ENERJİ SEKTÖRÜNDE SİBER RİSKLER TEHDİTLER VE ÖNLEMLER

Dr.CÜNEYT KALPAKOĞLU

Founder & CEO Endpoint-labs CYBER SECURITY R&D

cuneyt@Endpoint-labs.com

ihbar@siber-ihbar.com

2016
DÜNYA ENERJİ KONSEYİ
SİBER RİSKLER YÖNETİCİ ÖZETİ – I

WORLD ENERGY COUNCIL 2016

1- *Siber Tehditler Enerji Sektörü Yöneticileri için birinci öncelikli risk konuları içindedir.*

2- *Enerji sektörünün birbiriyle teknolojik iletişimsel bağlantısı ve sayısallaştırılması giderek artmaktadır.*

Akıllı şebekeler, akıllı cihazlar ve giderek artan internet ve internetin kritik rolü modern ekonominin işleyişinde enerji sektörünü çok daha çekici hale getirmiştir. Bu bağlamda sektör operasyonları kesmeye yönelik siber saldırıların öncelikli ve kritik hedefi halindedir.

3- *Siber Risk enerji sektöründe benzersiz bir tehdit kavramı haline gelmiştir.*

Bir saldırı Enerji altyapısında siber dünyadan başlayıp gerçek dünyada devasa bir felakete sebep olabilir. Büyük merkezileştirilmiş altyapılar özellikle risk altındadır ve potansiyel 'domino etkisi' ile örneğin nükleer, ve/ veya petrol üretim tesislerine yönelik siber saldırılar bir anda her yere yayılabilir

2016
DÜNYA ENERJİ KONSEYİ
SİBER RİSKLER YÖNETİCİ ÖZETİ - II

WORLD ENERGY COUNCIL 2016

4- *TEKNOLOJİ Üreticileri ve TEDARİKÇİLERİ, enerji altyapılarının ve kontrol sistemlerinin güvenliğini ve korunurluğunu sağlamak için kritik ve sorumlu bir rol üstlenmek durumundadır. Bu firmaların teslim ettikleri ürünlerde zorunlu olarak «Uluslararası Güvenlik Standarlarında» (yazılım/donanım) özellikle (**ICS**) ve (**SCADA**) güvenliğinin sağlandığı taahhüt edilmelidir.*

5- *Enerji Kurumları Siber tehditleri Temel Risk olarak görmektedirler.*

Enerji sektörünün birbiriyle bağlantısı ve sayısallaştırılması giderek artmaktadır. Akıllı şebekeler, akıllı cihazlar ve giderek artan internet ve internetin kritik rolü modern ekonominin işleyişinde enerji sektörünü çok daha çekici hale getirmiştir. Bu bağlamda sektör, operasyonları kesmeye yönelik siber saldırıların hedefi halindedir.
Buna ek olarak, enerji sektörünün çalışanlarının siber zafiyetler konusunda farkındalığı da kritiktir. Edilmelidir.
Etkili bir siber güvenlik stratejisinde İnsan hatası genellikle çok önemli bir faktördür
Siber saldırıların başarısında, siber risklerin farkındalığının yetersizliği de bir faktördür.

2016
DÜNYA ENERJİ KONSEYİ
SİBER RİSKLER YÖNETİCİ ÖZETİ

WORLD ENERGY COUNCIL 2016

6- *«SİBER SALDIRI SİGORTASI» , hasar olduğunda olası mali kayıpları dengelemek için bir çözüm olabilir.*

Bu bağlamda «Sigorta Sektörü» sözkonusu bu tip felaketler olduğunda özel bir enstrüman bulmaya yada çözüm geliştirmeye devam etmelidir.

Ortaya çıkacak muhtemel riskler açısından geçmişle ilgili olarak sınırlı veri bulunması «Siber Saldırı Sigortası» piyasasının olgunlaşmasını kısıtlamaktadır. Buna rağmen «Siber Saldırı Sigortası» geliştirme süreci çok faydalıdır. Bu konu önemlidir.

2016
DÜNYA ENERJİ KONSEYİ
ÖNERİLER

Tüm paydaşlar 4 alanda birlikte çalışmalıdırlar.

- Teknik ve insan faktörleri
- Siber risklerle ilgili bilgi paylaşımı
- Risk değerlendirmesi ve miktarı
- Standartların ve en iyi uygulamaların geliştirilmesi

1 ABD – KANADA 2013-2015

ELEKTRİK ÜRETİMİ SANTRALI

Sebep : İnsan Kaynaklı Hata / HACKING

ABD'de 50'den fazla elektrik santrali çalıştıran ve yöneten şirketin Kritik santral tasarımları ve Sistem şifreleri Müteahit firmadan çalındı.

2 ABD – 2003

NÜKLEER SANTRAL

Sebep : Malware / Kötücül Program

Tarihteki en hızlı bilgisayar solucanıydı. 2003 yılında, Ohio'daki Nükleer Santral özel ağında, 5 saat kadar bir Güvenlik izleme sistemini devre dışı bıraktı.

3 ABD – KANADA 2012

ELEKTRİK ÜRETİMİ SANTRALI

Sebep : İnsan Kaynaklı Hata / VİRÜS

Bir ABD elektrik santralinde ICS (**I**nternet **C**onnection **S**haring) sistemine bulaştırılan Mariposa adlı virüs, taşaron bir teknisyenin USB'si üzerinden sisteme yüklenmiş.
Ana Sistemi çok yavaşlatan bu virüs duraklamalara sebep olarak sistemin virüsten temizlenip devreye alınması 3 hafta'ya mal olmuş.

4 ABD 2013

BARAJ

Sebep : MALWARE

New York yakınlarında «Küçük Bowman Avenue Barajı»
Sel baskınları için kullanılan bu baraja saldıran korsanlar ,
Baraj sistemlerine kısmi erişim kazandı
Standart kötü amaçlı yazılımlar kullanarak,
Tüm altyapılardaki zafiyetleri ortaya çıkardılar.

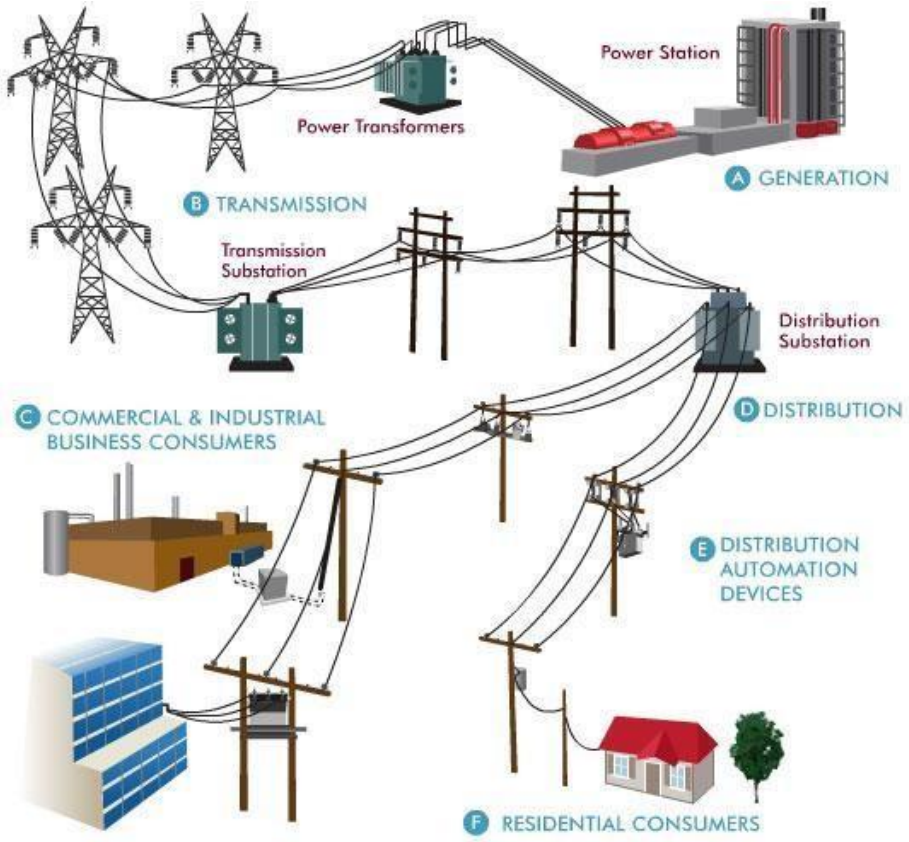
5 UKRAYNA 2015

GÜÇ ŞEBEKESİ

Sebep : İnsan Kaynaklı Hata / HACKING

3 enerji dağıtım şirketinin toplamda 80.000 enerji müşterisinin kesintiye uğramasına sebep olan bu çok iyi planlanmış saldırı, bir elektrik kesintisine neden olan ilk siber saldırı olarak tarihe geçti.

Bu Saldırı, doğrudan şirketlerin bilgi işlem personeline yönelik Hedef Odaklı Kimlik Avı saldırısıyla başladı.



6 SAUDİ ARABİSTAN 2012

PETROL ŞİRKETİ

Sebep : VİRÜS

Dünyanın en büyük petrol üreticisi olan 15-22 Ağustos 2012 tarihleri arasında **Suudi Aramco Petrol Firmasının** 30.000 adet windows işletim sistemi tabanlı bilgisayarı; **Shamoon** isimli zararlı yazılım tarafından, bilgisayarlarda bulunan dokümanların, e-postaların, resimlerin silinerek, yanan amerikan bayrağıyla değiştirildiği saldırıdır.

Asıl amacı ulusal ve uluslararası ölçekte petrol ve gaz akışını durdurmak olan saldırının, amacına ulaşamamış olması büyük bir şans gibi gözükse de tek bir iş kalemine yapılan en büyük saldırılardan biri olması sebebiyle Aramco Saldırısı büyük önem arz etmektedir.

Arabistan'da bir devlet kurumu olan Aramco'da meydana gelen hasar üretimi etkilemese de, petrol piyasasında ciddi paniğe neden olmuştu.

7 HOLLANDA 2012

İLETİŞİM SALDIRISI

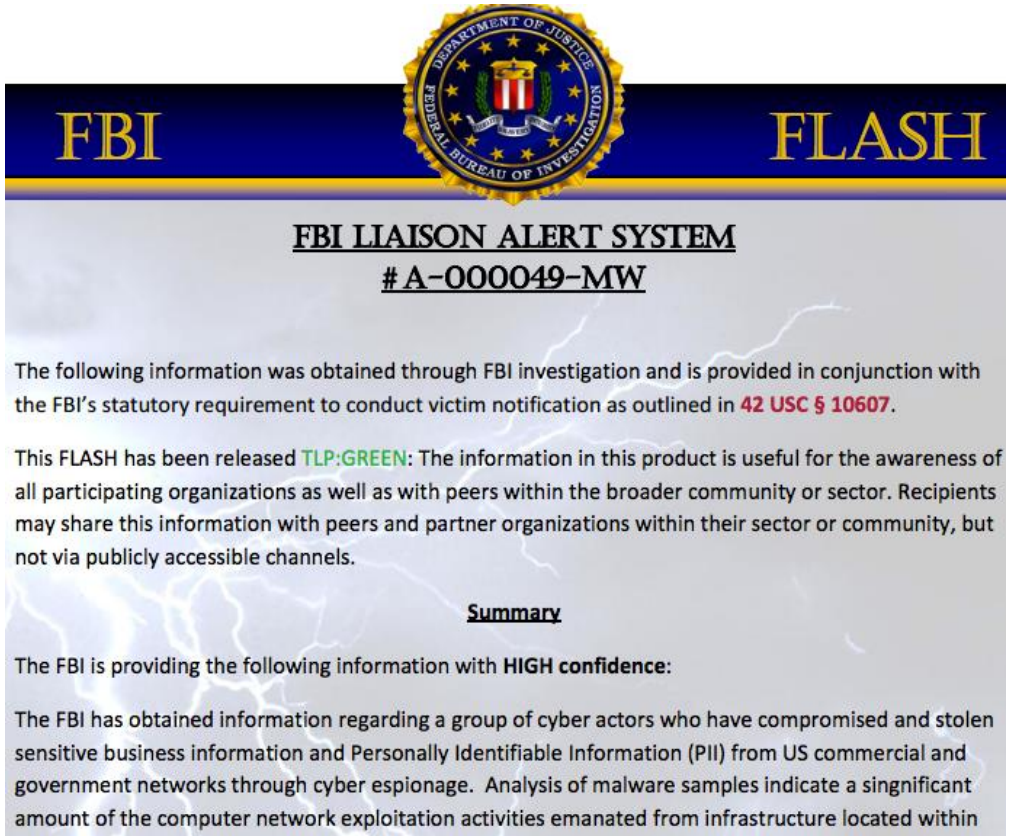
Sebep : HACKING

17 yaşındaki bir saldırgan yüzlerce sunucu ihlali sebebiyle tutuklandı. Sunuclar İletişim şirketi tarafından akıllı sayaç sistemini yönetmek için kullanılıyordu.

Hedef Odaklı Kimlik Avı nedir?

Hedef odaklı kimlik avı, yalnızca hassas verilere izinsiz erişim elde etme amacıyla yapılan hedefli e-posta dolandırıcılığıdır. Geniş kapsamlı, rastgele saldırı gerçekleştiren kimlik avı dolandırıcılığının aksine hedef odaklı dolandırıcılık, belirli bir gruba veya kuruluşa odaklanır.
Amacı fikri mülkiyet, finansal veriler, ticari veya askeri sırlar ve diğer gizli bilgileri çalmaktır.

Nasıl İşliyor ?



Güvenilir bir kaynaktanmış gibi görünen bir e-posta gelir, ancak hiçbir şeyin farkında olmayan alıcıyı kötü amaçlı yazılımlarla dolu sahte bir web sitesine yönlendirir. Bu e-postalar, kurbanlarının dikkatini çekmek için akıllıca taktikler kullanır.

Örneğin FBI, Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi'nden geliyor gibi görünen hedef odaklı kimlik avına karşı uyarıda bulunmuştur.Çoğunlukla bu saldırıların arkasında devlet tarafından desteklenen korsanlar ve hacktivistler bulunuyor.

Nasıl İşliyor ?

Siber suçlular da aynısını, gizli verileri devletlere ve özel şirketlere yeniden satma amacıyla yapıyor.
Bu siber suçlular, mesajları ve web sitelerini etkili şekilde kişiselleştirmek için bireysel olarak tasarlanan yaklaşımları ve toplum mühendisliği tekniklerini kullanıyor.

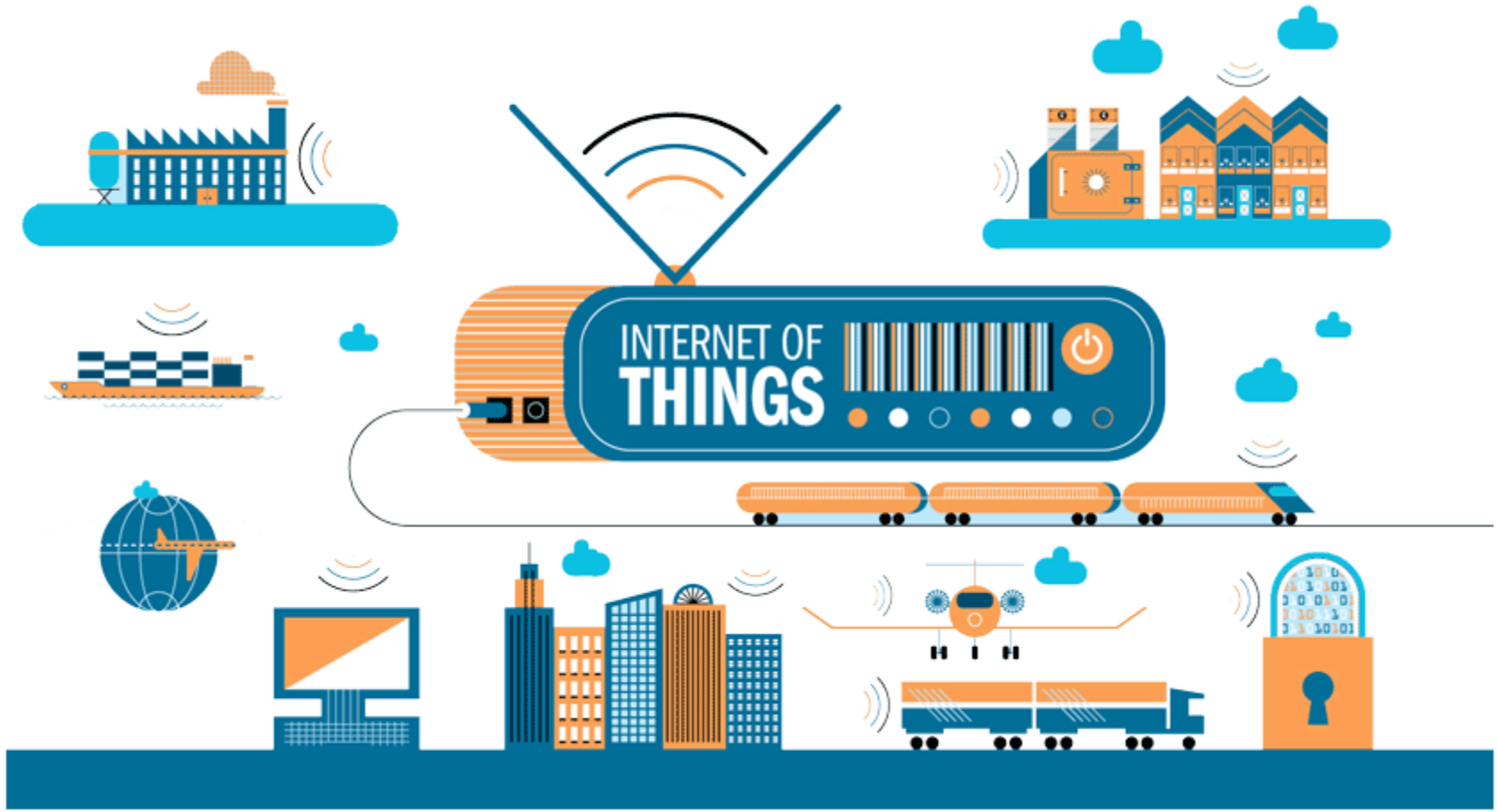
Bunun sonucunda, kuruluşların üst düzey yöneticileri gibi yüksek rütbeli hedefler bile kendilerini güvenli olduklarını düşündükleri e-postaları açarken bulabiliyorlar. Yapılan bu hata, siber suçluların ağlarına saldırmak için ihtiyaç duydukları verileri çalmasına iolanak veriyor.

Nasıl Engellenir?

Geleneksel güvenlik uygulamaları genellikle çok akıllıca hazırlanan bu saldırıları durduramaz. Bu nedenle, algılanmaları çok daha zor hale gelir. Bir çalışanın yaptığı hata işletmeler, devletler ve hatta kar amacı gütmeyen kuruluşlar için ciddi sonuçlar doğurabilir.

Dolandırıcılar, çaldıkları verilerle ticari açıdan hassas bilgileri ifşa edebilir, borsa fiyatlarını manipüle edebilir veya çeşitli casusluk eylemleri gerçekleştirebilir. Ayrıca hedef odaklı kimlik avı saldırıları, bilgisayarları gasp etmek için hizmet reddi saldırısı amacıyla kullanılan botnet'ler gibi çok büyük ağlara kötü amaçlı yazılımlar yerleştirebilirler.

Hedef odaklı kimlik hırsızlarıyla mücadele etmek için çalışanların gelen kutularında sahte e-posta bulunması ihtimali gibi tehditlere karşı uyanık olmaları gerekir. Eğitimin yanı sıra e-posta güvenliğine odaklı teknoloji de gereklidir.


INTERNET OF
THINGS

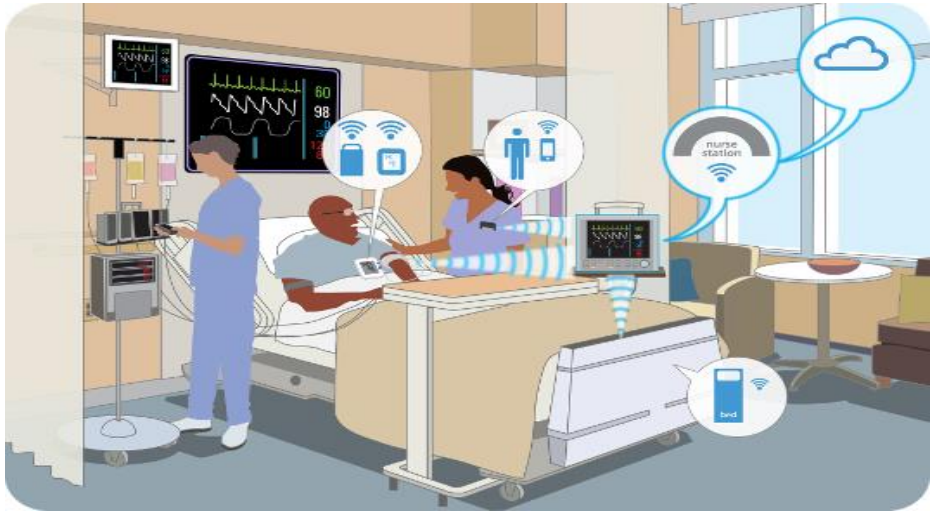
IOT Nedir ?

- Nesnelerin Interneti (IOT), fiziksel nesneler-cihazlar, araçlar, binalara gömülü olan elektronik, yazılım, sensörler vb gibi gömülü diğer unsurların ağ bağlantısıdır.- Bu Ağ vasıtasıyla toplanan veriler işlenir, değişime uğrar ve geri yollanır..

Çeşitli İsimler, Bir Kavram

- M2M (Machine to Machine)
- “Internet of Everything” (Cisco Systems)
- “World Size Web” (Bruce Schneier)
- “Skynet” (Terminator movie)

Giyilebilen
Teknoloji



Sağlık

Akıllı Ev Aletleri

Sınırsız Bağlantılar Dünyası

Dünya IOT Pazar Büyüklüğü

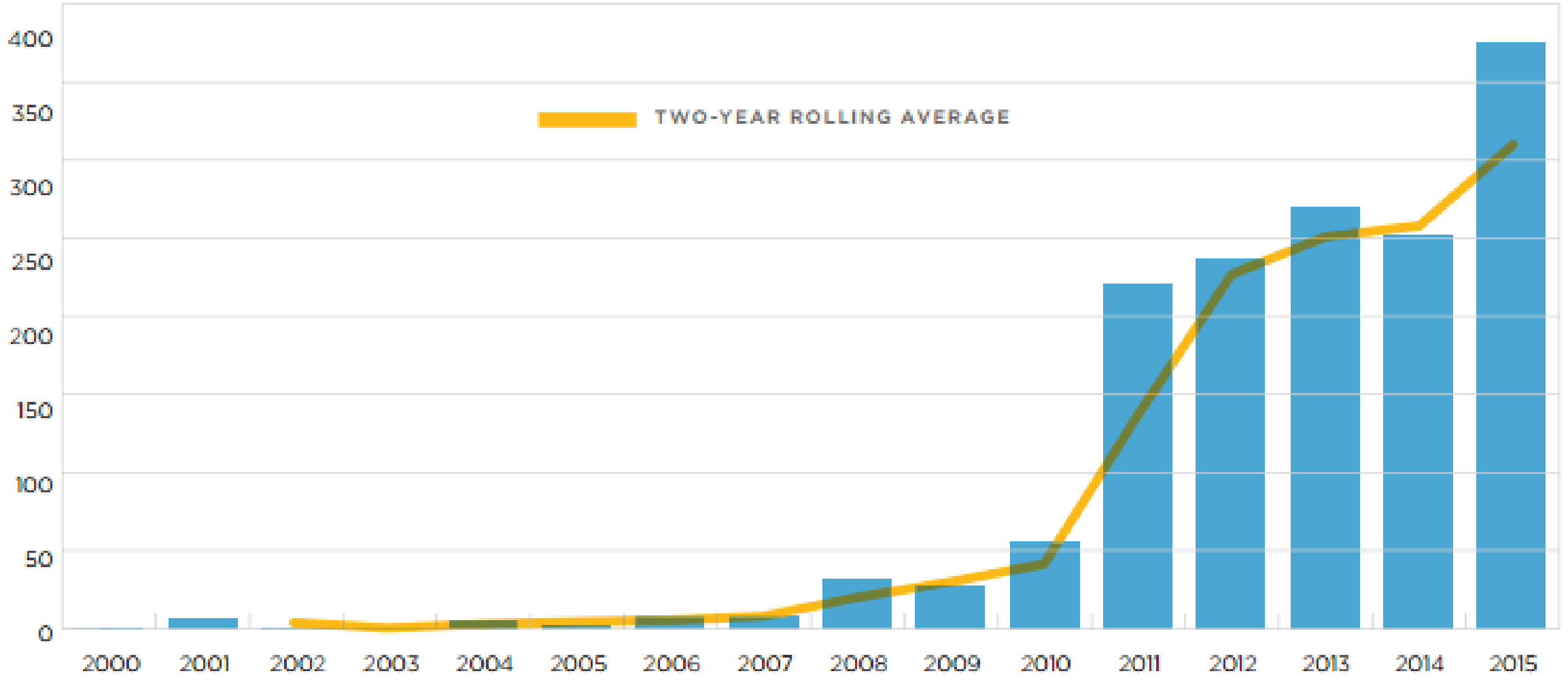
- 2013 yılında 9.1 milyar IoT ünitesi
- 2020 yılına kadar 28.1 milyar IoT ünitesi
- 1.9 trillion $ dan $7.1 trillion $ 2020 beklentisi

Enerji Sektöründe IOT Kullanımı

IOT/ ICS/SCADA RİSKLERİ

- Standart olarak zayıf ve gömülü kodlanmış yapı
- Firmware ve işletim sistemi güncellemsi çok zor
- Güvenlik açıklarının tespit ve onarımı için satıcı desteğinin eksikliği
- Korunmasız web arayüzleri (SQL enjeksiyonu, XSS)
- Kodlama hataları (bellek taşması)
- Açık metin protokolleri ve gereksiz açık portları
- DoS / DDoS riski
- Fiziksel hırsızlık ve kurcalanmaya uygun

FIGURE 1: ICS-SPECIFIC VULNERABILITY DISCLOSURES BY YEAR



[1] Keizer, Greg. "Is Stuxnet the 'best' malware ever?" Infoworld. 16 September 2010. http://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html
[2] OSISoft. OSIsoft Releases Multiple Security Updates for the PI System. 11 August 2015. https://techsupport.osisoft.com/Troubleshooting/Alerts/AL00289.
[3] Yokogawa. Yokogawa Security Advisory Report. 10 September 2015. http://web-material3.yokogawa.com/YSAR-15-0003E.pdf

ICS VULNERABILITIES EXPLOITED IN THE WILD

While ICS vulnerability disclosures were influenced by Stuxnet, we have not observed a corresponding increase in ICS vulnerability exploitation. We are aware of five ICS-specific vulnerabilities exploited in the wild (as shown in Figure 5). In addition, given the growth in researcher interest, we surmise that many other ICS-specific vulnerabilities have been exploited in the past, but have not been made public.

FIGURE 5: FIVE ICS VULNERABILITIES EXPLOITED IN THE WILD

VULNERABILITY TITLE	ATTACK	KNOWN VICTIMS	EXPLOITED	VULNERABILITY DISCLOSED	PATCH RELEASED
[redacted] loading mechanism vulnerability[5]	Stuxnet	NEDA Industrial Group, Natanz, Iran	July 2009	June 2010	September 2011
[redacted] insecure SQL Server authentication[6]	Stuxnet	NEDA Industrial Group, Natanz, Iran	July 2009	June 2010	July 2012
[redacted] Path Traversal[7,8]	Attributed to the Sandworm Team	Various	January 2012	June 2012	December 2013
[redacted] Plus unauthenticated firmware[9,10]	Attributed to the Sandworm Team	Kyivo-blenergo Energy Distribution Facility, Ukraine	December 2015	May 2016	Product Discontinued
[redacted] unauthenticated firmware[11]	Attributed to the Sandworm Team	Prykarpattya-oblenergo Energy Distirbution Facility, Ukraine	December 2015	May 2016	N/A

ÖNERİLER

1- Zafiyet Analizi
2- IOT/ICS/SCADA Güvenliği Testleri
3- Kaynak Kodu Analizi/Değerlendirme

ENDPOINT LABS ©

Teşekkür ederiz.

ihbar@siber-ihbar.com

Dr.CÜNEYT KALPAKOĞLU
Founder & CEO Endpoint-labs CYBER SECURITY R&D
cuneyt@endpoint-labs.com