COMODO LABORATUVARLARINDAN: Tüm Dünyada Kimlik Avına Yönelik Yeni Bir E-Posta Dolandırıcılık Hareketi Apple Kimliklerini Hedefliyor

Comodo Antispam Labs ekibi, Apple kimliğine sahip tüm işletmeleri ve tüketicileri hedefleyen ve kimlik bilgilerini, parola ve kredi kartı bilgilerini çalmak için tasarlanmış yeni bir global kimlik avı (phishing) tehdidi tespit etti. Apple, 800 milyondan fazla iTunes hesabı olduğunu rapor etmişti.*

“Sahte Apple” kimlik avı (phishing) e-postaları tıpkı Apple tarafından gönderilen kurumsal e-postalara benziyor; Apple logosunu da taşıyan e-postalarda Apple'ın fiziksek adresi ile birlikte Apple görevlilerine aitmiş gibi görünen bir e-posta adresi de veriliyor ve böylece alıcıda e-postanın gerçek olduğu yanılsaması yaratılıyor.

E-posta, alıcıya Apple hesaplarına bazı sınırlamalar getirildiğini ve bunu düzeltmek için alıcının verilen bağlantıdaki adreste bazı bilgileri girmesi gerektiğini söylüyor. Alıcı verilen bağlantıya tıkladığında, Apple'a aitmiş hissi ve görünümünü veren ek sayfalara yönlendiriliyor ve bu sayfalarda alıcıdan kredi kartı bilgilerini ve parolalarını doğrulaması isteniyor. Siber hırsızlar işte bu aşamada bilgileri çalıyor.

Comodo Antispam Labs ekibi bu Apple kimlik avı e-postasını yaptıkları IP, alan adı ve URL analizleri sonucunda ve Laboratuvarın Comodo İnternet güvenlik sistemlerinin kullanıcılarından gelen veriler üzerindeki sürekli izleme ve taramaları sonucunda tespit etti.

“Comodo Antispam Laboratuvarı, çevrim içi (online) dünyayı korumak ve güvenli bir yer haline getirmek için yenilikçi ve tescilli Comodo siber güvenlik teknolojilerini kullanan mühendislerden ve bilgisayar bilimcilerinden oluşan bir uzmanlık kaynağıdır." diyen Comodo Teknoloji Müdürü Fatih Orhan sözlerine şunları ekledi: “Siber suçluların bir adım önünde olan, BT ortamlarının ve işletmelerin güvenli olmasını sağlayan yenilikçi teknoloji çözümlerini geliştirip uygulamak için özenle çalışmaya devam edeceğiz.”

Şirketinizin BT ortamının kimlik avı (phishing) amaçlı saldırılara, kötü amaçlı yazılımlara, casus yazılımlara veya siber saldırılara maruz kaldığını düşünüyorsanız Comodo Antispam Labs güvenlik danışmanlarıyla irtibata geçin: https://enterprise.comodo.com/contact-us.php

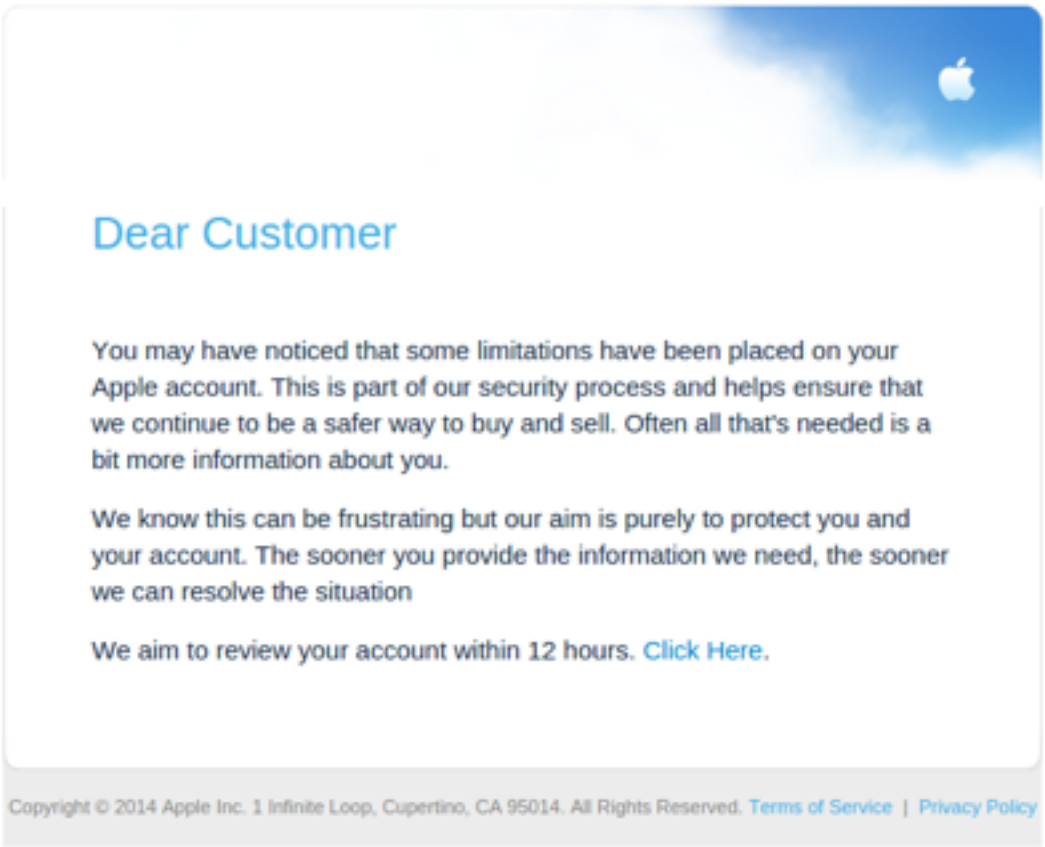
Comodo Antispam Labs tarafından tespit edilen Apple kimlik avı e-postaları hakkındaki bilgiler ve ekran görüntüleri aşağıda verilmiştir.

*Verilerin alındığı kaynak: Apple Shareholders Call, Forbes.com: http://www.forbes.com/sites/nigamarora/2014/04/24/seeds-of-apples-new-growth-in-mobile-payments-800-million-itune-accounts/

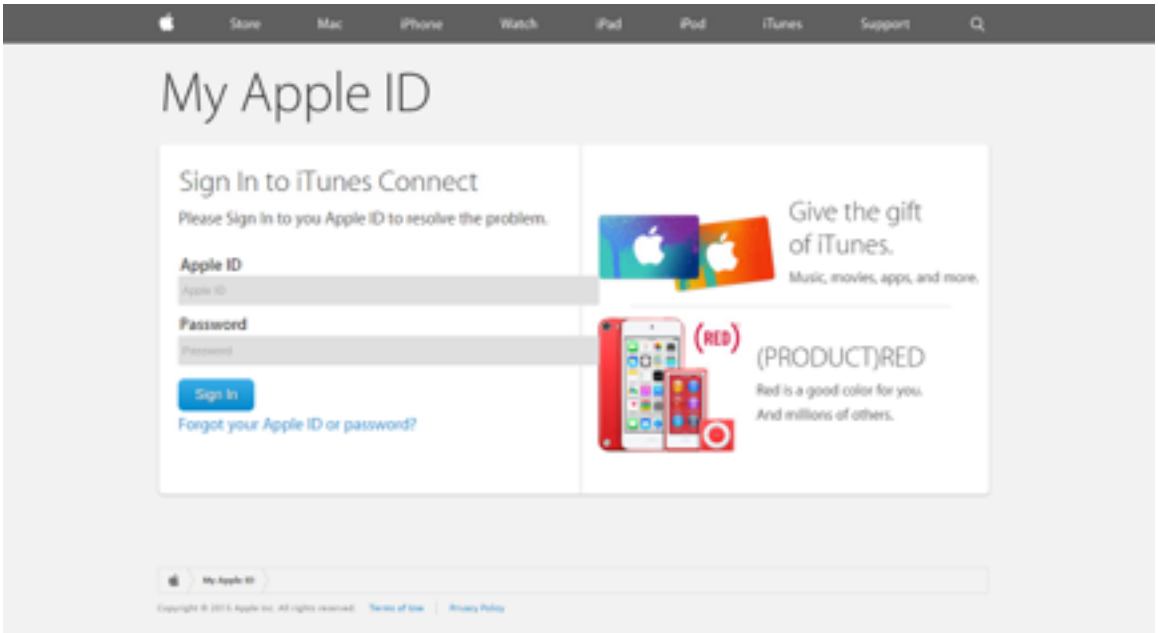
Kimlik Avı Ekran Görüntüleri ve Bilgileri

E-posta İçeriği

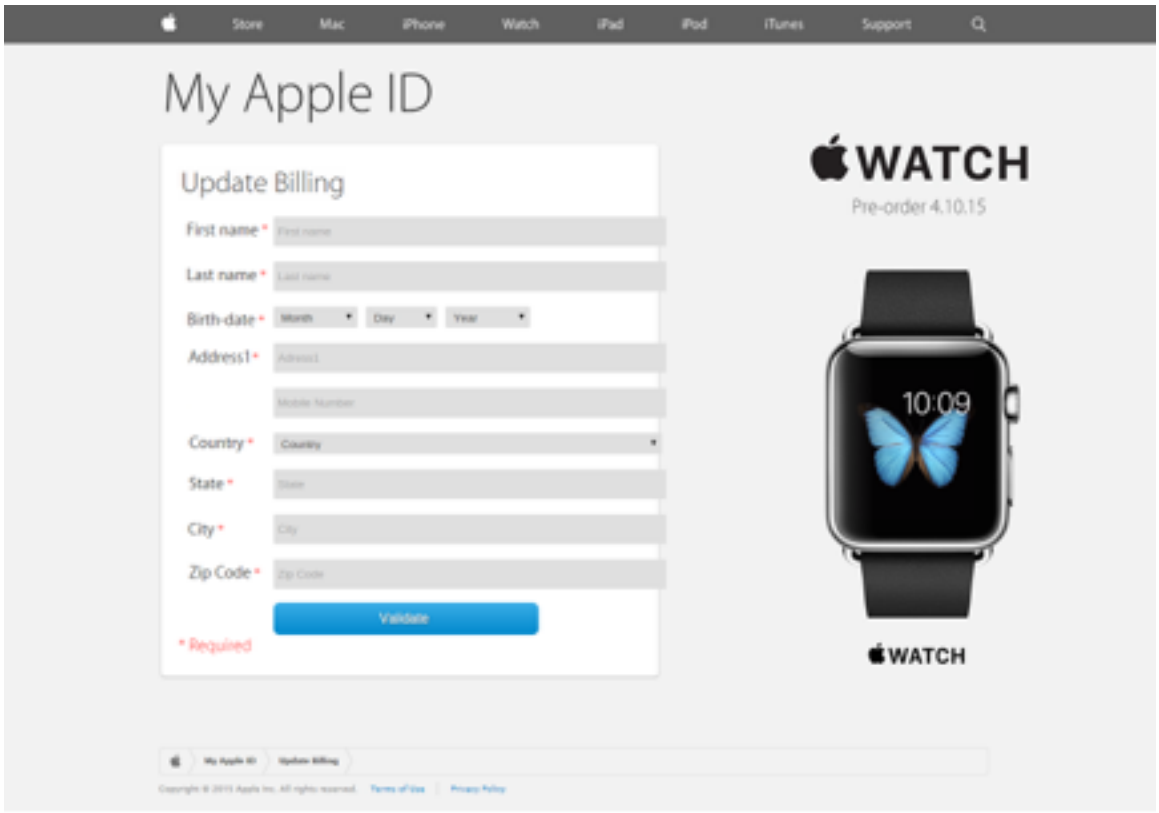
Kimden: Apple <verefy@appe.com>
Kime: *gizli*
Yanıtla: Apple <verefy@appe.com>
Konu: Apple Kimlik Bilgilerinizi Teyit Edin - AppleID Destek

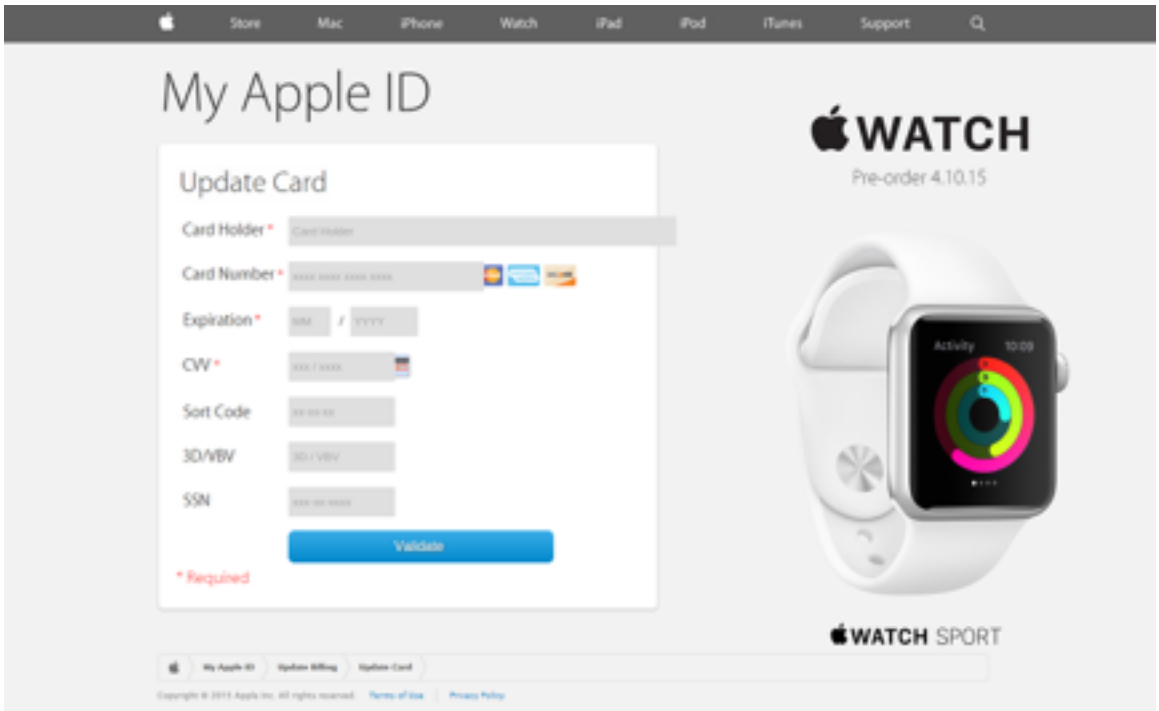


Alıcı yukarıdaki “Buraya Tıklayın” ("Click Here") bağlantısına tıkladığında aşağıdaki sayfaya gönderiliyor:



Kurban Apple ID kimlik bilgilerini ve parolasını girip "Oturum Aç" butonuna tıkladığında son sayfaya yönlendiriliyor; bu son sayfa ise siber hırsızlar için en önemli bölümler çünkü buralarda alıcıdan kişisel bilgilerini ve ardından kredi kartı bilgilerini girmesi isteniyor:


Store
Mac
iPhone
Watch
iPad
iPod
iTunes
Support
My Apple ID
Update Billing
First name *
Last name *
Birth-date *
Month
Day
Year
Address1 *
Country *
State *
City *
Zip Code *
Validate
* Required
WATCH
Pre-order 4.10.15
10:09
WATCH


Store
Mac
iPhone
Watch
iPad
iPod
iTunes
Support
My Apple ID
Update Card
Card Holder *
Card Number *
Expiration *
CVV *
Sort Code
3D/VBV
SSN
Validate
* Required
WATCH
Pre-order 4.10.15
Activity
10:09
WATCH SPORT

Bu son sayfada kredi kartı bilgileri alınıyor ve o aşamaya dek kimliği bilinmeyen kurban "Onayla" (Validate) butonuna bastığında siber hırsızlar tüm bilgileri almış oluyor.

BT'lerinin sahte Apple kimlik avı (phishing) e-postalarına maruz kalabileceğini düşünen sistem BT yöneticilerinin dikkat etmesi gereken adresler, kötü amaçlı URL'ler, alan adları ve IP adresleri aşağıda verilmiştir.

E-postanın geldiği adres: verify@appe.com
E-posta içindeki kötü amaçlı URL: https://srv80.prodns.com.br/~good/my-account/en/
URL Alan Adı: prodns.com.br
IP Adresi: 192.185.215.210