RAM Casusluğu

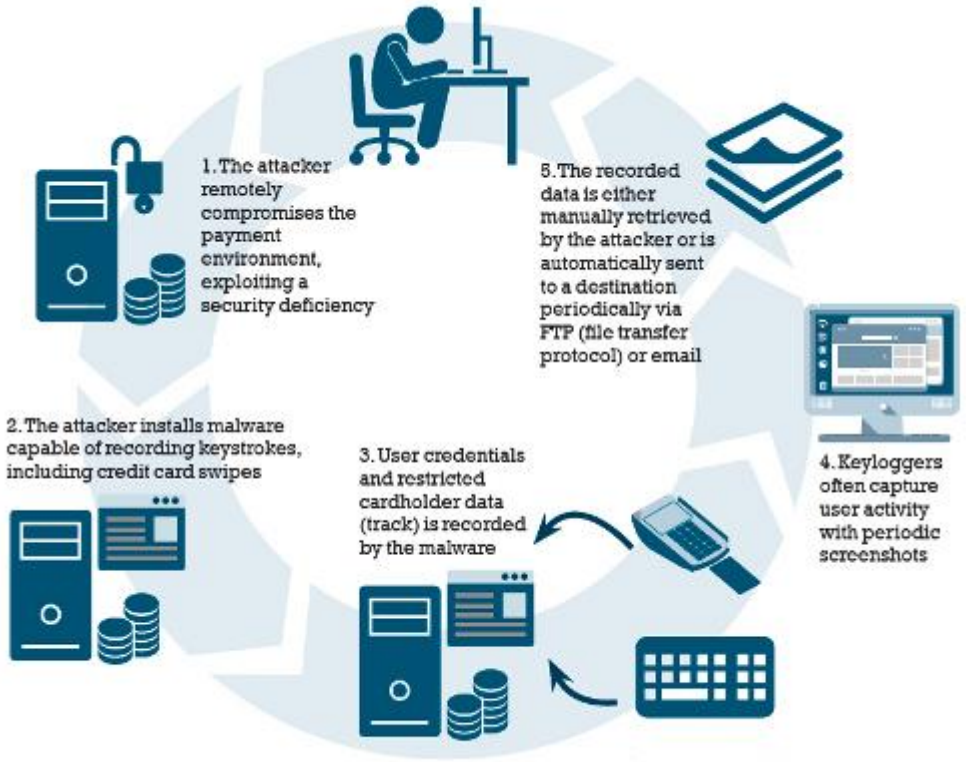
written by Mert SARICA | 1 April 2015

Yaşı yetenler, 2006 yılında yaşanan ve binlerce kredi kartı kopyalanması ile son bulan GİMA vakasını (#1, #2, #3, #4) hatırlayacaklardır. O zamanlarda alışveriş yaptığınız zaman, kredi kartınızı uzattığınız kasiyer, kredi kartınızı alarak POS da dahil olmak üzere mağazanın CRM sistemlerine bilgilerinizi (TRACK / isim, kart no, son kullanma tarihi, cvv2) kayıt etmek için önündeki kart okuyuculara kredi kartınızı okutur ve ardından size teslim ederdi. Gün gelip birileri kart okuyucunun bağlı bulunduğu sisteme zararlı bir kod yerleştirip bu bilgileri kötüye kullanmak için kayıt altına almaya ve kullanmaya başlayınca, GİMA vakası patlak verdi. Bu vaka aslında Türkiye'de kartlı ödeme sistemleri için bir milat oldu çünkü bu vaka sonrasında çipli kartların kullanımı zorunlu hale gelerek TRACK bilgisinin POS cihazları dışında başka cihazlara okutulmasının önüne geçildi. Hatta günümüzde bazı banka POS cihazlarının yan tarafında bulunan kart okuyucusuna kredi kartınızı okutmaya (swipe) çalıştığınız zaman POS cihazının "bu işlem desteklenmemektedir" şeklinde bir hata mesajı ile sizi güvenli ödeme kanalına (çip okuma) yönlendirdiğini görebilirsiniz. Özetle günümüzde alışveriş yaparken çipli kredi kartınızı POS cihazına bağlı olan kart okuyucuya okutursunuz, ardından PIN bilgisini girerseniz ve ardından bu bilgiler POS cihazına gönderilip, işlendikten sonra ilgili bankaya şifreli olarak gönderilmektedir. (Bu işlem esnasında kullanılan POS cihazını, donanımsal saldırılara karşı korunaklı, kapalı bir kutu gibi düşünebilirsiniz.)

Track bilgisinin dolandırıcılar tarafından papağan dediğimiz manyetik kart okuyucular ile rahatlıkla okunabileceğini ve kopyalanabileceğini asla unutmayın bu nedenle mağazalarda veya restaurantlarda kredi kartınızı POS cihazına kendiniz takmaya önem gösterin.

Bankacılık ve ödeme sistemleri olarak gerimizde olan ABD ve bazı ülkelerde durum ise biraz daha farklıdır. Bu ülkelerde çipli kartlar yaygın olarak kullanılmadığı gibi kredi kartının okutulduğu kart okuyucu ve bunun bağlı bulunduğu POS sistemi (bizdeki kapalı kutu POS cihazı, onlarda Windows üzerinde çalışan POS uygulaması) ilgili mağazanın kullandığı sistemler (windows yüklü bir PC) üzerinde çalışmaktadır. Durum böyle olunca da art niyetli kişiler tarafından ele geçirilen bu sistemlere yüklenen zararlı yazılımlar ile müşterinin kart okuyucusuna okuttuğu TRACK bilgisi, sistemin

belleği (RAM) üzerinden çalınabilmektedir. (ram scraping yöntemi)

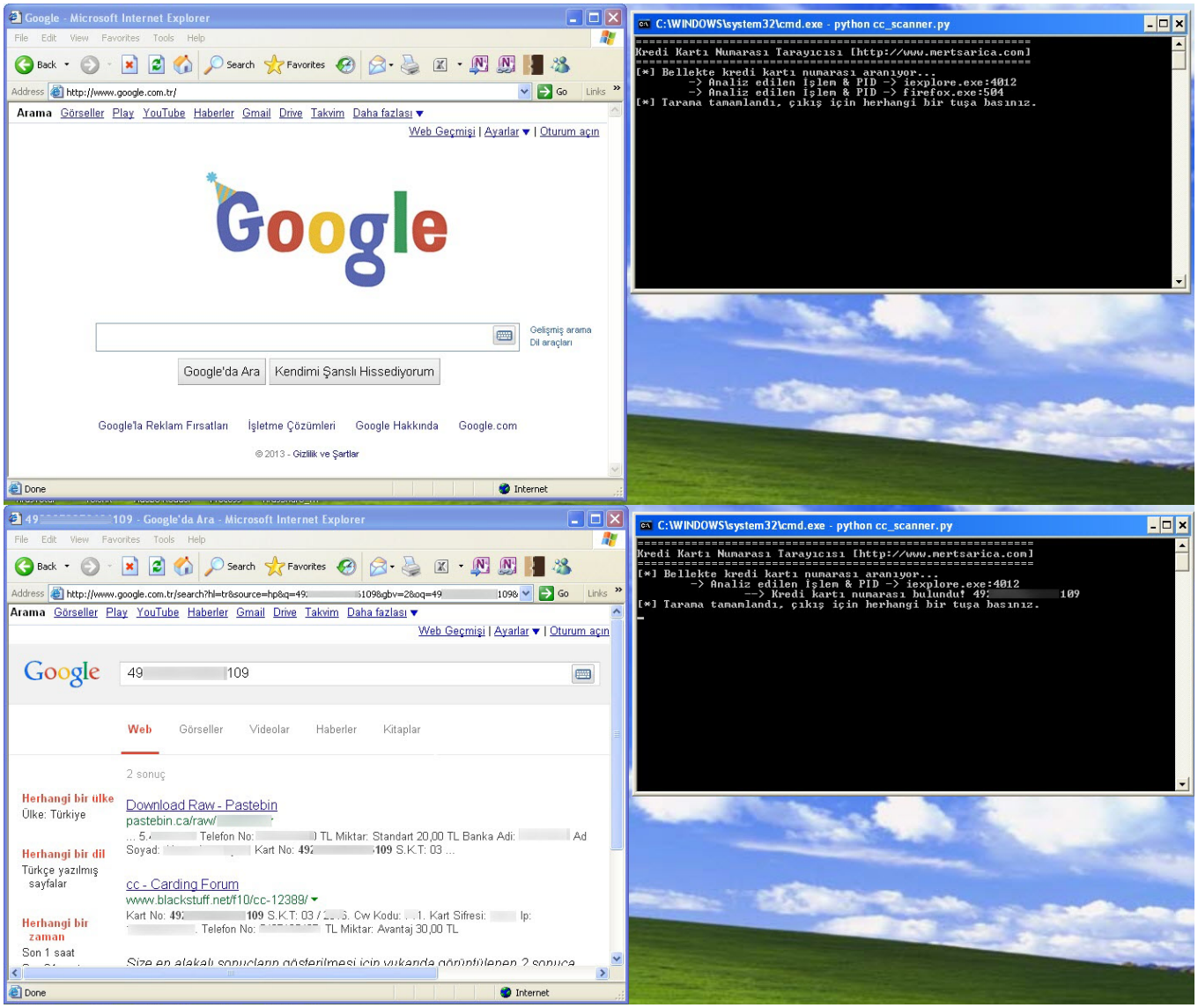


Bu yöntemden kısaca bahsetmek gerekirse, zararlı yazılımın yaptığı işlem, RAM üzerinde POS uygulaması tarafından kullanılan alanı bulmak ardından REGEX yardımı ile bu alanda kredi kartı numarasını aramaktır. Tabii bu REGEX'e göre 16 haneli numara aramak, hatalı sonuçlar da (false positive) üretebileceği için zararlı yazılım geliştiricileri burada kredi kartı numarasını doğrulamak için LUHN algoritmasından faydalanmaktadırlar.

Luhn algoritması, 1954 yılında, IBM firmasında çalışan Hans Peter Luhn tarafından kredi kartı numarası, IMEI, Kanada sosyal güvenlik numarası gibi numaraları doğrulamak amacıyla geliştirilmiş olan bir formüldür. Bu formül sayesinde kredi kartı bilgisi girilmesi istenen formlarda girilen kartın doğruluğu (TCKN kontrolü gibi düşünebilirsiniz) teyit edilmektedir.

Pratikte art niyetli kişilerin bu yöntemi kullanan bir araç yazmalarının ne kadar zor olabileceğini anlama adına Python ile RAM'i, REGEX ve Luhn algoritmasına göre tarayan ve kredi kartı numarası arayan bir araç hazırlamaya karar verdim. WinAppDbg Python modülü sayesinde yarım saat içinde CC Scanner adında basit bir araç geliştirebildim. (Kaynak kodunu kötüye kullanılmaması adına paylaşmıyorum.) Aracı test etmek için PasteBin sitesinden bulduğum örnek bir kart numarasını Google'da arattım ardından CC Scanner aracının bu kart numarasını RAM üzerinden tespit edip edemeyeceğini

kontrol ettiğimde başarıyla tespit edebildiğini gördüm ve görev başarıyla tamamlanmış oldu.



Umarım bu yazı ile bana sıkça sorulan “RAM’den kart bilgisi çalan zararlı yazılımları ülkemizde etkili mi?” , “Biz neden/nasıl oluyor da etkilenmiyoruz ?”, “art niyetli kişilerin kullandıkları yöntem nedir ?” , “bu yöntemi kullanmak zor mu yoksa kolay mı?” sorularına yanıt verebilmişimdir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.