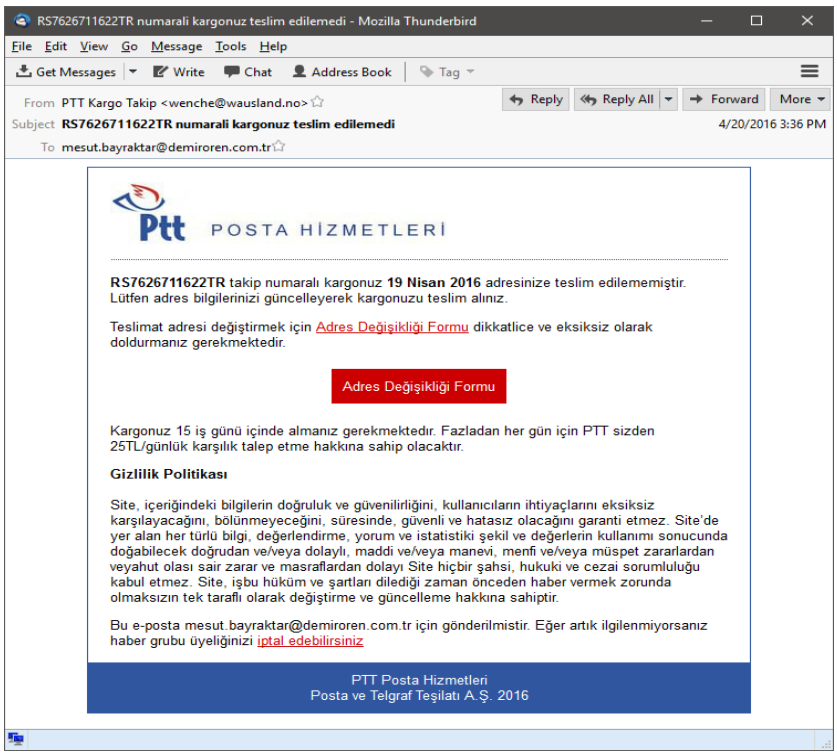
COMODO
Creating Trust Online®

Hackerlar PTT müşterilerinin peşinde

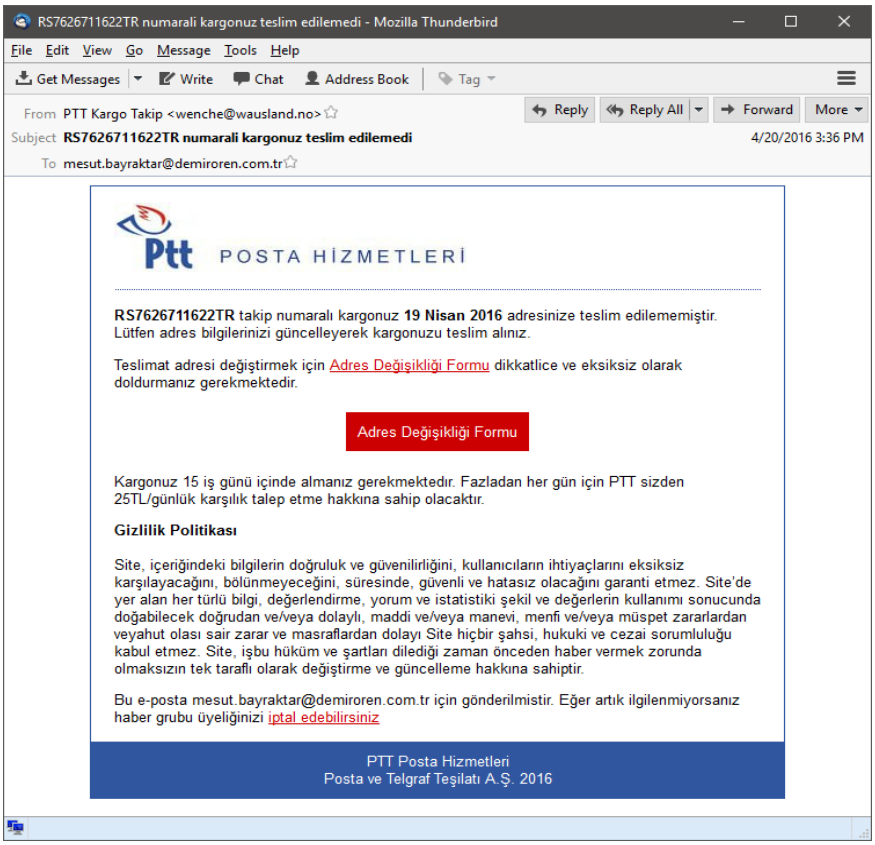
“PTT müşterilerini hedefleyen Cryptolocker saldırıları yoğun olarak tekrar gündemde”

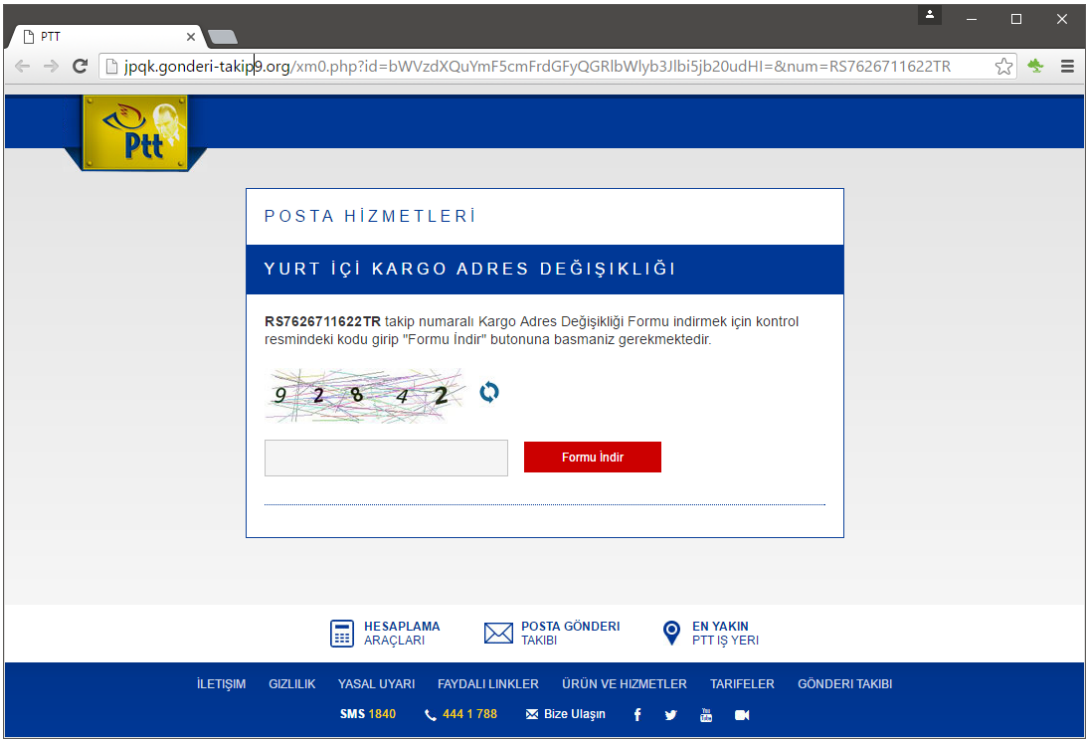
COMODO – 09.05.2016 İnternetteki virüs saldırılarıyla stratejik bir mücadele yürüten siber güvenlikte dünya devi Comodo, hackerların PTT ismini de kullanarak virüslü mesajlar ürettiğini belirledi. İnternet kullanıcılarına resmi olarak PTT’den geliyormuş gibi gönderilen e-postaların içeriğinde kargo gönderisinin adrese ulaştırılamadığı belirtiliyor ve kargonun alınması için adres değişikliği formunun doldurulmasını istiyor.
PTT görünümlü maillere dikkat edilmesi gerektiğini belirten Teknoloji Direktörü Fatih Orhan, “Sözkonusu e-mailler, resmi PTT e-mailleri şablonuna benzese de, e-mailin gönderen bilgisi sahtedir. Gönderen adı olarak “PTT”, “PTT Teslimat”, “PTT Kargo Takip” gibi tanımlamalar kullanılsa bile e-posta adresleri PTT'yle bağlantılı değildir” uyarısı yaptı. Comodo Antispam Laboratuvarının yaptığı farklı analizlerde kullanıcının gördüğü eposta adreslerinin bazılarının PTT resmi adresi ile aynı olduğu durumlara bile rastlanıldığı ifade edildi. Fakat bu durumlarda bile e-postanın içeriğinde bulunan zararlı bir bağlantı (link) tıklandığında kullanıcıyı farklı adreslere yönlendirilip, trojan/arka-kapı açan zararlı indirmeye yönelttiği, ve bu uygulamanın indirilip çalıştırılması sonucu kullanıcının bilgisayarında birçok zarara yol açtığı tespit edildi.
PTT’den geliyormuş gibi görünen e-postaların görünümü şu şekilde:



COMODO

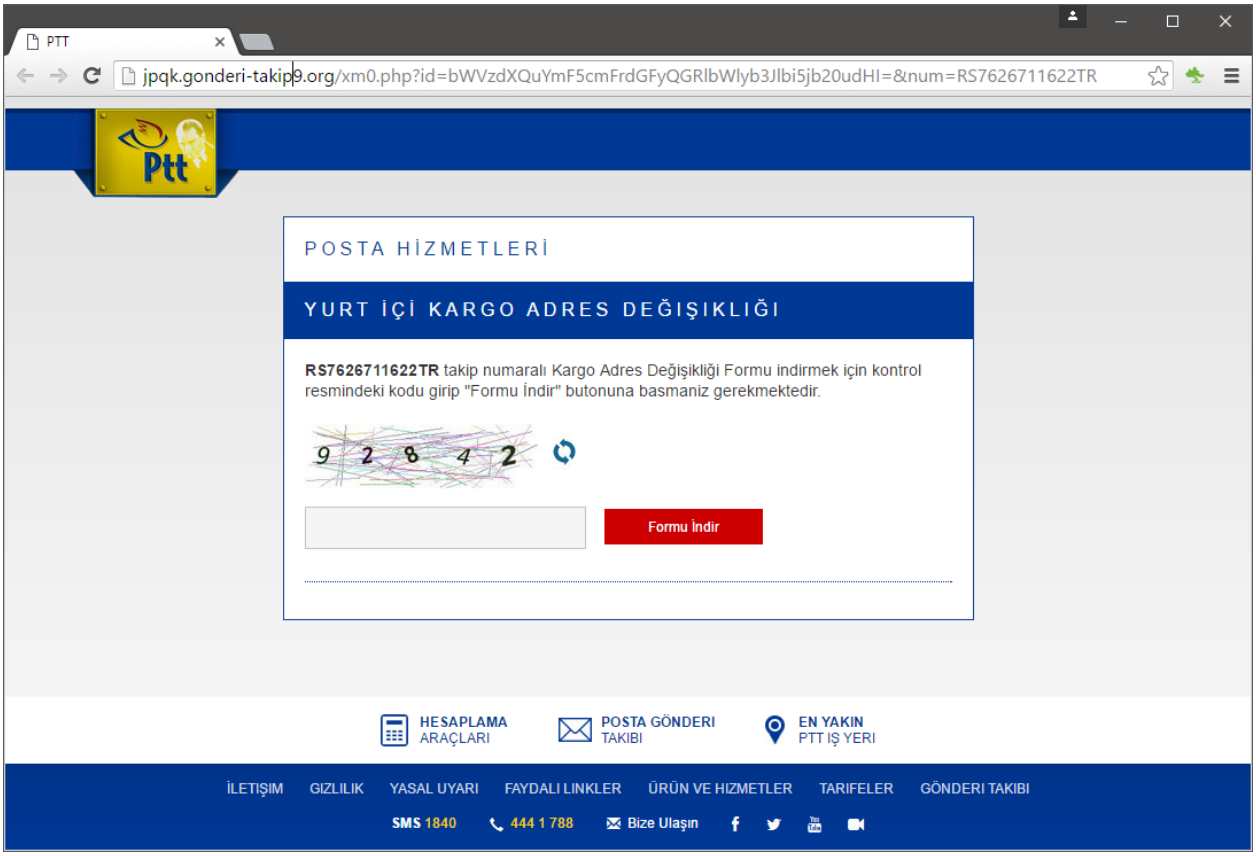
Creating Trust Online®





COMODO
Creating Trust Online®

Ekte görüleceği üzere; gönderen alan adının bilgilerine göre, alan adı 13 Ağustos 2012 tarihinde Norveç'te kaydedildi ve bu tarihten itibaren hiçbir güncelleme yapılmadı. Söz konusu e-mailde aynı URL'yi hedef alan üç tıklanabilir link bulunuyor. (http://schoolsite.org/Nn2ARipxXB/KMn7E1Cre5OX.php?id=mesut.bayraktar@demiroren.com.tr&num=RS7626711622TR).
Hedef URL açıldığında, kullanıcılar başka bir siteye yönlendirilmektedir (http://jhw.gonderi-takip9.org/nuy.php?id=bWVzdXQuYmF5cmFrdGFyQGRlbWlyb3Jlbi5jb20udHI=&num=RS7626711622TR).



Son web sitesinde ise CAPTCHA içeren bir form bulunuyor. Bu CAPTCHA sabit kodlu ve sayfanın yenilenmesiyle değişiyor. CAPTCHA girilerek butona tıklanması ile bir zip dosyası indirililebiliyor. Bu zip dosyasında “PTT_Yeni_Adres_Form.exe” adlı çalıştırılabilir bir dosya bulunuyor. Bu dosya, Comodo’nun ileri düzey zararlı analiz platformu Valkyrie tarafından incelendiğinde kötü amaçlı yazılım olarak sınıflandırılıyor. (https://valkyrie.comodo.com/get_info?sha1=2f86625d3125b48e1b41281a8f2a8ba422ba845f).