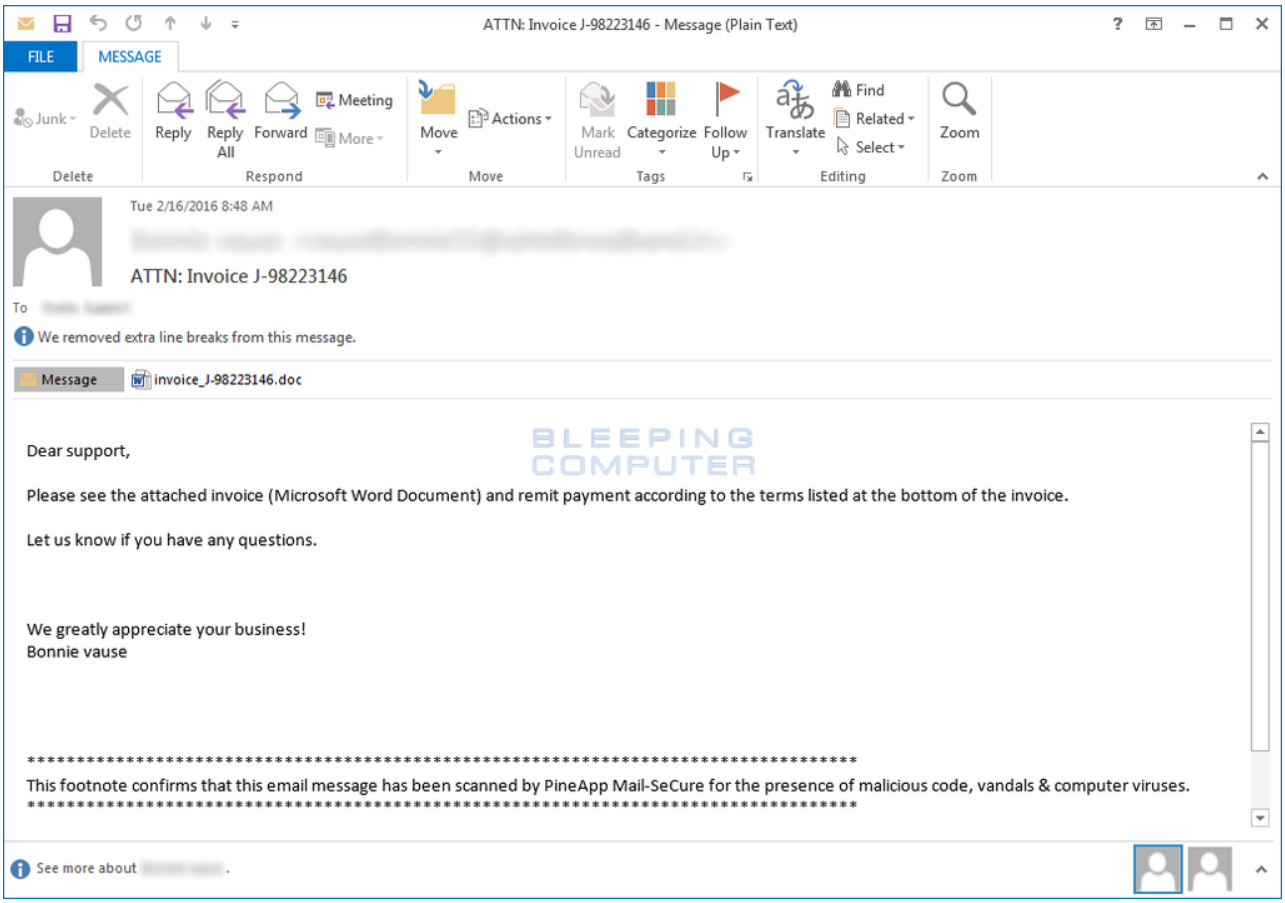
Locky virüsü nedir?

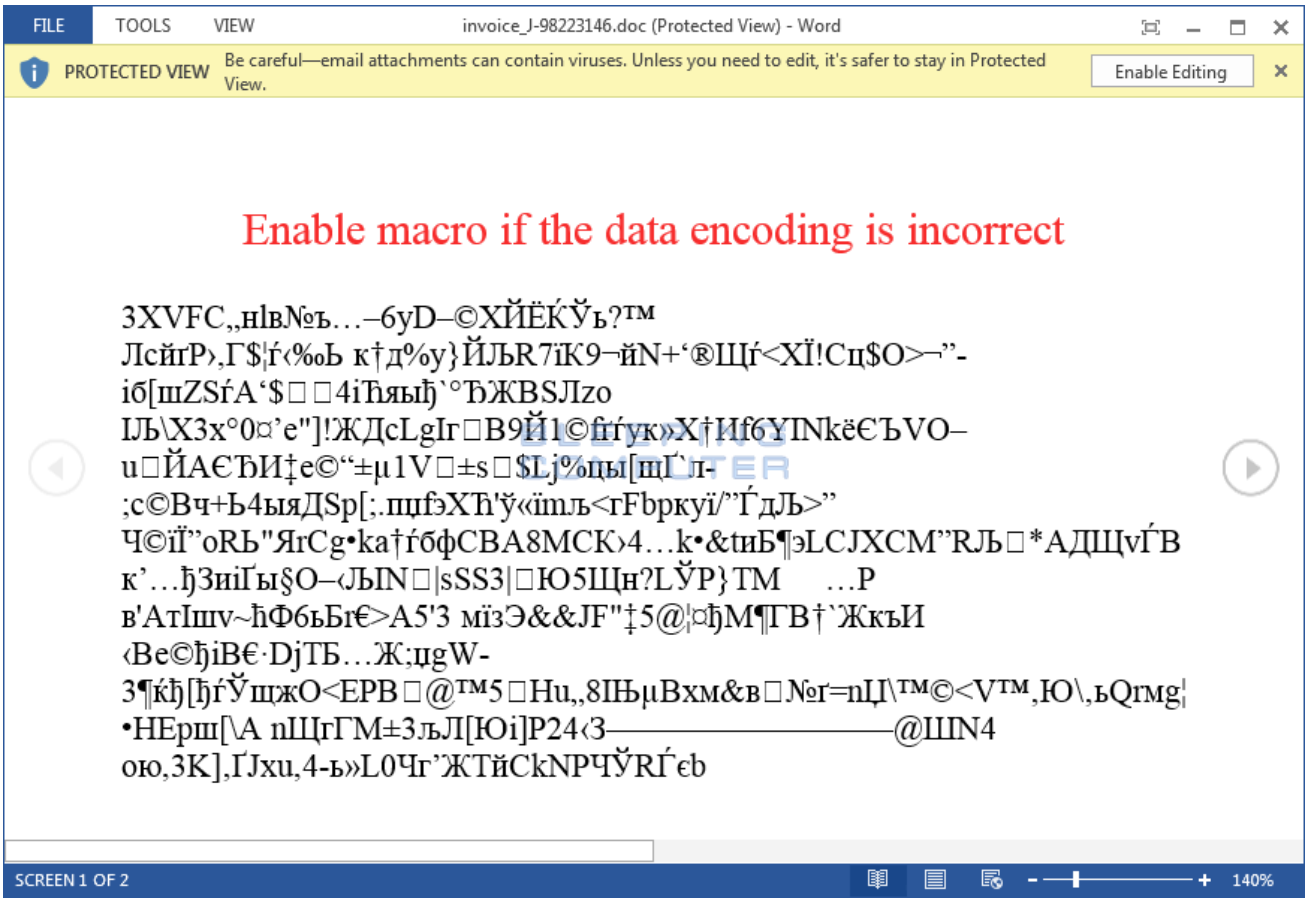
Son zamanlarda yaygın olan **dosya şifreleme** virüsleri bir çok kullanıcının başına dert olmuş durumda. Geçtiğimiz günlerde bu dosya şifreleme virüslerine bir yenisi daha eklendi. Virüsün adı ise **Locky. AES** şifreleme algoritmasını kullanan **Locky virüsü,** daha önceki **dosya şifreleme** virüslerine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

Locky virüsü bilgisayarıma 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 virüsü**nün ta kendisi.

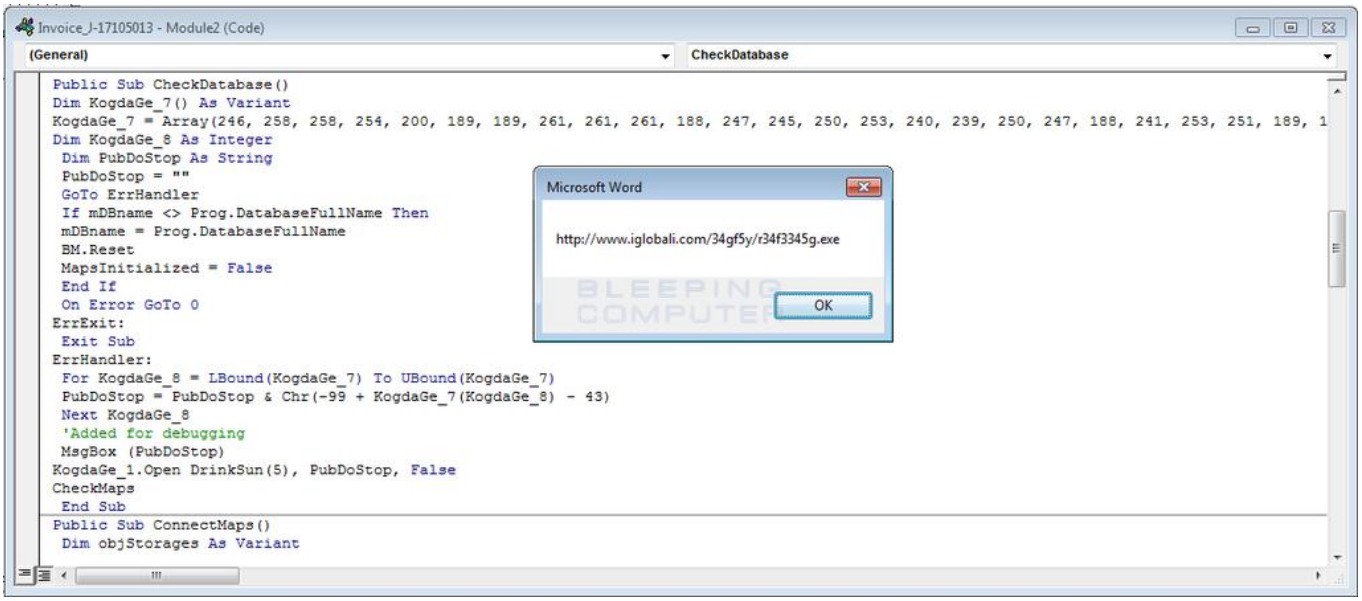


E-posta aracılığıyla gelen **ATTN: Invoice J-98223146.doc** uzantılı dosya açıldığında ise karşınıza şifrelenmiş, okunmaz bir doküman açılıyor. Bu okunamaz haldeki **ATTN: Invoice J-98223146.doc** dosyası sizden makroları etkinleştirmeniz için bir uyarı açıyor.



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 işlemerini 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.

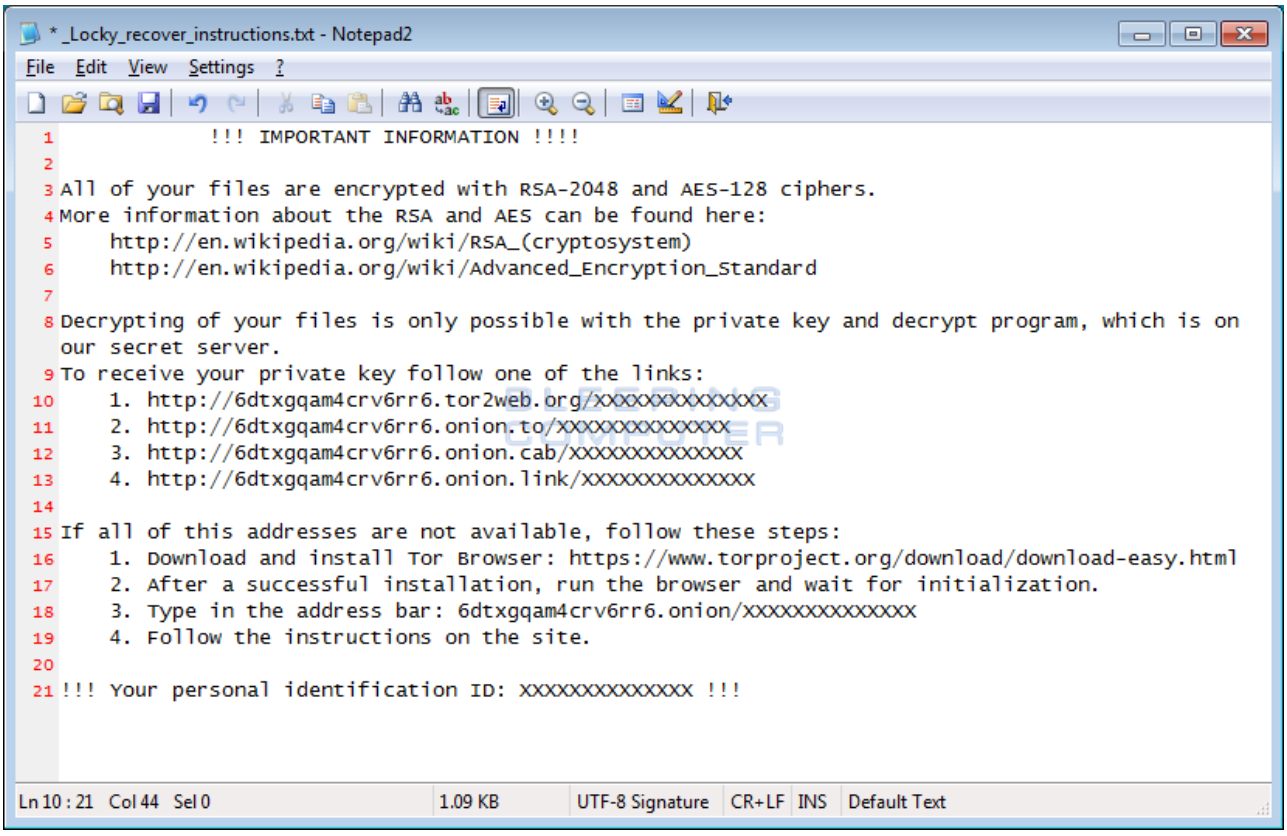
Ek olarak **Locky virüsü**nün aynı zamanda ağda bulunan dosyaları da şifrelediğini söyleyelim.

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