SALDIRIYA UĞRADIM? NE YAPMALIYIM?

Eğer form değiştirmemiş CryptoLocker virüsü ile karşı karşıyaysanız bunun için bir çözüm var. Öncelikle virüsü temizlemek sorun değil. Sorun olan .encrypted uzantılı dosyalar yani şifrelenmiş dosyalar. Daha önceki CryptoLocker virüsü örneklerinde virüs önemli dosyalarınızı AES-256-bit ile oldukça güçlü ve çözülmesi imkansız denecek bir şifreleme algoritması ile şifreliyordu. Eğer sizdeki form değiştirmemiş bir CryptoLocker virüsü ise bütün önemli dosyalarınız AES-256-bit ile şifrelenmiş demektir.

Aşağıda iki çözüm mevcut. Size bulaşan virüs farklı bir varyanta sahip olabilir. İkisini de denemenizde yarar var.

CryptoLocker virüsü gibi virüsler fidye virüsü olarak adlandırılır.
Geçtiğimiz yaz aylarında FireEye ve FOX IT adlı iki güvenlik şirketi CryptoLocker virüsünün şifrelediği dosyaları ve virüsü analiz ederek, tersine mühendislik yolu ile bir online şifre çözme uygulaması devreye aldılar. Eğer şansınız varsa CryptoLocker virüsünün form değiştirmemiş bir versiyonu ile karşı karşıyasınızdır.

Aşağıda hem CryptoLocker virüsü temizleme hem de şifreli dosyaların nasıl açılacağına dair bir çözüm yolu paylaşacağım. Denemenizde yarar var.

CryptoLocker virüsü nasıl temizlenir?

CryptoLocker virüsü temizleme işlemi iki adımdan oluşacak. Önce virüsün enfekte olduğu sistem temizlenecek daha sonra da şifreli dosyaların şifrelerinin nasıl çözüleceğini anlatacağım. Şuan için CryptoLocker virüsü temizleme için en etkin ve tek geçerli yol olarak bu anlatacağım yöntem söz konusu.

CryptoLocker virüsü şuanda pek çok güncel antivirüs tarafından tespit edilebiliyor ve temizlenebiliyor.

1. Öncelikle bilgisayarınızı virüs taramasından geçirin.
   Norton Power Eraser nedir? Nasıl Kullanılır? ile bilgisayarınızı önce taratın. Bu işlemden sonra Dr.Web CureIt! nedir? Dr.Web CureIt! nasıl kullanılır? ile bilgisayarınızı tarafın.
   Daha sonra bilgiayarın tamamen virüslerden arındığından emin olmak için Malwarebytes nedir? Malwarebytes nasıl kullanılır? ile bilgisayarınızı taratın. Burada 3 farklı antivirüs ile taratırmandaki sebep virüsün form değiştirmiş olma ihtimali. Eğer Norton Power Eraser virüsü bulursa ve temizlerse daha sonra sadece Dr Web veya Malwarebytes ile bilgisayarınızı taratmanız yeterlidir.
2. Daha sonra virüsün etkilediği dosyalardaki şifrelemeyi kaldırmak için aşağıdaki işlemleri deneyin
3.

CryptoLocker virüsünün şifrelediği dosyalar nasıl açılır?

CryptoLocker virüsü ile şifrelenen dosyalar AES-256 ile şifrelenir. Bu bir şifreleme algoritmasıdır ve AES-256 ile şifrelenen dosyalar normal koşullarda KEY yani anahtar dosya olmadan açılamazlar. Maalesef

ortalıkda tek bir **CryptoLocker** virüsü yok. Birden fazla taklitçi CryptoLocker virüsü mevcut.**Maalesef bu yöntem son zamanlardaki TTNET Fatura virüsü içinn geçerli değildir.**

CryptoLocker virüsünün şifrelediği dosyaların şifresini kaldırmak için aşağıdaki adımları takip edin:

CryptoLocker virüsünün şifrelediği dosya için Private KEY edinme:

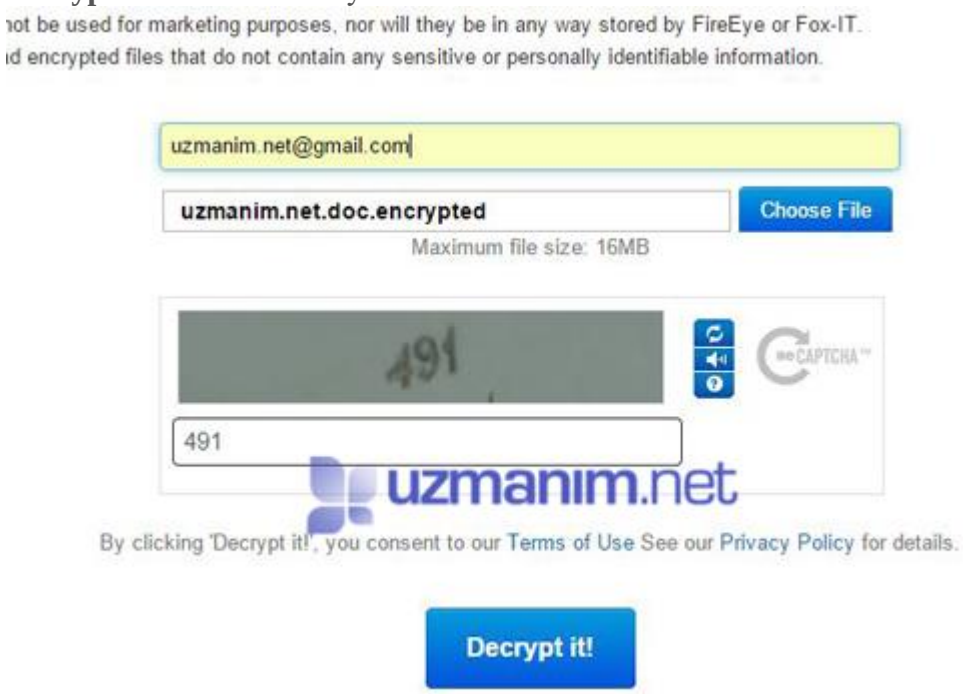
Private KEY CryptoLocker virüsünün şifrelediği dosyaları çözmek için gerekli anahtar metindir. Aşağıdaki adımlar ile bu KEY yani anahtarı nasıl oluşturacaksınız bulabilirsiniz.

1. Buradaya tıklayarak FireEye ve Fox IT web sitesi olan decryptcryptolocker web sitesini açın.
2. Formu doldurun. **Email** adresinizi yazın. Şifreyi çözmek için gerekli Key dosyası email adresinize gönderilecektir.

   Choose File butonuna tıklayarak **.encrypted** uzantılı şifreli dosyasınız seçin.

   reCAPTCHA ekranında ekranda resimde gördüğünüz karakterleri **Metni Yazın** yazan kutuya doğru şekilde yazın.

   Decrypt it! butonuna tıklayın.



3. **CryptoLocker File Upload Succes** mesajını göreceksiniz.
4. Mail adresinizi kontrol edin mail adresinize Results of DeCryptoLocker Service yazılı bir mesaj gelmiş olmalı.
5. Mailin içinde size ait Private Key bilgisi olacaktır. Private Key aşağıdaki metne benzeyen karakter topluluğudur:

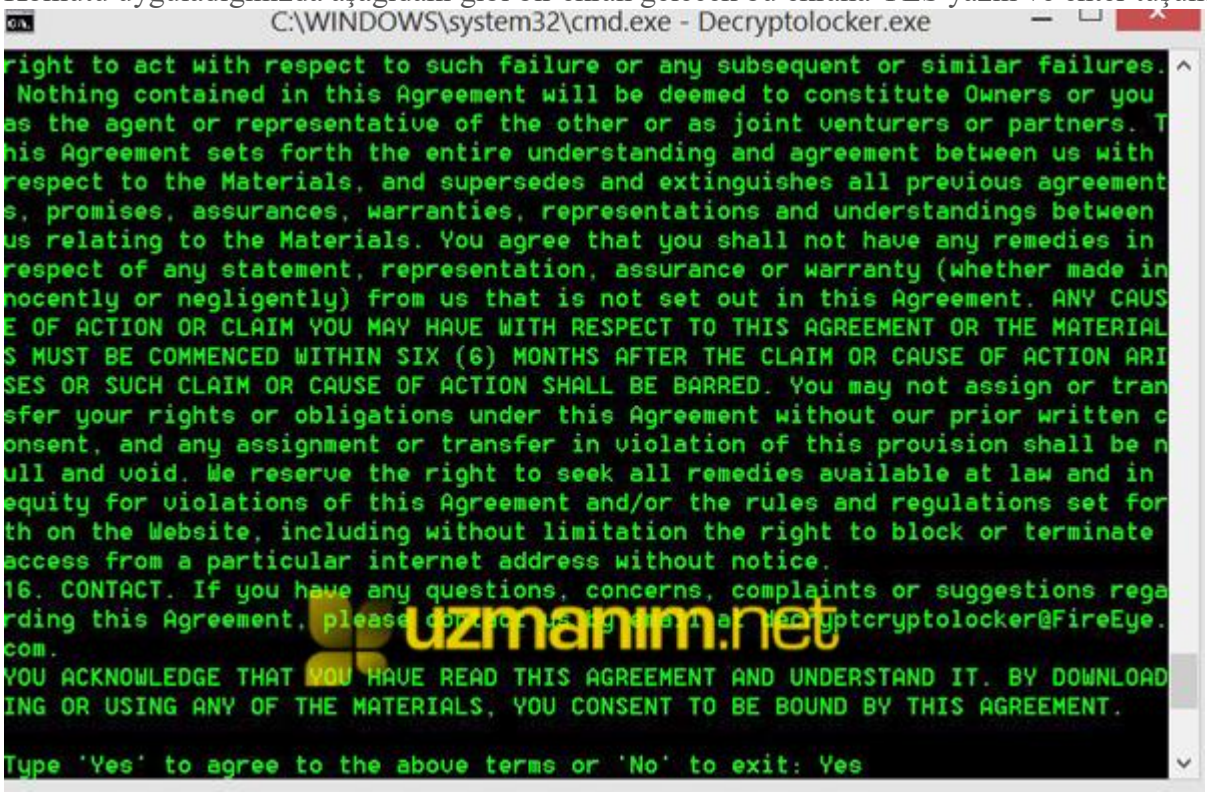
6. -----BEGIN RSA PRIVATE KEY-----
7. MIICWwIBAAKBgFEFU71H6IvEb1nFqcog3KCnPDWDGNYFkJ+gKOwQ5VOTCOkKjhwv
8. W25t6fJaWaEQEDDO0dmk58XFWU5MzYLyGWulgqRalzqe4kM1kZ1MzeL8stMyqfUP
9. AwxAtSbwmFEj3swZdulrqK7Mk9izzOqFta7ixOi+HGK+w/pyTF9C/yaJAgMBAAEC
10. gYA2ssb/Ec4AlkSqsdTYPmlVGLKAWhppW2ZxLfqSrTF1w92PH24jvyEWI6R+1tqN
11. 7z9PBEIOktNa5MpPH3Dbh8D69kuWgp7JQBhfyxnK8nRm0DMDO5Wc3RlVhLNTreRP
12. KKMwPELRVQEB9ZoLAZxEASkxlOrPAyWHbR4vJoeVrBB+VQJBAJKcIyWYm6y2SwRS

13. z7Z4FPPna7RAHkWepEPIgl/+hhYVO6V6rX9dSFHBLg7T+Fx2E/soTsx0+T677v8X
14. wQtf0MMCQQCNeQ78LjYQgn5TXJyxxSvofJpMAcsPaa3vLwFyF2f7KQuElzgiXkHJ
15. llUzBad2PEAvmq5JpM4bx7/hlf6hfjbDAkAQM/dicVJLLT5vNOPF69GM/zeVDT0L
16. PrQy1ZcrGssg56nW6Q8Bs4KJnosDkoOxXE9rA5Jp4EenmkeYo7xvEGDXAkEAid2h
17. Zsu50Bj69k3YPb1B7swOqWdN9XUtFVufcwmwQShcmxeqkoN8ZPDlklU+PpC0lC+P
18. DSFX4eak7Td47vPKdQJASaalvGHNgwm6HsnxUgz6jT2dmiPBXwY+TfIU1EzbOpJp
19. PMiN7YMTmPaAWS6Ldm4Reb4XOc/lMPeWolQflCRisQ==
    -----END RSA PRIVATE KEY-----
20. Bu, CryptoLocker virüsü'nün şifrelediği dosyayı çözmek için gerekli anahtar metindir.

PRIVATE KEY'i kullanarak CryptoLocker virüsünün şifrelediği dosyaların açılması

1. Buradan CryptoLocker temizleme programını indirin.
2. İndrmiş olduğunuz dosya Decryptolocker.exe dosyası virüsün şifrelediği dosyaları açacak uygulamadır.
3. Decryptolocker.exe dosyasını şifreli dosyanın olduğu klasöre kopyalayın.
4. Örneğin şifreli dosyalarımız Masaüstünde Özel klasöründa olsun. Decryptolocker.exe dosyasını özel klasörünün içine kopyalayın.
5. Decryptolocker.exe komut satırı uygulamasıdır. Yani bir takım komutlar kullanarak şifre çözme gerçekleşecek.
6. Komut istemini (CMD.exe) yönetici olarak çalıştırın. Bilmiyorsanız buradan nasıl yapıldığını öğrenebilirsiniz
   Windows 7'de CMD yönetici olarak nasıl çalıştırılır?
   Windows 8'de CMD yönetici olarak nasıl çalıştırılır?
7. Komut isteminden şifreli dosyanın olduğu klasöre girin. Örnekteki gibi özel klasörüne ulaşmak için şu komutu kullanın. Bu komut siste değişecektir. Örneğin kullanıcı adınız uzmanim.net yerine siz ne ise onu yazın.
   ```
   cd  c:\Users\uzmanim.Net\Desktop\Ozel
   ```
8. Daha önce bu klasöre kopyaladığınız Decryptolocker.exe dosyasını çalıştıracaksınız. Şu komutu uygulayın
   ```
   Decryptolocker.exe –key “Email ile gelen Key”  Şifrelidosya.doc
   ```
9. Key bölümünü size gelen maildeki aşağıdaki ifadeleride içeren karakter topluluğudur. Örnekteki gibi çift tırnak içinde mailin içindeki KEY'i komuta yapıştırın. Yukarıda örneğini vermiştim.
10. Kolaylık sağlaması için komutu notepad ile hazırladıktan sonra kopyala-yapıştır yapabilirsiniz.

11. Komutu uyguladığınızda aşağıdaki gibi bir ekran gelecek bu ekrana YES yazın ve enter tuşuna basın.



12. Daha sonra ekrana Successfully decrypted file: uzmanim.net.doc gibi bir mesaj gelirse dosyanız kurtuldu demektir.

Baştan da belirttiğim gibi **CryptoLocker** virüsü farklı şekillerde ortaya çıkabiliyor. Virüsün enfekte olduğu her sistem için vir Private Key gereklidir. Birden fazla sistem kullanıyorsanız bu işlemi yani Key alma işlemini tekrat etmeniz gerekecektir.

Ayrıca yukarıda anlatılan yöntem tüm **CryptoLocker** virüsü türevlerinde başarılı olamayabilir. Lütfen bunu bilerek bu işlemi yapın. Yukarıdaki işlemler sisteminize zarar vermez.

CryptoLocker virüsü temizlemek ücretsiz bir işlemdir. Yukarıda anlatılan servis ve programlar ücret gerektirmiyor.

Eğer bir klasörü tamamen şifrelemeden kurtarmak istiyorsanız o zaman aşağıdaki komutu kullanın.

```
Decryptolocker.exe –key “Key” C:\Klasör Adı\*
```

Eğer bir sürücüdeki tüm **CryptoLocker** virüsünün etkilediği şifreli dosyaları şifreden kurtarmak istiyorsanız

```
Decryptolocker.exe –key  “Key” -r C:\
```

komutunu kullanın.

Şuan CryptoLocker virüsüne karşı en etkili temizleme ve şifre kaldırma yöntemi yukarıda bahsettiğim yöntemdir. Bunun dışında yapılacak işlemler dosyalarınıza zarar verebilir. Bu sebepten dosyalarınızı manuel düzenlemeye, değiştirmeye çalışmayın.

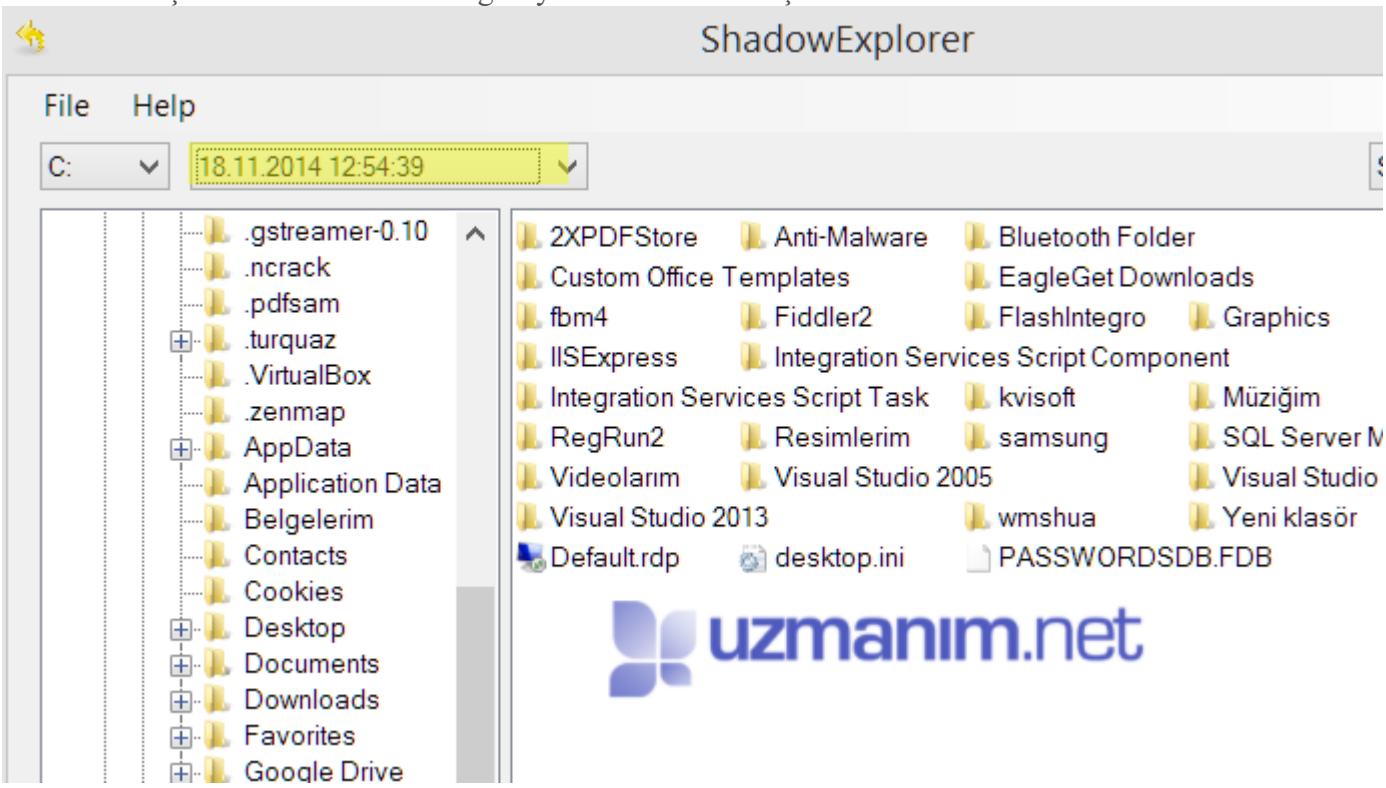
CryptoLocker virüsü tarafından şifrelenen dosyaları el ile kurcalamak dosyaların kalısı olarak bozulmasına sebep olur. Daha sonra bir şekilde Key üretilse bile bozuk dosya da çalışmayacaktır.

Çözüm 2: CryptoLocker virüsü Alternatif çözüm yolu:

TTNET Fatura virüsü için bu yöntem denenebilir. TTnet Fatura virüsü normalde kullanıcının yetkisi varsa gölge kopyaları siliyor. Fakat kullanıcınızın yetkisi yoksa silme işlemi başarılı olamıyor ve gölge kopya üzerinden dosyaları kurtarmak mümkün oluyor.

CryptoLocker virüsünden dosyaları kurtarmanın bir diğer yolu Sistem geri yüklemesi oluşturulmuş sistemlerde eski bir tarih üzerinden dosyanın gölge kopyasını almak. Fakat sizde sistem koruması açık ve bir geri yükleme noktası oluşturulmuş olmalı.

1. **ShadowExplorer uygulamasını buradan indirin.**
2. ShadowExplorer uygulamasını kurduktan sonra çalıştırın.
3. Virüsün bulaşma tarihinden önce bir geri yükleme noktası seçin.



4. Kurtarmak istediğiniz dosyayı sağ tuşla tıkayın ve Export'u seçin.
5. Nereye kaydetmek istiyorsanız oraya dosyanızı kaydedin.

C: karşısında kayıt göremiyorsanız gölge kopyanız yok veya virüs tarafından silinmiş demektir. Bu durumda yapabileceğiniz şuan için hiç bir işlem kalmıyor.

Cryptolocker şifre çözme yazılımı satın alsak kesin olarak dosyalarımız çözülür mü?

Bunun bir garantisi yok. Cryptolocker virüs saldırıları tek bir elden çıkmıyor. Parasını yani fidyeyi ödediği halde şifresi çözülmeyen kullanıcı mevcut.Fidye ödeyip dosyalarını kurtaranlar da elbette var.

Cryptolocker şifre çözme yazılımı satın alınarak şifre çözülüyorsa, neden biri satın aldığı programı internetten dağıtmıyor?

Korsanlar, cryptolocker şifre çözme yazılımını her bilgisayar için ayrı, özel olarak üretiyorlar. Yani sizin satın aldığınız bir program başka bilgisayarda çalışmayacaktır. Aynı şekilde başkasının aldığı yazılım sizin bilgisayarınızda çalışmayacaktır.

Internette para karşılığını Cryptolocker ile şifrelenen dosyaları çözdüğünü idda edenler var. Güvenilirler mi?

Hayır. Bu tür kişilere güvenmeyin. AES-256 şifreleme teknikniği henüz kırılabilmiş bir yöntem değil. Dünya genelinden bahsediyorum. Eğer böyle bir yetenek olsaydı tüm dünya adını zaten duyardı. O kişide sizin mağduriyetinizden yararlanmaya çalışmazdı.