**BASIN BÜLTENİ**

**Android telefonlarda, bankaların SMS onay mesajlarını etkisiz hale getiren malware tespit edildi**

**Fortinet, Türkiye’deki bankaların mobil uygulamalarını hedef alan ve bankaların SMS onay mesajlarını etkisiz hale getiren bir malware tespit etti. Zararlı yazılım kullanıcıların banka ve kredi kartı bilgilerinin yanı sıra sosyal medya hesaplarının giriş bilgilerini de ele geçiriyor.**

Yüksek performanslı siber güvenlik çözümleri alanında dünyanın önde gelen şirketlerinden Fortinet’in tespit ettiği Android.Banker isimli zararlı yazılım, kendisini “Flash Player” şeklinde gizleyerek büyük bankaların ve sosyal medya sayfaların uygulamalarını hedef alıyor.

Zararlı yazılım; Türkiye, ABD, Almanya, Fransa, Avustralya, Polonya ve Avusturya’da faaliyet gösteren 94 bankanın mobil uygulamasını hedef alıyor. Bankadan gelen SMS onayını da etkisiz hale getirebilen malware, çift faktörlü SMS kimlik doğrulama adımını da geçebiliyor. Türkiye’deki bankaların uygulamasını hedef almakla kalmayan yazılım; Google Play mağazası, Facebook, Facebook Messenger, Whatsapp, Skype, Snapchat, Twitter, Viber, Instagram ve Snapchat gibi sosyal medya hesaplarının kullanıcı bilgilerini de ele geçirebiliyor.

Malware, telefona yüklendiğinde “Flash Player” uygulamasının ikonu şeklinde görünüyor. Bu ikona tıklandığında açılan sayfada “**İptal**” ve “**Aktive Et**” seçenekleri bulunsa da “**İptal**” seçeneği tıklandığında yazılım, kullanıcı “**Aktive Et**” seçeneğini seçinceye kadar her seferinde kendisini tekrar açıyor. Bir kez “**Aktive Et**” tıklandığında ise yazılıma cihazın tam kontrolü için yetki verilmiş oluyor.

Telefonun kontrolü için yetkileri alan yazılım cihaz ile ilgili tüm bilgileri C&C (komuta kontrol) sunucusuna gönderiyor ve oradan gelecek komutları uygulamak için beklemeye geçiyor. Yazılımın gönderdiği bilgiler arasında; cihazın IMEI numarası, ISO ülke kodu, Android versiyonu, cihazın modeli, telefon numarası, yüklü uygulamalar gibi birçok önemli bilgi yer alıyor.

Banka ve sosyal medya uygulamalarını açan kullanıcı karşısında aslında gerçek sayfa yerine gerçeği ile neredeyse ayırt edilemeyecek bir sahte sayfa görüyor. Bu sayfaya girilen bilgiler ise saldırganın eline geçmiş oluyor.

### Nasıl silinir?

Uygulama iki yöntem ile telefonlardan silinebiliyor.

İlk adım uygulamaya verilen yetkilerin iptal edilerek ardından silinmesi. Bunun için **Ayarlar** > **Güvenlik** > **Cihaz Yönetimi** > **Google Play Servisi** > **Devre Dışı Bırak** yolunu takip ederek yazılıma verilen yetkiler iptal ediliyor. Ardından sahte “Flash Player” uygulamasının silinmesi için şu yolun takip edilmesi gerekiyor: **Ayarlar** > **Uygulamalar** > **Flash-Player-Güncelleme** > **Kaldır**.

Eğer yazılım “Aktive Et” seçeneği ile yetkilendirilmemişse bunun için farklı bir yol izlenmesi gerekiyor. Bunun da nedeni yazılımın yetki alıncaya kadar sürekli bir pencere açması ve kullanıcının **Ayarlar**> **Uygulamalar** > **Flash-Player-Güncelleme** > **Kaldır** yolunu takip etmesini engellemesi. Böyle bir durumda ise **ADB (Android Debug Bridge)** üzerinden “**adb uninstall [packagename]**” komutu ile yazılım telefondan silinebiliyor.

**İlgili Kişi:**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 927 23 97

erayc@marjinal.com.tr

**Fortinet hakkında**

Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet’in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 290 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.