CYBER WISE | ICSFUSION

Endüstriyel
Tesislere Yönelik

Saldırı Bilgilendirme Raporu

Nisan 2023

icsfusion.com

ICSFUSION

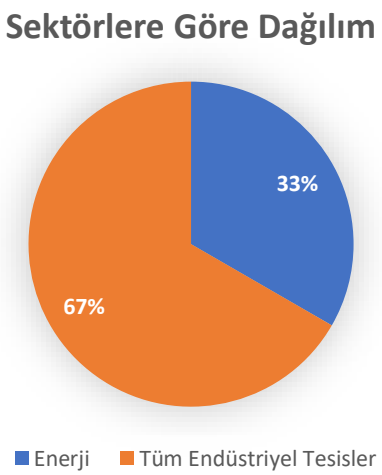
İÇİNDEKİLER

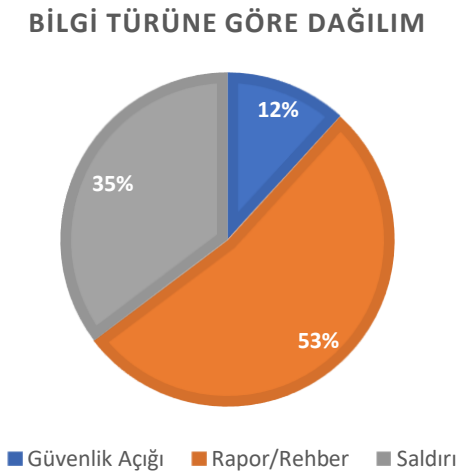
YÖNETİCİ ÖZETİ

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.

Nisan ayı raporu, Nisan ayında incelenen verilerden derlenen 14 farklı konuyu kapsamaktadır. Bu konuların %35'i saldırılarla ilgili haberler, %53'ü raporlar/rehberler ve %12'si güvenlik açıklarıyla ilgilidir.

Sektörlere göre ayrıldığında, raporda "tüm"endüstriyel tesisler ile ilgili konular %67 oranında ele alınırken, enerji sektörü ile ilgili konulara %33 oranında yer verilmiştir.





Ayrıca Nisan ayı raporunda, Nisan ayında gerçekleşen 300'ün üzerindeki fidye yazılımı vakası incelenmiş, sektöre yönelik gözlemler raporda incelemenize sunulmuştur.

6 Nisan 2023

1. HABERLER

1.1. Enerji Sektörüne Yönelik Siber Saldırıların Devam Edeceği Tahmin Ediliyor

Sekoia tarafından yayınlanan veriler, özellikle Rusya-Ukrayna ihtilafının ışığında, enerji sektörünün 2022'de Avrupa'nın endişe içerisinde olduğunu ortaya koydu. Sektör, casusluk, sızma ve sabotaj dahil olmak üzere çeşitli siber etkin operasyonların hedefi oldu. Ek olarak, Avrupa enerji sektörü, çoğunlukla Hizmet Olarak Fidye Yazılımı (RaaS) grupları tarafından yürütülen çifte gasp saldırıları ve hack-and-leak operasyonları olmak üzere kazanç odaklı kampanyalarla karşı karşıya kaldı.

Siber güvenlik şirketi, *"Gözlemlerimize dayanarak **LockBit, BlackCat, RagnarLocker, Cuba ve Hive** gibi grupların enerji sektörünü etkileyen fidye yazılımı kampanyaları yürüten en aktif topluluklar olduğunu"* açıkladı. *"Bu grupların çoğu, kazançlı kampanyalarda Hizmet Olarak Fidye Yazılımı (RaaS) modeli altında faaliyet gösteriyor. Rusça konuşan iştiraklerden oluşan BlackCat fidye yazılımı grubunun, 2022'de Batı Avrupa'daki kritik enerji altyapılarını hedef alan artan sayıda fidye yazılımı saldırısı iddiasında bulunduğunu gözlemledik."*

Sekoia araştırmacıları, enerji sektörünü etkileyen fidye yazılımı faaliyetlerinin doğası gereği hala fırsatçı olduğunu değerlendirdi. *"Fidye yazılımı tehdit aktörlerinin, fidye taleplerinin karşılanmasını sağlamak ve hatta daha yüksek bir fidye talep etmek için enerjiyle ilgili faaliyetlerin kritikliğine güvenmeleri oldukça olasıdır. Enerji sektörünün, fidye yazılımı grupları da dahil olmak üzere son derece organize siber suç aktörleri için birincil hedef olmaya devam edeceğini değerlendiriyoruz"* dediler.

Gönderi ayrıca, İsrail ile Lübnan arasındaki, özellikle Karish gaz sahasıyla ilgili olan deniz anlaşmazlığının yanı sıra İsrail ile **Türkiye** arasındaki gaz boru hattı tartışmalarının, enerji ile ilgili kuruluşları hedef alan İran bağlantılı bölgesel siber casusluk faaliyetleri için itici güç olabileceğini değerlendiriyor.

Geçen ay, ABD Senatosu Enerji ve Doğal Kaynaklar Komitesi, ülkenin enerji altyapısına yönelik siber güvenlik açıklarını incelemek için tam bir komite oturumu düzenledi. Komite ayrıca, enerji kaynaklarının ülkenin dost ve müttefiklerine karşı jeopolitik bir silah olarak kullanıldığını inceleyerek, düşmanların Amerikan altyapısına sızmak için siber saldırıları giderek daha fazla kullandığına ve enerji güvenliğini ve ekonomiyi etkilemek için çalıştığına dikkat çekti.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/utilities-energy-power-water-waste/sekoia-expects-hackers-to-continue-targeting-energy-sector-through-ransomware-hack-and-leak-attacks/

5 Nisan 2023

1.2. CISA JCDC Enerji Sektörüne Odaklanacak

CISA'nın Ortak Siber Savunma Topluluğu (JCDC) girişimi, siber tehditlerden korunmak ve bunlara yanıt vermek için operasyon planları oluşturacak.

Siber suçluları düşündüğünüzde aklınıza ne geliyor? Kime sorduğuna bağlı olarak, çeşitli cevaplar alacaksınız. Bazıları için siber suçlu, bazı Hollywood mecazlarına uyuyor: loş bir odada tek başına oturan, bir kişiden veya şirketten bilgi çalmak için klavyeyi öfkeyle basan bir kişi.

Yaygın tehdit ortamını dikkate alan ABD hükümeti, vatandaşları ve işletmeleri korumak için bir ekip oluşturmaya daha fazla kaynak ayırdığı görülüyor. Bu çaba , Siber Güvenlik ve Altyapı Güvenliği Ajansı'nın (CISA) 2018'de kurulmasıyla başladı.

Bir adım daha ileri giderek, 2021'de CISA, siber tehditlerden korunmaya ve bunlara yanıt vermeye yönelik operasyon planları oluşturmak üzere hükümet ve özel sektör temsilcilerini bir araya getirmek için formüle edilmiş bir girişim olan Ortak Siber Savunma Topluluğu (JCDC) kurulduğunu duyurdu.

JCDC, acil riskler (Rusya'nın Ukrayna'yı işgaliyle ilgili artan farkındalık, Log4Shell güvenlik açığı gibi) için işbirliğinin faydalarını gördüğü değerlendiriliyor ancak yakın zamanda oluşan tehditler söz konusu olduğunda topluluğun etkinliği tartışılıyor. Bu boşluğu gidermek için JCDC, gelecekteki siber riskler için proaktif önlemler planlıyor.

Enerji Sektöründe Siber Risk

Son yıllarda tehdit aktörlerinin saldırıları keskin bir şekilde artış göstermiştir. 2022 üçüncü çeyrekte enerji sektöründe rekor sayıda saldırı görüldü, bu trendin yavaşlaması beklenmiyor.

Kamu hizmeti sektörüne yönelik tehditler, 2021'de Colonial Pipeline yurtdışındaki siber suçlular tarafından hacklendiğinde gündeme geldi. Colonial Pipeline olayı en yüksek profilli kamu hizmeti hack'lerinden biri olsa da, elektrik şebekesi de saldırıya uğradı.

Kuzey Carolina, Moore County'de, bir elektrik trafo merkezine yapılan başarılı bir saldırı, binlerce insanı bir hafta boyunca elektriksiz bıraktı. Kısa bir süre sonra, saldırganlar Kuzeybatı Pasifik'teki altı istasyonu daha hedef aldı.

CISA, JCDC'nin eyalet, yerel ve bölgesel kuruluşlar için desteği ölçeklendirmek için planlama çabaları başlatacağını duyurdu. Öncelik, küçük ve orta ölçekli kritik altyapıyı desteklemek ve riskleri azaltmak ve olay durumunda hızlı bir müdahale protokolü tasarlamak için devlet ve özel sektör temsilcileriyle ortak çalışmak olarak belirtiliyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://securityaffairs.com/144466/security/cisa-jddc-energy-sector.html

11 Nisan 2023

1.3. ISA, İskoçya'da Enerji Odaklı Siber Güvenlik Zirvesine Ev Sahipliği Yapacak

Operasyonel teknoloji (OT) siber güvenlik fırsatlarının hızla büyümesine odaklanan ISA, 31 Mayıs ve 1 Haziran 2023 tarihlerinde endüstriyel siber güvenlik etkinliğines ev sahipliği yapacak ve 29-30 Mayıs tarihlerinde ayrıca eğitim oturumları düzenleyecek.

ISA , otomasyon ve kontrol sistemleri siber güvenlik standartları olan ISA/IEC 62443 dahil olmak üzere endüstriyel otomasyonda kullanılan birçok teknik standardı belirler. ISA, bu standartları geliştirmenin ve sürdürmenin yanı sıra siber güvenlik konusunda eğitim ve yetkilendirme sunar; ISASecure sertifikası ile ürünleri, süreçleri ve sistemleri onaylar ; ve üyelik konsorsiyumu ISA Global Cybersecurity Alliance (ISAGCA) aracılığıyla OT siber güvenliğinin önemi konusunda farkındalığı artırmaktadır.

OT Siber Güvenlik Zirvesi, operatörler, hizmet sağlayıcılar, yasal düzenleyiciler ve ekipman sağlayıcılar için yüz yüze görüşme fırsatı sunuyor. Bu iki aşamalı, iki günlük etkinlik iki ana başlık etrafında düzenlenecek: tedarik zinciri risk yönetimi ve ISA/IEC 62443'ü anlama üzerine ek panel tartışmaları ile tedarik zinciri ve tehdit istihbaratı konularıdır.

Etkinlik komitisesinin notu: *"OT siber güvenlik ortamına yönelik tehditleri azaltmak için neyin işe yaradığına dair daha fazla bilgi edinmek isteyen herkes, bu etkinliği hem bilgilendirici hem de yararlı bulacaktır. Delegeleri şahsen ve çevrimiçi olarak ağırlamayı dört gözle bekliyoruz."*

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://finance.yahoo.com/news/isa-host-energy-focused-cybersecurity-123000175.html?guccounter=1
https://www.streetinsider.com/Newsfile/ISA+to+Host+Energy-focused+Cybersecurity+Summit+in+Scotland/21489560.html

19 Nisan 2023

1.4. İran Hükümeti Destekli Bilgisayar Korsanları ABD Enerji ve Ulaşım Sistemlerini Hedefliyor

Mint Sandstorm, 2021'in sonları ile 2022'nin ortaları arasında ABD'deki kritik altyapıyı hedef alan saldırılarla İran hükümeti destekli olduğu düşünülen bir tehdit grubudur.

Microsoft Tehdit İstihbaratı ekibi, *"Mint Sandstorm alt grubu, teknik ve operasyonel olarak olgun, özel araçlar geliştirme ve N-day güvenlik açıklarını hızlı bir şekilde silah haline getirme yeteneğine sahip ve İran'ın ulusal öncelikleriyle uyumlu görünen operasyonel odağında çeviklik sergiledi"* dedi.

Hedeflenen varlıklar **limanlardan**, **enerji** şirketlerinden, transit sistemlerden ve büyük bir ABD kamu hizmeti ve **gaz** şirketinden oluşmaktadır. Faaliyetin, Mayıs 2020 ile 2021'in sonları arasında deniz, demiryolu ve benzin istasyonu ödeme sistemlerini hedef alan saldırılara misilleme niteliğinde olduğundan şüpheleniliyor.

Burada, İran'ın daha sonra İsrail ve ABD'yi ülkede huzursuzluk yaratmak amacıyla benzin istasyonlarına yönelik saldırıları planlamakla suçladığını belirtmekte fayda var.

Mint Sandstorm, Microsoft'un daha önce ***Phosphorus*** adı altında izlediği ve *APT35*, ***Charming Kitten, ITG18, TA453 ve Yellow Garuda*** gibi diğer siber güvenlik sağlayıcıları tarafından da izlenen tehdit aktörüne atanan yeni adıdır.

Terminolojideki değişiklik, kısmen artan "tehditlerin karmaşıklığı, ölçeği ve hacmi" nedeniyle Microsoft'un kimyasal elementlerden ilham alan takma adlardan hava durumu temalı yeni bir tehdit aktörü adlandırma taksonomisine geçişinin bir parçasıdır.

İran İstihbarat ve Güvenlik Bakanlığı (MOIS) adına faaliyet gösterdiği bilinen MuddyWater'ın (aka Mercury veya Mango Sandstorm) aksine, Mint Sandstorm'un İslam Devrim Muhafızları Birliği (IRGC) ile bağlantılı olduğu söyleniyor.

Teknoloji devi, *"Bu Mint Sandstorm alt grubuna atfedilen izinsiz girişlerde gözlemlenen yetenekler, operatörlerin C2 iletişimini gizlemesine, güvenliği ihlal edilmiş bir sistemde devam etmesine ve çeşitli yeteneklere sahip bir dizi uzlaşma sonrası aracı devreye almasına izin verdiği için endişe vericidir"* diye ekledi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://thecyberpost.com/news/hackers/attacks/iranian-government-backed-hackers-targeting-u-s-energy-and-transit-systems/
https://thehackernews.com/2023/04/iranian-government-backed-hackers.html

20 Nisan 2023

1.5. Cisco Kritik Güvenlik Açıkları İçin Yama Duyurusunda Bulundu

Cisco, bu hafta Industrial Network Director ve Modeling Labs uygulamalarını etkileyen kritik düzeydeki güvenlik açıkları için yamalar yayınladı.

Endüstriyel ağ yönetimi için tasarlanan Industrial Network Director (IND), ağ ve otomasyon cihazlarına görünürlük sağlar.

Geçtiğimiz ay Cisco, IND'nin web arayüzünde, işletim sisteminde komut yürütmek için uzaktan kullanılabilecek kritik öneme sahip bir açıklık için düzeltmeler yayınladı.

Bu hafta teknoloji devi ayrıca şirket içi bir ağ simülasyon aracı olan Modeling Labs'ın harici kimlik doğrulama mekanizmasındaki kritik öneme sahip bir açıklık için de yamalar yayınladı.

CVE-2023-20154 (CVSS puanı 9.1) olarak izlenen sorun açıklık Modeling Labs sürüm 2.5.1'in sürümünde giderilmiştir.

Geçtiğimiz ay şirket ayrıca, StarOS yazılımında ve BroadWorks ağ sunucusunda sırasıyla yetki yükseltme ve hizmet reddine (DoS) yol açabilecek yüksek önem dereceli güvenlik açıkları için yamalar duyurdu.

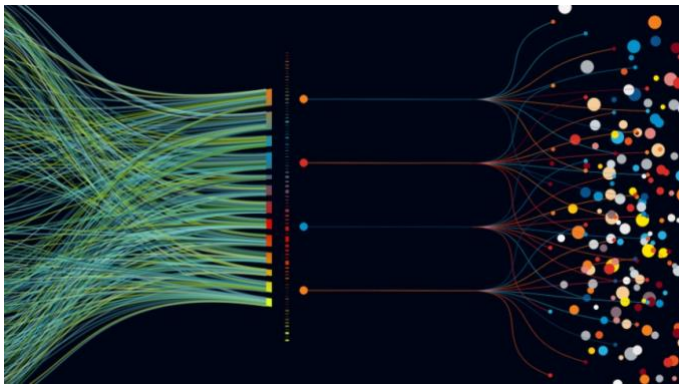
Teknoloji devi, bu güvenlik açıklarından herhangi birinin saldırılarda kullanıldığına ilişkin veri olmadığını aktarmıştır. Ancak, yama uygulanmamış Cisco ürünlerinin kötüye kullanıldığı bilindiğinden, işletmelerin mevcut düzeltmeleri mümkün olan en kısa sürede uygulamaları tavsiye ediliyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/cisco-patches-critical-vulnerabilities-in-industrial-network-director-modeling-labs/

24 Nisan 2023

1.6. Endüstriyel Güvenlik Sağlayıcıları, Kritik Altyapı Tehditleri Hakkında İstihbarat Paylaşmak İçin İş Birliği Yapıyor



Endüstriyel siber güvenlik alanında çalışan şirketler, tehdit istihbaratını paylaşmak için ETHOS adlı bir erken uyarı platformu kuruyor.

Endüstriyel siber güvenlik üreticileri, kritik altyapıya yönelik tehditler hakkında erken uyarılar sağlamak için açık kaynaklı, isteğe bağlı bir tehdit istihbaratı paylaşım portalı oluşturuyor.

Emerging Threat Open Sharing veya ETHOS adlı platform, kuruluşların tüm enerji sektörünü, boru hattı operatörlerini veya diğer endüstriyel sektörleri etkileyebilecek en son saldırılar veya güvenlik açıkları hakkında aynı bilgilere erişimi olmadığı için ortaya çıkan bilgi boşluklarını ortadan kaldırmak üzere tasarlandı.

Andrea Carcano, " *Oyunu yükseltmeye çalışıyoruz. Zekanız her zaman görebildikleriniz ile sınırlı olacak ve pazar payınızın ne kadar büyük olduğu önemli değil.”*

Kritik ağlara yönelik genel görünürlük eksikliği, ABD'de uzun süredir devam eden bir endişe olmuştur. Bu sorun nedeniyle Biden yönetimi, çeşitli kritik sektörler arasında görünürlüğü artırmak için birden fazla uygulama başlatmıştır.

“Sahip olabileceğimiz görünürlükte devasa bir gelişme. Daha önce hiç sahip olmadığımız bir zeka," şeklinde aktaran Carcano. *"Ülkede bugüne kadar X üretici alarmı, Y üretici alarmı, Z üretici alarmı içinde gömülü kalacak bir şeyler olup olmadığını gerçekten keşfedebiliriz."*

Marty Edwards ise yaptığı açıklamada, EKS altyapılarındaki asıl zorluğun, hangi tehditlerin bir kuruluş için gerçekten tehdit oluşturduğunu bilmek olduğunu söyledi.

Edwards, *"ETHOS, endüstri üyelerinden gerçek dünya tehdit bilgilerinin keşfedilmesini ve yayılmasını otomatikleştirerek gürültüyü kesmeyi amaçlayan, üretici bağımsız bir girişimdir"* dedi. *"Amaç, tüm topluluğa OT sistemlerindeki yeni ve bilinen güvenlik açıklarını hedefleyen tehditler hakkında daha fazla veri sağlamak olacak."*

ETHOS beslemesi herkese açık olmayacak. Bunun yerine, yalnızca her bir ETHOS örneği için kaydolanlar istihbaratı görebilecek ve paylaşabilecektir - şu anda istihbarat tipik olarak IP adresleri, etki alanları gibi verilerden oluşmaktadır. İlk beta yalnızca bir sunucu olacak ve genel üyelik başvuruları Haziran ayında başlayacak.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://cyberscoop.com/emerging-threat-open-sharing-industrial-cybersecurity/

24 Nisan 2023

1.7. Inea Endüstriyel Ürünündeki Kritik Açıklıklar, Endüstriyel Kuruluşları Uzaktan Saldırılara Maruz Bırakıyor

Inea RTU'larda bulunan kritik güvenlik açığı, cihazları uzaktan ele geçirmek ve endüstriyel kuruluşlarda kesintiye neden olmak için kullanılabilir.

Slovenya merkezli endüstriyel otomasyon şirketi Inea tarafından üretilen bir uzak terminal biriminde (RTU) bulunan kritik bir güvenlik açığı, endüstriyel kuruluşları siber saldırılara maruz bırakabilir.

Güvenlik açığının varlığı, geçen hafta ABD Siber Güvenlik ve Altyapı Güvenliği Dairesi'nin (CISA) kuruluşları bilgilendirmek için bir rehber yayınladığında gün ışığına çıktı.

CVSS puanı 10 olan CVE-2023-2131 olarak izlenen güvenlik açığı, 3.36'dan önceki ürün yazılımı sürümlerini çalıştıran Inea ME RTU'ları etkiliyor. CISA, ilgili güvenlik açığının uzaktan yetkisiz komut yürütülmesine imkan sağlayacağını bildirmiştir.

CISA'ya göre ürün dünya çapında enerji, ulaşım, su ve atık su gibi sektörlerde kullanılmaktadır.

Güvenlik açığı, Hollanda'daki Radboud Üniversitesi'nde siber güvenlik alanında yüksek lisans derecesi almaya çalışan bir araştırmacı olan Floris Hendriks tarafından keşfedildi.

Hendriks, güvenlik açığını EKS uzaktan yönetim cihazlarının güvenliğine yönelik daha büyük bir araştırma projesinin parçası olarak bulduğunu belirtmiştir. Araştırmacı ve Radboud Üniversitesi'nden başka bir araştırmacı yakın zamanda Contec ve Control By Web ürünlerinde de açıklıklar keşfetmişti.

Bu projenin bir parçası olarak Hendriks, Censys arama motorunu kullanarak cihazları keşfetmek için bir yöntem geliştirdi. Cihazlar çevrimiçi olarak tanımlandıktan sonra, aygıt yazılımları güvenlik açıkları açısından analiz edilebilmektedir.

Araştırmacı, SecurityWeek'e Inea RTU güvenlik açığının doğrudan internetten kimlik doğrulaması yapılmadan kullanılabileceğini aktarmıştır.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/critical-flaw-in-inea-ics-product-exposes-industrial-organizations-to-remote-attacks/

28 Nisan 2023

1.8. Tahmin: Küresel Endüstriyel Güvenlik Sistemleri Pazar Büyüklüğü 2030'a Kadar 91,71 Milyar Doları Aşacak

Küresel Endüstriyel Güvenlik Sistemleri Pazar Büyüklüğü/Pay Geliri Sonunda 2030'a Kadar 91,71 Milyar Doları Aşacak!

Küresel Endüstriyel Güvenlik Sistemleri Pazar büyüklüğü ve hisse gelirinin 2022'de yaklaşık 51,52 milyar ABD Doları değerinde olduğu ve 2023 ile 2030 arasında yaklaşık %7,52'lik büüyüme ile 2030 yılına kadar yaklaşık 91,71 milyar ABD Doları büyüyeceği tahmin edilmektedir.

"En son araştırma çalışmasına göre, küresel Endüstriyel Güvenlik Sistemleri Pazar büyüklüğü ve gelir açısından payına yönelik talep 2022'de 51,52 milyar ABD Doları değerindeydi ve 2030 yılına kadar yıllık bileşik bir büyümeyle yaklaşık 91,71 milyar ABD Dolarını aşması bekleniyor. "

Endüstriyel Güvenlik Sistemleri Nelerdir? Endüstriyel Güvenlik Sistemleri Sektörü Ne Kadar Büyük?

Endüstriyel güvenlik sistemleri, bir endüstriyel tesisin fiziksel ve dijital varlıklarının güvenliğini sağlamayı amaçlayan bir dizi prosedür, teknoloji ve düzenlemedir. Birincil amaçları, tehdit aktörkerlerini caydırmak ve bu varlıkların zarar görmesini önlemektir. Varlıkların sabotaj, casusluk ve terörizm gibi çok çeşitli güvenlik risklerine karşı korunması, burada tartışılan sistem ve yöntemlerin birincil amacıdır.

Endüstriyel güvenlik sistemleri pazarının tanımına endüstriyel güvenlik sistemlerine bağlı çeşitli ürün ve hizmetlerin üretimi ve dağıtımı da dahildir. Yangın ve duman dedektörleri, alarm sistemleri, erişim kontrol sistemleri, gözetleme kameraları ve izinsiz giriş tespit sistemleri dahil olmak üzere bir dizi farklı teknolojiyi bünyesinde barındırır. Buna ek olarak, danışmanlık, tasarım, kurulum, bakım ve kullanım talimatını içeren yan hizmetleri de içerir. Ürünlerinin, verilerinin ve fiziksel varlıklarının güvenliğini sağlamak amacıyla çalışan işletmelerin ve endüstriyel birimlerin sayısındaki artışın bir sonucu olarak son zamanlarda bu tür endüstriyel güvenlik sistemlerine olan ihtiyaç artmaktadır.

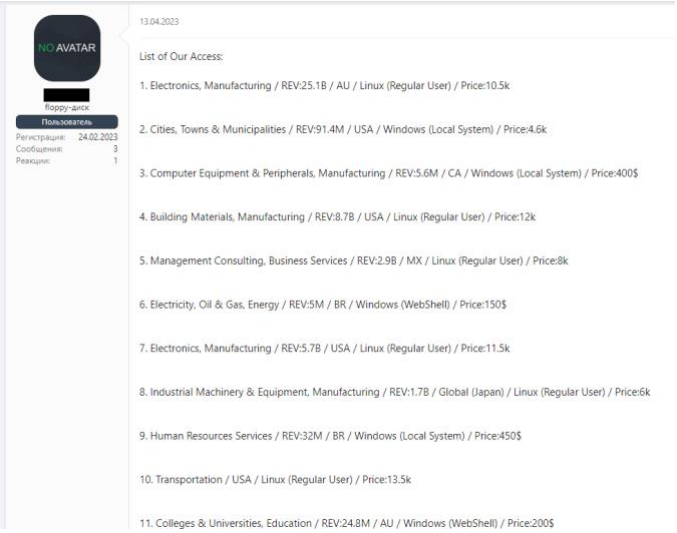
Endüstriyel Güvenlik Sistemleri Pazarı: Segmentasyon Analizi

Bölgesel yönetimlerin ulusal güvenliği korumak için çeşitli sistem ve teknolojilere yaptığı artan harcamalar, segmentin yüksek gelirinin ana itici gücüdür. Mevcut küresel siyasi durum muazzam bir değişim geçiriyor ve diğerlerinin yanı sıra Amerika Birleşik Devletleri, Çin, Tayvan, Japonya ve Kuzey Kore gibi ülkeler arasında çatışma olasılığına ilişkin endişelerde artış var. Sonuç olarak, güvenlik ihlallerinin önlenmesi amacıyla faaliyetlerin iyileştirilmesi ve güçlendirilmesi gerekliliği son zamanlarda yeni boyutlara ulaşmıştır.

TESPİT YERİ:
Sektör Haberleri

KAYNAK:
https://www.investorsobserver.com/news/qm-pr/7299798303530319

1.9. Enerji, İmalat ve Diğer Sektörlere Yönelik Erişim Satışı Duyuruları



Popüler Rus yeraltı forumunda bir ilk erişim aracısı (IAB) tarafından çeşitli sektörlere yönelik erişim satışı duyurusu gerçekleşmiştir.

Duyuru listesinde erişim satışı yapıldığı iddia edilen kuruluşa ait ülke, faaliyet sektörü, mali değer ve erişim tipi gibi unsurlara yer verilmiştir.

Erişim satışı duyurularında ülke ve faaliyet gösterilen sektöre yönelik veriler incelendiğinde, en çok hedef alınan sektörlerden biri imalat olurken, imalat sektöründe çoğunlukla ABD'nin hedef alınıyor olması dikkat çekmektedir. İlgili veri dikkate alındığında fidye yazılımı gruplarına ait hedef sektör – ülke sınıflandırmasında bir korelasyon olduğu görülmektedir. Bu da dolaylı olarak ilk erişim aracıları ile fidye yazılımı grupları arasındaki işbirliğini göstermektedir.

TESPİT YERİ:
Dark Web

KAYNAK:
hxxps[:]//xss[.]is/threads/86009/

24 Nisan 2023

1.10. Kuzey Koreli Bilgisayar Korsanları ABD ve Avrupa Enerji Sektörünü Hedefledi

Symantec Threat Hunter ekibine göre, kurumsal iletişim sağlayıcısı 3CX'in ağını tehlikeye atan X_Trader yazılım tedarik zinciri saldırısı, ABD ve Avrupa'daki birçok kritik altyapı kuruluşunu da etkiledi.

Trading Technologies ve 3CX'e yönelik saldırılarla bağlantılı olan Kuzey Kore destekli Lazarus Group, kurbanların sistemlerine çok aşamalı, modüler bir VEILEDSIGNAL arka kapısı yerleştirmek için trojanlaştırılmış bir X_Trader yazılım yükleyicisi kullandı.

Kötü amaçlı yazılım yüklendikten sonra kötü amaçlı kod çalıştırabiliyor ve Chrome, Firefox veya Edge işlemlerine bir C2 sunucu iletişim modülü enjekte edebiliyor. C2 modülü, adlandırılmış bir yöneltme oluşturmakta ve gelen mesajları dinleyerek bunları C2 sunucusuna göndermektedir.

Uzmanlar tarafından yapılan ilk soruşturma, kurbanlar arasında enerji sektöründeki isimsiz iki kritik altyapı kuruluşunun, biri ABD'de ve diğerinin Avrupa'da olduğunu ortaya çıkardı. Ayrıca 2 finans kurumu daha etkinlendiği duyuruldu.

Trading Technologies tedarik zinciri tavizi, finansal olarak motive edilmiş bir kampanyanın sonucu olsa da, Kuzey Kore destekli bilgisayar korsanı gruplarının siber casuslukla da tanındığı göz önüne alındığında, birkaç kritik altyapı kuruluşunun etkilenmesi bir endişe kaynağıdır. Bu saldırıdan etkilenen kuruluşların da sonraki sömürü için hedef alınması kuvvetle muhtemeldir.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securitylab.ru/news/537748.php

19 Nisan 2023

1.11. UK NCSC, Rus Gruplarının Kritik Ulusal Altyapıya Yıkıcı Saldırılar' Başlatabileceği Konusunda Uyardı

Birleşik Krallık'ın Ulusal Siber Güvenlik Merkezi (NCSC), kritik ulusal altyapı (CNI) kuruluşlarına, devlet bağlantılı gruplardan kaynaklanan yeni bir tehdide karşı uyarıda bulunan bir uyarı yayınladı. Tehdit, özellikle Rusya'nın Ukrayna'yı işgaline sempati duyan devlet yanlısı gruplardan geliyor ve son 18 ayda ortaya çıktığı belirtilmektedir. NCSC ayrıca, bazı grupların yıkıcı saldırılar başlatma niyetinde olduğunu belirttiğini ve CNI kuruluşlarının, savunmalarını güçlendirmek için NCSC'nin artırılmış tehdit kılavuzunda belirtilen adımları attıklarından emin olmaları gerektiğini belirtti.

"Son 18 ayda, yeni bir Rus siber düşman sınıfı ortaya çıktı. Bu devlet bağlantılı gruplar genellikle Rusya'nın işgaline sempati duyuyorlar ve finansal olarak değil ideolojik olarak motive oluyorlar" dedi. Bu gruplar, Rusya'nın algılanan çıkarlarıyla uyumlu olabilseler de, genellikle resmi devlet kontrolüne tabi değiller, bu nedenle eylemleri, geleneksel siber suç korsanlarına göre daha az kısıtlı ve daha geniş hedeflemeye sahip, bu da onları daha az tahmin edilebilir kılıyor.

Uyarı, bu grupların mali kazançla motive olmadıkları veya devletin kontrolüne tabi olmadıkları için eylemlerinin daha az tahmin edilebilir ve geleneksel siber suç aktörlerinden daha geniş hedef kitlesi olabileceğini ekledi.

Kısa vadede, gruplardan gelen herhangi bir faaliyetin Dağıtılmış Servis Dışı Bırakma (DDoS) saldırıları, web sitesi odaklı saldırılar veya yanlış bilgilerin yayılması şeklini alması muhtemel olsa da, bazı gruplar batılılara karşı daha yıkıcı bir etki elde etme arzusu içerisinde olduğunu dile getirdi.

NCSC kritik ulusal altyapıdan sorumlu müdür yardımcısı Dr. Marsha Quallo-Wright, *"Devlet bağlantılı bazı grupların CNI kuruluşlarına zarar verme niyetinde olduğu açık hale geldi ve sektörün bunun farkında olması önemlidir"* dedi. "Ortaya çıkan bu tehdidin ardından, CNI sektörlerine mesajımız, kendilerini korumak için şimdi mantıklı ve orantılı adımlar atmalarıdır. NCSC, siber tehdit arttığında atılması gereken adımlar konusunda kuruluşlara tavsiyelerde bulundu ve tüm CNI kuruluşlarının bunu şimdi takip etmesini şiddetle tavsiye ediyorum" dedi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/critical-infrastructure/russian-groups-could-launch-destructive-and-disruptive-attacks-on-critical-national-infrastructure-uk-ncsc-warns/

13 Nisan 2023

1.12. İsrail'deki Sulama Sistemleri, Endüstriyel Siber Saldırılar Sonucu Hacker Kesintiye Uğradı

Son zamanlarda İsrail'de sulama sistemleri, endüstriyel kontrol sistemlerini (EKS/ICS) hacklemenin ne kadar kolay olduğunu bir kez daha gösteren bir saldırıda kesintiye uğradı.

The Jerusalem Post, bilgisayar korsanlarının Ürdün Vadisi'ndeki çiftliklerdeki sulama sistemleri için su kontrol cihazlarını ve Galil Sewage Corporation'a ait atık su arıtma kontrol sistemlerini hedef aldığını bildirdi.

Çiftlikler olaydan önce İsrail Ulusal Siber Müdürlüğü tarafından uyarıldı ve yüksek siber saldırı riski nedeniyle bu sistemlere uzaktan bağlantıları devre dışı bırakmaları talimatı verildi. Ürdün Vadisi ve diğer bölgelerdeki yaklaşık bir düzine çiftlik bunu başaramadı ve su denetleyicileri siber saldırıya uğradı. Bu, otomatik sulama sistemlerinin geçici olarak devre dışı kalmasına yol açarak çiftçileri manuel sulamaya geçmeye zorladı.

.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/irrigation-systems-in-israel-disrupted-by-hacker-attacks-on-ics/

7 Nisan 2023

1.13. A.B.D. İç Güvenlik Komitesi, Deniz Limanlarında Faaliyet Gösteren Çin Vinçlerinin Getirdiği Tehditlerin Denetlenmesini İstiyor

ABD Temsilciler Meclisi İç Güvenlik Komitesi, geçtiğimiz ay ABD deniz limanlarında faaliyet gösteren Çin yapımı vinçlerin ticari, askeri ve endüstriyel operasyonlara yönelik siber güvenlik tehditleri hakkında İç Güvenlik Bakanlığı'ndan (DHS) yanıt istedi. Üyeler şimdi bu vinçlerin ABD limanlarında oluşturduğu tehditler hakkında denetim yapılması çağrısında bulundu.

Tennessee'den bir Cumhuriyetçi olan Mark E. Green ve House Committee, *"Bu endişeleri ele almak için, İç Güvenlik Komitesi, ülkemizin deniz limanlarındaki güvenlik açıklarını ve İç Güvenlik Bakanlığı'nın (DHS) dayanıklılık stratejilerini denetliyor"* dedi. İç Güvenlik Başkanı, New York'tan bir Cumhuriyetçi ve Siber Güvenlik ve Altyapı Koruma Alt Komitesi Başkanı Andrew Garbarino, Florida'dan bir Cumhuriyetçi ve Ulaştırma ve Deniz Güvenliği Alt Komitesi Başkanı Carlos Gimenez ve Kuzey Carolina'dan bir Cumhuriyetçi ve Gözetim Alt Komitesi Başkanı Dan Bishop, Soruşturmalar ve Sorumluluk Başkanı, bu hafta DHS Sekreteri Alejandro Mayorkas'a bir mektup yazdı.

"Bildiğiniz gibi DHS, ülkemizin liman güvenliği ve siber güvenliğinden sorumlu başlıca federal kurumdur. Amerika'nın tedarik zinciri ve ekonomik güvenliği, büyük ölçüde, yılda 5,4 trilyon dolar değerinde ticari ve askeri malın taşınmasına yardımcı olan deniz limanlarına bağlıdır."

Mektup, Kasım 2022'de iki meclisli bir grup üye tarafından ABD Başkanı Joe Biden'a gönderilen ve Çin'in ülkenin limanlarında oluşturduğu tehditlere karşı harekete geçilmesi ve kararlı bir yanıt verilmesi çağrısında bulunan bir mektubu takip ediyor. *"Bu çağrıyı yeniliyoruz. Diğer sorunların yanı sıra, ZPMC olarak da bilinen Shanghai Zhenhua Heavy Industries Co. tarafından üretilen Çin yapımı vinçlerin ABD limanlarının yüzde 80'inde kullanılmasını rahatsız edici buluyoruz."*

Gemiden kıyıya vinçler, deniz limanı operasyonlarında ve ABD ticari ve askeri tedarik zincirlerinde kritik bir rol oynamaktadır. Geçen ay Wall Street Journal'da bildirildiği üzere, ABD limanlarında kullanılan vinçlerin kabaca yüzde 80'i, China Communications Construction Co.'nun bir yan kuruluşu olan Çinli şirket Shanghai Zhenhua Heavy Industries Co. (ZPMC) tarafından üretiliyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/transport/homeland-security-committee-seeks-audit-of-threats-brought-by-chinese-cranes-operating-at-maritime-ports/

10 Nisan 2023

1.14. KELA, 2023'ün İlk Çeyreğinde Fidye Yazılımı ve Veri Sızıntısı Aktörlerinin En Çok Hedef Aldığı Üretim ve Endüstriyel Sektörleri Bildirdi

Siber suç tehdit istihbaratı firması KELA, imalat ve sanayi sektörlerinin bu yılın ilk çeyreğinde fidye yazılımı saldırganları ve veri sızıntısı aktörleri tarafından en çok hedef alındığını açıkladı. ***LockBit , Royal ve Alphv*** bu sektördeki saldırıların yüzde 50'sinden fazlasının arkasındayken, fidye yazılımı ve şantaj saldırılarının yüzde 45'ini kaydeden ABD hâlâ en çok hedef alınan ülke.

KELA: *'Fidye yazılım çetelerinin tedarik zincirinin önemli bir parçası olan ağ erişimi satışlarında ve fidye yazılım saldırılarında da bu yılın ilk çeyreğinde 2022'nin ortalama metriklerine göre artış gözlemledi'*

"2023'ün ilk çeyreğindeki en üretken fidye yazılımı ve veri sızıntısı aktörleri ***LockBit, Clop, Alphv, Royal ve Black Basta*** idi. Clop, çetenin iddia ettiği gibi, Fortra GoAnywhere MFT sistemindeki sıfırıncı gün güvenlik açığından (CVE-2023-0669) yararlanarak 130 kurbanı hedef alan en üretken ilk beş çete arasında yer aldı."

Fidye yazılımı saldırılarının sayısı, bu yılın ilk çeyreğinde, geçen yılın ilk çeyreğindeki ortalama sayıya kıyasla %30 artarak yaklaşık 900 kurbana ulaştı.

KELA, bu yılın ilk çeyreğinde en üretken fidye yazılımı ve veri sızıntısı aktörlerinin LockBit , Clop, Alphv (namı diğer BlackCat) , Royal ve Black Basta olduğunu ve her grup tarafından açıklanan yaklaşık 45 ila 270 kurban olduğunu açıkladı. LockBit, en aktif ikinci grup olan Clop'tan neredeyse 2,5 kat daha fazla olan 265'in üzerinde kurbanla ilk konumunu korudu. Ancak Mart 2023'te Clop hızı artırdı ve 100 kurban olduğunu iddia ederek LockBit'ten daha fazla saldırı ifşa etti. Zirvedeki çetelerden biri olan Alphv, kısa bir süre önce RAMP forumunda fidye yazılımlarının 'BlackCat 2.0: Sphynx' adlı yeni bir versiyonunun çıktığını duyurmuştu.

Ek olarak Clop ve Royal, 2022'de bu grupta yer almayarak en üretken ilk beş çete arasına girdiler. Görünüşe göre FBI operasyonunu durdurmadan önce en iyi gruplardan biri olan Hive'ın yerini aldılar.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/reports/kela-reports-manufacturing-industrial-sectors-most-targeted-by-ransomware-data-leak-actors-during-q1-2023/

2. FİDYE YAZILIMI SALDIRILARI

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

Enerji sektörü özelinde, en çok hedeflenen ülke **ABD** olurken bu sektörü en çok hedefleyen grup **Lockbit** olmuştur.

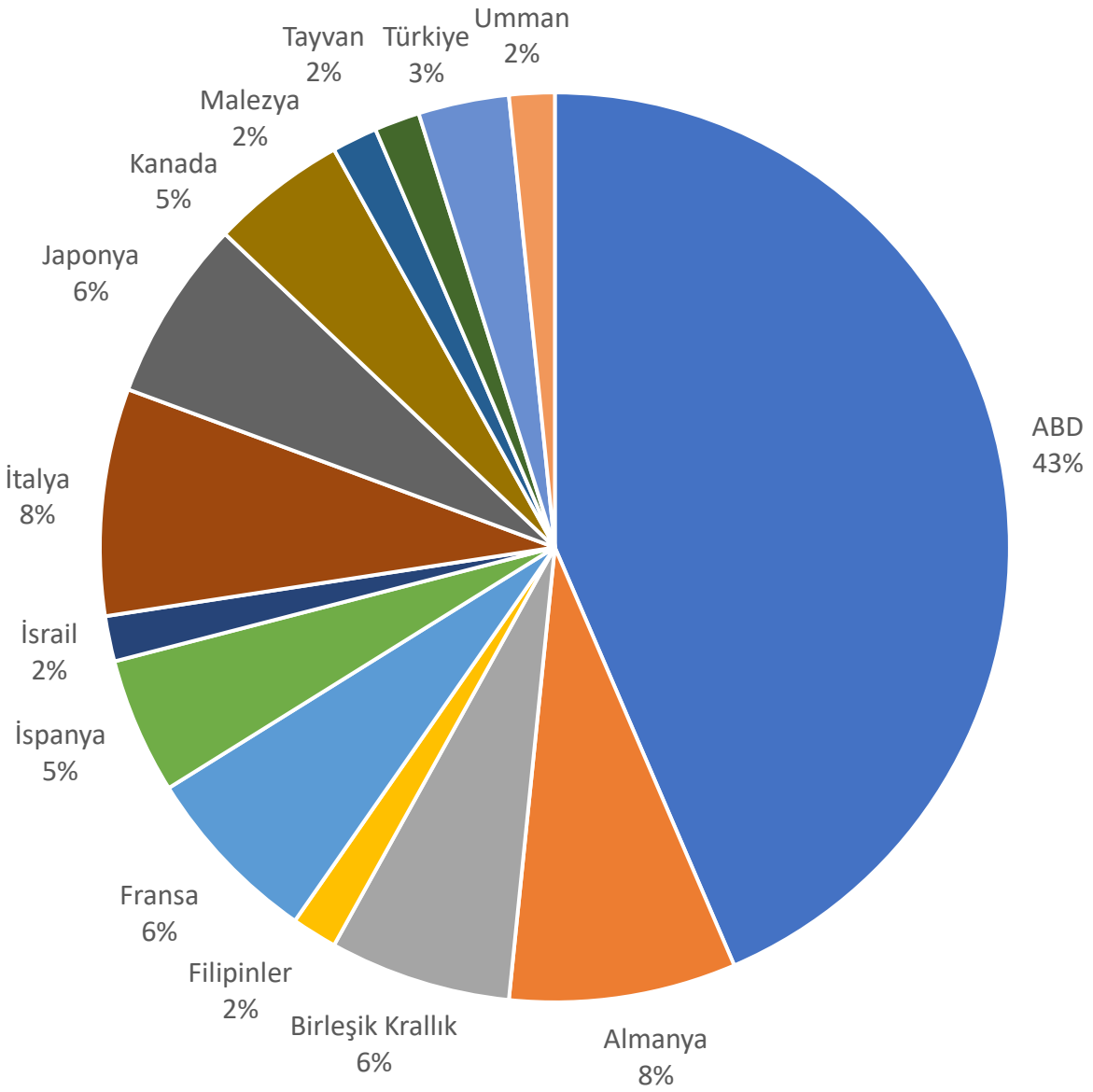
Grup	Hedef Sektör	Hedef Ülke
alphv	Enerji	ABD
lockbit3	Enerji	Güney Kore
lockbit3	Petrol ve Enerji	Brezilya
lockbit3	Enerji ve Altyapı	Kanada
play	Akaryakıt Dağıtımı	İrlanda
unsafeleak	Enerji	ABD
bianlian	Enerji	Kanada
bianlian	Enerji	ABD
lockbit3	Yenilenebilir Enerji	Malezya

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

Grup	%
Lockbit	34
Royal	15
Alphv	11
Bianlian	8
Blackbasta	6
Ransomhouse	3
Trigona	3
Medusa	3
Karakurt	3
Moneymessage	3
Blackbyte	2
Dunghill_leak	2
Unsafeleak	2
Diğer	5

Fidye yazılımı grupları Türkiye'de en çok imalat sektörünü hedef almışlardır. Türkiye özelinde, imalat sektörünü en çok hedef alan fidye yazılımı grubu 'Lockbit' olmuştur.

İmalat sektöründe Nisan ayında en çok hedef alınan ülkelere ait dağılım aşağıdaki grafikte izlenime sunulmuştur.



CYBER WISE | ICSFUSION

Endüstriyel Tesislere Yönelik

Saldırı Bilgilendirme Raporu

icsfusion.com