



Türkiye'de internet ve mobil bankacılık kanallarının yaygınlaşması, işlem hacminin yükselmesi ile birlikte karşılaşılan risk ve tehditler de hızla artıyor. Günümüzde artık basit ve kolay önenebilir saldırılar yerine çok daha karmaşık ve 'ancak uzmanlaşma' ile önenebilecek teknikler kullanılıyor. Bankacılık sektörüne yönelik saldırılar için kullanılan ve hedefe yönelik atak yapabilmek için tasarlanan zararlı yazılımlar zaman içerisinde çok karmaşık bir hale geldi ve artık birer saldırı kiti olarak dolandırıcılık dünyasında pazarlanıyor. Trojan gibi zararlı yazılımla yapılan dolandırıcılık teknikleri saldırı türlerinin en başında geliyor ve bankacılık kanalları için tehditler oluşturuyor. Bankacılık Trojan'ı olarak da adlandırılan bu zararlı yazılım türleri, kullanıcıların bilgisayar ve mobil cihazlarına bulaştıktan sonra, kullanıcıların önüne bilgilerini ve sabit şifrelerini/tek kullanımlık şifrelerini ele geçirecek ekranlar getiriyor.

Bu ekranlar vasıtasıyla elde edilen bilgiler kullanılarak müşteri bilgisi dışında işlemler gerçekleştiriliyor. Gün geçtikçe sayısı artan bankacılık trojanlarının en bilinenleri Zeus (türevleri), SpyEye olmasına rağmen, Trojan etkinliği ülkelere göre farklılık gösterebiliyor. Yükselmekte olan bu tehdidi fark eden Yapı Kredi, 2014 yılında internet ve mobil bankacılık kanallarındaki müşterilerini korumak amacıyla IHS Telekom ile birlikte kapsamlı bir Trojan Tespit Projesi başlattı.

IHS Kurumsal ve Yapı Kredi Dolandırıcılık ve Suistimalleri Önleme Birimi'nin ortak çalışması ile iki ay gibi kısa bir sürede hayata geçirilen proje, internet ve mobil bankacılık kanallarındaki trojan riskinin gerçek zamanlı olarak izlenmesini ve fraud (sahtecilik) faaliyetlerine, finansal işlem henüz gerçekleşmeden müdahale edilebilmesini sağladı. Trojan tespit sisteminin diğer dolandırıcılık katmanları ile entegre çalışabilmesi sayesinde ileri seviye ve karmaşık saldırılar artık Yapı Kredi Bankası tarafından etkin bir şekilde önlenabiliyor.

Müşteriler ile hiçbir etkileşime girmeden, gerçek zamanlı olarak tespit edilen trojan aktiviteleri, Yapı Kredi Dolandırıcılık ve Suistimalleri Önleme Birimi tarafından analiz edilerek engelleniyor. Bu transparan teknoloji sayesinde müşterilerin internet bankacılığı deneyimleri etkilenmiyor.

YAPI KREDİ KONUSU İLE İLGİLİ ŞUNLARI SÖYLÜYOR:

Dijital bankacılık dünyası işlem çeşitleri, müşteri sayısı, kullanılan teknoloji, yatırımları ile devasa bir yapı. Bankalar 15 yıllık alternatif dağıtım kanal deneyimleri ile geliştirdikleri elektronik bankacılık altyapıları sayesinde müşterilerine fiziki para yatırma haricindeki tüm işlemlerini PC, tablet, cep telefonu ve hatta giyilebilir teknolojiler ile hizmet verebilir hale geldiler.

Bu yapıya yatırım yapan bankalar için güvenilirlik ve prestijini artırılması, ürün satışının yaygınlaştırılması gibi sebeplerden dolayı önümüzdeki dönemlerde de dijital kanallar önemini koruyacak. Dijital kanalların hızlı, kolay ve sınırsız erişimi, ucuz işlem ücretleri, yüksek hizmet kalitesi gibi nedenlerden dolayı müşteriler tarafından yaygın olarak kullanılıyor. Rakamsal verilere bakıldığında sektördeki yüksek kalite - ucuz hizmet etkileşimi sayesinde 2006 yılına göre internet bankacılığı kullanıcı sayısının %350 artış göstererek 15 milyonun üzerine çıktığı görülüyor.

İnternet ve mobil kanalların ifade edilen yapısal ve fonksiyonel gelişimleri, beraberinde dolandırıcılık araçlarının da evrilmesi konusunu meydana getirdi. Artık basit bir keylogger veya sim kartın ele geçirilmesi yerine çok daha sofistike dolandırıcılıkların gerçekleştiğini söyleyebiliriz. Bu sebeple bankalar dijital alanda yapı ve süreçlerinin güvenliğini farklı katmanlara farklı önlemler geliştirerek sağlıyorlar.

Yapı Kredi olarak yaptığımız risk değerlendirmesi neticesinde müşteri cihazlarının oldukça önemli derecede güvenlik açığı oluşturduğunu gördük. Türkiye'deki teknoloji tüketicileri her ne kadar güncel cihaz modellerini takip etse de kullanım alışkanlıklarına yönelik güvenlik önlemleri konusunda yeterli bilinç düzeyine sahip değiller. PC'lerde lisanslı işletim sistemlerinin olmaması, orjinal ve güncel antivirüsler kullanılmaması, mobil cihazların yazılımlarının kırılması (root-jailbreak) gibi noktalar bunlardan bazıları. Güvenlik düzeyinin düşük olduğu bu cihazlardan internet bankacılığı işlemleri gerçekleştirildiğinde, çeşitli zararlı yazılımlar müşteriye ait hem şifre hem de bankalardaki davranış modelini çalarak dolandırıcılıklara sebep olabiliyor. IHS ile gerçekleştirdiğimiz proje ile bankamız, bu kapsamdaki müşterilerine aynı kalitedeki hizmetini vermeye devam ederken aynı zamanda onları finansal zarar veren durumlardan koruyarak çok daha güvenli dijital bankacılık ortamları oluşturur pozisyona geldi.

YAPI KREDİ BANKASI

MUTLU ATAKIŞI Uyum ve İç Kontrol/ Dolandırıcılık ve Suistimalleri Önleme Direktörü
UĞUR LEVENT ÖZCOŞKUN Uyum ve İç Kontrol/ Elektronik Bankacılık Suistimalleri Önleme Müdürü
SEBAHATTİN SEZER Uyum ve İç Kontrol/ Elektronik Bankacılık Suistimal İzleme ve Önleme Yöneticisi
AZİZ BELKAYA Bilişim Teknolojileri ve Operasyon Yönetimi/ Dijital Bankacılık Yazılım Geliştirme - Kıdemli Proje Mühendisi
KORHAN ŞEN Bilişim Teknolojileri ve Operasyon Yönetimi/ BT Güvenlik Yönetimi - Sistem Yöneticisi

IHS TELEKOM

BÜLENT ÖZKAN Genel Müdür Yardımcısı
KADIR YÜCEER Kurumsal Entegrasyon Müdürü

**BİR BAŞARI
HİKAYESİ**