Türk Telekom Siber Bülten

Nisan 2022
5. Sayı

Türk Telekom Güvenlik

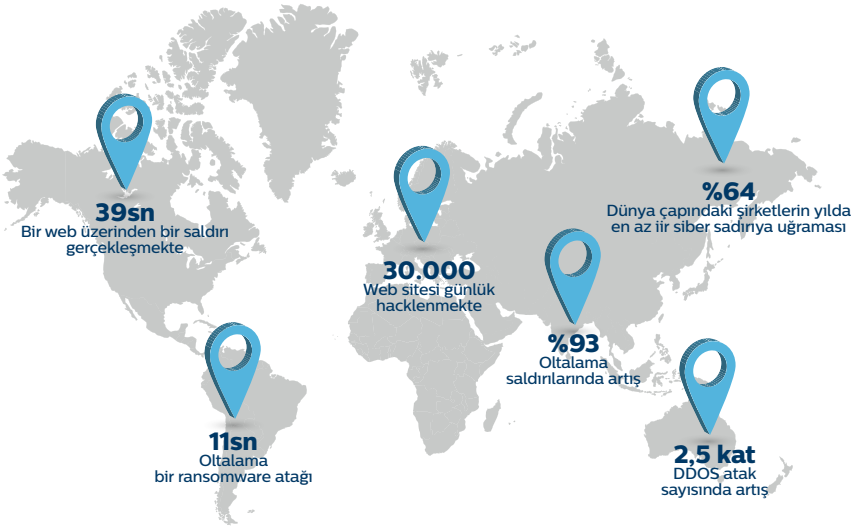
Türk Telekom
Değerli Hissettirir

İçindekiler

Yönetici Özeti

Global Atak Trendleri

2021 Yılı Atak Trendleri



2021 Yılı Yaşanan En Büyük Ataklar

Nisan 2021'de bir bilgisayar korsanlığı forumu üzerinden 533 milyon Facebook kullanıcısına ait kişisel veriler yayınlandı.

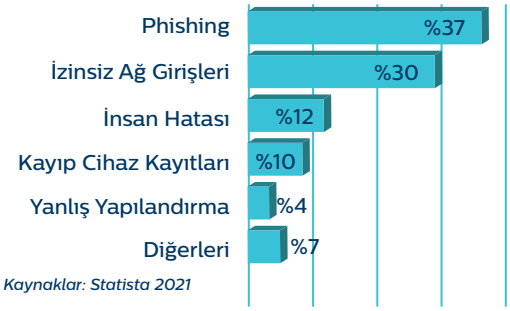
Bilgisayar korsanlarının API'den yararlanarak ulaştıkları 700 milyon Linkedin kullanıısı verileri Haziran 2021'de dark web üzerinden satışa çıktı.

4 farklı zero-day atağın Microsoft Exchange sunucularında keşfedilmesiyle kötü niyetli kişiler kullanıcı e-mail ve parolalarına tam erişim sağladı. Saldırıdan 250 bin sunucunun etkilendiği tahmin ediliyor.

Microsoft Exchange sunucularındaki zafiyetten yararlanarak Acer'ın finansal ve hassas dosyalarına erişen Reval hacker grubu 50 milyon dolarlık fidye talep etti.

Sigorta şirketi CNA Financial'ın, Mart ayında gerçekleşen bir siber saldırı sonrası, çalınan bilgileri geri alabilmek ve sisteme tekrar erşim sağlayabilmek için 40 milyon dolar fidye ödedi.

En Yaygın Atak Deneyimleri



Kaynaklar: Statista 2021

En Çok Atak Alan Sektörler

- Finans
- Bilişim ve İletişim Teknolojileri
- Üretim
- Perakende
- Sağlık

Türk Telekom Atak İstatistikleri

DDOS Atak Önleme

En Yüksek Atak Boyutu

320 Gbps

En Çok Atak Alan 5 Sektör

- Telekomünikasyon -%40
- Veri Merkezi -%15,7
- Kamu – %13,6
- Bilişim -%10,8
- Finans ve Bankacılık - %5

Atak Sayıları

4.141
1Gbps+ üzeri atak sayısı

	Gelişmiş Tehdit Önleme	Web Uygulama Güvenlik Duvarı	Temel Siber Güvenlik
Q1	%1	%7	%18
Q2	%7	%17	%14
Q3	%24	%57	%27
Q4	%69	%19	%40

Reşat Kökcen

Türk Telekom
ICT Ürün ve Çözüm Yönetimi
Grup Müdürü

Bilgi teknolojilerinin hızla yaygınlaşması, internete bağlı cihaz sayısının artması ve bireylerin mobilleşmesi ile birlikte şirketlerin/bireylerin dijital dönüşüm yolculukları hız kazanmaya devam ediyor. Statista'nın 2021 yılı raporuna göre, dünya çapında üretilen veri hacmi 2010 yılında 2ZB (2 Trilyon GB) iken 2020 yılında bu rakam 59 ZB'ye ulaştı. Toplam veri büyüklüğünün 2024 yılında ise 149 ZB olması bekleniyor.

Dijital veri hacminin her geçen gün artması ile birlikte verinin kıymetli bilgi formuna dönüşmesi, verinin gizliliği, bütünlüğü ve kullanılabilirliğini sağlamak adına Dünyada ve Ülkemizde siber güvenliğin en önemli konu başlıklarından biri haline geldiğini görüyoruz.
Kurumların teknolojiyi her zamankinden daha fazla kullanmaya başlamasıyla siber güvenlik alanında da çarpıcı yansımaları görülmeye başlandı. Saldırganlar; belirsizlik ortamından, benzeri görülmemiş durumlardan ve bilgi teknolojileri alanında yaşanan hızlı değişimden yararlanarak yeni siber tehditler ile hem kurumları hem de bireyleri daha fazla tehdit eder hale geldi.

Günümüz ve gelecek trendlerini göz önünde bulundurduğumuzda siber atak vektörlerinin ve çeşitliliğinin artması, kurumları siber tehditlere karşı alması gereken önlemleri de arttırmaya yönlendiriyor. Sürdürülebilir iş süreçleri için, atak yüzeylerinin tespiti, anlama ve önleme prosedürlerinin etkin çalışması; teknoloji, süreç ve insan kaynağı kavramlarının bütünsel olarak ele alınması ve altyapıların 7/24 yönetilmesi her zamankinden daha kritik bir önem arz ediyor. Siber güvenlik risklerine karşın teknolojilerinin önemi kadar, bu teknolojilerin yönetilmesi, işletilmesi ve 7/24 izlenerek müdahale edilmesi de önceliklendirilmesi gereken siber güvenlik önlemleri olarak değerlendiriyoruz.
Günümüzde kurumların altyapılarını korumak için yaptığı teknoloji yatırımları maalesef tek başına yeterli olmuyor. Kurumların; alt yapılarını anlamaları, potansiyel zafiyetlerinin farkında olmaları, siber güvenlik olgunluk ve farkındalık seviyelerini arttırmaları, uçtan uca siber savunmanın sağlanabilmesi adına oldukça önemli konu başlıkları haline geldi. Bu nedenle de artan belirsizlik ve çeşitlenen siber tehditlere karşı doğru ve tek noktadan müdahale edebilmek adına Siber Güvenlik Operasyon Merkezlerine(SOC) duyulan ihtiyaç giderek artıyor.
Türk Telekom olarak Türkiye'de siber güvenlik hizmeti sağlayan ilk telekom operatörü olmamızın sağladığı tecrübe ile 1500 metrekareyi aşan Siber Güvenlik Merkezimizde, müşterilerimize yakın geleceğin ve günümüzün siber saldırılarına karşı uçtan uca güvenlik hizmetleri sunuyoruz.

360 derece güvenlik yaklaşımını benimseyerek ve 7/24 izleme faaliyetlerini yerli milli siber istihbarat verileriyle zenginleştirerek sunduğumuz servislerle; SIEM ile network, EDR teknolojileriyle uç nokta verilerinin anlamlandırılması ve yönetimi ile otomatik aksiyon alabilecek teknolojileri bütünleşik bir mimaride sunuyoruz. Farklı vaka analizlerinde deneyim kazanmış global standartlarda sertifikalara sahip mühendislerimiz ile saldırgan bakış açısından da olaylara yaklaşarak altyapıların gelişimini ve bu minvalde yönetilmesini sağlıyoruz.

Türk Telekom olarak Türkiye'nin verisini Türkiye'de güvende tutmak için var gücümüzle çalışmaya, Siber Güvenlik Merkezimizi Türkiye'nin lider iletişim operatörü ve teknoloji şirketi olarak en ileri seviyede altyapılarla buluşturmaya ve kendi kaynaklarımızla siber güvenlik sektöründe öncülüğümüzü pekiştirerek tüm Kurumsal ve Kamu müşterilerimize katkı sağlayabilmek için çalışmaya devam ediyoruz.

1. Nesnelerin İnterneti (IoT) ile Birlikte Artan Siber Güvenlik Riskleri

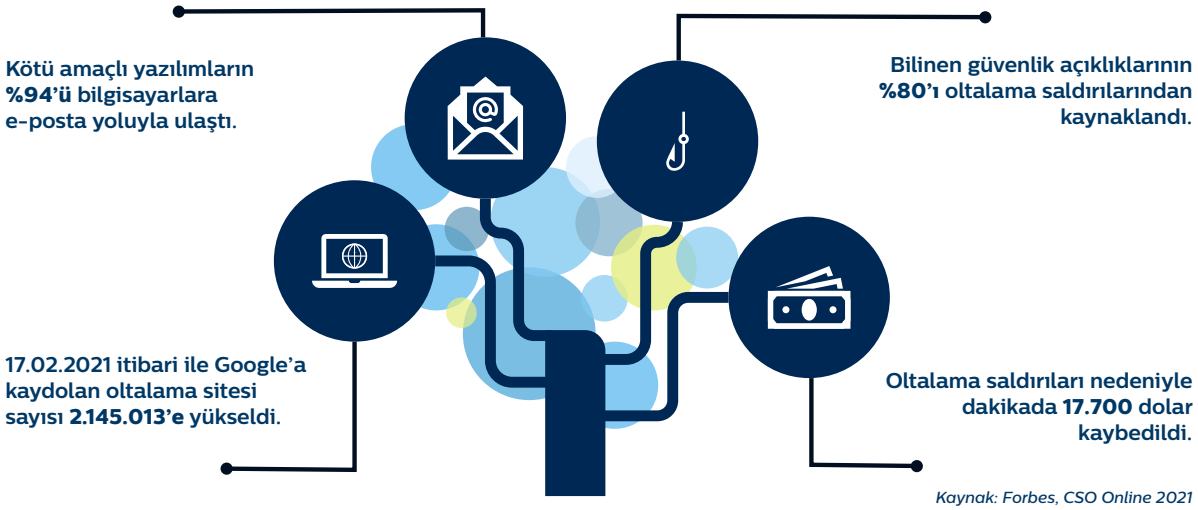
Her geçen gün genişleyen nesnelerin interneti kavramı (IoT), siber suçlar için de daha fazla fırsat anlamına geliyor. Nesnelerin İnterneti; internete bağlanan ve veri paylaşan bilgisayarlar, telefonlar, sunucular dışındaki tüm fiziksel cihazları ifade etmektedir. Bu cihazlara örnek olarak giyilebilir spor takip cihazları, akıllı ev eşyaları ve akıllı saatler de örnek olarak verilebilir. Tüm bu cihazları siber saldırılar için bir ağa giriş noktası olarak düşünebiliriz.

2026 yılına kadar dünya çapında
64 milyar IoT cihazının kurulu olacağı tahmin ediliyor. Uzaktan çalışmaya yönelik eğilim, bu artışın sağlanmasına yardımcı oluyor.

2. Sosyal Mühendislik Saldırıları Daha Akıllı Hale Geliyor

Kimlik avı gibi sosyal mühendislik saldırıları yeni tehditler değil ancak günümüz koşullarında uzaktan çalışma ve online işlemlerin artması ile birlikte daha yaygın hale geldiğini söylemek mümkün. Kurumlar kimlik avına karşı korumalarını sıkılaştırsa da siber saldırganlar da her zaman güncel konulara bağlı yeni yollar aramaya devam ediyor.

2020 yılında 2 kat artış göstererek en çok karşılaşılan siber atak türlerinden biri «Oltalama Saldırıları» oldu



Kaynak: Forbes, CSO Online 2021

3. Mobil Siber Güvenlik Riskleri

Dijitalleşen dünya ile birlikte mobil cihazların kullanımı ve buna bağlı olarak mobil ağlara yönelik gerçekleştirilen siber saldırılar artış göstermektedir. Mobil siber güvenlik, uç cihaz güvenliği, bulut güvenliği, ağ güvenliği ve giyilebilir cihazlar gibi internete bağlı cihazları kapsayan geniş bir konudur. Hızlanan dijital dönüşüm çağında, siber saldırılar hem bireyleri hem de kuruluşları hedef almak için yeni yollar ararken mobil cihaz kullanımının artması saldırganlar için daha geniş bir atak yüzeyi anlamına geliyor.

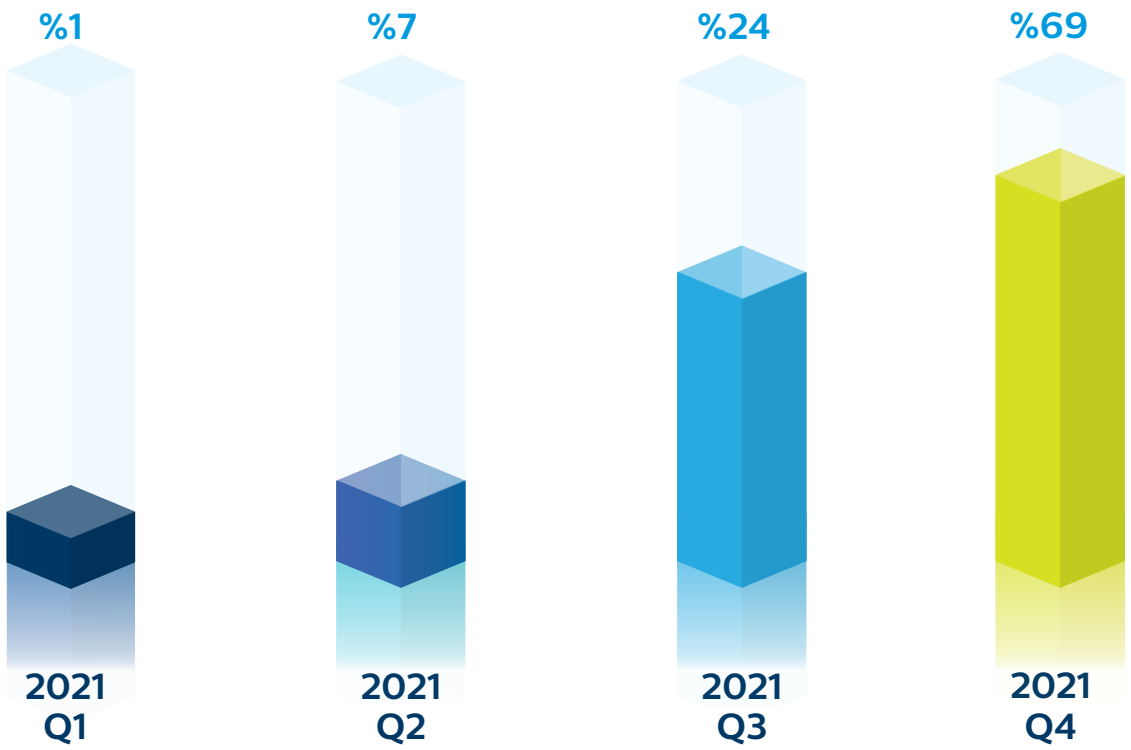
Araştırmaya katılanların **%40'ı** mobil cihazları şirketlerin en büyük güvenlik riski olarak görüyor*

IT çalışanlarının **%71'i** mobil cihazların iş açısından kritik öneme sahip olduğunu belirtiyor*

*Verizon Mobile Security Index Report, 2021

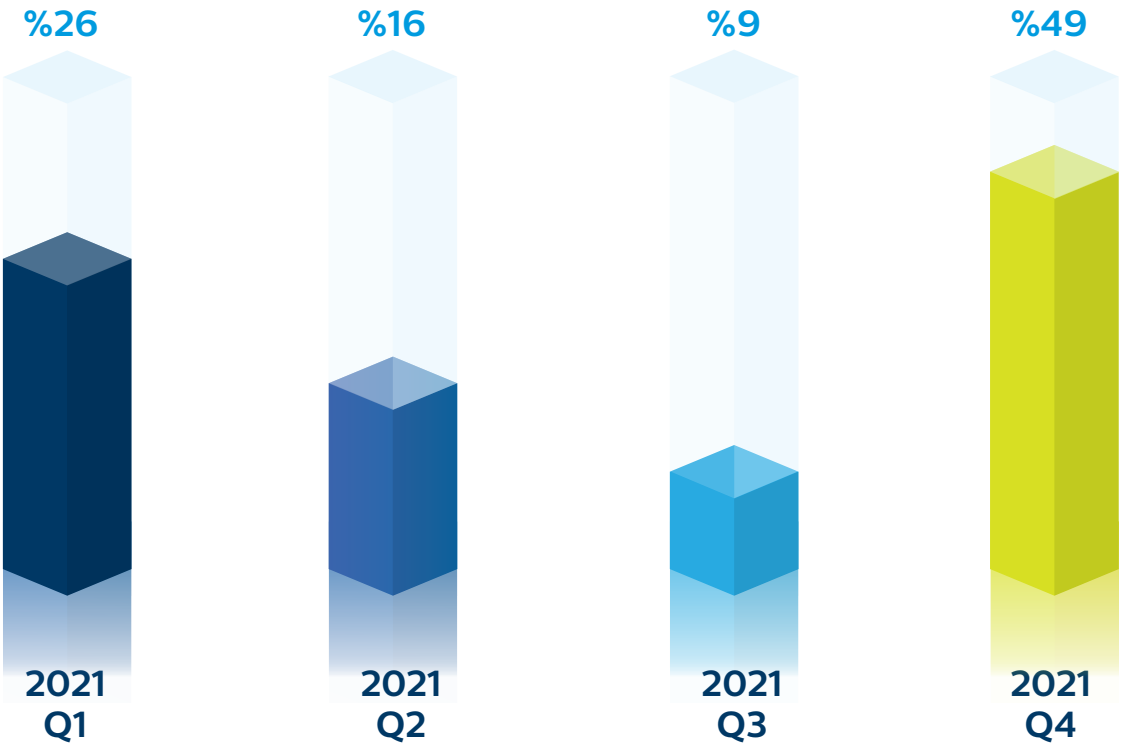
Türk Telekom Siber Atak İstatistikleri

1. Gelişmiş Tehdit Önleme (APT) Atak İstatistikleri



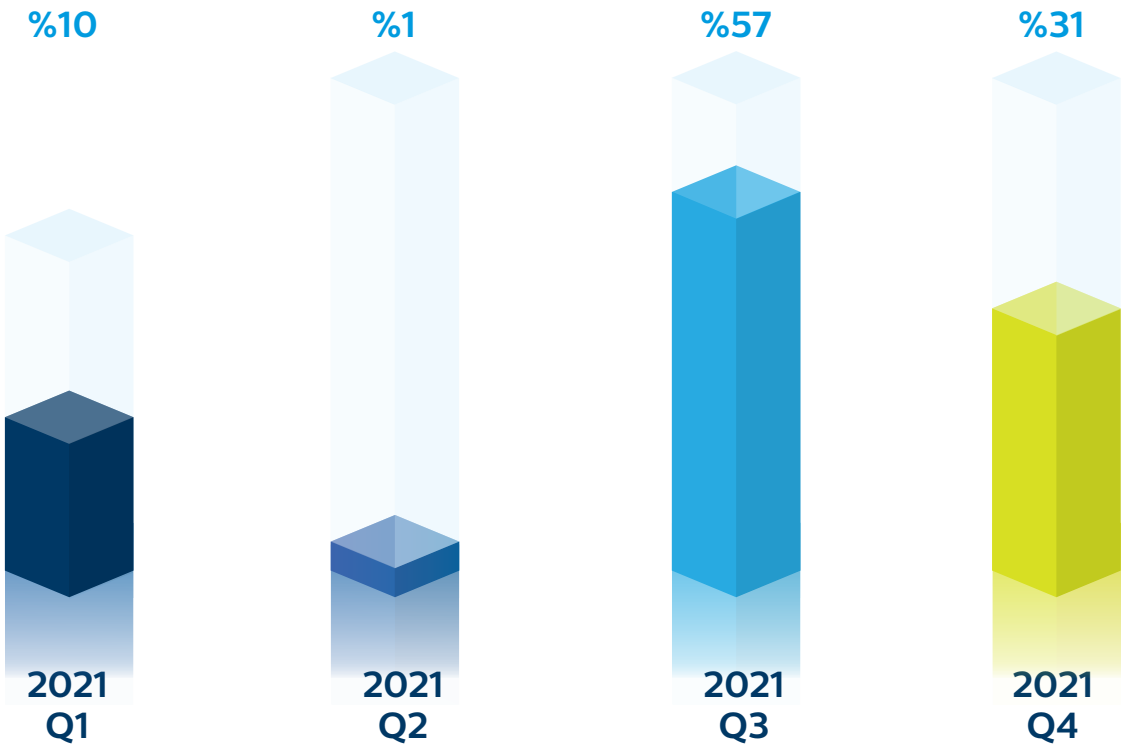
Türk Telekom APT hizmeti kapsamında 2021 yılı son çeyrekte önemli bir artış yaşanmıştır.

2. Antivirüs Servisinde Tespit Edilen Zararlı Yazılımlar



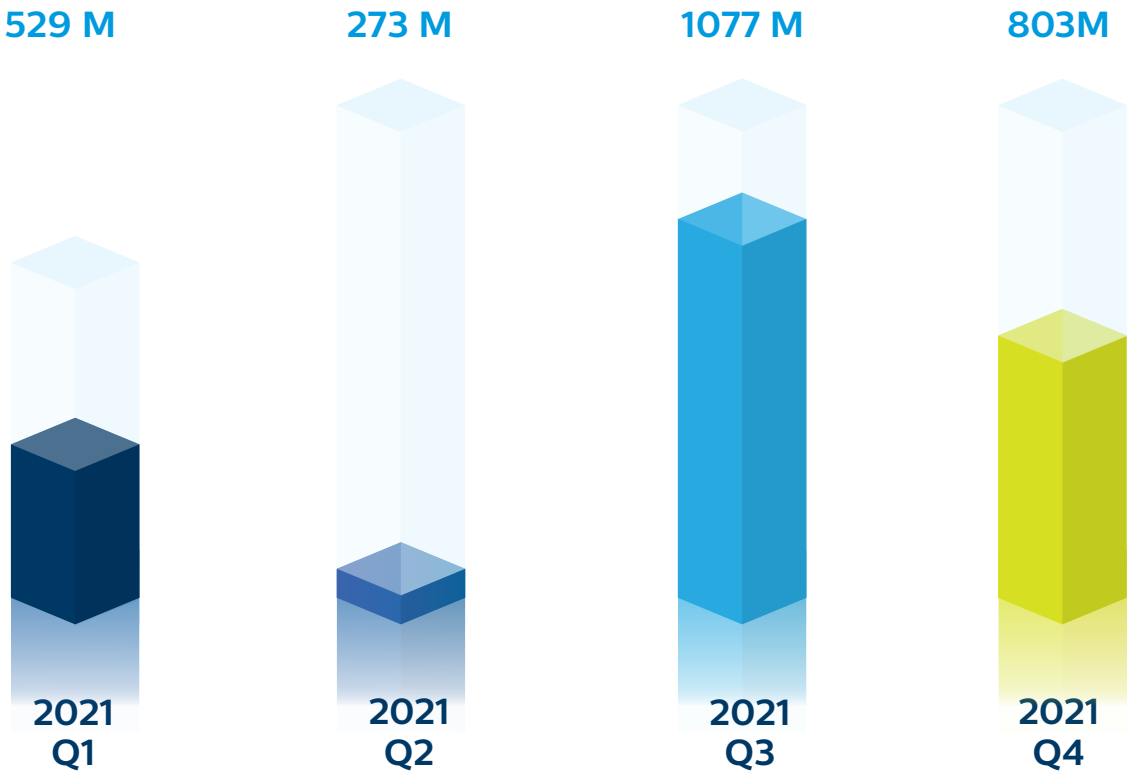
Türk Telekom antivirüs servisinde tespit edilen virüs, solucan ve zararlı yazılımların toplamının çeyrek bazlı dağılımı gösterilmektedir.

3. İçerik Filtreleme Servisinde Engellenen Zararlı Erişimler

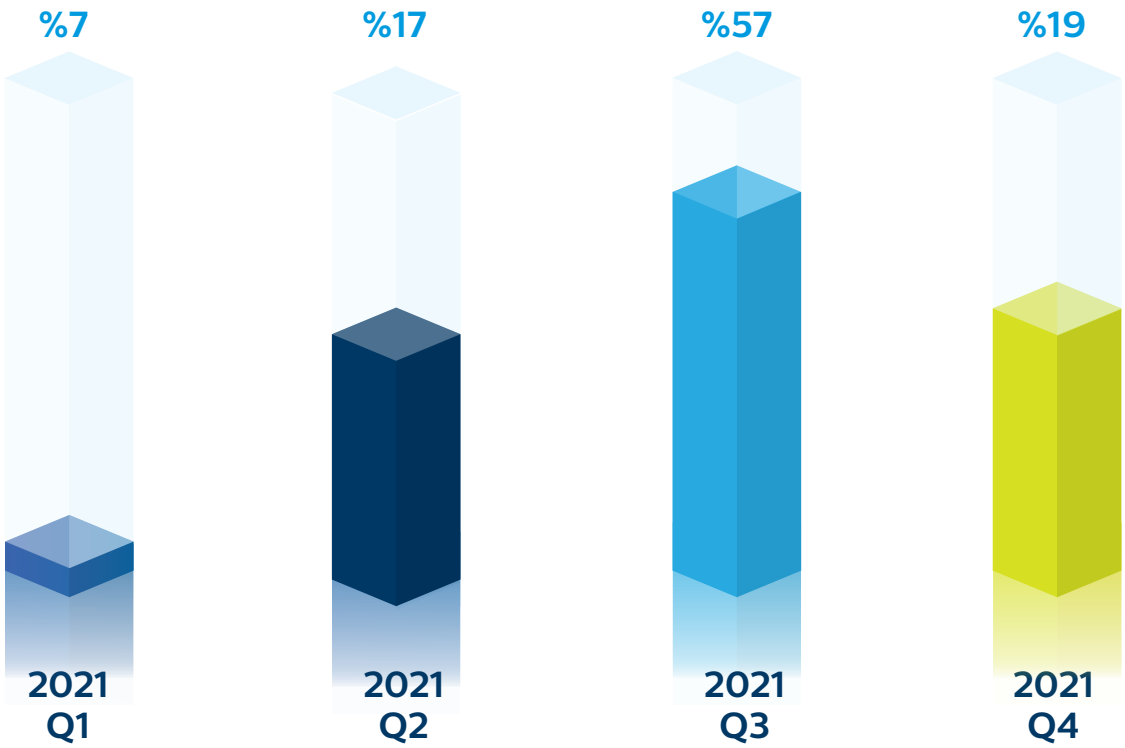


İçerik filtreleme servisinde engellenen zararlı erişim sayılarının çeyrek bazlı dağılımı gösterilmektedir.

4. Aktif Savunma (IPS) Sisteminde Tespit Edilen Zararlı Yazılımlar



5. Web Uygulama İstatistikleri



2021 yılının ikinci yarısında, ilk yarı yıla göre Türk Telekom WAF servislerinde tespit edilen atak sayısı 3 kat artış göstermiştir.

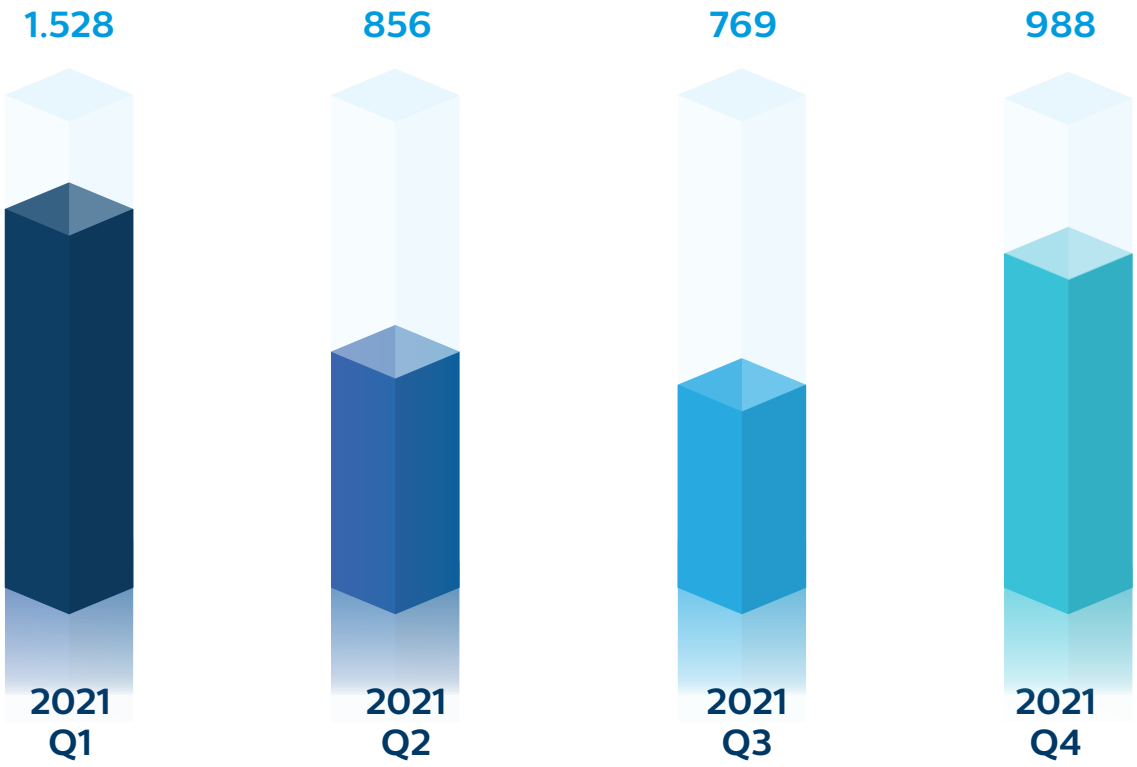
2021 İlk Yarısında Türk Telekom Web Uygulama Güvenliği (WAF) Servisinin Tespit Ettiği En Sık Karşılaşılan 10 Atak Türü

1. Session Hijacking
2. HTTP Parser Atak
3. Information Leakage
4. Other Application Activity
5. Injection Attempt
6. Vulnerability Scan
7. Abuse of Functionality
8. JSON Parser Attack
9. Detection Evasion
10. Cross Site Scripting (XSS)

5. DDOS Atak İstatistikleri

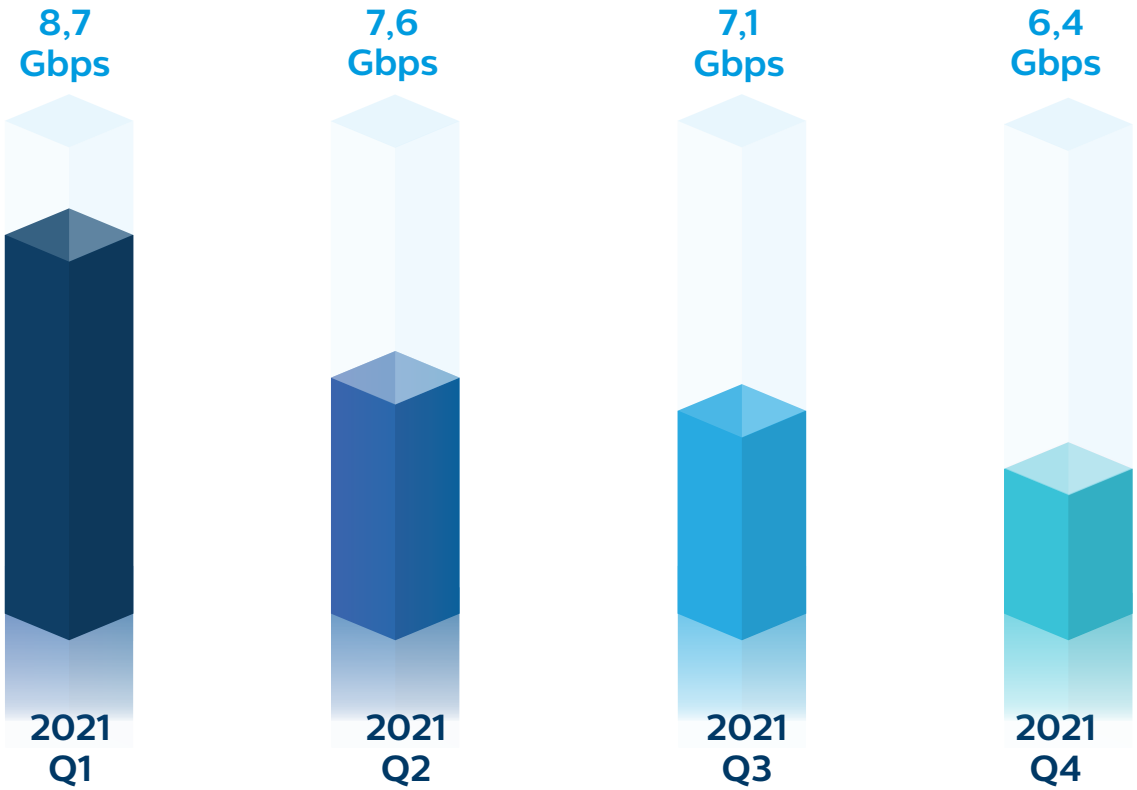
1 Gbps Üzeri Atak Sayıları

Türk Telekom DDOS Atak Önleme altyapısında tespit edilen ve engellenen 1 Gbps ve üzeri atak sayılarının çeyrek bazlı dağılımı



Ortalama Atak Büyüklükleri

Aşağıdaki grafik 1 Gbps üzerinde gerçekleşen DDOS ataklarında gerçekleşen bir saldırının ortalama büyüklüğünü ifade etmektedir.



«Başarı Hikayesi»

M. Levent Hatipoğlu

Yalova Belediyesi, Bilgi İşlem Müdürü

Belediyelerin dijital dönüşüm süreçleri nasıl gerçekleşti?

Yalova Belediyesi olarak 2011 yılından beri yürüttüğümüz dijital dönüşüme belediyeninvatandaşa dokunan iş süreçlerinin belirlenmesi ile başlamıştır. Bu çalışma sonucunda 500'e yakın dilekçe ve şikayet başlığı oluşturulmuştur. Sonrasında bu iş süreçlerinin tanımları yapılmış ve hizmetin kesintiye uğramadan devam etmesi için iş istasyonları ve organizasyon tanımları güncellenmiştir. Bu çalışmayla kamuda sıkça karşılaşılan kişiye bağımlı işler organizasyon tanımlarına bağlı hale getirilmiştir.

Belediyelerin en çok karşılaştığı siber saldırılar nelerdir?

Son zmanlarda tüm sektörlerde olduğu gibi kamuda da siber saldırı tehdidi iş devamlılığı açısından ciddi bir risk olarak ortaya çıkmaktadır. Belediyeler DDOS, Malware Oltalama saldırıları, SQL İnjection, fidye yazılım gibi akla gelebilecek her türlü saldırıya maruz kalmaktadır. Elektronik ortamda artan hizmet talebine karşılık sunulan hizmetler tüm kuruluşlarda IT departmanlarının iş yükünü ikiye üçe katlamasına rağmen iş gücü kaynağı aynı hızla büyümemektedir. Özellikle pandemi döneminde personellerin uzaktan çalışma mecburiyeti, uzak masaüstü hizmetlerinin açıklarından yararlanan saldırıları da arttırmıştır. Belediyeler de en az diğer kurumlar kadar siber saldırı tehdidi altında bulunmaktadır.

Artan siber saldırılara karşı Yalova Belediyesinin siber güvenlik yaklaşımı nasıldır?

Belediyemiz elindeki kaynaklarla siber güvenlikle ilgili güncel yaklaşımları olabildiğince takip edip sadece gereklilikleri yerine getirmek için değil bu anlayış ile siber saldırı risklerini en aza indirgemeye gayret göstermektedir. Tabii ki kamu sektöründe bu alanda hem yatırım yapmak hem de yeterli iş gücü kaynağına sahip olmak her zaman kolayca aşılabilecek bir engel olmamaktadır. Paydaşların değerli verilerini barındıran belediyeler için hizmet devamlılığını sağlayabilmek adına siber güvenlik yatırımları son derece hayati önem taşımaktadır.

Siber ataklar için aldığınız önlemler, yapılan yatırımlar nelerdir?

Bu noktada kurumumuz her türlü platformda, hızla artan hizmet beklentisiyle paydaşlarımıza daha çok kanaldan hizmet vermeye çalışırken hizmetlerin kesintiye uğramaması ve çok değerli verilerin korunabilmesini hedeflemektedir. Türk Telekom'da DDOS, WAF, Paylaşımlı SIEM gibi güvenlik hizmetlerinin yanı sıra Bulut Yedekleme çözümleriyle de tesis ettiğimiz iş ortaklığı neticesinde çevik yaklaşım prensibini benimsemektedir.

Türk Telekom Siber Güvenlik Servis Kataloğu

Erişim Bağımlı Güvenlik Hizmetleri

- DDOS Atak Önleme
- DDOS7+
- Güvenlik Duvarı (Firewall)
- Aktif Savunma Sistemi (IPS)
- İçerik Filtreleme
- Antivirus

Erişim Bağımsız Güvenlik Hizmetleri

- Gelişmiş Tehdit Önleme (APT)
- Web Uygulama Güvenlik Duvarı
- Paylaşımlı SSL VPN

Paylaşımlı Güvenlik Hizmetleri

Dedike Güvenlik Hizmetleri

- Atanmış Siber Güvenlik Servisleri (NAC, PAM vb.)
- Ağ ve Network Güvenlik Servisleri
- Kimlik ve Erişim Güvenliği
- Bütünleşik Tehdit Yönetimi (UTM)
- Ağ Erişim Kontrolü (NAC)
- Veri Kaybı Önleme (DLP)
- Uç Nokta Güvenliği
- Siber Güvenlik Eğitimleri
- Danışmanlık Hizmetleri

Siber Güvenlik Merkezi

- 7/24 Güvenlik Olay İzleme
- SIEM Danışmanlık
- Test ve Danışmanlık
- Güvenlik Cihaz Yönetimi
- SOAR
- DDOS Atak Simülasyonu
- Paylaşımı SIEM
- Siber Atlas
- Altay Oltalama Simülasyonu
- EDR+

Türk Telekom Siber Güvenlik Merkezi Hizmetleri

Siber güvenlik trendleriyle mücadelede teknolojilerin önemi kadar bu teknolojilerin yönetilmesi, işletilmesi ve 7/24 izlenerek müdahale edilmesi de kritik parametreler arasında yer almaktadır. Türk Telekom Siber Güvenlik Merkezi, süreçleri, teknolojileri ve personelleri bütünsel bir yaklaşım ile bir organizasyonun genel güvenlik duruşunu yönetmek ve geliştirmek için 7/24 hizmet vermektedir.

Avrupalı CERT/CSIRT toplulukları tarafından kabul gören Trusted Introducer (TR-CERT) ve TSE tarafından akredite edilmiş Türk Telekom Siber Güvenlik Merkezinde kurumların günlük operasyonlarını kolaylaştırmak için tek noktadan, çok yönlü ve SIEM markası bağımsız yapıda global standartlarda sertifikalara sahip mühendislerimiz ile 7/24 Olay Yönetimi, SIEM Danışmanlık, Paylaşımlı Hizmetler ve Test Danışmanlık servisleri sunulmaktadır.

7/24 Güvenlik Olay Yönetimi

TÜRK TELEKOM ÖNERİYOR UZMANLARI

7/24 güvenlik olay izleme hizmeti, izleme ve anomaly analizi yapılmaktadır. SIEM altyapısı kurulan müşterilerin usecaseleri özelinde oluşan alarmaların 7/24 izlenmesi, buradan oluşacak alarmların false/ positif analizi, olayların gelişmiş incelenmesiyle birlikte olay türünün belirlenerek kaynak tespitinin yapılması ve kök neden analizinin yapılmasını kapsamaktadır. 7/24 izleme ekibinde yer alan forensic analistler tarafından yapılan kök neden analizi sonucunda alınması gereken aksiyon önerileri Türk Telekom güvencesiyle sunulmaktadır.

Türk Telekom Siber Güvenlik Merkezi

Danışmanlık Hizmetleri

TÜRK TELEKOM ÖNERİYOR UZMANLARI

SIEM Danışmanlık Hizmetleri

SIEM Danışmanlık hizmetleri, varlıkların tespiti ve sınıflandırılması, envanter analizi yapılarak uygun log kaynaklarının belirlenerek SIEM'e entegre edilmesi, saldırı analizleri yapılarak korelasyon kontrolleri ve yeni korelasyon yazımı, event mapping gibi çalışmaların bütününü oluşturmaktadır.

Test Danışmanlık Hizmetleri

- Sızma Testi
- DDOS Atak Simülasyonu
- Altay Oltalama Simülasyonu
- Zafiyet Tarama
- KVKK Danışmanlığı
- Güvenlik Olgunluk Ölçümleme
- Red Team

Paylaşımlı Hizmetler

Paylaşımlı SIEM

SIEM ihtiyacı olan ve ihtiyacını servis olarak karşılamak isteyen müşterilere yerli milli üretici ile paylaşımlı SIEM hizmeti Türk Telekom tecrübesi, güvencesi ve kalitesi ile sunulmaktadır. Paylaşımlı SIEM hizmeti, ağ, donanım ve uygulamalar tarafından oluşan logların gerçek zamanlı olarak normalleştirilmesi ve ilişkilendirilmesiyle ilgili analizlerin sağlanması amaçlı logların merkeze toplanıp korele edilmesi, istihbarat verileriyle zenginleştirilmesi ve 7/24 izlenmesi ile hizmet süresi boyunca yönetmeliklere uyumlu olarak logların saklanmasını kapsamaktadır.

SOAR ile Otomatik Müdahale

SOAR(GüvenlikOrkestrasyon,Otomasyon ve Olay Müdahale) ile Otomatik Müdahale hizmeti, organizasyonların güvenlik tehdit verilerini ve farklı kaynaklardan gelen olayların toplanmasını sağlayarak, gelişmiş zeka ile güvenlik düzenlemeleri yaparak, tehdit verilerini belli bir otomasyona sokarak, toplanmış ve önceliklendirilmiş olaylar üzerinden yarı ya da tam otomatik olay müdahale süreçlerinin yönetimini kapsamaktadır.

Siber Atlas ile İstihbarat

Siber Atlas ile istihbarat hizmeti, müşteri verileri ile ilgili temel ve gelişmiş istihbarat verisi sunmaktadır. Temel paket kapsamında Yerel ve Global istihbarat kaynaklarından toplanan IOC verilerinin anlamlandırılarak güvenlik cihazlarını beslenmesi ve platform üzerinden tehdit istihbaratı analizlerini; gelişmiş paket içeriğinde otomatize edilmiş arayüzler ve siber güvenlik alanında uzmanlaşmış analistlerin yaptığı kurum özelindeki araştırmalar sonucunda elde edilen istihbarat verilerinin raporlanmasını içermektedir.

Dark Web ve Deep Web Takibi

Marka Koruma ve İstihbarat

Otomatik ve Manuel Zafiyet Tarama

Dolandırıcılıkla Mücadele İstihbaratı

Honeypot ile Veri Toplama

Sosyal Medya Takibi

Veri İhlal Takibi

Türk Telekom Siber Güvenlik Merkezi

Türk Telekom Siber Güvenlik Merkezi, Veri Güvenliği için 7/24 Hizmetinizde!

TÜRK TELEKOM ÖNERİYOR UZMANLARI

- Global standartlarda sertifikalara sahip alanında uzman kadromuz ile danışmanlık hizmetleri
- Yerli ve milli teknoloji ile Paylaşımlı SIEM hizmetinde bütünleşik güvenlik çözümleri
- SIEM, SOAR ve Siber İstihbarat hizmetleriyle 360° güvenlik yaklaşımı
- TSE ve Global sertifikalarla süreçleri akredite edilmiş merkezimizde test danışmanlık hizmetleri

Kurumunuza özel teknolojik çözümlerimiz ile ilgili detaylı bilgi almak için Türk Telekom satış yöneticiniz veya 444 5 444 ile iletişime geçebilirsiniz.

BU İŞTE BERABERİZ

Türk Telekom
Değerli Hissettirir