Elektrikli Araç Şarj Anomali Senaryosu

Şarj İstasyonu Kökenli Yan Hareket (Lateral Movement)

Anomali: Yerel Ağa Sızma Girişimi

Halka açık bir şarj istasyonu üzerinden kurumsal IT/OT ağına yetkisiz sızma.

Aşama 1: İlk Erişim (Initial Access)

Zayıf Kimlik Bilgileri

Uzaktan yönetim (SSH/Telnet) veya yerel web arayüzü için varsayılan veya zayıf şifre kullanımı.

Yazılım Zafiyeti

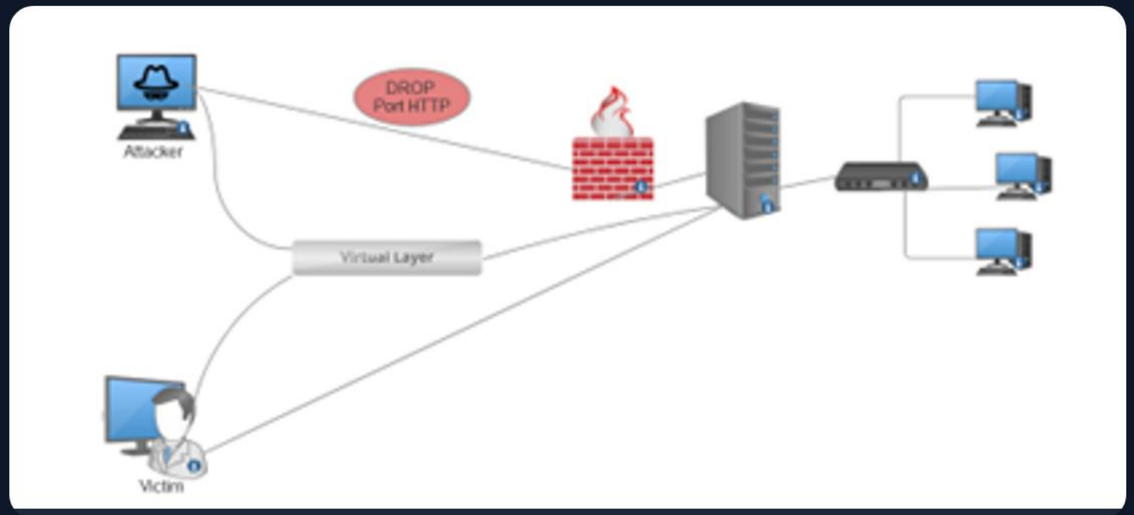
İstasyonun işletim sisteminde veya OCPP/diğer servislerde (Teşhis Portu) keşfedilen bir CVE veya zero-day.

Aşama 2: Anomali Oluşumu (Pivot & Keşif)

Pivot Noktası Olarak İstasyon

Saldırgan, istasyonun kontrolünü ele geçirdikten sonra, onu bir "pivot noktası" olarak kullanarak saldırı moduna alır:

- Yerel ağdaki diğer cihazlara (CCTV, sunucular, BMS) yönelik port tarama (port scanning) veya ARP sorguları başlatır.
- Ağdaki cihazların IP adreslerini, açık portlarını ve potansiyel zafiyetlerini listeler.



Anomali Nedeni: Yetersiz İzolasyon

DÜZ AĞ

(Flat Network)

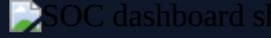
Kritik Zafiyet

Asıl anomali nedeni, şarj istasyonu ve kurumsal ağın VLAN veya güvenlik duvarı ile doğru şekilde izole edilmemesidir.

Bu "Düz Ağ" yapısı, saldırganın yanal hareket (lateral movement) yaparak tüm ağa kolayca yayılmasını sağlar.

Aşama 3: Algılama Mantığı

- **Giden Bağlantı Sayısı:** İstasyonun CSMS dışındaki, kurumsal ağdaki birçok farklı IP'ye (sıra dışı portlara) çok sayıda bağlantı isteği göndermesi.
- **Anormal Protokol Kullanımı:** Normalde (OCPP, DNS, NTP) yerine ağ keşfi için ICMP (Ping), NMAP veya Telnet gibi protokolleri aktif olarak kullanması.
- **Yüksek CPU/Bellek Yükü:** Cihazın normal döngüsünün çok üzerinde, sürekli tarama nedeniyle yüksek CPU veya bellek kullanımı göstermesi.



Aşama 4: Karar ve Tepki

Otomatik Müdahale

Eğer istasyon, normal çalışmasının %10'undan fazlasını ağ taraması için harcıyorsa:

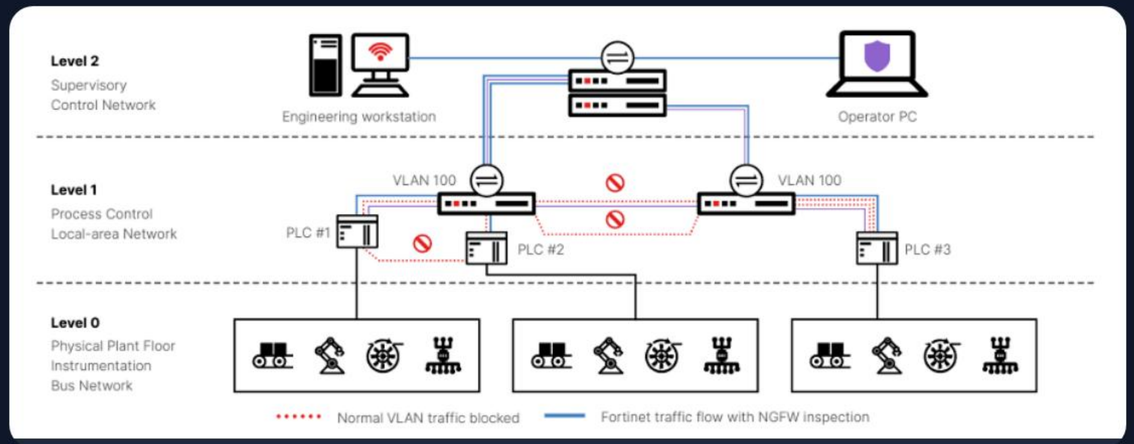
- **Hemen İzolasyon:** İstasyonun ağ bağlantısı (VLAN veya port) otomatik olarak kısıtlı moda alınır veya kesilir.
- **Bildirim:** Siber Olaylara Müdahale Ekibine (SOC) 'Kritik OT Cihazı Üzerinden Yan Hareket Girişimi' uyarısı gönderilir.
- **Adli Analiz:** Olayın kökenini bulmak için istasyonun log kayıtlarının yedeği alınır.

Kaynak Açıklaması: Ağ Segmentasyonu

ISA/IEC 62443 İhlali

Bu anomali, "Bölgesel ve Kanal Güvenliği" (Zoning and Conduits) ilkelerinin ihlal edilmesinden kaynaklanır.

Endüstriyel standartlara göre, Operasyonel Teknoloji (OT) varlıkları (Şarj İstasyonu) ile Bilgi Teknolojisi (IT) varlıklarının (Kurumsal Ağ) birbirinden ayrılması esastır.



Kaynak Açıklaması: Yan Hareket

> Dışarıdan erişilebilen, zayıf korunan "ağ cihazlarının" (IoT/OT) iç ağa sızmak için bir "basamak" (stepping stone) olarak kullanılmasıdır.
>
> — Lateral Movement (Yan Hareket) Metodolojisi

Saldırının keşif aşaması, MITRE ATT&CK çatısında T1046 (Network Service Scanning) tekniği ile eşleşir.

Öneriler: Güvenlik Mimarisi İyileştirmeleri (1/2)

VLAN/Ağ Segmentasyonu

Tüm şarj istasyonları, kurumsal ağdan tamamen izole edilmiş, sıkı kurallara tabi bir Ayrı VLAN veya DMZ ağına yerleştirilmelidir.

Çıkış Filtrelemesi (Egress Filtering)

Şarj istasyonundan çıkan trafiğe, sadece CSMS sunucusu, zaman sunucusu (NTP) ve DNS gibi kesinlikle gerekli hedeflere izin veren katı güvenlik duvarı kuralları uygulanmalıdır.

Öneriler: Güvenlik Mimarisi İyileştirmeleri (2/2)

Ağ Davranışı Analizi (NBA)

Ağdaki anormal davranışları (yüksek tarama trafiği, bilinmeyen protokollere bağlantı) gerçek zamanlı olarak izleyen bir SIEM veya IDS kullanılmalıdır.

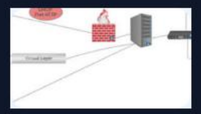
Micro-Segmentasyon

Kritik iç sistemler (BMS, Sunucular), şarj istasyonundan gelen her türlü trafiğe karşı ek olarak kendi aralarında da izole edilmelidir.

Q&A

Teşekkürler

Image Sources

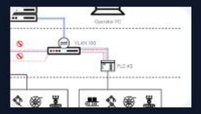


https://app.trustline.sa/media/blog/2024/08/26/im1.png

Source: www.trustline.sa

https://cdn.prod.website-files.com/66f7129d03527383bf3191ea/6835f8e46d03c43ec6cf0ef5_SOC%20Dashboard-image.png

Source: www.dropzone.ai



https://marvel-b1-cdn.bc0a.com/f00000000310757/www.fortinet.com/content/dam/fortinet/images/cyberglossary/vlan-traffic-blocked.png

Source: www.fortinet.com

https://read.xamk.fi/wp-content/uploads/2024/09/Krista-Pesonen_EV-Charging-Stations-763x551.jpg

Source: read.xamk.fi