### Hazırlayan: Ahmet Emir ÇETİN

### Tarih:30.10.2025

### Anomali Senaryosu Raporu

**Senaryo Adı:** Kriptografik Kimlik Sahteciliği ve Sistemik Dolandırıcılık (eMSP Alt-CA'sının Ele Geçirilmesi)

**Referans Makale:** Gelişmiş EV Şarj Ekosistemlerinde Siber-Fiziksel Anomali Senaryoları Kataloğu (2025); ISO 15118 Açık Anahtar Altyapısı (PKI) zafiyetleri.

### 1. Senaryonun Amacı:

Saldırının temel amacı, tüm "Tak ve Şarj Et" (Plug & Charge) ekosisteminin güvendiği zincirdeki kritik bir halkayı kırmaktır. Hedef, genellikle bir otomotiv üreticisi veya şarj operatöründen (CPO) daha az güvenlik bütçesine sahip olabilen bir e-Mobilite Hizmet Sağlayıcısının (eMSP) ağına sızmak ve araçlara kontrat sertifikası düzenleyen alt Sertifika Otoritesinin (sub-CA) özel anahtarını (private key) çalmaktır.

### 2. Senaryo Özeti:

Sofistike bir siber suç grubu, hedefledikleri bir eMSP'nin kurumsal ağına sızar. Ağ içinde yayılarak, kontrat sertifikalarını (araçların kimliklerini) imzalamak için kullanılan alt-CA sunucusunu bulur ve bu sunucudan özel anahtarı çalar. Bu anahtara sahip olan saldırganlar, artık kriptografik olarak meşru ve geçerli, sınırsız sayıda sahte araç kontrat sertifikası (eMAID) üretebilir. Bu sahte sertifikalar, "ömür boyu ücretsiz şarj" vaadiyle karanlık ağda (dark web) satılabilir veya büyük ölçekli şebeke saldırıları (V2G) için "hayalet" bir araç filosunu yetkilendirmek amacıyla kullanılabilir.

### 3. Hedef Varlıklar:

* **eMSP Alt-CA Özel Anahtarı:** Saldırının ana hedefi; tüm sahte sertifikaları imzalamak için gereken kriptografik anahtar.
* **eMSP Ağı ve Altyapısı:** Anahtarın çalınması için sızılan kurumsal ağ.
* **ISO 15118 Güven Altyapısı (PKI):** Tüm Plug & Charge ekosisteminin dayandığı ve bütünlüğü bozulan güven modeli.
* **Şarj Operatörleri (CPO'lar):** Sahte sertifikaları kabul etmek zorunda kalarak gelir kaybeden operatörler.

### 4. İlişkili Tehditler (STRIDE):

* **Spoofing (Kimlik Sahteciliği):** Saldırganlar, kriptografik olarak meşru (ancak sahte) binlerce araç kimliği yaratma yeteneği kazanır. Bu kimlikler, gerçek araçlardan ayırt edilemez.
*  **Tampering (Veri Manipülasyonu):** Tüm güven zincirinin bütünlüğü (integrity) temelden bozulur.
*  **Repudiation (İnkâr):** CPO'lar, sahte sertifikaların geçerli imzası nedeniyle bu işlemlere itiraz edemez. Saldırganlar, tüm ekosistem içinde serbestçe hareket edebilir.
*  **Elevation of Privilege (Yetki Yükseltme):** Saldırganlar, kendilerine "sınırsız ve ücretsiz şarj" yetkisi (ayrıcalığı) tanır.

### 5. Saldırıda Faydalanılan Zafiyetler:

* **Parçalanmış Güven Ekosistemi:** Plug & Charge modelinin, güvenliği için (bazıları daha az güvenli olabilecek) çok sayıda farklı eMSP'nin kendi alt-CA'larını koruyabilmesine dayanması.
*  **Yetersiz Anahtar Koruması:** Hedeflenen eMSP'nin, kritik alt-CA özel anahtarını, ağdan çalınmayı önleyecek bir Donanım Güvenlik Modülü (HSM) yerine, yazılım tabanlı bir sunucuda saklaması.
*  **Zayıf Kurumsal Güvenlik:** Saldırganların eMSP'nin ağına sızmasını ve ağ içinde yanal hareket etmesini sağlayan geleneksel siber güvenlik zafiyetleri (örn. zayıf parolalar, yamalanmamış sistemler).

### 6. Saldırı Adımları (Adım Adım Simülasyon):

1. **Aşama 1: Hedef Tespiti ve Keşif:** a. Organize bir suç grubu, ekosistemdeki en zayıf güvenlikli veya en stratejik eMSP'yi hedefler.
2.  **Aşama 2: İlk Sızma:** a. Saldırganlar, oltalama (phishing) veya eMSP'nin dışa açık sistemlerindeki bir zafiyeti kullanarak kurumsal ağa ilk erişimi sağlar.
3.  **Aşama 3: Yanal Hareket ve Keşif:** a. Saldırganlar, ağ içinde sessizce hareket ederek sertifika otoritesi (CA) altyapısını barındıran sunucuları tespit eder.
4.  **Aşama 4: Anahtar Hırsızlığı:** a. Sunucuya yönetici (admin) erişimi elde edilir ve alt-CA'nın özel anahtar dosyası (ve parolası) ağ dışına sızdırılır (exfiltrate).
5. **Aşama 5: Sahte Sertifika Üretimi (Minting):** a. Saldırganlar, çaldıkları bu özel anahtarı kullanarak, geçerlilik süresi uzun (örn. 10 yıl) binlerce sahte araç kontrat sertifikası (eMAID) üretir.
6. **Aşama 6: İstismar ve Ticarileştirme:** a. Üretilen bu sahte kimlikler, herhangi bir Plug & Charge uyumlu istasyonda (farklı operatörlere ait olsalar bile) enerji hırsızlığı için kullanılır veya karanlık ağda satılır.

### 7. Olası Sonuçlar ve Etkiler:

* **Sistemik Güven Çöküşü:** Plug & Charge kimlik doğrulama modelinin tamamı işlevsiz hale gelir ve güvenilirliğini yitirir.
* **Katasrofik Finansal Kayıplar:** Şarj operatörleri (CPO), sahte ancak kriptografik olarak geçerli bu sertifikaları reddedemez. Bu durum, tüm operatörler için devasa, faturalandırılamayan enerji maliyetleri ve gelir kayıpları anlamına gelir.
* **Ekosistemin Sürdürülebilirliğinin Tehdit Altına Girmesi:** Kullanıcıların ve operatörlerin sisteme olan güveninin tamamen yok olması, tüm Plug & Charge ekosisteminin uzun vadeli başarısını ve sürdürülebilirliğini tehlikeye atar.
* **Geniş Ölçekli Saldırı Riski:** Bu sahte kimlikler, V2G şebeke saldırıları gibi daha yıkıcı senaryolar için binlerce "hayalet" araçtan oluşan bir botnet'i yetkilendirmek için kullanılabilir.

### 8. Tespit Yöntemleri (Detection):

* **Finansal Anomali Tespiti:** CPO'ların, belirli bir eMSP'den kaynaklanan ve faturalandırılamayan şarj işlemlerinin hacminde ani ve anormal bir artış tespit etmesi.
* **Ağ Güvenlik İzlemesi (eMSP tarafında):** eMSP'nin, kendi CA sunucularına yönelik şüpheli erişim denemelerini veya kritik anahtar dosyalarının ağ dışına çıkarılma girişimlerini izlemesi.
* **Sertifika Şeffaflığı (CT) Logları:** (Eğer uygulanıyorsa) Bir eMSP-CA'dan anormal sayıda sertifika yayınlandığını izlemek için herkese açık CT loglarının denetlenmesi.

### 9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation):

* **Zorunlu Donanım Güvenlik Modülleri (HSM):** Tüm eMSP'lerin, alt-CA özel anahtarlarını, ağdan çalınmasını veya kopyalanmasını teknik olarak imkansız kılan, FIPS 140-2 Seviye 3+ gibi standartlara sahip fiziksel HSM cihazlarında saklamasını zorunlu kılmak.
* **Katı Güvenlik Denetimleri:** Plug & Charge ekosistemine (Root CA) dahil olmak isteyen tüm eMSP'ler için çok sıkı ve periyodik siber güvenlik denetimlerini (pentest dahil) zorunlu hale getirmek.
* **Hızlı ve Evrensel İptal Mekanizmaları:** Ele geçirilen bir alt-CA'yı ve ondan üretilen tüm sertifikaları ekosistem genelinde (tüm CPO'lar tarafından) hızla geçersiz kılacak (CRL/OCSP) acil durum mekanizmaları oluşturmak.
* **Risk ve Güven Bölümlemesi:** Tek bir eMSP'nin ele geçirilmesinin tüm sistemi çökertmesini önlemek için güven modelini daha az merkezi hale getirecek mimariler geliştirmek.