COMODO LABS: Siber hırsızlar Pandora Mücevherat'ın şifrelerini çalıyor

Siber hırsızlar bu kez dünyaca ünlü mücevher üreticisi ve satıcısı Danimarkalı Pandora Mücevherat'ı hedef aldı. Pandora Mücevherat'tan alışveriş yapan şirket ve müşterileri hedefleyen virüs saldırısını Comodo Antivirüs Laboratuvarları (CASL) ekibi ortaya çıkardı.

Pandora Mücevherat tıpkı diğer büyük markalar gibi tatil sezonlarında müşterilerine özel indirimler yapıyor. İşte bu dönemde; siber hırsızlar da harekete geçiyor ve elektronik postalar yoluyla şifre çalma olayları (phishing) artıyor.

Comodo ekibi; siber hırsızların Pandora Mücevherat müşterilerine kişiye özel kolye, yüzük ve bilezik ürünlerinde büyük indirim yapılacağını duyuran virüslü elektronik postalar hazırladığını belirledi. Bu elektronik postalar; Pandora'dan alışveriş yapan şirket ve kişilerin kredi kartı ve elektronik posta bilgilerini yakalamak için tasarlanmıştı. Virüslü elektronik postalar Pandora müşterilerine "Pandora İndirimi" konu başlığı ile
custserv@aquae.kao6161.com adresinden gönderildi.

Virüslü postalar müşterilerin elektronik posta kutularına düştüğünde; elektronik postaların hayali bir mücevher satıcısı tarafından gönderildiği görüldü.
Çünkü Pandora Mücevherat; yetkili satıcılarına, elektronik posta yoluyla ya da internet siteleri aracılığıyla müşterilere özel indirim duyurusu yapılmasına genelde izin veriyor. Bu yüzden de sözkonusu virüslü elektronik postaLar şüpheci olmayan müşteriler için büyük tehlike yaratıyor.
Comodo Antivirüs Laboratuvarları ekibi Pandora Mücevherat'ı hedef alan virüslü elektronik postayı IP, alan adı ve URL analizi yoluyla tanımladı.

Gönderilen bağlantıların, ziyaretçileri http://www.pandora.net adresine yönlendirmesi gerekirken; ziyaretçilerin http://www.bestpandorajewelry.com/index.html adresine ulaştıkları anlaşıldı.

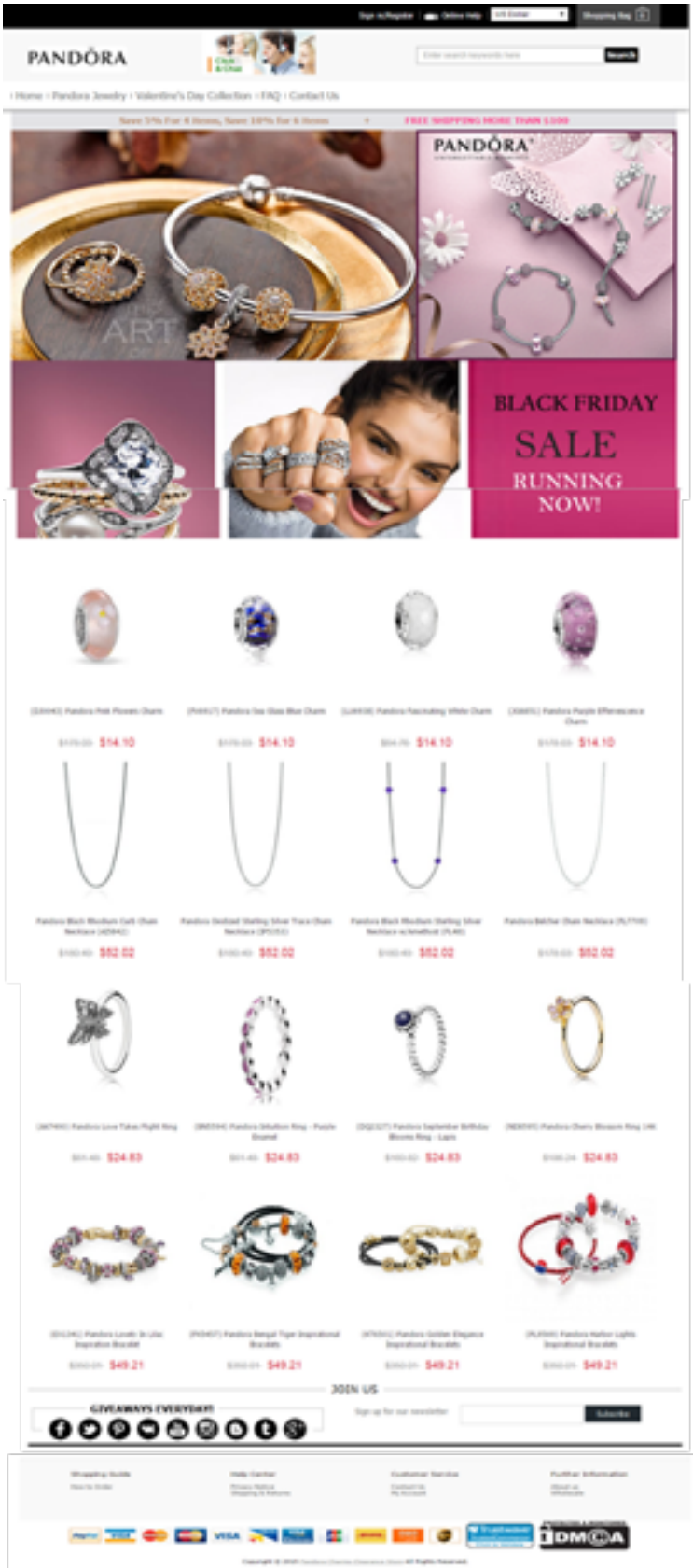
Comodo ve Comodo Antivirüs Laboratuvarları Teknoloji Direktörü Fatih Orhan, virüslü elektronik postaların günümüzde teknoloji kullanıcıları için en büyük tehditlerden biri olduğuna dikkat çekiyor. Orhan, "Çünkü bu elektronik postalar; müşteriler, şirketler ve markalar arasındaki güveni istismar ediyor. Hackerlar müşterilerin bilgilerini ve/veya elektronik posta bilgilerini çalmak için kendilerini bir şirket sahibi gibi; ya da bir e-ticaret sitesi veya popüler bir sosyal medya ağındanmış gibi gösterebiliyorlar" diyor. Fatih Orhan bu
yüzden Comodo'da çalışmaların 'çok özenle' yürütüldüğüne dikkat çekiyor ve "Siber suçlulardan bir adım önde olan, şirketleri ve BT ortamlarını güvende tutan yenilikçi teknoloji çözümleri üretmek için özenle çalışıyoruz" vurgusu yapıyor.

Comodo Antivirüs Laboratuvarları ekibi; tam gün Comodo çalışanı olan ve dünya çapında virüs, virüslü elektronik posta ve kötü amaçlı yazılımları analiz ederek filtreleyen 35'i aşkın BT güvenliği profesyoneli etik hackerlar, bilgisayar uzmanları ve mühendislerden oluşuyor. Ekip; günde bir milyondan fazla potansiyel virüslü elektronik postayı analiz ederek ulaştığı bulguları; mevcut müşteri tabanı ile genel olarak halkı, şirketleri ve internet topluluğunu güvenli kılmak için kullanıyor. Ekibin bu çalışmasına ABD, Türkiye, Filipinler ve Hindistan'daki ofisleri katkı sağlıyor.

Şirketinizin BT ortamının kötü amaçlı elektronik posta, yazılım, casus yazılım saldırıları veya siber saldırılar altında olduğaıseziyorsanız; Comodo'daki güvenlik danışmanları ile irtibat kurunuz: https://enterprise.comodo.com/contact-us.php

E-posta ve Ekran Görüntüleri

Alıcıların ilk karşılaştıkları elektronik posta ekranı, aşağıdaki gibidir. Elektronik postadaki "Shop Now" (Şimdi Satın Al) kısmı siber hırsızların; şirketlerin ve müşterilerin alışverişe başlamak için tıklamasını bekledikleri alandır. Hırsızlar bu kısım yoluyla söz konusu kişilerin elektronik posta bilgilerini ele geçirebilirler.



"Shop Now" kısmına tıklayan kullanıcıların yönlendirildiği HTML sayfası

BT'lerinin sahte e-mail tehtidine açık olduğunu düşünen Sistem BT Yöneticileri için, gönderenin e-mail alan adresi "aquae.kao6161.com" şeklindedir. Alan adresi 2015-03-31T00:00:00+08:00Z'de; Fucain, Çin'den alınmıştır.

###

İletişim:

Hilal Köylü

GTC İletişim Danışmanlığı

Telefon: +90 312 447 00 20

E-posta: hilal.koylu@gtc.com.tr