ECHO

CYBER THREAT INTELLIGENCE

2023 SALDIRI RAPORU

Fidye Yazılımı Saldırıları 2023

Hazırlayan

EchoCTI Team

@echocti @echocti echocti.com

İçindekiler

Yönetici Özeti

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.

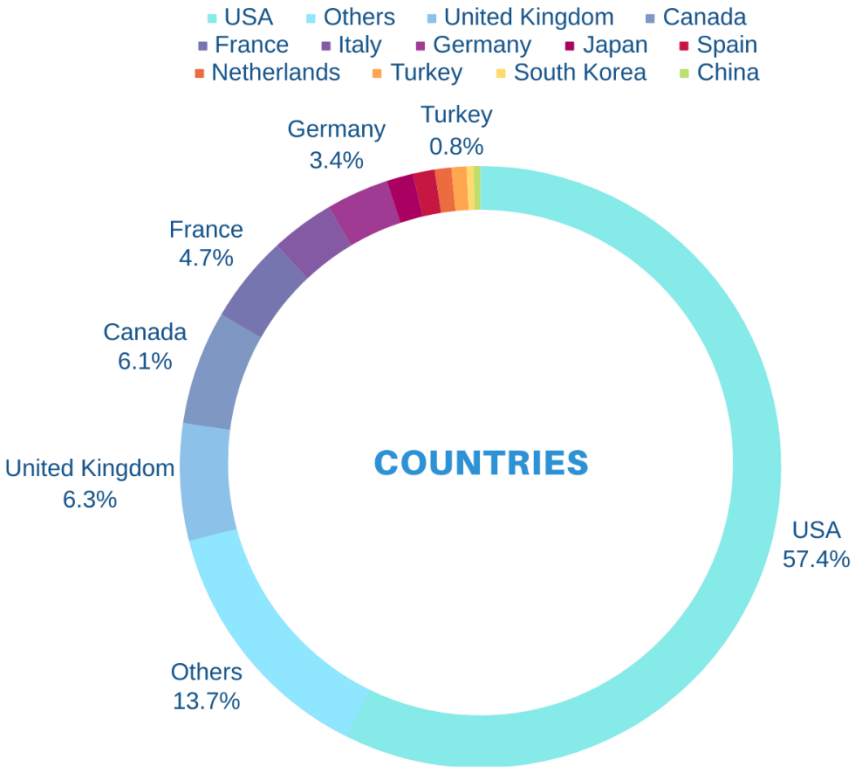
Dosyaların şifrelenmesi veya sistem erişiminin engellenmesi gibi yöntemlerle fidye yazılımları, kurumların normal işleyişini durdurabilir ve ciddi finansal zararlara yol açabilmektedir. Ayrıca, bu tür saldırılar kurumların itibarına da zarar vermektedir.

Bu rapor, yöneticilere ve ilgili paydaşlara fidye yazılımlarının doğasını, etkilerini ve alınabilecek önlemleri anlatarak, kurumların güvenlik politikalarını gözden geçirmesine ve güvenlik açıklarını kapatmasına yardımcı olabilir. Aynı zamanda bu rapor, fidye yazılımlarının potansiyel tehlikelerini vurgulayarak, kurumların daha güvenli bir çevrede faaliyet göstermelerine katkıda bulunmayı hedeflemektedir.

2023 Yılında Fidye Yazılımları

Fidye yazılımlarının yükselen etkisi 2023 yılında da devam etti. Bu yıl, fidye yazılımları küresel olarak yaygınlaşarak, çeşitli ülkelerde ve sektörlerde ciddi etkilere yol açtı.

Hedef Alınan Ülkeler



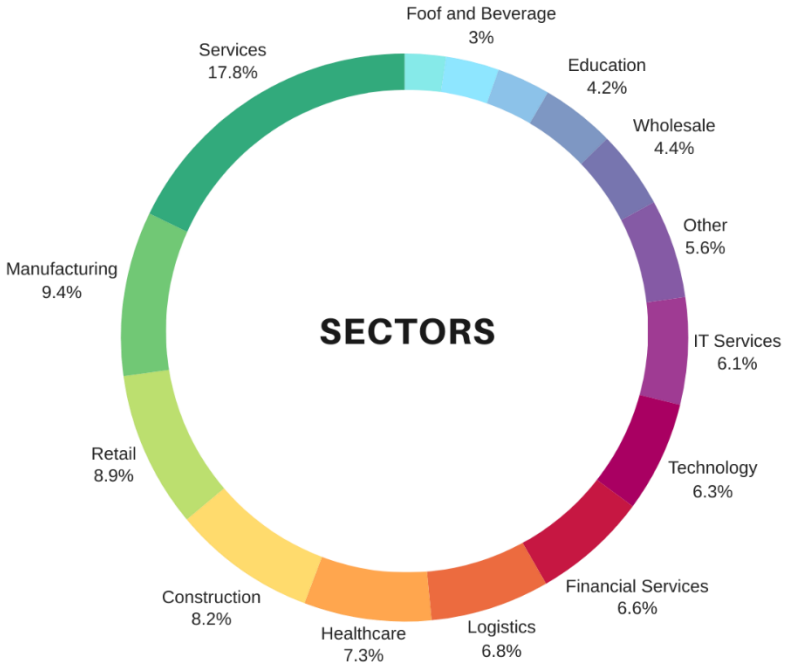
Şekil 1 Targeted Country by Ransomwares

Fidye yazılımları, 2023 yılında dünya genelinde yaygın etkilere sahipti. Enfekte olan sistem sayılarına bakıldığında, ABD 1478 sistemle en çok etkilenen ülke konumunda. Ardından Birleşik Krallık 162, Kanada 158 ve Almanya 87 enfekte sistemle sırasıyla yer aldı.

Diğer yandan, Çin 9, Güney Kore 10 ve Türkiye 21 enfekte sistemle daha düşük seviyelerde etkilendi. İtalya 88, Fransa 121, İspanya 30, Hollanda 23 ve Japonya 37 ise fidye yazılımlarının etkisine maruz kalan diğer ülkeler arasındaydı.

Bu veriler, fidye yazılımlarının coğrafi olarak farklı etki seviyelerine sahip olduğunu ve özellikle belirli ülkelerde daha yoğun bir şekilde görüldüğünü göstermektedir.

Hedef alınan Sektörler

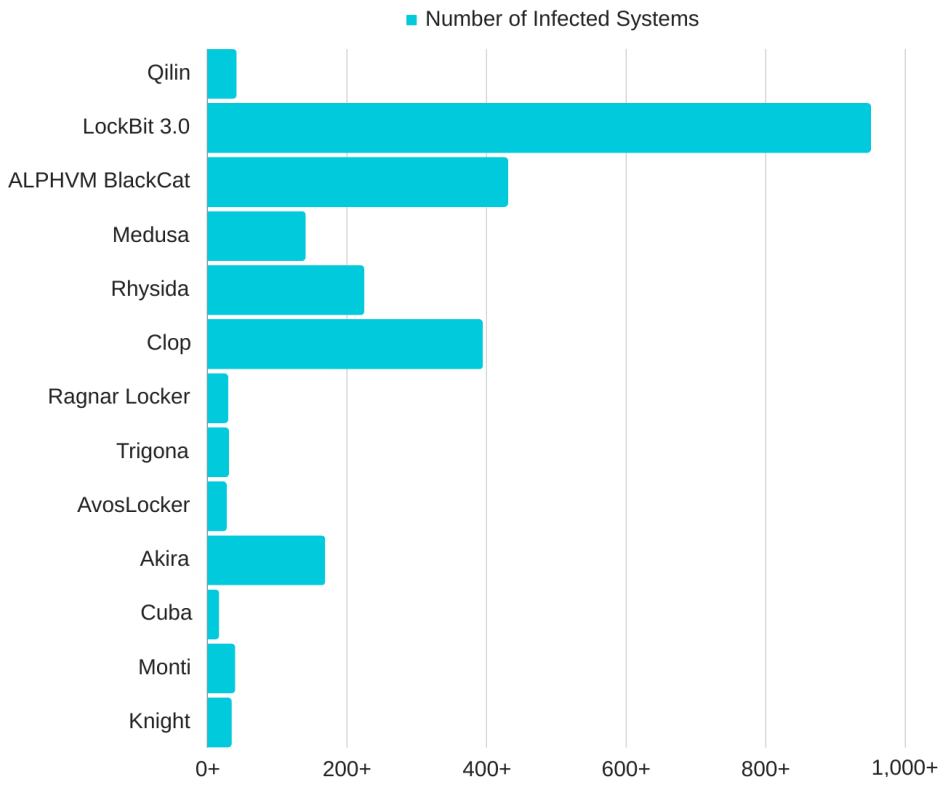


Şekil 2 Target Sectors

Bu veriler, fidye yazılımlarının geniş bir sektör yelpazesine yönelik tehdit oluşturduğunu gösteriyor. Farklı sektörlerin, saldırı sayıları açısından farklı düzeylerde etkilendiği ve bu saldırıların çeşitli endüstrilerde ciddi bir tehdit oluşturduğu ortaya çıkıyor.

En Etkili Fidye Yazılım 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 3 Number of Infected Systems

LockBit

LockBit 3.0, ilk ortaya çıktığı 2019 yılından beri fidye yazılımı ailelerinin arasında son derece tehlikeli bir üye olmuştur. Bu nedenle, Dünya genelinde birçok kuruluş için ciddi bir siber güvenlik tehdidi oluşturmaktadır. LockBit, kurban sistemlerdeki verileri şifreleyerek çalışmakta ve ardından verilerin çözümlenmesi karşılığında fidye talep etmektedir. Ancak LockBit 3.0, sadece verileri şifrelemekle kalmamakta, aynı zamanda çevrimiçi olarak bu verilerin yayınlanması tehdidi ile kurbanları zorlamaktadır, bu da organizasyonların itibarını ve güvenilirliğini zedelemektedir. LockBit 3.0, kurbanın sistemlerine dağıtıldığında oldukça gelişmiş şifreleme algoritmaları kullanmaktadır. Bu durum, verileri şifrelerinin kırılmasını son derece zorlaştırmakta ve kurbanları fidye ödemeye zorlamaktadır. Fidye, genellikle kripto para birimleriyle ödenmekte, dolayısıyla ödenen fidyenin izlenmesi imkânsız olabilmektedir. LockBit Fidye Yazılımı Ailesi hakkında daha fazla bilgi almak için ayrıca bakınız.

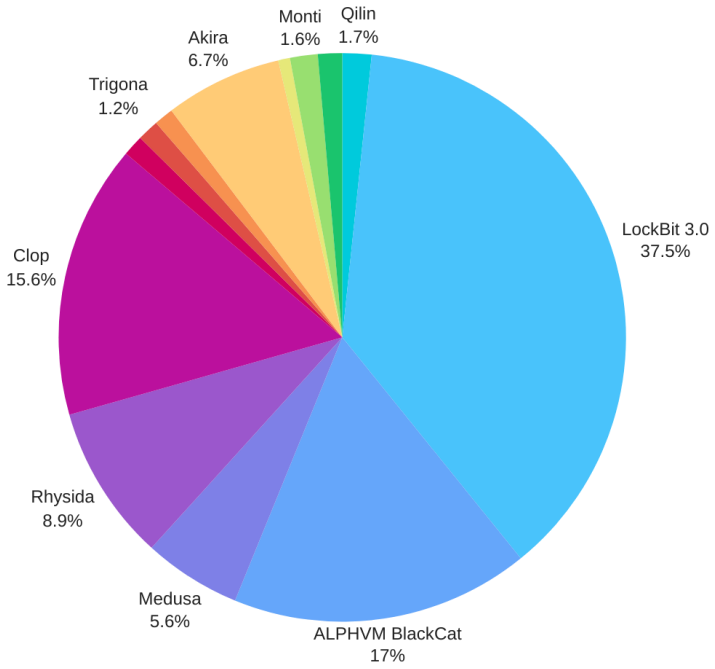
Şekil 4 Stopwatch of LockBit 3.0

BlackCat

BlackCat veya Noberus olarak da bilinen ALPHV, Hizmet Olarak Fidye Yazılımı (RaaS) operasyonlarının bir parçası olarak dağıtılan bir fidye yazılımı ailesidir. ALPHV, Rust programlama dilinde yazılmıştır ve Windows, Linux tabanlı işletim sistemleri (Debian, Ubuntu, ReadyNAS, Synology) ve VMWare ESXi üzerinde çalıştırmayı destekler. ALPHV, siber suç forumlarında ALPHV olarak pazarlanmaktadır, ancak sızıntı sitesinde görünen bir kara kedi simgesi nedeniyle güvenlik araştırmacıları tarafından genellikle BlackCat olarak adlandırılmaktadır. ALPHV'nin 18 Kasım 2021'den bu yana fidye yazılımı saldırılarında kullanıldığı gözlemlenmiştir.

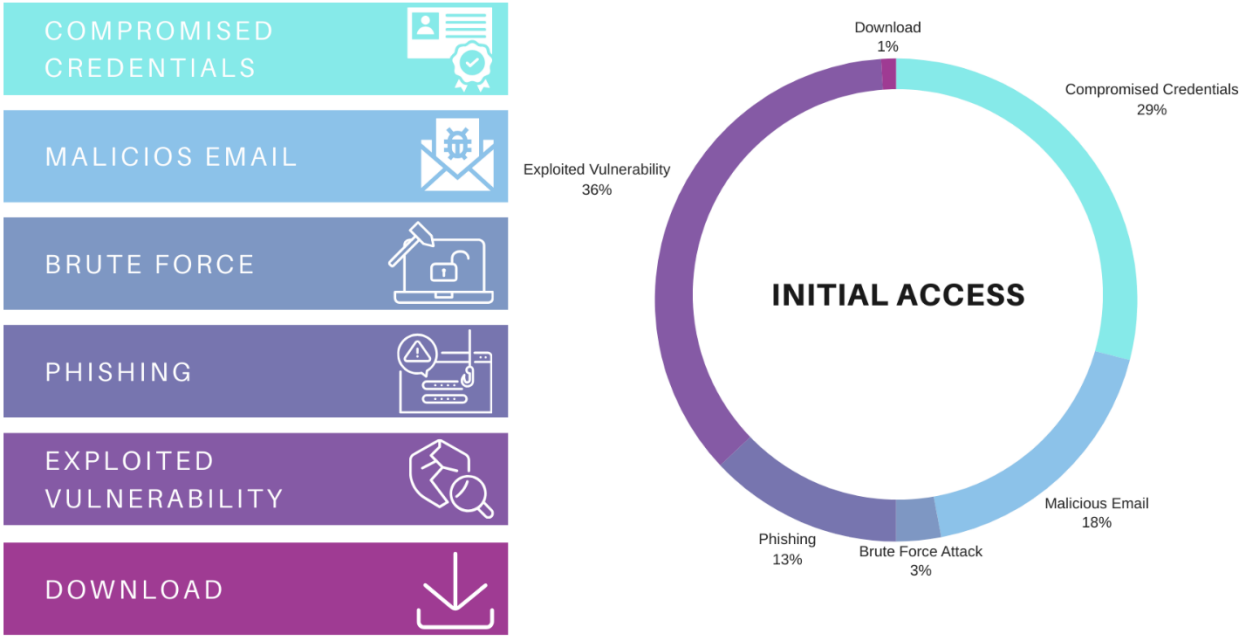
CLOP

Clop, kurbanın dosyalarını şifreledikten sonra ".clop" uzantısını kullanan bir fidye yazılımıdır. Clop'a ait bir başka benzersiz özellik de dizedir: "Dont Worry C|0P" fidye notlarına dahil edilmiştir. CryptoMix fidye yazılımının bir çeşididir, ancak kullanıcı alanı tespitinden kaçınmak için Windows Defender'ı devre dışı bırakmaya ve Microsoft Security Essentials'ı kaldırmaya çalışır.



Şekil 5 Rate of effects of Ransomware Families

En Çok Kullanılan Sızma Teknikleri (Initial Access)



Şekil 6 Most Initial Access Methods

Fidye yazılımlarının bulaşmasında kullanılan çeşitli sızma teknikleri, 2023 yılında farklı seviyelerde etkiler gösterdi. En çok tercih edilen teknikler arasında "Exploited Vulnerability" (36 saldırı), fidye yazılımlarının bulaştığı sistemlerdeki güvenlik açıklarını hedefleyerek ve bu açıkları kullanarak sisteme sızmak için yaygın bir yöntem olarak öne çıktı. Bu teknik ile saldırganlar, genellikle yazılım veya uygulama zayıflıklarından faydalanarak fidye yazılımlarını yaymaya çalışmaktadırlar.

Bunun yanı sıra, "Compromised Credentials" (29 saldırı) yani tehlikeye düşmüş kimlik bilgileri, saldırganların hedef sistemlere yetkisiz erişim sağlamak için kullanılan bir diğer yaygın teknikti. "Malicious Email" (18 saldırı) yoluyla yapılan saldırılarda, genellikle kullanıcıları yanıltarak veya kötü amaçlı ekler aracılığıyla fidye yazılımlarını yaymaya çalışan phishing saldırıları arasında yer alıyordu. "Phishing" (13 saldırı) ve "Brute Force Attack" (3 saldırı) ise kullanıcıların dikkatsizliklerinden veya zayıf şifrelerden faydalanarak sisteme sızmak için kullanılan diğer yaygın teknikler arasındaydı. "Download" (1 saldırı) ise az sayıda görülen bir teknikti ve genellikle güvensiz indirmeler yoluyla fidye yazılımlarının bulaşmasını sağlamaktaydı.

Bu veriler, fidye yazılımlarının sisteme sızmak için çeşitli teknikler kullandığını ve bu tekniklerin kullanım sıklıklarının farklılık gösterebildiğini gösteriyor. Bu nedenle, güvenlik açıklarının kapatılması, kullanıcıların eğitimi ve güvenlik yazılımlarının güncel tutulması gibi önleyici adımların alınması, fidye yazılımlarının etkilerini azaltmak için önemli bir faktördür.

2023 Yılında Yaşanan Önemli Fidye Yazılımı Vakaları

Henry Schein ve BlackCat Saldırıları: Sağlık Devi Üçüncü Kez Ransomware Saldırısına Uğradı

Henry Schein, son bir ay içinde BlackCat/ALPHV ransomware çetesi tarafından iki kez saldırıya uğradı. Şirket, uygulamalarının ve e-ticaret platformunun devre dışı bırakıldığını bildirerek siparişleri alternatif kanallarla almaya ve müşterilere sevkiyat yapmaya devam etti.

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.

LockBit Fidye Yazılımıyla Boeing'in Verileri Sızdırıldı: Gigabaytlarca Veri Tehlikede

LockBit fidye yazılımı çetesi, Boeing'in verilerini sızdırdı ve şirketin ticari uçaklar ve savunma sistemleri hizmeti veren en büyük havacılık şirketlerinden birinden 43GB'dan fazla veri yayınladı. Boeing, fidye ödemeyi reddettiği için hacker grubu verileri kamuya açık hale getirdi. Bu veriler arasında IT yönetim yazılımı için yapılandırma yedekleri ve izleme denetim araçlarına ait kayıtlar bulunuyor.

SysAid Sıfır Gün Açığı Clop Fidye Yazılımı Saldırılarında Kullanıldı

Microsoft Tehdit İstihbarat ekibi, hizmet yönetimi yazılımı SysAid'deki sıfır gün açığının Clop fidye yazılımı saldırıları için kullanıldığını keşfetti. Bu zafiyet, kurumsal sunuculara erişim sağlamak ve Clop fidye yazılımını dağıtmak amacıyla kötü niyetli aktörler tarafından kullanıldı.

Akira Fidye Yazılımıyla ABD'li Enerji Firmasının Veri İhlali: Kapsamlı Saldırı Ayrıntıları Paylaşıldı

BHI Energy, Akira fidye yazılımı çetesinin ağlarına nasıl sızdığını ve saldırı sırasında nasıl veri çaldığını detaylandırarak nadir bir şeffaflık örneği sergiledi. Bu enerji hizmetleri firması, Akira fidye yazılımı grubunun Mayıs 2023'te ağlarına sızarak büyük miktarda veri çaldığını ve ransomware saldırısını gerçekleştirdiğini açıkladı.

ALPHV Fidye Yazılımı Çetesi Florida Mahkeme Sistemlerine Saldırdı

ALPHV (BlackCat) fidye yazılımı çetesi, Florida'nın Kuzeybatı Bölgesi (İlk Yargı Devresi'nin bir parçası) mahkemelerini etkileyen bir saldırıyı üstlendi. Saldırganlar, hakimler dahil olmak üzere çalışanların Sosyal Güvenlik numaraları ve özgeçmişlerini ele geçirdiklerini iddia ediyorlar.

BlackCat Fidye Yazılımı, Sphynx Şifreleyici ile Azure Depolama Hizmetlerini Hedef Aldı

BlackCat (ALPHV) fidye yazılımı çetesi, Microsoft hesaplarını çalarak ve yeni keşfedilen Sphynx şifreleyiciyi kullanarak hedeflerin Azure bulut depolama alanlarını şifrelemeye başladı. Bu saldırıda toplamda 39 Azure Depolama hesabı şifrelendi.

Siemens Energy ve Schneider Electric, Clop Fidye Yazılımı Saldırısı Sonucunda Veri Sızıntısı Yaşadı

SIEMENS energy

Siemens Energy, Clop fidye yazılımı saldırıları sonucunda, MOVEit Transfer platformundaki sıfır gün açığı kullanılarak veri sızıntısı yaşandığını doğruladı.

Clop Fidye Yazılımı Saldırısı: Ontario Kurumuna Ait Veri Sızıntısı 3.4 Milyon Kişiyi Etkiledi

Ontario hükümeti tarafından finanse edilen sağlık kuruluşu olan Better Outcomes Registry & Network (BORN), Clop fidye yazılımının MOVEit hack olaylarının kurbanlarından biri oldu.

İtalyan Cloud Hizmet Sağlayıcısına Yönelik Lockbit 3.0 Fidye Yazılımı Saldırısı: Kamu Hizmetlerini Olumsuz Etkiledi

İtalya'nın Westpole adlı bulut hizmet sağlayıcısına Lockbit 3.0 fidye yazılımı saldırısı, PA Digitale şirketinin hizmetlerinin çökmesine ve 1300'den fazla kamu kuruluşunun etkilenmesine yol açtı. ACN, saldırıdan etkilenen 1000'den fazla kuruluşun verilerini kurtarmak için çaba gösteriyor. Bu saldırı, İtalyan kamu yönetiminin şimdiye kadar karşılaştığı en ciddi tehditlerden biri olarak nitelendiriliyor.


ECHO
CYBER THREAT INTELLIGENCE