Temassız Tehlike

written by Mert SARICA | 25 November 2011

Son günlerde sahip olduğum kredi kartlarına baktığımda hemen hemen hepsinin temassız kredi kartı (Mastercard ise Paypass yazısı, Visa ise PayWave amblemi) olduğunu farkettim. 2008 yılında temassız kredi kartlarının sayısı bir elin parmaklarını geçmezken günümüzde artık çoğu banka, müşterilerinin kredi kartlarını temassız kredi kartları ile yeniler oldu. Özellikle NFC (Near Field Communication) teknolojisinin cep telefonları ve akıllı telefonlarda yer alması ve yakın zamanda temassız alışverişe imkan sağlayacak olmaları nedeniyle kimi haber sitelerinde yer alan haberlere göre yakın zamanda temaslı ve temassız kredi kartları tarih olarak yerlerini bu cihazlara bırakıyor olacaklar.

Her ne kadar bu ve benzer haberlerin önümüzdeki 5 yıl içerisinde gerçekleşme olasılığı bana göre düşük olsa da bir güvenlik uzmanı olarak cüzdanımda RFID teknolojisini kullanan temassız kredi kartı taşımak yerine NFC teknolojisini kullanmayı tercih ederim. Bunun en büyük nedeni cüzdanınızda bulunan temassız kredi kartı haberiniz olmadan herhangi bir RFID okuyucu ile okunabilirken NFC teknolojisi kullanan bir cihazda bu olasılığın oldukça düşük olmasıdır nedeni ise bunun için öncelikle kredi kartı yerine kullanacağınız mobil uygulamayı çalıştırmış ve NFC vericisini devreye sokmuş olmanız gerekmektedir.

Peki benim gibi cüzdanında temassız kredi kartı taşıyanlar için durum ne kadar vahim veya gerçekten vahim mi ? Gelin bu soruya birlikte yanıt arayalım.

Eğer yıl 2008 olsaydı ve cüzdanınızda temassız kredi kartı taşıyor olsaydınız, meraklı bir kişi, RFIDIOt adındaki yazılım ve desteklediği RFID okuyucu ile temassız kredi kartınızın içinde yer alan etiketi okuyarak adınızı, soyadınızı, kredi kartı numaranızı ve kredi kartınızın son kullanma tarihini kolaylıkla öğrenebilirdi. Nasıl mı ? İşte böyle.

Günümüze gelecek olursak, aynı durumun halen geçerli olup olmadığının yanıtını geçtiğimiz günlerde aramaya koyuldum ve teste başlayabilmek için ilk olarak ihtiyaç duyacağım malzemeleri toplamaya başladım. Temassız kredi kartı olarak geçtiğimiz aylarda elime ulaşan Mastercard'ın temassız kredi kartını, RFID okuyucu olarak OmniKey CardMan 5321 cihazını, okuyucu yazılımı olarak ise RFIDIOt v1.0b yazılımını, işletim sistemi olarak üzerinde Python v2.7.1, pyreadline ve pyscard modüllerinin kurulu olduğu Windows 7 işletim sistemini

kullandım.

Teste başladığım zaman RFIDIOt yazılımının temassız kredi kartında yer alan etiketi okuduktan sonra “Unrecognized TAG (tanımlanamayan etiket)” hatasını döndüğünü gördüm. Hata ile birlikte dönen paketleri incelediğimde bu paketler içerisinde kredi kartı numaramın ve son kullanma tarihinin HEX değerlerinin yer aldığını gördüm. Yaklaşık 1.5 sene önce güncellenen RFIDIOt yazılımında yer alan tanımlı APDU komutlarının ve çözümleme (parse) fonksiyonlarının eski kaldığını düşünerek alternatif yazılımlar aramaya koyuldum ve Brad Antoniewicz‘in blogunda yer alan ChasePayPassBlink yazılımı ile karşılaştım. Ancak bu yazılımın Chase bankamatik/kredi kartına yönelik geliştirildiğini öğrendikten sonra elimde bulunan Mastercard’ın Paypass kredi kartı için bu yazılım üzerinde değişiklikler yapmam gerekeceğini anladım ve kısa bir araştırma ve çalışmanın sonucunda ortaya Paypass Kredi Kartı Okuyucu yazılımı çıkmış oldu. Yazılımı çalıştırır çalıştırmaz temassız kredi kartından kredi kartı numarasını ve son kullanma tarihini başarıyla okuyabildiğini gördükten sonra testi tamamladım.



2008 yılından farklı olarak temassız kredi kartında yer alan etikette artık müşteri adı ve soyadının yer almamasını sevinçle karşılamış olmama rağmen kredi kartı numarasının ve son kullanma tarihinin halen okunabiliyor olması her ne kadar direkt olarak dolandırıcılar tarafından alehyte kullanılamayacak olsa da sosyal mühendislik yöntemleri ile diğer bilgiler ile birleştirilerek kullanılma ihtimali konusunda düşündürtmeye yetti.

Peki ya sonuç ? Sonuç itibariyle cüzdanınızda veya cebinizde bulunan kredi kartı numaranız ve kredi kartınızın son kullanma tarihi bir şekilde (bu 2008 yılındaki videoda olduğu gibi koca bir RFID okuyucuyu cebinize yakınlaştırarak olabilir, RFID kapı anteni kullanılarak olabilir veya StrongLink gibi ufak bir okuyucu kullanarak olabilir) meraklı kişi veya kişiler tarafından okunabilir. Bu ihtimal düşük dahi olsa sizin için önemli bir husus ise çözüm önerisi olarak 20$ gibi cüzi bir ücret ödeyerek internetten sipariş edebileceğiniz RFID korumalı bir cüzdan kullanmanızı önerebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…