CYBER WISE | ICSFUSION

Endüstriyel Tesislere Yönelik

Saldırı Bilgilendirme Raporu

Ocak 2023

icsfusion.com

ICSFUSION

İÇİNDEKİLER

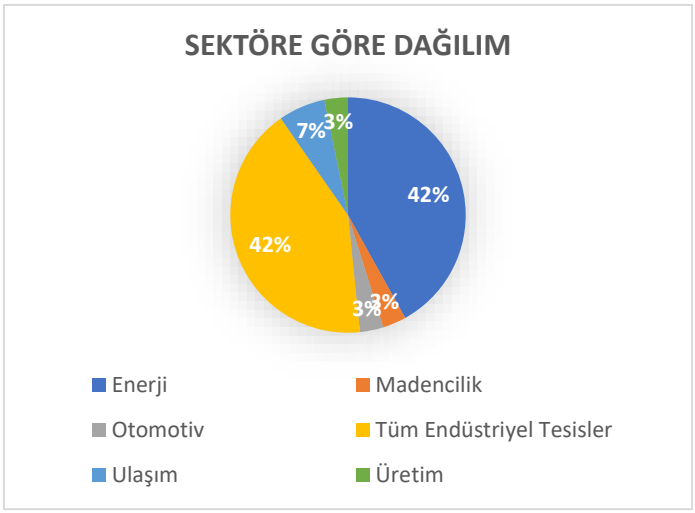
İÇİNDEKİLER

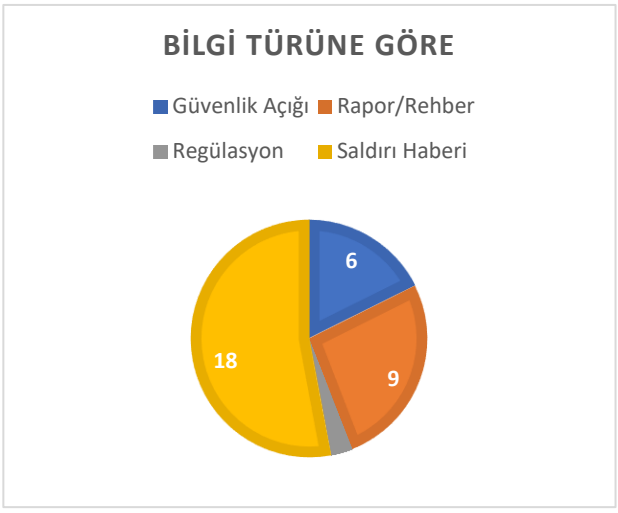
YÖNETİCİ ÖZETİ

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.

Rapor kapsamında elde edilen veriler *bilgi türüne göre* analiz edildiğinde ağırlıklı olarak "saldırı haberi", "güvenlik açığı" ve "rapor/rehber" olduğu görülmüştür.

Bu bilgilerin sektör dağılımı incelendiğinde ise ağırlıklı olarak enerji tesislerinin ön planda olduğu görülmektedir. Enerji sektörü özelinde petrol ve doğal gaz sektörünün gündemin büyük bir bölümünü oluşturduğu anlaşılmaktadır.





Endüstriyel tesisler açısından yönetilemeyen güvenlik açıklıkları, ransomware saldırıları halen gündemin sıcak konuları arasında yer almaktadır. Son dönemde özellikle kritik imalat sektörü başta olmak üzere otomotiv ve ulaşım/gemi taşımacılığı sektörüne yönelik tehditlerin arttığı görülmektedir.

17 Ocak 2023

1. HABERLER

1.1. CISC, Enerji Sektöründeki Kritik Altyapılar İçin Risk Değerlendirme Rehberi Yayınladı

Avustralya'nın Siber ve Altyapı Güvenlik Merkezi (CISC), Salı günü enerji sektöründeki kritik altyapılar için Risk Değerlendirmesi rehberini yayınladı. Belge, paydaşların ülkenin ekonomik ve sosyal refahı için gerekli olan varlıkların işletilmesiyle ilgili risklerin doğru bir şekilde tanımlanmasını garanti etmek için risk yönetimi yaklaşımlarını değiştirmeleri gerekliliğini vurgulamaktadır.

Risk Değerlendirmesi rehber dokümanı, Avustralya'nın kritik altyapısına yönelik bu tür risklerin değerlendirilmesinde rehberlik etmesi için tasarlanmıştır. *"Önerilen risk değerlendirme yaklaşımlarının sağlanması yoluyla, materyal, sektör paydaşlarının mevcut risk uygulamalarını uyarlamalarına yardımcı olmayı ve kuruluşların daha geniş ulusal kritik altyapı bağlamındaki riskleri anlamalarına yardımcı olmayı amaçlamaktadır."*

Belge, kurumların geçmişte riske bakışından farklı olabilecek kritik altyapı risklerini belirleyerek başlamaktadır. *"Avustralya'nın veya halkının sosyal veya ekonomik istikrarı, Avustralya'nın savunması veya ulusal güvenliği üzerinde en büyük etkiye sahip risklerin de dikkate alınması ve kritik altyapı birimlerinin mevcut risk yönetimi stratejileri içinde çerçevelenmesi gerekmektedir."*

Belgede, *"bu risk tanımlamasının bir parçası olarak kuruluşlar, varlıklarının gizliliğinin, kullanılabilirliğinin, bütünlüğünün ve güvenilirliğinin herhangi bir olay sırasında ve sonrasında nasıl etkilenebileceğini geniş ölçüde değerlendirebilir. Bu potansiyel 'ilgili etkiyi' anlamak, riske öncelik vermek ve hem riskin oluşma olasılığını en aza indirmenin hem de potansiyel etkiyi en iyi nasıl azaltacağınızı belirlemek için önemlidir."*

Avustralya Risk Değerlendirmesi danışma belgesi, *"Enerji Sektöründeki bazı kuruluşların güvenlikle ilgili düzenlemeleri zaten yürürlüktedir"* dedi. *"Sektördeki kuruluşların, Avustralya Enerji Sektörü Siber Güvenlik Çerçevesi (AESCSF) veya Avustralya Yurtiçi Gaz Güvenlik Mekanizması (ADGSM) gibi kılavuzları dikkate alması veya düzenleyici çerçeveler için eyalet veya bölge hükümetlerine bakması ve bunları nasıl dahil edebileceklerini düşünmesi gerekebilir.."* diye ekledi…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/utilities-energy-power-water-waste/australias-cisc-releases-risk-assessment-advisory-for-critical-infrastructure-across-energy-sector/

16 Ocak 2023

ICSFUSION

1.2. Siemens, Sewio, InHand Networks, SAUTER Controls, Hitachi Energy ve Johnson Controls Donanımında Bulunan ICS Güvenlik Açıkları

ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), geçen hafta birden çok kritik altyapı sektöründe kullanılan ICS (endüstriyel kontrol sistemleri) cihazlarında belirlenen önemli donanım açıklarını vurgulayan güvenlik tavsiyeleri yayınladı. Bu ürünler, Siemens, Sewio, InHand Networks, SAUTER Controls, Hitachi Energy ve Johnson Controls gibi çeşitli satıcıların ürünlerini kapsamaktadır.

CISA, Siemens'in S7-1500 CPU ürün ailesi donanımında bir güvenlik açığı yayınladı. Bu güvenlik açığından yararlanmak, aygıta fiziksel erişimi olan bir davetsiz misafirin aygıtın önyükleme görüntüsünü değiştirmesine ve denetlenmeyen kodu başlatmasına olanak sağlayabilir.

Birden çok kritik altyapı sektörüne dağıtılan CISA, ilgili dokümanlarda *"etkilenen cihazların donanımda değişmez bir güvenli kökü içermediğini"* söyledi. *"Bu nedenle, cihazda yürütülen kodun bütünlüğü, yükleme süresi boyunca doğrulanamaz. Aygıta fiziksel erişimi olan bir saldırgan, bunu aygıtın önyükleme görüntüsünü değiştirmek ve rastgele kod yürütmek için kullanabilir."*

Red Balloon Security'den Yuanzhe Wu ve Ang Cui, bu güvenlik açığını Siemens'e bildirdi. Alman şirketi, cihazları kilitli kontrol kabinlerine yerleştirmek ve donanımı yükseltmek gibi donanım kurcalamalarını önlemek için etkilenen cihazlara fiziksel erişimin güvenilir personelle sınırlandırılması çağrısında bulundu. Siemens, bu güvenlik açığını gidermek için ek PLC türleri için yeni donanım sürümleri üzerinde çalışıyor.

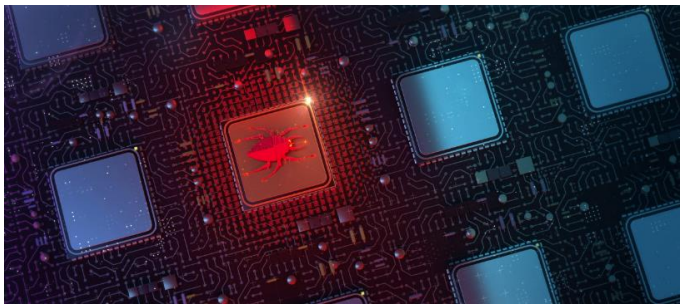
Başka bir CISA duyurusunda, ajans, Siemens Mendix SAML ekipmanı genelinde uzaktan istismar edilebilir ve düşük saldırı karmaşıklığına sahip bir güvenlik açığını ortaya çıkardı. Kritik altyapı sektörlerinde küresel olarak benimsenen web sayfası oluşturma güvenlik açığı sırasında girdilerin uygunsuz şekilde etkisiz hale getirilmesi, bilgisayar korsanının kullanıcıları kötü amaçlı bir bağlantıya erişmeleri için kandırarak hassas bilgiler elde etmesine olanak sağlayabilir. Kullanıcılara ekipmanlarını yükseltmeleri tavsiye edildi…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/cisa/ics-vulnerabilities-found-in-siemens-sewio-inhand-networks-sauter-controls-hitachi-energy-johnson-controls-hardware/

23 Ocak 2023

1.3. Endüstriyel Siber Güvenlik Şirketi, Endüstriyel Fidye Yazılımı Analizi: 2022 4. Çeyrek Raporu Yayınladı



2022'nin dördüncü çeyreğinde fidye yazılımları, dünya çapındaki endüstriyel kuruluşlar için önemli finansal ve operasyonel riskler oluşturmaya devam etti. Dragos, endüstriyel kuruluşları ve altyapıyı etkileyen 57 farklı fidye yazılımı grubunun faaliyetlerini aktif olarak izliyor ve analiz ediyor. Dragos, kamuya açıklanan olaylar, ağ telemetrisi ve dark web gönderileri yoluyla, bu 57 gruptan yalnızca 24'ünün 2022'nin 4. çeyreğinde aktif olduğunu gözlemledi. Bu süre zarfında Dragos, 128 olaydan yüzde 30 artışla 189 fidye yazılımı vakasını tespit etti.

Fidye yazılımı grupları, araçlarının verimliliklerini artırmaya, tespitten kaçınma yeteneklerini geliştirmeye ve yeni Taktikler, Teknikler ve Prosedürler (TTP) benimsemeye devam ediyor. RansomExx, ALPHV, Hive, Luna ve Qilin dahil olmak üzere birçok fidye yazılımı grubu kötü amaçlı yazılımlarını Rust programlama dilinde yeniden yazdı. Rust nispeten yeni bir programlama dili olduğu için, virüsten koruma çözümleri onu ve eski programlama dillerini anlayıp analiz edememekte, bu durum da tespit edilmeden önce kurban sistemleri etkilemek için daha uzun bir süre sağlamaktadır.

Black Basta, ALPHV, PLAY, Qilin ve Qyick gibi artan sayıda fidye yazılımı grubu, hedeflenen dosyaların içeriğinin yalnızca bazı kısımlarını şifrelemeye dayanan ve daha hızlı şifreleme süresi sağlayan "aralıklı şifreleme" adlı yeni bir taktik benimsedi. Şifrelemedeki bu azalma, anormal dosya bilgisi işlem etkinliklerini algılamaya dayanan otomatik algılama araçları tarafından algılanma şansını azaltmaktadır.

Dragos, geçtiğimiz çeyrekte iki veya daha fazla fidye yazılımı grubundan etkilenen birden fazla kurban gözlemledi; bu, grupların ilk erişimi aynı İlk Erişim Aracılarından (IAB'ler) ve Toptan Erişim Piyasalarından (WAM) satın almış olabileceğini gösteriyor. IAB'ler ve WAM'in bu taktiği, özellikle fidye yazılımı gruplarına sattıkları ilk erişimde kullandıkları ve endüstriyel kuruluşların fidye yazılımlarından karşı karşıya kaldıkları risk düzeyini yükselttikleri biliniyor. Örneğin, aşağıdaki fidye yazılımı grupları 2022'nin üçüncü çeyreğinde aynı kurbanları hedefledi:

- Alphav ve Vice Society
- Cuba ve Karakurt
- LockBit3 ve Everest

Lockbit 3.0, geçtiğimiz çeyrekte Lockbit 3.0 oluşturucusunu ve diğer yeni yeteneklerini tanıttıklarında yıllık yüksek oran olan yüzde 31'den, son çeyrekte endüstriyel kuruluşları ve altyapıyı etkileyen toplam 189 fidye yazılımı olayının yüzde 21'ini oluşturdu.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q4-2022/

20 Ocak 2023

1.4. Kritik İmalat Sektörü Saldırganların Hedefi Olmaya Devam Ediyor

Sektörde yapılan bir araştırma, üretim kuruluşlarının dörtte üçünden fazlasının sistemlerinde yama uygulanmamış yüksek önem dereceli güvenlik açıkları barındırdığını ortaya çıkardı.

SecurityScorecard'ın yeni telemetrisi, bu kuruluşlardaki yüksek önem dereceli güvenlik açıklarında yıldan yıla bir artış olduğunu gösteriyor.

SecurityScorecard'ın kurucu ortağı ve CEO'su Aleksandr Yampolskiy, 2022'de *"Üretim kuruluşlarının yaklaşık %76'sı, SecurityScorecard, platformumuzun bu kuruluşlara atfettiği IP adreslerinde yama uygulanmamış CVE'ler gözlemledi"* ni ifade etti.

Metal, makine, cihaz, elektrikli ekipman ve nakliye imalatını içeren bu kuruluşların yaklaşık %40'ı 2022'de kötü amaçlı yazılım bulaşmasına maruz kaldı.

Kritik üretim kuruluşlarının neredeyse yarısı (%48) SecurityScorecard'ın güvenlik derecelendirme platformunda "C" ile "F" arasında bir sıralama aldı.

Platform, DNS sağlığı, IP itibarı, web uygulama güvenliği, ağ güvenliği, sızan bilgiler, hacker sohbeti, uç nokta güvenliği ve yama yönetim performansı dahil olmak üzere on grup risk faktörü içermektedir.

Yampolskiy, üreticilere yönelik siber saldırıların ciddiyetinin dikkate değer olduğunu söylüyor.

"Bu olayların çoğu, genellikle bir suç grubu biçimindeki tehdit aktörünün haraç yoluyla para kazanmak için yola çıktığı fidye yazılımları içeriyor" diyor. *"Fidye yazılımı sorunu küresel olsa da, çeşitli jeopolitik hedefler peşinde koşan ulus-devlet aktörlerinden kritik altyapıya yönelik artan sayıda saldırının geldiğini gördük."*

Bu arada, Dragos ve IBM X-Force ekipleri tarafından yapılan olay müdahale araştırmaları, ezici bir çoğunlukla, en sıcak operasyon teknolojisi (OT) hedefinin imalat sektörü olduğunu ve bu kuruluşlara yönelik öncelikli tehdidin artık fidye yazılımları olduğunu gösterdi.

"Demokratik" Siber Güvenlik

Yampolskiy, Rusya gibi gelişmiş devlet destekli aktörlerin ABD genelinde sağlık hizmetlerinden enerjiye ve telekomünikasyona kadar birçok farklı kritik altyapı kuruluşunu hedef aldığını söylüyor…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/critical-manufacturing-sector-in-the-bulls-eye

19 Ocak 2023

1.5. Endüstriyel Siber Güvenlik Şirketi, 2022'nin İkinci Yarısını Kapsayan ICS Güvenlik Açıkları ve CVE Raporunu Yayınladı

ICS/OT siber güvenlik firması, 2022'nin ikinci yarısındaki CVE'lerin %35'inin yamalanamaz olduğunu ifade ediyor.

Erken aşama startup aşamasındaki bir ICS/OT siber güvenlik ve varlık izleme şirketi olan SynSaber, ikinci Endüstriyel Kontrol Sistemleri (ICS) Güvenlik Açıkları ve CVE'ler Raporu'nun yayınlandığını duyurdu. Rapor, aşağıdakileri belirlemek için 2022'nin ikinci yarısında CISA tarafından yayınlanan 920'den fazla CVE'yi analiz ediyor:

- Güvenlik açıklarını kim bildiriyor?
- Hangi çözümler (varsa) mevcuttur?
- Ciddiyet düzeyleri ve potansiyel etkileri nelerdir?
- Veriler, yılın ilk yarısında bildirilen CVE'lerle nasıl karşılaştırılır?

SynSaber'in CTO'su Ron Fabela, *"Yıllar geçtikçe, endüstriyel kontrol sistemlerinde bir güvenlik açığı ifşası seli yaşanıyor ve güvenlik topluluğu her bir açık noktasını düzeltmeye veya onarmaya çalışırken genellikle endişe yaratıyor - imkansız bir başarı"* dedi. *"Bu raporla amacımız, 920'den fazla CVE'yi analiz etmek ve hangi CVE'lerin en ciddiye alınması gerektiği ve hangilerinin kuruluşun risk yönetimi stratejisinin bir parçası olarak kabul edilebileceği konusunda ICS endüstrisi için öngörü toplamaktır."*

Önemli bulgular:

- 2022'nin ikinci yarısında bildirilen CVE'lerin %35'inin şu anda üreticiden temin edebileceği yama veya düzeltme yok (yılın ilk yarısında bu oran %13'tü).
- CVE'lerin %56'sı Orijinal Ekipman Üreticisi (OEM) tarafından bildirilirken, %43'ü güvenlik sağlayıcıları ve bağımsız araştırmacılar tarafından sunuldu (bu rakamlar 2022'nin ilk yarısıyla tutarlıydı).
- CVE'lerin %28'i, yararlanmak için sisteme yerel veya fiziksel erişim gerektirmektedir. (Bu oran 2022'nin ilk yarısında %23'idi).
- 2022'nin ikinci yarısında bildirilen CVE'lerin %22'si önceliklendirilebilir ve ele alınmalıdır. (organizasyon ve satıcı planlaması ile)

CISA ICS Önerileri ve diğer kuruluşlar aracılığıyla bildirilen CVE'lerin hacminin azalması muhtemel değildir. Varlık sahiplerinin ve kritik altyapıyı savunanların, iyileştirmelerin ne zaman mevcut olduğunu ve bu iyileştirmelerin nasıl uygulanması ve önceliklendirilmesi gerektiğini anlaması önem arz etmektedir.

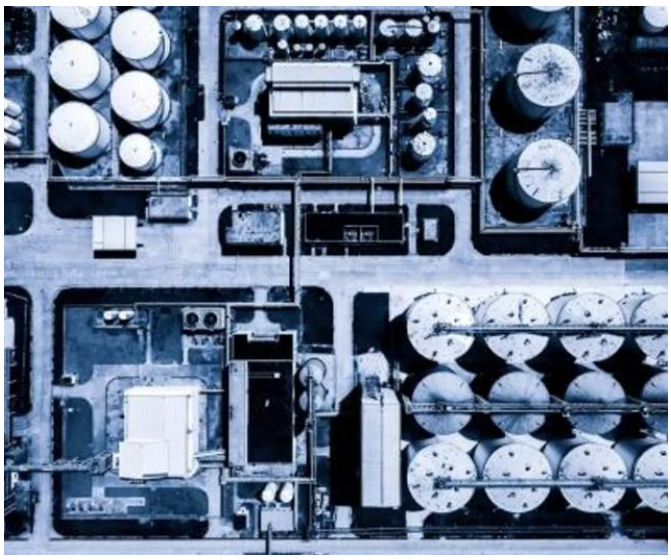
TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/synsaber-releases-ics-vulnerabilities-cves-report-covering-second-half-of-2022

19 Ocak 2023

ICSFUSION

1.6. Güvenli Olmayan Sunucular OT Ağlarını Tehlikeye Atıyor



Endüstriyel Siber güvenlik firması Claroty Team82'de güvenlik araştırmacısı olan Uri Katz, GE Proficy güvenlik açıklarına ilişkin tavsiyesinde, sunucuların bir kuruluşun IT ağı ile operasyonel teknoloji (OT) ağı arasında bir köprü olarak kullanılabileceğini belirtti.

Katz, *"IT ve OT ağları arasındaki benzersiz konumundan dolayı, saldırganlar historian sunucuları hedefliyor ve bu bileşenleri OT ağına bir pivot noktası olarak kullanabilirler,"* dedi ve ekledi: *"historian sunucular genellikle endüstriyel ağlar hakkında değerli veriler içerir. Proses verileri, performans ve bakım ile ilgili veriler de dahil olmak üzere tüm prosesler..."*

Operasyonel historian / süreç sunucular olarak da adlandırılan data histroian sunucuları, şirketlere endüstriyel kontrol sistemlerinden ve fiziksel cihaz ağlarından gelen verileri izleme ve analiz etme yeteneği verir. Esasen endüstriyel bir ortamda zaman serisi verilerini depolamak için bir veri deposu olan historian sunucular, kritik altyapı, üretim ve operasyonlar hakkında gerçek zamanlı bilgiler toplar.

Bununla birlikte, saldırganlar için data historian, bir ağın BT ve OT bölümleri arasında geçiş noktası olarak bir köprü oluşturur çünkü genellikle her ikisine de bağlı merkezi bir sunucudur. Bu nedenle, ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı'na (CISA) göre , historian sunucular, araya girme saldırıları ve veritabanı odaklı saldırılar dahil olmak üzere EKS ağlarında olası bir saldırı hedefi olarak görülmektedir.

CISA, BT ve OT ağlarını birleştirmek endüstriyel teknolojiyi daha çevik ve uygun maliyetli hale getirebilirken savunma stratejileri konulu belgede *"çoklu ağ entegrasyon stratejileri genellikle bir kuruluşun güvenliğini büyük ölçüde azaltan güvenlik açıklarına yol açar ve görev açısından kritik kontrol sistemlerini siber tehditlere maruz bırakabilir"* sözlerine yer verildi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/vulnerable-historian-servers-imperil-OT-networks

18 Ocak 2023

1.7. Yeni Amaçlar, Taktikler ve Kötü Amaçlı Yazılımlarla Silahlanmış Saldırganlar EKS'leri Tehdit Ediyor

Tehdit aktörleri, kritik altyapıya saldırmak için her yönden çeşitleniyor, tehdit ortamını bulandırıyor ve endüstriyel kuruluşları güvenliklerini yeniden düşünmeye zorluyor.

Yeni araştırmalara göre, kısmen Ukrayna'da devam eden ihtilafın körüklediği mali ve siyasi kazanç güdüsü, tehdit aktörlerini endüstriyel kontrol sistemlerini (ICS) her zamankinden daha yıkıcı siber saldırılara odaklanmaya teşvik etti ve kritik altyapılar için tehdit ortamını çeşitlendirdi.

Nozomi Networks'ün "OT/IoT Güvenlik Raporu: EKS'ye Derin Bir Bakış"a göre, saldırganların kendilerini yeni taktikler ve kötü amaçlı yazılımlarla donatarak işletmeleri 2023 boyunca devam etmesi tehdit etmesi bekleniyor.

Önceleri kötü amaçlı yazılım bileşenlerini bırakmak ve ağlara uzaktan erişim elde etmek için uzaktan erişim Truva Atlarını (RAT'ler) kullanarak ve dağıtık devre dışı bırakma saldırıları (DDoS) kullanarak ICS'ye yönelik saldırıları gerçekleştirenler devlet destekli tehdit gruplarıydı. Nozomi Networks güvenlik araştırmalarından Roya Gordon, saldırıların *"beklenmedik"* kesintiye neden olduğunu söylüyor. "*Tarihsel olarak, kritik altyapı kesintileri bir devlet destekli saldırı taktiği olarak görülüyordu"* diyor.

Bununla birlikte, Mayıs 2021'de artık kötü bir üne sahip olan Colonial Pipeline saldırısı, bu eğilimde önemli bir değişime işaret etti. Bu olayda, çalınan bir parolayla başlayan bir fidye yazılımı saldırısı, Amerika Birleşik Devletleri'nin doğusunda paniğe ve gaz kesintilerine neden oldu ve saldırganlar, yeni saldırı vektörlerinin ne kadar yıkıcı ve potansiyel olarak kazançlı olabileceğini fark etti.

Gordon, *"Colonial Pipeline saldırısı, siber suçluların, büyük ölçüde gerçek zamanlı verilere bağlı olma eğiliminde oldukları ve fidye taleplerini karşılama araçlarına sahip oldukları için, finansal kazanç için kritik altyapı üzerindeki fidye yazılımı saldırılarından nasıl yararlanabileceklerini gösterdi*" diye belirtiyor. Ardından, *"Rusya'nın geçen Şubat ayında Ukrayna'ya saldırmasıyla, endüstriyel kontrol sistemlerine yönelik saldırılar, geleneksel olarak veri ihlalleri ve DDoS saldırılarıyla tanınan bilgisayar korsanlarının, siyasi kazanç elde etmek için Ukrayna'daki demiryolları ve diğer kritik altyapılar gibi ulaşım sistemlerini ve diğer kritik altyapıları bozmak için yıkıcı silici kötü amaçlı yazılımlar kullanmasıyla siyasi bir hal aldı"* diyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/ics-ot/ics-confronted-by-attackers-armed-with-new-motives-tactics-and-malware

10 Ocak 2023

1.8. BART, Vice Society Veri İhlali İddialarını Araştırıyor

Vice Society, San Francisco ulaşım sistemini tehlikeye atmakla övünürken, BART operasyonları sürdürürken bir soruşturma başlattı.

San Francisco Körfez Bölgesi Hızlı Geçiş Sistemi (BART), ocak ayında fidye yazılımı grubu Vice Society tarafından en son kurbanları arasında listelendi.

Emsisoft'ta tehdit analisti olan Brett Callow, 6 Ocak'ta Vice Society BART paylaşımını işaret etti. Ancak BART'ın sözcüsü Alicia Trost, Dark Reading'e bir siber saldırı sonucunda herhangi bir hizmet kesintisi olmadığını ve bir soruşturmanın devam ettiğini söyledi.

Trost, Dark Reading'e e-posta ile *"Gönderilen verileri araştırıyoruz"* dedi. *"Açık olmak gerekirse, hiçbir BART hizmeti veya dahili iş sistemi etkilenmedi. Diğer devlet kurumlarında olduğu gibi, yanıt vermek için gerekli tüm önlemleri alıyoruz."*

Vice Society aynı zamanda ABD'de son zamanlarda meydana gelen bir dizi okul ihlalinin de arkasındaydı ve en son İngiltere'deki 14 okuldan oluşan bir gruptan çalınan kişisel bilgileri ifşa etti.

TESPİT YERİ:
Güvenlik Haberleri & Deep Web

KAYNAK:
https://www.darkreading.com/ics-ot/san-fran-bart-investigates-vice-society-data-breach
-

18 Ocak 2023

1.9. Endüstriyel Siber Güvenlik Şirketi Kritik Altyapılara Yapılan Siber Saldırılarda Önemli Artış Olduğunu Belirtti

Endüstriyel siber güvenlik şirketi Nozomi, 2022'nin ikinci yarısına ilişkin en son OT/IoT güvenlik raporunda, enerji, hastaneler, demiryolu ve imalat gibi hayati altyapılara yönelik yıkıcı ve kötü niyetli siber saldırıların hâlâ gözlemlendiğini ve önemli bir sorun olmaya devam ettiğini açıkladı. Firma ayrıca yıkıcı saldırılara, teknoloji kaynak kodunun çalınmasına ve silici kötü amaçlı yazılım kullanımına neden olan bilgisayar korsanlarını da izlediğini bildirdi.

Nozomi "Demiryollarına yönelik devam eden saldırılar, demiryolu operatörlerinin varlıklarını güvence altına almalarına yardımcı olacak yönergeleri harekete geçirdi. Hacktivistler, Rusya/Ukrayna savaşındaki siyasi duruşlarını ilerletmek için kritik altyapıya yıkıcı saldırılar başlatmak için silici kötü amaçlı yazılım kullanmayı seçtiler," şeklinde ifade ediyor. *"Siber tehditler geliştikçe ve yoğunlaştıkça, tehdit aktörlerinin kritik altyapıya gömülü Operasyonel Teknoloji (OT) ve Nesnelerin İnterneti (IoT) cihazlarını nasıl hedef aldığını anlamak önem arz ediyor."*
Ek olarak Nozomi, IoT honeypot içgörüleri ve hangi sektörlerin en savunmasız olduğunu belirlemek için ICS-CERT tavsiyelerinin analizini sağladı. Ayrıca, savunma mekanizmalarını güçlendirmek için tavsiyeler ve 2023'e hazırlanmaya yardımcı olmak için ortaya çıkan tehditler hakkında bir tahmin sundu.

Nozomi, İran'daki üç büyük çelik şirketinin geçen yılın Haziran ayının sonundan Temmuz ayına kadar devam eden bir siber saldırıya uğradığını bildirdi. Web sitesi ve üretim hattında aksamalara neden olan bu saldırılar, Gonjeshke Darandethat adlı bilgisayar korsanlığı yanlısı bir grup tarafından üstlenildi. *"Bu grup daha önce, yılın başlarında İran tren sistemine kötü amaçlı yazılım yerleştiren bir siber saldırının sorumluluğunu üstlenmişti. Bu olay, amaçları veya bağlantıları ne olursa olsun, kötü niyetli aktörlere karşı kritik altyapının savunmasızlığını gün ışığına çıkarıyor."*

Ağustos ve Eylül ayları arasında imalat, petrol, su ve elektrik dağıtım şirketlerine yönelik çok sayıda yıkıcı saldırı gerçekleşti.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/reports/nozomi-reports-significant-rise-in-cyberattacks-disrupting-critical-infrastructure-landscape-as-rats-targeted-ot/

17 Ocak 2023

1.10. Siber Güvenlik Şirketi Raporu, Kimlik Avı Veri Kümesinden Elde Ettiği Veriler İle OT Güvenliğine Işık Tutuyor

Mandiant araştırmacıları, 2022'de dünya çapındaki kuruluşlara teslim edilen 1700'ün üzerinde benzersiz, endüstriyel temalı kimlik avı örneğinden oluşan bir veri kümesini analiz ettiklerini söyledi. Ekip, milyonlarca örnek arasında arama yapmak ve kimlik avı e-postalarını tam olarak belirlemek için endüstriyel anahtar sözcüklerden oluşan özel bir dizi kullanarak veri kümesini oluşturdu.

Araştırmacılar, *"Potansiyel endüstriyel hedefli saldırıları avlamakla görevli savunucular, daha yüksek riskli tehditlere odaklanmak için genel kimlik avı girişimlerinin gürültüsünü ayıklayabilir ve basit tavizlerin, kritik üretim sistemlerini etkileyen daha etkili olaylara dönüşmesini engelleyebilir"* şeklinde ifade ettiler. *"Bu tehdit aktörlerinin hedefleri, operasyonel teknoloji (OT) sistemleri için çok az risk oluşturuyor gibi görünse de, tekniklerinin hızlı doğası ve profesyonelliği, OT savunucuları için geniş etkilere sahip."*

Mandiant, bilgisayar korsanlarının enerji, üretim ve su hizmetleri gibi endüstriyel sektörlere özgü terminoloji ve kavramlar içeren kimlik avı e-postaları yaydığını düzenli olarak gözlemlemiştir. Endüstriyel temalı yemlerin ve kimlik avı e-postalarının kullanılması, en azından bazı durumlarda, aktörlerin saldırılarını endüstriyel kuruluşları hedef alacak şekilde düzenlediklerini gösteriyor.

Araştırmacılar, kimlik avı kampanyalarının yem karmaşıklığı, araçları, hacmi ve hedefleri bakımından farklılık gösterdiğini söyledi. Bununla birlikte, çoğu kimlik avı kampanyasının ortak noktası, bir görevin en erken aşamalarını temsil ettikleri göz önüne alındığında, bir aktörün nihai hedefleri hakkında çok az bağlam ortaya koymalarıdır. Belirli kurbanları hedef almayan görünüşte basit kimlik avı, iş e-postasının ele geçirilmesi (BEC), fidye yazılımı dağıtımı, casusluk, veri sızıntıları veya siber-fiziksel saldırılar gibi tamamen farklı konseptlere ilişkin faaliyetler yayılabilir/çeşitlenebilir.

Mandiant, *"Endüstriyel temalı kimlik avı e-postaları, OT ile çalışan çalışanlar için yaygın olan özel bir dil kullandıklarından özellikle risklidir"* dedi. *"Bir kimlik avı kampanyası yürüten tehdit aktörü, kendi başına ciddi hasara neden olacak kadar uzmanlığa sahip olmasa bile, aktörler genellikle diğer aktörlerin kullanması için erişimi paylaşır, satar veya dağıtır…"*

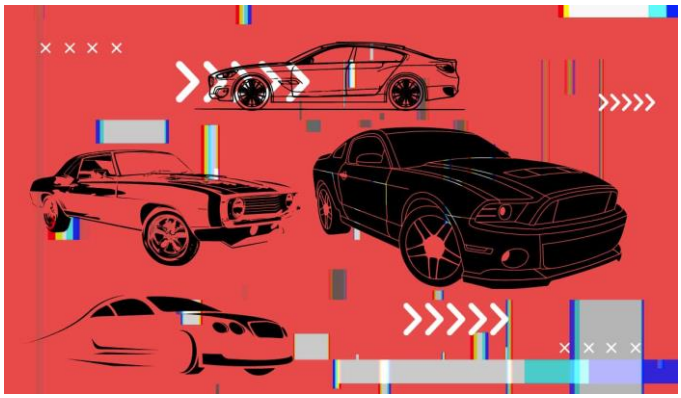
TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.mandiant.com/resources/blog/phishing-hunting-industrial-emails
https://industrialcyber.co/ransomware/mandiant-details-malicious-industrial-themed-phishing-emails-warns-of-broad-implications-for-ot-defenders/

9 Ocak 2023

ICSFUSION

1.11. Otomotiv Endüstrisi Kritik Dereceli API Güvenlik Açıklarından Etkileniyor



Etkilenen otomotiv devleri arasında BMW, Toyota, Ford, Honda, Mercedes-Benz ve çok daha fazlası yer alıyor.

Bu API güvenlik açıkları, araçları bilgi hırsızlığına, hesapların ele geçirilmesine, uzaktan kod yürütmeye (RCE) ve hatta motorları çalıştırma ve durdurma gibi fiziksel komutların ele geçirilmesine maruz bıraktı.

Bu açıklıklar 16 farklı üreticiye ait milyonlarca araç, arabaların kilidini açmak, çalıştırmak ve takip etmek için kötüye kullanılabilecek ve aynı zamanda araç sahiplerinin mahremiyetini etkileyebileceğini göstermektedir.

Bu güvenlik açıkları, araştırmacılar Neiko Rivera, Brett Buerhaus, Maik Robert, Ian Carroll, Justin Rhinehart ve Shubham Shah ile birlikte otomotiv endüstrisinin güvenlik eksikliklerine derinlemesine araştırma yapan güvenlik araştırmacısı Sam Curry tarafından bulundu.

Ayrıntılı bir raporda Curry, aşağıdakiler de dahil olmak üzere birçok otomotiv devine güç sağlayan otomotiv API'lerinde bulunan güvenlik açıklarını ortaya koydu. Açıklıklardan etkilenen başlıca markalar şu şekilde:

- Kia
- BMW
- Ford
- Honda
- Acura
- Jaguar
- Nissan
- Porsche
- Toyota
- Ferrari
- Spireon
- Reviver
- Genesis
- Hyundai
- Infiniti
- SiriusXM
- Land Rover
- Rolls Royce
- Mercedes-Benz

Araştırmacılara göre, hesapların ele geçirilmesi için bilgi hırsızlığı, uzaktan kod yürütme (RCE) ve hatta arabaların motorlarını çalıştırma ve durdurma gibi fiziksel komutları yürütmek mümkündü.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.hackread.com/automotive-industry-api-vulnerabilities/

19 Ocak 2023

1.12. Dünya Ekonomik Forumu: Petrol ve Gaz Endüstrisinde Siber Dayanıklılık Sağlanmalı

Petrol ve gaz endüstrisi, siber saldırılara karşı giderek daha savunmasız hale gelen çeşitli karmaşık sistemler ve teknolojiler kullanıyor.

Sektörün siber güvenlik durumunu iyileştirmek için Dünya Ekonomik Forumu, Petrol ve Gazda Siber Dayanıklılık girişimini oluşturdu. Siber Dayanıklılık Taahhüdü aracılığıyla, 20'den fazla küresel CEO, ekosistem genelinde siber dayanıklılığı iyileştirmek için birlikte çalışmayı taahhüt etti.

Petrol ve gaz endüstrisi, petrol ve gaz ürünlerini çıkarmak, taşımak ve rafine etmek için bir dizi karmaşık sistem ve birbirine bağlı teknoloji kullanır. Bu teknolojiler, enerji hizmetlerinin ve ürünlerinin dağıtımını desteklemek için gerekli olsa da, siber saldırılara karşı giderek daha savunmasız hale geliyor ve bu nedenle toplu dayanıklılık için siber güvenliği kritik hale getiriyor.

Dünya Ekonomik Forumu'nun Siber Güvenlik Merkezi, birden çok sektörde siber güvenliği güçlendirme çabalarının bir parçası olarak 2020'de Petrol ve Gazda Siber Dayanıklılık girişimini başlattı. Girişim, siber dayanıklılık konusunda ekosistemi büyütmek için birlikte çalışan 40'tan fazla kamu ve özel kuruluştan oluşan bir topluluktan oluşuyor.

Topluluğun en önemli girişimlerinden biri de Siber Dayanıklılık Taahhüdüdür. Bu doküman siber dayanıklılığa ortak bir yaklaşım benimsemeye ve sektördeki dijital altyapıyı ve varlıkları korumaya kendini adamış 21 petrol ve gaz baş yöneticisi tarafından onaylandı.

Taahhüdü onaylayanlar arasında Aker, Check Point Software Technologies, Claroty, Cognite, Dragos, Ecopetrol, Eni, EnQuest, Galp, Global Resilience Federation, Institute for Security and Safety (ISS), KnowBe4, Maire Tecnimont, Occidental, OT- ISAC, PETRONAS, Repsol, Shell, Suudi Aramco, Schneider Electric ve Suncor Energy bulunuyor.

Siber Dayanıklılık Taahhüdünü imzalayarak, tüm taraflar, siber farkındalığa sahip ve dayanıklı bir kurum kültürü geliştirme sürecinde liderlere ve yönetim kurulu üyelerine rehberlik edecek siber dayanıklılık ilkelerini onayladı.

"Tek başına çalışan bir şirket, ön kapıyı kilitleyip arka kapıyı ardına kadar açık bırakmak gibidir. Dünya çapında milyarlarca insanın bağlı olduğu kritik enerji altyapısını gerçekten korumak istiyorsak birlikte çalışmalıyız." — Amin H. Nasser, Suudi Aramco Başkanı ve CEO'su

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.weforum.org/impact/cyber-resilience-oil-and-gas/

3 Ocak 2023

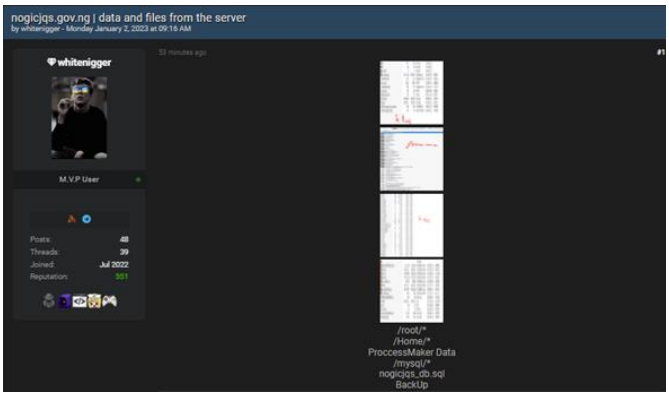
1.13. Nijerya Petrol ve Gaz Sektörü Saldırı Altında, Bilgisayar Korsanları NOGIC Verilerini Sızdırıyor

Gelen haberler Nijerya Petrol ve Gaz Endüstrisi İçeriği Ortak Yeterlilik Sistemi (NOGIC) JQS portalına erişilemediğini yönünde…

Bilinmeyen bir tehdit aktörü, Nijerya Petrol ve Gaz Endüstrisi İçerik Ortak Yeterlilik Sistemini (nogicjqs.gov.ng) hedef aldı ve verilerini, yedeklemeler ve MySQL verileri de dahil olmak üzere dosya listelerini gösteren örnek resimlerle birlikte hacker forumunda yayınladı.

Şu anda, Nijerya Petrol ve Gaz Endüstrisi İçeriği Ortak Yeterlilik Sistemi (NOGIC) JQS portalına erişilemiyor ve "bakım aşamasında" uyarısı alınmaktadır. Web sitesi (nogicjqs.gov.ng), uygulamanın güncellemelerden geçtiğini belirtiyor.

Bir tehdit aktörü, 2 Ocak'ta bilgisayar korsanı forumunda verilerin ekran görüntülerini yayınladı. Bu olayın arkasındaki saldırganların kimliği şu ana kadar belirlenemedi. Sözde fidye yazılımı saldırısının sorumluluğunu hiçbir grup üstlenmedi.



Figür 1: Bir yeraltı forumunda çalınan veri örneklerini gösteren gönderi.

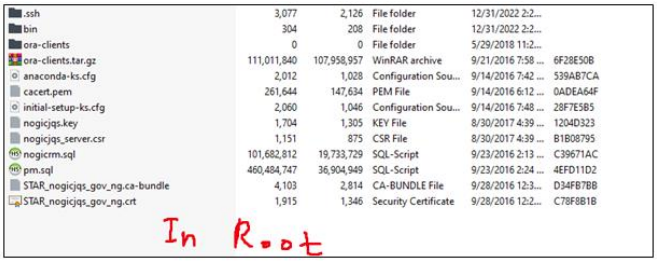


Figure 2: Çalınan veri örnekleri.

Nijerya petrol ve gaz endüstrisi, petrol hırsızlığı tartışması, fiyat artışı ve Escravos nehrinde petrol tabakalarının keşfedilmesiyle haberlerde yer aldı. Raporlara göre Nijerya, Afrika'nın birincil petrol sağlayıcısı ve günlük 1,2 milyon varil petrol üretiyor.

NOGIC JQS Web Sitesi

NOGIC JQS web sitesi, Nijerya petrol ve gaz endüstrisindeki yüklenicilerin kaydı, deniz aracı kaydı, doğrulama, ulusal beceri geliştirme için veritabanları, denizcilik destek tedarikçilerinin sınıflandırılması, gurbetçi kota uygulama yönetimi, ihale yönetimi vb. hizmetler sunmaktadır…

TESPİT YERİ:
Dark Web & Güvenlik Haberleri

KAYNAK:
https://thecyberexpress.com/nigerian-oil-gas-sector-hackers-target-nogic/
-

4 Ocak 2023

1.14. New York, Enerji Şebekelerini Siber Saldırılardan Koruyan Yasayı Kabul Etti

Mevzuat, kamu hizmetlerinin yıllık acil durum müdahale planlarında siber saldırılara hazırlanmalarını gerekli kılıyor.

New York Valisi Kathy Hochul, eyaletin enerji şebekesi için siber güvenlik korumaları oluşturmaya yönelik yasayı imzaladı.

Mevzuat (A.3904B/S.5579A olarak belirlenmiş), kamu hizmetlerinin tıpkı fırtına veya diğer tehlikeler için olduğu gibi yıllık acil durum müdahale planlarında siber saldırılara da hazırlanmasını gerektirecektir. Yeni korumalar aynı zamanda Kamu Hizmeti Komisyonu'na kritik altyapı ve müşteri verilerinin güvenliğini sağlamak için gelişmiş denetim yetkileri de veriyor.

Valilik, bu eylemin kritik altyapıya yönelik siber saldırılarda küresel bir artış olduğu sırada alındığını ve New York'un elektrik şebekesinin güvenilir ve güvenli kalmasını sağlayacağını söyledi.

Hochul, *"İlk modern elektrik şebekesi New York Eyaletinde inşa edildi ve 140 yıl sonra, siber güvenliğimizi güçlendirerek tüm New Yorklular için ışıkları açık tutmak için öncü adımlar atmaya devam ediyoruz."* dedi. *"Dünyanın finans başkenti ve temiz enerji lideri olarak New York'un bilgisayar korsanları için bir hedef olduğunu anlıyoruz. Bu kritik yasa, güvenilir elektrik hizmetlerine bağımlı olan milyonlarca New Yorklunun korunmasına yardımcı olacak ve temiz enerjiye sorunsuz bir erişim sağlayacaktır."*

Hem New York Eyalet Meclisi'nde hem de New York Eyalet Senatosu'nda oybirliğiyle kabul edilen A.3904B/S.5579A Mevzuatı, yerel dağıtım sistemi için korumaları güçlendiriyor ve kamu hizmetlerinin kritik altyapıyı siber saldırılara karşı güvence altına almasını şart koşuyor.

Bu eylem, Başkan Joe Biden'ın, enerji sistemi de dahil olmak üzere kritik altyapı için eyaletin belirlediği minimum siber güvenlik gereksinimlerini talep etmesinin ardından geldi. Son on yılda birçok örnekte, siber saldırıların elektrik şebekelerini kapatabileceği kanıtlanmıştır.

TESPİT YERİ:
Sektör Haberleri

KAYNAK:
https://www.tdworld.com/transmission-reliability/article/21257350/new-york-adopts-law-protecting-power-grid-from-cyber-attacks

18 Ocak 2023

1.15. DNV Gemi Yönetim Yazılımına Yönelik Fidye Yazılımı Saldırısı 1.000 Gemiyi Etkiledi

Norveç merkezli DNV, gemi yönetim yazılımına yönelik bir fidye yazılımı saldırısının 1.000 gemiyi etkilediğini söyledi.

Norveç merkezli endüstriyel risk yönetimi ve güvence çözümleri sağlayıcısı DNV, gemi yönetim yazılımına yönelik yakın tarihli bir fidye yazılımı saldırısının 1.000 gemiyi etkilediğini söyledi.

DNV, 9 Ocak'ta ShipManager yazılımının 7 Ocak'ta şirketi ilgili sunucuları kapatmaya zorlayan bir siber saldırıda hedef alındığını açıkladı.

17 Ocak'ta paylaşılan bir güncellemede şirket, 70 müşterisini ve yaklaşık 1.000 gemiyi etkileyen bir fidye yazılımı saldırısında hedef alındığını açıkladı.

DNV bir basın açıklamasında: *"DNV tarafından sağlanan başka herhangi bir yazılım veya verinin etkilendiğine dair hiçbir belirti yok. Sunucu kesintisi diğer DNV hizmetlerini etkilemez"* dedi.

Saldırının arkasında hangi fidye yazılımı grubunun olduğu ve herhangi bir verinin çalınıp çalınmadığı belli değil. SecurityWeek birkaç büyük grubun web sitelerini kontrol ettiğini akarsa da DNV'den hiç söz edilmedi. Bununla birlikte, tehdit aktörleri genellikle kurbanların adını verirdiğini ve yalnızca ilk müzakereler başarısız olduktan sonra çalıntı verileri sızdırmakla tehdit ettiği bilinmektedir.

DNV, denizcilik, enerji, petrol ve gaz, otomotiv ve havacılık, yiyecek ve içecek ve sağlık sektörleri için geniş bir hizmet yelpazesi sunmaktadır. Şirketin denizcilik endüstrisi için ShipManager yazılımı, gemi yönetimi operasyonları ve gemi tasarımı için tasarlanmıştır.

DNV, web sitesinde dünya çapında 300 nakliye şirketinin denizcilik yazılımını 6.000'den fazla gemi için kullandığını söylüyor.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/ransomware-attack-dnv-ship-management-software-impacts-1000-vessels/

12 Ocak 2022

1.16. 100'den Fazla Siemens PLC Modelinde Firmware Takeover Güvenlik Açığı Bulundu

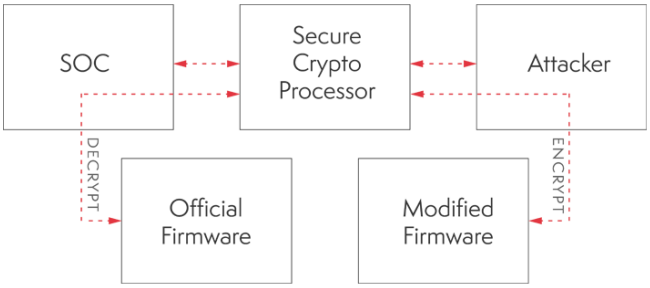
Güvenlik araştırmacıları, Siemens SIMATIC ve SIPLUS S7-1500 programlanabilir mantık denetleyicilerinde (PLC'ler), kötü niyetli bir aktör tarafından etkilenen cihazlara gizlice ürün yazılımı yüklemek ve bunların kontrolünü ele geçirmek için kullanılabilecek çok sayıda mimari güvenlik açığını ortaya çıkardı.

Red Balloon Security tarafından keşfedilen sorunlar CVE-2022-38773 (CVSS puanı: 4.6) olarak izlenmektedir.

Şirket, açıklıkların *"saldırganların korumalı tüm önyükleme özelliklerini atlamasına izin vererek verilerin kalıcı olarak keyfi olarak değiştirilmesine neden olabileceğini"* söyledi. İlgili zafiyetten 100'den fazla modelin etkinlendiği belirtilmektedir.

Açıklığın ciddi bir sonucu, tehdit aktörüne kötü amaçlı kod yürütme ve herhangi bir alarm oluşmadan cihazların tam kontrolünü ele geçirme yeteneği verebilmesidir.

Araştırmacılar, *"Bu keşfin, endüstriyel ortamlar için potansiyel olarak önemli etkileri var, çünkü bu açıklık, S7-1500 verilerinin kalıcı olarak keyfi olarak değiştirilmesine neden olabilir."*



Siemens, bu hafta yayınlanan bir duyuruda, planlanmış herhangi bir yama olmadığını söyledi, ancak donanım seviyesi saldırıları önlemek için işlemelere fiziksel güvenlik önlemlerini almaya yönlendirdi.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://thehackernews.com/2023/01/over-100-siemens-plc-models-found.html

10 Ocak 2023

1.17. Copper Mountain Mining, Fidye Yazılımı Saldırısının Ardından Operasyonel Üretime Devam Ediyor

Copper Mountain Mining, Aralık ayı sonlarında Copper Mountain Madenindeki BT sistemlerini ve şirket ofisini etkileyen fidye yazılımı saldırısı hakkında operasyonel bir güncelleme yayınladı. Şirket, üretimin yeniden başladığını ve bu kesinti süresi boyunca maden envanterinden Vancouver Limanı'na bakır konsantresi naklettiğini ve planlanan nakliye programını sürdürdüğünü doğruladı.

Kanadalı madencilik şirketi haftalık güncellemesinde, *"1 Ocak'ta Şirket, Copper Mountain Madenindeki birincil kırıcının faaliyetlerine yeniden başladı ve kısa bir süre sonra da Şirket, saldırının ardından önleyici olarak kapatılan fabrikadaki faaliyetlerine yeniden başladı"* dedi. *"4 Ocak'ta değirmen tam üretimdeydi ve kalan iş sistemleri tamamen restore edildiğinden operasyon şu anda stabilize ediliyor."*

Bildiride, Copper Mountain Mining'in harici ve dahili BT ekiplerinin, harici siber güvenlik uzmanlarıyla birlikte şirkete yönelik daha fazla riskleri azaltmak için aktif olarak ek önlemler almaya devam ettiği de eklendi. *"Şirketin birincil hedefi, tam iş işlevselliğine güvenli ve emniyetli bir şekilde geri dönmek olmaya devam ediyor"* diye ekledi.

Kanada, Vancouver merkezli madencilik şirketine yönelik fidye yazılımı saldırısı, şirketin Kuzey Amerika ve Avustralya'daki operasyonlarını etkileyen JBS USA'ya yönelik Haziran 2021 saldırısına benzer. Şirket, ABD yönetimine *"bir fidye yazılımı saldırısının kurbanı olduklarını"* bildirdi ve yönetime fidye talebinin Rusya merkezli olması muhtemel bir suç örgütünden geldiğini bildirdi.

Copper Mountain Mining, Aralık ayı sonlarında fidye yazılımı saldırısını doğruladı ve izole operasyonlar, mümkün olduğunda manuel süreçlere geçti ve fabrika, kontrol sistemi üzerindeki etkisini belirlemek için önleyici aksiyon olarak kapatıldı.

TESPİT YERİ:
Deep Web & Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/critical-infrastructure/copper-mountain-mining-resumes-operational-production-following-ransomware-attack/
-

13 Ocak 2023

1.18. Siber Güvenlik Şirketi: Küresel Olarak Enerji, Sağlık ve Perakende Sektörleri İçin 2022 Siber Saldırı Trend

Darktrace, küresel müşteri filosunda gözlemlenen 2022 saldırı verilerini ortaya koyan üç yeni siber tehdit trend raporu yayınladı. Sektör raporları enerji, sağlık ve perakende sektörlerini kapsamaktadır.

Darktrace Küresel Tehdit Analizi Başkanı Toby Lewis, *"Darktrace tarafından yayınlanan, türünün ilk örneği olan bu sektöre özel raporlar, savunma yaptığımız hızla gelişen tehdit ortamının temelini oluşturan verileri ortaya çıkarmak için önemli bir çabayı temsil ediyor"* yorumunu yaptı.

"Eğilimler, bilgisayar korsanlarının enerji sektörünün kaynaklarını kripto hırsızlığı biçiminde çekme eğiliminden, sağlık sektöründe veri hırsızlığına yol açan hasta verilerinin paha biçilmez doğasına kadar sektöre özgü önemli zorlukları ortaya koyuyor" yorumunda bulundu. Lewis. *"Perakende sektöründe kimlik bilgilerine dayalı saldırılardaki artış, kimlik hırsızlığının 2023 için önemli bir trend olacağı gerçeğini yansıtıyor; bu da, çalışanların eylemlerini zengin bağlamda anlamak ve belirli kimlik bilgileri kullanılarak gerçekleştirilen eylemleri doğrulamak için yapay zeka tabanlı davranış analitiğine olan ihtiyacı artırıyor."*

Enerji Sektörü: Önemli Bulgular

Darktrace'in enerji sektörü raporu, küresel bir enerji krizinin arka planında, kötü aktörlerin diğer cihaz ve ağlardan enerji ve işlem gücü çaldığı yasadışı kripto madenciliği tehditlerinin sektörde yükselişte olduğunu ortaya koyuyor. Önemli bulgular şunları içeriyor:

- Yüksek öncelikli kripto madenciliği, 2021'e kıyasla 2022'de Birleşik Krallık enerji sektöründe gözlemlenen tüm siber olayların 13 kat fazlasını oluşturdu.
- Yüksek öncelikli kripto madenciliği, 2021'e kıyasla 2022'de ABD enerji sektöründe gözlemlenen tüm siber olayların 3 kat fazlasını oluşturdu.

Rapor, her ikisi de Darktrace'in AI teknolojisi tarafından durdurulan sırasıyla bir Avrupa ve ABD enerji kuruluşundan elde edilen iki gerçek dünya kripto - madencilik tehdidi bulgusunu ifşa ediyor. Önceki durumda, saldırganlar kuruluştaki 5 dahili sunucuyu kullanarak toplu kripto madenciliği yeteneklerini bir araya getirmeye çalışırken yakalandı…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/attacks-breaches/darktrace-publishes-2022-cyberattack-trend-data-for-energy-healthcare-retail-sectors-globally

12 Ocak 2023

1.19. Küresel Enerji Sistemlerinin Güvenliği: Siber Fiziksel Güvenlik

Enerji, fidye yazılımı çeteleri ve merkezi olmayan cihazlar için artan mali ödüllerle devlet destekli tehdit aktörleri tarafından yürütülen hem fiziksel hem de siber güvenlik savaşı için yeni savaş alanı haline geldi.

Dünyanın kritik ulusal altyapısına (CNI) yönelik fiziksel tehdit hiç bu kadar büyük olmamıştı. Bir zamanlar Rus gazını Almanya'ya taşıyan Kuzey Akım 1 ve 2 yeraltı boru hatlarının en az 50 metresi, Eylül 2022'nin sonlarında düzenlenen bir saldırıda kesintiye uğratıldı, ancak kimin suçlanacağı belirsizliğini koruyor.

Daha yakın zamanlarda Rusya, Ukrayna'daki savaşını kendi füzeleri ve İran tarafından sağlanan Shahed-136 insansız hava araçlarıyla enerji altyapısını hedef almaya kaydırdı. Ukrayna Devlet Başkanı Volodymyr Zelensky'nin 18 Ekim'de attığı tweet'e göre, *"Ukrayna'daki elektrik santrallerinin %30'u yıkıldı ve ülke çapında büyük elektrik kesintilerine neden oldu"*, 1 Kasım'da ise Avrupa Komisyonu Enerji Komiseri Kadri Simson ile yaptığı görüşme sırasında, Zelensky, *"ülkenin enerji sistemlerinin %30 ila % 40'ı yok edildi"* dedi.

Büyüyen Siber Güvenlik Tehdidi

Bununla birlikte, Ukrayna'daki savaştan kaynaklanan fiziksel güvenlik tehditleri ve Doğu ile Batı arasındaki artan gerilimler, CNI'mıza yönelik tek ciddi tehdit değildir. Büyüyen bir siber güvenlik tehdidi de var. 7 Mayıs 2021'de, Houston, Teksas'tan çıkan ve güneydoğu ABD'ye benzin ve jet yakıtı taşıyan Colonial Pipeline, bir fidye yazılımı saldırısını kontrol altına almak için tüm operasyonlarını durdurmak zorunda kaldı.

Bu saldırıda bilgisayar korsanları, çalışanların Dark Web'de bulunan tek bir kullanıcı adı ve parolayı kullanarak şirketin sistemlerine uzaktan erişmesine izin veren bir VPN (sanal özel ağ) hesabı aracılığıyla giriş elde etti. Colonial, Rusya bağlantılı siber suç grubu Darkside'ın üyesi olan bilgisayar korsanlarına saldırıdan kısa bir süre sonra 4,4 milyon dolar fidye ödedi.

Bir yıldan kısa bir süre sonra, GRU'nun Rus siber askeri birimi tarafından işletildiği iddia edilen bir tehdit grubu olan Sandworm, adı açıklanmayan bir Ukraynalı güç sağlayıcının çalışmasını engellemeye çalıştı. Ukrayna Devlet Özel İletişim ve Bilgi Koruma Servisi yaptığı açıklamada: *"Saldırganlar, hedeflerinin çeşitli altyapı bileşenlerini ele geçirmeye çalıştı: Elektrik trafo merkezleri, Windows ile çalışan bilgi işlem sistemleri, Linux ile çalışan sunucu ekipmanı ve SSSCIP…"* söyledi…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.darkreading.com/physical-security/securing-the-world-s-energy-systems-where-physical-security-and-cybersecurity-must-meet

28 Ocak 2023

1.20. NATO, Rusya'nın Altyapılarına Yönelik 'Siber Saldırıları Modelliyor'

İngiltere'nin üst düzey diplomatlarından biri, İngiltere'nin Rusya'nın enerji tesislerini hacklemek için eğitim aldığını söyledi.

İngiltere'nin dışişleri bakan yardımcısı Oleg Syromolotov Cumartesi günü yaptığı açıklamada, İngiltere'nin Rusya'nın kritik altyapısına yönelik siber saldırıları modellediğini söyledi. Simüle edilen saldırıların enerji tesislerini içerdiği ve NATO'nun rehberliğinde yürütüldüğünü de sözlerine ekledi.

Bakan yardımcısı, yabancı aktörler tarafından Rus hükümet kuruluşlarına yönelik saldırı girişimlerinin geçen yıl boyunca *"iki ila üç kat arttığını"* belirtti.

Syromolotov, The Times tarafından geçen ay yayınlanan ve Birleşik Krallık stratejik komutanlığı komutan yardımcısı Korgeneral Tom Copinger-Symes'in Ulusal Siber Gücün Rus diplomasına sahip kişileri işe almak istediğini söylediği bir habere tepki gösteriyordu.

TASS haber ajansına konuşan Syromolotov, *"İngilizler, saldırı yeteneklerini Rusya'nın enformasyon [sektörünü] hedef almak için sistematik olarak kullanıyor"* dedi. Londra'nın düzenli olarak ortak NATO tatbikatları da dahil olmak üzere *"Rus kritik altyapısına"* yönelik saldırıları simüle eden tatbikatlar yaptığını da sözlerine ekledi.

Diplomat, *"Kaliningrad Bölgesi'ndeki devlet kurumlarına ve Moskova'nın enerji sistemine yönelik saldırı modellerini içeriyor"* dedi. Kaliningrad Bölgesi, Baltık Denizi'nde Polonya ve Litvanya ile sınır komşusu olan bir Rus alanıdır.

Syromolotov, geçen yıl Rusya'nın "*yurt dışından eşi benzeri görülmemiş siber saldırılar"* tarafından vurulduğunu ve izinsiz girişlerin çoğunun ABD ve diğer NATO üyelerinin yanı sıra Ukrayna'dan geldiğini söyledi.

Syromolotov'a göre en çok devlet hizmetleri hedef alındı. *"Dışişleri Bakanlığı defalarca saldırıya uğradı"* dedi. *"Genel olarak, geçen yıl yaklaşık 50.000 bilgisayar korsanı saldırısı püskürtüldü."*

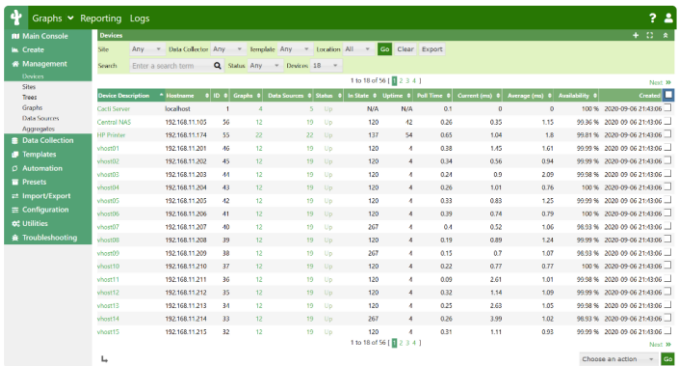
Basın servisine göre, 11 Nisan 2022'de, Rusya'nın Kozmonotluk Günü kutlamalarının arifesinde, bilgisayar korsanları ülkenin uzay ajansı Roscosmos'un web sitesini hedef aldı. Yine geçen yıl, davetsiz misafirler, bazı dahili belgeleri sızdırarak Rus ulusal posta hizmetinin yüklenicilerinden birinin veri tabanına erişim sağladılar…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.azerbaycan24.com/en/nato-state-modeling-cyber-strikes-on-russian-infrastructure-moscow/

13 Ocak 2023

1.21. Çoğu Cacti Kurulumu, İstismar Edilen Güvenlik Açığına Karşı Savunmasız



İnternete açık olan Cacti kurulumlarının çoğu, saldırılarda istismar edilen kritik öneme sahip bir komut enjeksiyon güvenlik açığına karşı yamalanmamıştır.

Operasyonel bir izleme ve hata yönetimi çerçevesi sunan açık kaynaklı bir web tabanlı ağ izleme ve grafik aracı olan Cacti, veri kaydetme aracı RRDtool için bir ön yüz uygulamasıdır.

Aralık 2022'nin başlarında, saldırganların Cacti çalıştıran sunucuda kod yürütmesine izin verebilecek bir kritik öneme sahip (CVSS puanı 9.8) komut enjeksiyon açıklığı olan CVE-2022-46169 için yamalar yayınlandı.

5 Aralık'ta yayınlanan Cacti sürümleri 1.2.23 ve 1.3.0, bu güvenlik açığı için düzeltme eklerini içercecek şekilde güncellenmiştir.

SonarSource'un 3 Ocak'ta CVE-2022-46169'un teknik analizini yayınlamasından birkaç gün sonra, Shadowserver Foundation, güvenlik açığını hedefleyen ilk istismar girişimlerini kaydettiği konusunda uyardı.

"…Cacti'nin kimliği doğrulanmamış uzaktan komut enjeksiyonu CVE-2022-46169 için istismar girişimlerini tespit etmeye başladık. Bunlar 3 Ocak'ta başladı. Shadowserver, yama uyguladığınızdan ve Cacti örneğinizi İnternet'e açık bırakmadığınızdan emin olun" denildi.

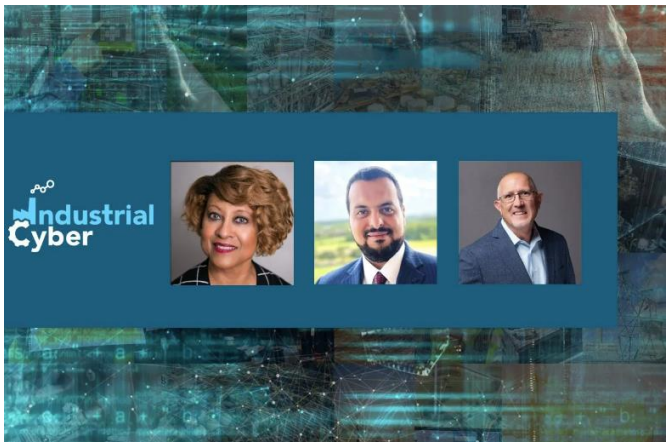
Bu hafta, saldırı yüzey yönetimi şirketi Censys, belirlediği 6.400 internet erişimli Cacti ana bilgisayarından yalnızca 26'sının aracın yamalı bir sürümünü çalıştırdığını ortaya çıkardı. Bu sunucuların çoğu Brezilya'da bulunuyor ve Endonezya ve ABD ilk üçe giriyor…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.securityweek.com/most-cacti-installations-unpatched-against-exploited-vulnerability/

15 Ocak 2023

1.22. Kritik Altyapı Sektörlerinde Fidye Yazılımı Saldırılarıyla Başa Çıkmak İçin Önleyici Mekanizmaları Oluşturmak



Kritik altyapı siteleri, son haftalarda ve aylarda fidye yazılımı saldırıları için ana odak noktasına dönüştü. Tehdit aktörleri hastaneleri, bir demiryolu şirketini, bir nakliye limanını, bir maden sahasını, bir posta dağıtım hizmetini ve devlet kurumlarını hedef alarak bu tür yıkıcı saldırıları istisnadan ziyade kural haline getirdi. Bu yükselen ve tehlikeli eğilimle başa çıkmak için, kritik altyapı sektörlerindeki kuruluşlar, bu sitelerdeki güvenlik açıklarını belirleyip ele almanın ve siber tehditlere karşı caydırıcılık seçenekleri için federal stratejiler geliştirmenin dışında, müttefiklerle koordinasyonu artırmalı, uygun siber güvenlik standartları geliştirmeli ve paylaşmalıdır.

Elektrik, su, telekom, ısıtma, ulaşım ve finansal hizmetler gibi kritik hizmetlere erişim esastır ve tipik olarak kritik altyapı sektörleri altında tanımlanır. Kritiklikleri, onları bir İnternet bağlantısından biraz daha fazlasıyla altyapıyı bozabilen ve bozan siber saldırganlar için ilgi çekici hedefler haline getiriyor.

Siber suç tehdit istihbaratı firması KELA tarafından yayınlanan veriler, 2022'de çeşitli platformlarda bilgisayar korsanları tarafından yaklaşık 2800 fidye yazılımı ve gasp saldırısı kurbanının iddia edildiğini ortaya koydu. Kurbanlar yaklaşık 60 farklı platformda listelendi ve bu kaynakların yaklaşık yüzde 52'si yalnızca 2022'de ortaya çıktı. KELA tarafından gözlemlenen müzakerelere göre ortalama fidye talebi yaklaşık 3,7 milyon ABD dolarıydı.

Geçen yıl KELA, gerçekten fidye yazılımı kullanan gruplar ile şifreleme kötü amaçlı yazılımı kullanmadan kendi yöntemlerini taklit edenler arasında ayrım yapmanın daha da zorlaştığını söyledi. KELA tarafından izlenen ilk beş saldırgan, 2022'deki tüm kurbanların yüzde 50'sinden fazlasından sorumluydu; LockBit, Alphv, Conti, Black Basta ve Hive fidye yazılımı ve haraç saldırıları uyguluyor, saldırıların yüzde 40'ı ABD'den sorumluydu ve Birleşik Krallık, Almanya, Kanada ve Fransa, her biri toplam kurbanların yüzde 4 ila 6'sını kapsamaktadır.

KELA verileri ayrıca, 2022'de en çok saldırıya imalat ve sanayi sektörlerinin maruz kaldığını, ardından profesyonel hizmetler sektörünün onu takip ettiğini ortaya koydu. Teknoloji, mühendislik ve danışmanlık sektörünün yanı sıra sağlık ve yaşam bilimleri sektörü de benzer sayıda kurbana sahipti...

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://industrialcyber.co/features/building-coping-mechanisms-to-deal-with-ransomware-attacks-across-critical-infrastructure-sectors/

20 Ocak 2023

1.23. Enerji Tedarikçisine Yönelik Siber Saldırı Şirket Operasyonlarını Aksatıyor

Kanada'nın Nunavut bölgesindeki Qulliq Energy Corporation'a (QEC) yönelik geniş kapsamlı bir siber saldırı, şirketin idari ofislerini felç etti.

Şirket yetkilileri, saldırının 15 Ocak'ta başladığını ve santrallerin normal şekilde çalışmaya devam etmesine rağmen şirketin müşteri hizmetleri ve idari ofislerindeki bilgisayar sistemlerinin kullanılamadığını söyledi.

Şirket, kredi kartıyla fatura ödemesi kabul etmemektedir ancak müşteriler nakit veya banka havalesi yoluyla ödeme yapabilmektedir.

Bölgenin başbakanı PJ Akeeagok yaptığı açıklamada, hükümetin olaya müdahale etmek için şirketle birlikte çalıştığını ve birkaç devlet dairesinin personel sağlamasıyla birlikte çalıştığını söyledi.

"Bu tür saldırılar suçtur. Uzman siber güvenlik ve avukatlar tutuldu. Kanada Kraliyet Atlı Polisi, QEC'nin devam eden soruşturmasına yardım ediyor," dedi Akeeagok. *"Kabine ve düzenli üyelerimiz durumdan haberdar ediliyor ve şirket ve kamu hizmetimiz tarafından alınan önlemlerin gidişatından eminler."*

QEC CEO'su Rick Hunt, şirketin potansiyel bir sorun olduğunu öğrenir öğrenmez olay müdahale planını etkinleştirdiğini söyledi. Şirket, saldırı sırasında hangi bilgilerin çalınmış veya erişilmiş olabileceğini belirlemeye çalışıyor.

Olay sırasında verilerin çalınması durumunda herhangi bir müşteriyi bilgilendirmeyi planlıyorlar, ancak insanları olağandışı etkinlik için banka ve kredi kartı hesaplarını izlemeye çağırdılar. Bilgisayar korsanlarının hesaplara erişmesi durumunda müşterilere şifrelerini değiştirmeleri de söylendi.

Şirketin, kesintileri bildirmesi veya başka sorunları olması gerekenler için hala çağrı merkezleri aktif durumda.

Nunavut, yaklaşık 40.000 kişilik bir nüfusa sahiptir ve Kanada'nın en büyük ve en kuzeydeki bölgesidir. Dünyanın en seyrek nüfuslu bölgelerinden biridir…

Bölge son dört yılda çok sayıda siber saldırıya maruz kaldı. 2019'daki bir fidye yazılımı saldırısı, QEC dışında hükümetin tüm BT sistemlerini ve hizmetlerini etkiledi. Netwalker fidye yazılımı grubu da 2020'de Northwest Territories Power Corporation'ın peşine düştü.

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://therecord.media/cyberattack-on-nunavut-energy-supplier-limits-company-operations/

15 Ocak 2023

1.24. Petrol Reçine Üreticisi Fidye Yazılımı Grubunun Kurbanı Oldu

Yuan Liang Industrial, petrol reçineleri üreten Tayvan merkezli bir şirkettir. Şirket Lockbit fidye yazılımı grubu tarafından hedeflendi. Fidye yazılımı grubuna ait blog sayfasında ilgili duyuru gerçekleştirildi. Ödeme yapılmadığı taktirde sızdırılan veriler fidye yazılımı grubunun blog sayfasında yayımlanması büyük bir olasılık olarak gündemdeki yerini koruyor.

Şirket hakkında: 1975 yılında kurulan, 250MT/ay kapasitesi ile çalışan Yuen Liang Industrial & Co. Ltd.'de yalnızca 10'dan fazla çalışan çalışmaktaydı. Yuen Liang, 1998 yılında ISO-9002 sertifikasını alan ilk petrol reçinesi üreticisi oldu ve o zamandan beri petrol reçinesi üretimi ve satışı konusunda uzmanlaştı. Üretim kapasitesinin kademeli olarak genişletilmesiyle Yuan Liang, 1999 yılında üst tedarikçi Arochem ile birleşti…

TESPİT YERİ:
Deep Web

KAYNAK:
-

20 Ocak 2023

1.25. Kritik ManageEngine RCE Açıklığı İşletmeleri Tehdit Ediyor

Birden fazla Zoho ManageEngine ürününü etkileyen kritik bir uzaktan kod yürütme (RCE) güvenlik açığı saldırganlar tarafından aktif olarak kullanılıyor.

İlk istismar girişimleri, Horizon3 güvenlik araştırmacılarının açıktan yararlanma kodunu ve kusurun derinlemesine teknik analizini yayınlamasından iki gün önce, Salı günü siber güvenlik firması Rapid7 tarafından gözlemlendi .

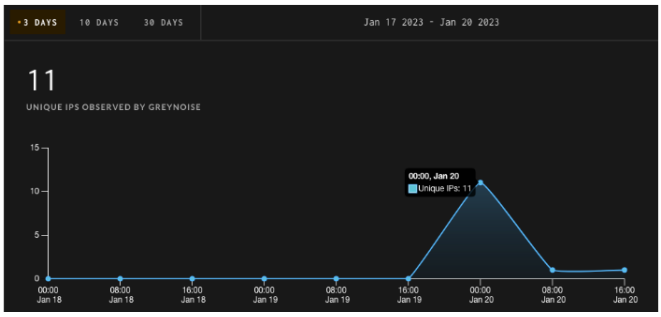
Siber güvenlik firması Rapid7, *"en az 24 şirket içi ManageEngine ürününü etkileyen bir ön kimlik doğrulama uzaktan kod yürütme (RCE) güvenlik açığı olan CVE-2022-47966'nın kötüye kullanılmasından kaynaklanan çeşitli güvenlik ihlallerine yanıt veriyor"* dedi.

"Rapid7, 17 Ocak 2023 (UTC) kadar erken bir tarihte kuruluşlar genelinde istismar gözlemledi."

Bu, *"birden fazla Zoho ManageEngine ürününü (SAML SSO'su etkinleştirilmiş) etkileyen CVE-2022-47966 kimliği doğrulanmamış RCE için en az 10 IP'den yararlanma girişimleri tespit ettiklerini"* söyleyen Shadowserver Foundation'daki araştırmacılar tarafından doğrulandı.

Bulguları, geçen hafta 12 Ocak'ta CVE-2022-47966 istismar girişimlerini izlemeye başlayan tehdit istihbaratı şirketi GreyNoise tarafından da doğrulandı.

GreyNoise, CVE-2022-47966 saldırılarına karşı savunmasız, İnternet'e açık ManageEngine bulut sunucularını hedefleyen 11 IP adresi algıladı…



Figür 1: CVE-2022-47966 istismarına (GreyNoise) bağlı IP'ler

CISA ve FBI daha önce, sağlık hizmetleri ve finansal hizmetler de dahil olmak üzere çok sayıda kritik altyapı sektöründen kuruluşların ağlarına web kabukları bırakmak için ManageEngine kusurlarından yararlanan devlet destekli tehdit aktörlerine karşı uyarmak için ortak tavsiyeler yayınladı…

TESPİT YERİ:
Güvenlik Haberleri

KAYNAK:
https://www.bleepingcomputer.com/news/security/critical-manageengine-rce-bug-now-exploited-to-open-reverse-shells/

13 Ocak 2023

1.26. Litvanya ve Letonya'yı Birbirine Bağlayan Doğalgaz Boru Hattında Patlama Meydana Geldi

Ülkenin gaz iletim operatörü Amber Grid, patlamanın Litvanya'nın kuzeyindeki Panevezys ilçesinde meydana geldiğini söyledi.

Litvanyalı yayın kuruluşu LRT, yaklaşık 250 kişinin yaşadığı Valakeliai köyünün önlem olarak boşaltıldığını söyledi.

Amber Grid'in genel müdürü Nemunas Biknius, Sky News'e patlamada kimsenin yaralanmadığını ve hiçbir mülkün zarar görmediğini ve patlamanın nedeni hakkında soruşturma başlatılacağını söyledi.

"Olayda şans eseri yaralanan olmadı ve yakın zamanda olayla ilgili soruşturma başlatacağız" dedi.

"Şu anda bunun kasıtlı olabileceğine dair bir kanıtımız yok, ancak soruşturma soruları yanıtlayacak."

Baltık Haber Servisi'ne göre, Letonya'nın enerji bakanı Raimonds Cudars'a patlamanın teknik bir kazadan kaynaklandığı bilgisi verildi...

Biknius daha önce yaptığı açıklamada, *"Olaydan sonra doğalgaz boru hattının vanaları sıkıldı. Gaz boru hattına herhangi bir zararlı etki görmüyoruz."*

Litvanyalı boru hattı şebeke operatörünün CEO'suna göre, geçici olarak askıya alınan Letonya'ya gaz arzı yeniden sağlandı...

"Bunun arka planında, hem oradaki savaş nedeniyle Ukrayna'da hem de Rusya'nın bazı bölgelerinde sivil enerji altyapılarına yönelik saldırılar gördük.

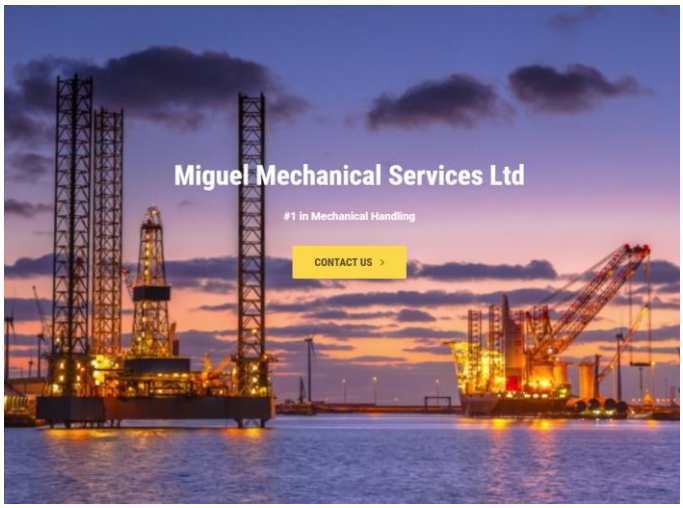
"Litvanya'daki boru hattının savaşla ilgili olup olmadığı net değil, ancak arkasında muhtemelen hain veya uğursuz bir motivasyon olmaksızın boru hatlarının başına gelen bir şey kesinlikle değil."

TESPİT YERİ:
Haberler

KAYNAK:
https://news.sky.com/story/explosion-hits-gas-pipeline-between-lithuania-and-latvia-nearby-village-set-to-be-evacuated-12785961

22 Ocak 2023

1.27. MMSL, LockBit Fidye Yazılımı Grubu Tarafından Hedeflendi



MMSL (Miguel Mechanical Services Limited), petrol ve gaz endüstrisinde faaliyet gösteren ABD merkezli bir şirkettir. Şirket LockBit fidye yazılımı grubu tarafından hedeflendi ve sızdırılan örnek verilere ait ekran görüntüleri gruba ait blog sayfasında yayımlandı.

Kuruluş kendini şu şekilde tanımlamaktadır: *"Miguel Mechanical Services Limited (MMSL), 1988'den beri Petrol ve Gaz Endüstrisinde bir hizmet sağlayıcı olarak varlığını sürdürmektedir. Bir Kuruluş olarak 25 yılı aşkın deneyimiyle, ilgili disiplinlerinde iyi eğitimli, deneyimli ve sertifikalı personel istihdam ediyoruz. En güçlü yanlarımızdan biri, iyi endüstriyel ilişkilerin ve güvenli çalışma uygulamalarının hüküm sürdüğü bir çalışma ortamı sağlama becerimizdir. Tüm bu faktörler, yönetim ekibimiz tarafından uygulanan vizyoner yönetim tarzıyla birleştiğinde, vinçlerin servis ve onarımı konusunda uzmanlaşmış lider şirketlerden biri olmamıza yardımcı oldu."*

TESPİT YERİ:
Deep Web

KAYNAK:
-

21 Ocak 2023

1.28. Kanada Merkezli Kuruluş Fidye Yazılımı Saldırısına Maruz Kaldı

Enerji tesislerine yönelik gerek imalat, gerek saha hizmetleri olarak çeşitli hizmetler sunan Kanada merkezli şirket Royal fidye yazılımı grubu tarafından hedef alındı. Şirkete ait sızdırılan verilerin bir kısmı fidye grubuna ait blog sayfasında yayımlandı.

Şirket kuyu tesisleri, ağır petrol tesisleri, gaz sıkıştırma, depolama terminalleri ve daha birçok alanda müteahhitlik, mekanik kurulum ve modifikasyon alanlarında hizmet vermektedir.

TESPİT YERİ:
Deep Web

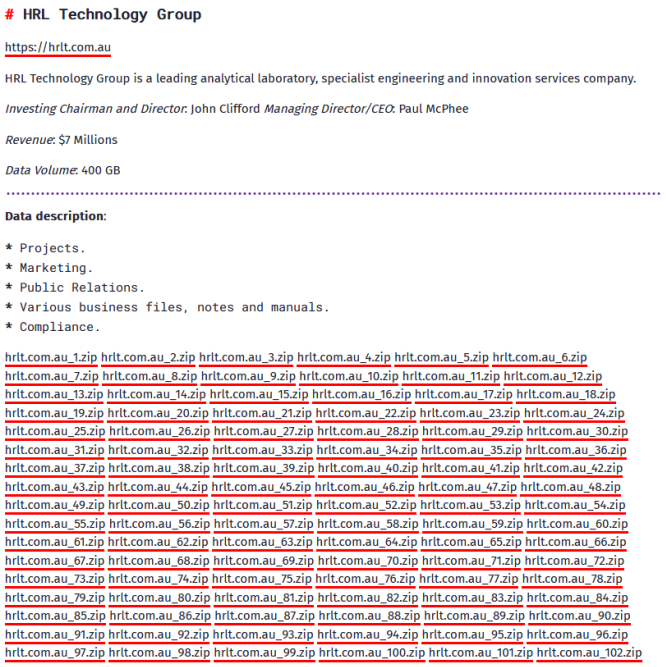
KAYNAK:
-

21 Ocak 2023

1.29. BianLian Grubunun Yeni Hedefi: HRL

HRL, enerjide dahil olmak üzere çeşitli endüstriler için hizmetler sunmaktadır. HRL, kuruluşlar için proses verimliliğini artırma, maliyet düşürme, karbon ayak izini azaltma ve sürdürülebilir üretim gibi konularda danışmanlık hizmeti sağlamaktadır.

Şirket BianLian fidye yazılımı grubu tarafından hedeflendi. Şirkete ait yaklaşık 400GB veri sızdırıldığı belirtilmektedir. Sızdırılan veriler Bianlian grubuna ait blog adreslerinde yayımlanmaktadır.



 # HRL Technology Group

https://hrlt.com.au

HRL Technology Group is a leading analytical laboratory, specialist engineering and innovation services company.

Investing Chairman and Director: John Clifford *Managing Director/CEO*: Paul McPhee

Revenue: $7 Millions

Data Volume: 400 GB

Data description:

* Projects.
* Marketing.
* Public Relations.
* Various business files, notes and manuals.
* Compliance.

hrlt.com.au_1.zip hrlt.com.au_2.zip hrlt.com.au_3.zip hrlt.com.au_4.zip hrlt.com.au_5.zip hrlt.com.au_6.zip
hrlt.com.au_7.zip hrlt.com.au_8.zip hrlt.com.au_9.zip hrlt.com.au_10.zip hrlt.com.au_11.zip hrlt.com.au_12.zip
hrlt.com.au_13.zip hrlt.com.au_14.zip hrlt.com.au_15.zip hrlt.com.au_16.zip hrlt.com.au_17.zip hrlt.com.au_18.zip
hrlt.com.au_19.zip hrlt.com.au_20.zip hrlt.com.au_21.zip hrlt.com.au_22.zip hrlt.com.au_23.zip hrlt.com.au_24.zip
hrlt.com.au_25.zip hrlt.com.au_26.zip hrlt.com.au_27.zip hrlt.com.au_28.zip hrlt.com.au_29.zip hrlt.com.au_30.zip
hrlt.com.au_31.zip hrlt.com.au_32.zip hrlt.com.au_33.zip hrlt.com.au_34.zip hrlt.com.au_35.zip hrlt.com.au_36.zip
hrlt.com.au_37.zip hrlt.com.au_38.zip hrlt.com.au_39.zip hrlt.com.au_40.zip hrlt.com.au_41.zip hrlt.com.au_42.zip
hrlt.com.au_43.zip hrlt.com.au_44.zip hrlt.com.au_45.zip hrlt.com.au_46.zip hrlt.com.au_47.zip hrlt.com.au_48.zip
hrlt.com.au_49.zip hrlt.com.au_50.zip hrlt.com.au_51.zip hrlt.com.au_52.zip hrlt.com.au_53.zip hrlt.com.au_54.zip
hrlt.com.au_55.zip hrlt.com.au_56.zip hrlt.com.au_57.zip hrlt.com.au_58.zip hrlt.com.au_59.zip hrlt.com.au_60.zip
hrlt.com.au_61.zip hrlt.com.au_62.zip hrlt.com.au_63.zip hrlt.com.au_64.zip hrlt.com.au_65.zip hrlt.com.au_66.zip
hrlt.com.au_67.zip hrlt.com.au_68.zip hrlt.com.au_69.zip hrlt.com.au_70.zip hrlt.com.au_71.zip hrlt.com.au_72.zip
hrlt.com.au_73.zip hrlt.com.au_74.zip hrlt.com.au_75.zip hrlt.com.au_76.zip hrlt.com.au_77.zip hrlt.com.au_78.zip
hrlt.com.au_79.zip hrlt.com.au_80.zip hrlt.com.au_81.zip hrlt.com.au_82.zip hrlt.com.au_83.zip hrlt.com.au_84.zip
hrlt.com.au_85.zip hrlt.com.au_86.zip hrlt.com.au_87.zip hrlt.com.au_88.zip hrlt.com.au_89.zip hrlt.com.au_90.zip
hrlt.com.au_91.zip hrlt.com.au_92.zip hrlt.com.au_93.zip hrlt.com.au_94.zip hrlt.com.au_95.zip hrlt.com.au_96.zip
hrlt.com.au_97.zip hrlt.com.au_98.zip hrlt.com.au_99.zip hrlt.com.au_100.zip hrlt.com.au_101.zip hrlt.com.au_102.zip

Grup tarafından sızdırılan verilerin projeler, pazarlama verileri, notlar, iş dosyaları vb. kapsadığı belirtilmektedir.

TESPİT YERİ:
Deep Web

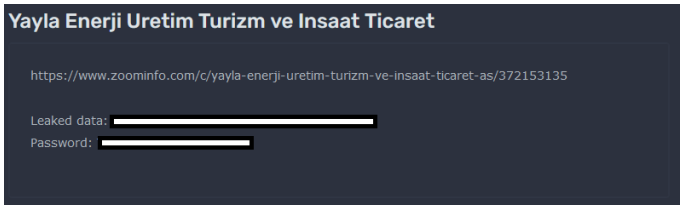
KAYNAK:
-

16 Ocak 2023

1.30. Türk Enerji Şirketi, Mallox Fidye Yazılımı Grubu Tarafından Hedeflendi

Yenilenebilir enerji alanlarına odaklanan şirket, Mallox fidye yazılımı grubu tarafından hedeflendi.

Grup sızdırdığını belirttiği verileri blog adreslerinde yayımladı. Sızdırıldığı belirtilen ilgili verilerin 43.6MB boyutunda olduğu belirtilmektedir.



Şirket hakkında: 1986 yılında şirketin unvanını Yayla İnşaat Sanayi ve Ticaret Ltd. Şti. olarak değiştiren Hüseyin Yayla, şirketin tüm hisselerini aile üyeleriyle birlikte alarak 1992 yılında şirketin tamamına sahip oldu. Bu süreçte 1990 yılında, 40 yıllık geçmişe sahip bu güçlü yapıyı altyapı projeleri alanına sokan Hüseyin Yayla, 1991 yılında şirket merkezini Ankara'ya taşıdı. 2000'li yıllarla birlikte üçüncü kuşağın da iş hayatına dahil olmasının ardından şirket ortakları enerji alanına, özellikle yenilenebilir ve temiz enerji yatırımlarına da ilgi göstermeye başladı. 2010 yılından itibaren inşaat sektörü ağırlıklı olan faaliyet konularını enerji ve turizm alanlarında çeşitlendirmeye başlayan şirket, 2012 yılında faaliyet konularına uygun olarak unvanını değiştirip Yayla Enerji Üretim Turizm ve İnşaat Tic. A.Ş. adını aldı...

TESPİT YERİ:
Deep Web

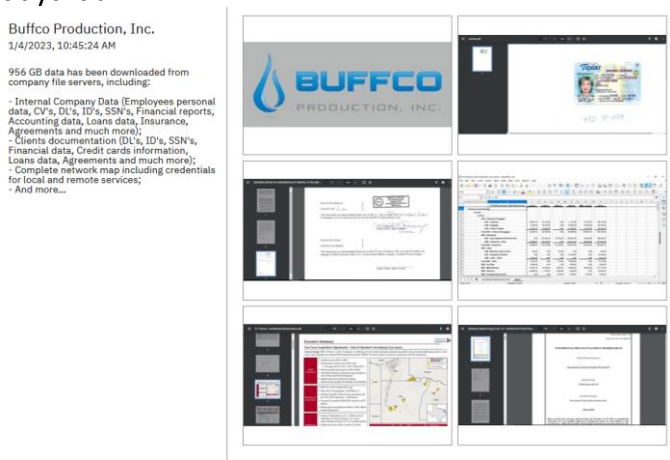
KAYNAK:
-

15 Ocak 2023

1.31. Buffco, Fidye Gruplarının Yeni Kurbanı Oldu

Petrol – Gaz arama ve üretimi alanlarında faaliyet gösteren ABD merkezli şirket fidye gruplarının yeni kurbanı oldu.

Kuruluş Alphv fidye grubu tarafından hedeflendi. Grup 1TB'a yakın veri sızdırdığını belirtmekte ve verilerin neleri kapsadığı ile ilgili bir liste ve örnek veri görüntüleri ile mevcut ihlali blog adresinden duyurdu.



Şirket hakkında: 1981 yılında kurulan Buffco Production, Inc. Teksas, Louisiana ve Oklahoma'da 400'den fazla kuyu işleten bir Doğu Teksas keşif ve üretim şirketidir. Buffco ayrıca beş eyalette 1.300'den fazla kuyuda operasyon dışı hisseye sahiptir. Buffco'nun envanteri geniş bir alana yayılıyor olsa da, işletilen kuyularımızın büyük çoğunluğu Doğu Teksas'ta bulunmaktadır.

TESPİT YERİ:
Deep Web

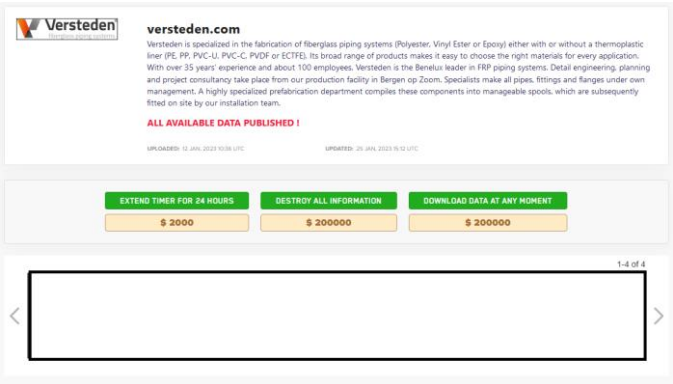
KAYNAK:
-

15 Ocak 2023

1.32. Versteden, Fidye Yazılımı Veri İhlali

Versteden: “35 yılı aşkın süredir müşterilerimizle birlikte boru hattı ve tesis inşaatı projelerinde yenilikçi çözümler üretiyoruz. Profesyonel hizmet kapsamımız, petrol, gaz ve diğer ortamların pompalanması, taşınması, depolanması ve dağıtımı sektörlerinde boru hatları ve tesislerin mühendislik, teslimat, inşaat ve devreye alınmasını içermektedir.”

Şirket LockBit grubunun saldırısına maruz kaldı. Versteden’a ait sızdırılan veriler LockBit fidye grubuna ait blog adreslerinde yayımlandı.



TESPİT YERİ:
Deep Web

KAYNAK:
-

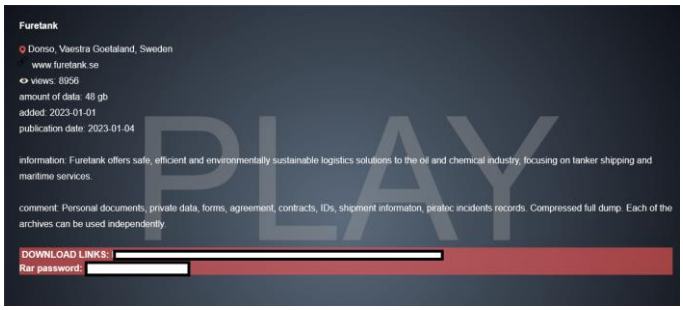
1 Ocak 2023

ICSFUSION

1.33. Furetank, Fidye Yazılımı Veri Sızıntısı

Furetank: “Furetank, tanker taşımacılığı ve denizcilik hizmetlerine odaklanarak petrol ve kimya endüstrisine güvenli, verimli ve çevresel olarak sürdürülebilir lojistik çözümler sunar. Şirketin gemilerinin ve operasyonlarının çevresel etkisini sürekli olarak azaltmak için çalışıyoruz.”

Kuruluş Play fidye yazılımı grubu tarafından hedeflendi. Sızdırılan 48GB boyutundaki tüm veriler grubun blog adreslerinde yayımlandı.



TESPİT YERİ:
Deep Web

KAYNAK:
-

11 Ocak 2023

1.34. Saldırgan Gruptan Yeni İddia: RTU Ransomware

11 Ocak 2023 sabahı erken saatlerde, "GhostSec" grubu, Telegram kanallarında, bir RTU'yu (uzak terminal birimi) ilk şifreleyenler oldukları bir EKS odaklı bir saldırı ile ilgili oldukça çarpıcı bir iddada bulundu:

"Herkes bir Windows masaüstüne, bazı sunuculara, bazı IoT'ye saldıran bir fidye yazılımını kesinlikle duymuştur, ancak saldırıya uğrayan ilk RTU'yu duyurmak istiyoruz!"

"EVET! Az önce tarihteki ilk RTU'yu şifreledik!"

İddiayla birlikte sağlanan kanıtları, bazı temel OSINT (açık kaynak istihbaratı) toplantılarını ve bu iddianın gerçekten de bu kadar çılgınca olup olmadığına dair içgörüleri inceleyelim…

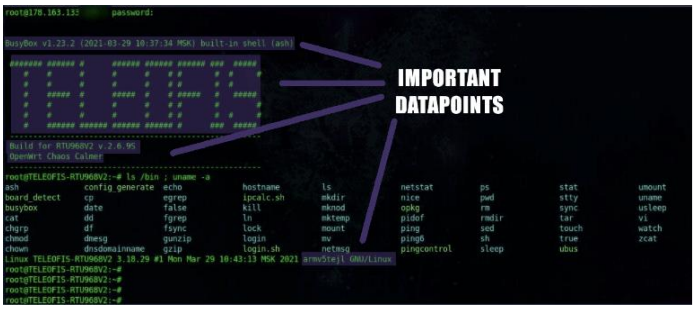
Genel Bakış

İlk olarak, endüstride bir RTU'nun ne olduğu ve ekran görüntülerinde gösterilen RTU ile ilgili ayrıntılarla başlayalım. Bir RTU'nun gerçekte ne olduğuna dair arka plan ayrıntıları için lütfen RealPars'ın şu gönderisine bakın: https://realpars.com/rtu/
GhostSec tarafından sağlanan ekran görüntülerinin, 1 numaralı iddianın öncesi ve sonrası kanıtı olması amaçlanmıştır.

Figür 1: Ana resim 1 ve analizimizin odak noktası

Birkaç önemli veri noktası:

- Banner, cihazın satıcısını TELEOFIS olarak belirtilir,
- RTU968V2 v.2.6.95 için derleme notları,
- OpenWrt Chaos Calmer ilginç,
- Çoğu endüstriyel RTU, Linux çalıştırmaz, ancak endüstriyel kontrol için özel olarak oluşturulmuş gerçek zamanlı işletim sistemleri kullanır.



TESPİT YERİ:
Güvenlik Haberleri & Telegram

KAYNAK:
https://synsaber.com/ghostsec-claim-rtu-ics-hack/
-

CYBER WISE | ICSFUSION

Endüstriyel Tesislere Yönelik

Saldırı Bilgilendirme Raporu

icsfusion.com