Yazar Kamil DEM?RTA?
Cumartesi, 11 Temmuz 2015 13:00

    �kemizdeki internet kullan?c?lar?n? hedef alan KriptoKilit sald?r?lar? daha �ce de ger�kle?mi?ti.[1,2] Fakat bu sefer KriptoKilit g�ncel s�r�m� ile daha b�y�k bir tehdit olarak kar??m?za �kt?. Kendini a�k bir ?ekilde CryptoLocker olarak tan?tan bu yeni zararl? yaz?l?m, yine kullan?c?lara ait belli uzant?lara sahip dosyalar? ?ifrelemekte ve bu verilerin kurtar?lmas? i�n kullan?c?lardan�?ifre �zme yaz?l?m?� ad?nda bir yaz?l?m sat?n almalar?n? istemektedir. <h2 style="text-align: left; margin-top: 5px; margin-bottom: 5px; font-size: 12px;"></h2> <h2 style="text-align: left; margin-top: 5px; margin-bottom: 5px; font-size: 12px;">Bula?ma ?ekli</h2> Zararl? yaz?l?m fatura epostalar? ?eklinde kullan?c?lara eposta g�dermektedir. ?ekil 1- CryptoLocker Taraf?ndan Kullan?c?lara G�derilen Eposta   ?ekil 1�de g�terildi?i �zere fatura tutar? y�ksek bir miktard?r. Faturan?n y�ksek tutar?ndan ��r fatura hakk?nda bilgi almak isteyen kullan?c?lar faturay? g�mek istediklerinde ?ekil 2� de g�terilen web adresine y�lendirilmektedirler. ?ekil 2- Fatura ?ndirme Sayfas?   Kap�y? girip indir butonuna t?klan?ld???nda �.zip� uzant?l? bir dosya indirmektedir. Bu dosyan?n i�nde ise �.exe� uzant?l? fatura dosyas? bulunmaktad?r. (D?KKAT: telefon, internet, banka vb sitelerden hi�ir zaman �.zip� uzant?l? <span

style="color: #333333; font-family: Tahoma, Arial, sans-serif; font-size: 12px; line-height: 16.7999992370605px; text-align: justify; background-color: #f4f4f4;"> .exe uzant?l? bir dosya i ren mail GELMEZZZ) ?ekil 3-?ndirilen Zararl? Dosya   ?ndirilen bu zararl? yaz?l?m l??t?r?ld???nda ise zararl? yaz?l?m kullan?c?n?n bilgisayar?na bula?makta ve i bo? olmayan .doc, .docx, .pdf, .txt, .7z, .rar, .zip tipinde olan dosyalar ?ifrelenmektedir. ?ifrelenen dosyalar?n yeni uzant?lar? .encrypted olmaktad?r. ?ekil 4te bu durum g terilmektedir.   ?ekil 4- ?ifrelenen Veriler (Uzant?lar?na bakt???n?zda .encrypted oluyor)

  ?ekil 5- Verilerin ?ifrelenmesinden Sonra Ekrana kan G nt   Zararl? yaz?l?m bilgisayardaki verileri ?ifreleme i?lemini bitirdikten sonra ekrana ?ekil 5teki gibi bir sayfa karmaktad?r. G ld? zere zararl? yaz?l?m ?ifrelenen veriler kar??l???nda ?ifre zme yaz?l?m? ad? alt?nda bir yaz?l?m?n sat?n al?nmas?n? istemektedir.   ?ekil 6- ?ifre zme Yaz?l?m? Sat?n Alma ?ekli ve Tutar?
 ?ekil 5 te kan g nt deki linke t?kland???nda asl?nda tor a?? zerinde olan fakat bir tor proxy hizmeti veren sunucu zerinden eri?ilebilen ?ekil 6 daki gibi ki?iye el bir web sayfas?na y lendirilme yap?lmaktad?r. <div style="font-family: Tahoma, Arial, sans-serif; line-height:

16.7999992370605px; font-size: 12px; color: #333333; text-align: justify; background-color: #f4f4f4;"> ?ifre &#65533;zme yaz?l?m?n?n sat?n al?nmas? konusunda ise 96 saat i&#65533;nde sat?n al?m? durumunda 2398 liradan 1198 liraya kadar indirim yapmaktad?r.   Zararl? yaz?l?m ilk yay?ld???nda antivir&#65533;s firmalar?n?n b&#65533;y&#65533;k bir &#65533;?unlu taraf?ndan tan?nmam??t?r. Virustotal sonu&#65533;ar? ?ekil 7&#65533;de g&#65533;terilmektedir.   ?ekil 7- Antivir&#65533;s Firmalar?n?n CryptoLocker Sonu&#65533;ar?   <h2 style="text-align: left; margin-top: 5px; margin-bottom: 5px; font-size: 12px;"></h2> <h2 style="text-align: left; margin-top: 5px; margin-bottom: 5px; font-size: 12px;">Dikkat Edilmesi Gerekenler </h2>   CryptoLocker gibi eposta yoluyla gelen zararl? yaz?l?mlardan etkilenmemek i&#65533;n gelen eposta adreslerine &#65533;k dikkat edilmelidir.?ekil 8&#65533;de ger&#65533;k bir ttnet fatura eposta adresi ile ?ekil 9&#65533;da zararl? yaz?l?m?n?n eposta adresleri g&#65533;terilmektedir.   ?ekil 8- Ger&#65533;k TTNet Fatura G&#65533;derim Adresi (T&#65533;rkiyedeki kurumsal firmalar?n &#65533;?unda web site adresinin sonunda .tr ifadesini g&#65533;&#65533;rs&#65533;n&#65533;z.

  ?ekil 9- Sahte Fatura G&#65533;derim Adresi

   <p

style="font-family: Tahoma, Arial, sans-serif; line-height: 16.7999992370605px; font-size: 12px; color: #333333; text-align: justify; background-color: #f4f4f4;">TTNet'in fatura g��nt�leme adresi "https//:efatura.ttnet.com.tr" iken zararl? yaz?l?m?n kulland??? ise "efatura.ttnet-fatura.info" ve �efatura.ttnet-fatura.biz" adresleridir. Eposta olarak g�derilen faturalar?n uzant?lar?na dikkat edilmelidir. CyrptoLocker zararl? yaz?l?m? bir .exe dosyas?d?r. Oysaki TTNet faturalar? pdf ?eklinde g�termektedir. Dosyalar?n uzant?lar? bilgisayarlarda normalde g��nmemektedir. Dosya uzant?lar?n? g�ebilmek i�n klas� ayarlar?ndan bilinen dosya t�rleri i�n uzant?lar?n? g�terme (Hide extensions for known types) ayar? de?i?tirilmelidir. ?ekil 10�da bu ayarlama g�terilmektedir. ?ekil 10- Dosya Uzant?lar?n?n G�terimi ?�n Yap?land?rma Ayn? zamanda Ttnet faturalar? kullan?c?lara faturalar? indirtmek yerine browserda g�termektedir. (?ekil 2�de ise sahte sayfa g�terilmi?tir.)   (Referanslar: http://www.bilgiguvenligi.gov.tr/ Osman Pamuk, Alican Akyol, T�?TAK B?LGEM SGE)   <h1 style="line-height: 16.7999992370605px; color: #333333; font-family: Tahoma, Arial, sans-serif; text-align: justify;">BU V?R? B?LG?SAYARA BULA?INCA NE OLUR:</h1>   <ul style="list-style-type: circle; color: #333333; font-family: Tahoma, Arial, sans-serif; font-size: 12px; line-height: 16.7999992370605px; text-align: justify; background-color: #f4f4f4;"> T? S���ERDEK? ?I??ma dosyalar?m?z ?ifrelenmi? olur ve ?ifrelerini ?zene kadar bir daha kullan?lmaz hale gelir.
  <ul style="list-style-type: circle; color: #333333; font-family: Tahoma, Arial, sans-serif; font-size: 12px; line-height: 16.7999992370605px; text-align: justify; background-color: #f4f4f4;"> Yede?imiz varsa bilgisayardaki vir�s? temizledikten sonra geri dosyalar?m?z? kopyalayabiliriz.
  <ul style="color:

#333333; font-family: Tahoma, Arial, sans-serif; font-size: 12px; line-height: 16.7999992370605px; text-align: justify; background-color: #f4f4f4;"> E?er yede?imiz yoksa vir&#65533;s&#65533; bula?t?ran ki?i zaten mail adresini klas&#65533;lere b?rak?yor ve sizden dosyalar?n?z? geri kurtarmas? i&#65533;n 1.000-2000 hesab?na para yat?rman?z? istiyor. Yat?rsan?z bile kurtaraca?? me&#65533;ul.

  <h1 style="line-height: 16.7999992370605px;">HANG? &#65533;LEMLER? ALMALIYIZ:</h1>
  Bilmedi?imiz ki?ilerden gelen mailleri a&#65533;amal?y?z

  <ul style="color: #333333; font-family: Tahoma, Arial, sans-serif; line-height: 16.7999992370605px; text-align: justify; font-size: 12px;"> Muhasebe vb. &#65533;k &#65533;emli bilgi i&#65533;ren bilgisayardan internete girmemekte fayda var.

  <ul style="color: #333333; font-family: Tahoma, Arial, sans-serif; line-height: 16.7999992370605px; text-align: justify; font-size: 12px;"> Antivir&#65533;s Programlar? Y&#65533;klemeliyiz. ve Programdan Mail g&#65533;venli?ini en &#65533;st d&#65533;zeye &#65533;karmal?y?z.
   <ul style="color: #333333; font-family: Tahoma, Arial, sans-serif; line-height: 16.7999992370605px; text-align: justify; font-size: 12px;"> Trojan temizleme programlar? y&#65533;klemeliyiz.
      Mutlaka EN AZ 2 TANE HAR?C? D?SK?M?Z Olmal?

  (2 adet 1TB diske en fazla 300TL-400TL verirsiniz ama birka&#65533;bin dolar vermekten ve riske atmaktan daha iyidir.)
 1. Diske G&#65533;L&#65533; YEDEK
 2. Diske HAFTADA B?R YEDEK ALMALIYIZ.
 VE BU D?SKLER? ASLA BA?KA B?R ?? ?&#65533;N KULLANMAMALIYIZ.
  Yedek sonras?nda &#65533;kart?p &#65533;k s?cak ve nem olmayan bir

ortamda saklamal?y?z.   <h1> Benim Al??veri? sitemden Disk almak isterseniz. www.sehrinfirsatlari.com</h1> <h2>(��n hemen elinize ge�esi i�n l�tfen HIZLI G�DER? �r�nleri se�niz.)</h2>