STM Cyber

TEMMUZ-EYLÜL 2024

SİBER TEHDİT DURUM RAPORU

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

ŞEKİLLER

GİRİŞ

2024 yılının üçüncü çeyreğinde Siber Güvenlik Müdürlüğü tarafından hazırlanan raporumuzda yine birbirinden ilginç konularla karşınızdayız. Bu bağlamda ilk olarak, "Web Atağının Hedef Altyapıdaki İzleri" konusu ile siber saldırıların izlerinin gözlemlenmesi ve analiz edilmesi konularına odaklanıyoruz. Ardından, "Dijital Operasyonel Dayanıklılık Yasası (DORA)" çerçevesinde işletmelerin dijital altyapılarını güçlendirmeleri için ihtiyaç duydukları gereksinimleri ve bu bağlamdaki en iyi uygulamalar ele alınacaktır. Hemen sonrasında, Cross-Site Scripting (XSS) zafiyetlerinin web uygulamalarında yaygın bir tehdit oluşturmasından ve bu zafiyetlerin azaltılması için alınabilecek önlemler detaylı bir şekilde ele alınacaktır. Ayrıca, "JWT Zayıf Gizli (*Secret*) Anahtar Kullanımı Kaynaklı Güvenlik Zafiyeti" başlığı altında JSON Web Token kullanımının içerdiği zafiyetlerin önemi ve dikkat edilmesi gereken noktalar aktarılacaktır.

Sonraki bölüm "Türkiye'yi Hedef Alan APT Gruplarına Genel Bir Bakış" konulu makalede Türkiye'yi hedef alan APT gruplarına genel bir bakış sunulacak ve bu tehditlerin nasıl tespit edilebileceği ve önlenebileceği üzerinde durulacaktır. Daha sonra, "Gelişmiş Kimlik Doğrulama Yöntemleri ve Önemi" konusu vurgulanarak, güvenliğin artırılması için kullanılan modern yöntemler ve bunların işletmeler üzerindeki etkileri değerlendirilecektir. Daha sonra "Lumma Stealer" bölümünde lumma stealer zararlı yazılımını analiz ediyor ve bu zararlı yazılımın detaylarını açıklıyoruz. Lumma Stealer zararlı yazılımı, veri hırsızlığı için geliştirilen yeni bir tehdit olarak dikkat çekmektedir. Son olarak "Event ve Incident Kavramlarının NIST Tanımlarıyla İncelenmesi" bölümünde NIST tanımlarıyla event ve incident kavramları arasındaki farkları inceledik, olay müdahale süreçlerinin nasıl daha etkili yönetilebileceğine odaklandık.

Bu çeyreğin dönem konusu olarak belirlediğimiz "Bilgi Teknolojileri (IT) ve Operasyonel Teknolojilerin (OT) Farklı Siber Güvenlik Öncelikleri" konusunu sizlerle paylaşıyoruz. Bu bölümde de IT ve OT gibi iki alan arasındaki farklılıkları ve buna bağlı güvenlik stratejilerini incelemeyi hedeflemekteyiz.

Son olarak her raporumuzda güncellediğimiz honeypot verilerimize yer ayırdık. Bu rapor, bilişim dünyasındaki güvenlik tehditlerini ve korunma stratejilerini anlamak isteyen herkes için önemli bir kaynaktır. Güvenlik bilincinizi artırmak ve siber tehditlere karşı daha hazırlıklı olmanız için bu raporu incelemenizi tavsiye ederiz. Güvende kalın!

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. WEB Atağının Hedef Altyapıdaki İzleri

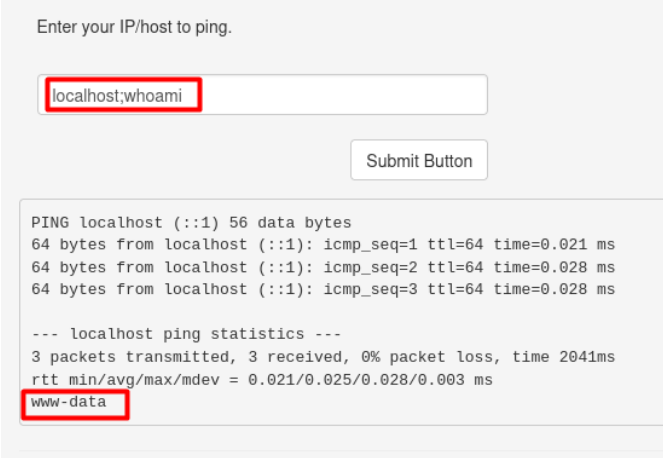
Siber Güvenlik Operasyon Merkezi (SGOM) tüm kurumlar için hayati bir birimdir[1]. Günümüzde kurumlar SGOM sorumluluklarını kendi içlerinde yerine getirmekte veya dışarıdan hizmet alarak olay müdahale süreçlerini icra etmektedir.

Siber Güvenlik Operasyon Merkezlerinde gerçekleştirilen faaliyetler SGOM Görünürlük Üçlüsü (Network, Endpoint ve SIEM/UEBA) ile gerçekleştirilir [2]. Bu görünürlük yeteneği kazanıldığında atakların veya anormal durumların tespiti kolaylaşmakta ve uzmanlara daha hızlı hareket etme yeteneği kazandırmaktadır.

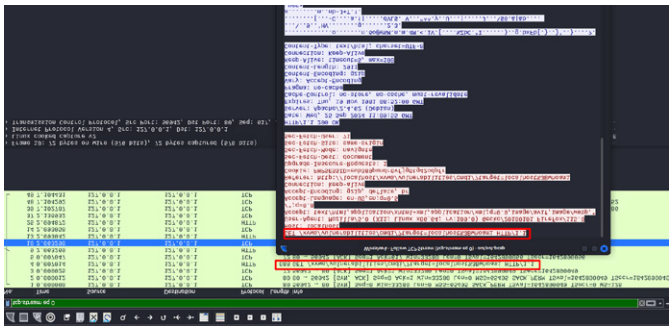
Bu çalışma, SGOM Görünürlük Üçlüsünü kapsamında, WEB Injection (OWASP Top Ten, 2021)[3] atağının zafiyetli bir web uygulamasının[4] laboratuvar ortamında hangi sistemlerde iz bırakabildiğini göstererek, Siber Güvenlik Analistleri için bir başvuru kaynağı oluşturma amacıyla yazılmıştır. Çalışma, senaryonun gerçekleşmesi için herhangi bir güvenlik önlemi alınmadan gerçekleştirilmiştir.

Bir web sitesindeki bir girdi çoğunlukla sunucu tarafında belli fonksiyonlara tabi tutularak bir çıktı üretilir. Çalışmada kullandığımız web hizmetinde, bir textbox'a host adı veya IP adresi girilip buton tıklandığında, web sunucusu

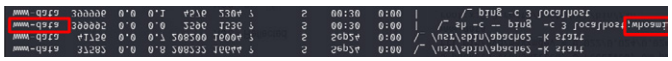
Şekil 1: SGOM görünürlük üçlüsü.



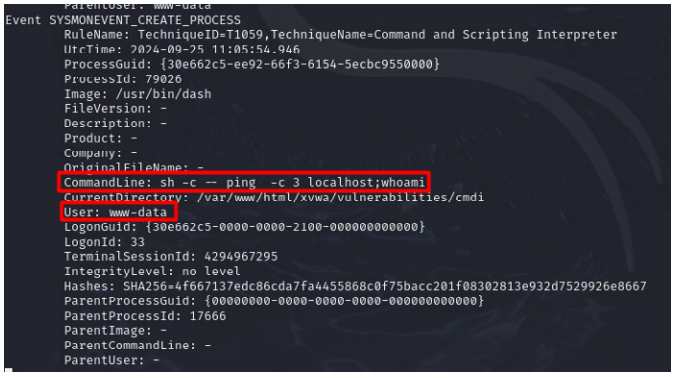
Şekil 2: Code injection.



Şekil 3: Web atağının ağ üzerindeki izleri.



Şekil 4: Atağın hedef sistemin ram'i üzerindeki izleri.



Şekil 5: Atağın sistem kayıtlarındaki izleri.

bu girdilere ping atarak çıktıyı kullanıcıya sunmaktadır. Senaryoda ";" kullanılarak code injection gerçekleştirilmiştir ve fazladan "whoami" komutu çalıştırılmıştır. Atağın sonucu olarak "www-data" kullanıcı adı web sayfasında çıktı olarak görülmüştür.

Bu atağın kurum varlıklarında görülme sırası Ağ, RAM ve LOG şeklinde olacaktır. Atak, ağ katmanında WAF, NFT/NTA, IDS/IPS araçlarıyla hedefe ulaşmadan önce tespit edilebilir veya engellenebilir. Yandaki ekran görüntüsünde atağın ağ üzerindeki izleri görülebilir.

Atak, hedef işletim sistemine ulaştığında RAM üzerinde uçucu bir veri oluşturacaktır. Aşağıdaki resimde, atağın hedef sistemin "process" listesindeki etkisi görülebilir. EDR çözümleri bu aşamada hedef sistemin korunmasına yardımcı olabilir veya kod tarafında girdi kontrolü vb. önlemler alınabilir.

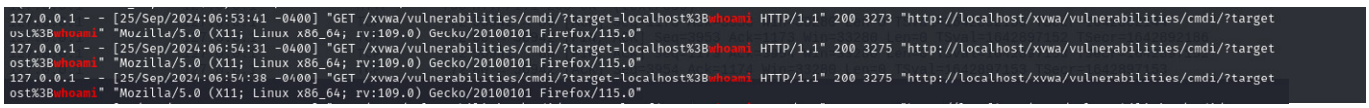
Eğer işletim sisteminin logları[5] tutuluyorsa atağın gerçekleştiği sistem kayıtlarına düşecektir. Burada yine web servis kullanıcısının "process" oluşturarak "whoami" komutunu çalıştırdığı görülmektedir.

Eğer etkilenen serviste loglama yeteneği aktifleştirildiyse atağın etkileri yine aşağıdaki gibi görülecektir. Eğer ki işletim sistemi ve ilgili hizmetin logları SIEM'e entegre edilirse görünürlük sağlanmış olacaktır.

Sonuç olarak analiz, bir web atağının hedef ağ, işletim sistemi ve servis üzerindeki izleri ortaya çıkarılarak ve SGOM görünürlük üçlüsüyle eşleştirilerek gerçekleştirilmiştir. STM Siber Füzyon Merkezi Kırmızı ve Mavi takım olarak müşterilerimize bu doğrultuda hizmetler sunmaktadır.

2. Dijital Operasyonel Dayanıklılık Yasası (DORA)

Dijitalleşmenin hızlanması, finansal kuruluşlar için dijital operasyonel riskleri daha görünür ve yönetilmesi zor hâle getirmiştir. Avrupa Birliği (AB), bu riskleri minimize etmek amacıyla Dijital Operasyonel Dayanıklılık Yasasını (DORA) yürürlüğe koymuştur. 17 Ocak 2025 itibariyle geçerli olacak olan DORA, AB sınırları içindeki tüm finansal kuruluşların bilgi ve iletişim teknolojileri (ICT) altyapılarını ve risk yönetim süreçlerini güçlendirmeyi zorunlu kılmaktadır. Ancak bu düzenlemenin etkileri, yalnızca AB ile sınırlı olmayıp küresel çapta da kendini hissettirecek gibi görünmektedir.



Şekil 6: Web servisi loglarında atağın izleri.

DORA'nın Amacı ve Kapsamı

DORA, dijital operasyonel risklerin yönetiminde iki temel amacı hedeflemektedir:

1. **ICT risk yönetimini kapsamlı şekilde ele almak:** DORA, finansal kuruluşların dijital operasyonel risklerini daha etkili bir şekilde yönetmesini zorunlu kılacak.
2. **AB genelinde ICT risk yönetimi düzenlemelerini uyumlu hâle getirmek:** DORA, farklı AB ülkelerinde mevcut olan ICT risk yönetimi düzenlemeleri arasındaki farklılıkları ortadan kaldırarak tek bir çerçeve oluşturacak.

DORA, sadece bankalar ve yatırım firmaları gibi geleneksel finans kuruluşlarını değil, aynı zamanda **kripto varlık hizmet sağlayıcıları** ve **kitle fonlama platformları** gibi yeni finansal teknolojilerle çalışan şirketleri de kapsamaktadır. Ayrıca, **üçüncü taraf teknoloji hizmet sağlayıcıları** da (bulut hizmeti sağlayıcıları, veri merkezleri vb.) DORA'nın belirlediği standartlara uyum sağlamak zorundadır.

ABD ve Çin'de Dijital Operasyonel Dayanıklılık Düzenlemeleri

ABD ve Çin'de, DORA benzeri düzenlemeler, finansal kuruluşların dijital risklerle başa çıkmalarını sağlamak amacıyla uygulanmaktadır.

ABD

1. **NYDFS Siber Güvenlik Yönetmeliği (23 NYCRR 500):** New York Eyaleti Finansal Hizmetler Departmanı, finansal kuruluşların siber risk yönetimini ve siber güvenlik olaylarını düzenleyici kurumlara raporlamasını zorunlu kılar. DORA ile benzer şekilde, NYDFS de siber olayların yönetimi ve raporlanması konusunda katı gereklilikler sunuyor.
2. **NIST Siber Güvenlik Çerçevesi:** ABD genelinde kullanılan NIST Cybersecurity Framework, finansal kuruluşların siber tehditlere karşı dirençli olmasını sağlamak amacıyla rehberlik ediyor. 2024 yılında güncellenen NIST Cybersecurity Framework DORA'ya benzer olarak, NIST çerçevesi de sürekli izleme ve test süreçlerine odaklanıyor.

Çin

1. **Siber Güvenlik Yasası (2017):** Çin'in Siber Güvenlik Yasası, finansal kuruluşların kritik bilgi altyapılarını koruma altına almayı ve dış hizmet sağlayıcılarını denetlemeyi zorunlu kılıyor. DORA gibi, Çin'in Siber Güvenlik Yasası da dış hizmet sağlayıcılarının güvenlik standartlarına uyumunu sağlamayı amaçlıyor.
2. **Kritik Bilgi Altyapısının Güvenliği Düzenlemesi (2021):** Bu düzenleme, dış hizmet sağlayıcılarının denetim altında tutulmasını ve operasyonel güvenliklerinin artırılmasını hedefliyor. DORA'nın üçüncü taraf sağlayıcılar üzerindeki kontrolleri ile benzer bir yaklaşım sergiliyor.
3. **Veri Güvenliği Yasası (2021):** Çin'in bu yasası, veri güvenliği ve olası ihlallere karşı hızlı müdahale gerekliliklerini kapsıyor. DORA'nın veri güvenliği ve ihlal bildirim süreçleriyle örtüşen bu yasa, Çin finansal sisteminin siber dayanıklılığını artırmayı amaçlıyor.

Birleşik Krallık ve Diğer Ülkelerde Benzer Düzenlemeler

1. **Birleşik Krallık:** Birleşik Krallık'ta **FCA** (Financial Conduct Authority) ve **PRA** (Prudential Regulation Authority) tarafından yürürlüğe konan düzenlemeler, finansal kuruluşların operasyonel risklerini yönetmelerini, dış hizmet sağlayıcılarını denetlemelerini ve kritik fonksiyonların sürekliliğini sağlamalarını zorunlu kılıyor. DORA ile benzerlik taşıyan bu düzenlemeler, dijital operasyonel risklerin minimize edilmesine yönelik adımlar içeriyor.
2. **Singapur – MAS TRM Guidelines:** Singapur Para Otoritesi (MAS), finansal kuruluşların teknoloji risklerini yönetmelerini ve dijital operasyonel risklerini azaltmalarını zorunlu kılan **Technology Risk Management Guidelines** adlı düzenlemeyi uygulamaktadır. Bu düzenleme, DORA gibi, üçüncü taraf ICT hizmet sağlayıcılarının denetlenmesini ve yönetilmesini gerektiriyor.
3. **Avustralya – APRA CPS 234:** Avustralya Prudential Regulation Authority (APRA) tarafından yürürlüğe konulan CPS 234 düzenlemesi, bilgi güvenliğinin ve dış hizmet sağlayıcılarının denetlenmesini zorunlu kılıyor. DORA'da da olduğu gibi, dış hizmet sağlayıcılarının güvenlik standartlarını karşılaması gerekiyor.

DORA'nın Uygulama Yol Haritası

DORA'nın uygulanması aşamalı bir süreç olarak belirlenmiştir ve tam uyumun 17 Ocak 2025'e kadar sağlanması gerekmektedir. Bu süreç, AB genelinde finansal kuruluşların ve teknoloji sağlayıcılarının yeni gerekliliklere uyum sağlaması için bir yol haritası sunuyor.

1. 2023-2024 – Hazırlık Aşaması:

- AB üyesi ülkelerdeki finansal kuruluşlar, DORA'nın gerektirdiği ICT risk yönetimi çerçevesini oluşturmaya başlayacak.
- Yönetim organları, DORA gerekliliklerini anlamak ve uyum stratejileri geliştirmek için geniş bilgi sahibi olmalıdır.

- Üçüncü taraf hizmet sağlayıcılarıyla yapılacak sözleşmelerde DORA'ya uygun düzenlemeler yapılmalıdır.

2. 2024 – Teknik Standartların Tamamlanması:

- **Avrupa Denetleyici Otoriteleri (ESA'lar)**, düzenleyici teknik standartları (RTS) ve uygulama standartlarını (ITS) yayınlayacaktır. Bu standartlar, finansal kuruluşların ICT sistemleri için hangi güvenlik önlemlerini uygulamaları gerektiğini belirleyecektir.
- **Avrupa Komisyonu**, kritik ICT sağlayıcılarına yönelik denetim çerçevesini tamamlayacaktır.

3. Ocak 2025 – Uyum ve Denetim Başlangıcı:

- DORA'nın gerekliliklerine uyum sağlamayan kuruluşlar, ulusal yetkililer tarafından denetlenecek. Uyum sağlamayan kuruluşlar için ceza uygulamaları yürürlüğe girecektir.
- DORA, finansal kuruluşların ICT altyapılarında düzenli testler yapılmasını, kritik olayların raporlanmasını ve üçüncü taraf hizmet sağlayıcılarının denetlenmesini zorunlu kılacaktır.

DORA'nın Öne Çıkan Gereklilikleri

DORA, finansal kuruluşlar ve ICT sağlayıcıları için dört ana alanda zorunlu standartlar getirmektedir:

1. **ICT Risk Yönetimi ve Yönetim:** Finansal kuruluşlar, ICT sistemlerini haritalamalı, kritik varlıkları belirlemeli ve risk yönetim süreçlerini tanımlamalıdır. Yönetim organları bu süreçlerden sorumlu tutulacaktır.
2. **Olay Müdahale ve Raporlama:** Kuruluşlar, siber olayları izlemeli ve raporlamalıdır. Bu süreç, ilk bildirim, ilerleme raporu ve nihai rapor aşamalarını içerir.
3. **Dijital Operasyonel Dayanıklılık Testleri:** Kritik finansal kuruluşlar, her üç yılda bir tehdit odaklı sızma testleri (TLPT) gerçekleştirmeli ve sonuçları düzenleyici otoritelere sunmalıdır.
4. **Üçüncü Taraf Risk Yönetimi:** Dış hizmet sağlayıcıları, finansal kuruluşlar tarafından denetlenmeli ve belirlenen güvenlik standartlarına uyum sağlamalıdır. Kritik hizmet sağlayıcılar, doğrudan Avrupa Denetleyici Otoriteleri tarafından denetlenecektir.

Türkiye'ye Etkileri

DORA'nın Türkiye'deki finansal kuruluşlar için de önemli etkileri olabilir. Özellikle AB ile ticari ilişkileri olan kuruluşlar, DORA gerekliliklerine uyum sağlamak durumundadır. Türkiye'deki **BDDK** (Bankacılık Düzenleme ve Denetleme Kurumu) tarafından yürürlüğe konan **Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Yönetmeliği**, Türkiye'nin DORA ile uyum sağlaması için güçlü bir temel sunmaktadır. Aynı zamanda **KVKK** (Kişisel Verilerin Korunması Kanunu) ile de örtüşen veri güvenliği gereklilikleri, Türkiye'nin dijital altyapısının güçlenmesine katkıda bulunacaktır.

Sonuç: DORA'nın Küresel Etkisi ve Uyum Süreci

DORA, AB finansal sisteminde dijital operasyonel riskleri yönetmek için kapsamlı bir düzenleme sunarken, ABD, Çin ve diğer ülkelerdeki benzer düzenlemelerle de uyumludur. Türkiye'deki finansal kuruluşların, DORA ve diğer küresel düzenlemelere uyum sağlaması, finansal sistemdeki rekabet avantajlarını artıracak ve AB ile olan ticari entegrasyonu güçlendirecektir.

3. Cross-Site Scripting (XSS) Zafiyetlerinin Azaltılması İçin Önlemler

XSS saldırıları, 2024 yılı itibarıyla web uygulamaları üzerinde hâlâ ciddi bir tehdit oluşturmaya devam ediyor. XSS, web uygulamalarındaki güvenlik açıklarının yüzde 50'sini oluşturarak en yaygın saldırı türlerinden biri hâline gelmiştir. Özellikle Document Object Model (DOM) tabanlı XSS saldırıları, artan istemci tarafı işleme uygulamaları ve tek sayfa uygulamaların (Single Page Applications - SPA) yaygınlaşmasıyla daha sık görülmekte ve tespit edilmesi zorlaşmaktadır[6].

Ayrıca, kalıcı XSS saldırıları da artmaktadır. Bu saldırılar, veritabanlarına yerleştirilen zararlı kodlar yüzünden kullanıcıların sürekli tehlike altında kalmasına neden olmakta ve oturum çalma ya da veri manipülasyonu gibi ciddi sonuçlara yol açabilmektedir[7].

Bu bağlamda, Cybersecurity and Infrastructure Security Agency (Siber Güvenlik ve Altyapı Güvenliği Ajansı - CISA) yazılım geliştiricilerin güvenli tasarım ilkelerini benimsemeleri gerektiğini vurgulamaktadır. XSS zafiyetleri, saldırganların kullanıcı tarayıcılarına kötü amaçlı komutlar enjekte ederek sistem güvenliğini tehlikeye atmalarına olanak tanır. Güvenli yazılım geliştirme ve düzenli güvenlik testleri yapılarak bu tür zafiyetlerin önüne geçmek büyük önem taşımaktadır[8].

CISA son raporlarında, XSS açıklarının, geliştiricilerin girdi doğrulama, sanitizasyon (veri temizleme) ve kaçış mekanizmalarını doğru uygulamamasından kaynaklandığı belirtilmektedir.

Geliştiricilere, web uygulamalarında güvenli kodlama prensiplerine uygun hareket etmeleri ve modern web çerçeveleri kullanmaları önerilmektedir. Bu çerçeveler, XSS zafiyetlerini engellemek için yerleşik güvenlik işlevlerine yöneliktir[9].

Önerilen Önlemler

Girdi Doğrulama ve Kaçış Mekanizmaları

Kullanıcı tarafından sağlanan veriler, Hypertext Markup Language (HTML) veya JavaScript gibi tarayıcı bileşenlerine doğrudan iletilmeden önce doğrulanmalı ve uygun kaçış mekanizmaları kullanılmalıdır. Kaçış mekanizmaları, özel karakterleri güvenli hâle getirerek zararlı kodların çalıştırılmasını engeller.

Örneğin:

- HTML Kaçışları:

  < karakteri <, > karakteri > olarak değiştirilir.

- JavaScript Kaçışları:

  Tırnak işaretleri (“, ‘) veya ters eğik çizgi (\) gibi özel karakterler kaçış karakterleriyle değiştirilir.

- SQL Kaçışları:

  Structured Query Language (SQL) enjeksiyon saldırılarını önlemek için SQL sorgularında kullanılan özel karakterler kaçış karakterlerine çevrilir.

Modern Web Çerçeveleri Kullanılması

- Geliştiricilerin XSS gibi açıkları önlemek için yerleşik güvenlik özelliklerine sahip modern web çerçevelerini kullanmaları önerilir.

Düzenli Güvenlik Testleri

Yazılım güvenlik açıklarını erken aşamada tespit etmek için düzenli güvenlik testleri yapılmalı ve statik ve dinamik analizlerle güvenlik zafiyetleri tespit edilmelidir.

Sonuç

XSS gibi kritik güvenlik açıklarının ortadan kaldırılması, yalnızca teknik önlemlerle sınırlı kalmamalıdır. Yazılım geliştiriciler, güvenli tasarım prensiplerine uyarak yazılım güvenliği kültürünü güçlendirmelidir.

4. JWT Zayıf Gizli Anahtar (Secret) Kullanımı Kaynaklı Güvenlik Zafiyeti

JWT Nedir?

JSON Web Token (JWT), taraflar (istemci/sunucu vb.) arasında kullanılacak bilgilerin JSON nesnesi olarak güvenli bir şekilde iletilmesi için kompakt ve bağımsız bir yol tanımlayan açık bir standarttır (RFC 7519). JWT’deki bilgiler isteğe bağlı olarak bir gizli (secret) veya açık/gizli anahtar (*public/private key*) kullanılarak dijital olarak imzalanabilmektedir[10], [11].

JWT Yapısı

JWT Anahtarı noktalarla ayrılmış ve Base64URL ile kodlanmış karakter serileri halinde üç bölümden oluşmaktadır. Başlık (*Header*), Yük (*Payload*), İmza (*Signature*)[11], [12], [13].

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Şekil 7: Üretilmiş JWT anahtar örneği.

Başlık (*Header*)

JWT anahtarında ilk sırada yer alan başlık verisi, kullanılacak algoritmayı ve anahtar tipini (HMAC SHA256 veya RSA gibi) belirten iki farklı alandan oluşmaktadır. Örneğin; HS256 değeri HMAC-SHA256 ile şifrelendiğini gösterir.

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Şekil 8: JWT başlık (header) örneği.

Yük (*Payload*)

Anahtarı kullanacak taraflar arasında ihtiyaç duyulan verileri içeren bölümdür. Talepler (Claims) olarak belirtilen veriler üç farklı türe ayrılmıştır. Bunlar:

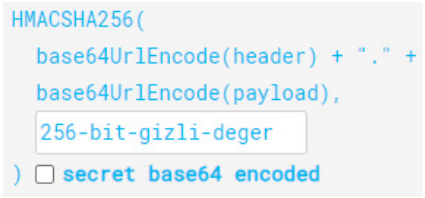
- **Kayıtlı (registered) talepler:** Zorunlu olmayan ancak kullanılması standart açısından tavsiye edilen bu talepler JWT’de ön tanımlı olarak belirlenmiş alanları içermektedir. Örnek olarak “exp”, “sub”, “iat” vb.
- **Açık (public) talepler:** Kayıtlı talepler gibi ön tanımlı alanlardan oluşmaktadır, ancak daha fazla değere sahiptir.
- **Gizli (private) talepler:** Anahtar değerini kullanacak taraflar (istemci/sunucu) arasında kullanılacak özel verileri içerir.

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

Şekil 9: JWT yük (payload) örneği.

İmza (*Signature*)

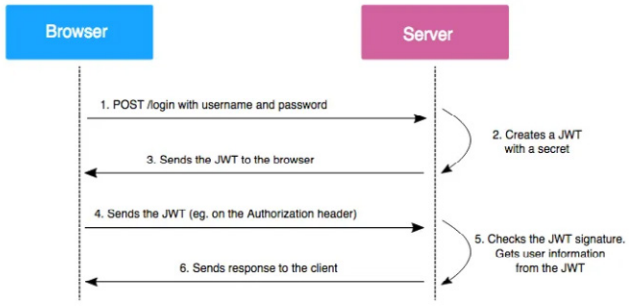
JWT anahtarının son kısmıdır. Bu kısmın oluşturulabilmesi için kodlanmış olarak başlık ve yük verisi ile birlikte uygulamaya özel bir gizli değer kullanılmalı ve imzalanmalıdır.



Şekil 10: HMAC SHA256 kullanılarak üretilecek imza (signature) örneği.

JWT Zayıf Gizli (*Secret*) Anahtar Kullanımı Kaynaklı Güvenlik Zafiyeti

JSON Web Token spesifikasyonu, geliştiricilerin yük taleplerini (*payload claims*) dijital olarak imzalamaları için çeşitli yollar sağlar. Bu, veri bütünlüğünü ve sağlam kullanıcı kimlik doğrulamasını garanti eder. Geliştiriciler HMAC imzalarını kullandıklarında, hem tokenları imzalamak hem de doğrulamak için kullanılan gizli (*secret*) bir anahtar temin etmeleri gerekmektedir. Bu gizli anahtar (*secret*) yeterince güçlü değilse, tüm imzalar ele geçirilebilir [13].

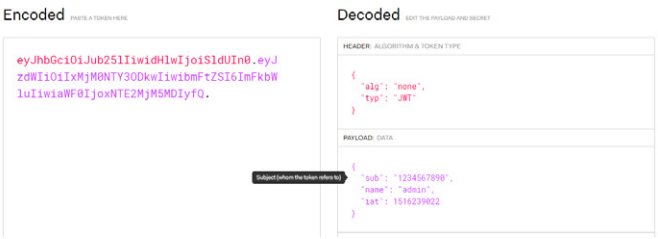


Şekil 11: JWT biçim/çalışma yapısı örneği.

Tüm JWT (JSON Web Token)'leri, sunucunun token imzasını doğrulamak için kullanması gereken algoritmayı belirten "alg" başlık parametresini içermelidir. Kriptoğrafik olarak güçlü algoritmalara ek olarak, JWT belirtimi ayrıca "unsecured" (unsigned) JWT'lerle kullanılabilen "none" algoritmasını da tanımlar. Bu algoritma sunucuda desteklendiğinde, hiç imzası olmayan tokenları kabul edebilir[14].

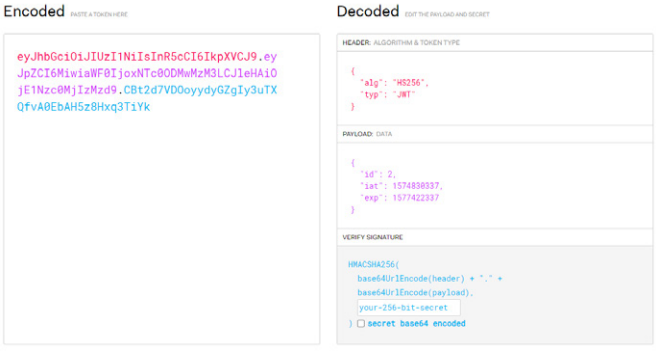
JWT başlığı istemci tarafında değiştirilebildiğinden, kötü niyetli bir kullanıcı "alg" başlığını "none" olarak değiştirebilir, ardından imzayı kaldırabilir ve sunucunun belirteci kabul edip etmediğini kontrol edebilir.

Kabul ederse, ayrıcalıklarını artırmak veya diğer kullanıcıları taklit etmek için JWT yükünde keyfi bir talep sağlayarak bu güvenlik açığından yararlanabilir. Örneğin, Şekil 1'de oluşturulmuş JWT token'a encode edilmiş, Şekil 2'de gösterilen belirteç bir "username": "joe" talebi içeriyorsa, bunu "username": "admin" olarak değiştirebilirler.

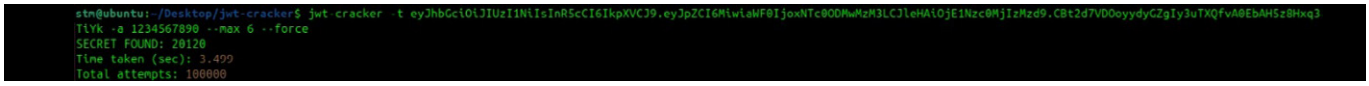


Şekil 12: "alg" başlığı "none" ve "paylod" içerisindeki "name" parametresi "admin" ile değiştirilerek oluşturulan JWT.

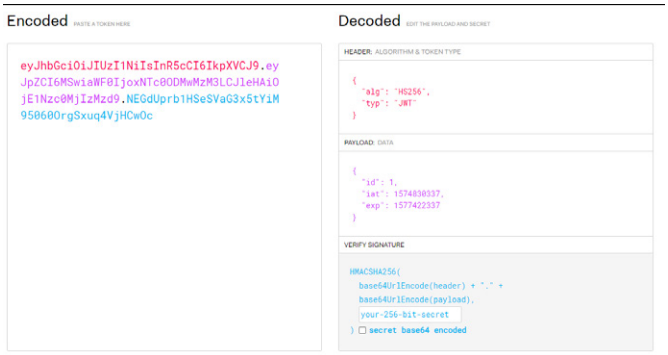
Geliştiriciler JWT anahtarı üreten kod parçasını yazarken bazen kolay tahmin edilebilir veya varsayılan değer (*default*) olarak bırakılan gizli anahtar (*secret*) kullanırlar. Saldırganlar, belirtilen yöntemlerle oluşturulan değeri kaba kuvvet (*brute force*) saldırılarıyla ele geçirebilir ve buldukları değeri kullanarak yeni yük bilgileriyle birlikte imzaladıkları JWT anahtar değerini sunucuya gönderebilirler[15].



Şekil 13: JWT token örneği.



Şekil 14: JWT İmza Anahtarına (Signing Key) Kaba Kuvvet (Brute Force) saldırısı gerçekleştirilmesi ve gizli anahtarın (secret) tespit edilmesi.



Şekil 15: Elde edilen gizli anahtar (secret) ile "id" parametre değeri "1" olan sahte bir JWT token oluşturulması.

Diğer Hususlar

- **Algoritma Karmaşası (*Algorithm Confusion*)**: Asimetrik bir algoritma için tasarlanmış bir sistem, bir JWT'yi HMAC simetrik algoritması veya "none" algoritması olarak işlemeye zorlanabilirse, geçerli bir JWT'nin kolayca sahtesi oluşturulabilir. Beklenmedik algoritmaların kabul edilmesini önlemek için onaylı algoritmaların bir beyaz listesi kullanılmalıdır[16].
- **Hassas İçerik *(Sensitive Content)***: JWT'ler base64URL ile kodlanmış olduğundan, kolayca çözülebilirler. Hassas veriler yük (payload) bölümünde depolanırsa, bu veriler kolayca ele geçirilebilir. Yük bölümü (payload), herkesçe erişilebilir verileri depolamak için kullanılmamalıdır.
- **Gizli Anahtar Açığa Çıkarılması (*Secret Disclosure*)** : Simetrik veya HMAC algoritması kullanımı durumunda, JWT token'ı oluşturmak ve doğrulamak için paylaşılan açık/gizli bir anahtar (*public/secret key*) kullanılır. Gizli (*Secret*) anahtarın istemci tarafından erişilen kod içerisinde bulunmaması veya kolayca tahmin edilebilir nitelikte oluşturulmaması gerekmektedir.
- **Key ID Saldırıları (*Attacks*)**: Key ID (kid) parametresi, kullanılan anahtara referansı içerir. Rastgele değerler kabul edilirse directory traversal ve Server-Side Request Forgery (SSRF) gibi saldırılara sebebiyet verebilir.

5. Türkiye'yi Hedef Alan APT Gruplarına Genel Bir Bakış

Gelişmiş Sürekli Tehditler (APT'ler), hedefe yönelik ve uzun süreli siber saldırılardır. Bu saldırılar, siber casusluk grupları tarafından ekonomik, politik ve stratejik avantajlar elde etmek amacıyla değerli bilgileri ele geçirmek için gerçekleştirilir. APT'ler, ulusal savunma, üretim ve finans gibi sektörleri hedefler ve fikri mülkiyet, askeri planlar ve kritik kaynaklar gibi yüksek değerli varlıkları odak noktası olarak alır.

Bu bölüm, Türkiye'deki APT faaliyetlerine odaklanmaktadır; ülkemizde APT olayları yaygın olmakla birlikte kamuoyuna açıklanan bilgiler sınırlıdır. Türkiye'deki şirketler, kritik altyapıyı ve hassas verileri korumak için siber güvenlik hizmet sağlayıcılarıyla işbirliği yaparak gizli tehdit istihbaratı toplama ve analiz etme süreçlerini uygulamaktadır.

Siber güvenlik uzmanları APT'lere karşı koymak için tehdit modellemesi adı verilen ve güvenlik açıklarını belirleyen, potansiyel etkileri ölçen ve koruyucu önlemleri önceliklendiren yapılandırılmış bir süreç kullanmaktadır. Siber hedeflemenin kilit aşamaları boyunca savunma stratejilerine rehberlik eden "siber ölüm zinciri" metodolojisinden de yararlanılmaktadır.

Yöntem

APT'leri tam anlamıyla kavrayıp onlara karşı savunma yapabilmek için açık kaynak istihbaratı (OSINT) ve tehdit aktörü profilleme ile taktik, teknik ve prosedür (TTP) analizi gibi çeşitli veri analiz teknikleri kullanılmıştır.

OSINT, web siteleri ve sosyal medya platformları gibi kaynaklardan kamuya açık bilgilerin toplanmasını içerir. Bu verileri analiz ederek APT gruplarının altyapısı, taktikleri ve olası hedefleri hakkında değerli bilgiler elde edilmiştir. Çalışma, Türkiye'yi hedef alan APT gruplarını tespit etmeye ve yapılan saldırıları OSINT kullanarak incelemeye odaklanmaktadır.

Ayrıca, Türkiye'deki APT faaliyetlerini anlamak için çeşitli raporlar ve yayınlar incelenmiştir. Tehdit istihbarat raporları ve akademik araştırmalar analiz edilerek gelişen trendler ve saldırı vektörleri hakkında bilgiler elde edilmiştir. Bu çalışmada, tehdit aktörü profilleri oluşturmak ve APT gruplarının TTP'lerini incelemek amacıyla raporlar ve yayınlar üzerinde bir analiz yapılmıştır. Tehdit aktörü profilleme, olası rakipler hakkında isim, açıklama, motivasyon, hedeflenen kurban ve hedefler gibi ayrıntılı profiller oluşturulmasına olanak tanır[17]. TTP analizi ise saldırganların saldırı sırasında kullandıkları taktikleri, teknikleri ve prosedürleri anlamamıza yardımcı olur. Bu teknikler, saldırganların düşünce yapısı ve yetenekleri hakkında pratik bilgiler sağlar ve daha bilinçli bir savunma stratejisi geliştirmek için kullanılabilir[18].

Türkiye'yi Hedef Alan APT Grupları

Siber güvenliğin dinamik ortamında, APT grupları, ulusal güvenlik için önemli bir tehdit oluşturmaktadır. Bu bölüm, MuddyWater, Cozy Bear, MurenShark ve StrongPity olmak üzere dört APT grubuna genel bir bakış sunmakta ve bu grupların geçmişleri, nitelikleri, TTP'leri (Taktikler, Teknikler ve Prosedürler) ve özellikle Türkiye'deki faaliyetleri bağlamında hedef aldıkları spesifik unsurlara odaklanmaktadır.

MuddyWater

MuddyWater, 2017'den beri aktiftir ve Türkiye de dahil olmak üzere Ortadoğu'ya odaklanmaktadır. Kesin bir

belirleme yapmak zor olsa da, grubun faaliyetleri İranlı tehdit aktörleriyle bağlantılı olduğunu düşündürmektedir. Türkiye'ye yönelik stratejik ilgisi, hükümet kurumları, telekomünikasyon ve kritik altyapı sektörlerini hedef almasıyla açıkça görülmektedir [19].

Cozy Bear (APT29)

Cozy Bear, 2010'ların ortalarından beri aktif olan ve Rus devleti tarafından desteklenen bir APT grubudur. Grubun, özellikle Rusya Dış İstihbarat Servisi'ne (SVR) bağlı Rus istihbarat kurumlarına atfedildiği bilinmektedir. Cozy Bear, dünya çapında faaliyet göstermekte ve sürekli saldırılar düzenlemektedir; bu saldırılarda oltalama, sıfır gün açıkları, özel zararlı yazılımlar ve araçlar kullanmaktadır. Hedefleri arasında hükümetler ve kritik altyapılar yer almaktadır [20].

MurenShark

MurenShark, nispeten yeni bir APT organizasyonu olup, Kuzey Kıbrıs'taki Yakın Doğu Üniversitesi gibi kuruluşları hedef alarak Türkiye'ye özel bir ilgi göstermektedir. Belirli bağlantılar açıkça belirtilmemiş olsa da, MurenShark'ın bağımsız faaliyetleri, Türkiye ve bölgesel dinamiklere odaklanan benzersiz bir profil sergilediğini göstermektedir. İleri düzey yetenekler kullanan grup, Türkiye'deki önemli kuruluşları, özellikle Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nu (TÜBİTAK) stratejik olarak hedef alarak fikri mülkiyet ve hassas verileri ele geçirmeyi amaçlamaktadır.

StrongPity

İlk olarak 2016 yılında gözlemlenen StrongPity'nin devlet destekli olduğu düşünülmekte ve dünya genelinde siber casusluk kampanyalarına katıldığı bilinmektedir. Kesin kökeni bilinmemekle birlikte, StrongPity, siyasi kuruluşları ve insan hakları örgütlerini hedef alan siber casusluk kampanyalarıyla ilişkilendirilmektedir. Watering hole saldırıları kullanmasıyla bilinen StrongPity, hedef kitlesinin sıkça ziyaret ettiği web siteleri üzerinden sistemleri ele geçirmek, hassas bilgileri çalmak ve kalıcı bir varlık sürdürmek amacıyla Truva atı zararlı yazılımını dağıtmaktadır. Hedefler arasında hükümet kuruluşları, sivil toplum örgütleri ve siyasi faaliyetler veya insan hakları savunuculuğu ile uğraşan kişiler yer almakta olup, bu faaliyetler Avrupa, Ortadoğu ve Kuzey Afrika'ya yayılmaktadır[21].

Vaka İncelemeleri

Bu bölüm, Türkiye'yi hedef alan bazı önemli APT kampanyalarının bir analizini sunmaktadır. Kampanyalar olarak APT29, MuddyWater ve MurenShark'ın geçmiş saldırıları ele alınmaktadır. Analiz sayesinde, bu gelişmiş tehdit aktörleri tarafından kullanılan taktiklerin, tekniklerin ve prosedürlerin nasıl evrildiği görülebilmektedir.

Örneğin, Mandiant ve Google'ın Tehdit Analiz Grubu (TAG) tarafından hazırlanan ortak bir rapor, APT29'un oltalama operasyonlarında bir artış olduğunun altını çizmekte, özellikle Ukrayna'nın karşı saldırısına kadar geçen süreçte ülkedeki yabancı büyükelçiliklerin hedef alındığını belirtmektedir. Raporda, Mart 2023'te Türkiye'de APT29 kampanyasında önemli bir gelişme yaşandığına dikkat çekilmekte ve *HTTP Smuggling* ile WordPress gibi ele geçirilmiş web hizmetlerinde ilk aşama yüklerin barındırılması gibi yöntemlerin kullanıldığı belirtilmektedir.

Türkiye'de, Şubat 2023 depremi sırasındaki kimlik avı saldırıları, APT29'un küresel olaylara uyarlanabilirliğini ve stratejik uyumunu ortaya koymuştur. Karmaşık saldırı taktikleri arasında sahte belgeler, kullanıcı aracısı filtreleme ve anti-analysis guardrails yer almakta olup, operasyonel güvenliği artırma ve tespit edilmekten kaçınma çabalarında kötü amaçlı yazılım dağıtımına yönelik dinamik ve gelişen yaklaşımı yansıtmaktadır [22].

Başka bir vakada, İran ile ilişkilendirilen devlet destekli bir tehdit aktörü olan MuddyWater grubunun yürüttüğü bir siber tehdit kampanyası incelenmiştir. Kampanya, yüksek düzeyde bir karmaşıklık sergilemiş ve Kasım 2021'e kadar Türkiye'deki hükümet kurumlarını, özellikle Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nu (TÜBİTAK) hedef almıştır. Saldırganlar, PDF olarak gizlenmiş kötü amaçlı Excel belgeleri ve çalıştırılabilir dosyalar kullanmış ve gizlenmiş VBA makroları, izleme belirteçleri ve zamanlama kontrolleri ile adaptasyon yeteneklerini göstermişlerdir. Enfeksiyon zinciri, gömülü bağlantılar içeren PDF'lerin dağıtımını içermiş, dinamik bir yaklaşımla zararlı XLS dosyaları ve Windows çalıştırılabilir dosyaları arasında değişiklikler yapılmıştır. Bu kampanyanın Türkiye'deki belirli kuruluşlara yönelik olması, MuddyWater'ın stratejik motivasyonlarını ve ısrarcılığını vurgulamaktadır[23]. Akademik araştırma, Türkiye'yi hedef alan bir APT grubu olan MurenShark tarafından düzenlenen siber casusluk kampanyasını da derinlemesine ele almaktadır. Bu kapsamlı gözlem, ele geçirilmiş sitelerin, özellikle Yakın Doğu Üniversitesi web sitesinin, çok yönlü dosya ve Komuta Kontrol (C&C) sunucuları olarak stratejik bir şekilde istismar edildiğini ortaya koymaktadır. MurenShark, ele geçirilmiş siteleri kullanırken hesaplı bir ihtiyat göstererek, operasyonel gizliliğin uzun süre korunmasına katkıda bulunmaktadır. Araştırma, saldırı bileşenlerini inceleyerek, gizliliği artıran ve adli analizleri zorlaştıran bir davranış ayırma modeli ortaya çıkarmaktadır. MurenShark'ın saldırıları, NiceRender, UniversalDonut, LetMeOut ve CobaltStrike gibi gelişmiş araçlar içermektedir. Dikkate değer bir vaka; MurenShark'ın Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na yönelik saldırısıdır. Oltalama e-posta taktikleri ve gelişmiş sızma yöntemleri ile işaretlenen bu saldırı, organizasyonun çeşitli tekniklerini vurgulamakta, hassas bilgileri toplamak amacıyla AgentTesla ve LetMeOut gibi Truva atı programlarını içermektedir. MuddyWater adlı başka bir APT grubu ile yapılan karşılaştırma, MurenShark'ın bileşen

tasarımındaki ve kaynak kullanımındaki titiz yaklaşımını ön plana çıkarmaktadır [24].

Sonuç

Günümüzde APT gruplarının tehdidi, ülkemiz de dahil olmak üzere küresel bir endişe kaynağıdır. Bu gruplar, taktik ve tekniklerini sürekli olarak geliştirmekte ve saldırılarını tespit etmeyi giderek daha zor hâle getirmektedir. Türkiye'yi hedef alan APT gruplarının kullandığı taktik, teknik ve prosedürler üzerinde odaklanmamız hayati önem taşımaktadır. Bu bilgi, hem organizasyonel hem de ulusal düzeyde etkili karşı önlemler uygulamak için gerekli olacaktır. Bu saldırıların karmaşıklığı arttıkça, bu büyüyen siber tehditlere karşı savunmamızı güçlendirmek için proaktif bir yaklaşım benimsemek gerekmektedir.

6. Gelişmiş Kimlik Doğrulama Yöntemleri ve Önemi

Dijital çağda, bilgi güvenliği her zamankinden daha kritik bir öneme sahiptir. Siber tehditlerin giderek daha sofistike hâle gelmesi, kişisel ve kurumsal bilgilerin korunmasını zorlaştırmaktadır. Bu bağlamda, kimlik doğrulama süreçlerinin güvenliği, veri korumanın temel taşlarından biri olarak ön plana çıkmaktadır. Geleneksel kimlik doğrulama yöntemlerinin yetersiz kaldığı durumlarda, gelişmiş kimlik doğrulama yöntemleri devreye girmektedir.

Şekil 16: Kimlik doğrulama.

Geleneksel Kimlik Doğrulama Yöntemleri

Geleneksel kimlik doğrulama yöntemleri genellikle kullanıcı adı ve şifre kombinasyonlarına dayanır. Ancak, bu yöntemlerde çeşitli güvenlik açıkları olması, şifrelerin çalınması, tahmin edilmesi veya paylaşılması söz konusu olabilmektedir. Bu nedenle, tek faktörlü kimlik doğrulama sistemleri, günümüzün siber tehditleri karşısında yetersiz kalmaktadır.

Gelişmiş Kimlik Doğrulama Yöntemleri

Çok Faktörlü Kimlik Doğrulama (MFA)

- Çok faktörlü kimlik doğrulama, kullanıcıların kimliğini doğrulamak için birden fazla bağımsız yöntem kullanır [25]. Bu yöntemler genel olarak üç ana kategori altında toplanır:
  - **Bilgi:** Kullanıcının bildiği şeyler (şifreler, PIN'ler).
  - **Sahiplik:** Kullanıcının sahip olduğu şeyler (telefonlar, akıllı kartlar).
  - **Biyometrik:** Kullanıcının fiziksel özellikleri (parmak izi, retina taraması).
- MFA, güvenliği artırarak tek bir doğrulama yönteminin başarısız olması durumunda ek bir güvenlik katmanı sağlar.
- **Biyometrik Kimlik Doğrulama:** Biyometrik kimlik doğrulama, kullanıcıların fiziksel ve davranışsal özellikleri temelinde kimliklerini doğrulamaktadır. Yaygın biyometrik yöntemler şunlardır:
  - *Parmak İzi Tanıma:* Kullanıcının parmak izlerini analiz edilerek kimliği doğrulanır.
  - *Retina ve İris Tarama:* Gözün retina veya iris desenlerini kullanılır.
  - *Yüz Tanıma:* Yüz hatları ve özellikleri analiz edilir.
- Biyometrik yöntemler, yüksek doğruluk oranları ve kullanıcı dostu olmaları nedeniyle tercih edilmektedir. Ancak, bu yöntemlerin de kısıtları ve gizlilik endişeleri söz konusudur.

Teknolojik Kimlik Doğrulama Yöntemleri

- **Akıllı Kartlar ve USB Anahtarlar:** Bu fiziksel cihazlar, güvenli bir kimlik doğrulama için donanım tabanlı çözümler sunmaktadır. Örneğin, bir USB anahtarına takılan bir şifreleme anahtarı, kullanıcı kimliğini doğrulamak için kullanılabilir.
- **OTP (One-Time Password) ve Token Sistemleri:** OTP, her giriş denemesinde yeni bir şifre sağlar. Token sistemleri ise fiziksel veya sanal bir cihaz kullanarak geçici şifreler oluşturur.

Davranışsal Analizler

Davranışsal analitikler, kullanıcının davranışsal kalıplarını analiz ederek kimliğini doğrular. Örneğin, bir kullanıcının klavye üzerindeki yazma tarzı veya mouse hareketleri incelenebilir. Bu yöntemle, kullanıcıların alışılmış davranışları tespit edilerek potansiyel sahteciliker belirlenebilir.

Gelişmiş Kimlik Doğrulama Yöntemlerinin Önemi

Gelişmiş kimlik doğrulama yöntemleri, veri güvenliğini artırarak çeşitli avantajlar sağlar:

- **Güvenlik Risklerini Azaltma:** MFA ve biyometrik yöntemler, kimlik hırsızlığı ve yetkisiz erişim gibi riskleri azaltır.
- **Kullanıcı Güveni:** Güçlü kimlik doğrulama yöntemleri, kullanıcıların sistemlere daha güvenli bir şekilde erişmesini sağlar.
- **Uyumluluk:** Birçok endüstri ve düzenleyici kuruluş, veri güvenliği ve kimlik doğrulama konusunda sıkı standartlar getirmiştir. Gelişmiş kimlik doğrulama yöntemleri, bu standartlara uyum sağlamada yardımcı olmaktadır.

Gelişmiş kimlik doğrulama yöntemleri, modern siber tehditlere karşı güçlü bir savunma mekanizması sunar. Tek faktörlü kimlik doğrulama yöntemlerinin yetersiz kaldığı durumlarda, MFA, biyometrik yöntemler ve diğer teknolojik çözümler, veri güvenliğini artırmak için yararlı olur. Bu yöntemlerin uygulanması bireylerin ve kuruluşların siber güvenliğini sağlamada önemli bir rol oynamaktadır. Dolayısıyla, kimlik doğrulama sistemlerinin düzenli olarak güncellenmesi ve iyileştirilmesi, siber tehditlere karşı en iyi korunma stratejilerinden biridir.

7. Lumma Stealer

Lumma Stealer, ilk kez 2022 yılında ortaya çıkan ve MaaS (Malware-as-a-Service) modeliyle satışa sunulan bir zararlı yazılımdır. Rusça konuşulan yer altı forumlarında ve Telegram kanallarında satılan Lumma Stealer, güncellemeler ve kullanıcı desteğiyle ilgili bilgilerle birlikte yaygınlaşmaktadır. C/C++ dillerinde yazılmış olan bu zararlı yazılım, LummaC adıyla da bilinir ve modern dağıtım yöntemleriyle geniş kitlelere ulaşmayı hedefler. Özellikle kimlik avı saldırıları, e-postaları, YouTube videolarındaki linkler ve LinkedIn üzerinden gerçekleştirilen saldırılar bu zararlının yayılmasında etkin rol oynamaktadır.

Lumma Stealer'ın asıl hedefi geniş bir veri yelpazesine ulaşarak kritik bilgileri ele geçirmektir. Tarayıcı çerezleri, kaydedilmiş şifreler, kripto para cüzdanları, FTP kimlik bilgileri gibi birçok hassas veri bu zararlı yazılımın hedefleri arasındadır. Kurbanın bilgisayarında bulunan diğer hassas verileri de ele geçirme kapasitesine sahip olan bu yazılım, saldırının boyutunu ve etkisini önemli ölçüde artırmaktadır. Lumma Stealer, sahte web sitesi güncellemeleri ve Google Play Store'da ChatGPT gibi yapay zekâ platformlarını taklit eden sahte uygulamalar aracılığıyla hedef sistemlere bulaştırılmaktadır[26]. Özellikle 2023 yılında popüler bir YouTuber'a yönelik bir saldırı, Lumma Stealer'ın kullanım alanlarının ne kadar yaygın olduğunu göstermiştir[27]: Bu olayda sahte Bandai Namco sponsorluk teklifiyle bir YouTuber hedef alınmış ve bir Dropbox linki aracılığıyla zararlı yazılım, hedef bilgisayara bulaştırılmıştır. Bu tür saldırılar, zararlı yazılım odaklarının geniş kitlelere ulaşmak için popüler çevrimiçi figürleri nasıl hedef aldığını göstermektedir.

Lumma Stealer, topladığı verileri Komuta ve Kontrol (C2) sunucusuna gönderir. Bu sunucuda verilerin şifresi çözülerek tespit edilmekten kaçınılır. Ayrıca, zararlı yazılım tespit edilmemek için dosya açıklamalarında genellikle crack'li yazılımlar veya meşru uygulamaların adlarını kullanmaktadır. Dosya açıklamalarında Ventoy, ASUSTeK Computer Inc., DupInOut Duplicate Finder gibi bilinen yazılımların isimleri kullanılarak, zararlı yazılımın meşru bir program gibi görünmesi sağlanmaktadır. Bu sayede kullanıcılar, sistemlerine crack'li bir yazılım indirdiklerini düşünürken zararlı bir yazılımı indirmektedir. Lumma Stealer, bu tür yöntemlerle antivirüs yazılımlarının dikkatini çekmemeyi ve geniş bir kitleye ulaşmayı hedeflemektedir.

Bu raporda zararlı yazılım analiz laboratuvarında incelenen 6PHM9GG3zOACOOY.exe Lumma Stealer zararlısına ait elde edilen bulgular verilmiştir.

Dosya bilgileri incelendiğinde, zararlı yazılımın kullanıcıları yanıltmak ve antivirüs yazılımlarından saklanmak amacıyla kendini "Ventoy" gibi yasal bir program olarak gösterdiği görülmektedir. Telif hakkı ve lisans bilgileri gibi yasal görüntüsü veren ayrıntılar eklenerek, dosyanın güvenilir bir yazılım olduğu izlenimi oluşturulmaktadır.

Anti-Debugging: Undhandled Exception Filter

Zararlı yazılım, çalıştığı sistemde bir debugger olup olmadığını tespit etmek için Unhandled Exception Filter mekanizmasını kullanmaktadır. Bu mekanizma, uygulamada yakalanmayan ve işlenmeyen istisnalarla ilgilenir [28]. Eğer programcı istisnayı işleme almazsa, işletim sistemi devreye girer ve programın güvenli bir şekilde sonlandırılmasını sağlar[29]. Programcı, bu mekanizmayı değiştirme imkânına sahiptir. Ancak, zararlı yazılım geliştiricisi UnhandledExceptionFilter fonksiyonunu maniple ederek, bu mekanizmayı kötüye kullanmış ve sistemin istismar edilmesine olanak vermiştir.

int 3 komutu, x86/64 mimarisinde bir kesme (*interrupt*) işlevi görür ve yazılımın debugger'da çalışıp çalışmadığına bağlı olarak iki farklı akışta ilerlemesini sağlar.

Zararlı yazılım bir debugger altında çalıştırıldığında, int 3 komutu debugger tarafından bir "breakpoint" olarak algılanır. Bu da yazılımın, bir debugger altında çalıştığını fark etmesine olanak tanır. Böyle bir durumda, zararlı yazılım herhangi bir zararlı faaliyet göstermeden kendini sonlandırır. Bu mekanizma, zararlı yazılımın analiz sürecinden kaçınmak için aldığı bir güvenlik önlemidir. Debugger ortamında çalıştığını fark eden yazılım, faaliyetlerini gizleyerek analizcilerin işini zorlaştırır ve zararlı kodun tespit edilmesini engeller.

Debugger olmayan bir ortamda çalıştırıldığında ise, int 3 komutuna ulaşıldığında, akış kötü niyetli geliştirici tarafından değiştirilmiş UnhandledExceptionFilter

fonksiyonuna yönlendirilir[30]. Yazılım, debugger bulunmadığını anladığında istisnayı kendi belirlediği şekilde işleyerek faaliyetlerine kesintisiz devam eder ve sistem üzerinde zararlı işlemlerini sürdürür.

Bu yapıyı atlatmak için, zararlı yazılımın kullandığı int 3 komutu, "no operation" anlamına gelen NOP (0x90) değeri ile patchlenmiştir, böylece anti-debugging tekniği etkisiz hâle getirilmiştir. NOP komutu, işlemciye herhangi bir işlem yapmamasını söyler ve programın akışını değiştirmez. Bu sayede, zararlı yazılımın debugger tarafından fark edilmesini sağlayan int 3 komutu devre dışı bırakılır. Böylelikle analizci, zararlı yazılımın anti-debugging korumalarını aşarak zararlı faaliyetlerini incelemeye devam edebilir.

FNV-1a (Fowler-Noll-Vo) 32-bit Hashing Algoritması

Zararlı yazılım, C2 sunucusuyla bağlantı kurmak için gerekli olan dll API'lerini FNV1-a hashing algoritmasının modifiye edilmiş bir versiyonuyla şifrelemiştir.

```
`
  v15 = v12 & 0xFFFFFFFC;
  v14 = 0xDCA9BCF;
  do
  {
    v16 = 0x1000193 * ((0x1000193 * ((0x1000193 * (v14 ^ *v9)) ^ v9[1])) ^ v9[2]);
    v17 = v9[3];
    v9 += 4;
    v14 = 0x1000193 * (v16 ^ v17);
    v15 -= 4;
  }
  while ( v15 );
}
```

Şekil 17: Zararlı yazılım tarafından modifiye edilmiş FNV-1a algoritması.

FNV-1a 32-bit hash'leme algoritmasında, başlangıç değeri olarak 0x811C9DC5 kullanılır. Ancak zararlı yazılımlar, algoritmanın tespitini zorlaştırmak için bu değeri değiştirerek modifiye edilmiş versiyonlarını tercih edebilir. Bu durumda, başlangıç değeri olarak 0xDCA9BCF kullanılmıştır. Standart FNV-1a algoritması, her bir bayta sırayla XOR işlemi uygulayıp, ardından FNV_PRIME ile çarparak 32 bitlik bir hash değeri oluşturur. Bu işlemler sırasında kullanılan 0xFFFFFFFF maskesi, sonuçların 32 bit sınırında kalmasını sağlar.

Zararlı yazılımın modifiye ettiği algoritmada ise performansı artırmak için veriler dört baytlık bloklar hâlinde işlenir. data_len & 0xFFFFFFFC ifadesiyle veri uzunluğu dört baytlık bloklara yuvarlanarak işleme alınır. Bu yöntem, özellikle büyük veri setlerinde hash işlemini hızlandırır. Aynı zamanda, kullanılan farklı başlangıç değeri ve blok bazlı işlem yaklaşımı, tespit araçlarının algoritmayı tanımasını zorlaştırır. Sonuç olarak, standart algoritma her baytı tek tek işleyerek çalışırken, modifiye edilmiş hâli performansı optimize ederek tespiti daha karmaşık hâle getirir.

Zararlı yazılım, bir API string'ini FNV-32 hash algoritmasıyla işleyerek bir hash değeri oluşturur. Bu hash değeri, fonksiyon çağrılmadan önce mevcut hash değeriyle karşılaştırılır. Eşleşme sağlandığında, fonksiyon sonlanır ve ilgili

Şekil 18: Dinamik API çözümleme işlemi.

API ismi geri döndürülür. Bu şifreleme algoritması, API isimlerinin doğrudan kullanılması yerine hash değerlerinin karşılaştırılmasını sağladığından, statik analiz araçları tarafından tespit edilmesini zorlaştırarak zararlı yazılımın gizlenmesine katkıda bulunur.

Algoritmanın kullandığı DLL'lerden biri olan winhttp.dll için kullanılan stringler ve hash değerleri:

WinHttpOpen 62B3486Bh	WinHttpConnect 0DFCB006Bh	WinHttpOpenRequest 496F8BF4h
WinHttpCrackUrl 0B0C94C10h	WinHttpSetTimeouts 2AB70A9h	WinHttpAddRequestHeaders 5B275FFFh
WinHttpSendRequest 0FAC074E6h	WinHttpReceiveResponse 53E744DBh	WinHttpQueryDataAvailable 687139C0h
WinHttpReadData 0B27C8613h	WinHttpWriteData 0DD44A73Ah	WinHttpCloseHandle 0E2D4035Bh

Tablo 1: WinHttp API string'leri ve hash değerleri.

Network

Zararlı yazılımın internet bağlantısı olmadığı zaman çalıştırıldığında, birden fazla sorgu yaptığı tespit edilmiştir. Özellikle mevcut C2 (*Command and Control*) sunucularından birinin kaldırılması veya erişilemez hâle gelmesi durumunda, yazılımın alternatif domain'lerle iletişime geçebilmesini sağlamak amacıyla bu çoklu sorgu mekanizması devreye girmektedir. Böylece, zararlı yazılım, C2 sunucularına kesintisiz bir şekilde bağlanmayı sürdürerek, komut ve kontrol akışını devam ettirebilir.

Zararlı yazılım internet bağlantısı altında çalıştırıldığında elde edilen bulgular:

Zararlı yazılımın yaptığı tüm request'ler incelendiğinde, enfekte olduğu sistemden topladığı verileri bir zip dosyasına dönüştürerek C2 sunucusuna ilettiği tespit edilmiştir. Request'lerin analizinde, zip dosyalarına ait "PK" magic header'ının bulunduğu tespit edilmiştir.

Bu durum, zararlı yazılımın topladığı bilgileri sıkıştırarak daha verimli bir şekilde ilettiğini ve olası veri sızıntısını gizlemek için zip formatını kullandığını ortaya koymaktadır. Bu yöntem, zararlı yazılımın hem veri aktarımını hızlandırmasını hem de analiz ve tespit süreçlerinden kaçınabilmesini sağlamaktadır.

Zararlı yazılım, "shinyearthtwio.shop" adlı komuta ve kontrol (C2) sunucusuyla bağlantı kurarak iletişimi

başlatmıştır. Sunucudan gelen yanıt "ok" olup, bu durum zararlı yazılımın başarılı bir şekilde sunucuyla bağlantı sağladığını ve request beklediğini göstermektedir.

Zararlı yazılım, bulaştığı sistemin user agent bilgilerini toplayarak bu bilgileri içeren POST istekleri göndermektedir.

Request'ler arasında HWID, PID, ACT VE LID gibi bilgiler bulunmaktadır. "lid=JangOo--" ifadesi, Lumma Stealer zararlı yazılımına ait bir build ID'sini temsil etmektedir. Bu ID, zararlı yazılımın C2 sunucusuna kendini tanıtma ve hangi versiyondan geldiğini bildirir.

Request'lerde gönderilen zip dosyaları incelendiği zaman elde edilen bilgiler:

Zararlı yazılım Chrome ve Edge tarayıcılarına ait çeşitli verileri toplayıp C2 sunucusuna iletmektedir. Bu veriler arasında çerezler, tarayıcı geçmişi, giriş bilgileri ve tarayıcı sürümü gibi bilgiler bulunmaktadır. Bu veriler .txt ve .sqlite dosyaları şeklinde kaydedilmiştir.

- Chrome ve Edge Tarayıcısına Ait Veriler:
  - Default
    - Network
      - Cookies
    - History
    - Login Data
    - Login Data For Account
    - Web Data
  - BrowserVersion.txt
  - dp.txt

SQLITE Browser ile analiz edilen sqlite3.dll dosyaları, zararlı yazılımın enfekte olduğu bilgisayardan çeşitli sorgu ve yanıtlar aracılığıyla kullanıcıya ait verileri topladığını göstermektedir. Bu veriler düzenlenerek C2 sunucusuna aktarılmaktadır.

C2 sunucusuna gönderilen diğer dosyalar:

- Processes.txt
- Software.txt
- Clipboard.txt
- Screen.png: Zararlı yazılım enfekte olduğu sistemde çalışırken ekran fotoğrafı almaktadır
- System.txt

System.txt dosyası incelendiğinde içerikte zararlı yazılımın sürüm bilgisi, kullanıcı ve bilgisayar detayları, antivirüs durumu (Windows Defender), donanım kimlikleri, RAM, CPU ve GPU gibi sistem özelliklerinin yer aldığı görülmektedir. LummaC2 derlenme zamanının 2 Ağustos 2024 olduğu bilgisi de system.txt dosyasına yazılmıştır.

Zararlı yazılım, Lumma Stealer'ın satış adresini 'txt' dosyasına ekleyerek, "telegram username: @lummanowork" şeklinde bir iletişim bilgisi sağlamıştır. Burada amaç, zararlı yazılımın geliştiricileri veya satıcılarıyla iletişim kurmak isteyen kişilere bir adres sağlamaktır.

Sonuç

Lumma Stealer, bulaştığı sistemlerde ciddi güvenlik riskleri oluşturan bir zararlı yazılımdır. Genellikle phishing (oltalama) yöntemleri ile yayılan bu zararlı yazılım, bulaştığı sistemlerde önemli bir tehdit oluşturarak kullanıcıların kritik verilerini hedef almaktadır.

Yapılan analizde, zararlı yazılımın anti-debugging teknikleri kullanarak analizden kaçınmayı hedeflediği tespit edilmiştir. Bu teknik, zararlı yazılımın tespit edilmesini ve analizini zorlaştırmaktadır. C2 sunucularını ve bu sunucular ile iletişimde kullanılan API'lerin çeşitli şifreleme algoritmalarıyla korunduğu gözlenmiştir. C2 sunucularında ".shop" uzantısının kullanıldığı görülmüş, Lumma Stealer'a ait diğer zararlı yazılımlarda ise ".site",".store", ".pics" ve ".homes" gibi farklı uzantılar kullanıldığı gözlemlenmiştir.

Zararlı yazılım, C2 sunucusuna istek yaparken "JangOo-- build id" değerini kullanmaktadır. Ancak Lumma Stealer'ın diğer varyantlarında farklı build id değerleri de kullanılabilmektedir. Lumma Stealer, bulaştığı sistemlerde özellikle Chrome ve Edge tarayıcılarından çerezler, tarayıcı geçmişi ve giriş bilgileri gibi hassas verileri ele geçirmektedir. Bunun yanı sıra, ekran görüntüleri, process'ler, yazılımlar ve sistem bilgileri gibi veriler de toplanarak C2 sunucusuna iletilmektedir.

Lumma Stealer, kritik verileri toplama ve iletme yeteneği ile önemli bir tehdit oluşturmaktadır. Tarayıcı tabanlı hassas verileri hedef alması ve gelişmiş şifreleme teknikleri kullanarak C2 sunucuları ile iletişim kurması, zararlı yazılımın etkisini artırmaktadır. Ayrıca, sistem dosyalarına Telegram satış adresi, derlenme zamanı bilgisi ve Lumma ID bilgisi ekleyerek saldırganlara kolaylık sağlamaktadır. Bu bulgular, Lumma Stealer'ın zararlı yazılım ekosisteminde gelişen ve yaygınlaşan bir tehdit olduğunu ortaya koymaktadır.

8. Event ve Incident Kavramlarının NIST Tanımlarıyla İncelenmesi

Bilgi güvenliği, günümüzde dijitalleşmenin etkisiyle organizasyonların en önemli önceliklerinden biri hâline gelmiştir. Bilgi sistemlerinin güvenliği, yalnızca verilerin korunmasıyla sınırlı kalmaz; bu sistemlerin düzgün çalışması, güvenlik tehditlerinin doğru bir biçimde tespit edilmesi ve yönetilmesi de kritik öneme sahiptir. Bu bağlamda, NIST (Ulusal Standartlar ve Teknoloji Enstitüsü), güvenlik olaylarını tanımlarken "event" ve "incident" kavramlarını ayırt etmek adına belirgin ve ayrıntılı tanımlar sunar. Her iki kavram da bilgi sistemlerinin güvenliğiyle doğrudan ilişkili olsa da, güvenlik yönetimi sürecinde farklı işlevlere ve öneme sahiptir. Bu çalışmada, NIST'in tanımları ışığında "event" ve "incident" kavramlarının güvenlik yönetimi süreçlerinde nasıl işlediği ayrıntılı olarak incelenecektir.

NIST'e Göre Event ve Incident Tanımları

NIST, güvenlik olaylarının yönetimi konusunda organizasyonlara rehberlik eden önde gelen referanslardan biridir. Özellikle NIST SP 800-61 (Computer Security

Incident Handling Guide) ve NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)[31] belgelerinde, güvenlik olaylarının tanımlanması ve yönetilmesi konusunda organizasyonlara ayrıntılı kılavuzluk sağlanmaktadır. NIST'e göre "event" ve "incident" kavramları birbirine bağlıdır, ancak her biri farklı türde olayları ve bu olaylara nasıl müdahale edilmesi gerektiğini ifade eder.

Event Tanımı

NIST'e göre "event" (olay), bir bilgi sisteminde meydana gelen herhangi bir durumu ifade eder. Bu durumlar, sistemin normal işleyişi sırasında ortaya çıkabilir ve her zaman güvenlik açısından tehdit oluşturmaz. NIST, "event" kavramını şu şekilde tanımlar:

"Event, bir bilgi sistemindeki her türlü değişiklik veya olaydır. Bu, bir kullanıcının sisteme giriş yapması, ağ trafiği, bir dosyanın açılması veya sistemin kapanması gibi olaylar olabilir"[32].

Yani, "event"ler, sistemin günlük işleyişinin doğal bir parçasıdır. Organizasyon, bilgi sistemlerinin düzgün işleyip işlemediğini izlemek amacıyla sürekli olarak bu olayları gözlemler. Çoğu durumda, event'ler zararsız olabilir. Örneğin, bir yazılım güncellemesinin başarıyla tamamlanması, bir kullanıcının sisteme giriş yapması ya da rutin bakım sırasında sistemin kapanması gibi olaylar event olarak kabul edilir. Bu tür durumlar bilgi güvenliği açısından tehdit oluşturmaz; ancak sistem performansını izlemek ve potansiyel tehditleri belirlemek amacıyla izlenir.

Event'ler, aynı zamanda organizasyonun bilgi sistemlerinin güvenlik durumu hakkında değerli bilgiler sunar. Ancak her event'in güvenlik açığı oluşturmadığı göz önünde bulundurulmalıdır. Örneğin, ağ trafiğinde bir anomali tespit edilmesi, bir event olabilir; fakat bu her zaman güvenlik ihlali anlamına gelmez.

Adverse Event (İstenmeyen Olay) Tanımı

NIST, event kavramını daha detaylı bir şekilde ele alarak "adverse event" (istenmeyen olay) terimini tanımlar. Adverse event, sistemlerin beklenen ve normal işleyişini ters yönde etkileyen olaylardır. Bu tür olaylar doğrudan bir güvenlik tehdidi oluşturmasa da, sistemin genel sağlığını ve performansını tehlikeye atabilirler. NIST'e göre, adverse event'ler "bilgi sisteminin düzgün çalışmasını engelleyebilecek ve potansiyel olarak zararlı etkiler yaratabilecek olaylar" olarak tanımlanabilir.

Adverse event'ler, kötüye kullanım veya kötü sonuçlar oluşturan olaylar olmasa da organizasyonların performansını etkileyebilir ve bu da bir incident'ın habercisi olabilir. Örneğin, bir donanım bileşeninin arızalanması, yazılım hataları veya ağ bağlantısındaki yavaşlamalar, bir adverse event olarak kabul edilebilir. Bu tür olaylar, sistemin genel güvenliğine yönelik potansiyel riskler oluşturabileceğinden, izlenmeli ve gerektiğinde müdahale edilmelidir. Adverse event'ler, genellikle izleme ve performans değerlendirme süreçlerinde tespit edilir ve organizasyonun dikkatini çeker.

Incident Tanımı

Incident (güvenlik olayı), daha spesifik bir güvenlik ihlali durumunu ifade eder. NIST'e göre bir incident, "bilgi güvenliği yönetim sistemi ile ilgili, organizasyonun bilgi güvenliğini tehlikeye atan veya zarar veren bir durumdur." (NIST SP 800-61). Bu tanım, bilgi sisteminin güvenlik mekanizmalarının ihlal edildiği veya sistemin işlevselliğinin tehdit altına girdiği bir durumu ifade eder.

Incident'lar genellikle ciddi güvenlik tehditlerine yol açar ve bu durumlar acil müdahale gerektirir. Örneğin, bir ransomware saldırısı, veri sızıntısı, yetkisiz erişim, hizmet kesintisi veya kötü amaçlı yazılım (*malware*) saldırıları gibi durumlar, birer güvenlik incident'ıdır. Incident'lar, organizasyonun bilgi güvenliğine zarar verebilir ve genellikle büyük etkiler yaratır. Örneğin, veri kaybı, kritik bilgilere yetkisiz erişim veya hizmet kesintileri organizasyonun iş süreçlerini doğrudan etkileyebilir. Bu tür olaylar sadece bilgi güvenliğini değil, organizasyonun itibarını, müşteri güvenini ve finansal durumunu da tehlikeye atabilir. NIST'e göre, incident yönetimi hızlı müdahale ve çözümleme süreçlerini başlatmayı gerektirir.

Event ve Incident Arasındaki Farkları Anlamak

Event ve incident kavramları, çoğu zaman karıştırılabilir veya birbirinin yerine kullanılabilir. Ancak NIST'in tanımlamaları, bu iki kavram arasındaki farkları net bir şekilde ortaya koymaktadır. Event ve incident arasındaki temel farkları anlamak, her iki kavramın güvenlik yönetimindeki rollerini doğru kavrayabilmek açısından oldukça önemlidir.

Olaya Müdahale Süreci

Event, organizasyonun bilgi sistemlerinin izlenmesi sırasında meydana gelebilecek ve potansiyel bir güvenlik tehdidi taşımayan durumlardır. Yani, sistemin verimliliğini değerlendirmek ve günlük operasyonları yönetmek amacıyla yapılan işlemler sonucu meydana gelen olaylardır. Event'ler, organizasyonun bilgi güvenliği yönetimi çerçevesinde izlenir. Örneğin, bir kullanıcının sisteme giriş yapması bir event oluşturur, ancak bu durum her zaman tehdit anlamına gelmez.

Buna karşılık, incident, organizasyonun güvenlik önlemlerinin ihlal edilmesi veya sistemin güvenliğinin tehdit altına girmesi durumudur. Incident'lar genellikle çok daha kritik ve acil müdahale gerektiren durumlardır. Örneğin, bir sistemin hack'lenmesi, verilerin çalınması veya bir ransomware saldırısının gerçekleşmesi gibi olaylar birer güvenlik incident'ıdır. Incident'lar, önemli zararlar

verebilir ve organizasyonun itibarını ciddi şekilde zedeleyebilir ve bu yüzden anında müdahale gerektirir.

Müdahale Zamanı ve Etkileri

Event'ler, genellikle anında müdahale gerektirmez ve izlemekle yetinilir. Bu olaylar, sistemin güvenlik durumu hakkında bilgi edinmek ve gelecekteki potansiyel tehditleri anlamak amacıyla analiz edilir.

Ancak incident'lar, anında müdahale gerektiren olaylardır. Güvenlik incident'ları, organizasyonun güvenliğini doğrudan etkileyen olaylardır ve çoğu zaman güvenlik politikalarını ihlal ederler. Bu tür bir durumda, sistem yöneticisi veya güvenlik ekibi hızla müdahalede bulunmalı, olası zararları minimize etmeli ve sistemin güvenliğini yeniden sağlamak için adımlar atmalıdır.

Event ve Incident Yönetimi Süreçleri

NIST, event ve incident yönetimi süreçleri için kapsamlı rehberlik sunar. Organizasyonların bu tür güvenlik olaylarını etkili biçimde yönetebilmesi için NIST'in önerdiği süreçleri doğru uygulamaları önemlidir.

Event Yönetimi

Event yönetimi, bilgi sistemlerinde günlük operasyonların izlenmesi, sistem performansının değerlendirilmesi ve olası güvenlik tehditlerinin tespit edilmesi sürecidir. NIST, event yönetimi sürecinde organizasyonların şu adımları izlemelerini önermektedir:

- **İzleme**: Sistemlerin ve ağların sürekli izlenmesi, eventlerin doğru bir şekilde toplanıp analiz edilmesi.
- **Günlük Kaydı**: Olay günlüklerinin toplanması ve incelenmesi, tehditlerin tespit edilmesine yardımcı olabilir.
- **İzleme ve Yanıt**: Event'lerin izlenmesi ve potansiyel tehditlerin tanımlanması.

Incident Yönetimi

Incident yönetimi, güvenlik tehditlerine anında müdahale ve çözümleme sürecini ifade eder. NIST'e göre, bir güvenlik incident'ı tespit edildiğinde organizasyonların şu adımları izlemeleri gerekmektedir:

- **Tespit Etme**: En başta, eventin analiz edilmesi ve incident olup olmadığının belirlenmesi.
- **Yanıt Verme**: Bir incident tespit edildiğinde, hemen müdahale edilerek zararların minimize edilmesi.
- **İyileştirme**: Olayın ardından, sistemin ve güvenlik önlemlerinin iyileştirilmesi gerekir.

Sonuç

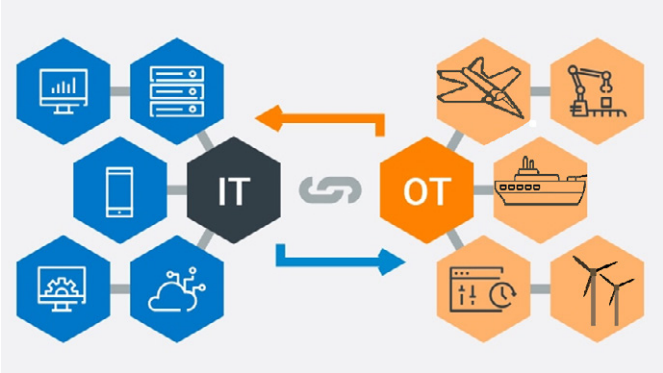
NIST'in event ve incident tanımları, bilgi güvenliği yönetim süreçlerinde kritik bir rol oynamaktadır. Event'ler, sistem izleme ve analiz süreçlerinin bir parçası iken, incident'lar ciddi güvenlik ihlallerini ifade eder ve acil müdahale gerektirir. Bu kavramların doğru bir şekilde anlaşılması, organizasyonların güvenlik yönetim süreçlerini daha etkin bir şekilde oluşturmalarına yardımcı olur. NIST'in rehberliği, organizasyonlara güvenlik olaylarını etkili bir biçimde yönetme yeteneği kazandırarak güvenlik önlemlerinin güçlendirilmesine katkı sağlar.

DÖNEM KONUSU

9. Bilgi Teknolojileri (IT) ve Operasyonel Teknolojilerin (OT) Farklı Siber Güvenlik Öncelikleri

Bilgi teknolojileri (IT) ve Operasyonel Teknolojiler (OT) farklı dinamikleri olan ancak zamanla beraber çalışma yetenekleri artan sistemlerdir. Bu sistemlerden bazıları Şekil 19'da gösterilmiştir.

Bilgi teknolojileri (IT) ve Operasyonel Teknolojiler (OT) hizmet sunmaya çalıştıkları alanlar özelinde farklı güvenlik önceliklerine sahiptir. OT sistemler genel olarak güvenilirlik (*safety*) odağında insan, çevre ve üretim süreçleri üzerinde daha büyük risklere sahiptir. Dolayısıyla uygulanan güvenlik kontrolleri güvenilirliği başa alır. Askeri alanda kullanılan gemi, uçak vb. platformlarda bu önceliklerin yanı sıra öncelik görevin (*mission*) yerine getirilmesidir. IT sistemlerinde ise öncelik, çevre ile olan fiziksel etkileşimden daha çok verinin gizliliği, bütünlüğü ve erişilebilirliği üzerine yoğunlaşmıştır.



Şekil 19: IT ve OT sistemler.

Siber güvenlik önemleri alınırken OT ve IT sistemler arasındaki göz önünde bulundurulması gereken temel farklılıklar şunlardır:

- OT sistemlerin gerçek zamana yakın çalışma göstermeleri beklenir. Söz konusu olan fiziksel ortam etkileşimi olduğu için gecikmelere karşı tolerans çok düşüktür. Bir OT sistemin güvenilirlik (*reliable*) ve her zaman beklenen doğru sonucu beklenen sürede verecek şekilde (*deterministic*) çalışması beklenir. IT sistemlerde gecikmeler karşı sistemin gereksinimlerine göre değişmekle beraber genel olarak OT sistemlere göre daha yüksek bir tolerans mevcuttur. Bu durumun sonucu olarak da OT sistemlerde gerçek zamanlı işletim sistemleri (RTOS) tercih edilmektedir.
- IT sistemler yüksek veri aktarımı gereksinimi önceliklendirmekte ve gecikmelere (Delay) karşı daha yüksek toleransa sahiptir. OT sistemlerde kararlı veri iletimi daha kritiktir. Verinin gönderimi esnasında uygulanacak güvenlik kontrolleri gecikmelere neden olmamalıdır.
- IT sistemler öncelikli olarak veri gizliliği (*confidentiality*) ve bütünlüğü (*integrity*) konularına odaklanmaktadır. OT sistemlerde güvenirlilik (*safety*) daha ön plana çıkmakta ve güvenlik (*security*) ile güvenilirlik (*safety*) ilişkisinin iyi anlaşılması büyük önem arz etmektedir. Güvenlik endişeleri güvenilirlik konusunda herhangi bir ihlale sebep olmamalıdır.
- OT sistemler bünyesinde kullanılan cihazların doğrudan fiziksel etkileri olmasından dolayı yapılan çalışmalarda OT sistem uzmanlarının fiziksel ortamları yöneten operatörlerle önemli düzeyde iletişimlerinin olması gerekmektedir. IT sistemlerde ise verinin kritikliğinin belirlenmesinden sonra varlık sahibiyle olan iletişim sınırlı kalmaktadır.
- OT sistemler güncellemelerin zor ve maliyetli olmasından dolayı genel olarak daha eski yapılar içermektedir. Bu yapılar 15 yıldan daha uzun kullanım sürelerine sahiptir. Bu sistemlerle ilgili geniş bilgi kaynaklarına ulaşmak her zaman pek mümkün olmayabilir. Bunun yanında bu yapılar eski olmalarının ve tasarımlarında güvenlik unsurlarının düşünülmemiş olmasından dolayı birçok noktada güvenlik eksiklikleri içermektedir. Şifreleme, kimlik doğrulama, yetkilendirme bu eksikliklerden bazılarıdır. IT sistemlerin kullanım süresi 3-5 yıl aralığında olup şimdilik daha güncel olmasından dolayı birçok güvenlik özelliğini bünyesinde barındırmaktadır. Gerekli görülen güvenlik özellikleri de IT sistemlerinin güncel ve yaygın yapısından dolayı kolayca entegre edilebilmektedir.
- OT sistemler çok geniş coğrafyalara dağılmış şekilde de olabilirken IT sistemler daha merkezi bir konumda bulunur. Bu durum OT sistemler için fiziksel güvenliği ve olaylara müdahaleyi zorlaştırabilmektedir.
- IT sistemlerinde hem üreticilerin hem de NIST, CIS, CSA vb. kuruluşların siber güvenlik ile ilgili birçok yönlendirici dokümanı bulunmaktadır. OT sistemlerde bu kaynaklar daha kısıtlı olmakla beraber en yaygın kullanılan siber güvenlik standardı ISA 62443 ailesidir. Bu standart çerçevesinde OT sistemlerde uygulanması beklenen temel gereklilikler Tablo 2'de gösterilmiştir. Bu gereksinimler daha detaylı güvenlik gereksinimlerine ayrılarak kullanılmaktadır.

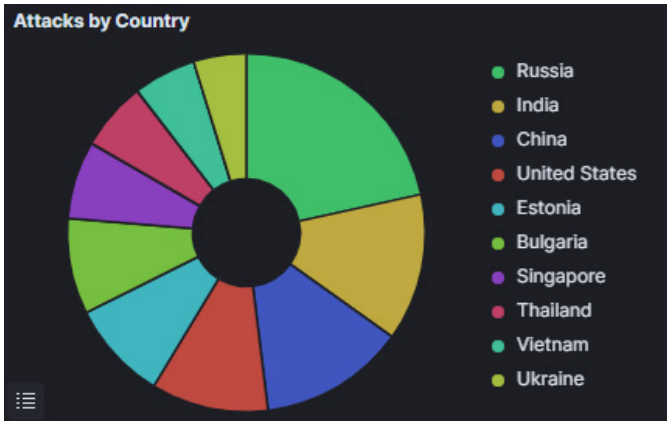
Temel Gereksinimler (IEC 62443)	Açıklama
Kimlik Tanımlama ve Kimlik Doğrulama	Tüm kullanıcıların (insanlar, yazılım süreçleri ve cihazlar) sistemlere erişmeye çalışırken güvenilir şekilde tanımlanmasını ve doğrulanmasını sağlar.
Erişim Kontrolü	Kimliği doğrulanmış kullanıcıların (insan, yazılım süreci veya cihaz) sisteme veya varlıklara istenen işlemi uygulamak için atanan ayrıcalıkların uygulanmasını sağlar. Bu ayrıcalıkların kullanımını izler.
Sistem Bütünlüğü	Sistemin bütünlüğünü sağlar ve yetkisiz manipülasyonu önler.
Veri Gizliliği	İletişim kanallarındaki ve veri depolarındaki bilgilerin gizliliğini sağlar. Yetkisiz ifşaları önler.
Kısıtlı Veri Akışı	Gereksiz veri akışını sınırlamak için kontrol sistemini bölgeler ve kanallar aracılığıyla bölümlere ayırır.
Olaylara Zamanında Yanıt	Güvenlik ihlallerine yanıt verir, yetkili mercileri bilgilendirir ve ihlalin kanıtlarını rapor eder. Olay sırasında zamanında düzeltici eylemler alır.
Kaynakların Kullanılabilirliği	Temel hizmetlerin bozulmasına veya servis dışı kalmasına karşı kontrol sisteminin kullanılabilirliğini sağlar.

Tablo 2: IEC 62443 temel gereksinimler.

OT ve IT sistemler ilk başlarda birbirlerinden tamamen izole şekilde çalışmakta ve OT sistemlerle özel protokollerle veri iletişimi geçekleştirilmekteydi. Zamanla Ethernet, IP ve kablosuz ağlar gibi maliyeti düşük teknolojilerin kullanılmasıyla OT ve IT sistemler benzerlikler göstermeye başladı. Bu yeni teknolojiler OT sistemlere uzaktan erişim gibi yeni yetenekler kazandırırken beraberlerinde siber güvenlik risklerini de getirmiştir. IT ve OT sistemlerin entegre çalıştıkları yapılarda bu entegrasyonun getirdiği riskler göz önünde bulundurularak risk analizi sonucu belirlenen kontroller uygulanmalıdır. Burada unutmaması gereken ve her iki sistem için geçerli olan bir başka konu da tedarik zinciridir. Son zamanlarda meydana gelen ve ölümle sonuçlanan bu tür saldırıları engellemek için her iki tür sistemde de gereken tedarik zinciri tedbirleri uygulanmalıdır.

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. Temmuz, Ağustos ve Eylül 2024 ayları boyunca honeypot sensörlerimize toplam 1.583.206 saldırı gelmiştir.



Şekil 20: Gelen saldırıların ülkelere göre dağılımı.

Toplanan veriler incelendiğinde, en çok saldırı gelen 10 ülke arasında ilk sırada Rusya (yüzde 21,57) olduğu, ardından sırasıyla Hindistan (yüzde 13,30), Çin (yüzde 13,19), ABD (yüzde 10,58) ve Estonya'nın (yüzde 9,01) yer aldığı görülmektedir.

Saldırıların Geldiği Ülke	Saldırı Sayısı
Rusya	204.709
Hindistan	126.184
Çin	125.164
ABD	100.435
Estonya	85.459
Bulgaristan	81.895
Singapur	66.772
Tayland	59.056
Vietnam	54.142
Ukrayna	45.182

Tablo 3: En çok saldırı gelen 10 ülke ve saldırı sayıları.

Tablo 4'te 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 girişimlerinden oluşmaktadır.

Saldırılan Port	Saldırı Sayısı
445 - SMB	401.261
5900 - VNC	390.981
22 - SSH	82.498
25 - SMTP	38.551
23 - Telnet	14.573
1080 - SOCKS Proxy	3.161
80 - HTTP	1.706
5555 - ADB	1.437
21 - FTP	787
5432 - PostgreSQL	496

Tablo 4: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Denenen Parola	Deneme Sayısı
123456	6.391
345gs5662d34	5.382
3245gs5662d34	5.380
123	2.906
admin	1.546
password	1.459
12345	910
1234	836
12345678	818
(boş)	784

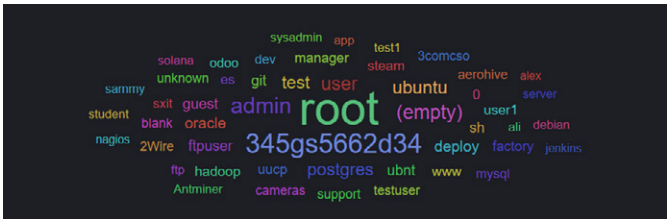
Tablo 5: SSH ve RDP honeypot'larımız üzerinde en çok denenen parolalar ve deneme sayıları.

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.

Şekil 21: Parola etiket bulutu.

Denenen Kullanıcı Adı	Deneme Sayısı
root	25.386
345gs5662d34	5.382
admin	2.889
(boş)	1.599
user	1.315
ubuntu	1.040
test	948
postgres	909
oracle	480
deploy	364

Tablo 6: SSH ve RDP honeypot'larımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.



Şekil 22: Kullanıcı adı etiket bulutu.

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] R. Putrus, "Best Practices for Setting Up a Cybersecurity Operations Center," 27 August 2021. [Çevrimiçi]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/best-practices-for-setting-up-a-cybersecurity-operations-center?gad_source=1&gclid=CjwKCAjw6c63BhAiEiwAF0EH1ERnTJzwMDyupF0lFOoxqdtJ0ycP7aFdmLFc0zxJwHKAMdLeg0rcHhoC_kQQAvD_BwE.

[2] Gartner, "soc-triad," 18 3 2019. [Çevrimiçi]. Available: https://cdn.prod.website-files.com/64e50cbe2b6f932c04238c14/65d87563e02e44294dcef543_SOC-visibility-triad.webp.

[3] "OWASP Top Ten," 2021. [Çevrimiçi]. Available: https://owasp.org/Top10/.

[4] S. Thomas, "xvwa," [Çevrimiçi]. Available: https://github.com/s4n7h0/xvwa.

[5] M. Russinovich ve T. Garnier, "Sysmon v15.15," 23 July 2024. [Çevrimiçi]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon.

[6] https://www.synopsys.com/blogs/software-security/why-cross-site-scripting-still-matters.html

[7] https://edg.io/technical-articles/cross-site-scripting-attacks-trends-and-best-practices/

[8] https://www.cisa.gov/news-events/alerts/2024/09/17/cisa-and-fbi-release-secure-design-alert-eliminating-cross-site-scripting-vulnerabilities

[9] https://www.bleepingcomputer.com/news/security/cisa-urges-software-devs-to-weed-out-xss-vulnerabilities/

[10] "RFC Editor," 08 Eylül 2023. [Çevrimiçi]. Available: https://www.rfc-editor.org/rfc/rfc7519.

[11] "STM ThinkTech," STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., 16 Kasım 2023. [Çevrimiçi]. Available: https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-temmuz-eylul-2023.

[12] "jwt.io," 8 Eylül 2023. [Çevrimiçi]. Available: https://jwt.io/.

[13] "PortSwigger," 20 Eylül 2024. [Çevrimiçi]. Available: https://portswigger.net/kb/issues/00200903_jwt-weak-hmac-secret.

[14] "akto.io," 20 Eylül 2024. [Çevrimiçi]. Available: https://www.akto.io/blog/jwt-none-algorithm-test.

[15] "auth0.com," 20 Eylül 2024. [Çevrimiçi]. Available: https://auth0.com/blog/brute-forcing-hs256-is-possible-the-importance-of-using-strong-keys-to-sign-jwts/.

[16] "Qualys Community," 16 Ekim 2022. [Çevrimiçi]. Available: https://blog.qualys.com/qualys-insights/2022/10/11/json-web-token-jwt-weaknesses.

[17] S. Irwin, "Creating a Threat Profile for Your Organization," 2014.

[18] [Çevrimiçi]. Available: https://www.maltego.com/blog/analyzing-attack-patterns-and-ttps/ .

[19] [Çevrimiçi]. Available: https://attack.mitre.org/groups/G0069/.

[20] [Çevrimiçi]. Available: https://attack.mitre.org/groups/G0016/.

[21] [Çevrimiçi]. Available: https://attack.mitre.org/groups/G0056/.

[22] [Çevrimiçi]. Available: https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing#:~:text=In%20March%202023%2C%20Mandiant%20identified,earthquake%20that%20struck%20southern%20T%C3%BCrkiye.

[23] [Çevrimiçi]. Available: https://blog.talosintelligence.com/iranian-apt-muddywater-targets-turkey/.

[24] [Çevrimiçi]. Available: https://nsfocusglobal.com/investigation-report-on-new-apt-organization-.

[25] Burr, William E., et al. Electronic Authentication Guideline. National Institute of Standards and Technology, 2006.

[26] https://protergo.id/hackers-use-fake-chatgpt-apps-to-push-windows-android-malware/

[27] https://medium.com/s2wblog/lumma-stealer-targets-youtubers-via-spear-phishing-email-ade740d486f7

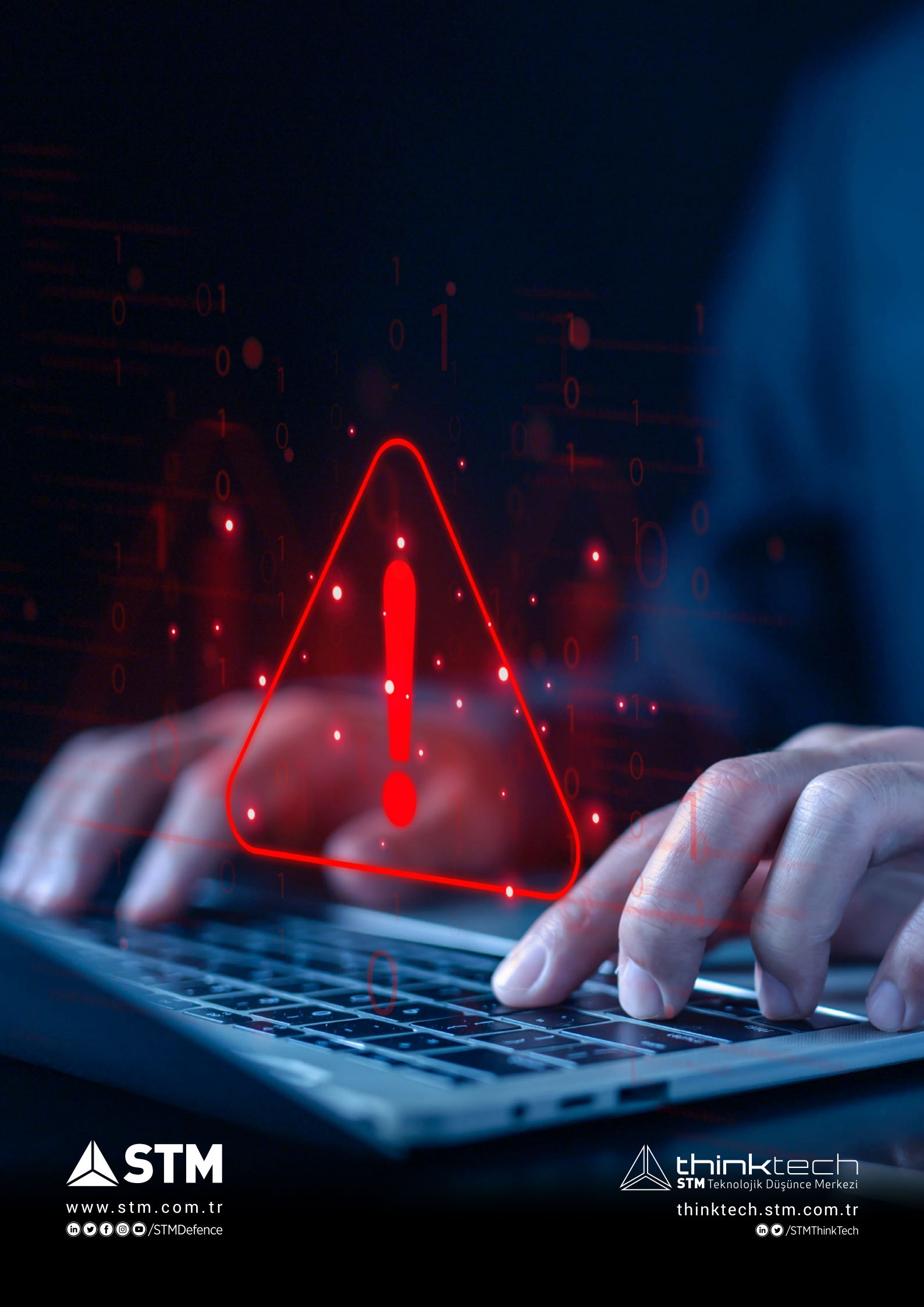
[28] https://medium.com/@meryemahiskali2/bir-anti-debugging-tekni%C4%9Fi-olarak-unhandledexceptionfilter-int-3- cb3c0f2ec3e1

[29] https://learn.microsoft.com/en-us/windows/win32/api/errhandlingapi/nf-errhandlingapi- setunhandledexceptionfilter

[30] https://anti-debug.checkpoint.com/techniques/exceptions.html

[31] NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

[32] NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide https://csrc.nist.gov/pubs/sp/800/61/r2/final



STM
www.stm.com.tr
/STMDefence

thinktech
STM Teknolojik Düşünce Merkezi
thinktech.stm.com.tr
/STMThinkTech