CYBER WISE | ICSFUSION

Endüstriyel
Tesislere Yönelik

Saldırı Bilgilendirme Raporu

Haziran 2023

icsfusion.com

İÇİNDEKİLER

YÖNETİCİ ÖZETİ 2

1. HABERLER 3

1.1. Kanada Siber Güvenlik Merkezi, Petrol ve Gaz Sektörünü Dijital Tedarik Zincirinden Kaynaklanan Siber Tehditlere Karşı Uyardı 3

1.2. Araştırmacılar, Wago ve Schneider Electric OT Ürünlerindeki Yeni Ciddi Açıklıklarını Ortaya Koydu 4

1.3. Moody's Siber Saldırılardan Etkilenen Altyapıların Kredi Notunu Düşürüyor 5

1.4. Suncor Energy Siber Saldırısı Petro-Kanada Benzin İstasyonlarını Etkiliyor 6

1.5. Araştırma: Yatırımın, Beceri Eksikliğinin ve Zayıf İşbirliğinin Enerji Sektöründe Büyük Zorluklar Yaratmaya Devam Ettiğini Gösteriyor 7

1.6. Siemens Energy, MOVEit Saldırısından Sonra Veri İhlalini Doğruladı 8

1.7. Endüstriyel Siber Güvenlik Şirketi, CosmicEnergy Kötü Amaçlı Yazılımının Endüstriyel Tesisler İçin 'Acil Tehdit' Olmadığını Belirtti 9

1.8. Schneider Güç Ölçer Güvenlik Açığı Elektrik Kesintilerine Kapı Açıyor 10

1.9. CISA, Yeni Güvenlik Açıkları Buluyor; Delta Electronics, Mitsubishi Electric, Hitachi Energy için Önceki Bildirimleri Güncelliyor 11

1.10. Çinli Tehdit Aktörü, Tayvan'ın Kritik Altyapısına Saldırmak için Değiştirilmiş Kobalt Saldırısı Varyantını Kullandı 12

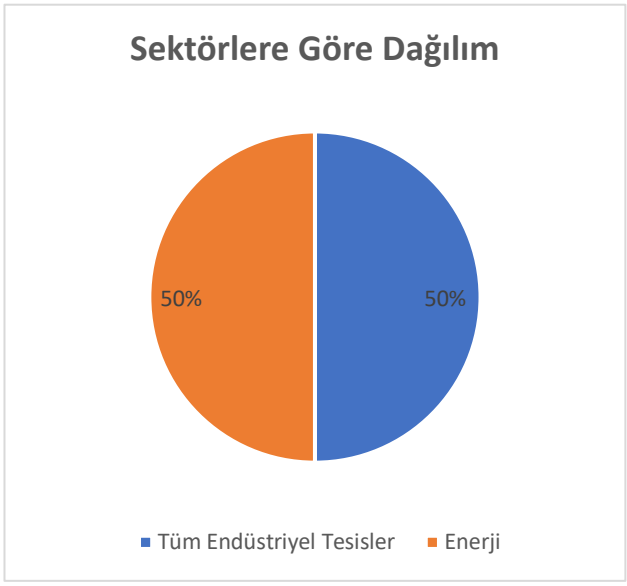
2. FİDYE YAZILIMI SALDIRILARI 13

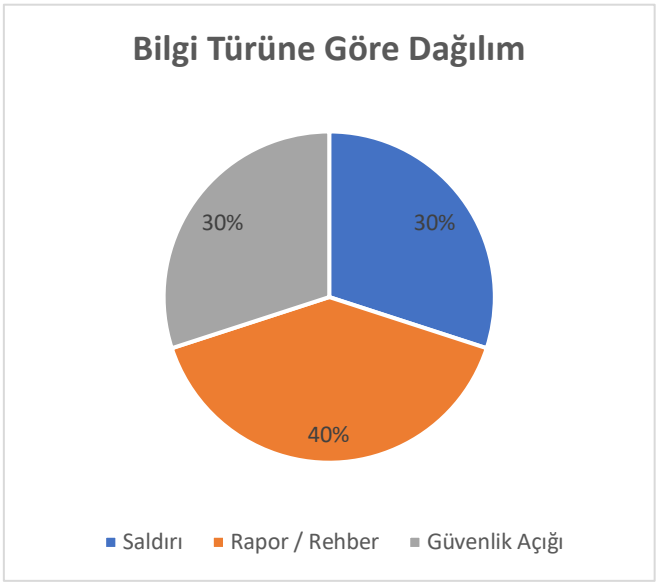
YÖNETİCİ ÖZETİ

Bu rapor, internet üzerinde açık kaynaklar kullanılarak oluşturulmuştur. Bunun yanı sıra çeşitli açık kaynak kodlu araçlar, dark web ve deep web kaynaklarından toplanan veriler Cyberwise ve ICSFusion endüstriyel siber tehdit istihbarat analistleri tarafından analiz edilmiş, endüstriyel tesislere yönelik yapılan saldırılar ve sektöre dair önemli görülen bazı haberler bu raporda incelemenize sunulmuştur.

Haziran ayı raporu, Haziran ayında incelenen verilerden derlenen 10 farklı konuyu kapsamaktadır. Bu konuların %30'u saldırılarla ilgili haberler, %40'ü raporlar/rehberler ve %30'ü güvenlik açıklarıyla ilgilidir.

Sektörlere göre ayrıldığında, raporda "tüm"endüstriyel tesisler ile ilgili konular %50 oranında ele alınırken, enerji sektörü ile ilgili konulara %50 oranında yer verilmiştir.





Ayrıca Haziran ayı raporunda, Haziran ayında gerçekleşen 400'ün üzerindeki fidye yazılımı vakası incelenmiş, sektöre yönelik gözlemler raporda incelemeye sunulmuştur.

26 Haziran 2023

1. HABERLER

1.1. Kanada Siber Güvenlik Merkezi, Petrol ve Gaz Sektörünü Dijital Tedarik Zincirinden Kaynaklanan Siber Tehditlere Karşı Uyardı

Kanada Siber Güvenlik Merkezi, petrol ve gaz sektörünü, orta ila yüksek karmaşıklığa sahip bilgisayar korsanlarının tedarik zincirini hedef alarak dolaylı olarak kuruluşlara saldırmayı düşünecekleri konusunda uyardı. Ajans ayrıca, sınır ötesi entegrasyon nedeniyle Kanada'nın petrol ve gaz altyapısının ABD varlıklarına yönelik siber faaliyetlerden etkilenme ihtimalinin de yakın olmasını bekliyor.

Kanada siber güvenlik ajansı, geçen hafta yayınlanan kılavuzda, bu rakiplerin tedarik zincirini hedef kuruluşun ağları ve OT (operasyonel teknoloji) hakkında tedarikçilerden ticari olarak değerli fikri mülkiyet ve bilgi elde etmeyi ve bir hedef kuruluşun ağlarına erişmenin dolaylı bir yolu olarak hedeflediğini söyledi.

"Petrol ve gaz sektör oyuncuları da dahil olmak üzere büyük endüstriyel işletmeler; laboratuvarlardan, üreticilerden, üreticilerden, entegratörlerden ve yüklenicilerden, çeşitli ürün ve hizmet tedarik zincirinin yanı sıra günlük işletme, bakım, modernizasyon ve yeni kapasitelerin geliştirilmesi için internet, bulut ve yönetilen hizmet sağlayıcılarına güveniyor."

Ajans, petrol ve doğalgaz işletmelerinin tedarik zincirine bağımlılığının, siber aktörlere içeriden korunan BT ve OT sistemleri hakkında bilgi ve erişim fırsatları sağlayan kritik bir güvenlik açığı olduğunu da sözlerine ekledi. *"Orta ve yüksek gelişmişliğe sahip aktörlerin önümüzdeki 12 ay ve sonrasında tedarik zincirini bu amaçlar için hedeflemeye neredeyse kesinlikle devam edeceğini değerlendiriyoruz."*

Kılavuz ayrıca, finansal olarak motive olmuş siber suçluların, özellikle business email compromise (BEC) ve fidye yazılımının Kanada petrol ve gaz sektörünün karşı karşıya olduğu ana siber tehdit olduğu konusunda değerlendirmelerde bulunuyor. Fidye yazılımı, Kanadalılara güvenilir petrol ve gaz tedariki için neredeyse kesinlikle birincil siber tehdit olduğu belirtiliyor. Ayrıca, Kanada'daki petrol ve gaz sektörünün büyük olasılıkla ticari veya ekonomik nedenlerle devlet destekli siber casusluk tarafından hedef alınmaya devam edeceği konusunda uyardı. Risk altında tescilli ticari sırlar, araştırmalar, iş ve üretim planları da dahil olmak üzere.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector
https://industrialcyber.co/mining-oil-gas/canadian-cyber-centre-warns-oil-and-gas-sector-of-cyber-threats-originating-in-digital-supply-chain/

20 Haziran 2023

1.2. Araştırmacılar, Wago ve Schneider Electric OT Ürünlerindeki Yeni Ciddi Açıklıklarını Ortaya Koydu

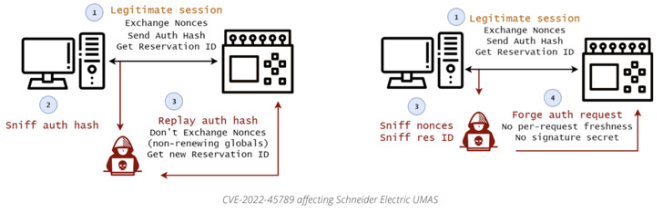
Wago ve Schneider Electric'in operasyonel teknoloji (OT) ürünlerinde üç güvenlik açığı açıklandı.

Forescout'a göre açıklıklar, toplu olarak OT: ICEFALL olarak adlandırılan ve şu anda 13 farklı üreticiyi kapsayan toplam 61 adetten büyük resmin bir parçasıdır.

Şirket, Hacker News ile paylaştığı bir raporda, "*OT: ICEFALL, OT cihaz üreticilerinde güvenli tasarım, yama ve test ile ilgili süreçlerin daha sıkı incelenmesine ve iyileştirilmesine duyulan ihtiyacı gösteriyor*" dedi.

Açıklıkların en ciddisi, güç sayaçlarının Schneider Electric'ten kullandığı ION / TCP protokolündeki kimlik bilgilerinin açık metin olarak gönderimini içeren CVE-2022-46680'dir (CVSS skor: 8.8).

Açıklığın başarılı bir şekilde kullanılması, tehdit aktörlerinin savunmasız cihazların kontrolünü ele geçirmesini sağlayabilir. CVE-2022-46680'in, Forescout tarafından Haziran 2022'de ortaya çıkarılan 56 kusurdan biri olduğunu belirtmekte fayda var.



Diğer iki yeni güvenlik açığı (CVE-2023-1619 ve CVE-2023-1620, CVSS puanları: 4.9), kimliği doğrulanmış bir saldırgan tarafından belirli hatalı biçimlendirilmiş paketler veya belirli istekler gönderilerek etkinleştirilebilecek WAGO 750 denetleyicilerini etkileyen servis sonlandırma (DoS) açıklıklarıyla ilgilidir.

OT: ICEFALL araştırmasını sonuçlandırırken Forescout, üreticilerin tasarım gereği güvenli uygulamalar konusunda hala temel bir anlayışa sahip olmadıklarını ve eksik yamalar yayınladıklarını ve uygun güvenlik testi prosedürlerini uygulayamadıklarını belirtiyor.

Şirket, *"Bu endişe verici çünkü OT ürünleri güvenlik kontrollerini uygulamaya başladıkça ve sertifikalandırıldıkça, güvenlik bakış açısının algısı değişebilir ve kontrolleri telafi etme konusundaki aciliyet duygusu düşebilir ve bu da yanlış bir güvenlik sorununa yol açabilir"* dedi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://thehackernews.com/2023/06/researchers-expose-new-severe-flaws-in.html

1 Haziran 2023

1.3. Moody's Siber Saldırılardan Etkilenen Altyapıların Kredi Notunu Düşürüyor

Moody's Investors Service, yakın zamanda Volt Typhoon adlı Çin devlet destekli bir hacker grubu tarafından yürütülen ABD kritik altyapı kuruluşlarını hedef alan gizli ve hedefli kötü amaçlı faaliyetlerin, ülkedeki kritik altyapı işletmeleri için risklerini artırdığını açıkladı. Bu bilgiler, risk değerlendirme firmasının siber saldırıların, diğer sektörlerden daha yüksek risk taşıdığını düşündükleri ve etkilenen altyapı için 'kredi negatif' olarak işaretledikleri ABD kritik altyapı işletmeleri için operasyonel risklerini artırdığını değerlendirmesine neden oldu.

ABD güvenlik kurumları ve uluslararası siber güvenlik yetkilileri tarafından yayınlanan ortak bir siber güvenlik rehberindeki ayrıntılarına göre, Volt Typhoon'un son faaliyetleri kritik ABD altyapı ağlarına sızdığını gösteriyor. ABD yetkilileri, Volt Tayfununun aynı teknikleri dünya çapındaki diğer sektörlere de uygulayabileceği konusunda uyarıyor.

Bu ay yayınlanan en son 'Kredi Görünümü'nde Moody's, CSA'nın kritik altyapı varlıklarına yönelik risklerle ilgili tavsiyesinin, diğer sektörlerden daha yüksek risk taşıdığını düşündüğümüz, etkilenen altyapı için kredinin negatif olduğunu söyledi.

Görünüm ayrıca, kritik altyapı için, operasyonel saldırılar uzun vadeli bir hizmet kesintisine, maddi varlıkların tahrip olmasına neden olabileceğinden, bilgi teknolojisi (BT) güvenliğinden ziyade operasyonel teknolojisi (OT) güvenliği için kredi riskinin daha keskin olduğunu da sözlerine ekledi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/news/volt-typhoon-leads-moodys-to-mark-critical-infrastructures-as-credit-negative-as-risk-more-acute-for-ot-security/

26 Haziran 2023

1.4. Suncor Energy Siber Saldırısı Petro-Kanada Benzin İstasyonlarını Etkiliyor

Kanada'daki Petro-Canada benzin istasyonları, ana şirketi Suncor Energy'nin bir siber saldırıya maruz kaldıklarını açıklaması nedeniyle müşterilerin kredi kartı veya ödül puanları ile ödeme yapmasını engelleyen teknik sorunlardan etkileniyor.

Suncor Energy, dünyanın 48. en büyük halka açık şirketi ve yıllık 31 milyar dolarlık geliri ile Kanada'nın en büyük sentetik ham petrol üreticilerinden biridir.

Şirket, saldırıyı hafifletmek için önlemler aldığını ve yetkililere durum hakkında bilgi verdiğini söyledi. Aynı zamanda, olay çözülene kadar müşteriler ve tedarikçilerle yapılan işlemlerin olumsuz etkilenmesini beklemektedir.

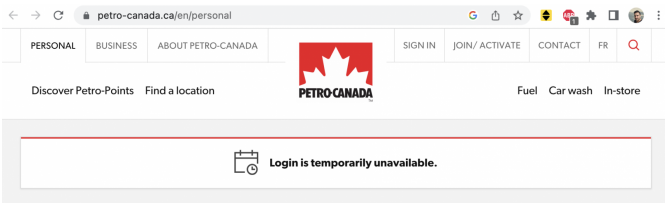
Suncord basın açıklamasında, "*Şu anda, bu durumun bir sonucu olarak müşteri, tedarikçi veya çalışan verilerinin tehlikeye atıldığına veya kötüye kullanıldığına dair herhangi bir kanıtın farkında değiliz*" diyor.

Şirket, siber güvenlik olayının türü ve sistemlerini etkileyen bir fidye yazılımı saldırısı olup olmadığı hakkında herhangi bir ayrıntı vermedi.

Petro-Kanada'nın Sistemleri Çalışamaz Hale Geldi

Kanada genelinde 1.500'den fazla benzin istasyonu işleten Suncor'un bir yan kuruluşu olan Petro-Canada da sorunlarla karşı karşıya olduğunu duyurdu.

Twitter'daki bir gönderide şirket, müşterileri şu anda uygulama veya web sitesi aracılığıyla hesaplarına giriş yapamayacakları konusunda uyardı ve neden olduğu rahatsızlıktan dolayı özür diledi. Bu kesinti, şirketin benzin istasyonlarında yakıt ikmali yaparken puan kazanmayı da engelliyor.



Ancak durum, kısa bildirimin sunduğundan çok daha kötü görünüyor.

Geçtiğimiz Cuma gününden bu yana birçok kişi Twitter'da Petro-Kanada istasyonlarında kredi / banka kartlarıyla ödeme yapmanın şu anda imkansız olduğunu ve tek seçenek olarak nakit para kullanıldığını bildirdi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://therecord.media/canadian-oil-giant-suncor-cyberattack
https://www.bleepingcomputer.com/news/security/suncor-energy-cyberattack-impacts-petro-canada-gas-stations/

8 Haziran 2023

1.5. Araştırma: Yatırımın, Beceri Eksikliğinin ve Zayıf İşbirliğinin Enerji Sektöründe Büyük Zorluklar Yaratmaya Devam Ettiğini Gösteriyor

Yeni DNV verileri, enerji endüstrisinin siber güvenlik tehditlerinden daha fazla haberdar olduğunu ve bunlara yönelik yatırımları artırdığını ortaya koyuyor. Hareket, artan jeopolitik gerilimler, ortaya çıkan uyumluluk gereklilikleri ve dijital olarak bağlı altyapının benimsenmesinin hızlanması arasında gerçekleşti. Araştırma ayrıca, yatırım, beceri eksikliği ve zayıf işbirliği sektör genelinde büyük zorluklar olmaya devam ettiğinden, güvenlik açısından kritik sistemlerin güvence altına alınmasına daha fazla odaklanılması gerektiğini tespit ediyor.

DNV, jeopolitik gerilimler ortaya çıkan tehditler konusunda artan farkındalığı tetiklediğinden, on enerji uzmanından altısının kuruluşlarının 2023'te siber güvenlik harcamalarını artırdığını söylediğini bildirdi. Bu, enerji endüstrisinin BT ve OT (operasyonel teknoloji) sistemlerine yönelik artan siber tehdidin farkında olduğu siber tehdit bilincinde bir adım değişikliği olarak geliyor. Bununla birlikte, endüstri profesyonelleri, güvenlik açısından kritik sistemleri korumak için bütçelerin hala çok düşük olduğu konusunda uyarıyorlar.

DNV, *"Ancak riskin farkındalığı, acil saldırı tehdidiyle sınırlı değil. Bu yılki araştırmamız, siber güvenliğin enerji endüstrisi için artan stratejik öneminin de altını çiziyor. Gerçekten de, 10 (%89) enerji uzmanından dokuzu, siber güvenliğin endüstrinin geleceğini mümkün kılan dijital dönüşüm girişimleri için bir ön koşul olduğuna inanıyor"* dedi.

Araştırma, Equinor, Dominion Energy, Vattenfall, Skagerak Energi dahil olmak üzere çeşitli enerji sektörü şirketlerinden uzmanlarla derinlemesine görüşmelerle tamamlanan 600 enerji uzmanından oluşan bir ankete dayanıyor.

Artan farkındalığa, olgunluğa ve siber güvenliğe yapılan yatırıma rağmen, yarısından azı, enerji profesyonellerinin yaklaşık yüzde 42'si kuruluşlarının yeterince yatırım yaptığını söylüyor. Her üç kişiden sadece biri, yaklaşık yüzde 36'sı, kuruluşlarının OT'lerini güvence altına almak için yeterli yatırım yaptığından emin.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/reports/dnv-reports-investment-skills-shortage-poor-collaboration-remain-major-challenges-across-energy-sector/

27 Haziran 2023

1.6. Siemens Energy, MOVEit Saldırısından Sonra Veri İhlalini Doğruladı

Siemens Energy, Clop grubu tarafından MOVEit Transfer platformunda sıfırıncı gün bir güvenlik açığı kullanarak verilerin çalındığını doğruladı.

Siemens Energy, 91.000 kişiyi istihdam eden ve yıllık 35 milyar dolar gelire sahip, Münih merkezli bir enerji teknolojisi şirketidir. Endüstriyel kontrol sistemleri (EKS/ICS), son teknoloji güç, ısı üretim üniteleri, yenilenebilir enerji sistemleri, tesis içi ve dışı enerji dağıtım sistemleri dahil olmak üzere çok çeşitli endüstriyel ürünler tasarlarmakta, geliştirmekte ve üretmektedir.

Şirket ayrıca petrol ve gaz endüstrisi için olay müdahale planları, güvenlik açığı değerlendirmesi ve yama yönetimi dahil olmak üzere çok çeşitli siber güvenlik danışmanlığı hizmetleri sunmaktadır.

Siemens Energy İhlali Doğruladı

Bu ay Clop, Siemens Energy'yi veri sızıntısı sitelerinde listeleyerek, şirketteki bir ihlal sırasında verilerin çalındığını belirtti.

Clop'un gasp stratejisinin bir parçası olarak, baskı uygulamak için önce bir şirketin adını veri sızıntısı sitelerinde listelemeye başlar, ardından nihai veri sızıntısını gerçekleştirir.

Şu anda hiçbir veri sızdırılmamış olsa da, bir Siemens Energy uzmanı, CVE-2023-34362 olarak izlenen bir MOVEit Transfer sıfırıncı gün güvenlik açığı kullanan son Clop veri hırsızlığı saldırılarından etkilendiğini doğruladı.

Ancak Siemens Energy, kritik verilerin çalınmadığını ve ticari operasyonların etkilenmediğini söylüyor.

Siemens Energy, Bleepingcomputer'a verdiği demeçte, *"Küresel veri güvenliği olayıyla ilgili olarak Siemens Energy hedefler arasında yer alıyor"* dedi.

"Mevcut analize dayanarak hiçbir kritik veriden ödün verilmedi ve operasyonlarımız etkilenmedi. Olayı öğrendiğimizde hemen harekete geçtik."

Schneider Electric'in Araştırması

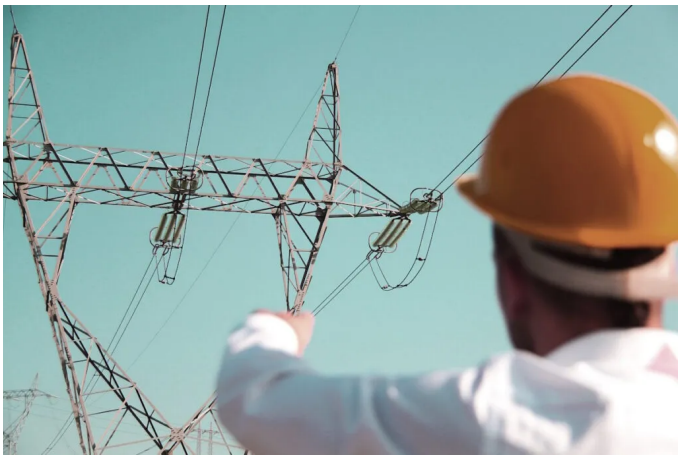
Clop, Siemens Energy ile birlikte başka bir endüstri devi Schneider Electric'in MOVEit Transfer sistemlerinden veri çaldığını iddia ediyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://therecord.media/ucla-siemens-energy-latest-moveit-victims
https://www.bleepingcomputer.com/news/security/siemens-energy-confirms-data-breach-after-moveit-data-theft-attack/

13 Haziran 2023

1.7. Endüstriyel Siber Güvenlik Şirketi, CosmicEnergy Kötü Amaçlı Yazılımının Endüstriyel Tesisler İçin ‘Acil Tehdit’ Olmadığını Belirtti



Endüstriyel siber güvenlik şirketi Dragos'taki tehdit istihbarat ekibi, CosmicEnergy'nin genel kod tabanının olgunluktan yoksun olması, hatalar içermesi ve Industryer2 veya CrashOverride gibi tam teşekküllü bir saldırı yeteneği olmaktan uzak olması nedeniyle Cosmicenergy'nin operasyonel teknoloji (OT) için acil bir tehdit olmadığını açıkladı. CosmicEnergy’nin kullanıldığına dair hiçbir kanıt bulunmadığını ve analizin, aracın muhtemelen bir eğitim tatbikatının parçası olduğunu veya tespit geliştirmede kullanıldığını gösterdiğini de sözlerine ekledi.

Dragos, geçen ay Mandiant'ın açıklamasının ardından bir blog yazısında, *“IEC 104 cihazlarını hedeflemek için tasarlanan bu kötü amaçlı yazılımın, uzak terminal birimlerine (RTU'LAR) bağlı mevcut Microsoft SQL (MSSQL) sunucularından yararlandığını söyledi. Dragos Threat Intelligence, kötü amaçlı yazılımları bağımsız olarak analiz etti ve güç kesintisi veya şebekeyi çalışamaz hale getiren yetenekler iddia eden medya görüşlerine karşı, CosmicEnergy'nin operasyonel teknoloji için acil bir tehdit olmadığı sonucuna vardı.”*

Dragos ayrıca, yazılım paketlerinin MSSQL içerip içermediğini görmek için operatörlerin üreticilere ulaşması gerektiğini söyledi. Ek olarak, operatörler ağ izlemelerinin sorunsuz olduğundan emin olmalı, ‘xp cmdshell’ uyarılarını izlemeli ve MSSQL Sunucularını denetlemelidir.

CosmicEnergy’ yi ele alan Dragos, potansiyel riskini azaltmak için kodlama hataları ve gelişim olgunluğu eksikliği olan bir eğitim aracı olduğuna dair göstergeler buldu. Keşfi, Pipedream'de de tanık olunan, bir etki elde etmek için bilinen standart EKS protokollerinden yararlanan ve araçlarını uygulamak için ‘lib60870-C’ gibi açık kaynaklı projeleri içeren geliştiricilere yönelik bir eğilime işaret ediyor.

Dragos, CosmicEnergy'nin konuşlandırıldığına dair hiçbir kanıt olmamasına rağmen, varlığının tüm kuruluşlardan güvenlik duvarı kurallarını ve yapılandırmalarını yeniden değerlendirmelerini ve ağlarından geçen EKS protokolleri hakkında görünürlük sahibi olmalarını sağlamasını istemesi gerektiğini söyledi. *"Bu, IEC104 hedefli araçların üçüncü keşfidir, bu nedenle kuruluşlar gelecekteki potansiyel saldırıları tespit etme ve azaltma olasılığını artırmak için dikkat etmeli ve iyi bir güvenlik yaklaşımı uygulamalıdır"* diye ekledi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/news/dragos-says-cosmicenergy-malware-is-not-immediate-threat-to-ics-provides-recommendations/

20 Haziran 2023

1.8. Schneider Güç Ölçer Güvenlik Açığı Elektrik Kesintilerine Kapı Açıyor

Schneider Electric ION ve PowerLogic güç sayaçlarındaki bir güvenlik açığı açıklandı: Her mesajda bir kullanıcı kimliği ve parolayı açık metin olarak iletiyorlar.

10 üzerinden 8,8'lik bir CVSS güvenlik açığı önem derecesi verildiğinde, hata, pasif müdahale yeteneklerine sahip bir saldırganın bu kimlik bilgilerini ele geçirmesine, ION / TCP mühendislik arayüzünde (SSH ve HTTP arayüzlerinin yanı sıra) kimlik doğrulamasına ve yapılandırma ayarlarını değiştirmesine veya potansiyel olarak ürün yazılımını değiştirmesine izin verecektir.

Forescout'ta güvenlik araştırması olan Daniel dos Santos: *"Bir operasyonel teknoloji (OT) ürününün kimlik bilgilerini açık metin olarak iletmesi artık kabul edilemez çünkü ağa erişimi olan ve trafiği izleyebilen herkes bunları elde edebilecek ve ardından cihazla neredeyse istediklerini yapabilecek"* diyor. Bu, talep (veya yük) daha sonra şebeke ağının diğer bölümlerine aktarılırken, kapanmaları tetikleyebilecek yük salınımlarına neden olmak için akıllı sayaç anahtarlarının kontrol edilmesini içerebilir. En kötü senaryoda, domino etkisi teorik olarak büyük çağlı enerji kesintilerine yol açabilir.

Forescout'un Icefall OT araştırmasının bir parçası olarak açıklanan bu güvenlik açığı, bugün Infosecurity Europe'da açıklanan üç güvenlik açığından biri, diğer ikisi ise WAGO 740 denetleyicilerindeki servis sonlandırma (DoS) güvenlik açıklarıdır. DoS sorunlarının her ikisine de önem derecesi 4.9 olarak verilmiştir.

Schneider, ION Protokolünün 30 yıldan uzun bir süre önce dijital güç sayaçlarına gelişmiş veri alışverişi sağlamak için oluşturulduğunu ve siber güvenliğin bir endişe kaynağı haline gelmesiyle protokolün kimlik doğrulama desteği ile geliştirildiğini söyledi.

Ancak bu, genellikle eski kodlarda olduğu gibi hala güvenlik açıklarının olmadığı anlamına gelmez. Aslında dos Santos, Schneider güvenlik açığının başlangıçta Haziran 2022'de 56 OT güvenlik açığının bir parçası olarak duyurulmak istendiğini, ancak yama işlemleri nedeniyle bekletildiğini söylüyor.

"Bu, daha erken bir zamanda tasarlanan şeylerin örneklerinden biri ve Schneider, bunun bir güvenlik açığı olduğunu kesinlikle kabul ediyor ve sorunu bularak ve çözerek günümüze getirmek için onlarla birlikte çalıştık" diyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/schneider-power-meter-vulnerability-power-outages

2 Haziran 2023

1.9. CISA, Yeni Güvenlik Açıkları Buluyor; Delta Electronics, Mitsubishi Electric, Hitachi Energy için Önceki Bildirimleri Güncelliyor

ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CSA) bu ay yayınlanan beş ADETEKS/ICS (endüstriyel kontrol sistemleri), Advantech ve HID Global'den gelen ekipmanlardaki donanım açıkları konusunda uyarıyor. Ajans ayrıca Delta Electronics, Mitsubishi Electric ve Hitachi Energy'den donanımdaki güvenlik açıklıklarıyla ilgili önceki tavsiyeleri de güncelledi. Bu bildirimler, EKS cihazlarını çevreleyen güncel güvenlik sorunları, güvenlik açıkları ve istismarlar hakkında zamanında erken aşama bilgiler sağlamaktadır.

CISA, Advantech'in Web Access Node ekipmanının, düşük saldırı karmaşıklığı kullanılarak uzaktan kullanılabilecek güvenlik açıkları içerdiğini açıkladı. Güvenlik açıkları, kod oluşturmanın yanlış kontrolünü (kod enjeksiyonu) ve *'tehlikeli türde dosyanın sınırsız yüklenmesini içermektedir.'*

CISA, Advantech WebAccess / SCADA v9.1.3 ve öncesinde, bir saldırganın işletim sistemindeki herhangi bir dosyanın (sistem dosyaları dahil) üzerine yazmasına, bir XLS dosyasına kod enjekte etmesine ve dosya uzantısını değiştirmesine izin verebilecek keyfi bir dosya üzerine yazma güvenlik açığı olduğunu ekledi.

"Advantech WebAccess / SCADA v9.1.3 ve öncesinde, bir saldırganın 'yönetici' kullanıcı olarak oturum açtığında bir ASP komut dosyasını bir web sunucusuna yüklemesine izin verebilecek keyfi bir dosya yükleme güvenlik açığı bulunmaktadır ve bu da keyfi kod yürütülmesine yol açabilir" şeklinde belirtildi. *"Advantech WebAccess / SCADA v9.1.3 ve öncesinde, bir saldırganın bir sertifika dosyasının dosya uzantısını yüklerken ASP'ye değiştirmesine izin verebilecek rastgele bir dosya yükleme güvenlik açığı bulunmaktadır ve bu da uzaktan kod yürütülmesine neden olabilir."* Her üç güvenlik açığı için de CVSS v3 taban puanı 7,2 olarak hesaplandı.

Kritik üretim, enerji, su ve atık su sistemlerinde kullanılan Advantech, WebAccess/ SCADA kullanıcılarının 9.1.4 sürümüne yükseltmeleri önerilmektedir.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/critical-infrastructure/cisa-finds-security-flaws-in-advantech-hid-global-hardware-updates-earlier-notices-for-delta-electronics-mitsubishi-electric-hitachi-energy/

2 Haziran 2023

1.10. Çinli Tehdit Aktörü, Tayvan'ın Kritik Altyapısına Saldırmak için Değiştirilmiş Kobalt Saldırısı Varyantını Kullandı

EclecticIQ araştırmacıları, kritik altyapı da dahil olmak üzere Tayvan devlet kurumlarını hedef almak için kullanılan Çinli bir tehdit aktörü tarafından işletilen kötü amaçlı bir web sunucusu tespit ettiklerini belirttiler.

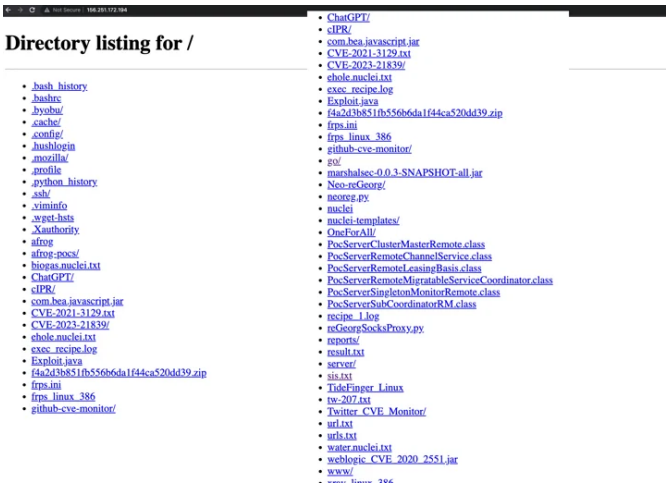
Komuta ve kontrol altyapısı halka açık bir şekilde internete maruz kaldı. Sunucuda bulunan günlük ve meta verilere dayanarak, EclecticIQ analistleri, tehdit aktörünün keşif, kötü amaçlı yazılım dağıtımı ve seçilen hedeflere yönelik sömürü sonrası dahil olmak üzere saldırgan siber operasyonlar gerçekleştirdiğini değerlendiriyor.

EclecticIQ analistleri, "Cobalt Strike Cat" olarak bilinen Cobalt Strike'ın değiştirilmiş bir versiyonunu belirlediler. Araştırmacılar bu günlükleri analiz ettiler ve tehdit aktörü taktikleri, teknikleri ve prosedürlerinin (TTP'ler) ayrıntılı bir haritasını oluşturdular.

Tehdit aktörü, öncelikle web hizmetlerini hedeflemek için dört farklı uzaktan kod yürütme (RCE) güvenlik açığından yararlanmaya odaklandı ve bazıları yalnızca Çin yeraltı forumlarında bulunan açık kaynaklı araçlara büyük ölçüde güvendi. Tehdit aktörü ayrıca kurbanın dahili web hizmetlerine servis sonlandırma saldırıları düzenledi.

Açığa Çıkan Tehdit Aktörü Altyapısı Saldırgan Araçları Ortaya Koyuyor

EclecticIQ analistleri IP adresi 156[.]251[.]172[.]194 olan bir web sunucusu keşfettiler. Sunucu, Şekil 1'de ayrıntılı olarak açıklanan dosya ve klasörlere hizmet vermek için SIMPLEHTTPSERVER adlı bir Python kitaplığının kullanıldığını gösteren HTTP başlık verilerini (SimpleHTTP / 0.6 Python / 3.8.10) içeriyordu.



Şekil 1: Mevcut araçları ve hedef listelerini gösteren açık tehdit aktörü altyapısının ekran görüntüsü.

Hedefli Saldırı Yaşam Döngüsü

Hedefli Saldırı Yaşam Döngüsü, düşman taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) yapılandırılmış bir şekilde haritalamak için kullanılan bir metodolojidir.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://blog.eclecticiq.com/chinese-threat-actor-used-modified-cobalt-strike-variant-to-attack-taiwanese-critical-infrastructure

2. FİDYE YAZILIMI SALDIRILARI

Haziran ayında faaliyetleri takip edilen fidye yazılımı saldırıları incelendiğinde; küresel olarak en çok hedef alınan sektörler **imalat, hizmet, finans** ve **eğitim** olmuştur.

Enerji sektörü özelinde, en çok hedeflenen ülke '**Almanya'** olurken bu sektörü en çok hedefleyen grup '**Alphv'** olmuştur.

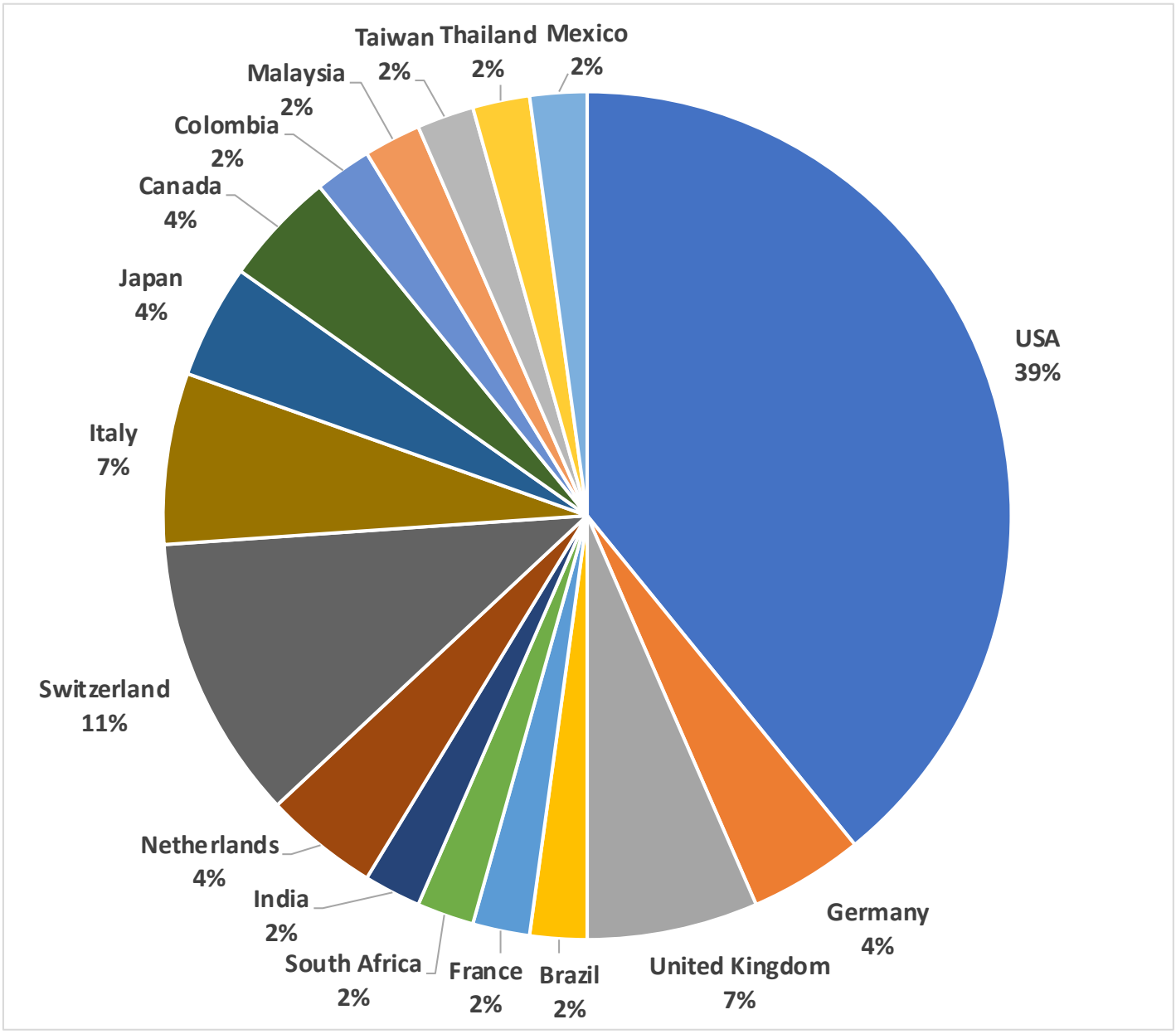
Grup	Hedef Sektör	Hedef Ülke
Darkrace	Enerji	Almanya
8base	Yenilenebilir Enerji	Brezilya
Alphv	Enerji	Angola
Clop	Enerji	Hollanda
Alphv	Petrol ve Gaz	Endonezya
Lockbit3	Enerji	Peru
Alphv	Enerji	ABD
Medusa	Enerji	Almanya
Clop	Enerji	Almanya

İmalat sektörünü en çok hedef alan fidye yazılımı gruplarının hedeflediği kuruluş oranında pazardaki payları aşağıdaki tabloda incelemeye sunulmuştur.

Grup	%
Lockbit3	17
Alphv	15
Akira	11
8base	11
Rhysida	9
Play	9
Snatch	9
Blackbasta	7
Clop	4
Diğer	8

Haziran ayında imalat sektörünü en çok hedef alan gruplar şunlardı: **Lockbit3**, **Alphv**, **Akira** ve **8base**.

İmalat sektöründe Haziran ayında en çok hedef alınan ülkelere dair dağılım aşağıdaki grafikte izlenime sunulmuştur.



CYBER WISE | ICSFUSION

Endüstriyel Tesislere Yönelik

Saldırı Bilgilendirme Raporu

icsfusion.com