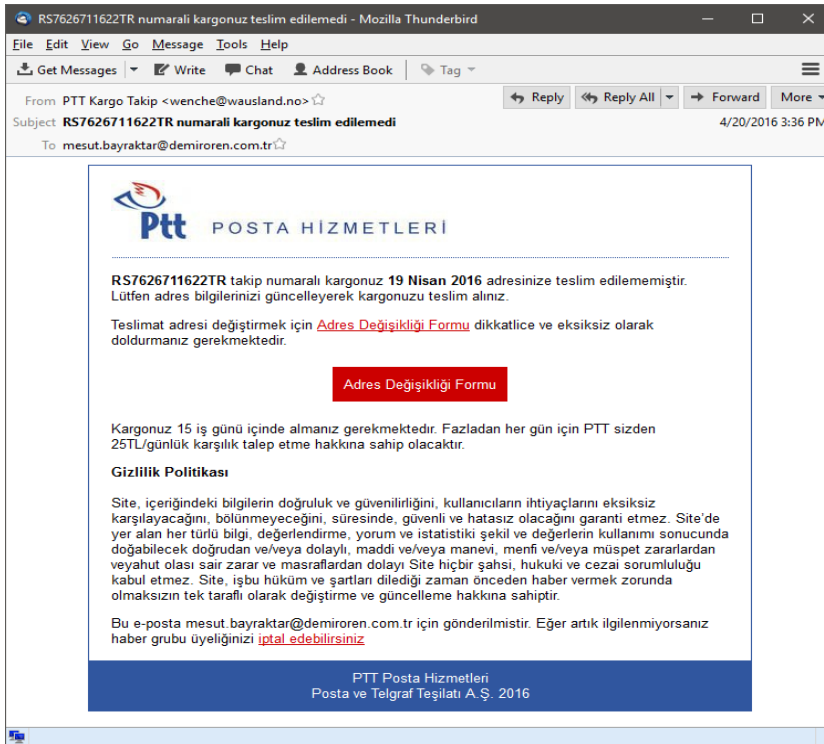


Hackerlar PTT müşterilerinin peşinde

“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 ulaştırılmadığı 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) tıklanıldığında 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®

RS7626711622TR numaralı kargonuz teslim edilemedi - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From PTT Kargo Takip <wenche@wausland.no>
Subject **RS7626711622TR numaralı kargonuz teslim edilemedi**
To mesut.bayraktar@demiroren.com.tr

4/20/2016 3:36 PM

PTT POSTA HİZMETLERİ

RS7626711622TR takip numaralı kargonuz **19 Nisan 2016** adresinize teslim edilememiştir. Lütfen adres bilgilerinizi güncelleyerek kargonuzu teslim alınız.

Teslimat adresi değiştirmek için [Adres Değişikliği Formu](#) dikkatlice ve eksiksiz olarak doldurmanız gerekmektedir.

Adres Değişikliği Formu

Kargonuz 15 iş günü içinde almanız gerekmektedir. Fazladan her gün için PTT sizden 25TL/günlük karşılık talep etme hakkına sahip olacaktır.

Gizlilik Politikası

Site, içeriğindeki bilgilerin doğruluk ve güvenilirliğini, kullanıcıların ihtiyaçlarını eksiksiz karşılayacağını, bölünmeyeceğini, süresinde, güvenli ve hatasız olacağını garanti etmez. Site'de yer alan her türlü bilgi, değerlendirme, yorum ve istatistikî şekil ve değerlerin kullanımı sonucunda doğabilecek doğrudan ve/veya dolaylı, maddi ve/veya manevi, menfi ve/veya müspet zararlardan veyahut olası sair zarar ve masraflardan dolayı Site hiçbir şahsi, hukuki ve cezai sorumluluğu kabul etmez. Site, işbu hüküm ve şartları dilediği zaman önceden haber vermek zorunda olmaksızın tek tarafı olarak değiştirme ve güncelleme hakkına sahiptir.

Bu e-posta mesut.bayraktar@demiroren.com.tr için gönderilmiştir. Eğer artık ilgilenmiyorsanız haber grubu üyeliğinizi [iptal edebilirsiniz](#)

PTT Posta Hizmetleri
Posta ve Telgraf Teşiratı A.Ş. 2016

PTT

jpqk.gonderi-takip9.org/xm0.php?id=bWVzdXQuYmF5cmFrdGFyQGRlbnWlyb3Jlbi5jb20udHI=&num=RS7626711622TR

PTT POSTA HİZMETLERİ

YURT İÇİ KARGO ADRES DEĞİŞİKLİĞİ

RS7626711622TR takip numaralı Kargo Adres Değişikliği Formu indirmek için kontrol resmindeki kodu girip "Formu İndir" butonuna basmanız gerekmektedir.

9 2 8 4 2

Formu İndir

HESAPLAMA ARAÇLARI POSTA GÖNDERİ TAKİBİ EN YAKIN PTT İŞ YERİ

İLETİŞİM GİZLİLİK YASAL UYARI FAYDALI LINKLER ÜRÜN VE HİZMETLER TARİFELER GÖNDERİ TAKİBİ

SMS 1840 444 1 788 Bize Ulaşın

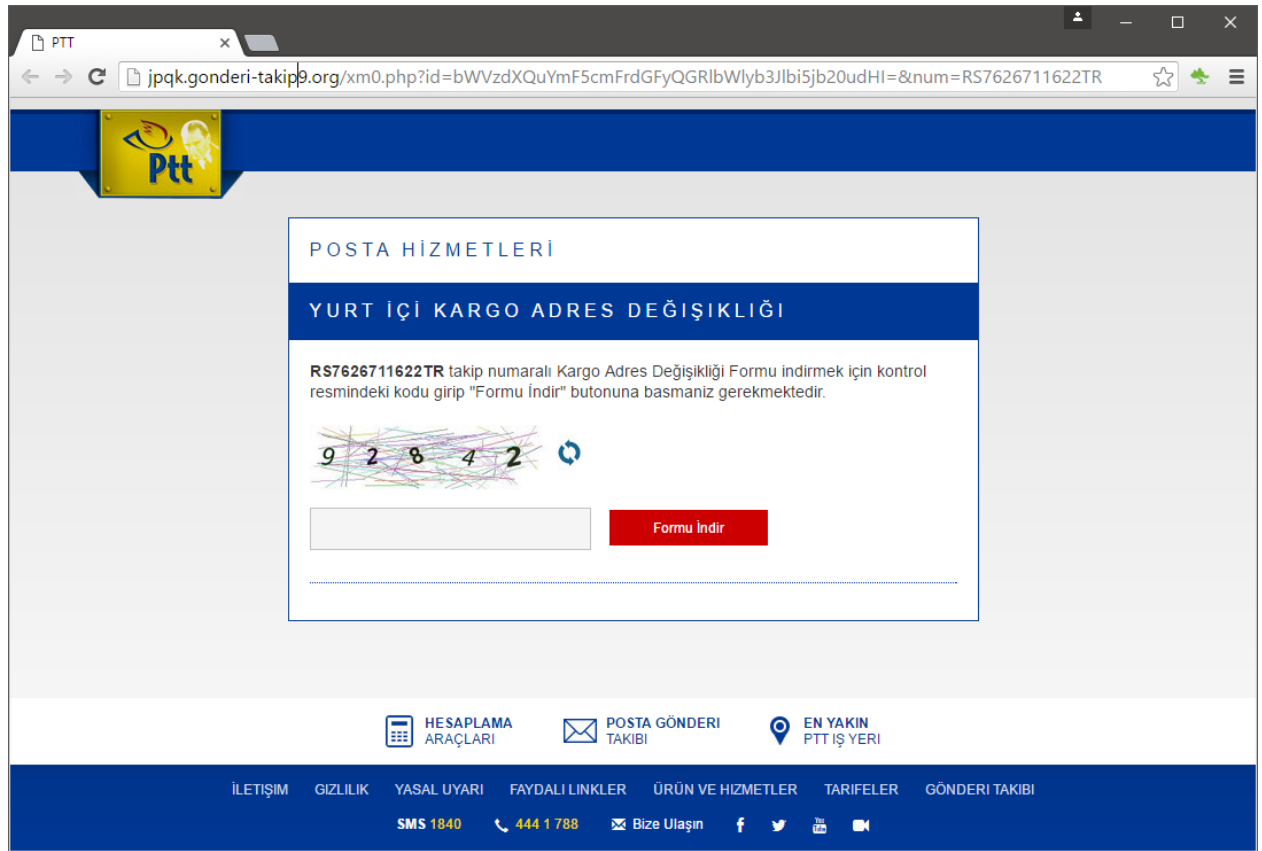
COMODO

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/Nn2ARipxB/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 indirilebiliyor. 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).