedbirlere genel bir bakış aşağıdaki gibi ele alınabilir.

**Varlık Yönetimi Sürecinin Yürütülmesi**: Platform üzerinde bulunan bütün enformasyon varlığı envanterinin güncel olarak tutulması gerekir. Bu envanter mobil ve taşınabilir cihazları da kapsamalıdır. Envanter tutulurken ilgili varlığın sahibi, sorumlusu, kritikliği gibi konular ele alınmalıdır. Tasarım aşamasında tüm detayların ortaya konamayacağı aşikârdır, o nedenle sürekli güncelleme yapmak ve gözden geçirmek gerekir.

**Ağ Yönetimi ve Güvenliği**: Ağ segmentasyonları mümkün olduğunca granüler yapılmalı ve ağlar arasında etkileşime sadece gerektiği kadar yer verilmelidir. Segmente edilmiş ağa sadece yetkili kişiler ve yetkili cihazlar erişebilmelidir. Ağ güvenliğinin sağlanabilmesi için idari (politika/prosedür), fiziksel ve teknik güvenlik tedbirleri alınmalıdır. Ağ içinde ve ağlar arasında olan hareketler izlenmeli, anomaliler tespit edilip müdahale edilmelidir.

**Yazılım Güvenliği**: Geliştirilebilecek, tedarik edilebilecek ve dışarıdan gelebilecek kötücül yazılımlar için tedbirler alınmalıdır. Geliştirmede güvenli yazılım geliştirme prensipleri uygulanmalı ve metodolojik yaklaşımlar kullanılmalıdır. NIST "Secure Software Development Framework (SSDF)"[11] ve OWASP "Application Security Verification Standard"[12] kullanılması tavsiye edilen başlıca çerçevelerdir. Ayrıca tedarik edilen yazılımların fonksiyon ve güvenlik testleri uygun bir şekilde yapılmalıdır. Yazılım güvenliği ile ilgili bir diğer husus ise zararlı yazılımlardır. Komponentlerin zararlı yazılımlardan korunabilmesi için antimalware sistemleri etkin bir şekilde kullanılmalıdır.

**Erişim Güvenliğinin Sağlanması:** Yazılımların ve kişilerin etkileşiminin granüler olacak şekilde sınırlandırılması, izlenmesi ve kontrol edilmesi sağlanmalıdır. Uzaktan erişim ile ilgili kontrol ve kısıtlar uygulanmalıdır.

**Olay Müdahale Yönetiminin Yapılması**: Unutmamak gerekir ki, gemi platformu IT ve OT ürünleri barındıran bir sistemdir. Personel buna göre eğitim almalıdır. Yaşanabilecek her senaryo için yönergeler hazırlanmalı, rol sorumlulukları belirlenmeli ve belirli aralıklar ile ilgili senaryolar üzerinden tatbikatlar gerçekleştirilmelidir.

**Veri Yedekleme ve Geri Döndürme Süreçlerinin Yürütülmesi:** Planlamalar ve testler yapılmalıdır. Planlamalar yapılırken hangi verinin ne sıklıkta yedeklenmesi gerekliliği, yasal yükümlülükler kati suretle ele alınmalıdır. Yedekten dönme testleri düzenli olarak yapılmalıdır.

**Risk Yönetimi:** Risk yönetim süreci işletilmelidir. Bu süreç için birden çok seviyede kalıtsal olacak şekilde risk analizi yapmak sağlıklı olacaktır. Örneğin sistemlere yönelik risk analizi akabinde bileşenler özelinde bir risk analizi yapmak sağlıklı olacaktır.

**Politika, Prosedür ve Kılavuzlar:** Siber güvenlik ile ilgili tüm süreçler sistematik olarak yürütülmelidir. Sistematik yürütmenin temel unsurlarından biri yazılı tanımlamadır. Yukarıda belirtilen temel unsurlar "nasıl?" sorusuna cevap verecek şekilde yazılı hâle getirilmelidir.

Denizcilik sektörü, küresel ekonomide, insan taşımacılığında ve askeri alanda kritik bir öneme sahiptir. Teknolojinin getirdiği fırsatları en iyi şekilde değerlendirebilmek için, siber güvenlik tehditlerine karşı proaktif önlemler almak ve güvenlik stratejilerini sürekli güncellemek gerekir. Denizcilik sektörünün dijital dönüşümü ancak böyle güvenli bir şekilde sürdürülebilir.

## 2. Polyfill.io Tedarik Zinciri Saldırısı

Polyfill.io, eski tarayıcılar için modern JavaScript desteği eklemeyi sağlayan popüler bir açık kaynak kütüphanesidir. Geliştiricilere büyük kolaylık sağlayan bu kütüphane, dünya genelinde milyonlarca web sitesinde kullanılmaktadır. Haziran 2024'te, popüler bir JavaScript polyfill kaynak koduna kötü amaçlı kod yerleştirildiği duyurulmuştur. Bu saldırı, aralarında Intuit gibi halka açık şirketler de bulunan yüz binlerce web sitesini etkilemiştir[13].

### Benzer Geçmiş Olaylar

Bu saldırı, XZ backdoor vakası ile benzerlik taşımaktadır. XZ Utils projesine sızan bir saldırgan, projeye sofistike bir arka kapı yerleştirerek sistemleri geniş çapta tehlikeye atmıştır. Bu durum, üçüncü taraf bileşenlerin sürekli izlenmesinin ve güvenlik kontrollerinin önemini vurgulamaktadır[14].

### Önlemler ve Öneriler

Bu tür saldırılara karşı alınabilecek bazı önlemler şunlardır[15]:

a. **Yerel Barındırma:** Kritik kütüphaneleri yerel olarak barındırmak, uzaktan kod manipülasyonunu engeller. Örnek:

```
<!-- Uzaktan yüklemek yerine yerel barındırma -->
<script src="/local/path/to/polyfill.min.js"></script>
```

b. **Sürekli İzleme:** Üçüncü taraf bağımlılıkları sürekli olarak izleyen araçlar kullanın. Reflectiz gibi hizmetler,

sürekli tehdit yönetimi sağlayabilir ve potansiyel güvenlik açıklarına karşı uyarı verebilir.

c. **Kod İncelemeleri ve Denetimler:** Tüm üçüncü taraf bileşenlerin düzenli kod incelemelerini ve denetimlerini gerçekleştirin. Örnek:

```
shell

# npm paketlerini kontrol etmek için bir güvenlik denetimi

npm audit
```

d. **Alt Kaynak Bütünlüğü (Subresource Integrity - SRI):** SRI, bir CDN'den sağlanan içeriğin değiştirilmediğini garanti edebilir. Beklenen bir sürüme/hasha sabitlenmiş ve denetlenen içeriğin sağlandığını garanti eder.

e. **İçerik Güvenliği Politikası (Content Security Policy - CSP):** Güçlü bir CSP'nin uygulanması, komut dosyalarının yüklenebileceği kaynakları kısıtlar. Bu, kötü amaçlı komut dosyalarının çalışmasını engelleyebilir.

f. **Düzenli Güncellemeler:** Tüm kütüphanelerin ve bağımlılıkların güncel tutulması. Birçok saldırı, daha sonraki sürümlerde yamalanmış bilinen güvenlik açıklarını kullanır.

#### Örnek Kod: Polyfill.io Kullanımı

Polyfill.io'yu güvenli bir şekilde kullanmak için aşağıdaki örnekler göz önünde bulundurulabilir:

```
<!-- Uzak sunucu yerine yerel barındırma -->
<script src="/local/path/to/polyfill.min.js"></script>

<!-- Alternatif olarak, güvenilir bir CDN'den yükleme -->
<script src="https://cdn.jsdelivr.net/npm/polyfill@latest"></script>
```

Polyfill.io saldırısı, yazılım geliştirme tedarik zincirindeki risklerin yönetiminin önemini vurgulamaktadır. Geliştiricilerin ve kuruluşların, üçüncü taraf bileşenlerin güvenliğini sağlamak için sürekli izleme ve güvenlik denetimleri yapması kritik öneme sahiptir. Bu önlemler, benzer saldırıların önlenmesine yardımcı olabilir ve dijital ekosistemin güvenliğini artırabilir.

Bu saldırı, yazılım tedarik zinciri siber güvenliğinin önemini ve kritikliğini bir kere daha ortaya koymaktadır.

## 3. QR Kod Tabanlı Saldırılar ve Güvenlik Önlemleri

#### QR Kod Nedir?

QR kod (Quick Response Code), dijital cihazlar tarafından anında okunmak ve yorumlanmak üzere tasarlanmış bir barkod türüdür. Bu kodlar, web sitesi açmak, dosya indirmek, kişi eklemek, Wi-Fi ağına bağlanmak ve ödeme yapmak gibi çeşitli işlemleri gerçekleştirebilir. Ancak, bu kullanışlılıkları aynı zamanda güvenlik risklerini de beraberinde getirmektedir.

#### QR Kodlarının Güvenlik Tehditleri

a. **Zararlı Yazılım Saldırıları:** Dolandırıcılar sahte QR kodları oluşturabilir ve bunları meşru görünen yerlere yerleştirerek, cihazınıza kötü amaçlı yazılım bulaştırabilirler. Bu tür QR kodlarının taranması, cihazınızın sahte bir web sitesinden bir uygulama indirmesini tetikleyebilir.

b. **Kimlik Avı Saldırıları (QRishing):** QR kodları, sahte bankacılık veya alışveriş sitelerine yönlendirebilir ve kullanıcı bilgilerini çalabilir. QRishing saldırıları, QR kodları tarandığında kullanıcıları kimlik avı sitelerine yönlendirir. Check Point Harmony Email ekibi, Ağustos ve Eylül 2023 arasında QR kod kimlik avı saldırılarında yüzde 587 oranında artış olduğunu raporlamıştır.[16]

c. **Konum Bilgisi Açığı:** QR kodları, tarandığında yaklaşık konumunuzu belirleyip üçüncü şahıslara gönderebilir.

d. **Kişisel Bilgi Sızıntısı:** QR kodları, telefon numaranız gibi kişisel bilgileri üçüncü şahıslara iletebilir. Bu, telefon numaranızın kimliğinizle ilgili diğer bilgilerle birleştirilmesine yol açabilir.

e. **Cihaz İşlevlerini Tetikleme:** QR kodları, cihazınızda çeşitli işlemleri (Wi-Fi ağına bağlanma, SMS gönderme vb.) tetikleyebilir.

f. **Finansal Dolandırıcılık:** Saldırganlar, ödeme yapılacak QR kodlarını manipüle ederek paranın kendi hesaplarına yönlendirilmesini sağlayabilir. QR kodların Quishing ve QRLJacking yöntemleri ile istismar edildiği belirtilmektedir[17]:

**QRLJacking**, QR kodları kullanılarak gerçekleştirilen bir tür oturum ele geçirme saldırısıdır. Bu saldırıda, saldırganlar, kullanıcıların oturum açma işlemleri sırasında kullandıkları QR kodları manipüle eder. Örneğin, bir kullanıcı bir web sitesinde QR kodu tarayarak oturum açtığında, saldırgan, kullanıcının kimlik bilgilerini ele geçirir ve oturumunu kontrol altına alır. Bu saldırı türü, özellikle QR kodları ile oturum açma (login) veya doğrulama işlemlerinin kullanıldığı senaryolarda yaygındır.

#### Alınabilecek Güvenlik Önlemleri

a. **Güvenilmeyen QR Kodlarından Kaçınmak:** Rasgele web sitelerinden veya sosyal medyadaki resmi olmayan sayfalardan gelen QR kodlarını taramayın[18].

b. **Antivirüs Yazılımı Kullanmak:** Telefonunuza antivirüs yazılımı yükleyerek kimlik avı sitelerinden ve kötü amaçlı yazılımlardan korunabilirsiniz.

c. **İki Faktörlü Kimlik Doğrulama (2FA):** Tüm hesaplarınızda 2FA'yı etkinleştirerek ek bir güvenlik katmanı sağlayın.

d. **Canlı Konumu Kapalı Tutmak:** Cihazınızın konumunu kapalı tutarak konum bilgilerinizin üçüncü şahıslar tarafından ele geçirilmesini önleyin.

e. **Cihazı Güncellemek:** Cihazlarınızı ve yazılımlarınızı en son güvenlik yamalarıyla güncel tutarak potansiyel tehditlerden korunabilirsiniz.

f. **OCR Tabanlı Güvenlik Önlemleri:** Güvenlik çözümlerinde Optik Karakter Tanıma (OCR) özelliğini kullanarak, QR kodlarının içeriğini URL'ye çevirebilir ve bu URL'yi analiz ederek kötü amaçlı bağlantıları tespit edebilirsiniz.

QR kodlar, hayatımızı kolaylaştıran kullanışlı araçlar olmalarına rağmen, siber güvenlik açısından dikkatli kullanılmaları gerekir. Güvenilmez kaynaklardan gelen QR kodlarını taramaktan kaçınmak, güvenlik yazılımları kullanmak ve cihazları güncel tutmak gibi önlemler, QR kodlarının yaratabileceği güvenlik tehditlerini minimize etmeye yardımcı olacaktır. Quishing saldırılarının artışı, kullanıcıların daha dikkatli ve bilinçli olmaları gerektiğini göstermektedir. Siber güvenlik uzmanlarının bu tehditlerle başa çıkmak için OCR tabanlı güvenlik çözümleri ve diğer ileri teknolojileri kullanmaları önemlidir.

## 4. Yeni Saldırı Tekniği "Sleepy Pickle" Makine Öğrenmesi Modellerini Hedef Alıyor

Trail of Bits şirketinin siber güvenlik araştırmacıları, makine öğrenmesi modellerine sızarak veri çalabilen ve yapay zekânın çıktılarını manipüle edebilen Sleepy Pickle adlı bir saldırı tekniğini duyurdu. Bu saldırı tekniği, bilgisayarı hedeflemek yerine doğrudan makine öğrenmesi modelini hedef almaktadır.

### Makine Öğrenmesi Modellerinde Serialization ve Deserialization

Bir makine öğrenmesi modelinin, istenilen gereksinimlere uygun olarak seçilip eğitilmesinden sonra, diske kaydedilmesi işlemine serialization denir. Bu saldırı türünde kullanılan serialization formatı Pickle'dır. Pickle, python objelerinin serialization ve deserialization işlemleri için kullanılan bir formattır. Bir modeli Pickle ile serialization yaptıktan sonra çıktı olarak ".pkl" uzantılı bir dosya elde edilir. Bu ".pkl" uzantılı dosya, modelin istenilen sistemlere taşınmasına olanak sağlar. Ancak Pickle, deserialization sırasında rasgele kod yürütme olanağı sağlar. Bu durum saldırıya olanak veren bir zayıflıktır. Modele serialization yapıldıktan sonra, model diskten çekilip kullanıma hazır veya geri eğitilebilir hale getirilir [19].

### Saldırı Süreci

Saldırıyı başlatmak için Flicking adlı açık kaynak aracı kullanılmaktadır[20]. Flicking, zararlı Pickle dosyaları oluşturmayı, tersine mühendislik yapmayı ve analiz etmeyi sağlayan bir araçtır. Flicking kullanılarak, hedefin eğittiği makine öğrenmesi modeline saldırganın yazdığı zararlı Python kodu enjekte edilir ve çıktı olarak ".pkl" dosyası oluşturulur. Saldırının bir sonraki aşaması ise bu zararlı yazılım enjekte edilmiş modelin hedefe iletilmesidir. Bunun için saldırganlar, sahte e-posta yoluyla kullanıcıları kandırıp kişisel bilgilerini çalmaya çalıştıkları oltalama saldırısını veya iletişim kurulan iki taraf arasına girip verileri izlemesine ve manipüle etmesine olanak tanıyan aradaki adam saldırısını kullanmaktadır. Kurban, kendisine ulaşan maillerden bu zararlı modeli indirip deserialize ederse, saldırganın gönderdiği zararlı Python kodunu da çalıştırmış olur[21]. Model, içine enjekte edilmiş zararlı yazılıma bağlı olarak çok daha büyük bir alan kapladığı için zararlı yazılımın tespit edilip analiz edilmesi, klasik bir zararlı yazılımla yapılan saldırılara kıyasla çok daha zor olacaktır. Ayrıca, deserialization işlemi dinamik bir olay olduğundan yazılan zararlı Python kodu diskte statik analiz yapılarak tespit edilemez[22].

### Saldırı Sonrası

Zararlı yazılım enjekte edilmiş bir model çalıştırıldıktan sonra, modelin davranışları saldırgan tarafından manipüle edilebilmekte ve modele bir arka kapı (backdoor) yerleştirilebilmektedir. Bunun yanı sıra, saldırganlar, model eğitiminde kullanılan gizli ve önemli bilgilere de erişim sağlayabilmektedir[23].

### Sleepy Pickle'dan Sticky Pickle'a

Trail of Bits şirketinden araştırmacılara göre, bu saldırı türünün tek ürünü Sleepy Pickle değil. Sleepy Pickle'in bir varyantı olan Sticky Pickle, saldırıyı daha da tehlikeli hale getirerek uzun süre sistemde tespit edilmeden kalabilen bir saldırıya evrimleşmektedir. Sticky Pickle, iki yeni özellik içermektedir. İlk özellik kendi kendini kopyalama mekanizmasıdır. Bu özelliğe sahip zararlı yazılım, kendini etkilenen modelin sonraki sürümlerine de kopyalayarak varlığını devam ettirebilmekte ve bu sayede saldırı, kullanıcı yeni bir model kullanıp yeni bir pickle dosyası oluştursa bile kalıcı hâle gelmektedir. Diğer bir önemli özellik ise Sticky Pickle'ın, obfuscation yöntemlerini kullanarak kendini dosya tarayıcıları tarafından tespit edilemez hâle getirmesidir. Bu yeni özellikler sayesinde hedef ne kadar yeni bir model kullansa ve yeni pickle dosyası oluştursa da saldırı kalıcılaşmaktadır [24].

### Saldırıdan Sakınma Yolları

Bu tür risklerden kaçınmak için kullanıcıların makine öğrenmesi modellerini yalnızca güvenilir kaynaklardan ve kuruluşlardan indirmeleri ve modellerin bütünlüğünü doğrulamaları yardımcı olacaktır. Pickle yerine SafeTensor gibi güvenli dosya formatları kullanmak ek bir güvenlik katmanı sağlar. Güvenilir olmayan durumlarda, modeli izole bir sandbox ortamında test etmek doğru bir seçenektir[25].

### Sonuç

Sonuç olarak, yeni bir saldırı türü olan Sleepy Pickle, ML modellerine zararlı yazılım enjekte edilerek oluşturulan ".pkl" uzantılı dosyaların hedef bilgisayarlarda çalıştırılmasıyla gerçekleşmektedir. Bu olası saldırılardan etkilenmemek için modelleri güvenilir kaynaklardan elde etmek ve bu tür modelleri öncelikle sandbox ortamlarında açmak iyi bir seçenek olacaktır [26].

## 5. Memory Tagging Extension (MTE) - Tiktag Saldırıları

### Memory Tagging Extension (MTE) Nedir ve Neden Kullanılır

Bellek Etiketleme Uzantısı (MTE), Armv8.5-a ve sonrasında çıkan mimarilerde kullanılan bir donanım özelliğidir. Belleği belirli büyüklükteki bölgelere ayırır, her bellek bölgesine ve bu bölgeyi işaret eden işaretçilere (pointer) bir etiket atar. Böylece yazılımın güvenlik ve istikrarını geliştirir.

MTE özelliğinin kullanılma sebepleri başlıca şunlardır:

- **Bellek Hatalarını Tespit Etme:** MTE, serbest bırakılan belleğin kullanılması (use-after-free) ya da bellek taşması gibi bellekle ilgili hataları yakalayabilir. Bu hatalar program ve donanımın çökmesine, güvenlik açıklarına ve öngörülemeyen program davranışlarına yol açabilir.
- **Daha Güvenli Geliştirme:** MTE, geliştiricilerin bellek hatalarını test sırasında ve hatta kullanım sırasında bile daha kolay tespit etmesine ve düzeltmesine yardımcı olur. Böylece daha güvenli ve sağlam yapılı uygulamalar geliştirilmesine yardımcı olur.
- **Geliştirilmiş Güvenlik:** MTE, bellek zafiyetlerinin önüne geçerek saldırganların yazılımda bulunan zayıflıkları kullanmasını zorlaştırır [27].

### Branch Prediction

İşlemci mimarisinde kullanılan bir teknik olan dallanma öngörüsü (branch prediction), bir dallanma işleminin (if-else gibi) sonucunu tahmin etmeye çalışır ve bu sayede işlemcinin hız kazanmasını sağlar.

Yürütme sırasında bir dallanma işlemi yürütüleceği zaman bellek öngörüsü ile işlemin sonucu tahmin edilir ve tahmin edilen sonuca ait işlemler yürütülür. Böylece işlemci dallanma işleminin sonuçlanmasını beklemek yerine yürütüleceğini tahmin ettiği işlemleri yürütür ve zamandan tasarruf eder. Tahmini doğru ise doğru işlemleri yürütmüş olur ve zamandan kazanır; tahmini yanlış ise doğru sonuca ait işlemleri yürütür ama zamandan bir kazanç sağlamaz. Tahmin sonucu işlemlerin yürütülmesine spekülatif yürütme adı verilir. Genellikle işlemcinin yürüttüğü dallanma işlemi sayısı arttıkça doğru sonucu tahmin etme oranı da artar [28].

### Tiktag-v1 Nedir, Nasıl Çalışır

Tiktag-v1, ARM işlemcilerdeki MTE özelliğini atlatmak için işlemcinin spekülatif yürütmenin çalışma şeklini kullanan bir yöntemdir. MTE'yi atlatmak için kullandığı yöntem ise spekülasyonu küçültme yöntemidir.

İşlemci dallanma öngörüsünü yapar ve spekülatif yürütme işlemini başlatır. Öngörüde yanıldığını anladığında spekülatif yürütme işlemi sırasında yürütmeye başladığı işlemleri geri alarak "spekülasyonu küçültür". Böylece spekülatif yürütmeyi başlatmadan önceki durumuna geri döner ve doğru işlemleri yürütmeye başlar.

Bir saldırgan, aynı bellek bölgesine spekülatif olarak erişen bir kod parçası yazabilir. Bu kod işlemcinin dallanma öngörüsü mekanizmasını manipüle ederek spesifik bir sonucu tahmin etmek amacıyla yazılır. Kod çalıştırıldığında saldırgan işlemcinin önbellek üzerindeki yaptığı değişiklikleri ve bu sırada harcadığı zamanı tespit eder. MTE kontrolünün doğru ya da yanlış sonuç vermesine bağlı olarak işlemcinin davranışı değişebilir. MTE tahmini doğru ise işlemci hızında bir değişiklik olmaz ve saldırgan tahmininin doğru olduğunu anlar çünkü dallanma öngörüsü doğru tahmin edilmiştir; tahmin yanlış ise işlemci dallanma öngörüsündeki hatasını anlar ve dallanma öncesi durumuna geçer, bu işlemler işlemci hızını düşürür ve saldırgan bunu fark ederek yaptığı tahminin yanlış olduğu sonucunu çıkarır. Bu işlemleri tekrarlayarak saldırgan hedeflediği bellek bölgelerinin MTE etiketlerini tahmin edebilir [29].

### Tiktag-v2 Nedir, Nasıl Çalışır

Tiktag-v2'nin amacı "store-to-load forwarding blockage" mantığıyla spekülatif yürütme sırasında MTE etiketlerini açığa çıkarmaktır. Program bellekte bir bölgeye veri saklamak için yazma işlemi yaptığı ve program akışı gereği yazdıktan hemen sonra aynı bellek bölgesinden bu veriyi okumak istediği zaman, işlemci zamandan tasarruf için bu veriyi belleğe gidip okumak yerine kendi hafızasından okur. İşlemcinin zamandan tasarruf etmek için kullandığı bu yönteme "store-to-load forwarding" denir.

Spekülatif yürütme sırasında işlemci MTE etiketi kontrolü sağlanamadığında ise zamandan kazandığı bu yöntemin kullanılmasını engeller. Bunun sebebi ise MTE etiketinin doğrulanamaması sebebiyle kullanılacak verinin doğruluğundan emin olunamamasıdır.

Saldırgan aynı bellek bölümüne spekülatif olarak saklama ve okuma işlemini sırasıyla yapan bir kod yazabilir ve saklama ile okuma işlemleri arasındaki süreyi ölçebilir. Bellek bölgesine yaptığı yazma işleminin MTE etiketinin

doğrulanması başarılı olursa "store-to-load forwarding" işlemi gerçekleşir, üstelik daha hızlı gerçekleşir. Eğer MTE etiketini doğrulama işlemi başarısız olursa işlemcide zaman kaybı yaşanır ve saldırgan bu zaman kaybını fark eder. Bu süreç tekrarlanarak işlemlerin gerçekleşme süresi analiz edilebilir ve MTE etiketi ortaya çıkarılabilir [29].

**Etkilenen Ürünler Nelerdir**

Tiktag-v1 ve Tiktak-v2 saldırılarından etkilenen ürünler arasında ARM işlemcilerini kullanan mobil cihazlar yer almaktadır. Android işletim sistemlerinin MTE özelliğini kullanan bazı sürümleri bu saldırılara karşı savunmasız olabilir. Buna dahil olarak ARM işlemcisini kullanan yönlendiriciler (router) ve endüstriyel kontrol sistemleri gibi gömülü sistemler de güvenlik için MTE özelliğini kullanıyorsa bu saldırılardan etkilenebilir [29].

# DÖNEM KONUSU

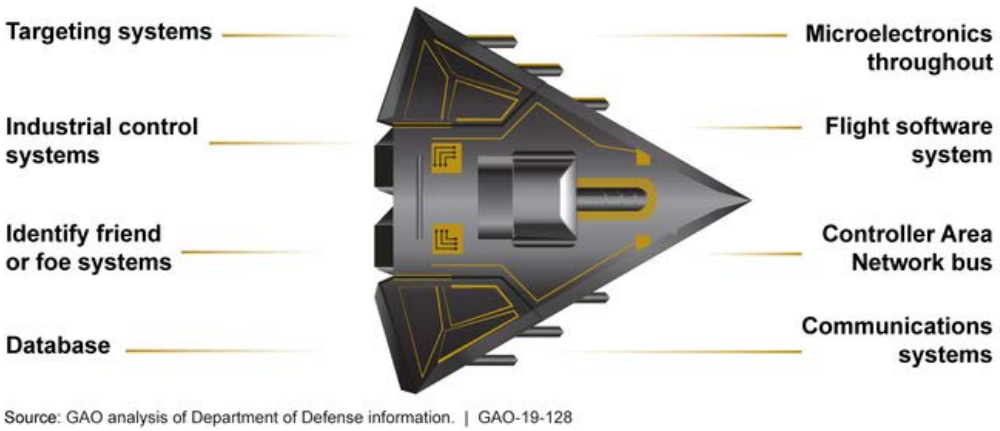
## 6. Silah Sistemlerinin Siber Dayanıklılığını Artırmak

Günümüz silah sistemleri büyük ölçüde bilgisayarlaştırılarak gömülü yazılım ve bilgi teknolojisi sistemleri ile donatılmıştır. Bu nedenle, silah sistemlerinin siber güvenliği, modern savunma ve güvenlik stratejilerinin vazgeçilmez bir parçasıdır. Şekil 1'de de bir örneği gösterildiği gibi silah sistemlerinin sahip olduğu Platform Bilgi Teknolojileri (Platform Information Technology -PIT), internet protokollerini ve yaygın son kullanıcı işletim sistemleri ve yazılımlarını kullanan geleneksel sistemlerden oldukça farklıdır ve farklı sorunlarla karşılaşırlar. PIT, gerçek zamanlı çalışır, donanımla ayrılmaz bir şekilde bütünleşir ve genellikle özel işletim sistemleri ve yazılımlar kullanır. Silah sistemlerine kurulumları nedeniyle, PIT'deki değişiklikler (güvenlik önlemleri dahil) genellikle ağırlık, ısı dağılımı ve gecikme ile sınırlıdır. Geleneksel bilgi teknolojisi için geliştirilmiş siber güvenlik ve siber dayanıklılık çözümleri silah sistemleri gibi platformlar için genellikle uygun değildir.

Bu nedenle, siber güvenlik ve siber dayanıklılığı tasarım aşamasında proaktif olarak yönetebilmek önemlidir. Araştırmalar, bu tür koordine edilmiş siber güvenlik ve siber dayanıklılık yaklaşımlarının programlar için daha verimli ve genel yatırım getirisinin daha iyi olduğunu göstermiştir [30].

Silah sistemlerinin siber güvenlik açısından kritik önemde olmasının nedenleri arasında şunları belirtebiliriz:

- **Görev İcraatı:** Silah sistemleri, tasarlandıkları görevleri yerine getirmek için güvenli bir şekilde çalışmalıdır. Siber saldırılar, bu sistemlerin işlevselliğini bozabilir veya tamamen devre dışı bırakabilir.
- **Ulusal Güvenlik:** Silah sistemleri, bir ülkenin savunma ve güvenlik stratejisinin temel unsurlarındandır. Bu sistemlerin siber saldırılara karşı korunması, ulusal güvenliğin sağlanması açısından kritik öneme sahiptir.
- **Veri Güvenliği:** Silah sistemleri, hassas ve gizli bilgileri işler. Bu bilgilerin siber saldırılarla çalınması veya manipüle edilmesi, düşmanların stratejik avantaj elde etmesine yol açabilir.
- **Operasyonel Güvenlik:** Siber saldırılar, silah sistemlerinin operasyonel kapasitesini düşürebilir veya yanlış yönlendirebilir. Bu durum, askeri operasyonlarda başarısızlıklara ve beklenmedik kayıplara yol açabilir.
- **Dayanıklılık:** Silah sistemlerinin siber tehditlere karşı dayanıklı olması, uzun vadeli etkinliklerini ve güvenilirliklerini artırır. Dayanıklı sistemler, saldırılardan sonra daha hızlı toparlanabilir ve operasyonlarına devam edebilir.
- **Yasal ve Etik Sorumluluklar:** Ülkeler ve askeri organizasyonlar, silah sistemlerinin güvenliğini sağlamakla yasal ve etik olarak yükümlüdür. Bu sorumlulukların ihlali, ciddi yasal sonuçlar ve itibar kaybına yol açabilir.




**Şekil 1:** Emsal bir silah sistemi bileşenleri[31].

- **Ekonomik Maliyetler:** Siber saldırılar, silah sistemlerinde ciddi hasarlara yol açabilir ve bu hasarların onarılması büyük maliyetler gerektirebilir. Güvenli sistemler, uzun vadede maliyetleri azaltabilir.
- **Müttefiklerle Güven:** Güvenli silah sistemleri, müttefik ülkeler ve partnerlerle güvenilir ilişkiler kurmanın temelidir. Bu sistemlerin güvenliği, ortak operasyonların başarısı için hayati önem taşır.

Peki, silah sistemlerinin siber güvenlik ve siber dayanıklılığını artırmak için olası önlemleri ve aktiviteleri, program ofisleri tarafından yönetilen projelerin yaşam döngüsüne ve dolayısıyla mühendislik aktivitelerine nasıl entegre etmeliyiz?

Bu amaçla, ABD Hava Kuvvetleri Stratejik Sistemler Program Yönetimi tarafından araştırılması talep edilmiş ve RAND AIR FORCE tarafından yürütülerek 28 Mart 2024 tarihinde yayınlanmış araştırma projesini inceleyeceğiz[30]. Rapor, silah sistemlerinin, proje yaşam döngüleri boyunca siber güvenlik ve siber dayanıklılığını yönetmenin temelini atmaktadır. Araştırma ve geliştirmeden, projelerin elden çıkarılma sürecine kadar dahil edilmesi gereken tüm faaliyetleri ana hatlarıyla belirleyerek, silah sisteminin siber tehditlerin bulunduğu bir ortamda çalışabilmesi için gereken tüm ihtiyaçları karşılamasını sağlamak amaçlanmıştır.

Mevcut durumdaki temel bulgular belirlenecek olursa; projelerin tasarım, operasyon ve sürdürülebilirlik aşamalarında siber güvenliğin yeri şu şekilde saptanmıştır.

- Tasarım aşamasında, sistem güvenliği mühendisliği son zamanlarda silah sistemlerinin siber güvenlik ve siber dayanıklılığı için Savunma Bakanlığı (Department of Defense -DoD) politikasına dahil edilmiştir, ancak bu uygulama DAF (Department of the Air Force) genelinde henüz yaygın hâle gelmemiştir ve hizmet seviyesinde bunun nasıl yapılacağına dair net bir politika veya rehberlik bulunmamaktadır. Risk Yönetim Çerçevesi'ne (Risk Management Framework -RMF) aşırı güven devam etmektedir, ki bu çerçeve büyük ölçüde sistem mühendisliğinden sonra uygulanmaktadır.
- Operasyon ve sürdürülebilirlik aşamasında, silah sistemlerinin günlük güvenlik izlemesinin büyük bir kısmı yürütülmektedir. Ancak;
  - Silah sistemlerine yönelik yetkili araçlar sağlanmamaktadır.
  - Elde bulunan araçlar silah sistemlerini kapsamlı bir şekilde izleyememekte veya savunamamaktadır.
  - Ne yapması gerektiğine dair teknik emirler verilmemektedir.
  - Politika, silah sisteminin siber durumu veya siber olaylar hakkında program ofislerine geribildirim yapılmasını genellikle gerektirmez. Siber güvenlik ve siber dayanıklılık, mevcut sürdürülebilir mühendislik veya yaşam döngüsü sürdürülebilirlik planlarının merkezi bir parçası değildir.

Ek olarak; GAO raporu[31] DOD'nin mevcut durumda siber dayanıklılığı olan silah sistemleri geliştirme yeteneğini zorlayacak engellerin özetle şunlar olduğunu saptamıştır:

- Sistem sahipleri, sınıflandırma nedeniyle, bağlandıkları sistemlerin zafiyetleri hakkında bilgi sahibi olmadıklarını belirtmişlerdir. Bir sistemin ancak en zayıf halkası kadar güvenli olduğu düşünüldüğünde sistemin bağlı olduğu diğer sistemler hakkında sınırlı bilgi sahibi olması bir bariyer olarak öne çıkmaktadır.
- Bir silah sistemi siber saldırıya uğradığında, bilginin sınıflandırma türü nedeniyle DOD program yetkililerine istihbarat topluluğu tarafından bu saldırının ayrıntıları verilmemektedir.
- Bazı sistem operatörlerinin (sistem güvenlik operatörleri dahil) zafiyet ve açıklık bilgilerine erişimi bulunmamaktadır.
- Bazı donanma gemilerinin gizli bilgi alma ve saklama yetkisi bulunmamaktadır.

Yukarıdakileri maddeleri değerlendirdiğimizde programlar arasında zafiyet ve tehdit bilgileri paylaşılmadığı için DOD'nin, silah sistemleri portföyü genelindeki zafiyetler hakkında daha az bilgi sahibi olacağı sonucu çıkacaktır. Hatta hatalı tasarımlar yeni tasarımlarda da tekrarlanacaktır. Ancak bir yönden de hassas bilgi korumanın avantajı olarak potansiyel düşmanların bilgi ele geçirmesinin önüne geçilmektedir.

Silah sistemlerinin kritikliğinden dolayı, her silah sisteminin yaşam döngüsü boyunca siber güvenlik ve siber dayanıklılığı için entegre bir mühendislik tabanlı plan geliştirilmesi ve sürdürülmesi gereklidir.

Tasarım aşamasında yapılabilecekler şu şekilde belirlenebilir:

- Tasarım aşamasında siber güvenlik aktivitelerini yürütebilmek için program planına ve sözleşme belgelerine ilgili siber güvenlik standartları ve tasarımların siber dayanıklılığını doğrulamak için kullanılacak yöntemler eklenmelidir. Bu yöntemler spesifik ve ölçülebilir olmalıdır.

GAO raporunun önceliği[31] tasarım aşamasında yapılabileceklere aşağıdakilerin eklenmesidir:

- Siber güvenlik gereksinimleri belirlenmeli ve verinin sistemler arasında nasıl girdi/çıktı olarak kullanıldığı, transfer edildiği, işlendiği, saklandığı saptanmalıdır. Bunları belirlemek, sistemlerin atak yüzeyini görmekte ve kullanılacak siber güvenlik kontrollerini belirlemekte işe yarayacaktır.
- Risk analizi çalışması ön tasarım aşamasında başlatılarak siber güvenlik riskleri görülmeli ve uygulanabilecek siber güvenlik kontrolleri değerlendirilmelidir.

- Silah sistemleri geliştirilirken siber güvenlik testlerinin yapılması sağlanmalıdır. Bu testler, sistem entegrasyon testleri ve operasyonel testler sırasında yapılabilir.

Öte yandan siber güvenlik ve siber dayanıklılık için, sürdürülebilir mühendislik ve yaşam döngüsü sürdürülebilirlik planlarının daha fazla kullanılması gereklidir. Bu aşamada yapılabilecekler şu şekilde belirlenebilir:

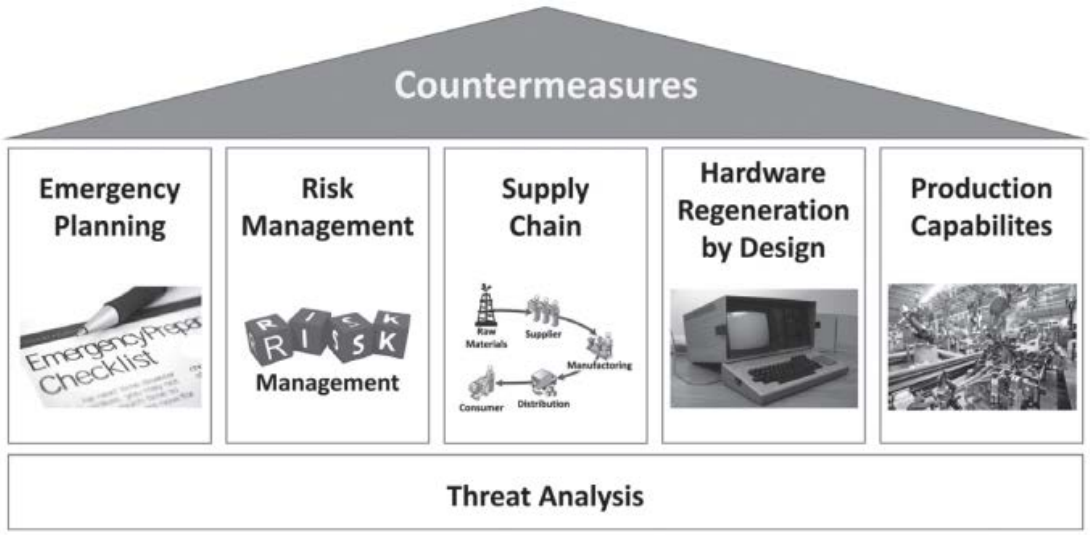
- Silah sisteminin kendisinin ve alt sistemlerinin, onaylı uygulamalarla siber takibinin sağlanması gereklidir. Bu sayede, sistemlerin siber güvenlik zihniyetiyle titizlikle tasarlanmış, geliştirilmiş ve test edilmiş, böylece siber saldırı vektörlerinin takip edilmiş olması sağlanabilir.
- Siber izlemeyi sağlamak için görev savunma ekipleri kurulmalıdır.
- Sistem sınırları içinde herhangi bir olağandışı davranış veya siber olay hakkında dışarıdan bilgi alınabilecek bir akış sağlanmalıdır.
- Sistem sınırları içinde gerçekleşen tüm konfigürasyon değişiklikleri takip edilmeli ve yönetilmelidir.

Şekil 2'de ana başlıklar halinde verildiği gibi CCDCOE raporu[32] özellikle tedarik zincirinin kritikliğini vurgular. Günümüzün karmaşık silah sistemlerinin bileşenleri ve bunların en iç bileşen parçaları, özellikle sensörleri, iletişim sistemlerini, veri alışverişi ve silah sistemlerini kontrol eden çipler, genellikle yüzlerce şirket ve binlerce insanı içeren uzun bir tedarik zinciri tarafından teslim edilen COTS ürünleridir. Rapor, tehditlerin sadece çiplerin üretim sürecinde değil, özellikle tasarım aşamasında mevcut olduğunun altını çizmektedir. Bu nedenle, güvenilir bir tedarik zinciri oluşturmak için gereksinim aşamasından nakliyeye kadar tüm adımlar dikkate alınmalıdır. Ancak, küreselleşmiş iş süreçleri ve ekonomik gerçeklik kabul edilmeli ve tedarik zinciri ile başa çıkmak için uygun bir strateji düşünülmelidir. Örneğin, tasarım ve geliştirme araçları için güvenlik, süreçlerin ve teknolojilerin araştırmaları artırılarak ve finanse edilerek sağlanabilir. Ayrıca yarı iletken bileşenlerin düzenli olarak değiştirilmesi değil, aynı zamanda sahte veya manipüle edilmiş çiplerin tespit yöntemleri, yeni donanımla uyumsuzluk durumunda sistem çekirdek unsurlarının göç stratejileri gibi uyumluluk sorunlarıyla nasıl başa çıkılacağına dair önlemlerin sağlanması gereklidir.

Bunlara ek olarak, yaşam döngüsü yönetim planları, her silah sisteminin operasyonlar, sürdürülebilirlik ve imha sırasında siber güvenlik ve siber dayanıklılığın nasıl sağlanacağını içerecek şekilde oluşturulmalıdır. Siber güvenlik, RMF tarafından uygulanan bir etkinlik olarak değil, sağlam mühendislik ve sürekli dikkat gerektiren bir süreç olarak görülmeli ve RMF tarafından sürekli olarak titizlikle değerlendirilmelidir.

## 7. Honeypot Verileri

Bu rapor üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. Saldırıların en çok toplandığı ülkeler, portlar, en çok denenen kullanıcı adları ve parolalar, veriler azalan sırada listelenerek inceleme için sunulmuştur. Nisan, Mayıs ve Haziran ayları boyunca Honeypot sensörlerimize toplam 1.390.611 saldırı gelmiştir.




**Şekil 2:** Silah sistemleri siber güvenliği için uygulanabilecek kontrol grupları[32].


**Şekil 3:** Gelen saldırıların ülkelere göre dağılımı.

| Saldırıların Geldiği Ülke | Saldırı Sayısı |
|---|---|
| Ukrayna | 138.412 |
| ABD | 127.544 |
| Rusya | 108.243 |
| Hindistan | 85.933 |
| Singapur | 78.607 |
| Almanya | 77.051 |
| Mısır | 75.874 |
| Çin | 70.538 |
| Estonya | 49.717 |
| Vietnam | 44.742 |

**Tablo 1:** En çok saldırı gelen 10 ülke ve saldırı sayıları.

| Saldırılan Port | Saldırı Sayısı |
|---|---|
| 445 - SMB | 344.756 |
| 5900 - VNC | 308.406 |
| 22 - SSH | 54.140 |
| 25 - SMTP | 32.716 |
| 23 - Telnet | 18.751 |
| 110 - POP3 | 3.657 |
| 21 - FTP | 1.270 |
| 80 - HTTP | 552 |
| 5432 - PostgreSQL | 536 |
| 5555 - ADB | 284 |

**Tablo 2:** En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen 10 ülkenin ilk sırasında Ukrayna (yüzde 18,66) olduğu, sonrasında sırasıyla ABD (yüzde 17,19), Rusya (yüzde 14,59), Hindistan (yüzde 11,58) ve Singapur'un (yüzde 10,59) yer aldığı görülmektedir.

Tablo 2'de de görüldüğü üzere en çok saldırı 445 portuna gelmiştir. 445 portunda sunucuların yazıcı ve paylaşılan dosyalar için kullandığı SMB servisi çalışmaktadır. Bu yüzden SMB servisinin diğer servislerden daha çok saldırı alması beklenen bir durum olarak kabul edilebilir.

İkinci sırada 5900 numaralı port VNC (Virtual Network Computing) yer almaktadır. VNC uzaktan masaüstü erişimi sağlayan bir protokol olduğundan, bu porta yapılan saldırılar sıklıkla yetkisiz erişim ve kötü amaçlı yazılımların bulaşması amacıyla gerçekleştirilmiş olabilir.

Üçüncü sırada 22 numaralı port (SSH) yer almaktadır. SSH (Secure Shell), güvenli uzaktan yönetim ve dosya transferi için kullanılan standart bir protokoldür. Bu porta yapılan saldırılar genellikle yetkisiz erişim denemeleri ve veri çalma girişimlerinde gerçekleştirilir.


**Şekil 4:** Parola etiket bulutu.

| Denenen Parola | Deneme Sayısı |
|---|---|
| 345gs5662d34 | 4.458 |
| 3245gs5662d34 | 4.443 |
| 123456 | 3.037 |
| password | 1.479 |
| 123 | 1.272 |
| Password | 1.226 |
| admin | 1.077 |
| 12345678 | 1.073 |
| 12345 | 630 |
| Passw0rd | 586 |

**Tablo 3:** SSH ve RDP honeypot'larımız üzerinde en çok denenen parolalar ve deneme sayıları.

| Denenen Kullanıcı Adı | Deneme Sayısı |
|---|---|
| root | 26.825 |
| 345gs5662d34 | 4.458 |
| admin | 2.564 |
| user | 1.160 |
| test | 965 |
| postgres | 878 |
| ubuntu | 841 |
| (boş) | 810 |
| ftpuser | 381 |
| oracle | 295 |

**Tablo 4:** SSH ve RDP honeypot'larımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.


**Şekil 5:** Kullanıcı adı etiket bulutu.

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan 123456, 345gs5662d34, admin, password gibi terimler gözlemlenmektedir. Bu parolaların test veya deneme süreçleri tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir. Ayrıca kolay hatırlanması ve girilmesi için herhangi bir harf, özel karakter içermeden sadece sıralı sayılar ile oluşturulmuş parolalar kullanmaktan kaçınılmalıdır.

Denenen kullanıcı adları incelendiğinde, yeni kurulan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin (örn. ubuntu, postgres, oracle, testuser) kullanılmaması tavsiye edilmektedir.

# KAYNAKÇA

[1] UNCTAD, "Review of Maritime Transport," 2020. [Çevrimiçi]. Available: https://unctad.org/system/files/official-document/rmt2020_en.pdf.

[2] NIST, "NIST Cybersecurity Framework (CSF)," [Çevrimiçi]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[3] ISO, "ISO27001," [Çevrimiçi]. Available: https://www.iso.org/standard/27001.

[4] BIMCO, "The Guidelines on Cyber Security Onboard Ships," [Çevrimiçi]. Available: (4) https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

[5] "Rec 166 – Recommendation on Cyber Resilience,» [Çevrimiçi]. Available: https://iacs.org.uk/resolutions/recommendations/161-180/rec-166-new-corr2-cln.

[6] IACS, "Cyber resilience of ships," [Çevrimiçi]. Available: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf.

[7] IACS, "Cyber Resilience of on-board Systems and Equipment," [Çevrimiçi]. Available: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-rev1.

[8] IMO, "GUIDELINES ON MARITIME CYBER RISK MANAGEMENT," [Çevrimiçi]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf.

[9] LR, "Cyber safe for marine," [Çevrimiçi]. Available: https://www.lr.org/en/services/classification-certification/cyber-resilience/cyber-safe-for-marine/?creative=696313830157&keyword=cyber%20security%20maritime&matchtype=p&network=g&device=c&utm_source=google&utm_campaign=maritime-energy-transition&utm_medi.

[10] IACS, "Computer-based systems," [Çevrimiçi]. Available: https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e22-rev2-cln-2.

[11] NIST, "Secure Software Development Framework (SSDF)," [Çevrimiçi]. Available: https://csrc.nist.gov/pubs/sp/800/218/final.

[12] OWASP, "Application Security Verification Standard," [Çevrimiçi]. Available: https://github.com/OWASP/ASVS.

[13] O. Nir, "reflectiz," 22 04 2024. [Çevrimiçi]. Available: https://www.reflectiz.com/blog/polyfill. [Erişildi: 05 07 2024].

[14] A. Sharma, "Bleeping Computer," 21 07 2021. [Çevrimiçi]. Available: https://www.bleepingcomputer.com/news/security/npm-package-steals-chrome-passwords-on-windows-via-recovery-tool/ . [Erişildi: 05 07 2024].

[15] "Dev.to," 27 06 2024. [Çevrimiçi]. Available: https://dev.to/snyk/polyfill-supply-chain-attack-embeds-malware-in-javascript-cdn-assets-55d6. [Erişildi: 05 07 2024].

[16] C. H. Baron, "Abnormal security," 06 02 2024. [Çevrimiçi]. Available: https://abnormalsecurity.com/blog/data-shows-c-suite-receives-42x-more-qr-code-attacks. [Erişildi: 05 07 2024].

[17] C. H. Baron, "Abnormal Security," 09 04 2024. [Çevrimiçi]. Available: https://abnormalsecurity.com/blog/qr-code-phishing-attacks-quishing . [Erişildi: 05 07 2024].

[18] "Vade Secure,» 21 09 2023. [Çevrimiçi]. Available: https://www.vadesecure.com/en/blog/qrishing-attack-microsoft-cloudflare. [Erişildi: 05 07 2024].

[19] 17 6 2024. [Çevrimiçi]. Available: https://www.bankinfosecurity.com/sleepy-pickle-researchers-find-new-way-to-poison-ml-a-25538. [Erişildi: 28 6 2024].

[20] 26 3 2024. [Çevrimiçi]. Available: https://github.com/trailofbits/fickling?tab=readme-ov-file#pickle-code-injection. [Erişildi: 28 6 2024].

[21] 13 6 2024. [Çevrimiçi]. Available: https://thehackernews.com/2024/06/new-attack-technique-sleepy-pickle.html. [Erişildi: 28 6 2024].

[22] 17 6 2024. [Çevrimiçi]. Available: https://www.bankinfosecurity.com/sleepy-pickle-researchers-find-new-way-to-poison-ml-a-25538. [Erişildi: 28 6 2024].

[23] 17 6 2024. [Çevrimiçi]. Available: https://www.bankinfosecurity.com/sleepy-pickle-researchers-find-new-way-to-poison-ml-a-25538. [Erişildi: 28 6 2024].

[24] 13 6 2024. [Çevrimiçi]. Available: https://thehackernews.com/2024/06/new-attack-technique-sleepy-pickle.html. [Erişildi: 28 6 2024].

[25] 14 6 2024. [Çevrimiçi]. Available: https://medium.com/@amirulizzuddin120/understanding-the-security-risks-of-sleepy-pickle-in-machine-learning-b08daaf3a20f. [Erişildi: 28 6 2024].

[26] 14 6 2024. [Çevrimiçi]. Available: https://medium.com/@amirulizzuddin120/understanding-the-security-risks-of-sleepy-pickle-in-machine-learning-b08daaf3a20f. [Erişildi: 28 6 2024].

[27] M. Lu, "Memory Safety: How Arm Memory Tagging Extension Addresses this Industry-wide Security Challenge," 24 02 2023. [Çevrimiçi]. Available: https://newsroom.arm.com/blog/memory-safety-arm-memory-tagging-extension#:~:text=Through%20Arm%20CPUs%20built%20on,silicon%20vendors%20and%20device%20manufacturers..

[28] M. Zubair, "What is branch prediction?," 2024. [Çevrimiçi]. Available: https://www.computerhope.com/jargon/b/branch-prediction.htm.

[29] J. P. e. a. Juhee Kim, "TIKTAG: Breaking ARM's Memory Tagging Extension with Speculative Execution," 13 06 2024. [Çevrimiçi]. Available: https://arxiv.org/pdf/2406.08719.

[30] D. Snyder ve C. Heitzenrater, "Enhancing Cybersecurity and Cyber Resiliency of Weapon Systems," 28 Mart 2024. [Çevrimiçi]. Available: https://www.rand.org/pubs/research_reports/RRA1506-2.html.

[31] "Weapon Systems Cybersecurity," Ekim 2018. [Çevrimiçi]. Available: https://www.gao.gov/assets/gao-19-128.pdf.

[32] "Weapons Systems and Cybersecurity," 2016. [Çevrimiçi]. Available: https://www.ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech