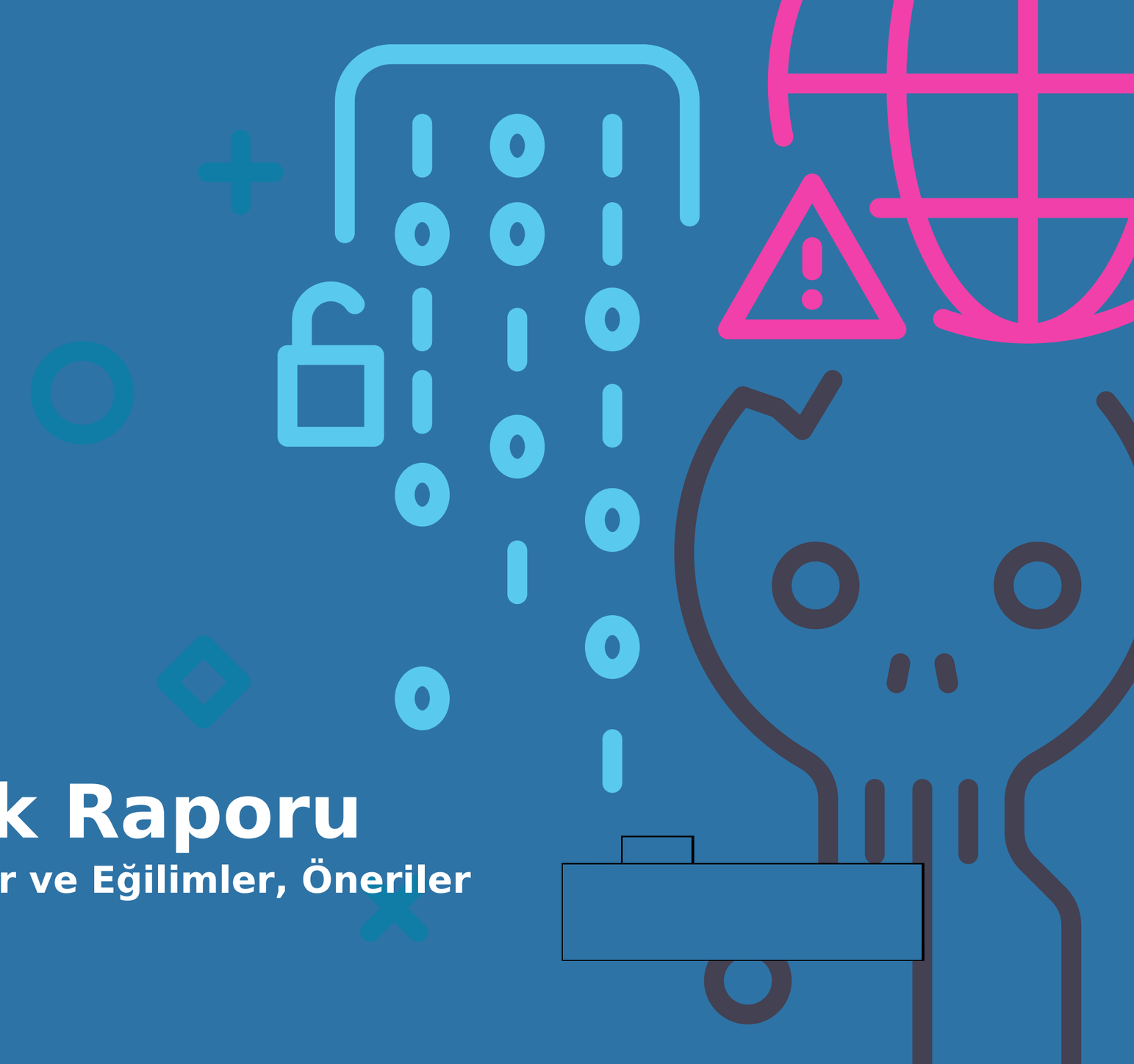
NOZOMI NETWORKS LABS

CERRUS

OT/IoT Güvenlik Raporu

Siber Savaş Bilgileri, Tehditler ve Eğilimler, Öneriler

2022 1.Yarı İnceleme | Ağustos 2022



Yönetici Özeti

Siber tehdit ortamı sürekli değişirken, bunun kuruluşunuzu nasıl etkilediğini anlamak her zamankinden daha önemli. Son altı ayda, tehdit aktörleri tarafından yeni taktiklerin kullanımının yanı sıra saldırıların sıklığı ve karmaşıklığında bir artış gördük. Bir zamanlar olası olmadığı düşünülen tehditler birdenbire olağan hale geldi.

Örneğin, daha önce fidye yazılımı tarafından hedef alınmayan şirketler artık kendilerini bu saldırıların alıcı tarafında buluyorlar. Bu değişime ek olarak, tehdit aktörleri, kötü niyetli etkinliklerinin güvenlik çözümleri tarafından algılanmasını engellemeye devam ediyor.

Güvenliği güçlendirmek ve gelecekteki tehditleri en aza indirmek için şirketler, kendilerini en iyi nasıl koruyacakları konusunda bilinçli kararlar verebilmeleri için siber risk maruziyetlerine ilişkin gerçek zamanlı bilgilere ihtiyaç duyarlar.

Bu Raporda:

- Siber güvenliğin mevcut durumunu **gözden geçireceğiz.**
- Tehdit ortamındaki temel eğilimleri belirleyeceğiz ve bunları ele almak için **çözümler sunacağız.**
- **Rusya/Ukrayna krizini,** tanıtılan yeni kötü amaçlı araçlar ve kötü amaçlı yazılımların yanı sıra bu çatışmanın bize saldırgan yetenekleri hakkında nasıl fikir verebileceğini vurgulayarak özetleyeceğiz.
- Nesnelerin İnterneti (IoT) botnetleri, ilgili Saldırı Göstergeleri (IoC'ler) ve tehdit aktörü Taktik Teknikleri ve Prosedürleri (TTP'ler) hakkında **bilgi sağlayacağız.**
- Önerileri ve tahmin **analizimizi paylaşacağız.**

2022 1.YARI TEHDİT GÖRÜNÜMÜ

Rusya, Şubat ayında Ukrayna'yı işgal etmeye başladığından beri şunları gördük:

Hacktivist etkinlikler

Devlet Destekli APT'ler ve siber suçlar

Wiper malware

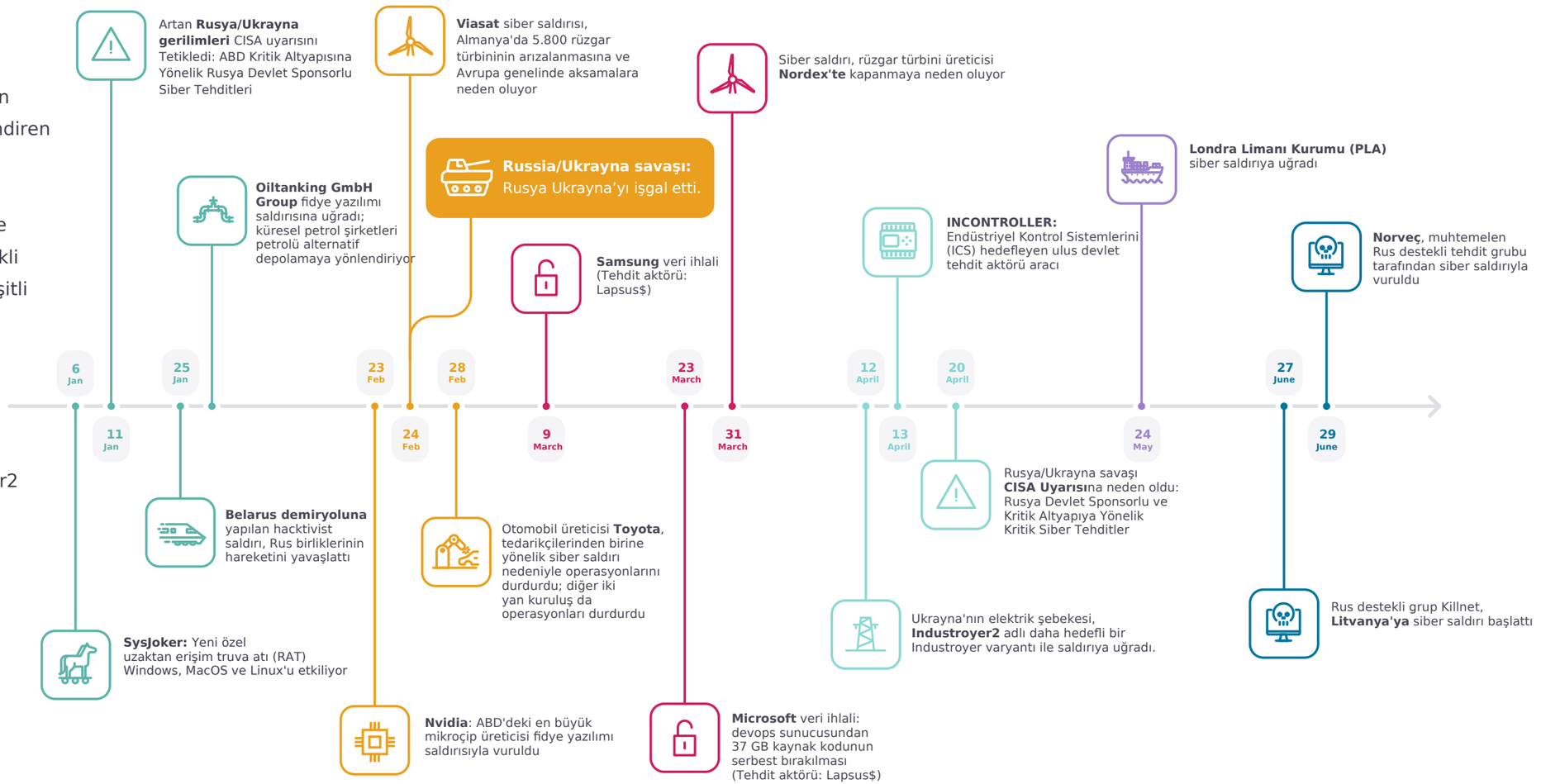
Industroyer2

2022'nin İlk Yarısındaki Önemli Siber Olayların Zaman Çizelgesi

Bu sayfadaki zaman çizelgesi, Ocak ve Haziran 2022 arasında mevcut tehdit ortamını şekillendiren birkaç önemli siber olayı vurgulamaktadır.

Rusya, Şubat 2022'de Ukrayna'yı işgal etmeye başladığından beri, hacktivistler, devlet destekli APT'ler ve siber suçlular dahil olmak üzere çeşitli tehdit aktörlerinden faaliyetler gördük.

Ayrıca, wiper kötü amaçlı yazılımın güçlü bir Şekilde kullanıldığını gördük ve endüstriyel ortamlarda yaygın olarak kullanılan IEC-104 protokolünü kötüye kullanmak için Industroyer2 adlı bir Industroyer varyantı geliştirildi.



IoT Botnet Görünümü

Nozomi Networks Labs'ın honeypot'ları, analiz edildiğinde tehdit aktörü faaliyetlerine ilişkin bazı ilginç bilgiler sağlayan veriler toplar. 2022'nin ilk yarısında aşağıdaki eğilimleri gözlemledik:

- **En çok saldıran ülkeler:** En çok siber etkinlik, Çin ve Amerika Birleşik Devletleri ile ilişkili IP adreslerinden geliyor. Gelişmiş teknoloji ve imalat endüstrileri nedeniyle saldırı yüzeyleri giderek artıyor.
- **Sabit kodlanmış kimlik bilgilerini içeren protokoller:** Mirai, başlangıçta Telnet'i kötüye kullanan popüler bir botnettir, ancak tehdit aktörleri kaynak kodunu halka yayınladıktan sonra, SSH ve diğer protokolleri hedef alacak şekilde değiştirildi.
- **Kullanılan en önemli kimlik bilgileri:** "root" ve "admin" kimlik bilgileri, tehdit aktörlerinin tüm sistem komutlarına ve kullanıcı hesaplarına erişmesine izin verebileceğinden, çeşitli varyasyonlarda kullanılan bariz çekici hedeflerdir.
- **En fazla farklı saldırgan IP adresi sayısı:** Honeypot'larımız kötü amaçlı etkinliklerle ilişkili IP adreslerini toplarken, toplanan 5.000'e yakın benzersiz saldırgan IP adresiyle Mart en aktif ay oldu.

En çok çalıştırılan komutlar:
Enable, shell, system ve which gibi ilk 10 komutu belirledik.
Bu komutların her birini yaklaşık 12.500 bot çalıştırdı

Mart
botnet'ler için en aktif ay oldu.

5,000
Farklı saldırgan IP adresi tespit edildi.

2022'nin ilk yarısında IoT botnet etkinliği hakkında daha fazla bilgi edinmek için **Detaylı Raporumuzu (İngilizce)** okuyun.

Güvenlik Açığı Görünümü

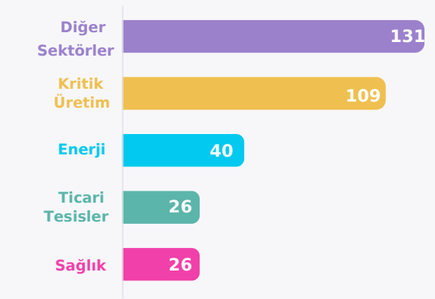
Birçok Operasyonel yazılım ve donanım ürününün güvenlik durumu, çoğunlukla güvenlik araştırmacıları tarafından keşfedilen güvenlik açıkları aracılığıyla açığa çıkar. 2022'nin ilk yarısında, 303'ü 2022'de yeni duyurulan 560 ICS-CERT tarafından yayınlanan Ortak Güvenlik Açıkları ve Etkilenmeler (CVE'ler) vardı. 2021'in ikinci yarısına kıyasla %14 daha az CVE rapor edildi.

Bildirilen CVE'lerden 131'i birden fazla sektörü etkiledi. Kritik imalat, bildirilen 109 CVE ile en doğrudan etkilenen sektör oldu. Enerji 40 ile takip etti ve sağlık ve ticari tesisler 26 ile üçüncü oldu. Ek olarak, CVE tavsiyelerinde 172 ilişkili ürünle 60 farklı satıcıdan bahsedildi.
Etkilenen satıcılar 2021'in ikinci yarısına göre %27 arttı ve etkilenen ürünler %19 arttı.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

560
CVE yayınlandı

EN ÇOK ETKİLENEN SEKTÖRLER



Öneriler

Bir kuruluş içindeki farklı paydaşlar tarafından uygulanabilecek proaktif güvenlik önlemleri almaya artan bir ihtiyaç vardır. Bu, güvenlik konularında farklı bakış açılarına sahip olabilecek BT ekipleri, uyum görevlileri ve risk yöneticilerini içerir. Öncelikli güvenlik uygulamaları şunları içermelidir:

- Doğru bir varlık envanterinin tutulması
- VPN teknolojisindeki en son yamaları uygulamak
- Ayrıcalıklı erişim yönetimi
- Vishing veya SIM değiştirmeye açık olmayan güçlü Çok Faktörlü Kimlik Doğrulama (MFA) kullanma
- Sık şifre değişiklikleri ve
- Vishing ve genel sosyal mühendislik konusunda artan çalışan eğitimi

Ek Önlemler:

Yedeklemeler: Bir fidye yazılımı veya wiper kötü amaçlı yazılım saldırısının tam bir veri kaybıyla sonuçlanmadığından emin olmak için verilerinizi düzenli olarak yedekleyin, yedekleme sisteminizi test edin ve yedeklemenizin aynı ağda değil, saha dışında bir konumda depolandığından emin olun.

Tehdit İstihbaratı: Siber tehdit istihbaratı, kuruluşların sistemlerini ve verilerini korumalarına yardımcı olmak için siber tehditler hakkında bilgi toplama, analiz etme ve yayma uygulamasıdır. Bu bilgiler, kötü amaçlı yazılım imzalarını, saldırı vektörlerini ve güvenlik açığı (IoC) göstergelerini içerebilir.

Bulut Güvenliği: Bulut sağlayıcınızın sağlam bir itibara sahip olduğundan ve ISO 27001 veya SOC 1/2/3 sertifikaları gibi endüstri standartlarıyla uyumlu olduğundan, depolanırken veya aktarılırken verileri şifrelediğinden ve 2FA ve kimlik yönetimi araçlarını kullandığından emin olun.

Tehdit Tespiti: Tehdit tespiti, potansiyel tehditleri gerçek zamanlı olarak tespit etmek ve yanıtlamak ve ayrıca gelecekteki olaylar için uyarılar sağlamak için kullanılır. Tehdit tespitinde sistemler, bir IP adresinden gelen olağandışı miktarda trafik veya belirli bir hizmete çok sayıda bağlantı yapılması gibi şüpheli etkinlikler için ağı izler. Bu, zaman içinde anormal etkinlik izlenerek veya bilinen güvenlik açıkları için ağ taranarak yapılabilir.

Yazılım Malzeme Listesi (SBOM): SBOM, her bileşenin kaç farklı sürümünün bulunduğu ve bunların nerede kullanıldığı hakkında size bir fikir verir, böylece zaman içindeki değişiklikleri izleyebilir ve bunların diğer bileşenlerde sorun yaratmadığından emin olabilirsiniz. Ayrıca, hangi bileşenlerin diğerlerinden daha açık veya daha savunmasız olduğunu ve bu güvenlik açıklarını nasıl azaltacağınızı anlamanıza yardımcı olabilir.
SBOM'lar henüz yaygın olarak kullanılmasa da, bu teknolojinin gelişimini izlemeye değer.

DAHA GÜÇLÜ GÜVENLİK İÇİN ANAHTAR TEHDİT ÖNLEMLERİ

Öngörüler

Bu son analize dayanarak, 2022'nin geri kalanında görmeyi düşündüğümüz temel siber güvenlik trendlerinden bazıları aşağıdadır:

- Daha fazla EKS/OT ile ilgili saldırı
- Fidye yazılımı tehdidi aktörleri kritik altyapı şirketlerini hedef almaya devam edecek
- Daha büyük şirketleri hedef alan daha fazla saldırı
- Teknoloji kaynak kodunun çalınması
- Bu yılın başlarında kurulan özel/hükümet girişimlerinin şekillenmesiyle siber politikalarda ve yönetişimde artış

Detaylı OT/IoT Güvenlik Raporu’nu inceleyin

Nozomi Networks Labs mevcut tehdit ortamını sizin için analiz etti:

- En son fidye yazılımı ve IoT botnet saldırıları
- ICS, OT/IoT cihaz güvenlik açığı ve istismar eğilimleri
- Siber tehdit iyileştirme stratejilerinizi iyileştirme adımları

İndir (İngilizce) **Guardian Demo**

Nozomi Networks

OT ve IoT Güvenlik and Görünürlük için Lider Çözüm

Nozomi Networks, endüstriyel siber güvenlik ve operasyonel kontrol için yeniliklere öncülük ederek dijital dönüşümün hızını artırıyor. Sektöre liderlik ederek, artan siber riskleri operasyonel ağlara yönlendirmeyi mümkün kılıyoruz. Nozomi Networks, tek bir çözümde, dünyanın dört bir yanındaki binlerce en büyük kritik altyapı, enerji, üretim, madencilik, ulaşım ve diğer endüstriyel sitelere OT görünürlüğü, tehdit algılama ve içgörü sağlar.

Bize Ulaşın

NN-SEC-RP-ES-2022-1H-001

nozominetworks.com | cerrus.io