ECHO

CYBER THREAT INTELLIGENCE

İSTİHBARAT RAPORU 2023

ENERJİ SEKTÖRÜNE YÖNELİK SALDIRI RAPORU

İçindekiler

Yönetici Özeti

Bu yönetici özeti, enerji sektörünü hedef alan siber saldırıların önemini ve etkilerini ele almaktadır. Son yıllarda enerji sektöründe yaşanan siber saldırılar, işletmeler için büyük bir tehdit haline gelmiştir. Bu saldırılar, enerji şirketlerinin altyapıları, enerji üretim sistemleri, dağıtım ağları ve hatta enerji ticaret platformları gibi kritik alanları hedeflemektedir.

Enerji sektörü, siber saldırılara karşı hassas bir konumdadır. Sektördeki kritik altyapıların ve verilerin korunması, enerji üretiminin sürekliliği ve enerji güvenliği açısından büyük bir önem taşımaktadır. Siber saldırılar, veri hırsızlığı, operasyonel kesintiler, enerji arzının tehlikeye atılması gibi ciddi sonuçlara yol açabilir.

Son yıllarda enerji sektöründe yaşanan siber saldırıların sayısında belirgin bir artış gözlemlenmektedir. Bu artış, enerji şirketlerinin siber tehditlere karşı daha iyi hazırlıklı olmaları gerektiğini göstermektedir. Eurocontrol raporlarına göre, siber saldırılar son dört yılda yıllık bazda en az %530 daha fazla gerçekleşmektedir. Bu, enerji sektörünün güvenliğini artırmak için kapsamlı güvenlik önlemlerinin alınması gerektiğini göstermektedir.

Siber saldırganlar, sürekli olarak gelişen teknikler ve taktikler kullanarak güvenlik önlemlerini aşmayı hedeflemektedir. Saldırıların arkasında farklı motivasyonlar bulunmaktadır, bunlar arasında mali kazanç sağlama, enerji arzını kesme, casusluk faaliyetleri veya siber saldırı yeteneklerini sergileme gibi amaçlar yer almaktadır.

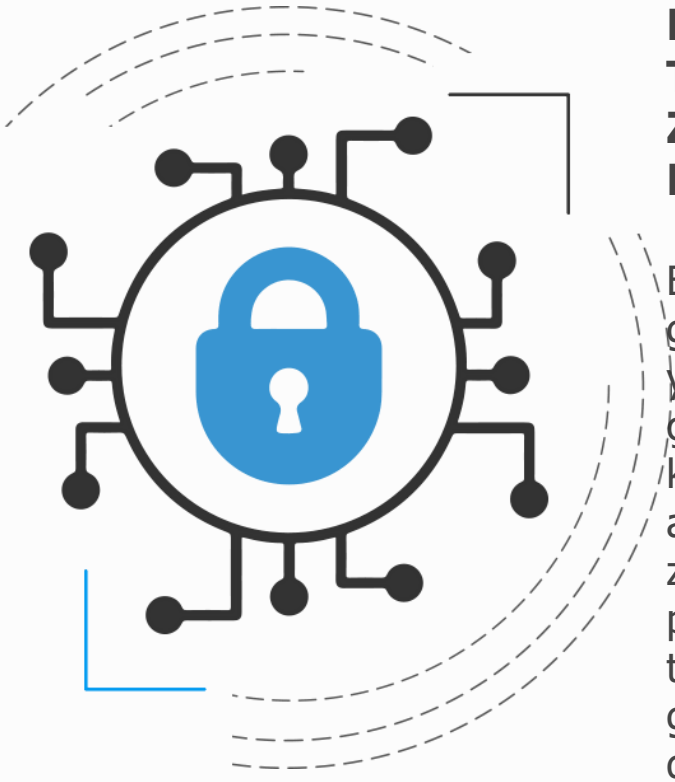
Enerji sektörü, siber güvenlik konusunda sürekli olarak güncel kalması gereken bir alandır. Gelecekteki tehditlerin önlenmesi için sektör, güvenlik politikalarını sürekli gözden geçirmeli, personel eğitimine yatırım yapmalı ve teknolojik gelişmeleri yakından takip etmelidir.

Bu rapor, enerji sektöründeki yöneticilerin, siber saldırı tehditlerine karşı daha fazla bilinçlenmelerine ve gerekli önlemleri alarak şirketlerini ve sektörü korumalarına yardımcı olmayı amaçlamaktadır. Siber güvenlik, enerji sektörünün devamlılığını ve güvenliğini sağlamak için bir öncelik haline gelmelidir.

2023 Yılında Yaşanan Saldırı ve Olaylar

Ukrayna'da Enerji Sektörüne Yönelik Siber Saldırı Girişimi

Ukrayna'nın kritik enerji altyapısı, APT28 adlı Rus tehdit aktörü tarafından düzenlenen siber saldırı girişimine karşı Bilgisayar Acil Durum Müdahale Ekibi (CERT-UA) tarafından etkili bir şekilde savunuldu. Saldırının, kötü amaçlı bir ZIP arşivi içeren bir phishing e-postası ile başladığı ve uzaktan komut yürütmeyi içerdiği belirtildi.



LinkedIn Üzerinden Enerji ve Telekom Sektörlerini Hedef Alan Zararlı Yazılım Ailesi Tespit Edildi – RedEnergy –

Brezilya ve Filipinler'deki enerji, petrol, gaz, telekom ve makine sektörlerine yönelik saldırılarda kullanılan veri çalmayı şifreleme ile birleştirerek kurbanlara maksimum zarar vermeyi amaçlayan RedEnergy adında yeni bir zararlı yazılım tespit edildi. LinkedIn profilleri üzerinden iletişime geçen tehdit aktörlerinin, sahte web tarayıcı güncellemeleri ile oltalama kampası düzenlediği tespit edildi.

YoroTrooper: Hükümet ve Enerji Sektörlerini Hedef Alan Siber Casusluk Kampanyası Ortaya Çıktı

Bilinmeyen bir siber tehdit aktörü olan YoroTrooper, Haziran 2022'den bu yana Avrupa'da hükümetleri, enerji sektörünü ve uluslararası organizasyonları hedef alan karmaşık bir siber casusluk kampanyasının parçası olarak faaliyet gösteriyor. Başarılı saldırılardan çalınan veriler arasında kimlik bilgileri, tarayıcı geçmişi ve çerezler, sistem bilgileri ve ekran görüntüleri yer alıyor.

Ukrayna Enerji Sektörünü Hedef Alan NikoWiper Kötü Amaçlı Yazılımı Ortaya Çıktı

Rusya ile ilişkilendirilen Sandworm adlı siber tehdit aktörünün, Ukrayna'daki bir enerji sektörü şirketini hedef alan bir saldırının bir parçası olarak NikoWiper adlı bir wiper (veriyi silen) kötü amaçlı yazılım türünü kullandığı tespit edildi. Bu saldırıların, Rus silahlı kuvvetlerinin Ukrayna enerji altyapısına yönelik füze saldırılarıyla çakıştığı için benzer hedeflere işaret ettiği gözlemlenmektedir.

Iran Hükümeti Destekli Hacker Grubu, ABD Enerji ve Ulaşım Sistemlerini Hedef Alıyor

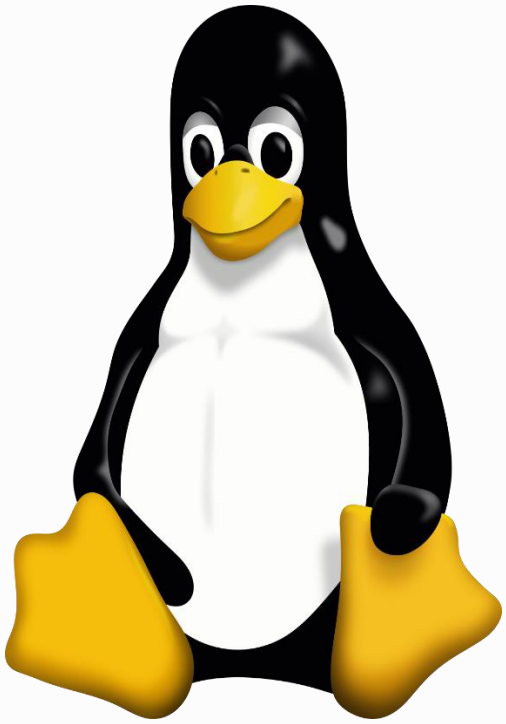
Mint Sandstorm olarak bilinen İran hükümeti destekli tehdit aktörü, 2021 yılının sonlarından 2022 yılının ortalarına kadar ABD'nin kritik altyapısını hedef alan saldırılara bağlanmıştır. Microsoft Tehdit İstihbarat ekibinin yaptığı bir analize göre, bu Mint Sandstorm alt grubu teknik ve operasyonel olarak olgun, özel araçlar geliştirebilen ve hızla N-day (sıfır gün) güvenlik açıklarını kullanabilen bir yetkinliğe sahiptir ve operasyonel odaklamasında İran'ın ulusal önceliklerine uygun bir çeviklik sergilemiştir.

Sanayi Kontrol Sistemlerindeki Güvenlik Açıkları Yükseliyor: 2023 Yılında Üçte Birinden Fazlası Düzeltilememiş

2023 yılının ilk yarısında bildirilen endüstriyel kontrol sistemlerini (ICS) etkileyen güvenlik açıklarının yaklaşık %34'ü düzeltme veya yama bulunmuyor. Bu, geçen yıl %13'ten önemli bir artışı temsil ediyor. 2023 yılının ilk yarısında ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) aracılığıyla toplam 670 ICS ürün zafiyeti bildirildi.

Space Pirates ,Rusya ve Sırbistan'da Siber Kampanya Başlattı

Uzay Korsanları (Space Pirates) olarak bilinen tehdit aktörü, son bir yıl içinde Rusya ve Sırbistan'da en az 16 kuruluşa karşı gerçekleştirilen saldırılarla ilişkilendirilmiş ve yeni taktikler kullanarak ve silah stoklarına yeni siber silahlar ekleyerek dikkat çekiyor. Hedefler, Rusya ve Sırbistan'da devlet kurumları, eğitim kurumları, özel güvenlik şirketleri, havacılık üreticileri, tarım üreticileri, savunma, enerji ve sağlık firmalarını içeriyor.



ChamelDoH: Gizli CnC için DNS-over-HTTPS Tünellemesi Kullanan Yeni Linux Backdoor Ortaya Çıktı

ChamelGang olarak bilinen tehdit aktörü, yeteneklerini genişletmek için daha önce belgelenmemiş bir implant kullanarak Linux sistemlere arka kapı bıraktığı gözlemlendi. ChamelDoH olarak adlandırılan kötü amaçlı yazılım, DNS-over-HTTPS (DoH) tünellemesi yoluyla iletişim kurmak için C++ dilinde geliştirilmiş bir araçtır. 2021 yılının Eylül ayında ortaya çıkan ve saldırılarını Rusya, ABD, Hindistan, Nepal, Tayvan ve Japonya'daki yakıt, enerji ve havacılık üretimi endüstrilerine yönelik olarak detaylandırıldı.

APT28, Ukrayna Hükümet Kurumlarına Sahte "Windows Güncellemesi" E-postaları ile Hedef Aldı

Ukrayna Bilgisayar Acil Durum Tepki Ekibi (CERT-UA), ülkedeki çeşitli hükümet kurumlarını hedefleyen Rus devlet destekli hackerların gerçekleştirdiği siber saldırıları uyararak dikkat çekti. Bu phishing kampanyası APT28 grubu tarafından gerçekleştirildi. Saldırı e-postalarının konu başlığının "Windows Güncellemesi" olduğu ve güvenlik güncellemeleri bahanesiyle çalıştırılması gereken bir PowerShell komutunu içerdiği iddia edilen Ukraynaca talimatlar içerdiği tespit edildi.

Lazarus X_TRADER Saldırısı, 3CX Sızıntısının Ötesinde Elektrik ve Enerji Sektörüne İlişkin Elektro Kritik Altyapıları Etkilediği Ortaya Çıktı

Kuzey Kore'nin ünlü hacker grubu olan Lazarus, 3CX'i hedef alan bir dizi arz zinciri saldırısının arkasındaydı ve ayrıca, Trojan haline dön X_TRADER uygulamasını kullanan finansal işlemlerle uğraşan iki kritik altyapı kuruluşu ve iki işletmeyi etkiledi.

Iran Hükümeti Destekli Hackerlar, ABD Enerji ve Ulaşım Sistemlerini Hedef Aldığı Ortaya Çıktı

Mint Sandstorm olarak bilinen İran hükümeti destekli bir aktör, 2021 yılının sonlarından 2022 yılının ortalarına kadar ABD'nin kritik altyapısına yönelik saldırılarla ilişkilendirildi. Hedeflenen kurumlar arasında deniz limanları, enerji şirketleri, ulaşım sistemleri ve büyük bir ABD enerji ve gaz şirketi bulunmaktadır. Bu faaliyetlerin, 2020'nin Mayıs ayından 2021'in sonlarına kadar geçen süre zarfında denizcilik, demiryolu ve benzin istasyonu ödeme sistemlerine yönelik saldırılara misilleme olarak gerçekleştirildiği tahmin edilmektedir.

CISA, Hitachi Energy, mySCADA, ICL ve Nexx Ürünlerini Etkileyen Kritik ICS Hataları Hakkında Uyardı

Amerika Birleşik Devletleri Siber Güvenlik ve Altyapı Güvenliği Ajansı tarafından (CISA), Hitachi Energy, mySCADA Technologies, Industrial Control Links ve Nexx ürünlerini etkileyen kritik hataları içeren sekiz Endüstriyel Kontrol Sistemleri (ICS) bildirisi yayınlandı.

Microsoft Outlook Zafiyeti Devlet Kurumlarına Yapılan Saldırılarda Kullanıldı

Rusya Devleti tarafından desteklendiği düşünülen tehdit aktörlerinin, uzak bilgisayardaki NTLM hash bilgisinin ele geçirilebilmesine olanak sağlayan "CVE-2023-23397" outlook zafiyetini kullanarak enerji, askeri ve ulaşım sektörlerine ait birçok devlet kurumu hedef alındı.

ESXiArgs Ransomware Saldırısı Avrupa'da Birçok Kurumu Hedef Aldı

ESXiArgs fidye yazılımı, eski ESXi sürümlerini kullanan veya güvenlik güncellemelerini yapmayan bilgisayarları hedef alarak toplam 14 enerji kurumunda zarara yol açtı.

Lazarus, Güvenlik Güncellemesi Yapılmayan Zimbra Cihazlarını Hedef Aldı

Kuzey Kore'nin Lazarus grubuna bağlı siber saldırganlar, güvenlik güncellemesi yapılmayan Zimbra cihazlarını hedef alarak yeni bir siber casusluk kampanyası başlattı. Saldırılar, enerji, araştırma, savunma ve sağlık sektörlerinin tedarik zincirlerine sızma girişimini içerecek şekilde düzenlendiği tespit edildi. Saldırganların, bu güncellemeleri yapmayan cihazları hedef alarak yaklaşık 100 GB veri çalmış olabilecekleri tahmin edilmektedir.

Büyük Çaplı QR Kodlu Phishing Saldırısı Enerji Şirketlerini Hedef Alıyor

Mayıs 2023'ten itibaren başlayan büyük çaplı bir phishing kampanyası, QR kodlarını kullanarak ABD'deki önde gelen enerji şirketlerini hedef alıyor. Saldırının, QR kodlarıyla kullanıcıların Microsoft kimlik bilgilerini çalmayı amaçladığı ve enerji sektörünün bu kampanyada öne çıktığı tespit edildi. QR kodlarının kullanılması, anti-phishing çözümlerini atlayabilme avantajı sunabildiği için kampanya, Mayıs ayından bu yana %2,400'ün üzerinde büyüdü. QR kodlarının bu şekilde kötüye kullanılması, siber tehdit aktörlerinin yeni taktikler denediğini göstermektedir.

Avustralyalı Yazılım Sağlayıcı ENERGY ONE Siber Saldırıya Maruz Kaldı

Avustralyalı yazılım sağlayıcısı Energy One kurumunun, belirli kurumsal sistemlerini etkileyen bir siber saldırıya maruz kaldığı açıklandı. Şirket, olayın ardından bir soruşturma başlattı ve Avustralya Siber Güvenlik Merkezi ile ilgili İngiliz yetkililere bilgi verdi. Saldırıya yanıt olarak, şirket kurumsal ve müşteri odaklı sistemleri arasındaki bazı bağlantıları devre dışı bıraktı. Saldırının ilk vektörünün veya saldırganların kimliğinin henüz belirlenmediği ve saldırı nedeniyle tehdit aktörlerinin müşteri verilerine erişip erişmediği belirsizliğini koruyor.

Enerji Sektöründe Kritik Açık Sömürülmeye Devam Ediliyor: CVE-2022-29303

Güneş enerjisi izleme ürünü Contec SolarView üzerinde bulunan CVE-2022-29303 güvenlik açığı, enerji sektöründeki organizasyonları hedef alan potansiyel saldırılara açık bir kapı bırakıyor. Yapılan gözlemlere göre, Mirai botnet'in yeni bir varyantı da bu açığı hedef alıyor. Shodan kullanarak internet üzerinde 615'ten fazla SolarView kurulumu bulundu, bunların 425'i savunmasız sürümler çalıştırıyor. Bu nedenle enerji sektöründe etkilenen organizasyon sayısı gün geçtikçe artmaya devam ediyor.

Schneider Electric ve Siemens Energy, MOVEit Saldırısının Kurbanları Arasına Dahil Oldu

Clop fidye yazılımı grubu, Schneider Electric ve Siemens Energy gibi endüstri devlerini içeren beş yeni MOVEit (CVE-2023-34362) saldırısı kurbanını dark web leak sitesine ekledi. Sızdırılan kurbanların listesi:

- werum.com
- Schneider Electric (http://se.com)
- Siemens Energy (http://siemens-energy.com)
- UCLA (http://ucla.edu)
- Abbie (http://abbvie.com)

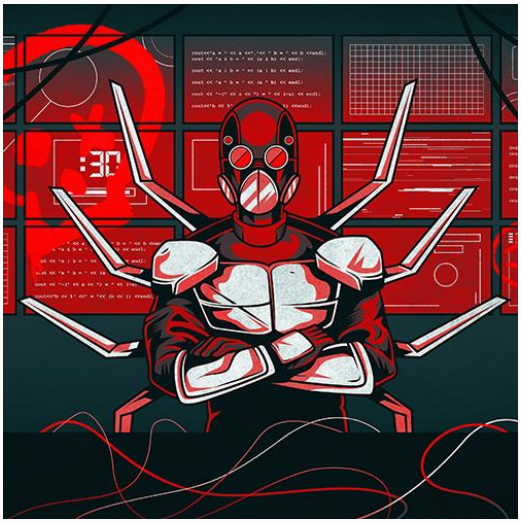
Enerji Şirketi Suncor, Kanada'daki Petro-Canada Gaz İstasyonlarında Siber Saldırıya Maruz Kaldı

Suncor Energy'nin yaşadığı siber saldırı, Kanada'daki Petro-Canada gaz istasyonlarının ödeme işlemlerini etkiledi Etkilenen gaz istasyonlarındaki müşteriler, kredi kartı ile ödeme yapamadılar. Suncor, olayı üçüncü taraf uzmanların yardımıyla araştırmak için hemen önlem aldı.

2023 Yılında Enerji Sektörünü Hedef Alan APT Grupları

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

Bitwise SPIDER



Bitwise Spider APT grubu, devlet kurumları, büyük şirketler ve kritik altyapıları olan ülkelerin özellikle savunma, enerji, iletişim ve teknoloji sektörlerini hedef bir APT (Advanced Persistent Threat) grubudur.

Saldırılarda kullanılan zafiyetler ve saldırı teknikleri:

- Active Directory
- Shadow copy
- UAC Bypass
- ESXI

Bitwise Spider, gelişmiş saldırı vektörleri kullanarak hedef ağlara sızar. Bunlar arasında phishing e-postaları, güvenlik açıklarını kullanma, zararlı yazılım enjeksiyonu, sosyal mühendislik ve gelişmiş süreç kaçırma teknikleri bulunur.

Bitwise Spider APT grubu, özelleştirilmiş zararlı yazılımlar kullanır. Bu zararlı yazılımlar, casusluk faaliyetleri için tasarlanmıştır ve genellikle gelişmiş zararlı yazılım analiz yöntemleriyle tespit edilmeleri zordur. Bitwise Spider grubunun geliştirdiği bilinen iki zararlı yazılım ailesi bulunmaktadır: LockBit Fidye Yazılımı ve StealBit InfoStealer Zararlı Yazılımı.

Bitwise Spider APT grubunun kurumlara etkileri:

1. Veri Hırsızlığı
2. Repütasyon Zararı
3. Finansal Kayıplar
4. Rekabet Avantajının Azalması
5. Saldırı Maliyetleri

IoC için tıklayın.

Berserk Bear

Berserk Bear, ayrıca Energetic Bear veya Dragonfly olarak da bilinen, siber casusluk faaliyetleri yürüten bir Gelişmiş Sürekli Tehdit (APT) grubudur.

Berserk Bear'ın operasyonlarının odak noktası enerji sektöründeki kuruluşlardır, özellikle enerji şebekeleri, petrol ve gaz şirketleri ve diğer kritik altyapı sağlayıcıları.

Bu sistemlere izinsiz erişim sağlayarak grup, istihbarat toplamayı, operasyonları bozmak ve önemli kaynaklar üzerinde kontrol sağlamayı amaçlamaktadır.

Berserk Bear, hedeflerine ulaşmak için çeşitli gelişmiş teknik ve taktikler kullanmaktadır. Bunlar arasında, genellikle zararlı ekleri veya bağlantıları içeren özenle hazırlanmış e-postaların belirli kişilere gönderildiği **spear-phishing** kampanyaları bulunmaktadır. Grup **watering hole** saldırılarına başvurur, hedefledikleri kuruluşlar tarafından sıkça ziyaret edilen meşru web sitelerini tehlikeye atarak zararlı yazılım veya zafiyetleri kullanır.

Berserk Bear, özellikle endüstriyel kontrol sistemlerinde (ICS) kullanılan yazılım ve sistemlerdeki zafiyetleri sömürme yeteneğiyle dikkat çekmektedir. Kritik altyapıları ihlal etme kabiliyeti, hedeflenen kuruluşlara ve etkilenen sektörlerin genel istikrarına önemli riskler taşımaktadır.

Grup, 2015 ve 2016 yıllarında Ukrayna'daki enerji şebekelerini etkileme rolü nedeniyle uluslararası dikkat çekmiş ve yetenekleri ve potansiyel etkisi vurgulanmıştır. Enerji sektörü birincil odak noktası olsa da, Berserk Bear'ın Amerika Birleşik Devletleri ve Avrupa dahil diğer sektörler ve ülkelerdeki kuruluşlara yönelik saldırıları da bilinmektedir.

Faaliyetlerinin gizlilik gerektirmesi nedeniyle, Berserk Bear hakkında detaylı bilgilere genellikle sınırlı ve yakından korunan bir şekilde erişilmektedir. Güvenlik araştırmacıları ve hükümet kurumları, bu sürekli ve son derece yetenekli APT grubunun oluşturduğu tehditleri anlamak ve karşılamak için faaliyetlerini izlemeye devam etmektedir.

APT28

APT28, "Fancy Bear" veya "Sofacy Group" olarak da bilinir, Rusya ile ilişkilendirilen gelişmiş bir siber casusluk ve siber saldırı grubudur.

Bu grubun faaliyetleri genellikle Rus hükümeti veya Rus istihbarat ajanslarıyla bağlantılı olduğu iddia edilmektedir.

APT28, 2007'den beri aktif olan bir grup olarak bilinir ve çeşitli hedeflere yönelik karmaşık siber saldırılar gerçekleştirmiştir.

APT28'in tam olarak hangi Rus ajansıyla ilişkilendirildiği belirsizdir, ancak bu grup Rusya'nın siber casusluk kapasitesini kullanan birbirinden ayrı birimlerle bağlantılı olabilir. Grup, 2007'den itibaren çeşitli uluslararası olaylara karışmıştır.

Faaliyet Alanları:

APT28, özellikle NATO ülkeleri, Avrupa hükümetleri, Ukrayna ve Gürcistan gibi Rusya'nın stratejik olarak ilgilendiği bölgelere yönelik siber saldırılarla tanınır. Ayrıca ABD'deki seçimlere müdahale etme girişimleri de dahil olmak üzere uluslararası politika ve seçimlere müdahale etme amacıyla faaliyet göstermiştir.

Saldırı Teknikleri:

APT28, gelişmiş ve karmaşık siber saldırı teknikleri kullanır. Spear phishing (hedefe yönelik sahte e-postalar), zararlı yazılım bulaştırma ve sızma yöntemleri gibi yöntemleri ustaca uygularlar. Ayrıca hedef kuruluşların ağlarını uzun süre boyunca izleme yeteneğine sahiptirler, bu da istihbarat toplamak ve hedeflerini daha etkili bir şekilde anlamalarına olanak tanır.

Bilinen Saldırılar:

APT28, dünya çapında bir dizi yüksek profilli saldırıya karıştı. Özellikle, 2016 Amerika Birleşik Devletleri başkanlık seçimlerine müdahale etme girişimleri büyük dikkat çekti. Ayrıca Ukrayna'ya yönelik saldırılar, NATO kurumlarına yönelik siber saldırılar ve Avrupa'daki enerji sektörüne yönelik casusluk faaliyetleri gibi birçok olay APT28 ile ilişkilendirilmiştir.

Amaç ve Hedef:

APT28'nin nedenleri ve hedefleri tartışmalıdır, ancak genellikle Rusya'nın ulusal çıkarlarına hizmet ettiği veya Rus hükümetinin politik amaçlarını desteklediği düşünülmektedir. Bu grup, stratejik, askeri ve politik bilgi toplamak amacıyla faaliyet gösterir ve bu bilgileri çeşitli amaçlar için kullanabilir.

IoC için tıklayın.

APT31

APT31 veya bilinen diğer adıyla Zirconium, gelişmiş kalıcı bir tehdit (APT) grubudur.

Bu grup, çoğunlukla Çin merkezli olduğuna inanılan sofistike bir siber casusluk grubudur.

APT31, siber casusluk, bilgi toplama ve diğer siber saldırıları gerçekleştirme amacıyla faaliyet gösterir.

Başlıca Özellikleri:

1. Çin Hükümeti ile İlişkilendirilme: APT31, Çin hükümeti ile ilişkilendirilen bir siber casusluk grubu olarak bilinir. Ancak, Çin hükümeti bu tür ilişkileri sıklıkla reddeder.
2. Sofistike Saldırılar: APT31, hedeflerine yönelik sofistike ve karmaşık saldırılar gerçekleştirir. Bu saldırılar, gelişmiş kötü amaçlı yazılımlar, sıfır gün saldırıları ve karmaşık ağ penetrasyon tekniklerini içerebilir.
3. Bilgi Toplama: Grup, özellikle teknoloji, enerji, havacılık ve askeri sektörlerde faaliyet gösteren şirketlerin bilgilerini toplamak için faaliyet gösterir. Bu bilgiler, Çin hükümetinin stratejik çıkarlarını desteklemek amacıyla kullanılabilir.
4. Uzun Süreli Faaliyet: APT31, uzun vadeli hedeflere yönelik çalışır ve kuruluşların ağlarını uzun süre boyunca izleme yeteneğine sahiptir. Bu, hedeflerini daha iyi anlamalarına olanak tanır.

Bilinen Saldırılar:

APT31'nin dünya çapında bir dizi yüksek profilli saldırıya karıştığına inanılıyor. Özellikle, fikri mülkiyet hırsızlığı, teknoloji şirketlerine yönelik siber casusluk faaliyetleri ve yabancı hükümetlere karşı istihbarat operasyonları gibi olaylarla ilişkilendirilmiştir.

Amaç ve Hedef:

APT31'nin ana nedenleri ve hedefleri, Çin'in ulusal çıkarlarına hizmet ettiği veya Çin hükümetinin politik amaçlarını desteklediği düşünülmektedir. Grup, stratejik bilgi ve teknolojiyi çalmak amacıyla faaliyet gösterir.

IoC için tıklayın.

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.

Mint Sandstorm

Mint Sandstorm, gelişmiş kalıcı tehdit (APT) gruplarından biridir ve siber casusluk faaliyetleri yürüten bir siber saldırı grubudur.

Bu grup, özellikle Asya-Pasifik bölgesindeki hükümetler, askeri kurumlar ve büyük işletmeler gibi yüksek profilli hedefleri hedef alır.

Mint Sandstorm, karmaşık ve hedefe yönelik siber saldırılar gerçekleştiren disiplinli bir aktör olarak bilinir.

Başlıca Özellikleri:

1. Asya-Pasifik Odaklı: Mint Sandstorm, çoğunlukla Asya-Pasifik bölgesindeki hedeflere odaklanır. Bu bölge, grup için stratejik öneme sahip hükümetler, savunma kurumları ve ekonomik güçler içerir.
2. Hükümet ve Savunma Hedefleri: Grup, askeri ve hükümet hedeflerini siber casusluk amaçları için hedef alır. Bu, hükümet politikaları, askeri stratejiler ve ulusal güvenlikle ilgili bilgileri hedefler.
3. Karmaşık Saldırılar: Mint Sandstorm, hedefe yönelik ve özel olarak hazırlanan karmaşık siber saldırılar gerçekleştirir. Bu, gelişmiş kötü amaçlı yazılımların ve siber casusluk araçlarının kullanılmasını içerebilir.
4. Gizli Kalma Yeteneği: Grup, faaliyetlerini genellikle uzun süre boyunca gizli tutar ve tespit edilmemek için çeşitli yöntemler kullanır.

Bilinen Saldırılar:

Mint Sandstorm APT grubunun belirli saldırılarına dair kamuya açıklanmış ayrıntılar sınırlıdır, çünkü grup genellikle tespit edilmemek için çok dikkatli davranır. Ancak, grup, özellikle Asya-Pasifik bölgesindeki askeri ve hükümet hedeflerine karşı siber casusluk operasyonları gerçekleştirdiği bilinmektedir.

Amaç ve Hedef:

Mint Sandstorm'un ana amacı, Asya-Pasifik bölgesindeki siyasi ve stratejik gelişmeleri anlamak ve hükümetlerin, askeri kurumların ve büyük şirketlerin faaliyetleri hakkında değerli bilgilere erişmektir. Bu grup, bu bilgileri stratejik avantaj sağlamak için kullanır.

IoC için tıklayın.

ALPHA SPIDER

Alpha Spider APT grubu, siber saldırılarda bulunan ve gizli kalma yeteneğine sahip olan bir gelişmiş kalıcı tehdit (APT) grubudur.

Alpha Spider'ın saldırıları genellikle hükümet kurumları, askeri kuruluşlar, enerji şirketleri ve finansal kuruluşlar gibi stratejik sektörlere odaklanmaktadır.

Bu grup, gelişmiş hedefli saldırı tekniklerini kullanarak sistemlere sızma girişiminde bulunur ve hassas verileri ele geçirmeyi hedefler.

Alpha Spider, siber casusluk faaliyetleriyle bilinir ve genellikle bilgi toplama, entelektüel mülkiyet hırsızlığı ve stratejik bilgilerin sızdırılması gibi amaçları güder. Grup, siber saldırılarında gelişmiş malware araçları, exploitler ve sosyal mühendislik taktiklerini kullanır. Ayrıca, ileri düzey gizlilik ve gizlenme teknikleriyle tespit edilmeden kalma yeteneğine sahiptir.

Alpha Spider APT grubu, sürekli olarak saldırı taktiklerini ve tekniklerini geliştirir ve günceller. Bu nedenle, bilgi güvenliği uzmanları ve siber güvenlik ekipleri, bu grubun faaliyetlerini takip etmek ve savunma stratejilerini güncellemek için sürekli olarak analizlerini yapmaktadır.

Alpha Spider APT grubunun hedefleri ve saldırı yöntemleri hakkında daha fazla bilgi edinmek, savunma mekanizmalarının güçlendirilmesi ve saldırılara karşı daha etkili önlemler alınması açısından büyük önem taşır.

Cosmic Wolf

Cosmic Wolf APT grubu, siber saldırılarda bulunan gelişmiş bir kalıcı tehdit (APT) grubudur. Bu grup, çeşitli sektörlerdeki hedeflere karşı karmaşık ve sofistike saldırılar gerçekleştirerek bilgisayar korsanları tarafından yönetilir.

Cosmic Wolf'un hedefleri genellikle hükümet kurumları, askeri birimler, büyük şirketler ve kritik altyapılar gibi stratejik öneme sahip kuruluşlardır. Grup, finansal kazanç, casusluk veya politik amaçlarla saldırılar düzenleyebilir.

Cosmic Wolf, gelişmiş saldırı teknikleri kullanarak hedef sistemlere sızmayı hedefler. Bu grup, hedef kuruluşları belirlemek ve zayıflıkları tespit etmek için kapsamlı bir istihbarat toplama sürecinden geçer. Ardından, özel olarak tasarlanmış kötü amaçlı yazılımları, exploitleri ve sosyal mühendislik yöntemlerini kullanarak hedef sistemlere sızar.

Cosmic Wolf, saldırılarından önce ve sonra ağlarındaki izlerini gizlemek için gelişmiş gizlenme ve kötü amaçlı faaliyetlerini kamufle etme tekniklerini kullanır. Bu sayede tespit edilmelerini zorlaştırır ve izlerini takip etmek ve saldırılarını engellemek daha zor hale gelir.

Bu APT grubu, sürekli olarak saldırı tekniklerini geliştirir ve günceller. İleri düzey araştırma ve geliştirme çalışmalarıyla kendini yenileyerek savunma önlemlerini aşma girişiminde bulunur. Bu nedenle, güvenlik uzmanları ve siber güvenlik ekipleri, Cosmic Wolf'un faaliyetlerini izlemek, saldırılarını tespit etmek ve koruma stratejilerini güncellemek için sürekli olarak çalışmaktadır.

Cosmic Wolf APT grubunun faaliyetlerini anlamak ve koruma önlemlerini güçlendirmek, hedeflenen kuruluşlar için büyük önem taşır. Bu grupla ilgili güncel bilgilere erişmek ve saldırılarını engellemek için güvenlik topluluğunun iş birliği ve bilgi paylaşımı önemlidir.

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