ANOMALİ SENARYOSU: RANSOMWARE (FİDYE YAZILIMI) VE SOSYAL MEDYA PLANI

Hazırlayan: Özgün Deniz Sevilmiş

Senaryo Adı: Sahte Firmware Güncellemesi ile Şarj İstasyonunu Ele Geçirme (Ransomware)

---

1. ANOMALİ SENARYOSUNUN AÇIKLAMASI

Nedir? Şarj istasyonları, güvenli çalışmak için periyodik yazılım güncellemelerine (Firmware) ihtiyaç duyar. Bu senaryoda bir saldırgan, merkezi yönetim sistemi (CSMS) gibi davranarak istasyona sahte bir güncelleme paketi gönderir.

Nasıl Gerçekleşir? İstasyon, zayıf doğrulama protokollerini (OCPP L02) kullanan bir güncelleme isteği aldığında, paketin kaynağını sorgulamadan yükler. Ancak bu paket aslında bir **Ransomware (Fidye Yazılımı)**içerir. Güncelleme sonrası istasyonun tüm şarj fonksiyonları kilitlenir; cihaz hizmet veremez hale gelir ve ekranında "Hizmetin açılması için fidye ödenmelidir" mesajı belirir. Bu durum hem operasyonel duraksamaya hem de ciddi bir itibar kaybına yol açar.

---

2. LİNKEDİN ŞİRKET HESABI PAYLAŞIM TASLAĞI

Başlık: ⚡ Şarj İstasyonunuz Siber Saldırganlar Tarafından Rehin Alınabilir mi?

Açıklama: Elektrikli araç şarj istasyonları (EVSE) sadece birer güç ünitesi değil, internete bağlı akıllı sistemlerdir. Peki, bu ekosistemin güvenliği ne kadar sağlanıyor? 🛡️

Projemizin 3. haftasında, siber dünyanın en yıkıcı tehditlerinden biri olan **"Ransomware (Fidye Yazılımı)"**saldırısını şarj altyapıları üzerinde simüle ettik!

🚀 **Neler Yaptık?** Yetkisiz bir firmware güncellemesi üzerinden istasyonun nasıl tamamen işlevsiz hale getirilebileceğini ve fiziksel olarak nasıl kilitlenebileceğini canlandırdık.

🔬 **Sonuç:** Geliştirdiğimiz **Yapay Zeka Destekli Saldırı Tespit Sistemi (IDS)**, bu sıra dışı veri trafiğini ve yetkisiz komut enjeksiyonlarını saniyeler içinde fark ederek saldırıyı daha gerçekleşmeden engelledi. Veri bütünlüğünü koruyor, geleceğin mobilite altyapısını siber tehditlere karşı daha dirençli hale getiriyoruz! 💪💻

#CyberSecurity #EVCharging #Ransomware #SmartMobility #AI #SoftwareEngineering #FutureTech

---

3. GÖRSEL VE TASARIM ÖNERİLERİ

1. **Dashboard Görüntüsü (En Etkili):** Geliştirdiğimiz IDS yazılımının terminal ekranında bastığı parlak kırmızı **"🚨 ANOMALY DETECTED: Ransomware Pattern Blocked"** uyarısı ile bir şarj istasyonu görselinin yan yana geldiği profesyonel bir kolaj.
2. **Sanal Kilit Metaforu:** Bir şarj kablosunun üzerinden geçen verilerin dijital bir tünelde akarken, saldırı paketlerinin (0x777 ID'li veriler) yeşil bir güvenlik kalkanına çarparak durdurulduğu modern bir 3D illüstrasyon.
3. **İnfografik:** Normal şarj akışını gösteren düzenli bir trafik grafiği ile saldırı anında meydana gelen "Flood" (veri yağmuru) etkisini kıyaslayan teknik bir analiz görseli.