ECHO

CYBER THREAT INTELLIGENCE

YIL SONU RAPORU

2023

@echocti

@echocti

echocti.com

İçindekiler

Yönetici Özeti

Bu rapor, 2023 yılı boyunca gözlemlenen siber güvenlik alanındaki önemli gelişmeleri özetlemektedir. İlgili başlıklar altında raporlanan olaylar, belirli siber tehditler ve sektördeki önemli eğilimlerin analizini sunmaktadır.

Phishing, zararlı yazılım saldırıları ve fidye yazılımı saldırıları, bu dönemde öne çıkan siber tehditler arasında yer aldı. Kötü niyetli aktörler, kullanıcıları manipüle etmek ve hassas bilgilere erişmek için phishing saldırılarını arttırdılar. Benzer şekilde, zararlı yazılım ve fidye yazılımı saldırıları, kurumların faaliyetlerini olumsuz etkileyerek ciddi riskler oluşturdu.

2023 yılında, belirli siber tehdit aktörlerinin etkinlikleri gözlemlendi. Bu aktörler, karmaşık ve değişken saldırı teknikleri kullanarak kendilerini öne çıkardılar. Aynı zamanda, belirli ülkeler ve sektörler, saldırılara karşı daha fazla maruz kaldılar. Bu durum, siber güvenlik stratejilerinin özellikle sektörel ve coğrafi bazda daha özenli bir şekilde ele alınması gerektiğini vurgulamaktadır.

Önemli veri ihlalleri, kurumların hassas bilgilerini tehlikeye attı ve güvenlik açıklarının kritik olduğunu bir kez daha gösterdi. Bu ihlaller, siber savunma stratejilerinin güçlendirilmesi ve iyileştirilmesi gerekliliğini ortaya koydu.

Son olarak, keşfedilen önemli zafiyetler, sistemlerimizdeki açıkları açıkça gösterdi. Bu zafiyetlerin tespit edilmesi, düzeltilmesi ve gelecekteki saldırılara karşı daha güçlü bir savunma mekanizması oluşturulması kritik bir öncelik haline geldi.

Siber güvenlik tehditleri sürekli olarak evrilmekte olup, kurum olarak güvenlik stratejilerimizi güncellemeye ve iyileştirmeye odaklanmaktayız. Bu rapor, 2023 yılındaki önemli siber güvenlik trendlerini özetlemekte olup, gelecek yıl için daha sağlam bir güvenlik altyapısı oluşturmak adına yol gösterici olacaktır.

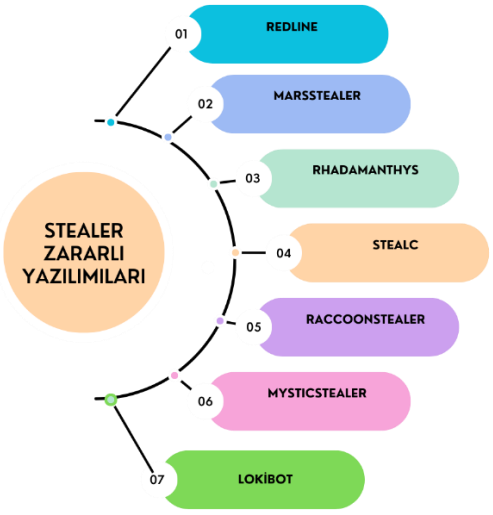
Zararlı Yazılım Saldırıları

Zararlı yazılım saldırıları, siber güvenlik alanında önemli bir tehdit oluşturmaya devam etti ve 2023 yılında bu alandaki gelişim dikkat çekiciydi. Zararlı yazılımların sürekli evrim geçirerek daha sofistike hale gelmesi, kurumlar ve bireyler için ciddi bir risk oluşturdu. Bu yıl içerisinde, özellikle üç tür zararlı yazılım saldırısı sıkça karşımıza çıktı: Bilgi Hırsızları (Stealer) ve Uzaktan Erişim Truva Atı (RAT).

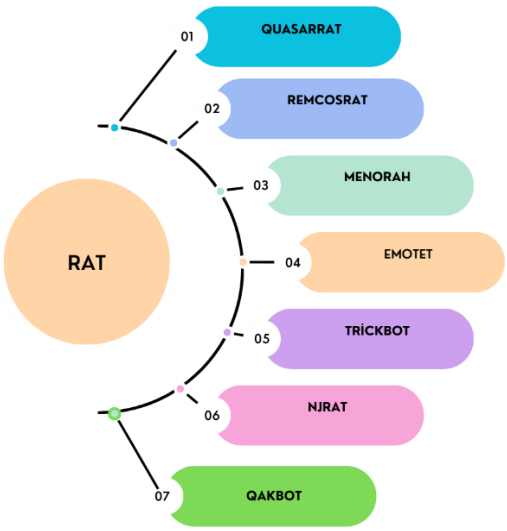
Stealer, kullanıcıların tarayıcı verilerini, şifreleri, oturum açma bilgilerini ve diğer hassas bilgilerini çalmayı hedefleyen zararlı bir yazılım türüdür. Bu yıl içinde, tuş kaydedici yazılımlar (keylogger), çerez hırsızları ve diğer stealer yazılımları, saldırganların sıklıkla kullandığı araçlar arasında yer aldı.

RAT (Remote Access Trojan), saldırganlara uzaktan erişim sağlayarak kurbanın bilgisayarını uzaktan kontrol etmeyi amaçlayan zararlı yazılımlardır. RAT, saldırganlara bilgisayarı ele geçirme, dosya indirme ve diğer zararlı faaliyetlerde bulunma imkânı verir. Bu yıl içinde, çeşitli RAT saldırıları kurumlar üzerinde ciddi etkiler yarattı ve bu tür yazılımların kullanımında artış gözlendi.

2023 yılında en çok etki gösteren Stealer Zararlı Yazılım aileleri



2023 yılında en çok etki gösteren RAT Zararlı Yazılım aileleri



Korunmak için alınabilecek önlemler arasında güvenlik yazılımlarının düzenli olarak güncellenmesi, güçlü şifre politikalarının benimsenmesi ve çok faktörlü kimlik doğrulama gibi güvenlik önlemlerinin uygulanması bulunmaktadır. Ayrıca, çalışanların düzenli güvenlik eğitimlerine tabi tutulması ve bilinmeyen kaynaklardan gelen dosyaların ve linklerin açılmaması konusunda farkındalığın artırılması da büyük önem taşımaktadır.

Zararlı yazılım saldırıları, siber güvenlik stratejilerindeki zayıflıkları hedefleyen ve sürekli gelişen bir tehdit olarak önemini korumaktadır. Bu nedenle, güncel ve kapsamlı bir güvenlik politikası benimseyerek, zararlı yazılımlara karşı etkin bir savunma sağlamak kritik bir gerekliliktir.

Fidye Yazılımı Saldırıları

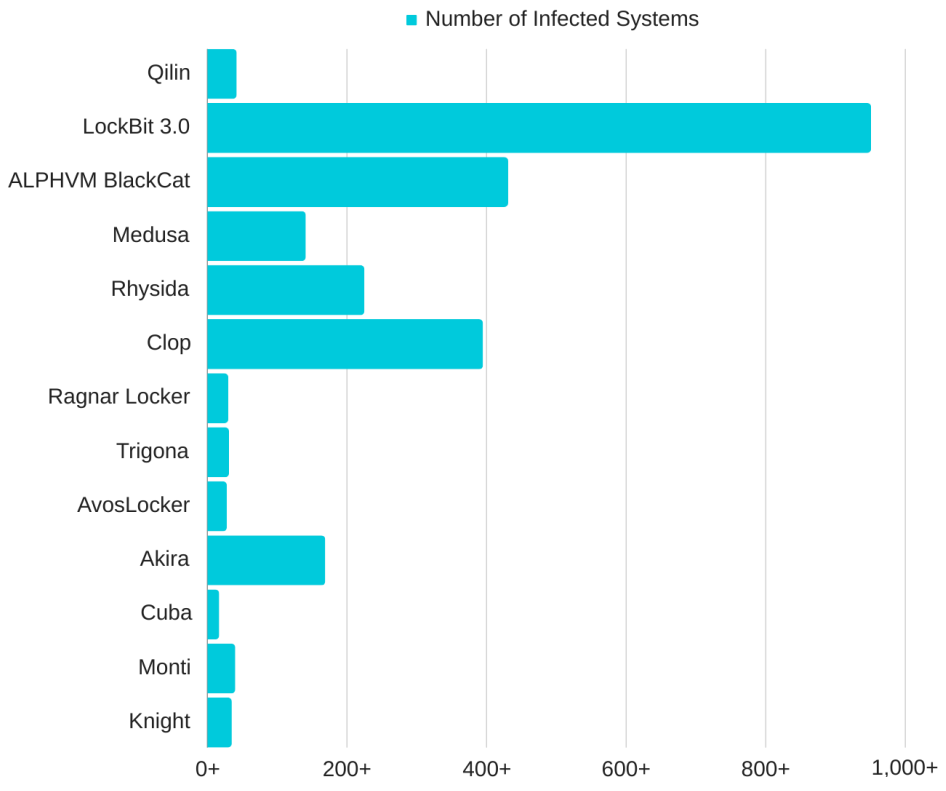
Fidye Yazılımları, bilgisayar sistemlerine sızarak dosyaları şifreleyen veya erişimi engelleyen kötü niyetli bir yazılım türüdür. Genellikle dosyaların veya sistemlerin kilidini açmak için fidye talep etmektedirler.

Bu yazılımlar, bireysel kullanıcıların yanı sıra kurumsal ağları, hükümet sistemlerini, sağlık sektörünü ve finansal kurumlarını da hedef almaktadır. Bu zararlı yazılım, genellikle internet üzerinden gelen e-posta ekleri, kötü amaçlı web siteleri veya güvenlik açıklarını kullanarak sistemlere bulaşmaktadırlar.

Dosyaların şifrelenmesi veya sistem erişiminin engellenmesi gibi yöntemlerle fidye yazılımları, kurumların normal işleyişini durdurabilir ve ciddi finansal zararlara yol açabilmektedir. Ayrıca, bu tür saldırılar kurumların itibarına da zarar vermektedir. Daha detaylı bilgi için 2023 Fidye Yazılımları Saldırı Raporumuzu inceleyebilirsiniz.

En Etkili Fidye Yazılımı Aileleri

Fidye yazılımları, 2023 yılında dijital dünyanın en ciddi tehditlerinden biri haline geldi. Bu yazılımların gelişmiş ve karmaşık yapıları, kurumları ve bireyleri hedef alarak veri kaybına ve mali zararlara neden olabiliyor. Özellikle belirli fidye yazılımı aileleri, hedef odaklı ve sistematik saldırılarla tanınıyor. LockBit, BlackCat ve Clop gibi fidye yazılımı aileleri, kurumların savunma mekanizmalarını aşmayı başararak genellikle büyük fidyeler talep ediyorlar. Bu saldırılar genellikle manuel olarak yönetilen ve hedef odaklı eylemlerden oluşurken, kurumların finansal kayıplarına ve itibar kaybına neden oluyorlar.



Şekil 1 Number of Infected Systems

En Aktif Tehdit Aktörleri

Siber güvenlik alanında, belirli gruplar ve aktörler, karmaşık ve etkili saldırılarıyla öne çıkarak siber tehdit ortamını şekillendiriyor. 2023 yılında, belirli gruplar yüksek profilli siber saldırılar gerçekleştirerek dikkat çekti.

Kuzey Kore Merkezli **Lazarus Grubu**

Lazarus Grubu, Kuzey Kore ile ilişkilendirilen ve finansal hırsızlıkların yanı sıra casusluk faaliyetlerini de içeren sofistike saldırılar gerçekleştiren bir grup olarak bilinir. Bu grup, bankacılık kurumlarına ve kripto para birimi borsalarına yönelik saldırılarla tanınmıştır.

Lazarus APT grubu, 2023 yılında 240 milyon doların üzerinde kripto varlığını çaldı. Sadece son bir yılda, Lazarus APT grubu, Atomic Wallet'tan (100 milyon dolar), CoinsPaid'ten (37.3 milyon dolar), Alphapo'dan (60 milyon dolar) ve Stake.com'dan (41 milyon dolar) dahil olmak üzere çeşitli işletmelerden 240 milyon doların üzerinde kripto varlığı çaldı. Grup ayrıca, son zamanlarda profesyonel global kripto para borsası CoinEx'ten 31 milyon dolar çaldığı şüphesi altında.

Rusya Merkezli **Fancy Bear (APT28) ve Cozy Bear (APT29)**

Fancy Bear ve Cozy Bear, genellikle Rusya istihbaratıyla ilişkilendirilen APT (Advanced Persistent Threat) gruplarıdır. Fancy Bear, hedef ülkelerin hükümet kurumları, medya ve enerji sektörleri gibi çeşitli kurumları hedef alarak casusluk ve bilgi çalma operasyonları gerçekleştirirken, Cozy Bear ise özellikle teknoloji şirketleri ve savunma sektörüne odaklanmıştır.

Çin Merkezli **APT40 ve APT41**

Çin merkezli APT40 ve APT41, Çin devletiyle ilişkilendirilen ve çeşitli sektörlere yönelik geniş kapsamlı saldırılar gerçekleştiren gruplardır. APT40, denizcilik endüstrisi ve hükümet kurumlarına odaklanırken, APT41 daha geniş bir yelpazede telekomünikasyon, oyun endüstrisi ve sağlık sektörü gibi alanları hedeflemektedir.

İran Merkezli **APT33 ve APT34**

APT33 ve APT34, İran kaynaklı siber casusluk gruplarıdır ve enerji, havacılık ve finans gibi sektörlere yoğunlaşmışlardır. APT33, özellikle enerji sektöründe faaliyet gösterirken, APT34 ise teknoloji ve finans kuruluşlarına odaklanmıştır.

En Çok Hedef Alınan Ülke ve Sektörler

2023 yılı, siber saldırılar açısından belirli ülkeler ve sektörler için daha riskliydi. Üç ülke ve üç sektör, siber saldırıların en yoğun olduğu alanlar olarak dikkat çekti.

En Çok Hedef Alınan Ülkeler

1. Amerika Birleşik Devletleri (ABD)

ABD, siber saldırıların en fazla hedef aldığı ülkelerin başında gelmektedir. Özellikle devlet kurumları, teknoloji şirketleri ve finans sektörü, sürekli ve karmaşık saldırılarla karşı karşıya kalmıştır. Siber casusluk ve fidye yazılımı saldırıları, ABD'nin siber güvenlik açısından hassas olduğu sektörler arasındadır.

2. Birleşik Krallık

Birleşik Krallık, siber saldırıların hedefindeki diğer bir ülkedir. Özellikle enerji, sağlık ve eğitim sektörleri, yoğun ve hedefe yönelik saldırıların hedefi haline gelmiştir. Farklı gruplar ve aktörler, ülkenin çeşitli endüstrilerindeki altyapıları hedef alarak ciddi riskler oluşturmuştur.

3. Almanya

Almanya da siber saldırılar açısından etkilenen ülkelerden biridir. Özellikle imalat endüstrisi, teknoloji şirketleri ve sağlık sektörü, sürekli olarak hedef alınan sektörler arasındadır. Veri ihlalleri ve fidye yazılımı saldırıları, ülkenin siber güvenliği için önemli bir tehdit oluşturmaktadır.

En Çok Hedef Alınan Sektörler

Finans Sektörü: Finans sektörü, siber suçluların en çok hedef aldığı sektörlerden biridir. Bankalar, finansal kuruluşlar ve kripto para birimi borsaları, sürekli olarak fidye yazılımı saldırılarına ve veri ihlallerine maruz kalmaktadır.

Sağlık Sektörü: Sağlık sektörü, özellikle pandemi döneminde hedef alınan bir sektör olmuştur. Hastaneler, sağlık kuruluşları ve tıbbi araştırma birimleri, siber suçluların hassas sağlık verilerine erişmeye çalıştığı saldırılara maruz kalmıştır.

Eğitim Sektörü: Eğitim kurumları, öğrenci bilgileri ve akademik verilerin yanı sıra, uzaktan eğitim sistemlerinin zayıf noktaları nedeniyle siber saldırıların hedefi olmuştur. Özellikle online eğitim süreçlerinde yaşanan zafiyetler, siber suçluların dikkatini çekmiştir.

Türkiye'de En Çok Hedef Alınan Sektör: Türkiye'de, finans sektörü, siber saldırıların en çok hedef aldığı sektör oldu. Bankalar, finans kuruluşları ve ödeme sistemleri, fidye yazılımları ve diğer zararlı yazılımların saldırı hedefi haline gelmiştir.

Önemli Veri İhlalleri

Yakult Avustralya, 95 GB veri ihlali ile karşı karşıya

Yakult Australia, bir "cyber incident" yaşadığını doğrulayarak DragonForce adlı siber suçlu grubunun gerçekleştirdiği bir saldırı sonucunda etkilendiğini açıkladı. Şirket, Avustralya ve Yeni Zelanda'daki IT sistemlerinin zarar gördüğünü belirtirken, DragonForce grubunun 95 GB veri sızdırdığı iddia ediliyor. Sızdırılan veriler arasında şirket belgeleri, çalışan kayıtları ve kimlik belgeleri gibi hassas bilgiler bulunuyor. DragonForce, şirketlere ödeme yapmamaları halinde bu tür verileri halka açık olarak sızdırma taktiği izliyor.

Kanada hükümeti veri ihlalini açıkladı

Kanada'da, Brookfield Global Relocation Services (BGRS) ve SIRVA Worldwide Relocation & Moving Services adlı iki taşeron şirketin hacker saldırısına uğradığı ve hassas bilgilerin sızdırıldığı açıklandı. Bu saldırılar, Kanada hükümeti çalışanlarına hizmet veren taşeronların sistemlerindeki verilerin çalınmasına neden oldu. LockBit fidye yazılımı çetesi, SIRVA'nın sistemlerine sızdığını iddia etti ve 1,5TB boyutunda belgeleri ifşa etti.

McLaren Health Care, veri ihlalinin 2,2 milyon kişiyi etkilediğini açıkladı

McLaren Health Care, temmuz ayının sonları ve Ağustos'ta meydana gelen bir veri ihlali sonucunda 2,2 milyon kişinin hassas kişisel bilgilerinin tehlikeye girdiğini açıkladı. Sızıntı, sosyal güvenlik numaraları, sağlık sigortası bilgileri, tıbbi kayıtlar ve daha fazlasını içeriyordu.

Seiko, fidye yazılımı saldırısının hassas müşteri verilerini açığa çıkardığını açıkladı

Seiko, bu yılın başlarında yaşanan bir Black Cat fidye yazılımı saldırısının müşteri, iş ortağı ve personel bilgilerini açığa çıkardığını doğruladı. Saldırı sonucunda Seiko'nun 'Grup', 'İzleme' ve 'Aletler' departmanlarının elinde bulunan toplam 60.000 'kişisel veri' zarar gördü. Fidye yazılımı grubu, üretim planları, çalışan pasaport taramaları, yeni model çıkarma planları, özel laboratuvar test sonuçları ve mevcut ve gelecek Seiko saatlerinin gizli teknik şemalarını içeren bilgileri çaldığını iddia etti.

BHI Energy 690 GB veri ihlaline uğradığını açıkladı

BHI Energy, Akira fidye yazılımının ağlarını nasıl hacklediğini ayrıntılı bir şekilde paylaştı. Akira, Mayıs 2023'te VPN kimlik bilgileriyle BHI ağına giriş yaparak 690 GB veri dahil olmak üzere 767.000 dosyayı çaldı. Firma hemen yetkilileri bilgilendirdi ve dış uzmanlarla iş birliği yaparak saldırıdan etkilenen sistemleri kurtarmaya çalıştı. Şirket, verileri geri yüklemeyi başardı ve fidye ödemeden sistemlerini restore etti. Saldırı sonucunda çalışanların kişisel bilgileri çalındı; mağdurlara Experian üzerinden iki yıllık kimlik hırsızlığı koruma servisine kaydolma talimatları verildi.

Casio, 149 ülkedeki müşterileri etkileyen veri ihlalini açıkladı

Casio Şirketinin ClassPad eğitim platformunun sunucularına sızan bir saldırganın veri ihlali, 149 ülkeden müşterileri etkilediğini ortaya koydu. Saldırı sonucunda kişisel bilgiler, ödeme yöntemleri, lisans kodları ve sipariş detayları gibi bilgilerin sızdığı tespit edildi. Firma, geliştirme ortamındaki ağ güvenlik ayarlarının yanlış yapılandırılması ve yetersiz işletim yönetimi nedeniyle saldırının gerçekleştiğini belirtti.

Medusa Saldırısıyla Toyota Finansal Hizmetler Veri İhlali: 8 Milyon Dolarlık Talep

Toyota Finansal Hizmetler (TFS), Medusa fidye yazılımının şirkete yönelik saldırısını doğruladı ve izinsiz erişim tespit ettiğini açıkladı. Veri sızıntısı tehdidi altında olan şirketin Avrupa ve Afrika'daki sistemlerinden bazılarında yetkisiz erişim saptandı ve fidye yazılımının 8 milyon dolar talep ettiği belirtildi.


ECHO
CYBER THREAT INTELLIGENCE