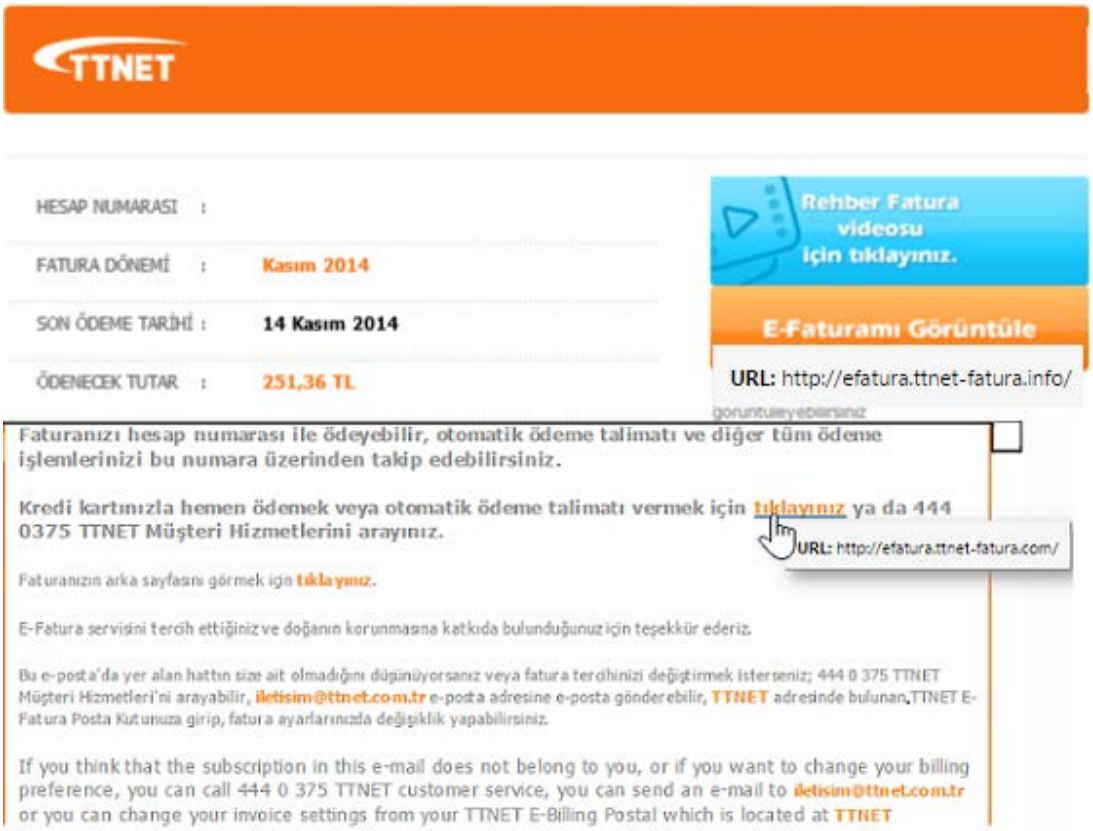
Ülkemizdeki internet kullanıcılarını hedef alan KriptoKilit saldırıları daha önce de gerçekleşmişti. Fakat bu sefer KriptoKilit güncel sürümü ile daha büyük bir tehdit olarak karşımıza çıktı. Kendini açık bir şekilde CryptoLocker olarak tanıtan bu yeni zararlı yazılım, yine kullanıcılara ait belli uzantılara sahip dosyaları şifrelemekte ve bu verilerin kurtarılması için kullanıcılardan **"Şifre çözme yazılımı"** adında bir yazılım satın almalarını istemektedir.

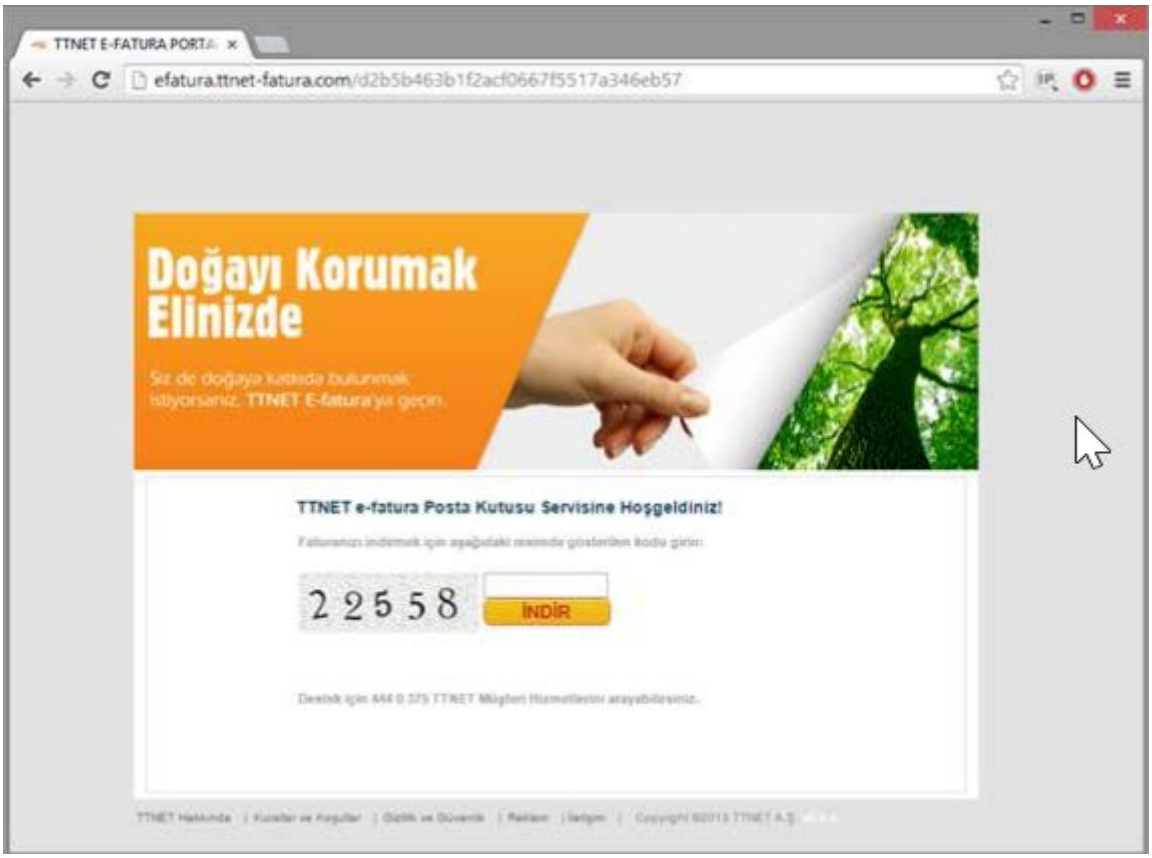
Bulaşma Şekli

Zararlı yazılım fatura epostaları şeklinde kullanıcılara eposta göndermektedir.



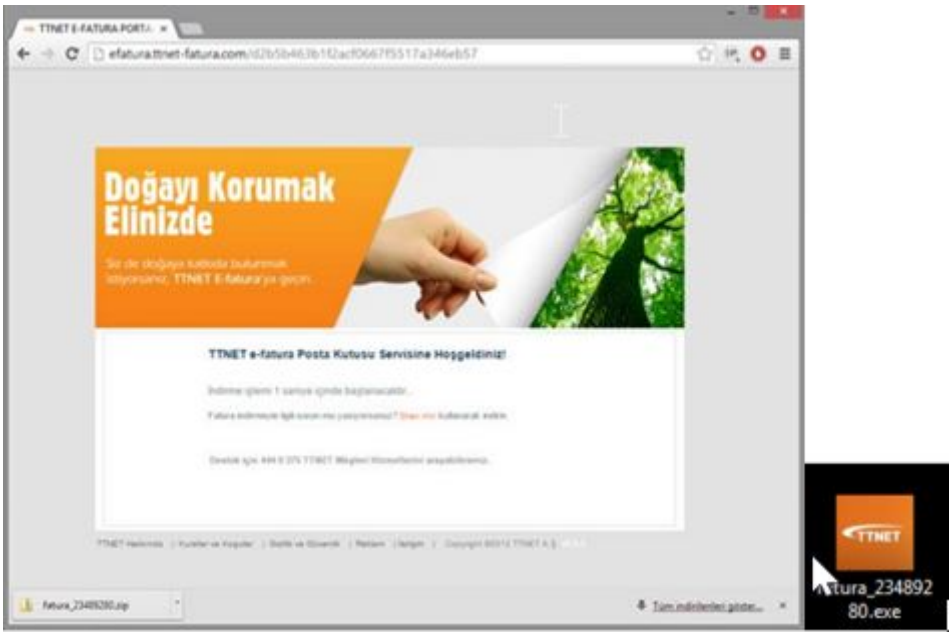
Şekil 1- CryptoLocker Tarafından Kullanıcılara Gönderilen Eposta

Şekil 1'de gösterildiği üzere fatura tutarı yüksek bir miktardır. Faturanın yüksek tutarından ötürü fatura hakkında bilgi almak isteyen kullanıcılar faturayı görmek istediklerinde **Şekil 2**' de gösterilen web adresine yönlendirilmektedirler.



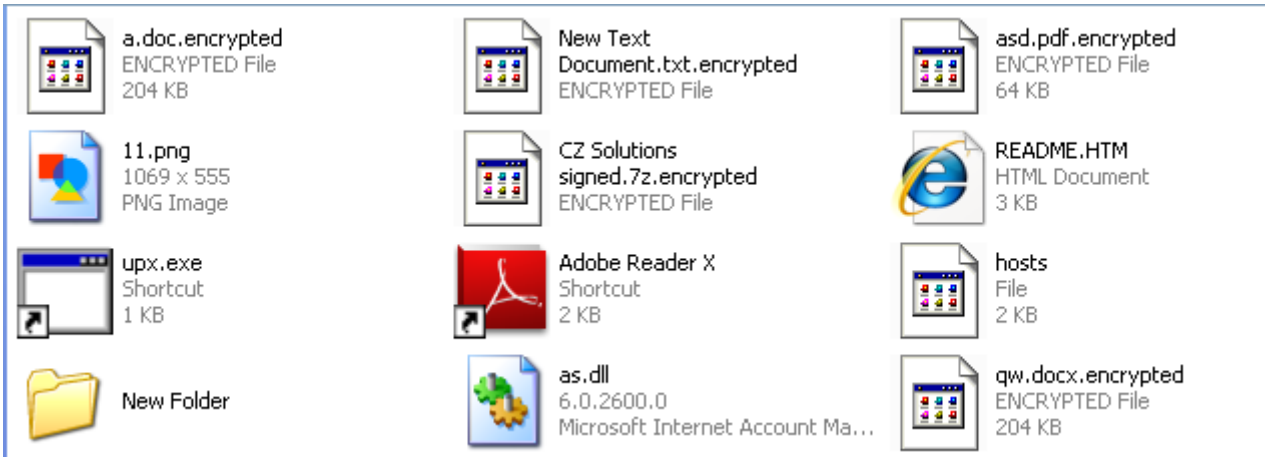
Şekil 2- Fatura İndirme Sayfası

Üretilen kodu girip indir butonuna tıklanıldığında **".zip"** uzantılı bir dosya indirmektedir. Bu dosyanın içinde ise **".exe"** uzantılı fatura dosyası bulunmaktadır.

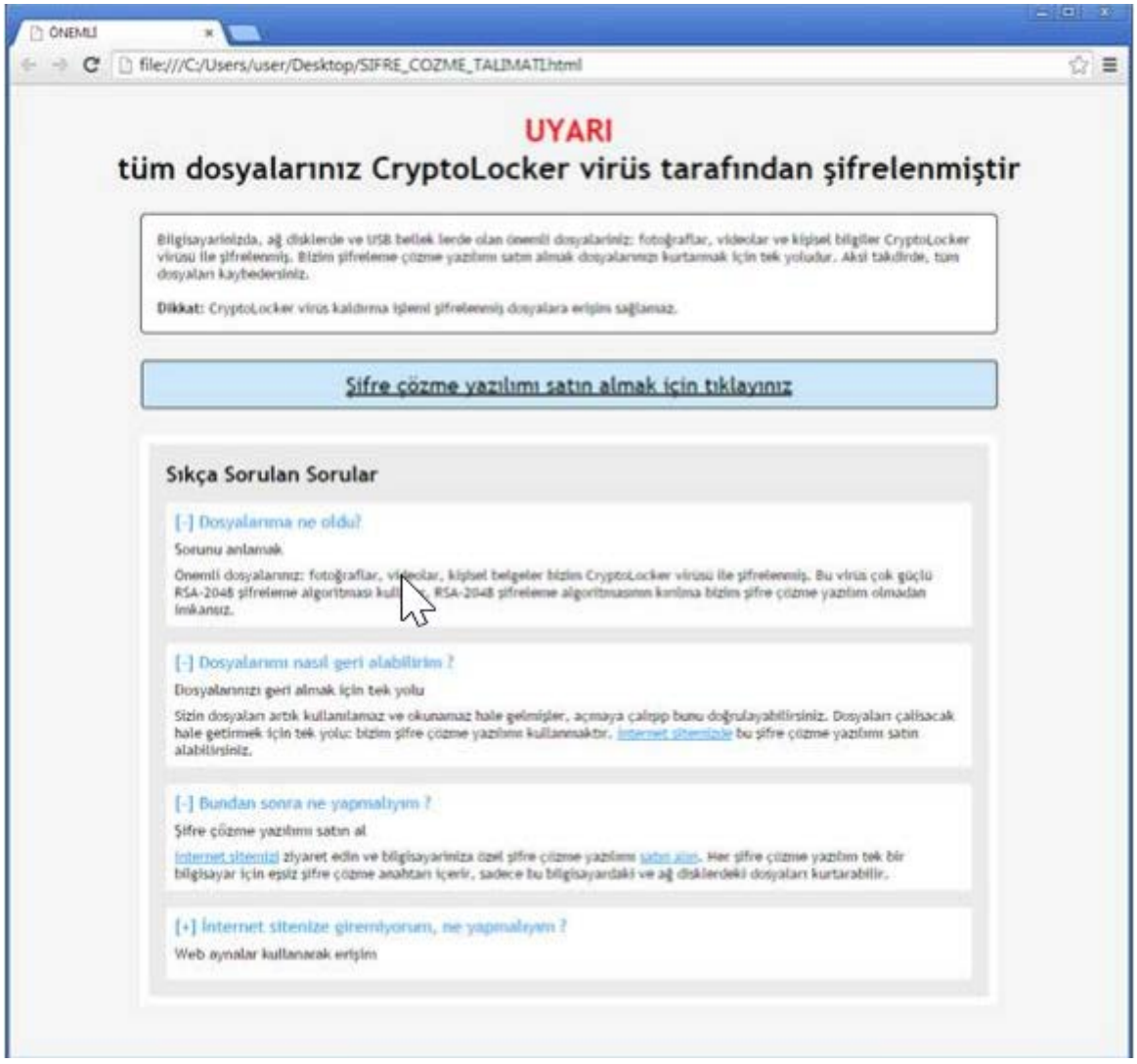


Şekil 3-İndirilen Zararlı Dosya

İndirilen bu zararlı yazılım çalıştırıldığında ise zararlı yazılım kullanıcının bilgisayarına bulaşmakta ve içi boş olmayan .doc, .docx, .pdf, .txt, .7z, .rar, .zip tipinde olan dosyalar şifrelenmektedir. Şifrelenen dosyaların yeni uzantıları .encrypted olmaktadır. **Şekil 4**'te bu durum gösterilmektedir.

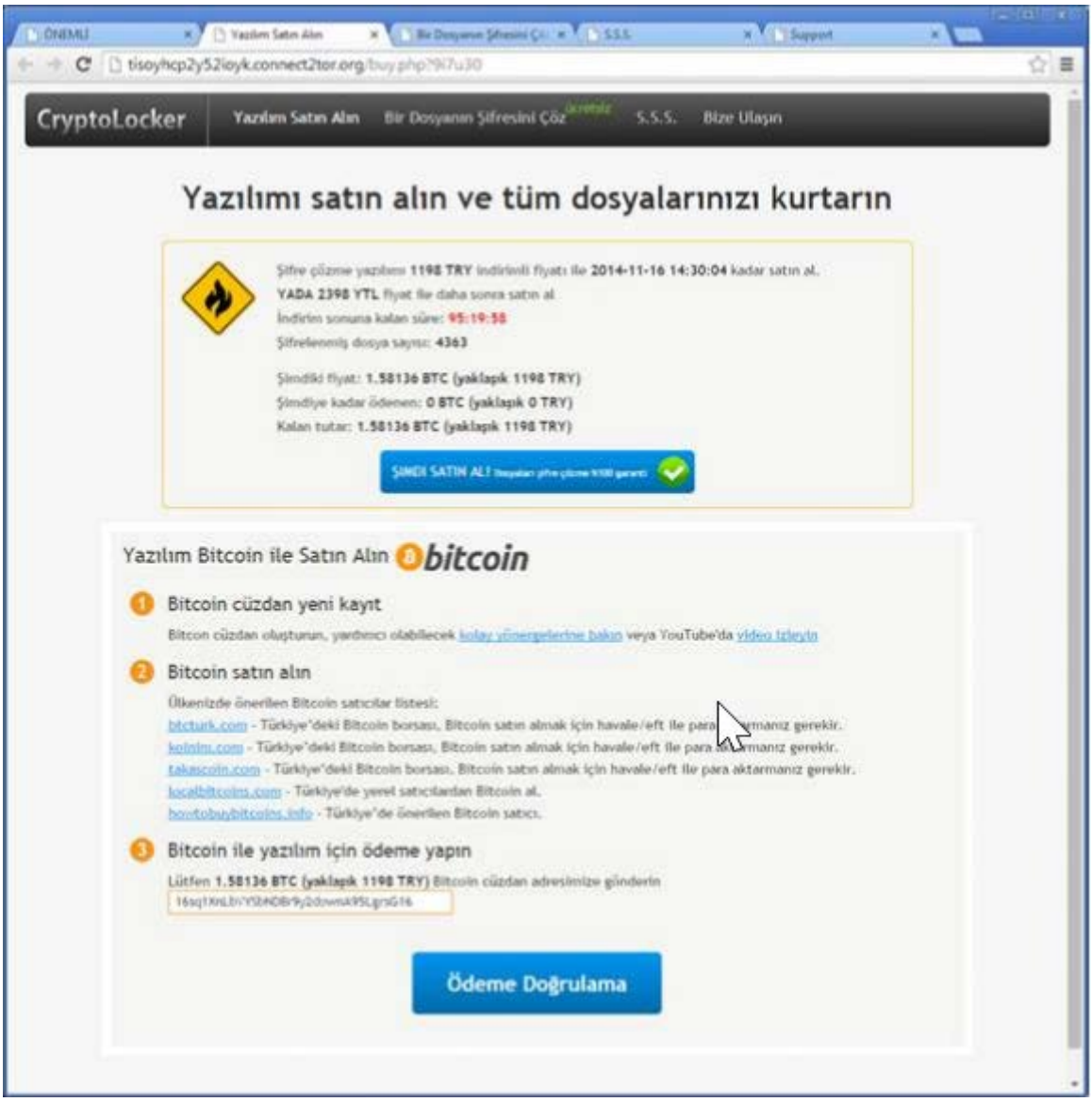


Şekil 4- Şifrelenen Veriler



Şekil 5- Verilerin Şifrelenmesinden Sonra Ekrana Çıkan Görüntü

Zararlı yazılım bilgisayardaki verileri şifreleme işlemini bitirdikten sonra ekrana **Şekil 5**'teki gibi bir sayfa çıkarmaktadır. Görüldüğü üzere zararlı yazılım şifrelenen veriler karşılığında Şifre çözme yazılımı adı altında bir yazılımın satın alınmasını istemektedir.

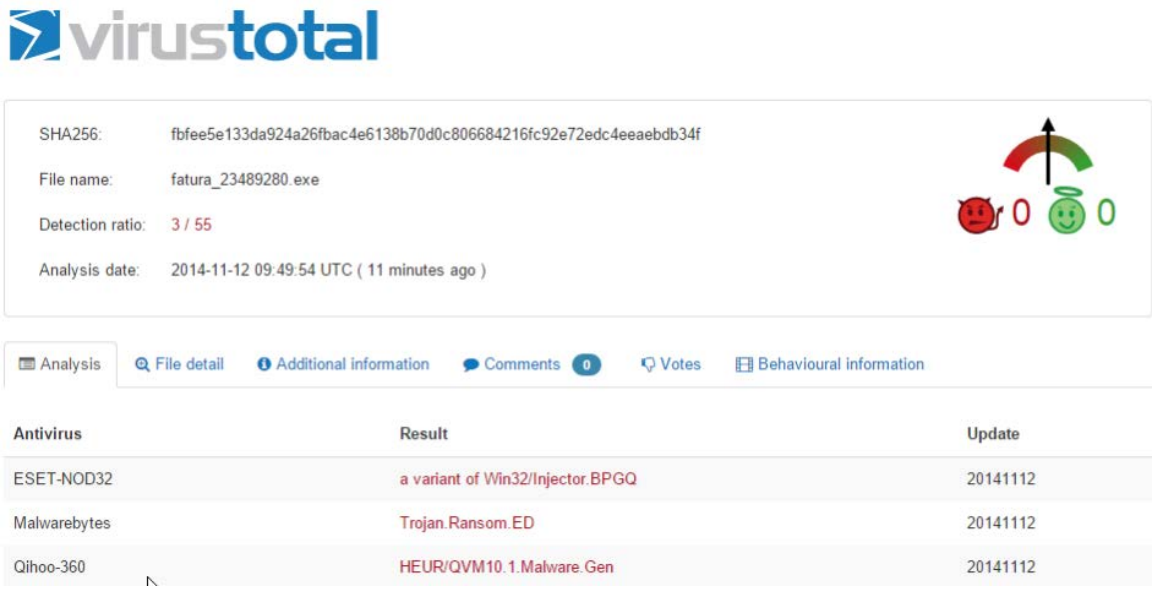


Şekil 6- Şifre Çözme Yazılımı Satın Alma Şekli ve Tutarı

Şekil 5' te çıkan görüntüdeki linke tıklandığında aslında tor ağı üzerinde olan fakat bir tor proxy hizmeti veren sunucu üzerinden erişilebilen **Şekil 6**' daki gibi kişiye özel bir web sayfasına yönlendirilme yapılmaktadır.

Şifre çözme yazılımının satın alınması konusunda ise 96 saat içinde satın alımı durumunda 2398 liradan 1198 liraya kadar indirim yapmaktadır.

Zararlı yazılım ilk yayıldığında antivirüs firmalarının büyük bir çoğunlu tarafından tanınmamıştır. Virustotal sonuçları **Şekil 7**'de gösterilmektedir.



Şekil 7- Antivirüs Firmalarının CryptoLocker Sonuçları

Dikkat Edilmesi Gerekenler

CryptoLocker gibi eposta yoluyla gelen zararlı yazılımlardan etkilenmemek için gelen eposta adreslerine çok dikkat edilmelidir. **Şekil 8**'de gerçek bir ttnet fatura eposta adresi ile **Şekil 9**'da zararlı yazılımının eposta adresleri gösterilmektedir.

<faturahatirlatma@ttnetbilgilendirme.com.tr>

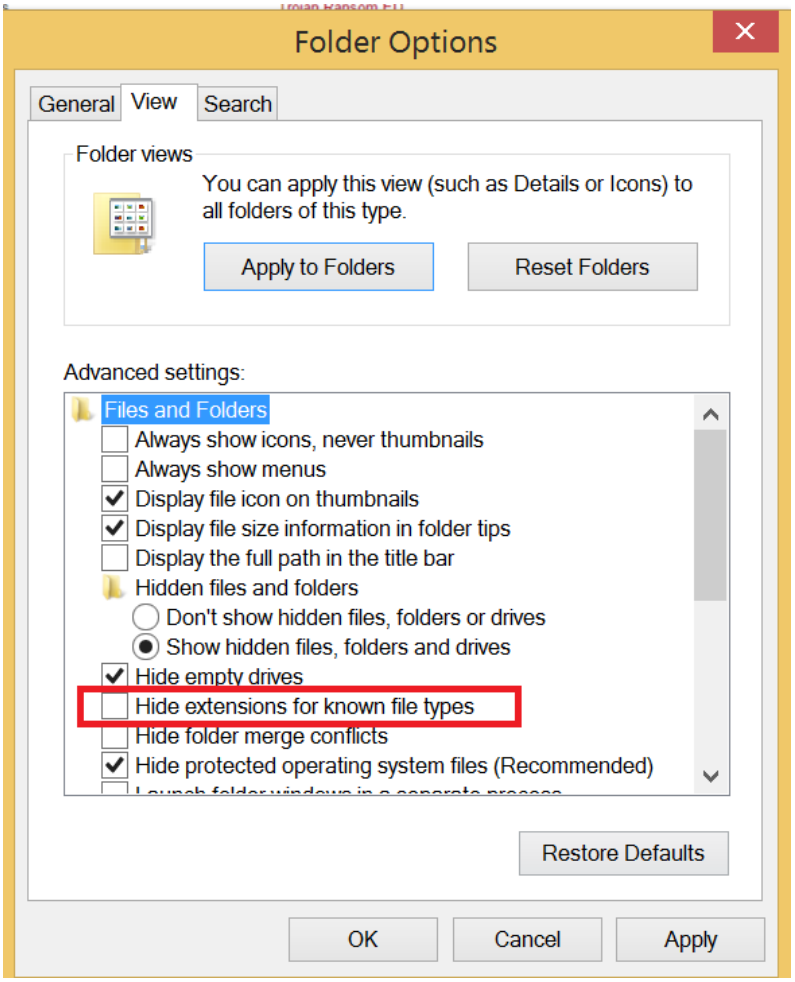
Şekil 8- Gerçek TTNet Fatura Gönderim Adresi

From: odeme@ttnet-fatura.com [mailto:odeme@ttnet-fatura.com]

Şekil 9- Sahte Fatura Gönderim Adresi

TTNet'in fatura görüntüleme adresi **"https//:efatura.ttnet.com.tr"** iken zararlı yazılımın kullandığı ise **"efatura.ttnet-fatura.info"** ve **"efatura.ttnet-fatura.biz"** adresleridir.

Eposta olarak gönderilen faturaların uzantılarına dikkat edilmelidir. CyrptoLocker zararlı yazılımı bir .exe dosyasıdır. Oysaki TTNet faturaları pdf şeklinde göstermektedir. Dosyaların uzantıları bilgisayarlarda normalde görünmemektedir. Dosya uzantılarını görebilmek için klasör ayarlarından bilinen dosya türleri için uzantılarını gösterme (*Hide extensions for known types*) ayarı değiştirilmelidir. **Şekil 10**'da bu ayarlama gösterilmektedir.



Şekil 10- Dosya Uzantılarının Gösterimi İçin Yapılandırma

Aynı zamanda Ttnet faturaları kullanıcılara faturaları indirtmek yerine browserda göstermektedir. **Şekil 11**‘ da gerçek Ttnet fatura görüntüleme ekranı gösterilmektedir. **Şekil 2**’de ise sahte sayfa gösterilmiştir.

Şekil 11- Gerçek Fatura Görüntüleme Sayfası

Sonuç olarak, internetten indirilen dosyalar, epostalar açılmadan önce dikkatle okunmalıdır. Epostayı gönderen adreslere, epostanın içeriğine, indirilen dosyanın uzantısına dikkat edilmeli ve emin olunduktan sonra dosyalar açılmalıdır.