ECHO

CYBER THREAT INTELLIGENCE

FİNANS SEKTÖRÜ

SALDIRI RAPORU

2023

@echocti

@echocti

echocti.com

İçindekiler

Yönetici Özeti

Bu rapor, 2023 yılında finans sektörüne yönelik siber saldırılar hakkında kapsamlı bir inceleme sunmaktadır. Finans sektörünün giderek dijitalleşmesi ve siber tehditlerin artan karmaşıklığı, finans kuruluşlarının siber güvenlik önlemlerini gözden geçirmesini zorunlu kılmaktadır. Rapor, bu tehditleri ve sektörün güvende kalma stratejilerini anlamak için önemli bir kaynaktır.

Raporda, 2023 yılında finans sektöründe görülen siber saldırı türleri ve bu saldırıların sıklığı üzerine odaklanılmıştır. Ayrıca, siber saldırıların arkasındaki aktörlerin kimlikleri ve motivasyonları da ele alınmıştır. Öne çıkan siber saldırı olayları incelenerek, sektördeki olası etkileri değerlendirilmiştir.

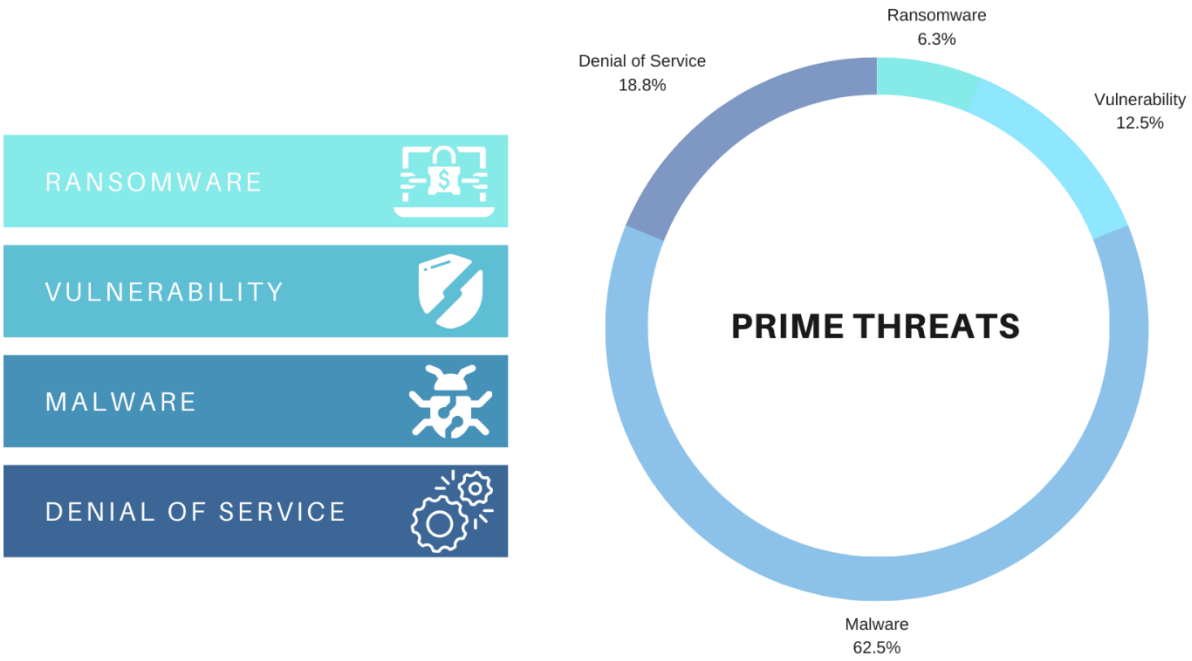
Finans sektörü liderlerine, siber güvenlik önlemlerini güçlendirmeleri ve gelecekteki tehditlere karşı hazırlıklı olmaları için öneriler sunulmuştur. Acil durum müdahale planlarının oluşturulması ve siber güvenlik en iyi uygulamalarının benimsenmesi, finans sektörünün siber saldırılara karşı direncini artırabilir. Gelecekteki tehditlere karşı proaktif bir yaklaşım benimsemek, finans kuruluşlarının verilerini ve itibarlarını korumalarına yardımcı olabilir.

Bu rapor, finans sektörü liderlerinin siber güvenlik stratejilerini güçlendirmelerine ve gelecekteki siber tehditlere karşı hazırlıklı olmalarına rehberlik etmek için tasarlanmıştır. Finans sektörü, siber güvenlik konusundaki ciddiyeti artırmalı ve siber saldırılara karşı etkili bir savunma sağlamalıdır.

Siber Saldırılar ve Trendler

2023 Yılında Finans Sektöründe Gözlemlenen Siber Saldırı Türleri

Bu rapor, 2023 yılında finans sektörünü hedef alan siber saldırı türlerini incelemekte ve bu saldırı türlerinin finans kuruluşlarına yönelik tehditleri nasıl etkilediğini ele almaktadır. Ayrıca, Grafik 1'de siber saldırı türlerinin finans sektöründeki yükselen saldırı trendlerine nasıl katkıda bulunduğu gösterilmektedir.



Grafik 1 Prime Threats

Ransomware

Ransomware, finans sektörünün 2023 yılında karşı karşıya kaldığı en büyük siber saldırı tehditlerinden biridir. Bu saldırı türü, kötü niyetli yazılımın hedef sistemi kilitleyerek verilere erişimi engellemesi ve genellikle fidye ödenene kadar verilerin serbest bırakılmaması ile karakterizedir. Ransomware saldırıları finans kuruluşları için büyük bir risk oluşturur ve bu tür saldırılara karşı güçlü bir savunma gerekmektedir.

Malware

Malware, finans sektörünü hedef alan siber saldırıların sıkça kullanılan bir bileşenidir. Kötücül yazılım, finans kuruluşlarının ağlarına sızarak bilgi çalma, izleme veya zararlı işlemler gerçekleştirme yeteneğine sahiptir. Bu tür saldırılar, hassas finansal verilerin sızdırılmasına veya finans kuruluşlarının operasyonlarının bozulmasına yol açabilir. Genellikle finans kuruluşlarına ait müşteriler hedef alınmaktadır. Bilgileri ele geçirilen müşterilerin, hizmet aldıkları kuruluşlarda bulunan tüm varlıkları tehlikeye girmektedir.

Vulnerability

Siber saldırganlar, kurumların kullanmakta olduğu teknolojilerdeki açıkları kullanarak siber saldırılar gerçekleştirebilmektedir. Bu tür saldırılar, finans kuruluşlarının güvenlik sistemlerini aşma veya hassas bilgilere erişim sağlama amacı gütmektedir.

Denial of Service

Hizmet reddi saldırıları, finans sektöründe sıkça karşılaşılan siber tehditlerden biridir. Bu tür saldırılar, kurumların hizmet sunma yeteneklerini aksatabilmekte ve hatta hizmetlerini çevrimdışı bırakabilmektedir. Hizmet reddi saldırıları, kurumların itibarına, müşteri memnuniyetine ve operasyonel sürekliliğine zarar verebilmektedir.

2023 Yılında Finans Sektöründe Gerçekleşen Siber Saldırılar

Deutsche Bank Veri Sızıntısında Müşteri Verilerinin Etkilendiğini Onayladı

Deutsche Bank, bir hizmet sağlayıcısındaki veri sızıntısının müşteri verilerini etkilediğini doğruladı. Banka, olası bir MOVEit Transferi veri hırsızlığı saldırısının etkisi altında olduğunu belirtti ve siber güvenlik önlemlerini güçlendirmek amacıyla olayı soruşturuyor. Almanya genelinde 100'den fazla şirketin etkilendiği düşünülen olay, Clop fidye yazılımının MOVEit saldırı dalgasıyla ilişkilendirildi.

Level Finance Kripto Borsası, İki Güvenlik Denetimine Rağmen Hacklendi

Level Finance, akıllı sözleşmesindeki bir güvenlik açığından yararlanan hackerlar tarafından 214.000 LVL tokeni (yaklaşık 1,1 milyon dolar) çalındığı tespit edildi. Saldırı, likidite havuzu ve DAO hazinesini etkilemedi, ancak LVL tokenine değer kaybettirdiği gözlemlendi.

Lazarus Grubu, Güney Koreli Finansal Kuruluşu Zero-Day Açıklarından Yararlanarak Siber Saldırılara Devam Ediyor

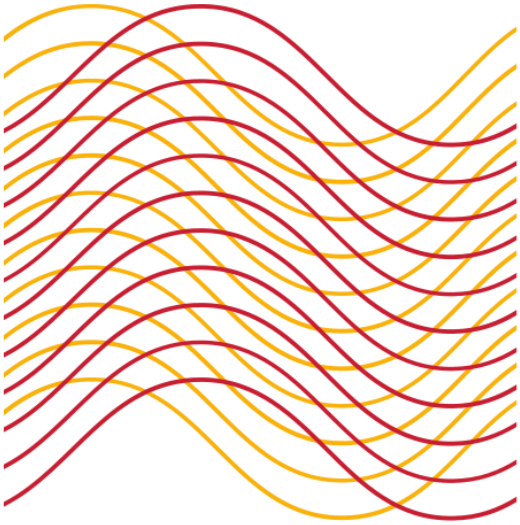
Kuzey Kore bağlantılı Lazarus Grubu, Güney Koreli finansal kuruluşlara, bir yıl içinde iki kez, gizli bir yazılımdaki zero-day güvenlik açıklarından yararlanarak saldırdı. Saldırganlar, ilk saldırıda kamu kurumları ve üniversiteler tarafından yaygın olarak kullanılan bir sertifika yazılımının savunmasız bir sürümünü kullandı. Ekim 2022'deki yeniden sızma girişimi de aynı programdaki bir başka zero-day açığından yararlanmayı içerdiği tespit edildi.

Microsoft, JetBrains TeamCity Zafiyetini Kullanan Kuzey Kore Saldırıları Hakkında Uyarıda Bulundu

Microsoft, Kuzey Kore tehdit aktörlerinin JetBrains TeamCity'deki kritik bir güvenlik açığını kullanarak savunmasız sunuculara saldırdığını bildiriyor. Saldırılar, Diamond Sleet ve Onyx Sleet olarak bilinen Lazarus Group'un parçası olan iki tehdit grubu tarafından gerçekleştiriliyor ve çeşitli tekniklerle TeamCity sunucularını hedef alıyor.

Alman Mali Kurumunun Sitesi DDoS Saldırısına Maruz Kaldı

Alman Federal Finansal Denetleme Kurumu (BaFin), yaptığı açıklamada, bir dağıtılmış hizmet engelleme (DDoS) saldırısının web sitesine etki ettiğini duyurdu. BaFin, Almanya'nın finansal düzenleme otoritesi olup, 2,700 bankayı, 800 finansal ve 700 sigorta hizmeti sağlayıcısını denetleme sorumluluğuna sahiptir. Saldırı sonucunda BaFin, kamu web sitesini "bafin.de" adresinden geçici olarak kapatma kararı alındığı ancak diğer önemli sistemlerinin sorunsuz çalıştığı belirtildi.

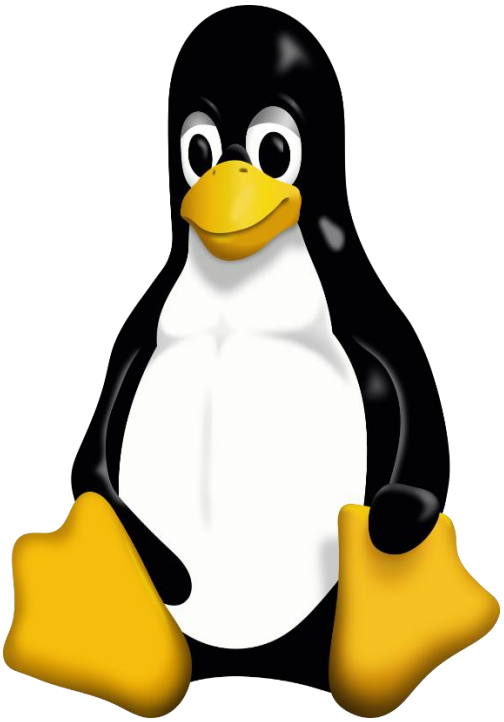


Ukraynalı Hackerlar, Rus Bankaları İçin Hizmet Sağlayıcısını Devre Dışı Bıraktı

Cyber.Anarchy.Squad adlı Ukraynalı hacker grubu, Rus telekom sağlayıcısı Infotel JSC'yi devre dışı bırakan bir saldırıyı üstlendi. Moskova merkezli Infotel, Rus Merkez Bankası ile diğer Rus bankaları, online mağazalar ve kredi kurumları arasında bağlantı hizmetleri sağlamaktadır. Saldırı sonrasında Rusya genelinde birçok büyük bankanın online ödemeler yapamayacak şekilde bankacılık sistemlerine erişimi kesildi.

Çin'in BlackTech Hacker Grubu, ABD ve Japon Şirketlerini Hedef Almak İçin Router Cihazlarını Kullandı

Japonya ve ABD siber güvenlik ajansları, Çin merkezli bir devlet destekli hacker grubu olan BlackTech'in, şubelerin router'larını gizlice değiştirerek bunları çeşitli şirketlerin ağlarına erişim noktası olarak kullanma girişiminde bulunduğuna dair uyarılarda bulundu.



Finans Devlerini Hedef Alan AitM Phishing ve BEC Saldırılarını Ortaya Çıktı

Bankacılık ve finans hizmetleri organizasyonları, yeni çok aşamalı bir "AitM" phishing ve iş e-postası komplosu saldırısının hedefi oldu. Saldırı, saldırganların esnek bir şekilde phishing sayfalarını hedeflerine uyarlamalarına ve oturum çerezlerini çalmalarına olanak tanıyan endirekt bir proxy kullanımına odaklanarak gerçekleştirildi.

Scattered Spider Fidye Yazılımı Saldırıları ile Tehdit Oluşturmaya Devam Ediyor

Scattered Spider olarak bilinen tehlikeli bir tehdit grubunun, hedeflenen firmalarda yeni işe alınmış gibi davranarak normal işe alma süreçlerine karıştığı ve dünya genelinde hesapları ele geçirme stratejisini kullandığı tespit edildi. Bu finansal motivasyonlu hacker grubu "en tehlikeli finansal suç gruplarından biri" olarak tanımlandı. Operasyonel esnekliğini ve saldırı modeline SMS phishing, SIM takası ve help desk dolandırıcılığı gibi unsurları katan bu grup, tehlikesini sürdürmeye devam etmekte.

FakeCalls Android Kötü Amaçlı Yazılımı, Yeni Versiyonu Tespit Edildi

Güney Kore'de gündemde olan Android kötü amaçlı yazılım FakeCalls, finans kuruluşlarını taklit ederek banka müşterilerinden kredi kartı bilgilerini çalmaya çalışıyor. Köklü bir sorun olan sesli dolandırıcılık (vishing) Güney Kore'de 2020'de kurbanlara 600 milyon doların üzerinde maliyet getirdi. FakeCalls zararlı yazılımının yeni sürümlerinin, analiz araçlarını atlatmak için yeni teknikler bulundurduğu ve saldırıya uğrayan cihazlardan ses ve video akışlarını çalma yeteneğine sahip olduğu belirtildi.

Xenomorph Android Zararlı Yazılımı Güncellendi, Bankaları Hedeflemeye Devam Ediyor

Xenomorph Android zararlı yazılımının üçüncü sürümü, otomatik transfer sistemine ve 400 bankadan veri çalma yeteneğine sahip olarak piyasaya sürüldü. Otomatik fon transferleri gerçekleştirebilme ve kimlik bilgilerini çalma yeteneğine sahip Xenomorph, en gelişmiş ve tehlikeli Android zararlı yazılım trojanlarından biri olarak kabul ediliyor.

İmzalı Windows Sürücüsü Kullanan Bluebottle Hackerları, Bankalara Saldırı Gerçekleştirdi

Fransızca konuşulan ülkelerde faaliyet gösteren Bluebottle hacker grubu, imzalı bir Windows sürücüsü kullanarak bankalara yönelik saldırılar gerçekleştirdi. İmzalı kötü amaçlı sürücünün, güvenlik ürünlerini devre dışı bırakmak için kullanıldığı tespit edildi. Bu saldırıların, bankalardan 11 milyon doların üzerinde varlık çalan bir tehdit aktörü tarafından düzenlendiği tahmin edilmektedir. Bluebottle grubunun OPERA1ER hacker grubunun taktiklerini benimsemesi nedeniyle bu grupların aynı olabileceği düşünülmektedir.

İran Kaynaklı Bir Siber Casusluk Grubu, Orta Doğu'daki Finans ve Hükümet Kurumlarını Hedef Alıyor

Orta Doğu'da finans, hükümet, askeri ve telekomünikasyon sektörlerine yönelik karmaşık siber casusluk kampanyası düzenleyen Scarred Manticore adlı grubun, İran'ın İstihbarat ve Güvenlik Bakanlığı ile bağlantılı olduğu düşünülüyor. Tespit edilen bu kampanyada, bilinmeyen bir pasif kötü amaçlı yazılım çerçevesi olan LIONTAIL kullanıldığı ve özellikle Windows sunucularının hedef alındığı gözlemlendi. Grup, saldırıları gerçekleştirmek için özel web kabukları (shell), DLL arka kapıları ve sürücü tabanlı implantlar kullanmaktadır.

Latin Amerika'daki Kullanıcılara Yönelik Yeni Finansal Tehdit: JanelaRAT

Latin Amerika'daki kullanıcıları hedef alan JanelaRAT adlı finansal zararlı yazılımın, DLL side loading teknikleri kullanarak LATAM banka ve finans kurumlarından hassas bilgileri ele geçirebildiği tespit edildi. JanelaRAT, DLL size loading yöntemiyle tespitleri atlatmakta ve meşru kaynaklardan alınan ZIP arşivleri ile yayılmaktadır. Ayrıca zararlı yazılımın, fare girişlerini takip etme, tuş vuruşlarını kaydetme ve ekran görüntüleri alma gibi özelliklere sahip olduğu tespit edildi.

Mali Dolandırıcılık İçin Erişilebilirlik Özelliğini Kullanan MMRat Android Truva Atı Ortaya Çıktı

Güneydoğu Asya'yı hedef alan MMRat Android truva atı, Haziran 2023'ten beri mobil cihazları ele geçirip mali dolandırıcılık faaliyetlerinde bulunuyor. Zararlı yazılım, özel bir komut kontrol protokolü kullanarak büyük veri transferi gerçekleştiriyor ve Endonezya, Vietnam, Singapur ve Filipinler gibi ülkelerdeki kullanıcıları hedef alıyor. MMRat, resmi görünümlü phishing siteleri aracılığıyla yayılıyor ve hükümet ya da arkadaşlık uygulaması gibi kamufle oluyor. Uygulama, Android erişilebilirlik servisi ve MediaProjection API gibi araçları kullanarak cihazlarda kötü amaçlı faaliyetlerde bulunuyor.

Google Ads Üzerinden Yayılan LOBSHOT Finans Truva Atı Tehlikesi

LOBSHOT, Google Ads'ı kullanarak kötü amaçlı yazılım yayınlayan bir tehdit aktörü tarafından geliştirilen bir finans truva atıdır. Zararlı yazılım, sahte sayfalardan edinilen meşru araçları taklit ederek, hVNC bileşeni aracılığıyla bilgisayarlara gizlice erişim sağlama yeteneğine sahiptir. Daha önce Dridex bankacılık truva atı ile ilişkilendirilen TA505, LOBSHOT'u kullanarak veri hırsızlığı ve finansal dolandırıcılık amacıyla kötü amaçlı yazılım araçlarını genişletmektedir.

Nexus Android Banking Trojan

Yükselen bir Android bankacılık truva atı olan Nexus, 450'den fazla finans uygulamasını hedef alarak sahtekârlık faaliyetlerinde bulunuyor. Nexus, ATO saldırıları gerçekleştirmek üzere tasarlanmış olup, kullanıcı kimlik bilgilerini çalmak, SMS'leri ele geçirmek ve fidye yazılımı modülü entegre etmek gibi ana özelliklere sahiptir. Nexus'un, Türkiye'de özellikle yaygın olarak kullanıldığı ve finansal dolandırıcılığa karşı yeni bir tehdit oluşturduğu belirtilmektedir.

PixPirate: Brezilya'ya Yönelik Yeni Android Banking Trojan

Brezilya finans kurumlarını hedef alarak PIX ödeme platformunu kötüye kullanan PixPirate adlı Android bankacılık truva atı yazılımı ortaya çıktı. Araştırmacılar, PixPirate'in Automatic Transfer System (ATS) özelliği ile kötü niyetli para transferini otomatikleştirme yeteneğine sahip olduğunu belirtiyor. PixPirate, Google Play Protect'i devre dışı bırakma, SMS'leri ele geçirme ve itirazsız reklamları kullanma gibi özellikleriyle dikkat çekiyor.

2023 Yılında Finans Sektörünü Hedef Alan APT Grupları

Ekibimiz tarafından yapılan incelemeler sonucunda, bazı APT gruplarının bu yılın başından itibaren Finans Sektörünü hedef aldığı tespit edilmiştir. Raporun bilgilendirme amacı doğrultusunda söz konusu APT gruplarına ait bilgilere aşağıda yer verilmiştir.

BlackTech

BlackTech, gizli operasyonları ve karmaşık saldırılarıyla tanınan bir Gelişmiş Kalıcı Tehdit (APT) grubudur.

Genellikle Asya-Pasifik bölgesinde faaliyet gösteren bu grup, özellikle Tayvan, Japonya ve Güney Kore gibi ülkelerdeki hükümetler, teknoloji şirketleri ve savunma sanayi gibi stratejik sektörleri hedef almaktadır.

Başlıca Özellikleri:

1. Hassas Hedef Odaklı: BlackTech'in saldırıları genellikle hükümet kurumları, savunma yüklenicileri ve yüksek teknoloji şirketleri gibi hassas sektörlere yöneliktir.
2. Özelleştirilmiş Zararlı Yazılımlar: Grup, kendi ihtiyaçlarına uygun özel zararlı yazılımlar geliştirmekte ve kullanmaktadır. Bu yazılımlar genellikle gelişmiş kötü amaçlı yazılımlar (malware) ve casus araçları içerir.
3. Suikast Kampanyaları: BlackTech, belirli kişilere veya kuruluşlara yönelik suikast kampanyalarını içeren hedeflenmiş saldırılarda uzmandır. Bu, genellikle sosyal mühendislik taktikleri ve gelişmiş casus yazılım kullanımını içerir.

Bilinen Saldırıları:

BlackTech'in WaterBear olarak adlandırılan bir saldırı kampanyası, belgeleri hedef bilgisayar sistemine bulaştırmak için suistimal edilen güvenlik açıklarını içeren karmaşık bir saldırı vektörünü içermektedir. DinoDrop adlı zararlı yazılımı kullanarak hedef sistemlere sızma yeteneklerini genişletir ve bilgi çalmak için bu aracı kullanır.

Amaç ve Hedefleri:

BlackTech'in ana amacı, stratejik öneme sahip hükümet ve endüstri sektörlerinden hassas bilgileri ele geçirmektir. Bu bilgiler genellikle stratejik planlar, savunma teknolojileri veya ekonomik veriler gibi kritik konularda olabilir. Grup, bu bilgileri kullanarak siyasi veya ekonomik avantajlar elde etmeyi amaçlar.

APT34

APT34, yani bilinen adıyla OILRIG, İran merkezli bir gelişmiş kalıcı tehdit (APT) grubudur.

Bu grup, İran'ın stratejik çıkarlarını desteklemek amacıyla siber casusluk ve siber saldırıları gerçekleştiren bir istihbarat birimi olarak kabul edilir.

APT34, çeşitli sektörlere yönelik siber saldırılar yapma yeteneğine sahiptir ve İran hükümeti tarafından desteklenmektedir.

Başlıca Özellikleri:

1. İran Hükümeti Bağlantısı: APT34, İran hükümeti ile yakından ilişkilendirilen bir siber casusluk grubudur. Grup, İran'ın stratejik çıkarlarını desteklemek amacıyla faaliyet gösterir.
2. Hedef Çeşitliliği: APT34, enerji, savunma, telekomünikasyon, finans ve hükümet gibi bir dizi sektöre yönelik saldırılar gerçekleştirir. Hedefler arasında genellikle yabancı hükümetler, şirketler ve düşman ülkelerin stratejik pozisyonları bulunur.
3. Sosyal Mühendislik Yetenekleri: Grup, hedeflerine sızmak için sosyal mühendislik taktiklerini kullanır. Bu, kurbanların güvenini kazanmak ve kötü amaçlı yazılımları yaymak için manipülasyon ve dolandırıcılık içerebilir.
4. Zararlı Yazılımlar: APT34, kötü amaçlı yazılım kullanımında uzmandır. Özellikle, çeşitli türde zararlı yazılımları hedeflerine sızmak için kullanır.

Bilinen Saldırılar:

APT34'nin en dikkat çekici saldırılarından biri, dünya çapında çok sayıda hükümet ve özel sektör kuruluşuna karşı gerçekleştirilen Phosphorus kampanyasıdır. Bu kampanya, hedeflere yönelik siber casusluk ve bilgi toplama operasyonlarını içerir.

Amaç ve Hedef:

APT34, İran hükümetinin stratejik çıkarlarını korumak ve ileriye taşımak amacıyla faaliyet gösterir. Hedefleri arasında yabancı hükümetler, enerji sektörü, askeri savunma ve stratejik bilgi bulunur.

IoC için tıklayın.

Lazarus

Lazarus, dünya çapında operasyonlar yürüten ve kökeni Kuzey Kore'ye dayandırılan bir gelişmiş kalıcı tehdit (APT) grubudur.

Bu siber saldırı grubu, çeşitli siber casusluk, finansal suçlar ve siber sabotaj operasyonları ile tanınır.

Lazarus, oldukça karmaşık ve hedefe yönelik siber saldırılar gerçekleştiren bir grup olarak bilinir ve dünya genelindeki hükümetler, finansal kuruluşlar ve büyük şirketler arasında yüksek profilli hedeflere odaklanır.

Başlıca Özellikleri:

1. **Kuzey Kore Bağlantısı:** Lazarus APT grubunun kökeni, Kuzey Kore olarak belirtilir ve bu nedenle devlet destekli bir grup olduğuna inanılır.
2. **Siber Casusluk ve Finansal Suçlar:** Grup, siber casusluk operasyonlarının yanı sıra finansal suçlar konusundaki yetenekleriyle de dikkat çeker. Daha önce banka soygunları, kripto para hırsızlıkları ve fidye yazılım saldırıları gerçekleştirmişlerdir.
3. **Yüksek Profilli Hedefler:** Lazarus, hükümetler, finans kuruluşları ve büyük şirketler gibi yüksek profilli hedefleri hedef alır. Özellikle finans sektörüne yönelik saldırılar, grup için finansal kazanç elde etmenin bir yolu olarak öne çıkar.
4. **Karmaşık Kötü Amaçlı Yazılımlar:** Grup, karmaşık kötü amaçlı yazılımlar ve siber casusluk araçları kullanır. Bu, saldırılarının tespit edilmesini zorlaştırır.

Bilinen Saldırılar:

Lazarus APT grubunun en ünlü saldırılarından biri, 2014'teki Sony Pictures saldırısıdır. Grup ayrıca finansal kuruluşları hedefleyen çok sayıda büyük saldırı gerçekleştirmiştir. Bunlar arasında 2016'daki Bangladesh Merkez Bankası hacklemesi ve 2017'deki WannaCry fidye yazılım saldırısı bulunur.

Amaç ve Hedef:
Lazarus APT grubunun ana amacı, Kuzey Kore hükümetinin çeşitli amaçları doğrultusunda faaliyet göstermektir. Bu amaçlar arasında finansal kazanç, casusluk ve ulusal çıkarları koruma yer alır. Grup, uluslararası finansal sistemi hedef alarak gelir elde etmeye çalışırken, aynı zamanda casusluk operasyonları yürüterek bilgi toplamaya odaklanır.

IoC için tıklayın.


ECHO
CYBER THREAT INTELLIGENCE