Farkında mısınız ?

written by Mert SARICA | 5 May 2010

Oldum olası cep telefonuma gelen reklam mesajlarından nefret etmişimdir. Usanmadan bıkmadan ulaşılabilir olanlara ulaşıp bir daha reklam mesajı göndermemeleri konusunda kendilerinden her defasında ricada bulunurum ne mutluki kimileri bir daha reklam mesajı göndermezler, Garanti Bankası gibi müşteri memnuniyetine önem vermeyen (6 defa haklı müşteri hattını arayıp rica etmeme rağmen reklama devam!) kurumlar ise reklam mesajı göndermeye devam ederler.

Yine geçtiğimiz günlerde bir öğlen vakti cep telefonuma bir mesaj geldi, "Yine mi Garanti, yine mi Bonus" diye mesaja baktığımda bu defa yanıldığımı gördüm çünkü son günlerin moda mesajlarından biri olan ve dolandırıcılar tarafından gönderilen "Tebrikler hediye kol saati kazandınız hemen 0532 111 85 85'i arayın" mesajını almıştım. Son günlerde dolandırıcılar ya bedava kol saati ya da bedava checkup kazandınız şeklinde cep telefonlarına mesajlar göndererek insanların kredi kartı bilgilerini toplayarak yüklü miktarda para çekerek insanları dolandırıyorlar. Konu ile ilgili daha detaylı bilgiye buradan ulaşabilirsiniz.

Yıllardan beri kullandığım bir numara olması nedeniyle bu mesajları almayı aslında pek fazla yadırgamıyordum çünkü alışveriş esnasında alınan bu ve benzer bilgilerin bir şekilde değerlendirilip nakte döndürüldüğünden hiç şüphem yoktu. İşim gereği her konuya ister istemez art niyetli insanların gözünden bakmayı alışkanlık haline getirmiş biri olarak "acaba niyetim sms ile reklam yapmak olsaydı veya bir kişinin cep telefonu bilgisini öğrenmek olsaydı bunu nasıl başarabilirdim" sorusu uzun zamandan beri aklımın bir köşesinde yanıtlanmayı bekliyordu.

Bir ilan aramak için geçtiğimiz günlerde meşhur bir ilan arama web sitesini ziyaret etmem gerekmişti. İlan ara menüsündeki kategorilerde yer alan son 1 aylık ilanlara göz attığımda (~ 450.000 ilan) dikkatimi en çok çeken kısım ilan sahiplerinin isim, soyad ve cep telefonu bilgilerini vermekten hiç çekinmedikleri olmuştu.

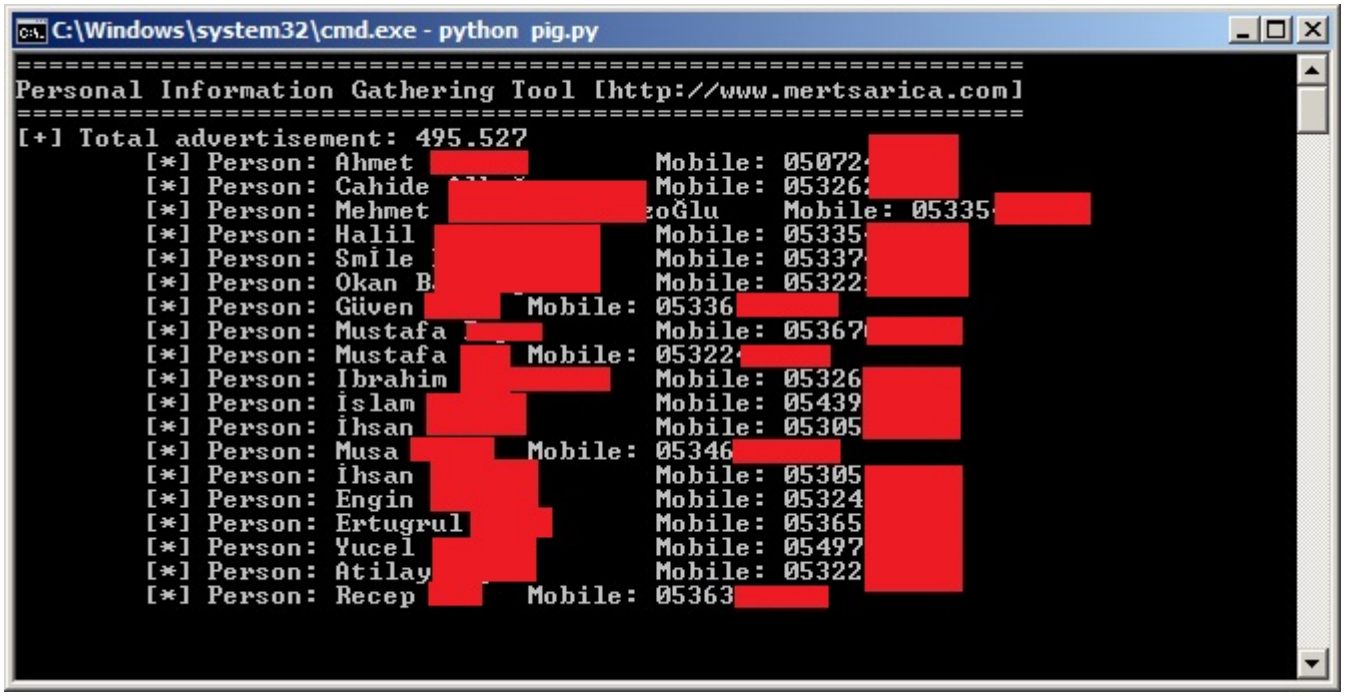
Belki farkındalık eksikliği belki kendi tercihleri ancak isim, soyad ve cep telefonu bilgisi özellikle günümüzde bankaların internet bankacılığı girişlerinde zorunlu tuttuğu tek kullanımlık şifre ile oldukça önem kazanmış

ve dolandırıcıların sosyal mühendislik saldırılarını başarıya ulaştırabilmeleri için sahip olmak istedikleri bilgiler arasında üst sıralarda yer almaktadır.

Örneğin penetrasyon testlerinde, sosyal mühendislik saldırısının asıl amacı hedef sisteme sızmak, erişim bilgilerini almak için hedef kişiyi kandırmak ve sizle bu bilgileri paylaşmasını veya size erişim vermesini sağlamaktır. Ancak gerçek hayatta dolandırıcıların amacı sosyal mühendislik ile kişisel bilgilerini nakte çevirmek için veya internet bankacılığı hesabınıza erişmek için bu bilgileri toplamak olabilir. Dolandırıcı benim isim, soyad ve cep telefonu bilgim ile beni nasıl daha kolay kandırabilir sorusuna hemen ufak bir örnek ile yanıt vereyim.

Örneğin art niyetli bir kişi tarafından kurbanın e-posta şifresini ele geçirmek için gönderdiği bir yemleme (phishing) e-postasında “Merhaba, E-posta sistemimizdeki bir arıza nedeniyle şifrenizin güncellenmesi gerekmektedir, lütfen doğrulama amacıyla kullanıcı adınızı ve parolanızı bize iletin” şeklinde bir mesaja yer vermesi kurbanı kandırmak için yeterli olmayabilir fakat “”Merhaba Mert SARICA, E-posta sistemimizdeki bir arıza nedeniyle şifrenizin güncellenmesi gerekmektedir. 05xx xxx xx xx numaralı cep telefonunuza yeni şifrenizi gönderebilmemiz için doğrulama amacıyla kullanıcı adını ve parolanızı bize iletin” şeklinde hazırlanmış bir mesajın başarıya ulaşma ihtimali bir önceki mesaja kıyasla daha yüksek olacaktır.

Peki bu art niyetli kişilerin bu bilgileri isim, soyad ve cep telefonu bilgilerinin paylaşıldığı bu ve benzer ilan sitelerden toplamak ne kadar kolay olur sorusuna yanıt aramaya koyuldum ve hemen bir senaryo ürettim. Örneğin art niyetli bir kişi bu meşhur ilan arama sitesinde yer alan tüm ilanlardaki isim, soyad ve cep telefonu bilgilerini toplamak istiyorsa yapacağı ilk iş ne olur dedim ve akıl hastası değilse teker teker tüm ilanları gezmek tercih edeceği en son yol olur bu nedenle program yazmak ilk tercihi olur dedim ve ben de ufak bir program yazmaya karar verdim ve karar verdikten 4 saat sonra program hazırdı.



Siz siz olun kişisel bilgilerinizi özellikle internet sitelerinde paylaşmadan önce nelere mal olabileceğini ve kimlerin eline geçebileceğini tekrar düşünün. Bir sonraki yazıda görüşmek dileğiyle hoşçakalın…

Not: Bu program bilgi güvenliği farkındalığını arttırmak amacıyla programlanmıştır. Etik değerler ve güvenlik gerekçelerinden ötürü kimseyle paylaşılmamıştır, paylaşılmayacaktır.