Firmware Supply Chain Attack Anomalisi

1. **Durum:** Şarj istasyonlarına (EVSE) gelen veya merkezden dağıtılan firmware güncelleme zincirine bir saldırgan sızar ve cihazlara imzasız / değiştirilmiş / zararlı firmware paketleri dağıtır. Güncelleme mekanizması doğrulama yapmadığı veya güvenli değilse saldırgan kodu yaygın şekilde enjekte eder.

2. **Olası Sebepler:**

    a. Firmware paketlerinin **dijital imza** veya hash ile doğrulanmaması.
    b. Güncelleme sunucusuna **zayıf erişim kontrolü** / çalınmış kimlik bilgileri.
    c. Güncellemelerin **şifrelenmemiş** (HTTP) veya doğrulamasız kanallardan gelmesi (MITM riski).
    d. Tedarik zincirinde üçüncü taraf tedarikçilerdeki güvenlik zafiyeti.
    e. CI/CD veya build sunucularının ele geçirilmesi; sahte firmware oluşturma.
    f. Cihazlarda **secure boot** veya imza doğrulama mekanizmasının olmaması/kapalı olması.

3. **Tespit yöntemleri / göstergeler:**

    a. **Firmware hash / dijital imza uyuşmazlığı**: Cihaz yerel hash değeri üretici veritabanındakiyle eşleşmiyorsa uyarı.
    b. **Beklenmeyen firmware versiyonları**: Hedef cihazlarda kayıtlı versiyon geçmişi ile uyuşmayan versiyon tespit edilmesi.
    c. **Güncelleme kaynağı kontrolü**: Güncelleme kaynağı IP/hostu izin verilen listede değilse alarm.
    d. **Anormal ağ davranışı**: Cihazların normalde bağlanmadığı uzak IP'lere/ağlara bağlantı; yüksek outbound trafik.
    e. **Sistem loglarında zaman uyumsuzluğu / yeniden başlatma artışı**: Çok sayıda eş zamanlı yeniden başlatma veya servis kesintisi.
    f. **Beklenmeyen servis/port açılışları** veya yeni arka kapı prosesleri.
    g. Fiziksel: cihazın LED/ekranında beklenmeyen mesajlar, servis modu göstergeleri.

4. **Etki / riskler**

    a. **Geniş çaplı kontrol kaybı:** Saldırgan istasyonları uzaktan yönetebilir (şarjı durdurma, limit değiştirme).

b. **Fiziksel hasar / güvenlik riski:** Batarya/şebeke üzerinde anormal komutlarla hasar veya yangın riski.
c. **Gizlilik ve veri sızıntısı:** Kullanıcı kimlik bilgileri, faturalama verileri çalınabilir.
d. **Sürekli gizlenme (persistence):** Firmware ile kalıcı yetki elde edilmesi.
e. **Tedarik zinciri etkisi:** Bir istasyonda başlayan saldırı, tüm ağ üzerindeki cihazlara yayılabilir.
f. İtibar / finansal kayıp / regülasyon cezası.

5. Kısa tespit kuralları & metrikler

a. **Hash Doğrulama Oranı:** %100 tüm firmware güncellemelerinde SHA-256 doğrulaması.
b. **Kaynak Beyaz Listesi:** Tüm firmware update talepleri yalnızca onaylı 3 sunucudan gelmeli — aksi halde alarm.
c. **Anormal Yeniden Başlatma Eşiği:** Saat başına 2'den fazla yeniden başlatma: uyarı.
d. **Outbound Bağlantı Eşiği:** Cihaz başına 1'den fazla eş zamanlı dış bağlantı yoksa normal; aşılırsa incele.
e. **Versiyon Tutarsızlığı:** Merkezi veritabanı ile cihaz versiyon farkı %0 olmalı; fark bildirimi anında.

6. Önerilen önlemler

a. **Dijital imza / kod imzalama:** Her firmware paketini dijital olarak imzala; cihaz sadece imzalı paketleri yüklesin.
b. **Secure Boot / Trusted Boot:** Cihaz açılırken bootloader imza doğrulaması yapsın.
c. **Güncelleme sunucularında TLS + mutual authentication:** Hem sunucu hem cihaz karşılıklı sertifika kontrolü.
d. **Hash kontrolü + versiyon kontrolü:** SHA-256 hash + versiyon geçmişi merkezi logda tutulmalı
e. **Network segmentasyonu:** Cihaz yönetim ağı ile müşteri trafik ağı ayrı olsun
f. **CI/CD güvenliği:** Build sunucularını HSM/TPM ile koru, erişim günlükleri, 2FA, minimal erişim.
g. **İzleme (IDS/IPS + SIEM):** Firmware update eventlerini, hafif anormallikleri, outbound bağlantıları izle.

h. **Saha güvenliği:** Fiziksel erişim kontrolleri (kilit, alarm) ve tamir/güncelleme prosedürleri.
i. **Tedarikçi denetimi:** Üçüncü taraf kod ve bileşenlerin güvenlik denetimleri, kayıtlı hash'lerin saklanması.
j. **Rollback & Kill-switch:** Zararlı güncelleme tespit edilirse merkezden hızlı rollback veya cihaz karantinaya alma.

7. Kısa müdahale adımları

a. Şüpheli cihaz(lar)ı ağdan izole et.
b. Cihaz loglarını ve firmware hash'lerini topla, merkezi kayıtla karşılaştır.
c. Eğer hash uyuşmuyorsa cihazı salt-read moda al, güncellemeyi iptal et, forensik imaj al.
d. İlgili IP/sertifika/CI kaynaklarını blokla; tedarik zincirindeki son güvenli sürümü geri yükle.
e. Kullanıcıları/bilgileri etkilenmişse bildirim süreçlerini başlat.
f. Olay sonrası root-cause analysis, yeni önlemler ve patch.