ECHO

CYBER THREAT INTELLIGENCE

# SİBER SALDIRI RAPORU

## 2024 Yılı İlk Yarı Özel

@echocti @echocti echocti.com

# İçindekiler

# Yönetici Özeti

2024 yılının ilk yarısında, global siber güvenlik ortamında önemli değişiklikler ve zorluklar ortaya çıkmıştır. Bu dönemde, siber tehditlerin artışı ve çeşitlenmesi, organizasyonlar ve bireyler için kritik güvenlik risklerini gündeme getirmiştir. Ransomware saldırıları, veri sızıntıları ve kritik zafiyetler gibi anahtar konular, mevcut tehdit manzarasını kapsamlı bir şekilde şekillendirmiştir.

Ransomware saldırılarında gözlemlenen belirgin artış, siber güvenlik alanında ciddi bir endişe kaynağı olmuştur. 2023 yılının aynı dönemi ile kıyaslandığında, bu tür saldırılarda %48 oranında bir artış yaşanmış, en çok karşılaşılan ransomware aileleri arasında LockBit, ransomhub ve Play ransomware dikkat çekmektedir. Aylık bazda saldırı sayılarındaki değişimler, ransomware tehditlerinin giderek daha karmaşık hale geldiğini ve hedeflerin genişlediğini göstermektedir.

Veri sızıntıları açısından, 2024 yılının ilk yarısında sızdırılan veri miktarı [toplam veri miktarı] GB/TB olarak belirlenmiştir. Büyük veri sızıntısı olayları arasında [büyük veri sızıntısı olayları] öne çıkmaktadır. Bu durum, kişisel ve kurumsal verilerin korunmasına yönelik risklerin arttığını ve veri koruma stratejilerinin gözden geçirilmesi gerektiğini ortaya koymaktadır.

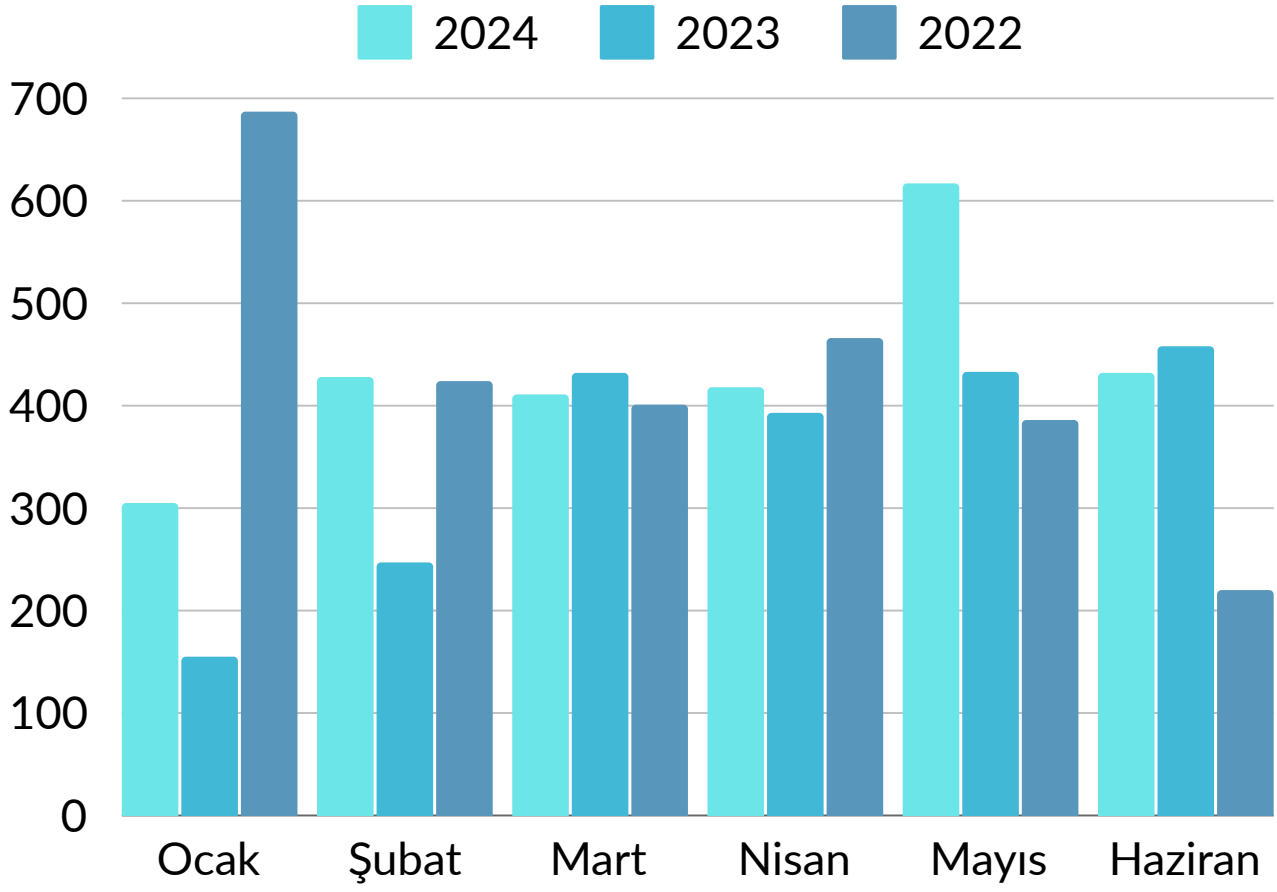
Kritik zafiyetler ise siber tehditlerin karmaşıklığını ve güvenlik açıklarını artırmıştır. [Kritik zafiyetler ve sömürülme örnekleri] gibi önemli zafiyetler, güvenlik stratejilerinin güçlendirilmesi ve güncel tehditlere karşı etkin önlemler alınması gerekliliğini vurgulamaktadır.

Sonuç olarak, 2024 yılının ilk yarısında karşılaşılan ransomware saldırı artışı, veri sızıntıları ve kritik zafiyetler, siber güvenlik tehditlerinin ve risklerinin devam ettiğini göstermektedir. Organizasyonların, bu tehditlerle etkili bir şekilde başa çıkabilmeleri için güvenlik önlemlerini güçlendirmeleri, veri koruma stratejilerini güncellemeleri ve kritik zafiyetleri sürekli olarak izlemeleri gerekmektedir. Gelecek dönemde bu tehditlere karşı hazırlıklı olmak, güvenlik risklerini azaltmada kilit rol oynayacaktır.

# Ransomware Saldırıları

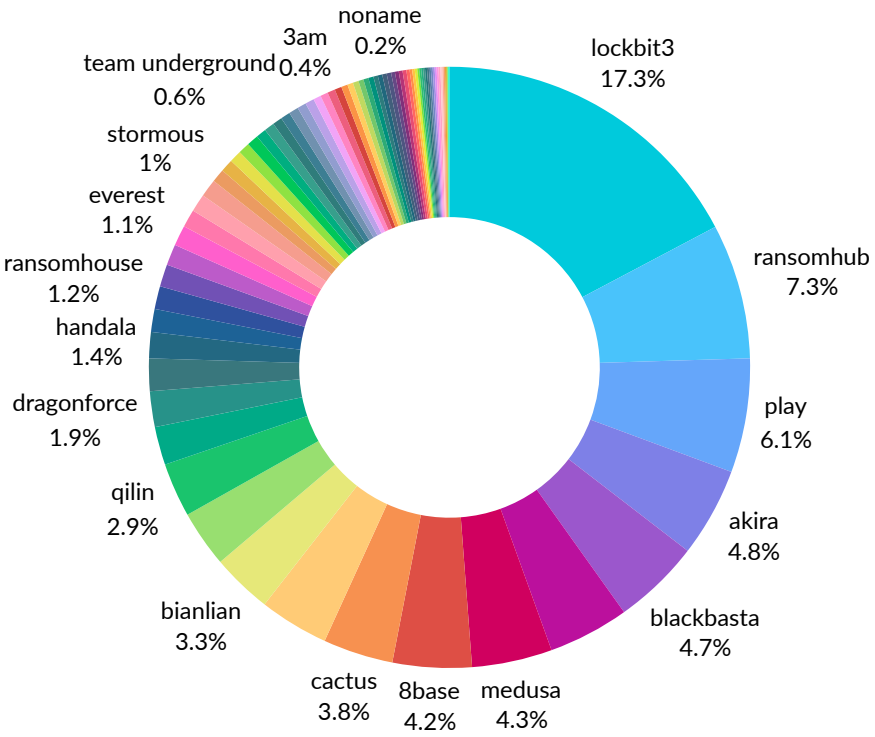
## Son Üç Yılın İlk Altı Ayında Karşılaşılan Ransomware Vakaları

Karşılaştırmalı olarak 2023 yılı ile incelendiğinde, 2024 yılının ilk yarısında ransomware vakalarının genel olarak artış gösterdiği görülmektedir. Ocak ayında 158 vaka olan ransomware saldırı sayısı, 2024'te 308'e çıkmış, bu durum %95'lik bir artışı temsil etmektedir. Şubat ayında 253 olan saldırı sayısı, 2024'te 441'e çıkarak %74'lük bir artış göstermiştir. Mart ayında ise, 2023'te 434 olan vaka sayısı, 2024'te 418 olarak kaydedilmiştir. Ancak Nisan, Mayıs ve Haziran aylarında bu artış devam etmiş, 2024'te sırasıyla 395, 438 ve 465 olan vaka sayıları, 2024 yılında önemli bir artış trendini göstermektedir. Bu artışlar, ransomware tehditlerinin daha yaygın ve sofistike hale geldiğini, organizasyonların bu tür saldırılara karşı daha dikkatli ve hazırlıklı olmaları gerektiğini göstermektedir. Özellikle Mayıs ayında yaşanan keskin artış, belirli dönemlerde yoğunlaşan saldırı aktivitelerinin siber güvenlik stratejilerini güçlendirmek için kritik olduğunu işaret etmektedir.



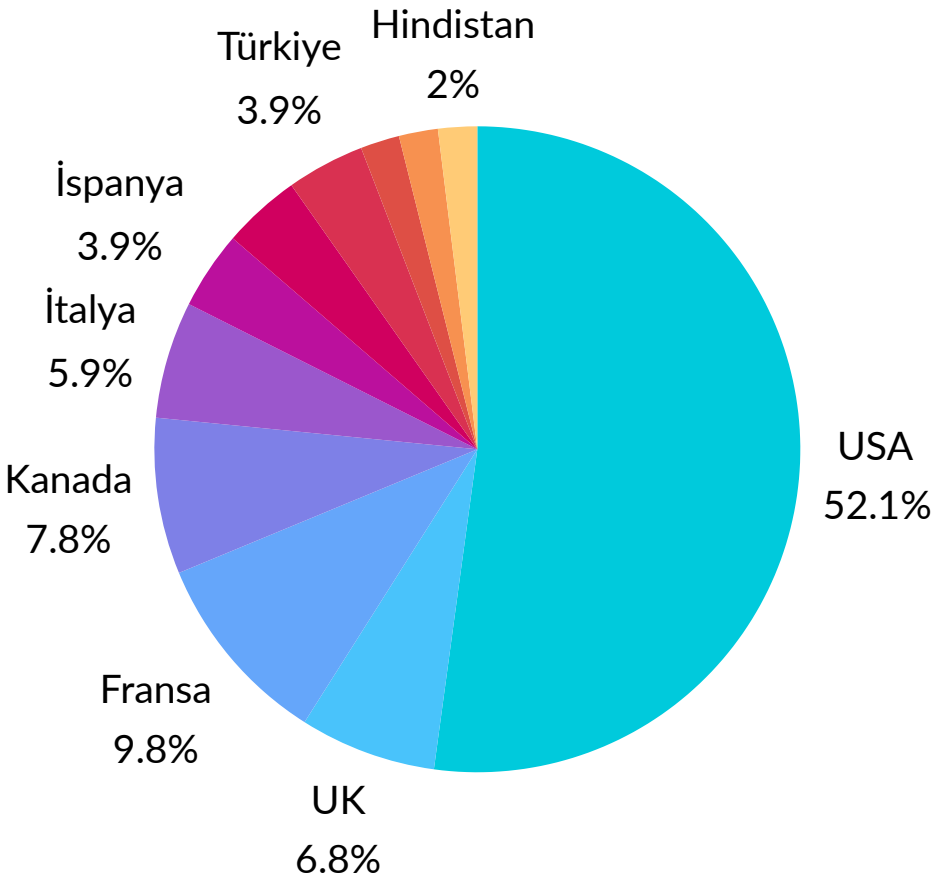
# En Çok Karşılaşılan Ransomware Aileleri

Karşılaştırmalı olarak 2023 yılı ile incelendiğinde, 2024 yılının ilk yarısında ransomware vakalarının genel olarak artış gösterdiği görülmektedir. Ocak ayında 158 vaka olan ransomware saldırı sayısı, 2024'te 308'e çıkmış, bu durum %95'lik bir artışı temsil etmektedir. Şubat ayında 253 olan saldırı sayısı, 2024'te 441'e çıkarak %74'lük bir artış göstermiştir. Mart ayında ise, 2023'te 434 olan vaka sayısı, 2024'te 418 olarak kaydedilmiştir. Ancak Nisan, Mayıs ve Haziran aylarında bu artış devam etmiş, 2024'te sırasıyla 395, 438 ve 465 olan vaka sayıları, 2024 yılında önemli bir artış trendini göstermektedir.



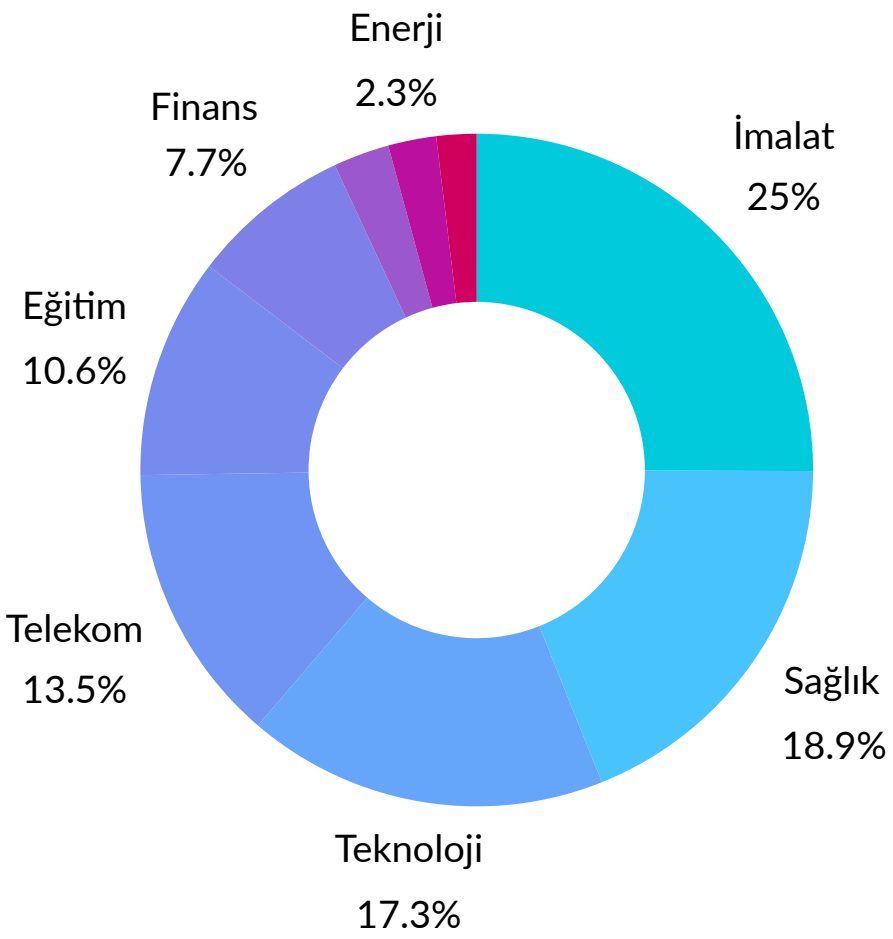

Bu ransomware aileleri, farklı yöntemler ve hedeflerle saldırılar gerçekleştirmiş olup, genel tehdit manzarasında önemli bir yer tutmaktadır. Özellikle LockBit 3, 504 kurbanla en yaygın tehdit olarak öne çıkmaktadır. Diğer önemli tehditler arasında RansomHub, Play, Akira, ve BlackBasta gibi aileler yer almaktadır. Ransomware tehditlerinin bu denli yaygın ve çeşitli olması, organizasyonların bu tür saldırılara karşı daha hazırlıklı ve dirençli olmaları gerektiğini göstermektedir. Bu durum, güvenlik stratejilerinin sürekli olarak gözden geçirilmesini ve güçlendirilmesini zorunlu kılmaktadır. Ayrıca, belirli ransomware ailelerine karşı özelleştirilmiş savunma mekanizmalarının geliştirilmesi, saldırıların etkisini azaltmada kritik rol oynayacaktır.

# Ransomware Saldırılarının Ülkelere Göre Dağılımları




Bu tablo, ilk 10 ülkedeki kuruluşlar hakkındaki fidye yazılımı saldırılarının dağılımını göstermektedir. Bahsedilenlerin %52,1'i ile Amerika Birleşik Devletleri önemli bir şekilde önde giderken, onu Birleşik Krallık ve Fransa takip ediyor. Bu veriler, fidye yazılımı tehditlerinin coğrafi odağını ve kuruluşların bu siber riskler bağlamında en sık tartışıldığı ülkeleri yansıtmaktadır.

# Ransomware Saldırılarının Sektörlere Göre Dağılımları

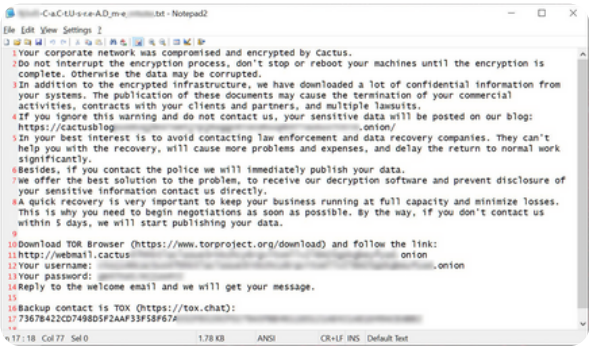



Bu grafik, fidye yazılımı saldırılarında hedeflenen ilk 10 sektörü göstermektedir. İmalat sektörü, pozisyonların %25'ini oluşturarak listenin başında yer alırken, onu Sağlık, Teknoloji ve Telekomünikasyon gibi sektörler takip ediyor.

# Önemli Fidye Yazılımı Vakaları

## Schneider Electric Cactus Fidye Yazılımı Saldırısına Uğradı

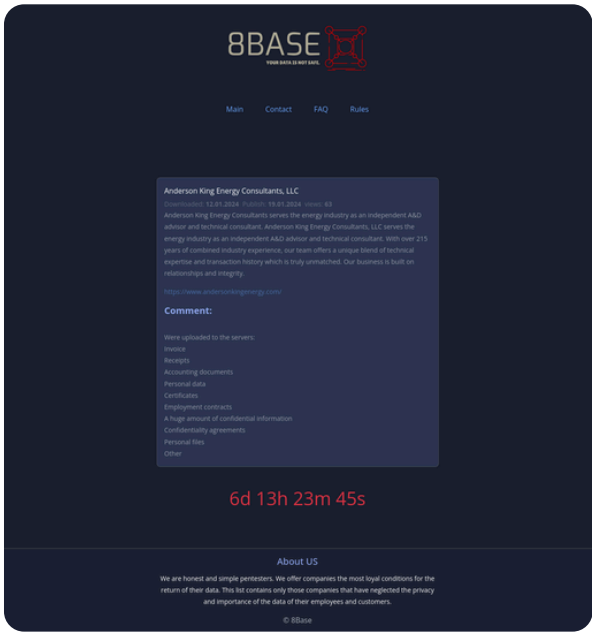
Enerji yönetimi ve otomasyon şirketi Schneider Electric, Cactus fidye yazılımı saldırısına maruz kaldı. Saldırı, Schneider Electric'in Sürdürülebilirlik İş bölümünü hedef aldı ve şirketin cloud platformunu kesintiye uğrattı.




Fidye yazılımı çetesi, saldırı sırasında terabaytlarca kurumsal veri çaldı ve şirkete fidye ödenmezse bu verileri sızdırmakla tehdit etti. Saldırıdan etkilenen Sürdürülebilirlik İş bölümü, kurumsal kuruluşlara danışmanlık hizmetleri sunmakta ve yenilenebilir enerji çözümleriyle ilgili tavsiyelerde bulunmaktadır. Çalınan verilerin güç kullanımı, endüstriyel kontrol sistemleri ve enerji düzenlemeleri hakkında hassas bilgiler içerebileceği belirtilmektedir.

Schneider Electric, saldırının sadece Sürdürülebilirlik İş bölümünü etkilediğini açıklamıştır. Schneider Electric, Clop fidye yazılımı grubu tarafından daha önce hedef alınmıştı ve bu yeni saldırılarla benzerlik göstermektedir.

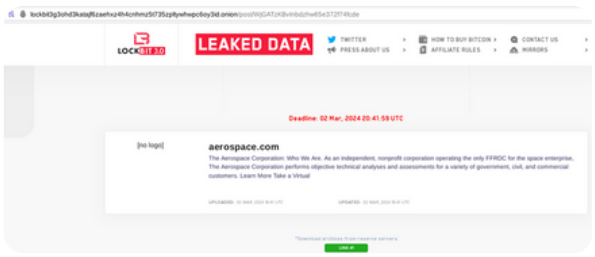
## Anderson King Enerji Danışmanları 8Base Fidye Yazılımı Saldırısına Uğradı




A&D danışmanlığı ve teknik danışmanlık hizmetleri veren Anderson King Energy Consultants, 8Base fidye yazılımı saldırısına uğradı.

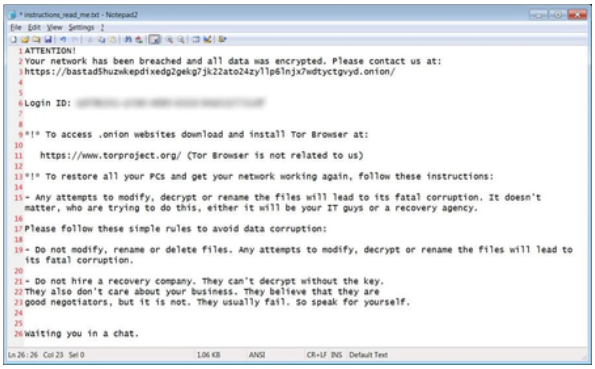
# Aerospace LockBit Fidye Yazılımı Saldırısına Uğradı

Hindistan'ın Aerospace Laboratories (NAL) adlı büyük havacılık araştırma şirketi, kötü şöhretli fidye yazılım grubu LockBit tarafından saldırıya uğradı. LockBit, NAL'ı karanlık web sızıntı sitesine ekleyerek, kuruluşun verilerini yayınlamakla tehdit etti. Sızan bilgilere göre, LockBit, çalındığı iddia edilen sekiz belgeyi yayınladı, bunlar arasında gizli mektuplar ve bir çalışanın pasaportu da bulunuyor.




. NAL'ın web sitesi kapalı olduğu için şirket ya da Hindistan siber ajansı CERT-In henüz konuyla ilgili resmi bir açıklama yapmadı. Geçtiğimiz ay, LockBit, Çin Sanayi ve Ticaret Bankası'nın (ICBC) ABD şubesini hedef alarak ABD Hazine piyasasındaki işlemleri aksatmıştı ve bankanın fidye ödediği belirtilmişti. LockBit'in iş modeli, kötü amaçlı yazılımını diğer bilgisayar korsanlarına satmak olan "hizmet olarak fidye yazılımı" olarak biliniyor.

# Hospital Corporation of America (HCA) BlackBasta Saldırısı




ABD'nin büyük hastane zinciri HCA, BlackBasta fidye yazılımı grubu tarafından hedef alındı. Bu saldırı, birçok hastanede operasyonel kesintilere neden oldu ve hasta verilerinin şifrelenmesiyle sonuçlandı. Şirket, fidyenin ödenmesiyle ilgili zorlu bir süreç yaşadı ancak sonunda saldırıyı atlatmayı başardı.

# Data Leaks

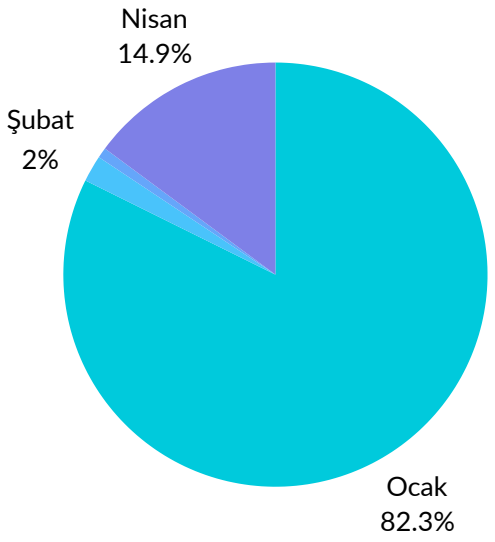
2024 yılının ilk yarısında, veri ihlalleri siber güvenlik ortamında ciddi bir endişe kaynağı olmuştur. Bu dönemde, milyonlarca kayıt çeşitli saldırılar sonucunda sızdırılmış ve bu durum, hem bireyler hem de organizasyonlar için önemli güvenlik riskleri oluşturmuştur.

**35,927,479,085**
**Sızdırılan Kayıtlar**

2024 yılı boyunca rapor edilen toplam veri ihlallerinin boyutu ve sızdırılan kayıt sayıları, bu tehdidin büyüklüğünü gözler önüne sermektedir. 2024 yılının ilk altı ayında yaşanan veri ihlalleri, toplam 35,927,479,085 kaydın sızdırıldığını ortaya koymaktadır. Bu büyük ölçekli veri ihlalleri, kişisel ve kurumsal verilerin güvenliğinin ne kadar kritik olduğunu bir kez daha göstermektedir. Bu tür ihlaller, kullanıcı bilgilerinin yanı sıra, finansal veriler ve diğer hassas bilgilerin de tehlikeye girmesine neden olmuştur.

## MOAB (Mother of All Breaches)

2024 yılının ilk yarısında yaşanan en büyük veri ihlallerinden biri, "Mother of All Breaches" (MOAB) olarak adlandırılan olaydır. Bu veri ihlalinde, milyonlarca kullanıcının kişisel bilgileri siber suçlular tarafından ele geçirilmiştir. MOAB ihlali, özellikle geniş kapsamı ve etkisi nedeniyle dikkat çekmektedir. Sızdırılan veriler arasında isimler, e-posta adresleri, telefon numaraları ve hatta finansal bilgiler yer almaktadır. Bu ihlal, kullanıcıların kimlik hırsızlığına ve finansal dolandırıcılıklara maruz kalma riskini büyük ölçüde artırmıştır. Olayın ardından, etkilenen kullanıcıların kişisel bilgilerini koruma altına alabilmeleri için hızlı ve etkili önlemler alınması zorunlu hale gelmiştir.



## Discord Veri İhlali

Popüler mesajlaşma ve sosyal medya platformu Discord, 2024'te büyük bir veri ihlaliyle karşı karşıya kalmıştır. Bu ihlal, milyonlarca kullanıcının kişisel ve hesap bilgilerinin sızdırılmasına yol açmıştır. Saldırganlar, Discord'un veri tabanlarına erişim sağlayarak kullanıcı adları, e-posta adresleri, şifreler ve özel mesajlar gibi hassas bilgilere ulaşmıştır. Discord, bu ihlalin ardından güvenlik protokollerini gözden geçirmiş ve kullanıcılarını güçlü şifreler kullanmaları ve iki faktörlü kimlik doğrulama (2FA) gibi ek güvenlik önlemleri almaları konusunda uyarmıştır. Ayrıca, etkilenen kullanıcılara potansiyel kimlik hırsızlığı ve dolandırıcılıklara karşı dikkatli olmaları tavsiye edilmiştir.

## 916 Google Firewall Veri İhlali

2024 yılının ilk yarısında, Google'ın popüler güvenlik hizmetlerinden biri olan Google Firewall, büyük bir veri ihlali yaşamıştır. "916 Google Firewall İhlali" olarak bilinen bu olayda, siber suçlular, Google'ın güvenlik sistemlerindeki bir açıktan yararlanarak milyonlarca kullanıcının verilerine erişim sağlamıştır. Sızdırılan veriler arasında kullanıcı adları, IP adresleri, tarayıcı geçmişleri ve diğer hassas bilgiler bulunmaktadır. Bu ihlal, kullanıcıların çevrimiçi gizliliğini ve güvenliğini ciddi şekilde tehlikeye atmıştır.

Google, bu olayın ardından güvenlik açıklarını kapatmak ve benzer ihlallerin önüne geçmek için kapsamlı bir inceleme başlatmıştır. Kullanıcılara, hesaplarını güvende tutmak için şifrelerini düzenli olarak değiştirmeleri ve güvenlik ayarlarını sıkılaştırmaları önerilmiştir.

## iSharingSoft Veri İhlali

Lokasyon paylaşım ve takip hizmetleri sunan iSharingSoft, 2024 yılında büyük bir veri ihlali ile karşı karşıya kalmıştır. Bu ihlal, milyonlarca kullanıcının konum bilgileri, kişisel bilgileri ve hesap verilerinin sızdırılmasına neden olmuştur. Siber suçlular, iSharingSoft'un veri tabanlarına sızarak kullanıcıların gerçek zamanlı konum bilgilerini ve geçmiş konum verilerini ele geçirmiştir. Bu durum, kullanıcıların fiziksel güvenliğini tehlikeye atmış ve mahremiyetlerini ihlal etmiştir. iSharingSoft, ihlalin ardından kullanıcılarını bilgilendirmiş ve güvenlik önlemlerini artırmıştır. Kullanıcılara, konum paylaşımı ayarlarını gözden geçirmeleri ve yalnızca güvendikleri kişilerle konum bilgilerini paylaşmaları tavsiye edilmiştir.

# Kritik Zafiyetler

2024 yılında, siber güvenlik dünyasında birçok kritik güvenlik zafiyeti tespit edildi ve saldırganlar tarafından aktif olarak istismar edildi. Bu zafiyetler, yazılım ve sistemlerin güvenliğini ciddi şekilde tehdit etti ve büyük ölçekli güvenlik ihlallerine neden oldu. Öne çıkan bazı kritik güvenlik zafiyetleri ve bunların etkileri şu şekildedir:

- **CVE-2024-1709**: Bu zafiyet, Microsoft Windows işletim sisteminde tespit edildi. Saldırganların, kullanıcıların verilerini çalmasına veya sistemde kötü amaçlı yazılım çalıştırmasına olanak tanır. Bu açık, işletim sistemi bileşenlerinde bulunan bir hatadan kaynaklanmaktadır ve sistemlerin güncellenmesiyle giderilmiştir.
- **CVE-2024-27322:** Atlassian Confluence ürününde tespit edilen bu zafiyet, saldırganların uzaktan kod çalıştırmasına olanak tanır. Confluence kullanıcıları, sistemlerini en son sürüme güncelleyerek bu zafiyeti kapatmalıdır.
- **CVE-2024-2389:** VMware vSphere Client'da tespit edilen bu güvenlik açığı, saldırganların kimlik doğrulama atlatmasına ve yönetici hakları kazanmasına olanak tanır. Bu açık, hassas verilerin çalınmasına veya sistemin kontrol altına alınmasına neden olabilir.
- **CVE-2024-20353:** Apache Log4j kütüphanesinde tespit edilen bir güvenlik açığı, saldırganların uzaktan kod çalıştırmasına ve sistemlere erişim sağlamasına olanak tanır. Log4j kullanıcıları, bu kritik zafiyeti kapatmak için kütüphanenin güncel sürümünü kullanmalıdır.
- **CVE-2024-20359:** Adobe Acrobat Reader'da bulunan bir güvenlik açığı, saldırganların PDF dosyaları aracılığıyla kötü amaçlı kod çalıştırmasına olanak tanır. Kullanıcılar, bu zafiyeti kapatmak için yazılımın en son sürümünü yüklemelidir.
- **CVE-2024-26234:** Cisco IOS ve IOS XE yazılımlarında tespit edilen bu zafiyet, saldırganların uzaktan kod çalıştırmasına ve ağ cihazlarının kontrolünü ele geçirmesine neden olabilir. Bu açık, Cisco tarafından yayınlanan yamalarla giderilmiştir.
- **CVE-2024-29988:** Linux çekirdeğinde tespit edilen bir güvenlik açığı, saldırganların yerel yetki yükseltme yapmasına ve sistemde root yetkisi kazanmasına olanak tanır. Bu zafiyet, çekirdeğin güncellenmesiyle kapatılmıştır.

- **CVE-2024-23917 (TeamCity):** Bu zafiyet, TeamCity On-Premises sürümlerinde tespit edildi. HTTP(S) erişimi olan bir saldırganın kimlik doğrulama kontrollerini atlatarak yönetici yetkileri kazanmasına olanak tanır. Etkilenen sürümler 2017.1 ile 2023.11.2 arasındaki tüm sürümleri kapsar. Bu açık, 2023.11.3 sürümüyle giderilmiştir.
- **CVE-2024-30051 (Windows DWM Core Library):** Microsoft Windows DWM Core Library'de tespit edilen bu yerel yetki yükseltme zafiyeti, CVSSv3 skoru 7.8 olarak değerlendirildi. Saldırganın, sistemde SYSTEM yetkisi kazanmasına olanak tanır. Bu zafiyet, Google Threat Analysis Group, Google Mandiant ve Kaspersky araştırmacıları tarafından keşfedildi ve aktif olarak istismar edilmiştir.
- **CVE-2024-30040 (Windows MSHTML):** Bu zafiyet, Windows MSHTML (Trident) motorunda bir güvenlik özelliği atlama açığı olarak tespit edildi ve CVSSv3 skoru 8.8 olarak değerlendirildi. Saldırganlar, sosyal mühendislik yöntemleri kullanarak kurbanın özel olarak hazırlanmış bir belgeyi açmasını sağlayabilir ve bu belgeyi açtıktan sonra hedef sistemde kod çalıştırabilirler.
- **CVE-2024-3400:** Google Chrome tarayıcısında tespit edilen bir güvenlik açığı, saldırganların zararlı web siteleri aracılığıyla kullanıcıların verilerini çalmasına ve tarayıcıda kod çalıştırmasına olanak tanır. Chrome kullanıcıları, tarayıcılarını en son sürüme güncelleyerek bu zafiyeti kapatmalıdır.
- **CVE-2024-21678 (Atlassian Confluence):** Atlassian Confluence Data Center ve Server ürünlerinde tespit edilen bir saklanan XSS zafiyeti, saldırganların zararlı kod enjekte etmesine olanak tanır. Bu zafiyet, birçok DoS zafiyeti ile birlikte, yüksek önem derecesinde değerlendirilmiştir.

# Siber Saldırılardan Nasıl Korunabilirsiniz?

Kurumunuzun siber alanda güvenliğini sağlamak istiyorsanız eğer, alınması gereken bazı önlemler bulunmaktadır.

**Kullandığımız Yazılımlarda Zafiyet Var mı?**

Zafiyetli olduğu açıklanan yazılımlar eğer kurumunuzda da kullanılıyorsa, bu yazılımların güncellenmesi gerekmektedir. Eğer kullandığınız yazılım uzun bir süredir güncelleme desteğini vermiyor ise, rakip bir ürünün kullanımına geçilmelidir. Aksi takdirde saldırganlar bu yazılım açıklarından faydalanarak kurum içerisindeki ağa erişebilir ve uç noktadaki cihazlar üzerinde zararlı davranışlarda bulunarak sisteme zarar verebilirler.

**Çalışanlarımıza ait Kişisel Bilgiler Sızdırılmış mı?**

Özellikle kurum yöneticilerinin kurumsal hesap bilgileri üçüncü taraf yazılımlardan kaynaklı olarak sızdırılabilmektedir. Sızdırılan bu hesap bilgileri kullanılarak phisihing kampanyaları gerçekleştirilebilir veya sızdırılan hesap bilgilerinin türüne ve önemine göre, şahıs üzerinden kuruma zarar verilebilir. Bu durumların önüne geçmek için belirli periyodlar ile personellerden kurumsal hesap şifrelerini değiştirmeleri istenebilir.

**Çalışanlarımız Siber Güvenlik Konusunda Yeterli Farkındalığa Sahipler mi?**

Alınması gereken belki de en mühim önlem insan farkındalığıdır. Özellikle, bilişim alanına nispeten uzak kalan fakat aynı ağda bulunan çalışanların siber güvenlik farkındalığı eğitimleri almaları elzemdir. Tanımlanan çalışan profili, siber saldırganlar tarafından ilk alınan hedeflerdir. Bu noktada farkındalık eğitimleri ile bu konunun önüne geçebilirsiniz.

**Özetle**,
Her türlü önlem alındığı bir durumda bile siber saldırıya uğrayabilir ve bu saldırıdan zarar alabilirsiniz. Önemli olan alınabilecek potansiyel zararı en aza indirebilmektir.


CYBER THREAT INTELLIGENCE