



ASAL FAKTÖRLER

Mobil cihazlara App Store üzerinden saldırı

ÇETİN KAYA KOÇ koc@krip.to

Mobil sistem uzmanları, kullanıcıları virüs, kötü niyetli yazılım (malware) yazılım ve trojanlara karşı yıllardır uyardıydılar. Ancak böyle gelişmeler birkaç önemsiz olay dışında gerçekten de olmadı. Ancak son birkaç yıldır, Apple stratejisi ile olağanüstü bir şekilde yaygınlaşan App Store teknolojisi bunu değiştireceğe benziyor.

Örneğin çok yaygın bir gelişme var. Türkiye'de örneklerini gördüğümüz gibi birçok banka iPhone, BlackBerry, Windows Mobile ve Google Android platformları için mobil uygulama geliştirip, ilgili App Store ortamlarında kullanıcılara sunmaktalar. Müşteriler belirli kurulum ve aktivasyon işlemlerinden sonra, bunları kullanarak hesaplarına ulaşıyorlar ve borsa işlemlerinden bankacılık işlemlerine (havale, EFT) kadar onlarca işlemi gerçekleştirmekteler. Bu benim de bildiğim ve kullandığım bir teknoloji.

Ancak bir yandan bankalar App Store teknolojisinden yararlanırken, sahte mobil bankacılık uygulamaları da App Store'larda belirmeye başladı. Bunlar gerçek uygulamalardan görsel olarak ayıredilemiyor ve asıl amaçları kullanıcının login bilgilerini elde etmek! Üstelik App Store işletim metodları bunu mümkün de kılıyor. Bir kere Apple, RIM ve Google sundukları (başkaları tarafından üretilmiş) uygulamaların güvenliği veya güvenilirliği konusunda bir garanti vermediklerini en baştan kullanıcıya söylüyorlar. Yani kullanıcılar App Store üzerinden bir uygulama alıp kurdukları zaman, riskleri kabul etmiş durumdadır. Bu jailbroken cihazların App Store sistemleri (Cydia gibi) içinde (belki artırılmış olarak) bir risk. Aslında işletim sistemi bir uygulamanın diğerinin verilerine ulaşmasına engel. Zaten sorunda bu değil. Yüklediğiniz bir oyun programının, yine aynı cihazdaki bankacılık uygulamasının bilgilerine ulaşması söz konusu değil. Burada zincirin zayıf halkası yine kullanıcı. Eğer trojan uygulama, kendisinin geçerli ve doğru bir uygulama olduğuna kullanıcıyı inandırabilirse, elinden login bilgilerini alabilir.