CYBER WISE | ICSFUSION

Endüstriyel Tesislere Yönelik

Saldırı Bilgilendirme Raporu

Mart 2023

icsfusion.com

ICSFUSION

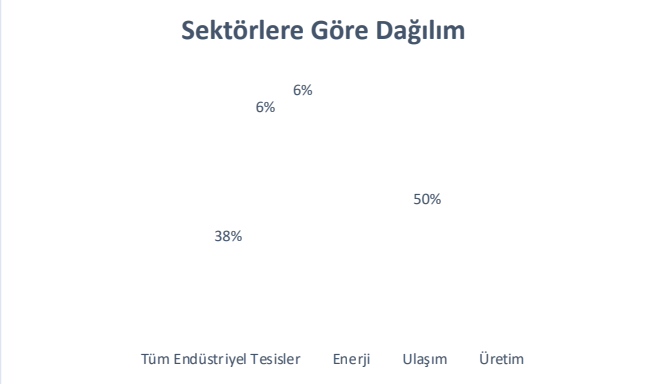
İÇİNDEKİLER

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.

Mart ayı raporu, Mart ayında incelenen verilerden derlenen 17 farklı konuyu kapsamaktadır. Bu konuların %31'i saldırılarla ilgili haberler, %44'ü raporlar/rehberler ve %25'i güvenlik açıklarıyla ilgilidir.

Rapor konuları sektörlere göre ayrıldığında, raporda "tüm"endüstriyel tesisler ile ilgili konular %50 oranında ulaşırken, enerji sektörü ile ilgili konulara %38 oranında yer almaktadır.

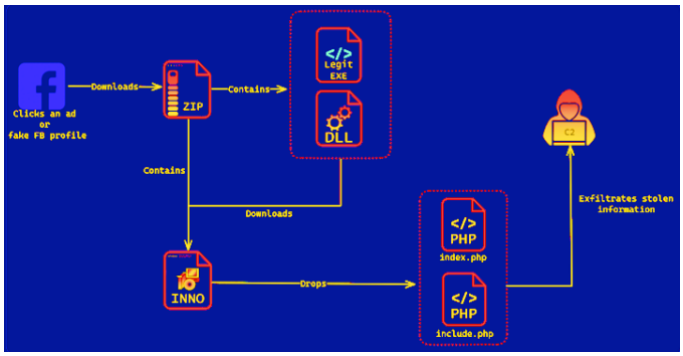


Ayrıca Mart ayı raporunda, Mart ayında gerçekleşen 400'ün üzerindeki fidye yazılımı vakası incelenmiş, sektöre yönelik gözlemler raporda incelemenize sunulmuştur.

7 Mart 2023

1. HABERLER

1.1. SYS01stealer: Kritik Altyapı Firmalarını Hedeflemek İçin Facebook Reklamlarını Kullanan Yeni Tehdit



Siber güvenlik araştırmacıları, Kasım 2022'den bu yana kritik devlet altyapısı çalışanlarını, üretim şirketlerini ve diğer endüstriyel sektörleri hedefleyen SYS01stealer adlı yeni bir zararlı keşfetti.

Morphisec ilgili raporda , "Kampanyanın arkasındaki tehdit aktörleri, kurbanları kötü amaçlı bir dosya indirmeye ikna etmek için oyunlar, yetişkinlere uygun içerik ve crackli yazılımlar gibi bileşenleri tanıtan Google reklamlarını ve sahte Facebook profillerini kullanarak Facebook işletme hesaplarını hedefliyor" dedi.

"Saldırı, oturum bilgileri, gibi hassas bilgileri çalmak için tasarlanmış."

İsrailli siber güvenlik şirketi, kampanyanın başlangıçta Zscaler tarafından Ducktail adlı mali amaçlı bir siber suç operasyonuna bağlı olduğunu belirtmişti.

Bununla birlikte, DuckTail etkinlik kümesini ilk olarak Temmuz 2022'de belgeleyen WithSecure, iki izinsiz giriş setinin birbirinden farklı olduğunu söyleyerek, tehdit aktörlerinin ilişkilendirme çabalarını nasıl karıştırıp tespitten kaçmayı başardığını gösteriyor.

Morphisec'e göre saldırı zinciri, bir kurbanın sahte bir Facebook profilinden veya reklamından bir URL'ye tıklaması ve crackli yazılım veya yetişkin temalı içerik olduğu iddia edilen bir ZIP arşivini indirmesi için ikna edilmesiyle başlamaktadır.

Zararlı, Chromium tabanlı web tarayıcılarından (ör. Google Chrome, Microsoft Edge, Brave, Opera ve Vivaldi) Facebook çerezlerini toplamak, kurbanın Facebook bilgilerini uzak bir sunucuya sızdırmak ve rasgele dosyaları indirip çalıştırmak için tasarlanmış durumdadır.

Ayrıca, zararlı buluşmış ana bilgisayardan komuta ve kontrol (C2) sunucusuna dosya yüklemek, sunucu tarafından gönderilen komutları çalıştırmak ve yeni bir sürüm çıktığında kendini güncellemek için de donatılmıştır.

Gelişme, Bitdefender'ın, kullanıcıların Facebook ve YouTube hesaplarını ele geçirmek ve kripto para madenciliği yapmak için ele geçirilmiş sistemlerden yararlanmak için tasarlanmış S1deload olarak bilinen benzer bir zararlı kampanyasını ortaya çıkarmasıyla netlik kazandı.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://thehackernews.com/2023/03/sys01stealer-new-threat-using-facebook.html

9 Mart 2023

ICSFUSION

1.2. Etkili ICS/OT Güvenliğinin 5 Kritik Bileşeni

Bu yazıda ele alından kontroller ve süreçler, kritik altyapı kuruluşlarının kendi risk profillerine göre uyarlanmış bir ICS güvenlik programı oluşturmasına yardımcı olabilir.

Endüstriyel kontrol sistemi (EKS/ICS) saldırı yüzeyinin hızla genişlemesi yeni bir konu değildir. Altyapıların hızla dijitalleşmesi, IT-OT yakınsaması ve Nesnelerin İnterneti (IoT) yaygın kullanımı, artan jeopolitik gerilimlerin dalgalı etkilerine kadar, kritik altyapı sektörlerindeki kuruluşlar, uzun süreli devre dışı kalmaya dahi neden olabilecek ivmesi sürekli artan endüstriyel saldırılara dirençli olacak şekilde konumlandırılmalıdır. Mevcut riskler olarak hali hazırda insanları ve toplulukları ciddi şekilde tehdit etmektedir.

EKS/ICS tehditleri doğası gereği farklılıklar taşımaktadır. Temel olarak parasal kazanç veya veri hırsızlığına dayanan kurumsal BT ağlarına yönelik geleneksel saldırıların aksine, devlet destekli saldırganlar genellikle operasyonları kesintiye uğratmak, fiziksel hasara yol açmak ve hatta can kaybına yol açan yıkıcı olayları kolaylaştırmak gibi kötü niyetli amaçlarla kritik altyapı sistemlerini hedefleyebilmektedir.

Endüstriyel tesislere saldırılar masal ya da kurgu değil artık gerçek. Şubat ayı başlarında, ABD Temsilciler Meclisi alt komitesinin liderleri, ABD Enerji Bakanlığı'nı geçen yaz Rus bilgisayar korsanlığı grubu Cold River tarafından hedef alınan üç nükleer araştırma laboratuvarı hakkında bilgi vermeye çağırdı. Ya da 2016 yılında Rus devlet destekli Crashoverride olayını ele alalım. Sonuç olarak, Ukrayna'nın başkenti Kiev'in bir kısmı gece boyunca bir saatlik bir elektrik kesintisi yaşamıştı.

Etkili ICS/OT Güvenliğinin Beş Bileşeni

Aşağıdaki beş kritik kontrolü kapsayan bir ICS/OT güvenlik çerçevesini benimsemek, bu dengeyi sağlamanın anahtarıdır.

1- Endüstriyel siber güvenlik olaylarının yönetimi
2- Katmanlı ve savunulabilir mimari
3- Endüstriyel ağ ve güvenlik görünürlüğü
4- Uzak erişim güvenliği
5- Risk bazlı zafiyet yönetimi

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/5-critical-components-of-effective-ics-ot-security-

13 Mart 2023

1.3. CISA Şimdi Kritik Altyapıyı Fidye Yazılımına Karşı Savunmasız Cihazlar Konusunda Uyarıyor

Mart ayında, ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), kritik altyapı kuruluşlarının bilgi sistemlerini fidye yazılımı saldırılarına karşı korumalarına yardımcı olacak yeni bir pilot programı duyurdu.

Siber güvenlik ajansı, *"30 Ocak 2023'te başlayan Fidye Yazılımı Güvenlik Açığı Uyarı Pilotu (RVWP) aracılığıyla, CISA, kritik altyapı kuruluşlarını, sistemlerinin fidye yazılımı tehdit aktörleri tarafından kullanılabilecek güvenlik açıklarına maruz kalabilme durumu konusunda uyarmak için yeni bir çaba harcıyor"* dedi.

CISA'nın yeni kurulan Fidye Yazılımı Güvenlik Açığı Uyarı Pilotu (RVWP) programının iki hedefi bulunuyor: kritik altyapı varlıklarının ağlarını, fidye yazılımı saldırganlarının genellikle ağları ihlal etmek için kullandıkları güvenlik açıklarına sahip İnternet'e açık olan sistemleri taramak ve savunmasız kuruluşların, saldırıya uğramadan önce kusurları düzeltmesine yardımcı olmak.

Siber güvenlik ajansı, *"RVWP'nin bir parçası olarak CISA, genellikle fidye yazılımı saldırılarıyla ilişkilendirilen güvenlik açıklarını içeren bilgi sistemlerini proaktif olarak belirlemek için mevcut yetkililerden ve teknolojiden yararlanır"* dedi.

"CISA, etkilenen bu sistemleri tespit ettikten sonra, bölgesel siber güvenlik personelimiz sistem sahiplerini güvenlik açıkları konusunda bilgilendirir ve böylece zararlı izinsiz girişler meydana gelmeden önce zamanında önlem alınması sağlanır."

Bu, Colonial Pipeline, Kaseya ve JBS Foods ağlarına enfekte olarak fidye yazılımı saldırılarıyla başlayan, kritik altyapı kuruluşlarını ve ABD devlet kurumlarını hedef alan bir dizi siber saldırının ardından neredeyse iki yıl önce başlayan ve giderek artan fidye yazılımı tehdidini savuşturmak için daha geniş bir çalışmasının parçasıdır.

Haziran 2021'de ajans, Siber Güvenlik Değerlendirme Aracı (CSET) için yeni bir modül olan Fidye Yazılımına Hazırlık Değerlendirmesini (RRA) yayınladı .

RRA, kuruluşların fidye yazılımı saldırılarını önleme ve kurtarmaya hazır olma durumlarını değerlendirmelerine yardımcı olur ve farklı siber güvenlik olgunluk düzeyleri için özelleştirilebilir.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.bleepingcomputer.com/news/security/cisa-now-warns-critical-infrastructure-of-ransomware-vulnerable-devices/

20 Mart 2023

1.4. Biden'ın PCAST Kuruluşu, Siber-Fiziksel Dayanıklılık Üzerinde Çalışmak ve Kritik Altyapıyı Güçlendirmek İçin Çalışma Grubu Kurdu

A.B.D. Başkanının Bilim ve Teknoloji Danışma Konseyi (PCAST) geçen hafta kamu, özel sektör ve akademiden, danışman ve uzmanlardan oluşan siber-fiziksel dayanıklılık üzerine bir çalışma grubu kurulduğunu duyurdu. Çalışma grubu, kritik altyapılar arasında güven oluşturmak için çalışacak birkaç PCAST üyesinden ve diğer uzmanlardan oluşacağı belirtilmektedir.

Yaklaşık olarak önümüzdeki altı ay boyunca grup, başkana öneriler formüle etmek için çok sayıda kuruluşa ve uzmana danışacak. Çalışma Grubu'nun eş başkanları ve üyeleri, Beyaz Saray'daki bir blog yazısında şunları yazdı: *"Katılımımız, NIST, MITRE, DARPA ve DHS gibi kuruluşlardaki siber dayanıklılık konusundaki liderleri içerecektir."* Mevcut Çalışma Grubu eş liderleri Eric Horvitz ve Phil Venables, Çalışma Grubu üyeleri ise Jon Levin, Bill Press, Vicki Sato, Lisa Su ve Kathy Sullivan oluşmaktadır.

PCAST, Başkan'a ve Beyaz Saray'a bilim, teknoloji ve yenilik politikası tavsiyelerinde bulunmakla görevli, federal hükümet dışından gelen tek danışman kuruluştur. Yürütme Emri tarafından kurulan, çeşitli bakış açıları ve uzmanlıklara sahip endüstri, akademi ve kar amacı gütmeyen kuruluşlardan bireylerden oluşan bağımsız bir Federal Danışma Komitesidir. PCAST ayrıca bilim, teknoloji ve inovasyon politikası ile bilimsel ve teknolojik bilgileri içeren konularda Başkan için kanıta dayalı öneriler geliştirir.

PCAST kuruluşu, Ulusal Bilimler, Mühendislik ve Tıp Akademilerinin seçilmiş 20 üyesi, dört MacArthur 'Genius' Üyesi, iki eski Kabine sekreteri ve iki Nobel ödüllü dahil olmak üzere 30 üyeden oluşur. Üyeleri arasında astrofizik ve tarım, biyokimya ve bilgisayar mühendisliği, ekoloji ve girişimcilik, immünoloji ve nanoteknoloji, nörobilim ve ulusal güvenlik, sosyal bilimler ve siber güvenlik ve daha pek çok alanda uzman bulunmaktadır.

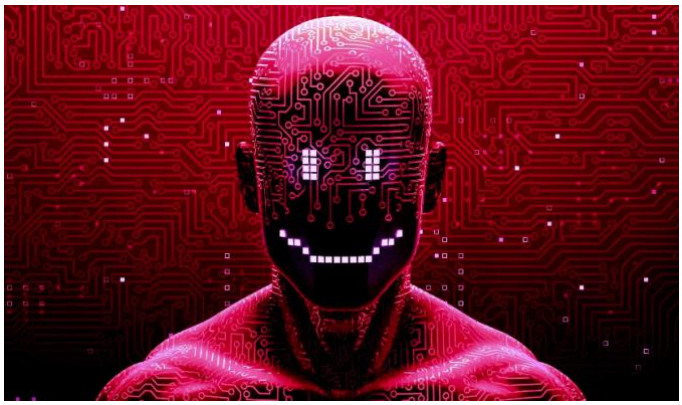
En son gönderi, *"birçok farklı alandan, muhtemelen doğrudan danışabileceğimizden daha fazla insanın bu çalışmaya katkıda bulunmak için değerli bakış açılarına sahip olabileceğini kabul ediyor. Bunlar, siber-fiziksel dayanıklılığımızı geliştirebileceğini düşündüğünüz yeni fikirler, mevcut fikirler, yöntemler veya projeler şeklinde olabilir. Hatta dayanıklılığımızı azaltan mevcut uygulamaları kaldırma veya düzenleme biçimini bile olabilir. Sunumların kısa ve öz olmasını ve özel mülkiyete tabi olmamasını veya kamuya ifşa için uygunsuz olmasını memnuniyetle karşılıyoruz"* dedi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/cisa/bidens-pcast-body-sets-up-working-group-to-work-on-cyber-physical-resilience-strengthen-critical-infrastructure/

14 Mart 2023

1.5. YoroTrooper Siber Casusları, BDT Enerji Kuruluşlarını ve AB Büyükelçiliklerini Hedef Alıyor



"YoroTrooper" adlı yeni bir tehdit aktörü, en az Haziran 2022'den beri Bağımsız Devletler Topluluğu (BDT) ülkelerindeki hükümet ve enerji kuruluşlarını hedef alan siber casusluk kampanyaları yürütüyor.

Cisco Talos'a göre, tehdit aktörü sağlık hizmetleriyle uğraşan kritik bir Avrupa Birliği ajansının, Dünya Fikri Mülkiyet Örgütü'nün (WIPO) ve çeşitli Avrupa büyükelçiliklerinin hesaplarını ele geçirdi.

YoroTrooper'ın araçları, emtia ve özel bilgi hırsızları, uzaktan erişim truva atları ve Python tabanlı kötü amaçlı yazılımların bir kombinasyonunu içermektedir. Bulaşma, kötü amaçlı LNK ekleri ve aldatıcı PDF belgeleri içeren kimlik avı e-postaları yoluyla gerçekleşmektedir.

Cisco Talos, YoroTrooper'ın hesap kimlik bilgileri, tanımlama bilgileri ve tarama geçmişleri dahil olmak üzere virüslü uç noktalardan büyük hacimli verileri sızdırdığına dair kanıtlara sahip olduğunu bildirdi.

YoroTrooper, PoetRAT ve LodaRAT gibi diğer tehdit aktörleriyle ilişkili kötü amaçlı yazılım kullanırken, Cisco analistleri bunun yeni bir faaliyet kümesi olduğuna inanmak için yeterli göstergeye sahip.

Hedeflenen BDT Ülkeleri

2022 yazında YoroTrooper, Belarus veya Rus varlıkları gibi davranan e-posta etki alanlarından gönderilen bozuk PDF dosyalarını kullanarak Belarus varlıklarını hedef aldı.

Eylül 2022'de grup, Rus devlet kurumlarını taklit eden birkaç yazım hatası alan adı kaydetti ve .NET tabanlı implantların VHDX tabanlı dağıtımını denedi.

Yıl sonuna kadar takip eden aylarda siber casuslar, 'Stink Stealer' adlı Python tabanlı özel bir implant yerleştirerek odak noktalarını Belarus ve Azerbaycan'a kaydırdılar.

2023'te tehdit aktörleri, hedefin sistemine tuzak belgeler ve implantlar indirmek için HTA'yı kullandı ve Tacikistan ve Özbekistan hükümetine karşı özel bir Python zararlısı konuşlandırdı.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.bleepingcomputer.com/news/security/yorotrooper-cyberspies-target-cis-energy-orgs-eu-embassies/

17 Mart 2023

1.6. Hitachi Energy, Clop GoAnywhere Saldırılarının Ardından Veri İhlalini Doğruladı

Hitachi Energy, Clop fidye yazılımı çetesinin bir GoAnywaywhere sıfır gün güvenlik açığı kullanarak verileri çalmasının ardından bir veri ihlaline maruz kaldığını doğruladı.

Hitachi Energy, Japon mühendislik ve teknoloji devi Hitachi'nin enerji çözümleri ve güç sistemlerine odaklanan bir departmanıdır. Yıllık geliri 10 milyar dolardır.

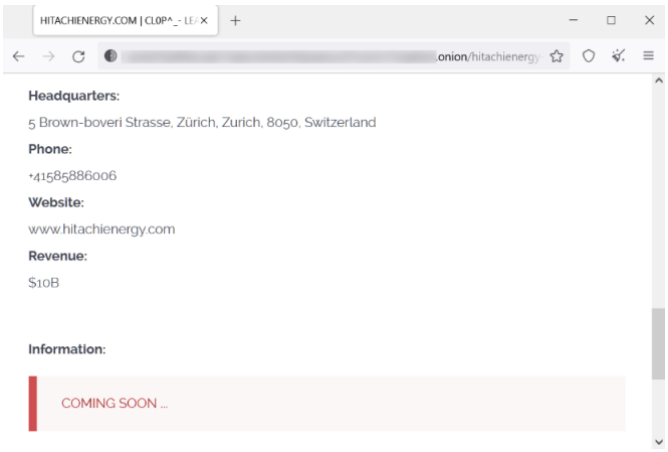
Saldırı, ilk olarak 3 Şubat 2023'te açıklanan ve şimdi CVE-2023-0669 olarak izlenen Fortra GoAnywhere MFT'deki (Yönetilen Dosya Aktarımı) sıfırıncı gün güvenlik açığından yararlanılarak gerçekleştirildi.

Hitachi, *"Kısa bir süre önce FORTRA GoAnywhere MFT (Yönetilen Dosya Aktarımı) adlı bir üçüncü taraf yazılım sağlayıcısının, CLOP fidye yazılımı grubu tarafından gerçekleştirilen ve bazı ülkelerde çalışan verilerine yetkisiz erişimle sonuçlanabilecek bir saldırının kurbanı olduğunu öğrendik"* dedi.

Firma, olaya hemen müdahale ettiğini, etkilenen sistemin (GoAnywhere MFT) bağlantısını kestiğini ve ihlalin etkisini belirlemek için dahili bir soruşturma başlattığını söylüyor.

Etkilenen tüm çalışanlar, geçerli veri koruma yetkilileri ve kolluk kuvvetleri, güvenlik olayı hakkında doğrudan Hitachi tarafından bilgilendirildi.

Firmanın yaptığı açıklamada, *"Bugüne kadar, ne ağ operasyonlarımızın ne de müşteri verilerinin güvenliğinin veya güvenilirliğinin tehlikeye atıldığına dair hiçbir bilgimiz yok."*



Görsel1: Clop fidye yazılımının Hitachi'ye yönelik yaptığı duyuru paylaşımı.

Etki Şekillenmeye Başlıyor

Fortra, Şubat ayının başında GoAnywhere güvenli dosya paylaşım ürünü için sıfır gün açık olduğunu kabul ettiğinde, BleepignComputer bunun 2021'de benzer bir ürün olan Accellion FTA'yı hedef alan önceki saldırılara benzer bir etkiye sahip olabileceğini tahmin etti.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.bleepingcomputer.com/news/security/hitachi-energy-confirms-data-breach-after-clop-goanywhere-attacks/

24 Mart 2023

1.7. ABD Senatosu Enerji Komitesi, Enerji Altyapısının Kritik Bileşenlerine Yönelik Siber Güvenlik Risklerini Ele Alıyor

ABD Senatosu Enerji ve Doğal Kaynaklar Komitesi, Perşembe günü ülkenin enerji altyapısına yönelik siber güvenlik açıklarını incelemek için tam bir komite toplantısı düzenledi. Komite ayrıca, enerji kaynaklarının ülkenin dostlarına ve müttefiklerine karşı jeopolitik bir silah olarak kullanıldığını ve düşmanlarının enerji güvenliğini ve ekonomiyi kötü yönde etkilemek için Amerikan altyapısına sızmak için siber saldırıları giderek daha fazla kullanmaya başladığını belirtti.

Duruşmanın tanıkları arasında ABD Enerji Bakanlığı'nın (DOE) Siber Güvenlik, Enerji Güvenliği ve Acil Müdahale Ofisi (CESER) Direktörü Puesh M. Kumar, bir endüstriyel siber güvenlik şirketinin CEO'su ve kurucu ortağı Robert M. Lee yer aldı.

Başkan Senatör Joe Manchin, *"Hızla değişen siber tehdit ortamı, eğrinin ilerisinde olmamızı ve ulusal güvenliğimiz, kamu sağlığı ve güvenliğimiz ve ekonomimizin zararına hazırlıksız yakalanmamamızı sağlamak için sürekli federal dikkat ve stratejik dayanıklılık gerektirecek"* dedi. *"Hükümetimiz son on yılda federal koordinasyonu geliştirmek, araştırma ve geliştirmeye yönelik fonları artırmak, istihbarat yayılımını geliştirmek ve mevcut kamu-özel sektör ortaklıklarını geliştirmek için önemli adımlar attı."*

Tehdit ortamını ele alan Senatör Manchin, siber tehditlerin bireysel kötü aktörlere, ulusötesi organize suçlara, devlet destekli gruplara ve uluslara atfedilebileceğini söyledi. *"Ulusal İstihbarat Dairesi Başkanlığı'nın 2022 Yıllık Tehdit Değerlendirmesi, Çin'i ABD Hükümeti ve özel sektör ağlarına yönelik en geniş ve en aktif siber tehdit olarak değerlendirdi. Buna ek olarak, değerlendirme Rusya'yı özellikle kritik altyapımızı hedeflemeye odaklanan en büyük siber tehdit olarak tanımlıyor"* dedi.

"Rusya'nın 2015'te Ukrayna'nın elektrik şebekesini devre dışı bırakan siber saldırısı, elektrik şebekesi gibi kritik altyapıya yönelik büyük ölçekli siber saldırı olasılığına karşı bir uyandırma çağrısıydı" diye ekledi. *"Putin'in Ukrayna'daki acımasız saldırganlığı, Rusya'nın Ukrayna'nın müttefiklerine karşı Ukrayna'ya silah ve yardım göndermeye misilleme olarak siber saldırıları kullanmak gibi aşırı ve tehlikeli taktiklere giderek daha fazla bel bağlaması olasılığını artırdı."*

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/utilities-energy-power-water-waste/us-senate-energy-committee-addresses-cybersecurity-risks-to-critical-parts-of-energy-infrastructure/

24 Mart 2023

1.8. 'Bitter' Casus Bilgisayar Korsanları Çin Nükleer Enerji Kuruluşlarını Hedef Alıyor

'Bitter APT' olarak izlenen bir siber casusluk korsanlığı grubunun yakın zamanda, cihazlara kötü amaçlı yazılım indiricileri bulaştırmak için kimlik avı e-postaları kullanarak Çin nükleer enerji endüstrisini hedef aldığı görüldü.

Bitter, Asya-Pasifik bölgesindeki enerji, mühendislik ve devlet sektörlerindeki yüksek profilli kuruluşları hedef aldığı bilinen Güney Asyalı olduğundan şüphelenilen bir bilgisayar korsanlığı grubudur.

Mayıs 2022'de Bitter APT'nin, Güneydoğu Asya'daki hedeflere 'ZxxZ' adlı bir truva atı yüklemek için kötü amaçlı XLSX belge ekleriyle hedef odaklı kimlik avı e-postaları kullandığı tespit edildi.

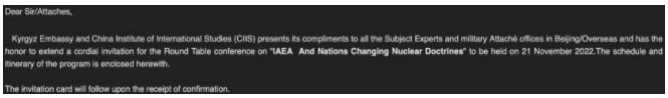
Ağustos 2022'de Meta, Bitter APT'nin Yeni Zelanda, Hindistan, Pakistan ve Birleşik Krallık'taki kullanıcılara karşı 'Dracarys' adlı yeni bir Android casus yazılım aracı kullandığını bildirdi.

Bu bilgisayar korsanlığı kampanyası, aynı tehdit aktörünün geçmiş kampanyalarıyla eşleşen gözlemlenen TTP'lere (taktikler, teknikler ve prosedürler) dayalı olarak bunu Bitter APT'ye bağlayan Intezer'deki tehdit analistleri tarafından keşfedildi.

Çin'in Nükleer Alanını Hedef Alıyor

Bitter, Intezer tarafından bulunan yeni kampanyada, Kırgızistan'ın Pekin'deki Büyükelçiliğinden geliyormuş gibi davranarak çeşitli Çinli nükleer enerji şirketlerine ve bu alanla ilgili akademisyenlere e-postalar gönderiyor.

E-posta, Kırgız Büyükelçiliği, Uluslararası Atom Enerjisi Kurumu (IAEA) ve Çin Uluslararası Çalışmalar Enstitüsü (CIIS) tarafından sözde düzenlenen nükleer enerji konulu bir konferansa davet gibi görünüyor.


Dear Sir/Attaches,

Kyrgyz Embassy and China Institute of International Studies (CIIS) presents its compliments to all the Subject Experts and military Attaché offices in Beijing/Overseas and has the honor to extend a cordial invitation for the Round Table conference on "**IAEA And Nations Changing Nuclear Doctrines**" to be held on 21 November 2022.The schedule and itinerary of the program is enclosed herewith.

The invitation card will follow upon the receipt of confirmation.

Görsel2: Kimlik avı e-posta içeriği.

E-postayı imzalayan isim gerçektir, Kırgızistan Dışişleri Bakanlığı yetkilisine aittir ve Bitter APT'nin iletişimlerine meşruiyet katmaya yardımcı olan ayrıntılara gösterdiği özeni göstermektedir.

Alıcılardan, konferans için bir davetiye kartı içerdiği varsayılan ancak gerçekte Microsoft Derlenmiş HTML Yardım dosyası (CHM) veya kötü amaçlı bir Excel belgesi içeren e-postanın RAR ekini indirmeleri istenir.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.bleepingcomputer.com/news/security/bitter-espionage-hackers-target-chinese-nuclear-energy-orgs/
https://www.binarydefense.com/threat_watch/bitter-apt-targeting-chinese-nuclear-energy-organizations/

7 Mart 2023

1.9. Bitrix CMS Güvenlik Açığının Sömürülmesi Rusya'da EKS Saldırılarında Artışa Neden Oluyor

Kaspersky, Rusya'daki EKS/ICS bilgisayarlarına yönelik saldırılarda bir artış gördüğünü raporladı ve bunu CVE-2022-27228 olarak izlenen bir Bitrix CMS güvenlik açığının kötüye kullanılmasıyla ilişkilendiriyor.

Siber güvenlik firması Pazartesi günü, 2022'nin ikinci yarısına odaklanan güncel EKS tehdit bilgilendirme raporunu yayınladı. Şirket, 2022'de ürünleri tarafından korunan küresel cihazların %40,6'sındaki tehditleri engellediğini söyledi; bu, 2021'e kıyasla hafif bir artış göstermektedir. (%39,6 ve 2020 (%38,6).

Bu cihazlar, HMI'ları, SCADA sistemlerini, historian'ları, veri ağ geçitlerini, mühendislik iş istasyonlarını, endüstriyel ağların yönetimi için kullanılan bilgisayarları ve endüstriyel sistemler için yazılım geliştirmek için kullanılan cihazları içermektedir.

Ancak 2022'nin ikinci yarısındaki en önemli artış, saldırıların yüzde dokuz arttığı ve Rusya'daki EKS bilgisayarlarının %39,2'sinin hedef alındığı görüldü.

Kaspersky'ye göre bu artış, ürünlerinin kötü amaçlı komut dosyalarını ve kimlik avı sayfalarını engellediği EKS cihazlarının yüzdesindeki önemli artıştan kaynaklanıyor.

"Ağustos ve Eylül 2022'de kötü amaçlı komut dosyaları ve kimlik avı sayfalarının engellendiği EKS bilgisayarlarının yüzdesindeki ani artış ve sonraki aylardaki yüksek rakamlar, web sitelerinin (endüstriyel kuruluşlarınkiler dahil) kitlesel olarak ele geçirilmesinden kaynaklanıyordu." diye açıkladı.

CVE-2022-27228 olarak takip edilen ve istismar edilen güvenlik açığı, Bitrix Site Manager uygulamasının 'Polls, Votes' modülünü etkiliyor. Güvenlik açığı, kimliği doğrulanmamış uzaktaki bir saldırganın rastgele kod yürütmesine olanak tanımaktadır.

Bitrix24, Mart 2022'de güvenlik açığı için yamalar duyurdu . O sırada, açığı bulan Rus siber güvenlik firması Positive Technologies'den bir araştırmacıydı. Rusya'nın yanı sıra Beyaz Rusya, Kırgızistan, Özbekistan ve Kazakistan gibi ülkelerdeki EKS bilgisayarları, Bitrix CMS tarafından desteklenen web sitelerine yönelik CVE-2022-27228 istismarının bir sonucu olarak kötü amaçlı komut dosyaları ve kimlik avı sayfalarıyla giderek daha fazla hedefleniyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/exploitation-of-bitrix-cms-vulnerability-drives-ics-attack-surge-in-russia/
https://www.darkreading.com/application-security/40-global-ics-systems-attacked-malware-2022

14 Mart 2023

1.10. Yeni EKS Yamaları: Siemens ve Schneider Electric İçin 100'den Fazla Güvenlik Açığı Duyurusu

Siemens ve Schneider Electric, Mart 2023 Salı Yaması güvenlik tavsiyeleriyle 100'den fazla güvenlik açığını ele aldı.

Siemens

Siemens yalnızca yedi yeni tavsiye yayınladı ve bunlar toplam 92 güvenlik açığını ilgilendiriyor. Ancak, büyük bir çoğunluğu Siemens ürünlerine özgü olmak yerine üçüncü taraf bileşenlerin kullanımıyla meydana geldiği görülmektedir..

Örneğin, Ruggedcom ve Scalance ürünlerinde Linux çekirdeği, Busybox, OpenSSL ve OpenVPN gibi bileşenleri etkileyen 65 güvenlik açığı yamalandı. Bu açıklıkların kötüye kullanılması, hizmet reddi (DoS) durumuna veya kod enjeksiyonuna yol açabilmektedir.

Üçüncü taraf bileşenlerini etkileyen on yedi güvenlik açığı, Scalance cihazlarında yamalanmıştır. Bu güvenlik açıklarının kötüye kullanılması, bir DoS durumuna veya hassas verilerin ifşasına yol açabilmektedir.

Siemens ayrıca Scalance W1750D cihazlarında birkaç OpenSSL güvenlik açığının ele alındığını da duyurdu.

Wind River VxWorks'ü etkileyen yüksek önem dereceli bir DoS güvenlik açığı, Siprotec 5 cihazlarında yamalanmıştır.

Üçüncü taraf bileşenlerini etkileyen güvenlik açıklarına ek olarak Siemens, müşterilerini Mendix SAML modülünü etkileyen kritik bir kimlik doğrulama atlama sorunu hakkında da bilgi paylaştı.

Şirket ayrıca, Ruggedcom Crossbow cihazlarında yüksek önem düzeyine sahip sorunlar da dahil olmak üzere hak yükseltme, bilgi ifşası ve SQL enjeksiyonu hatalarını duyurdu.

Siemens'in bu güvenlik açıklarından bazıları için henüz gerçek yamalar yayınlamadığını belirtmekte fayda var. Bazı durumlarda, şu anda yalnızca çevreleyici güvenlik önlemleri bulunmaktadır.

Schneider Electric

Schneider Electric, toplam 10 güvenlik açığını kapsayan üç yeni öneri yayınladı.

Kılavuz doküman, PowerLogic güç sayaçlarındaki kritik bir güvenlik açığını içermektedir. Açıklık, DoS saldırıları veya uzaktan kod yürütme için kullanılabilmektedir.

Başka bir kılavuz, IGSS SCADA ürününde bulunan sekiz güvenlik açığına ilişkin bilgi içermektedir. Çeşitli IGSS modülleri, 'yüksek' ve 'orta' önem dereceleri atanan DoS ve uzaktan kod yürütme sorunlarından etkilenmektedir.

Son kılavuz ise, kullanıcıları EcoStruxure Power Monitoring Expert ürününü etkileyen bir oturum ele geçirme sorunu hakkında bilgi içermektedir.

Salı günü Siemens ve Schneider ayrıca müşterileri yamaların kullanılabilirliği, yeni CVE'ler, etkilenen ürün listelerindeki değişiklikler ve diğer bilgiler hakkında bilgilendirmek için düzinelerce önceki tavsiyeleri güncelledi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/ics-patch-tuesday-siemens-schneider-electric-address-over-100-vulnerabilities

22 Mart 2023

1.11. Hacktivistler Giderek Artan Bir Şekilde OT Sistemlerini Hedef Aldıklarını İddia Ediyor

Ocak 2023'te Anonymous'a bağlı bilgisayar korsanlığı grubu GhostSec, sosyal medyada, endüstriyel otomasyon cihazlarının uzaktan izlenmesi için bir tür operasyonel teknoloji (OT) cihazı olan Belarus uzak terminal birimini (RTU) şifrelemek için fidye yazılımı dağıttığını iddia etti.

Araştırmacılar, OT güvenlik uzmanları ve medya kuruluşları iddiaları analiz ettiler ve aktörün iddia edilen saldırının sonuçlarını abarttığı sonucuna vardılar.

Bu özel olayda önemli bir etki olmamasına rağmen, olay, bilgisayar korsanlarının OT ortamlarına yönelik risk boyutuna ilişkin daha geniş bir tartışmaya yönelik artan ihtiyacı vurgulamaktadır. Son birkaç yıldır Mandiant, çeşitli bilgisayar korsanlarının OT sistemlerini hedef aldıkları iddialarının izini sürdü ve bunun sonucunda fiziksel hasar olduğunu iddia etti. Rusya'nın devam eden Ukrayna işgali gibi farklı bölgelerdeki jeopolitik gerilimlerle şiddetlenen bu aktörler son zamanlarda faaliyetlerini yoğunlaştırdı.

Çoğu durumda, bilgisayar korsanlarının iddiaları abartılı veya asılsız olabilmektedir. Yanlış iddiaların sayısı bazen çürütmek için zorlayıcıdır. Bununla birlikte, çoğu iddianın yanlışlığına rağmen, EKS'yi hedefleyen bilgisayar korsanlığı faaliyeti sıradan hale geldiğinde, gerçek ve hatta önemli EKS olaylarının olasılığı artar. Coğrafi konum, milliyet, dil veya ilgili sektöre dayalı olarak siyasi olaylarla veya sosyal anlaşmazlıklarla algılanabilir bir şekilde ilişkilendirilen kuruluşlar için risk daha yüksektir.

Bu blog gönderisinde Mandiant, OT sistemlerini hedef alan son bilgisayar korsanlığı etkinliğinin kapsamlı bir analizini sunuyor. Mandiant, OT savunucuları için olası sonuçları tartışmak için önceden açıklanmayan ve bilinen olaylardan elde edilen bilgilerden yararlanmıştır. Ortaya çıkan bilgisayar korsanlığı eğilimleri hakkındaki farkındalık, OT savunucularının karşı önlemlere öncelik vermesine ve bilgisayar korsanlığı örtüsünden yararlanan devlet destekli cepheleri ayırt etmesine yardımcı olmaktadır.

Hacktivistler Giderek Artan Bir Şekilde OT'yi Hedeflediklerini ve Etkilediklerini İddia Ediyor

2021'de Mandiant, aktörlerin birden çok sektörde internete maruz kalan varlıkları hedef aldığı düşük karmaşıklık tavizlerinde artan bir eğilimi açıklayan bir blog gönderisi yayınladı. “Analiz ettiğimiz vakaların çoğu, görünüşe göre mali veya fırsatçı motivasyonlarla yürütüldü. Ancak diğerleri, OT cihazlarını hedeflediklerini iddia eden veya diğer aktörleri OT sistemlerine nasıl saldıracakları konusunda bilgilendirmek için eğitim kılavuzları yayınlayan bilgisayar korsanlığı grupları tarafından ideolojik motivasyonlarla yürütüldü”

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.mandiant.com/resources/blog/hacktivists-targeting-ot-systems
https://cyberscoop.com/hacktivist-target-operational-technology/

29 Mart 2023

1.12. ABD Enerji Sektörü, Çin Yapımı Şebeke Teknolojisinden Kaynaklanan Siber Riskle Karşı Karşıya

Cyberscoop'un bildirdiğine göre, ABD için ulusal bir güvenlik riski oluşturan ABD elektrik şebekesindeki Çin ekipmanlarının bilinmeyen yaygınlığı konusunda alarmlar verildi.

Bir senatör "ABD, Çin menşeli elektrik şebekesi ekipmanlarını belirlemek için acilen harekete geçmeli" dedi.

Bu arada, Enerji Bakanlığı Siber Güvenlik Ofisi, Enerji Güvenliği ve Acil Müdahale Direktörü Puesh Kumar, Enerji Bakanlığı'nın Çin'de üretilenleri belirlerken en kritik şebeke sistemi bileşenlerini daha iyi anlamak için harekete geçtiğini belirtti. Kumar, Enerji Departmanının farklı şebeke ekipmanlarındaki güvenlik açıklarını belirlemek için ulusal laboratuvarlarla da işbirliği yaptığını, ancak Çin ekipmanlarını analiz etmek için daha kapsamlı bilgi paylaşım çabalarına ihtiyaç duyulduğunu söyledi.

Kumar konuşmasında şunları söyledi: *"Hepimiz kendi siber tehditlerimizi kendi alanlarımızda görüyoruz, ancak noktaları birleştirmiyoruz. Görmüyoruz: Eğer bu batıda oluyorsa, doğuda da mı oluyor? Bu noktaları özel sektör ağlarından ve siber teknoloji şirketlerinden öğrendiklerimizle istihbarat topluluğuyla nasıl birleştirebiliriz?"*

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.scmagazine.com/brief/threat-intelligence/us-energy-sector-facing-cyber-risk-from-chinese-made-grid-tech

22 Mart 2023

1.13. WellinTech “Data Historian” Bileşenlerinde Bulunan Yüksek Derecede Güvenlik Açıkları

Cisco Talos araştırmacıları, WellinTech'in KingHistorian data historian yazılımında yüksek önem düzeyine sahip iki güvenlik açığı buldu.

Cisco'nun Talos tehdit istihbaratı ve araştırma birimi, geçen yıl WellinTech'in KingHistorian data historian yazılımında keşfedilen iki yüksek önemdeki güvenlik açığının ayrıntılarını bu hafta açıkladı.

Çin merkezli endüstriyel otomasyon yazılım şirketi WellinTech, KingHistorian'ı 'muazzam miktarda' endüstriyel kontrol sistemi (EKS) verisi toplamak ve işlemek için tasarladı.

Talos araştırmacıları, data historianIN iki açıklıktan etkilendiğini keşfettiler. CVE-2022-45124 olarak izlenen zafiyet bir kimlik doğrulama paketine müdahale edebilen bir saldırganın sistemde oturum açmış meşru kullanıcının kullanıcı adını ve parolasını ele geçirmesine izin verebilmektedir.

İkinci sorun olan CVE-2022-43663, arabellek taşmasını tetikleyen özel hazırlanmış bir ağ paketi gönderilerek kullanılabilmektedir. Açıklığın keyfi kod yürütme için mi yoksa yalnızca sistemi devre dışı bırakmak için mi kullanılabileceği henüz net değil.

Üretici, Aralık 2022'de güvenlik açıkları hakkında bilgilendirildi ve bu ayın başlarında yamalar yayınladı.

Cisco, bu güvenlik açıklarının olası istismarından kaynaklanan gerçek dünya etkisi hakkında herhangi bir bilgi paylaşmadı, ancak siber güvenlik şirketlerinden gelen önceki raporlara göre, bir data historian tehlikeye atmak tehdit aktörleri için çok yararlı olabilmektedir.

Ocak ayında, endüstriyel güvenlik şirketi Claroty, araştırmacıları tarafından GE Digital Proficy Historian ürününde bulunan birkaç güvenlik açığını açıklamıştı. Şirket o sırada, açıkların casusluk için kullanılabileceği veya endüstriyel ortamlarda hasara ve kesintiye neden olabileceği konusunda uyarıda bulunmuştu.

Historian sunucuları, hem BT hem de OT sistemlerine erişim sağlayarak, bilgisayar korsanlarının değerli bilgilere erişim elde etmek veya ağdaki diğer sistemlere geçmek için güvenliği ele geçirilmiş cihazlardan yararlanmasına olanak tanımaktadır.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/high-severity-vulnerabilities-found-in-wellintech-industrial-data-historian/

22 Mart 2023

1.14. ENISA: Fidye Yazılımları AB Taşımacılık Sektöründeki OT Sistemlerini Hedef Alabilir

ENISA, fidye yazılımı ve verilerle ilgili saldırıların, AB'de ulaşım sektörüne yönelik en büyük siber güvenlik tehditleri olduğunu belirtti.

Fidye yazılımı, AB'de ulaşım sektörü için en büyük tehdit haline geldi ve Avrupa Birliği Siber Güvenlik Ajansı (ENISA), fidye yazılımı gruplarının operasyonel teknoloji (OT) sistemlerini etkilemesini öngörüyor.

ENISA'nın yeni bir raporuna göre, havacılık, deniz, demiryolu ve karayolu taşımacılığı kuruluşlarını hedef alan genel siber saldırı sayısı Ocak 2021 ile Ekim 2022 arasında arttı ve olayların çoğundan (%54) siber suçlular sorumlu.

Fidye yazılımı, gözlemlenen olayların %38'inde kullanılan birincil tehdit olarak ortaya çıktı ve veriyle ilgili saldırılar %30 ile ikinci sırayı aldı.

Kötü amaçlı yazılım (%17), DoS ve DDoS (%16), kimlik avı (%10) ve tedarik zinciri saldırıları (%10) ile ihlaller, dolandırıcılık ve güvenlik açığı istismarı da gözlemlendi.

Bir fidye yazılımı saldırısının parçası olarak, tehdit aktörleri bir hedefin sistemlerini tehlikeye atar, dosyaları şifreleyen kötü amaçlı yazılımları dağıtır ve şifre çözme anahtarları karşılığında bir fidye ödemesi talep eder. Birkaç yüksek profilli saldırı da dahil olmak üzere belirlenen olayların önemli bir bölümünü temsil eden fidye yazılımı, kötü amaçlı yazılımdan ayrı olarak sunulur.

"Ekim 2022'ye kadar toplanan olaylarla ilgili veriler, 2022 boyunca fidye yazılımı saldırılarının bildirilmesinde bir artış olduğunu gösteriyor. Taşımacılık sektörüne bildirilen fidye yazılımı saldırılarının sayısı, 2021'de %13'ten 2022'de neredeyse iki katına çıkarak %25'e yükseldi. Fidye yazılımlarının aksine, biz 2021'e kıyasla 2022'de kötü amaçlı yazılım olaylarında bir düşüş gözlemledik (%11'den %6'ya)," diye açıklıyor ENISA.

Ajans, *"fidye yazılımı gruplarının öngörülebilir gelecekte OT operasyonlarını büyük olasılıkla hedef alacağı ve kesintiye uğratacağı"* şeklindeki önceki uyarısını yineledi.

Şimdiye kadar, OT sistemlerinin ve ağlarının yalnızca tüm ağlar etkilendiğinde veya güvenlik açısından kritik BT sistemleri kullanılamaz hale geldiğinde etkilendiğini kaydetti.

Ancak ENISA, artan sayıda endüstriyel kontrol sistemi (EKS/ICS) güvenlik açıkları, büyüyen IT-OT bağlantısı ve böyle bir durumun önemli iş ve sosyal etkisi dahil olmak üzere çeşitli faktörler nedeniyle ulaşım sektöründeki OT sistemlerinin doğrudan hedef alındığını değerlendiriyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/ransomware-will-likely-target-ot-systems-in-eu-transport-sector-enisa/

22 Mart 2023

1.15. CISA Endüstriyel Kontrol Sistemlerindeki Kritik Güvenlik Açıkları Konusunda Uyarıyor

ABD Siber Güvenlik ve Altyapı Güvenliği Dairesi (CISA), geçtiğimiz ay Delta Electronics ve Rockwell Automation'ın ekipmanlarını etkileyen kritik açıklıklara ilişkin uyarıda bulunan 8 Endüstriyel Kontrol Sistemleri (EKS/ICS) tavsiyesi yayınladı.

Buna, Delta Electronics'in gerçek zamanlı bir cihaz izleme yazılımı olan InfraSuite Device Master'daki 13 güvenlik açığı dahildir. Açıklıktan 1.0.5'ten önceki tüm sürümler sorunlardan etkilenmektedir.

CISA, *"Bu güvenlik açıklarının başarılı bir şekilde kullanılması, kimliği doğrulanmamış bir saldırganın dosyalara ve kimlik bilgilerine erişmesine, ayrıcalıkları artırmasına ve uzaktan rasgele kod yürütmesine izin verebilir"* dedi.

Listenin başında CVE-2023-1133 (*CVSS puanı: 9.8*), InfraSuite Device Master'ın doğrulanmamış UDP paketlerini kabul etmesi ve içeriğin serisini kaldırması ve böylece kimliği doğrulanmamış bir uzak saldırganın rastgele kod yürütmesine izin vermesi gerçeğinden kaynaklanan kritik bir açıklık bulunmaktadır.

CISA , diğer iki güvenlik açığı CVE-2023-1139 (*CVSS puanı: 8.8*) ve CVE-2023-1145 (*CVSS puanı: 7.8*) de uzaktan kod yürütme elde etmek için silah haline getirilebileceğini belirtmektedir.

Bu açıklıkları Piotr Bazydlo ve isimsiz bir güvenlik araştırmacısı, CISA'ya bildirmiştir.

Diğer bir güvenlik açığı grubu, Rockwell Automation'ın ThinManager ThinServer'ı ile ilgilidir ve istemci ve uzak masaüstü protokolü (RDP) sunucu yönetim yazılımının aşağıdaki sürümlerini etkilemektedir:

- 6.x – 10.x
- 11.0.0 – 11.0.5
- 11.1.0 – 11.1.5
- 11.2.0 – 11.2.6
- 12.0.0 – 12.0.4
- 12.1.0 – 12.1.5
- 13.0.0 – 13.0.1

Sorunların en ciddi olanı, kimliği doğrulanmamış bir uzak saldırganın dizine rasgele dosyalar yüklemesine izin verebilecek CVE-2023-28755 (*CVSS puanı: 9.8*) ve CVE-2023-28756 (*CVSS puanı: 7.5*) olarak izlenen açıklıktır. Daha da rahatsız edici bir şekilde, saldırgan CVE-2023-28755'ı mevcut yürütülebilir dosyaların üzerine trojenleştirilmiş sürümlerle yazmak için silah haline getirebilir ve potansiyel olarak uzaktan kod yürütülmesine yol açabilir.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://thehackernews.com/2023/03/cisa-alerts-on-critical-security.html

7 Mart 2023

1.16. Fidye Yazılımlarının Favori Hedefi: Kritik Altyapı ve Endüstriyel Kontrol Sistemleri

Sağlık, imalat ve enerji sektörleri fidye yazılımlarına karşı görece en savunmasız sektörlerdir.

Ulusal savunma ve güvenlik uzmanları, gelecekteki savaşların ateşli silahlarla değil, insanların günlük yaşamları için bağımlı oldukları hizmetleri devre dışı bırakmak için tasarlanmış kodlarla yürütüleceğini uzun süredir tahmin ediyorlardı.

Mayıs 2021'de, Colonial Pipeline'ı bir fidye yazılımı saldırısı vurduğunda güvenlik uzmanlarının en büyük korkuları gerçek oldu. ABD'nin kuzeydoğusundaki çoğu bölgeye gaz sevkiyatı neredeyse bir gecede durduruldu. Sistemler sonunda geri yüklenmiş olsa da, olay bugün hala gündemdeki yerini koruyor ve ve bize siber saldırıların kritik altyapıya karşı yıkıcı potansiyeli hatırlatıyor. O zamandan beri, benzer altyapı saldırıları dünyanın birçok yerinde manşetlere konu oldu ve giderek artan bir şekilde devlet destekli olmayan aktörler tarafından gerçekleştiriliyor.

Securin (*eski adıyla Cyber Security Works*) araştırmacıları, " 2. Çeyrek/3. Çeyrek Fidye Yazılımı Dizin Raporu ", fidye yazılımlarının kritik altyapı kuruluşlarında konuşlandırılan endüstriyel kontrol sistemleri (EKS/ICS) üzerindeki etkisinin haritasını çıkardı. En riskli üç sektörü şu şekilde belirlediler: **sağlık**, **enerji** ve **imalat**. Araştırmacılarımız ayrıca 16 fidye yazılımı güvenlik açığını ve bunları kullanan Ryuk, Conti, WannaCry ve Petya gibi kötü aktörleri inceledi. Makalenin sonuna, güvenlik açıklarının ve etkilenen üreticilerin tam listesini içeren bir tablo ekledik.

Her başarılı saldırıda, fidye yazılımı grupları daha cesur hale gelmekte ve maksimum gasp için krizlerden en çok acıya neden olabilecek sektörleri hedef almaktadır. Tehdit aktörlerini ve yöntemlerini anlamak, kritik sektörleri korumanın ve operasyonları sorunsuz sürdürmenin anahtarıdır.

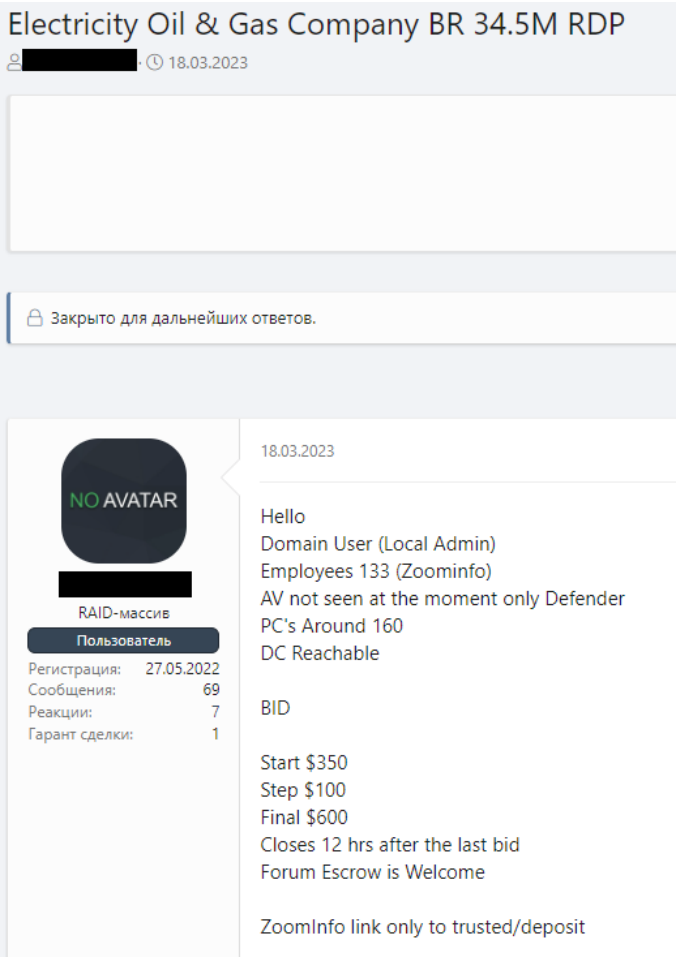
TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/ransomware-s-favorite-target-critical-infrastructure-and-its-industrial-control-systems

18 Mart 2023

1.17. Petrol ve Gaz Sektöründeki Bir Kuruluşa Yönelik Erişim Satışı İddiası

Popüler Rus yeraltı forumunda bir ilk erişim aracısı (IAB) petrol ve gaz sektöründe faaliyet gösterdiğini belirttiği bir şirkete yönelik erişim satışı iddiasında bulunmaktadır.



Aktör, şirketin kurumsal ve iç ağına yönelik çeşitli veriler hakkında bilgi verirken, mevcut satış için forum aracılarını (escrow) kullanmaya açık olduğunu belirtmesi, satış iddiasının gerçek olma olasılığını artırmaktadır. IAB'lerin sık müşterileri arasında fidye yazılımı grupları yer almaktadır.

TESPİT YERİ:
Dark Web

KAYNAK:
-

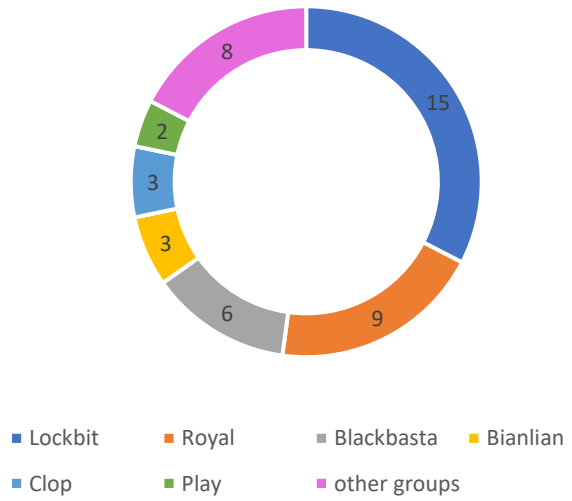
2. FİDYE YAZILIMI SALDIRILARI

Mart ayında, faaliyetleri takip edilen fidye yazılımı saldırıları incelendiğinde; **enerji**, **petrol ve gaz**, **elektrik-altyapı** sektörlerinde **ABD** ve **Birleşik Krallık** en çok hedeflenen ülkeler arasında yer almışlardır. '**Clop**' enerji sektörünü en çok hedefleyen fidye yazılımı grubu olmuştur.

Grup	Hedef Sektör	Hedef Ülke
vicesociety	Enerji	İspanya
royal	Enerji	ABD
blackbasta	Enerji	İtalya
clop	Enerji	Almanya
clop	Enerji	Birleşik Krallık
clop	Enerji	Birleşik Krallık
clop	Enerji	İsviçre
clop	Enerji	Kolombiya
clop	Enerji	Türkiye
ransomhouse	Enerji	Endonezya
lockbit3	Enerji	ABD
alphv	Elektrik-Altyapı	ABD
blackbyte	Elektrik-Altyapı	Birleşik Krallık
lockbit3	Elektrik-Altyapı	Hindistan
royal	Elektrik-Altyapı	ABD
stormous	Elektrik-Altyapı	Hollanda
lockbit3	Petrol ve Gaz	ABD
clop	Petrol ve Gaz	Peru

Bu ay en çok hedeflenen sektör **imalat** olurken, bu sıralamayı hizmet, bilişim, finans ve sağlık sektörü izlemiştir.

İmalat sektörüne yönelik fidye yazılımı vakaları incelendiğinde, saldırıyı gerçekleştiren grup ve grubun imalat sektöründe kaç adet firmayı hedeflediği aşağıdaki grafikte incelemeye sunulmuştur.



CYBER WISE | ICSFUSION

Endüstriyel Tesislere Yönelik

Saldırı Bilgilendirme Raporu

icsfusion.com