FİDYE VİRÜSLERİ
KORUNMA YÖNTEMLERİ VE ÇÖZÜM ÖNERİLERİ

Cryptolocker ve Ransomware (fidye) virüsleri en tehlikeli zararlı yazılımlardan ve maalesef ki farklı varyasyonları ile karşımıza çıkmaya devam ediyor. İlk zamanlarda çözüm bulunamayan virüslere karşı geliştirilen önlem ve çözümler söz konusu ancak bu çözümler yeni virüs varyantları nedeniyle kısa süre içerisinde çözümler etkinliğini yitirebiliyor. 2014 yılı sonlarından itibaren ülkemizde yayılmaya başlayan bu virüs türlerinin dünya genelinde otuzdan fazla ransomware çeşidi bulunmaktadır. Bunların ülkemizde 11 çeşidi etkili olmuştur. Virüsü yayan ağın şimdiye kadar 1,5 milyon doları aşan gelir elde ettiği tahmin ediliyor. Böylesine büyük bir pastanın varlığını bilmek sorunu anlamamıza yardımcı olacaktır.

Bu tip virüsler, bilgisayar kullanıcılarının dikkatsizliği ve zaaflarını kullanarak etkinlik sağlamak üzere tasarlanmışlardır. Tabi ki kullanıcının yetersizliği de virüsün etkinliğini sağlayan en önemli faktörler arasında. Bu tip virüslerden korunmanın en etkili yolu, tüm bilgisayar kullanıcılarında farkındalık yaratarak, konu hakkında bilgilendirmek. İşimizin doğası gereği Ofislerimizdeki bilgisayarlarda depoladığımız verilerimiz en önemli sermayemiz doğal olarak teknoloji ilerledikçe korunmak hayati derecede önemli olmaktadır.

Cryptolocker zararlı yazılımları etkinleştiği bilgisayarda, kullanıcı yetkisinin erişimine açık olan tüm sabit diskler, flash diskler, usb diskler, bulut tabanlı depolama alanları ve ağ sürücülerindeki tüm verileri şifreler. Özet olarak ofisinizde virüsün etkinleştiği bir Terminal makinaya bulaşan virüs paylaşım yetkisi bulunan tüm bilgisayarlardaki verileri de etkilemektedir.

Önceleri Türk Telekom ve TTNET e-faturaları, PTT kargo gibi gönderilen sahte e-postalar, zamanla yerini devlet kurumları adıyla gönderilmiş sahte e-postalara ve son zamanlarda ise ***Turkcell e-fatura sahte e-postaları şeklinde daha profesyonelce hazırlanmış ve daha hedefli ataklarla karşımıza çıkıyor.*** Üstelik tek risk e-posta ekleri veya linkler değil, web siteleri, RDP (uzak masa üstü bağlantısı) portlarından ve güvelik açıklarından bulaşabiliyor.

" Cryptolocker 19.01.2016 tarihinden itibaren sahte Turkcell e-postası olarak gönderilmektedir. Virüs şifrelediği dosyaların uzantısını ".encrypted" olarak değiştirmektedir. ""

Aşağıda sahte Turkcell e-posta örneği verilmiştir. Bu tip e-postalarda ancak ekler açıldığında veya e-posta içindeki linklere giriş yapıldığında virüs bilgisayarınıza bulaşır. Bu tip **sahte e-postaları belirlemek için şu hususlara dikkat ediniz;**

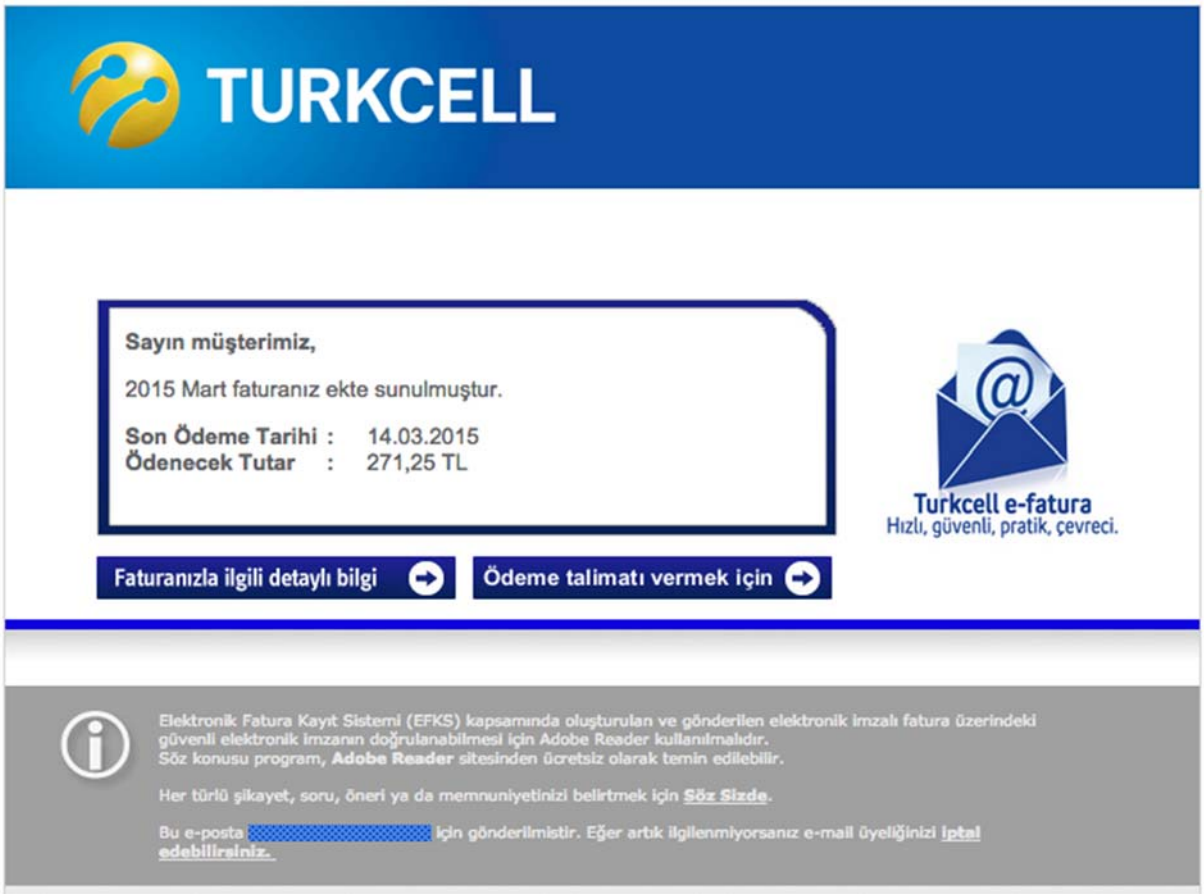
- e-postanın ilgili kuruma bildirdiğiniz e-posta hesabına ait olduğundan emin olunuz.
- Gelen e-posta da gönderici adresini doğrulayınız; örneğin Turkcell resmi adresi http://www.turkcell.com.tr/ dir. Sahte e-postalarda, "turkcell-fatura.org" veya "turkcell-fatura.biz" ve benzeri bir çok sahte adres kullanılabilir.
- Turkcell, Türk Telekom vb kurumlardan gelen e-postalarda aşağıdaki örnekte olduğu gibi "Sayın Müşterimiz" şeklinde hitap kullanılmaz. İlgili kurumlardan gelen gerçek e-postalarda hitap olarak mutlaka adınız soyadınız yer alır.
- Yine benzeri kurumlardan gelen e-postalarda mutlaka abone numaralarınız yazılır, "xxxxx hesabınıza ait" vb şekilde bilgiler yer alıyorsa sahte e-posta karşılaşmışsınızdır.

- İlgili kurumlardan geldiğine emin olmadığınız e-posta eklerini asla açmayınız. Unutmayınız ki ".zip, .rar, .7z, .pdf" gibi uzantılı dosyalara kolaylıkla zararlı kodlar yerleştirilerek virüs yazılımı haline getirilebilir.
- Mümkün oldukça e-fatura indirmelerini ilgili kurumun on-line web servisleri üzerinden indiriniz.

Asla şunları yapmayınız:

- ***Gelen e-postalar üzerindeki linklere tıklamayınız, bu linklerden indirilen dosyaları asla açmayınız.***
- ***Emin olmadığınız e-posta eklerini asla açmayınız.***
- ***Antivirüs yazılımlarınızı asla devre dışı bırakmayınız.***
- ***Ücretsiz veya her gün güncellenmeyen Antivirüs yazılımlarına itibar etmeyiniz.***
- ***Torrent üzerinden yasal olmayan yazılımlar indirmeyiniz.***

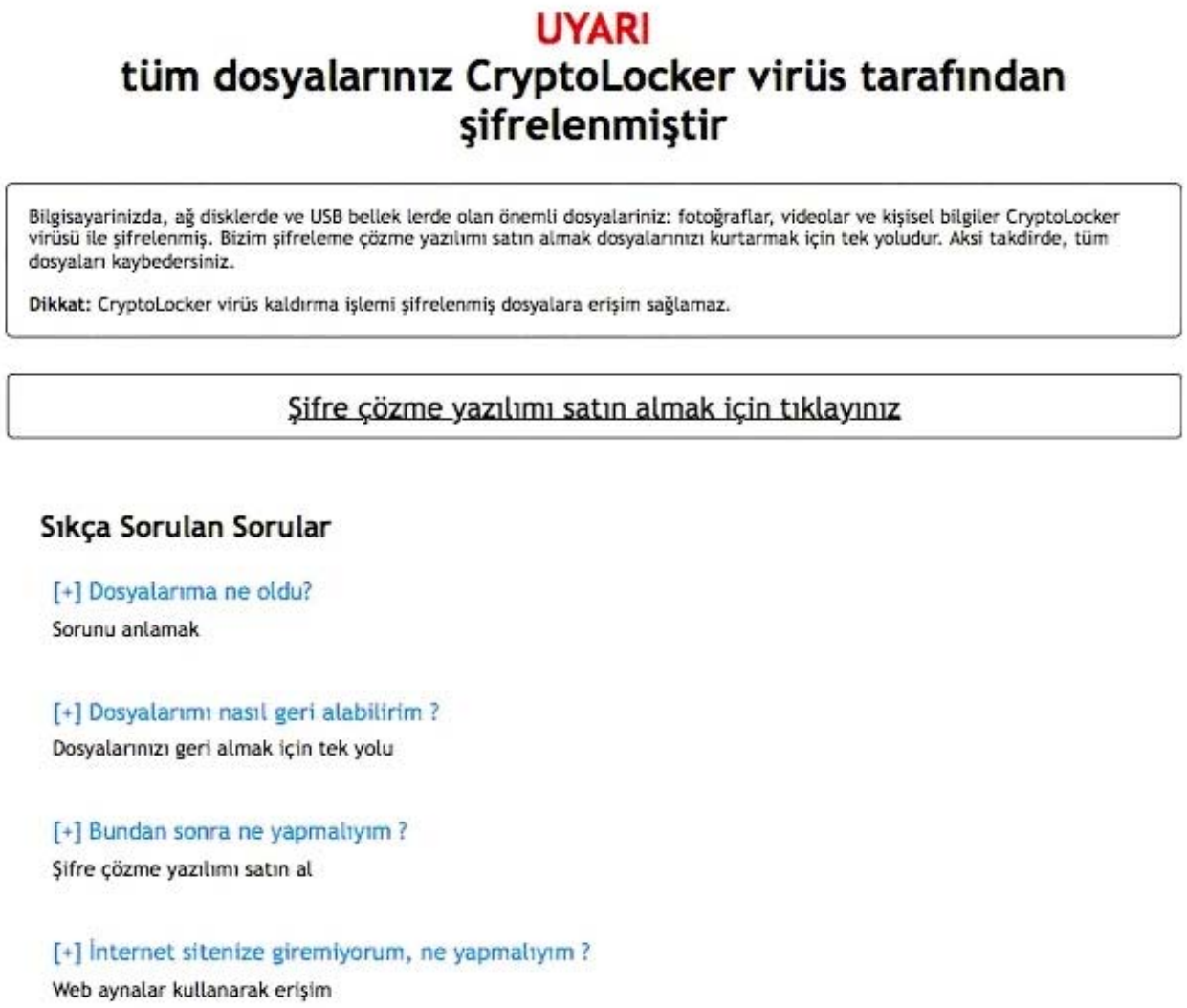
Örnek bir sahte e-posta



Virüs bilgisayarınızda ya da mobil cihazlarınızda ulaşabildiği tüm dosyalarınızı şifreler ve bu şifrenin çözülmesi için sizden para talep edilir. Virüsün son versiyonu kurbanlarını ödeme için tor ağı üzerindeki ödeme noktasına yönlendiriyor. İstenen fidye miktarı ise; 500$, 500eur veya 0,5 bitcoin gibi tutarlar olabiliyor. Bu tür sorunlarda kesinlikle fidye ödemeyiniz. Yaşanan deneyimlerden ödeme yapanlardan büyük bir kısmına ödeme ulaşmadı bahanesiyle çözüm sunulmuyor. Üstelik fidye ödemesi yapmak etik olmadığı gibi illegal bir durum ve hepsinden önemlisi yeni kurbanlar için finansör olmanız anlamına da geliyor.

"" Lütfen bu yazımızı ofislerinizdeki tüm çalışanlarınızın da okumasını sağlayınız. ""

Saldırıya uğramış bilgisayarın masaüstüne bırakılmış uyarı;



Cryptolocker virüsü bilgisayarınızın işletim sistemine ve çalışma prensibine zarar vermez. (Yeni tip virüsün bilgisayarı çalışamaz hale getirdiği iddia edilse de, şimdilik böyle bir vaka ile karşılaşılmamıştır.) Virüs; aslında sizin de farklı araçlarla yapabileceğiniz bir şifreleme uygular ve dosyalarınızın uzantısını değiştirerek ".encrypted, ccc, vvv, xxx, ttt, micro, LOL" vb. uzantılara çevirebilir, ya da dosya ismini tamamen değiştirebilir. Çeşitli açık kaynak şifreleme kütüphaneleriyle ve çok güçlü olan bu şifreleme, çeşitli yol ve yöntemlerle kırılmaya çalışılsa dahi, yıllar alacak kadar karışık ve uzun bir şifrelemedir. Ancak bazı tersine mühendislik çalışmaları ile şifrenin elde edilebilmesi mümkün olabilmektedir.

Cryptolocker virüsleri bilgisayardan kolaylıkla temizlenebilir, asıl sorun bilgisayardan temizlemek değil, şifreli dosyaları açabilmektir. Virüsü temizleseniz ve hatta işletim sisteminizi yeniden yükleseniz dahi verileriniz şifreli olarak kalmaya devam edecektir. Bu sebeple, önceliğiniz virüsü temizlemek değil, verileri kurtarmak olmalıdır.

Nasıl Bulaşır?

Ülkemiz Cryptolocker saldırılarında dünyada 4. Sırada yer almaktadır.

Bu tip virüslerin bulaşma yol ve yöntemleri genel olarak şöyledir;

- Mail ekine ve linkine tıkladığınızda
- Torrent'lerden ya da farklı bir kaynaktan indirdiğiniz resmi olmayan oyun, film, müzik dosyalarıyla
- Online film, dizi izleme platformlarında çalıştırdığınız flash/java eklentileriyle
- Ele geçirilmiş ve resmi olduğunu düşündüğünüz kaynaklardan indirdiğiniz uygulamalar ile (örnek: ammyy admin)
- Web tarayıcı eklentileriyle
- Çeşitli blog ve haber portalları (istemsiz)
- Çeşitli ilan siteleri (istemsiz)

UNUTMAYINIZ; virüslerden, sistem çökmelerinden, donanım arızalarından korunmanın en önemli ve en kolay yolu, DÜZENLİ VE SÜREKLİ YEDEK ALMAKTIR.

- ***Yedeklerinizi, harici sabit diske düzenli olarak alınız.***
- ***Yedekleme amacıyla kullandığınız sabit disklerinizi asla sürekli sisteme bağlı bırakmayınız.***
- ***Yedekleme diskiniz mutlaka birden fazla olmalıdır.***
- ***Bulut depolama alanlarına ilişkin şifrelerinizi asla bilgisayarınıza kaydetmeyiniz, bulut depolama alanlarına ilişkin ilgili hizmet sağlayıcının sunduğu ara yazılımlarını asla kullanmayınız. Bulut alanlara yedeklemeyi mutlaka manuel internet tarayıcıları üzerinden gerçekleştiriniz.***

Çalışan zararlı uygulama nasıl temizlenir?

Zemana Antimalware: Bilgisayarınızı taratarak zararlıdan temizleyebilirsiniz. Yerli bir üretici tarafından geliştirilen bu yazılımı isterseniz satın alarak cihazlarınızı daha sonra gelebilecek malware saldırılarına karşı koruyabilirsiniz.
Zemana Antimalware indirmek için: https://www.zemana.com/AntiMalware

Alternatif olabilecek bir başka yazılım;
Malwarebytes uygulaması ile bilgisayarınızı zararlıdan temizleyebilirsiniz.
Malwarebytes indirmek için: http://downloads.malwarebytes.org/file/mbam/

Daha sonra bilgisayarınızda Combofix çalıştırabilirsiniz:
Combofix için (opsiyonel): http://www.bleepingcomputer.com/download/combofix/

Ve son olarak Antivirüs yazılımınız ile tam sistem taraması yaptırınız.

Hatırlatmak isteriz, zararlı yazılımları (virüs) temizlemek tek başına yeterli değildir, esas önemli olan şifrelenmiş verilerin şifrelerinin çözülmesidir.

Virüs bulaştı, verilerime ulaşamıyorum, ne yapmalıyım?

Virüs bulaştı ve yukarıda örneğini verdiğimiz dosya şifrelemesiyle karşılaştığınızda öncelikle asla panik yapmayınız. Ülkemizde şu ana kadar görülen virüslerin oluşturduğu hasarların yaklaşık %80 'i çözüme kavuşturulmuştur. Maruz kaldığınız virüs türüne göre çözüm maliyeti ve süresi değişmektedir. Maruz kaldığınız virüs versiyonu ve verilerinizin durumu değerlendirilerek çözüm geliştirilmesi gerekmektedir. Örneğin, verilerinizin istikrarlı ve güncel yedeği varsa ek maliyete katlanmadan çözüme kavuşabilirsiniz. Bunlar yoksa sisteminizin durumuna ve maruz kaldığınız hasara göre çözüm önerileri için Odamız Bilgi Teknolojileri İzleme Komisyonu üyelerinden destek alabilirsiniz. Oda üyelerimiz için ülkemizdeki en yetkin çözüm ortaklarıyla görüşmeler yapılmış, uygun ücret karşılığı destek sağlanması amacıyla ön anlaşma sağlanmıştır.

Verileriniz şifrelendiğinde;

- Bilgisayar sistemine asla müdahale etmeyiniz,
- Sabit disklerinizi asla formatlamayınız, (verilerinizi kalıcı olarak kaybedebilirsiniz)
- Bilgisayarınızdan asla herhangi bir dosyayı silmeyiniz,
- Verilerinizdeki şifrelerin çözülmesi için asla müdahalede bulunmayınız, (şifre çözüm denemeleri dosya yapılarını bozabilir, kurtarma olanaklarına kalıcı olarak zarar verebilirsiniz.)
- Maruz kaldığınız virüs türüne ve sisteminizin yapısına uygun çözüm önerilerimiz için derhal odamızla irtibata geçiniz,
- Virüsün bulaştığını ve dosyaları şifrelemeye başladığında farkındaysanız hemen bilgisayarınızı kapatınız. (Yapılan testlerde bilgisayar sistemi tekrar başladığında zararlı yazılımlarının kaldığı yerden devam etmediği tespit edilmiştir. Tabi virüs versiyonuna göre bu durumun değişme ihtimali vardır.)

Nasıl Korunabiliriz, Korunmak İçin Ne Yapmalıyız?

Yukarıda verilen kullanıcı tedbirlerine ek olarak;

- Bilgisayarlarımızda/cihazlarımızda lisanlı işletim sistemi ve yazılımlar kullanmalı,
- Yazılımlarımızı sürekli güncel tutmalı,
- Etkili ve profesyonel nitelikli anti virüs yazılımları kullanılmalı, her zaman aktif ve güncel tutmalı,
- İşletim sistemlerinde (Windows vb.) güvenlik duvarını asla devre dışı bırakmamalı,
- Bilgilerimizi düzenli olarak güvenli ve sistem bağlantısı olmayan ortamlarda yedeklemeli,
- İnternet bağlantısını sağlayan modemlerde güvenlik duvarı (firewall) aktifleştirmeliyiz.

Yukarıdaki tedbirler önemli ölçüde güvenlik sağlayacaktır ancak bunlara ek olarak İleri düzey kullanıcılar İçin veya Sistem Uzamanı yardımıyla alınabilecek önlemler şunlardır;

- Yerel ağdaki sunucu ve terminal bilgisayarlarımızda gereksiz paylaşımları devre dışı bırakmalı.
- Bilgisayarınızdaki Guest ve Administrator kullanıcıları devre dışı bırakılmalı,
- Kullanıcı hesaplarınıza basit olmayan ve standart dışı kullanıcı şifreleri atayınız,
- Ayrıca local policy uygulayarak bilgisayarınızın %appdata% ve %temp% klasörlerinden uygulama çalıştırmasını engelleyiniz,
- Ayrıca tüm klasörleriniz için shadow copy özelliğini aktif edip, shadow copy yönetim aracı vsssadmin.exe'nin ismini değiştiriniz.