İletim ve Dağıtım Sistemlerinde Siber Güvenlik

Çağrı POLAT
Era Sistem Bilişim ve Danışmanlık Hizmetleri

İletim ve Dağıtım Sistemlerde Siber Güvenlik

İçerik

- Güvenlik Tanımı, Kritik Sistemlerde Güvenlik
- Elektrik Üretim, İletim ve Dağıtım Sistemlerinin Otomasyonu
- Elektrik Altyapısının Güvenliği İçin Teknik ve Yönetimsel Uygulamalar
- 2016-2019 Ulusal Siber Güvenlik Stratejisi
- SCADA İletişim Protokolleri
- SCADA Güvenlik Tehditleri
- SCADA Güvenlik Önlemleri
- Bilinen SCADA Zafiyetleri
- Kritik Altyapılarda Yaşanmış Siber Saldırı Vakaları
- Sorular

Güvenlik Tanımı

ISO 27002:2005 Bilgi Güvenliğini aşağıdakilerin şekilde tanımlar:

- Gizlilik
- Bütünlük
- Erişilebilirlik

Kritik Sistemlerde Güvenlik

Elektrik üretim, iletim ve dağıtım sistemleri ülkedeki önemli kritik altyapılardandır. Bu altyapıların daha kolay ve etkin yönetim için büyük ölçüde SCADA sistemleri kullanılmaktadır. [1]

Kritik sistemlerin güvenliğinde çok katmanlı yönetilebilir güvenlik mimarisi benimsenmelidir. (Defense-in-Depth)
(Router – 1. Katman Firewall – DMZ – NIPS – SIEM – Antivirüs – HIPS - 2. Katman Firewall vb.)

Elektrik Üretim, İletim ve Dağıtım Sistemlerinin Otomasyonu

Günümüzde enerji üretim, iletim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesini de sağlayan SCADA (Veritabanlı Merkezi Kontrol ve Gözetleme Sistemi) tarafından yapılmaktadır [1].

SCADA uygulaması ilk olarak 1960'lı yıllarda Kuzey Amerika'da hayata geçirilmiştir. İlk yıllarda, SCADA sistemlerinin kurulum ve bakım maliyetleri oldukça yüksek olmasına karşın, teknolojideki gelişmeler ile tercih edilir hale gelmiştir [2].

Sahadaki uzak terminal birimlerinin(fiziksel saha ekipmanları ile bağlantıyı sağlar) koordineli çalışması, gelen bilgilerin yorumlanarak kullanıcılara sunulması, kullanıcıların isteklerinin uzak terminal birimlerine iletilerek kumanda fonksiyonlarının sağlanması, diğer yazılım katmanları ile entegrasyonunu SCADA sisteminde merkezi yönetim birimi yerine getirmektedir [1].

Küçük SCADA sistemlerinde merkezi terminal birimi tek bir PC'den oluşabilir. Buna karşın daha büyük SCADA sistemleri çoklu sunucular, dağıtılmış yazılımlar ve yedekleme birimlerinden oluşabilir [1].

LAN ve WAN protokolleri (IP ve benzeri) sunucuyla iletişim ekipmanları arasındaki iletişimi sağlamaktadır. İşte zafiyetler de tam bu noktada başlamaktadır. Bu yüzden SCADA sistemlerinin siber savaşlara ve siber terörist girişimlere açık olması gibi bir güvenlik sorununu gündeme getirmektedir [3].

Elektrik Altyapısının Güvenliği İçin Teknik ve Yönetimsel Uygulamalar

Bazı kurumlar SCADA sistemlerinin internete bağlı olmadığını öne sürerek güvenli olduklarını düşünmektedir.

Siber atakların arttığı günümüzde Stuxnet zararlı yazılımı bunun doğru olmadığını açıkça göstermiştir. İran nükleer araştırmalarının yapıldığı sistemler internete bağlı olmamasına karşın Stuxnet zararlı yazılımı sisteme bulaşmıştır [4].

İngiltere'de kritik altyapıların güvenliği konularında çalışma yapan CPNI (Center for Protection of National Infrastructure) proses kontrol ve SCADA sistemlerin güvenliği konusunda bir rehber yayınlamıştır. Yayınlanan rehberde aşağıdaki güvenlik önlemelerinin alınması tavsiye edilmiştir [5].

- İş risklerinin anlaşılması
- Güvenli mimarinin gerçeklenmesi
- Olayları ele alma yeteneğinin oluşturulması
- Farkındalığın artırılması ve yeteneklerin geliştirilmesi
- Üçüncü parti risklerin yönetimi
- Projelerin güvenlikle birlikte ele alınması
- Sürekli bir yönetişim modelinin kurulması

2016-2019 Ulusal Siber Güvenlik Stratejisi (9 Eylül 2016)

Kritik altyapı sektörleri: 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma" ve "Bankacılık ve Finans" sektörlerini kapsar.

2016-2019 döneminde, mevcut riskleri, belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar şunlardır:

1. Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar (Ek-B) tarafından denetlenmesi.
2. Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması.
3. Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi.
4. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması.
5. Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması

EK - B: Düzenleyici ve Denetleyici Kurum Listesi
1. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)
2. Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK)
3. Enerji Piyasası Düzenleme Kurumu Başkanlığı (EPDK)

SCADA İletişim Protokolleri

- Endüstriyel uygulamalarda kullanılan birçok cihaz, bilgisayarlara veya birbirlerine bağlanabilmek için EIA standartları olan RS-232, RS-422 ve RS-485 kullanmaktadır [7].

- SCADA-IT arası haberleşmede standart IT veri iletimi protokolleri (Modbus RTU/TCP IP, RP-570, Profi-Bus, Can-Bus)kullanılmaktadır [7].

- Modbus, 1979 yılında Modicon(Schneider Elektrik) tarafından PLC'ler ile kullanılmak için geliştirilen bir seri haberleşme protokolüdür. Günümüzde TCP üzerinden kullanılmaktadır [6]:

- Modbus TCP port 502 üzerinden çalışmaktadır.

- port:"502" country:tr ile internetten bir çok cihaz bilgisine erişmek mümkün (Akköprü HES)

- Modbus TCP/IP zafiyetleri [6]:
  - Açık metinli bir protokoldür
  - Ortadaki adam saldırılarına açıktır (Mitm)
  - Kimlik doğrulama yoktur

SCADA Güvenlik Tehditleri

- SCADA Genel Tehditler
- SCADA Ağ Tehditleri
- SCADA İstismar Tehditleri
- SCADA Uzaktan Erişim Tehditleri
- SCADA Yerel Cihaz Tehditleri
- SCADA DoS & DDoS Tehditleri
- SCADA Veri Bütünlüğü Tehditleri
- Kritik Enerji Altyapılarına Yapılan APT Saldırıları

SCADA Genel Tehditler

- Bu sistemler diğer sistemlere nazanar daha az güvenlik gereksinimleri duyulan riskli sistemlerdir, yamalar?
- SCADA sistemlerde yetki & sorumlulukların belirlenmemesi tehditinin var olması
- SCADA cihazlarının internete açık halde kullanılması ve içeriden dışarıya, dışardan içeriye erişimin mümkün olması.
- SCADA cihazlarının fiziksel güvenliklerine dikkat edilmelidir.
- SCADA ağlarında sadece güvenlikten sorumlu adanmış kişiler mevcut mu?
- SCADA şifrelerinin basit ve ön tanımlı şekilde koyulması/bırakılması veya kaba kuvvet saldırısı ile çözülebilecek kolay şifreler kullanılması ve hiçbir zaman değiştirilmemesi
- İlgili ağ cihazları için kablo güvenliği, iletişim güvenliği ve cihaz güvenliği alınmalıdır.
- Sistem odası güvenliği uygun durumda mı? (Sensörler yardımı ile 7/24 izleniyor mu?)
- Aktif cihazlar bilgi sızıntısı açısından kontrol ediliyor mu?

SCADA Ağ Tehditleri

- SCADA sistemlerin ağ mimarileri detaylıca incelenmeli ve risk yaratacak basit ağ yapılandırılmalarından kaçınılmalıdır.
- SCADA sistemlerde sahadan veri toplama cihazların olduğu ağ yani kritik işlemlerin çalıştığı ağı diğer ağlardan ayrılmalıdır.
- SCADA sistemlerinde kablosuz ağ kesinlikle kullanılmamalıdır.
- SCADA sistemlerinde Bluetooth kesinlikle kullanılmamalıdır.
- SCADA ağında trafik dış ülkelere ve ağ dışına çıkıyor mu? Dışarıya bağlantı var mı? Veya tam tersi dış firewall dan iç SCADA ağına bir istek var mı?
- SCADA ağında trafik analiz edilmelidir.
- DMZ yanlış kurulumları ve yanlış yapılandırılan cihazlar ciddi risklere neden olabilir.
- İç ağda sadece belirli IP adreslerinden kritik cihazlara erişim sağlanmalı ayrıca sadece belirli IP adresler tarafından yönetilmesinin sağlanması gerekir.
- Kritik cihazlar internete açık mı?

SCADA İstismar Tehditleri

- SCADA sistemlerin çeşitli markalar ile alakalı çıkan istismar kodları nette mevcut, ilgili birisi o ağda istismar kodlarını çalıştırabilir.
- SCADA sistemlerin güncellenmesi hemen hemen yapılmamaktadır, yani 7-8 yıllık çıkan zafiyetler aslında kapatılmadığı için hala ciddi risk taşımaktadır. Var olan firmware'ler cihazlara geçilmemektedir.
- SCADA sistemlerin kontrolünü sağlayan işletim sistemleri ömür süresi dolmuş(Windows XP, Windows Server 2003) işletim sistemleri ile yapılma ihtimali var.
- Yöneten cihazlar kolaylık sağlaması adına Anti virüssüz ve Güvenlik Duvarı kapalı şekilde kullanılmaktadır.
- SCADA zafiyet tehditlerinden haberdar mıyız?
- Kritik altyapılar içinde çalışan aktif cihazların(yönlendirici, anahtar) güvenliğine bakıyor muyuz?

SCADA Uzaktan Erişim Tehditleri

- SCADA sistemlerine internet üzerinden (uzaktan) erişim sağlama.
- Uzaktan erişim güvensiz RDP üzerinden mi sağlanma.
- Uzaktan erişim VPN gibi tünelleme ile yapılıp bunları kayıtlarının sürekli incelenmemesi.
- Uzaktan erişimde Teamviewer, Ammyy, Logmein gibi yazılımlara izin verilmesi.
- SCADA uzaktan erişimleri nasıl ve kimin isteği ile açılıyor? Bunlar yazılı bir prosedüre bağlı mı?
- VNC, RDP gibi uygulamalar standart portlar ve kolay şifreler ile kullanma.
- Uzaktan bağlantılarda kullanılan kullanıcı yetkilendirilmesi nasıl ve neye göre yapılmaktadır?
- Uzak bağlantılar güvenli mi? (HTTPS/HTTP)
- Aktif cihazlara erişim Telnet üzerinden erişmek.
- Dışardan destek alınan tedarikçilerin kolaylık olsun diye güvensiz uzak bağlantı yöntemlerine yönelmesi

SCADA Yerel Cihaz Tehditleri

- SCADA yöneten Windows ve Linux vb. cihazlarda açık ve kullanımda olan portların farkında mıyız? Hangi port hangi amaçla açık?
- Zamanlanmış görevler belirli aralıklarla kontrol edilmeli, bir zararlı bu şekilde tetikleniyor olabilir.
- Yerel cihazlar yetkisiz hesap ile çalıştırılmalıdır.
- Dışardan ve içerden e-mail alamaması sağlanmalıdır.
- Cihazlarda USB portları kapalı olmalı ve üzerlerinde CD/DVD çalıştıracak aygıtlar olmamalıdır. Malware?
- SCADA cihazları ağ yapılan paylaşım klasörlerine erişmemeli ve bağlantısı olmamalıdır.
- SCADA ağlarında VINN veya ek modem takmak ve çalıştırmak mümkün olmamalıdır.
- Cihazlarda işletim sistemi ve anti virüs açısından güncel mi, ayrıca cihaz kendi firewall'u açık mı? Herhangi bir program için bir imtiyaz verilmiş mi?
- Bu cihazların ürettiği log kayıtlarına ne sıklıkla bakılıyor, anlık risk tehdit algılama imkanı var mı?

DoS & DDoS Tehditleri

- Kablo ile gittiğimiz kritik cihazlarda servis ve cihaz durmasına karşı önlemler var mı?
- DoS ve/veya DDoS için alınmış bir önlem veya eylem planı var mı?
- Servis reddi saldırı tatbikatları yapılıyor mu?
- Kritik sistemlerin durma veya susma ihtimaline karşı kurumun iş sürekliliği planı var mı?
- Ağdaki aktif cihazlar ve ICS'lere DoS ve/veya DDoS testleri yapılıyor mu?

SCADA Veri Bütünlüğü Tehditleri

- Kritik sistemlerin bağlı olduğu ağa bağlı telefon ve bilgisayarlarda eski işletim sistemlerinin kullanılması
- Yedeklemeler eksiksiz yapılmaması ve veri kaybı tatbikatlarının yapılmaması
- İş sürekliliği testleri planlanıp uygulanmaması
- Sistemin bir eşleniği canlı bir yerde çalışmasının sağlanmaması, bir terslik durumunda ne kadar kısa sürede sistem tekrar ayağa kalkabilir?
- Kritik veriler buluta veya başka bir şehre, ülkeye gidiyor mu?
- Acil durum senaryoları ve simülasyonlarının planlanması ve uygulanması gerekmektedir.
- Dropbox, Onedrive vb. bulut çözümleri ağda kullanılıyor mu?

Kritik Enerji Altyapılarına Yapılan APT Saldırıları

- Bilinen ilk siber salgın, 1988'de Robert Morris'in ürettiği Morris solucanıyken, bugün APT (Advanced Persistant Threats) dediğimiz, Türkçeye 'Gelişmiş Sürekli Tehdit' ya da 'Hedef Odaklı Saldırılar' olarak çevrilen siber silahlar kamu kurumlarını, kritik altyapıları ve büyük şirketleri hedef alan en önemli tehditlerdir.
- Tespiti oldukça güç olan, özel geliştirilmiş teknikler barındıran APT'ler klasik virüslerden ve siber silahlardan birçok özelliği ile ayrılmakta, hedef odaklı olup günümüzde siber savaşlarda aktif olarak kullanılmakta ve özellikle kritik altyapıları hedef almaktadır.
- Yöntemleri ileri olan, bulaştığı sistemlerde uzun süre fark edilmeden çalışabilen ve büyük devletler tarafından finanse edilen saldırganlar basit siber saldırılarda olduğu gibi sadece veri çalmayı değil, stratejik öneme sahip bilgilere erişmeyi hedeflemektedirler.
- İran'ın nükleer programını hedef almış Stuxnet, hemen arkasından benzer kodlarla geliştirildiği düşünülen Duqu ve Flame, APT saldırılarının en iyi örneklerindendir [7].

SCADA Güvenlik Önlemleri

- SCADA sistemler ve bunu kontrol eden cihazlar internetten izole, nete çıkamayan bir durumda olmalıdır.
- Çok katmanlı (Anti virüs, Katmanlı FW, IDS/IPS vb.) yönetilebilir güvenlik mimarisi kurgulanmalı ve işletilmelidir.
- SCADA sistemler ile alakalı cihazlar 7/24 merkezi olarak izlenmeli ve ters durumlar için alarm uyarıları kurulmalıdır.
- Ağda iç logları anlamlandırmak adına SIEM ürünlerinden ve korelasyon işlemleri kurgulanmalı ve yardım alınmalıdır.
- SCADA sistemlerinde uzman kişiler tarafından yılda 2 defa sızma testi ve pasif dinleme gerçekleşti mi? Sonuçlar yorumlanmalıdır.
- Olası Zero-Day ve APT saldırılarını haber verecek yapılar kurulmalı ve bunlar sistemlerde çalıştırılıyor olmalıdır.
- İlgili kritik altyapı ile alakalı risk analizinin eksiksiz yapılması sağlanmalı ve eylem planları oluşturulmalıdır.
- ISO27001:2013 BGYS ve Enerji Altyapıları İçin ISO 27019:2013 ilgili kurumda kurulması ve eksiksiz işletilmesi sağlanmalıdır.
- Kritik altyapı ve bileşenlerin güvenlik işlemleri dökümante edilmeli ve uygulanmalıdır.
- İçeriden olabilecek tehditler için saldırı tespit sistemi (IPS) ve saldırı engelleme sistemi (IDS) kurgulanmalı ve ağ trafiği izlenmelidir.
- İnsan kaynaklı tehditlerin önüne geçmek adına yılda 2 defa teknisyen, mühendis, yönetici ve çalışan seviyesinde Bilgi Güvenliği Farkındalık Eğitimleri düzenlenmeli, aktif oltalama simülasyonları yapılmalıdır.
- Ağa yeni bir cihaz takıldığında buna izin vermeyecek yapının kurulması (802.1x).
- Kuruluşlarda siber saldırı tatbikatların/simülasyonların SOME ekibi tarafından belirli aralıklarla yapılması ve gerekli aksiyonların alınması.

Bilinen SCADA Zafiyetleri

Siemens

- ICS-ALERT-11-080-01 : Siemens Tecnomatix FactoryLink Vulnerabilities
- ICS-ALERT-11-161-01 : Siemens S7-1200 PLC Vulnerabilities
- ICS-ALERT-11-186-01 : Siemens SIMATIC Controllers Password Protection Vulnerability
- ICS-ALERT-11-204-01B : Siemens S7-300_S7-400 Hardcoded Credentials (Update B)
- ICS-ALERT-11-332-02A : Siemens SIMATIC WinCC Flexible (Update A)
- ICS-ALERT-11-332-01A : Siemens Automation License Manager Vulnerabilities (Update A)
- ICS-ALERT-13-016-02 : Offline Brute-Force Password Tool Targeting Siemens S7

Siemens Zafiyetleri

Schneider Electric

- ICS-ALERT-11-346-01 : Schneider Electric Quantum Ethernet Module Credentials
- ICS-ALERT-12-020-03B : Schneider Electric Modicon Quantum Vulnerabilities (Update B)
- ICS-ALERT-13-016-01A : Schneider Electric Product Vulnerabilities (Update A)
- ICS-ALERT-15-224-02 : Schneider Electric Modicon M340 PLC Station P34 Module Vulnerabilities
- ICS-ALERT-16-256-02 : Schneider Electric ION Power Meter CSRF Vulnerability

Schneider Zafiyetleri

- ICS-ALERT-16-286-01 : Sierra Wireless Mitigations Against Mirai Malware
- ICS-ALERT-16-263-01 : BINOM3 Electric Power Quality Meter Vulnerabilities
- ICS-ALERT-16-256-01 : FENIKS PRO Etnet Energy Meter Vulnerabilities
- ICS-ALERT-16-256-02 : Schneider Electric ION Power Meter CSRF Vulnerability
- IR-ALERT-L-16-230-01 : Navis WebAccess SQL Injection Exploitation
- ICS-ALERT-16-230-01 : Navis WebAccess SQL Injection Vulnerability
- ICS-ALERT-16-182-01 : Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities
- ICS-ALERT-16-099-01B : Moxa NPort Device Vulnerabilities (Update B)
- IR-ALERT-H-16-056-01 : Cyber-Attack Against Ukrainian Critical Infrastructure

2016 yılı ICS Zafiyetleri

Kaynak: https://ics-cert.us-cert.gov/alerts

(Industrial Control Systems Cyber Emergency Response Team)

Kritik Altyapılarda Yaşanmış Siber Saldırı Vakaları

KIEV'DEKI BÜYÜK ELEKTRIK KESINTISI!

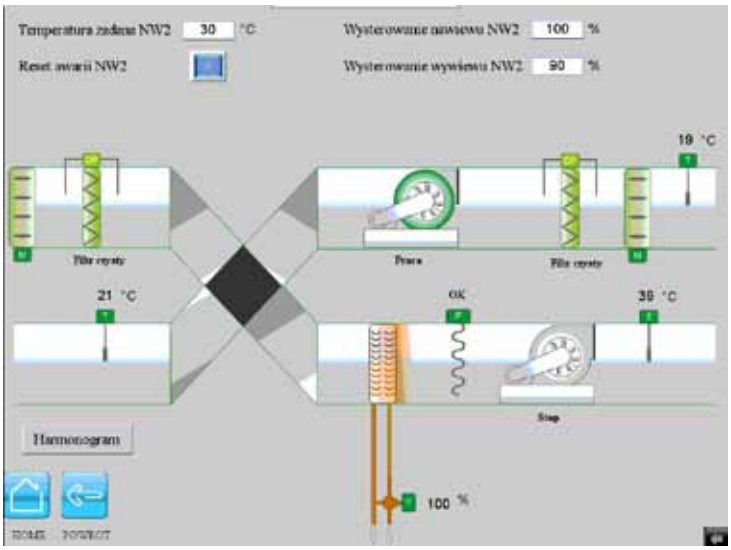
Ukrayna'da 17-18 Aralık 2016 tarihlerinde kentin önemli bir bölümünü karanlığa gömen bu kesintinin gerçekleştirilen ve tarihin en büyük siber saldırılarından biri olduğu anlaşıldı. Bu saldırıdan kuzey istasyonuna bağlı 330 kilovatlık ünite ve SCADA sistemleri oltalama saldırısından etkilenmişti. Ayrıca saldırıların uzun süre önceden planlandığı ortaya çıktı. Kaynak

ENERJI SEKTÖRÜ HEDEF ALINDI

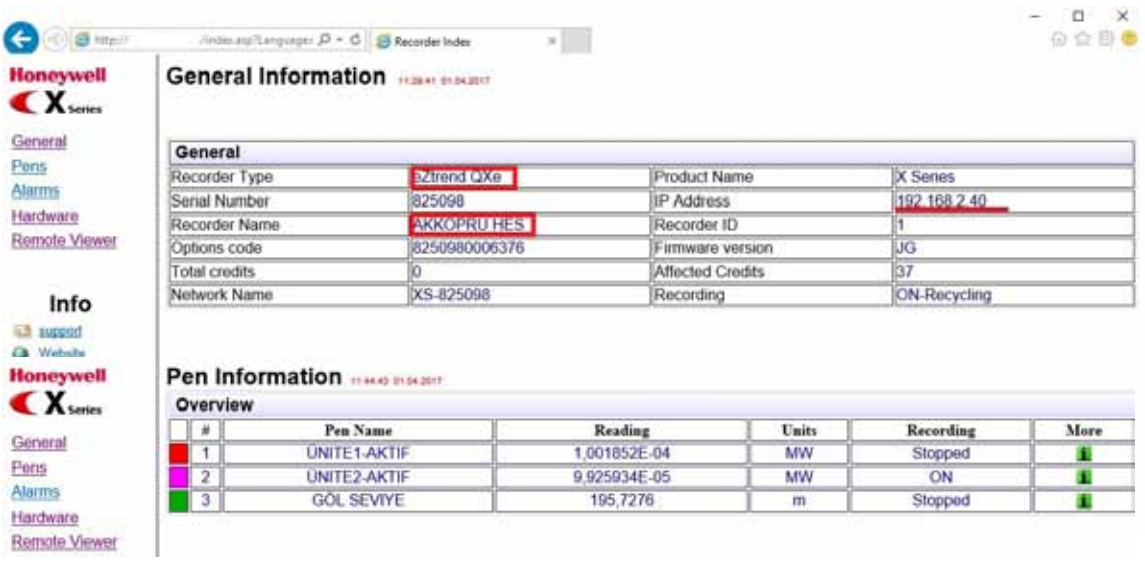
Güvenlik araştırmacıları Ortadoğu'daki enerji şirketlerini hedef alan yeni bir hacker grubu tespit etti. İlk olarak Ocak ve Şubat aylarında gözlenen saldırılarda "Laziok" olarak adlandırılan bir çeşit malware kullanıldığı tespit edildi.

Saldırılar genellikle petrol, gaz ve helyum endüstrilerini hedef alıyor ve saldırılara maruz kalan kurbanların ortalama %25'i Birleşik Arap Emirliklerinde bulunuyor. Suudi Arabistan, Pakistan ve Kuveyt de Laziok malware'ına maruz kalan ülkelerden bazıları. ABD de malware'dan etkilenen diğer bir ülke.

Kullanıcı gelen mailde bulunan eki açarsa – genellikle bir Excel dosyası – exploit kodu aktif hale geliyor ve malware sisteme bulaşıyor. Kaynak



İnternete Açık Bir SCADA(Video var)



İnternetten Kolayca Erişilebiliyor

Kaynakça:

[1] Çelikkol, M. K. S. 4. Ağ ve Bilgi Güvenliği Sempozyumu Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği. BİLDİRİLER KİTABI, 19.

[2] http://www.dpstele.com/dpsnews/techinfo/scada/scada_knowledge_base.php, (27 Mart 2017 erişilebilir durumda)

[3] Ten C., Liu C., Manimaran G., "Vulnerability Assessment of Cybersecurity for SCADA Systems", IEEE Transactions On Power Systems, Vol. 23, No. 4, 2008

[4] http://www.bilgiguvenligi.gov.tr/zararliyazilimlar/zararli-yazilimlarin-yeni-hedefi-hangikritik-altyapi-sistemleri-olacak.html (10 Ağustos 2011 erişilebilir durumda)

[5] http://www.cpni.gov.uk/protectingyourassets/scada.aspx (25 Ocak 2011 erişilebilir durumda)

[6] https://www.bgasecurity.com/makale/endustriyel-it-sistemlerinde-siber-guvenlik (01 Nisan 2017 erişilebilir durumda)

[7] https://www.slideshare.net/ZhreAydn/kritik-enerji-altyapilarinin-korunmasi-ve-siber-gvenlik (01 Nisan 2017 erişilebilir durumda)