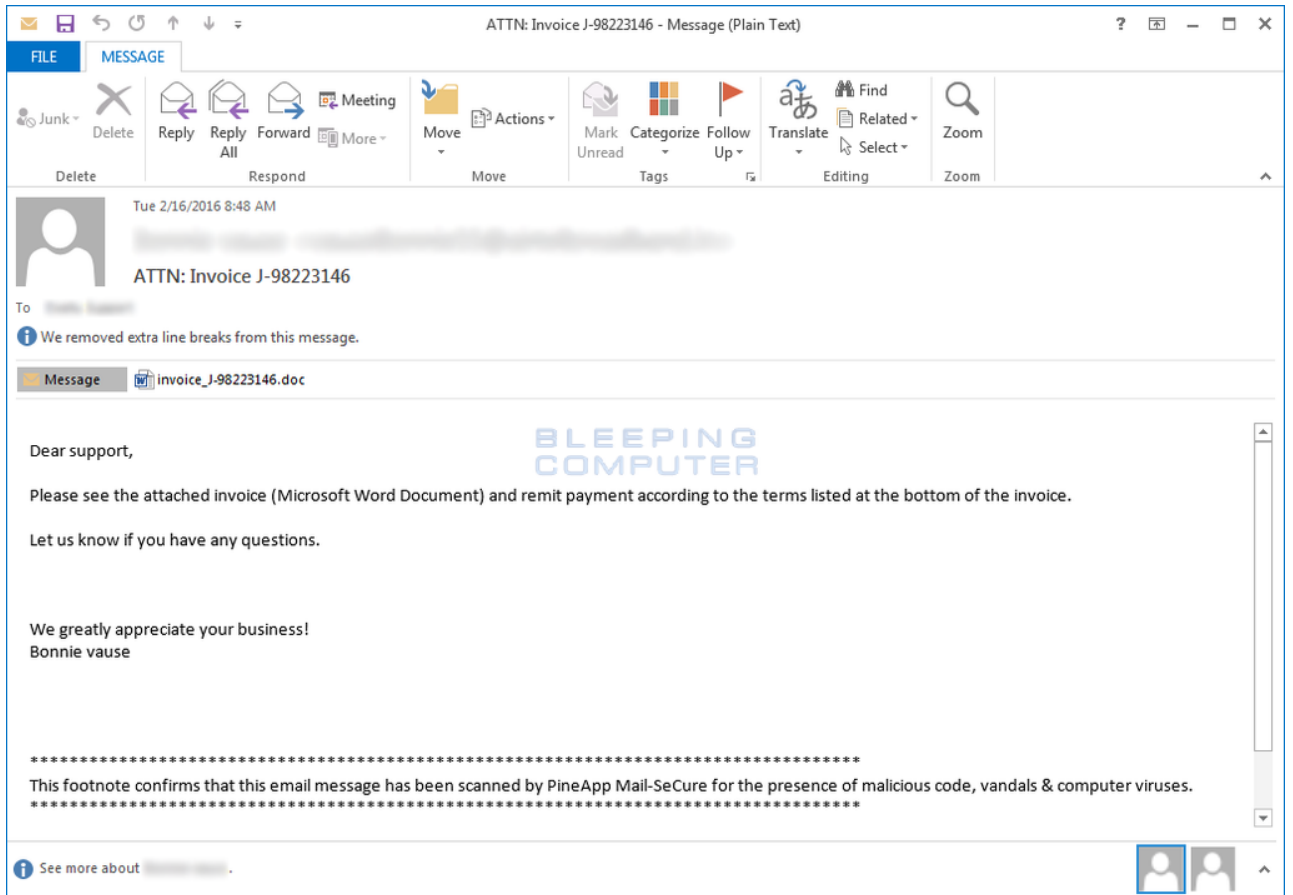


Locky virüsü nedir?

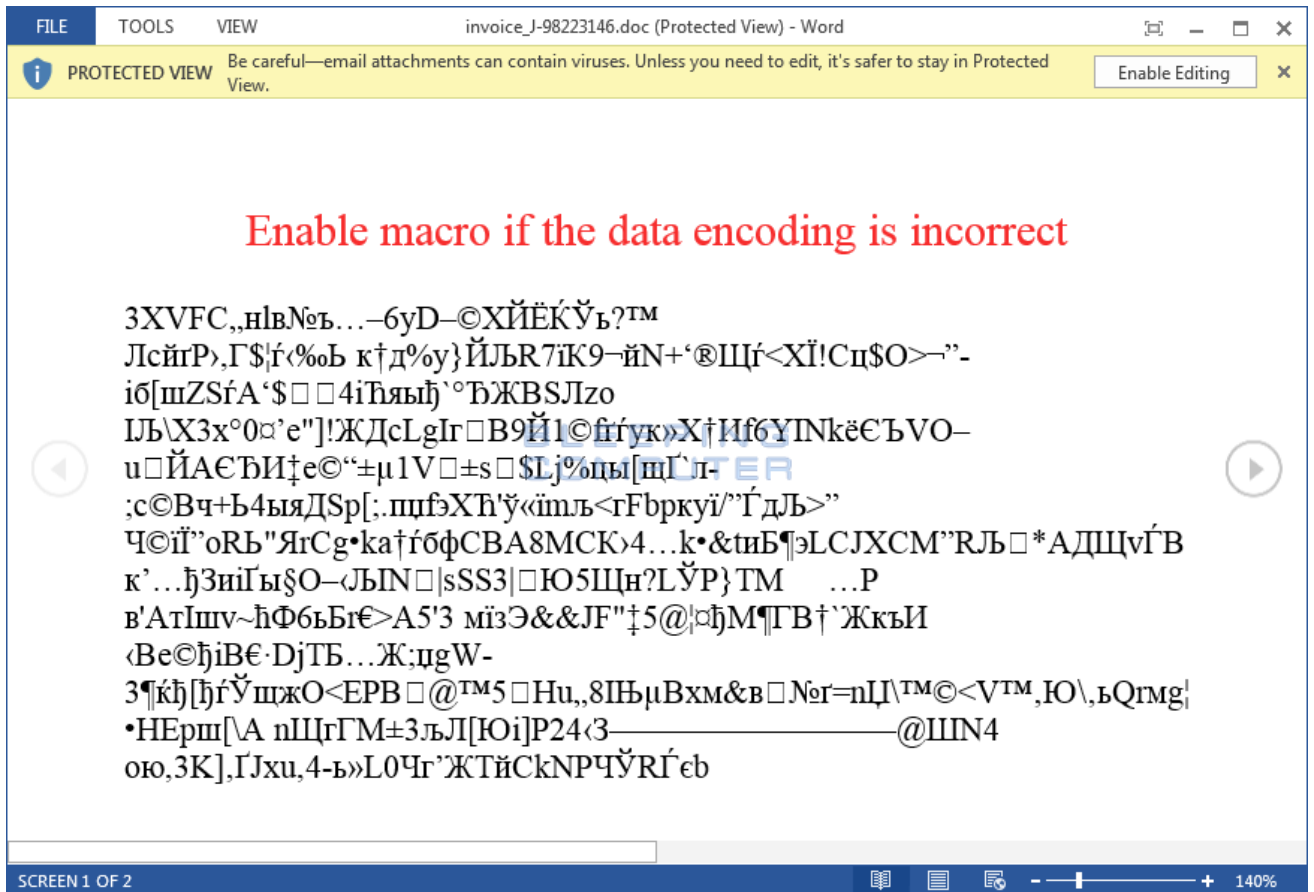
Son zamanlarda yaygın olan **dosya şifreleme** virüsleri bir çok kullanıcının başına dert olmuş durumda. Geçtiğimiz günlerde bu dosya şifreleme virüslerine bir yenisi daha eklendi. Virüsün adı ise **Locky**. **AES** şifreleme algoritmasını kullanan **Locky virüsü**, daha önceki **dosya şifreleme** virüslerine göre oldukça profesyonel bir şekilde hazırlanmış gibi gözüküyor.

Locky virüsü bilgisayarına nasıl bulaştı?

Locky virüsü, bilgisayarınıza e-posta adresinize gelen **ATTN: Invoice J-98223146** başlıklı mail aracılığıyla bulaşıyor. Bu mailin içerisinde bulunan **ATTN: Invoice J-98223146.doc** uzantılı Word dosya eki **Locky virüsünün** ta kendisi.

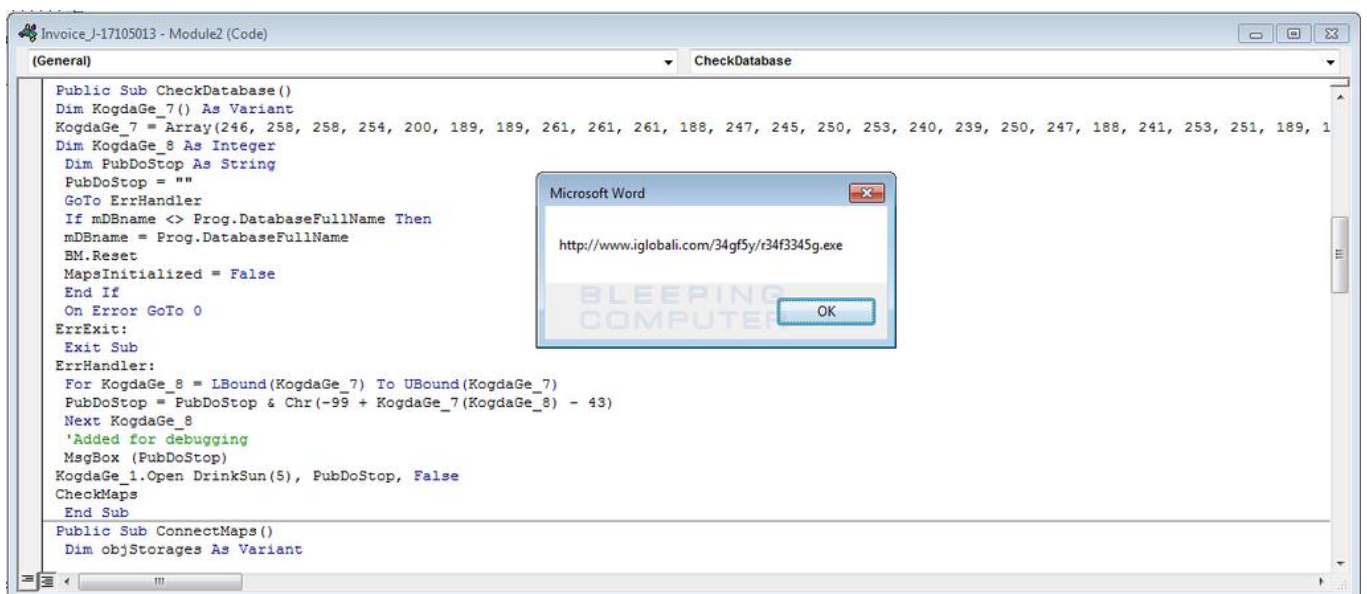


E-posta aracılığıyla gelen **ATTN: Invoice J-98223146.doc** uzantılı dosya açıldığında ise karşınıza şifrelenmiş, okunmaz bir doküman açılıyor. Bu okunamaz haldeki **ATTN: Invoice J-98223146.doc** dosyası sizden makroları etkinleştirmeniz için bir uyarı açıyor.



Kurban makroları etkinleştirdikten sonra **Locky virüsü**, uzak sunucudan gerekli dosyalarını indiriyor.

Locky virüsü, şifreleme işlemini başlatmak için indirdiği gerekli dosyalarını **%Temp%** klasöründe tutuyor. Gerekli dosyalarının tamamlanması durumunda ise **Locky virüsü** şifreleme işlemlerini başlatıyor.



Locky virüsü, ATTN: Invoice J-98223146.doc uzantılı belgenin makrolarının etkinleştirilmesinin ardından bilgisayarın tüm sürücülerini tarayarak hedefinde olan dosya uzantılarını şifreler.

Locky virüsünün şifrelediği dosya uzantıları:

.mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .tar.bz2, .tbk, .bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .php, .ldf, .mdf, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .asc, .lay6, .lay, .ms11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx, .docm, .docx, .DOT, .max, .xml, .txt, .CSV, .uot, .RTF, .pdf, .XLS, .PPT, .stw, .sxw, .ott, .odt, .DOC, .pem, .csr, .crt, .key, wallet.dat

Locky virüsünün bulaştığı dosya yolu ve klasör isimleri:

tmp, winnt, Application Data, AppData, Program Files (x86), Program Files, temp, thumbs.db, \$Recycle.Bin, System Volume Information, Boot, Windows

Locky virüsü şifrelediği dosyaların ismini de değiştirmektedir.

Örneğin **uzmanim.net.jpg** uzantılı bir dosya **Locky virüsü** ile şifrelendikten sonra **F67091F1D24A922B1A7FC27E19A9D9BC.locky** olarak değişiyor.

Ek olarak **Locky virüsünün** aynı zamanda ağda bulunan dosyaları da şifrelediğini söyleyelim.

Locky virüsü, hedef aldığı dizinlerdeki dosyaları şifreledikten sonra aşağıda bulunan kodu çalıştırarak sistem gölge kopyalarını da silmektedir. Bu yüzden Shadow Explorer gibi yazılımlar **Locky virüsünün şifrelediği dosyaları kurtarmak** için başarısız olacaktır.

Locky virüsünün gölge kopyalarını silmek için çalıştırdığı kod:

```
vssadmin.exe Delete Shadows /All /Quiet
```

Locky virüsü bütün bu şifreleme algoritma işlemlerini tamamladıktan sonra masaüstünde **_Locky_recover_instructions.txt** adında bir doküman oluşturacaktır. Bu dokümanda **Locky virüsü**, şifrelediği dosyalar hakkında bilgi vermektedir.

```
* _Locky_recover_instructions.txt - Notepad2
File Edit View Settings ?
1      !!! IMPORTANT INFORMATION !!!!
2
3 All of your files are encrypted with RSA-2048 and AES-128 ciphers.
4 More information about the RSA and AES can be found here:
5     http://en.wikipedia.org/wiki/RSA_(cryptosystem)
6     http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
7
8 Decrypting of your files is only possible with the private key and decrypt program, which is on
  our secret server.
9 To receive your private key follow one of the links:
10    1. http://6dtxgqam4crv6rr6.tor2web.org/xxxxxxxxxxxxxxxx
11    2. http://6dtxgqam4crv6rr6.onion.to/xxxxxxxxxxxxxxxx
12    3. http://6dtxgqam4crv6rr6.onion.cab/xxxxxxxxxxxxxxxx
13    4. http://6dtxgqam4crv6rr6.onion.link/xxxxxxxxxxxxxxxx
14
15 If all of this addresses are not available, follow these steps:
16    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
17    2. After a successful installation, run the browser and wait for initialization.
18    3. Type in the address bar: 6dtxgqam4crv6rr6.onion/xxxxxxxxxxxxxxxx
19    4. Follow the instructions on the site.
20
21 !!! Your personal identification ID: xxxxxxxxxxxxxxxxxxx !!!
Ln 10 : 21 Col 44 Sel 0      1.09 KB      UTF-8 Signature CR+LF INS Default Text
```

Locky virüsü bilgisayarınız duvar kağıdını da değiştirmektedir. **Locky virüsü** bulaşan bilgisayarlarda duvar kağıdı aşağıdaki gibi görünmektedir.

```
!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/
2. http://6dtxgqam4crv6rr6.onion.to/
3. http://6dtxgqam4crv6rr6.onion.cab/
4. http://6dtxgqam4crv6rr6.onion.link/

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv6rr6.onion/
4. Follow the instructions on the site.

!!! Your personal identification ID: !!!
```