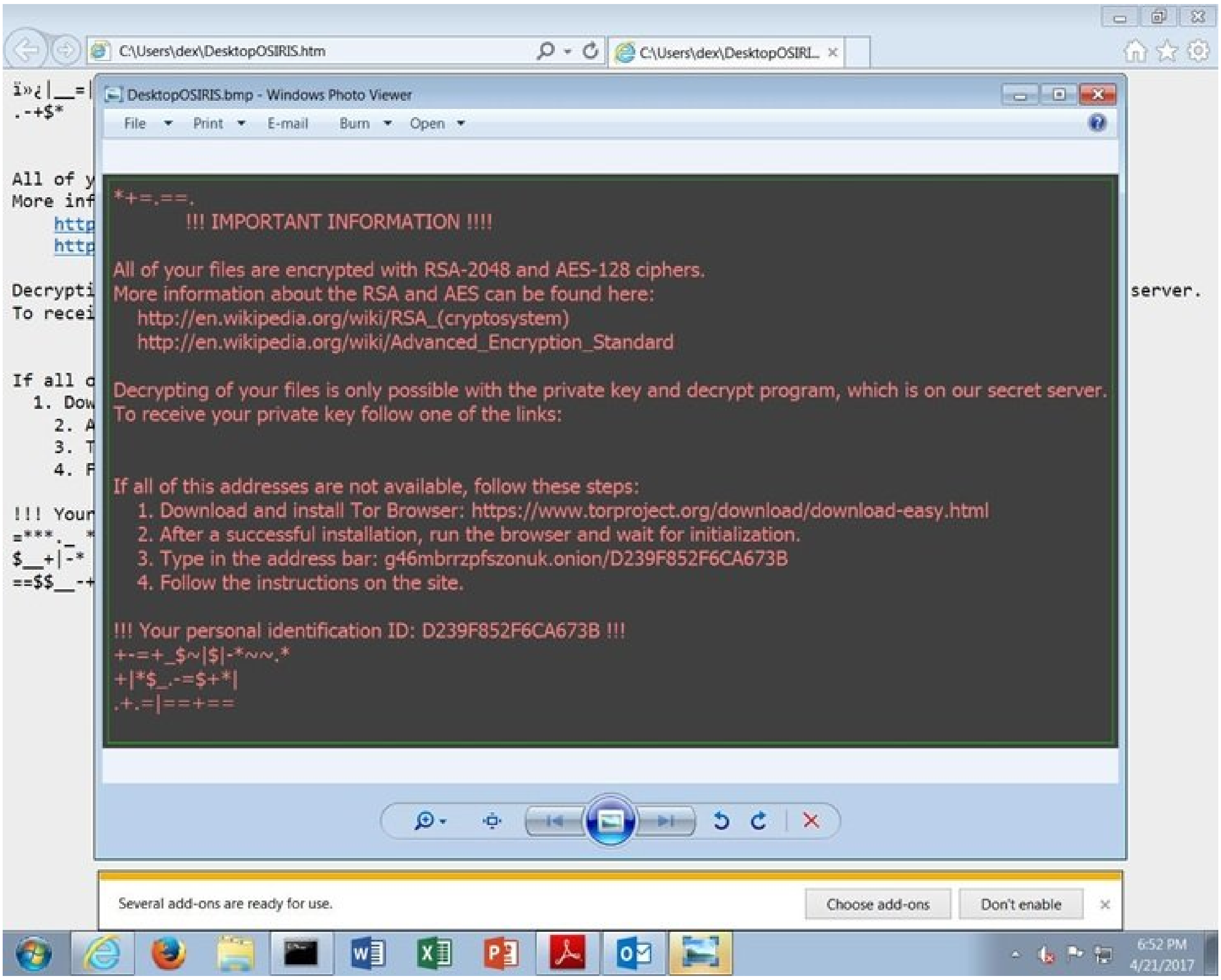
[illegible] [illegible] [illegible] Necurs [illegible] [illegible]

[illegible] Locky [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]


C:\Users\dex\DesktopOSIRIS.htm
C:\Users\dex\DesktopOSIRI...
DesktopOSIRIS.bmp - Windows Photo Viewer
File
Print
E-mail
Burn
Open
Several add-ons are ready for use.
Choose add-ons
Don't enable
6:52 PM
4/21/2017

```
*+=.==.
        !!! 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:


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: g46mbrrzpfszonuk.onion/D239F852F6CA673B
    4. Follow the instructions on the site.

!!! Your personal identification ID: D239F852F6CA673B !!!
+-=+_$~|$|-*~~.*
+|*$_.-=$+*|
.+.=|==+==
```

[illegible] [illegible].

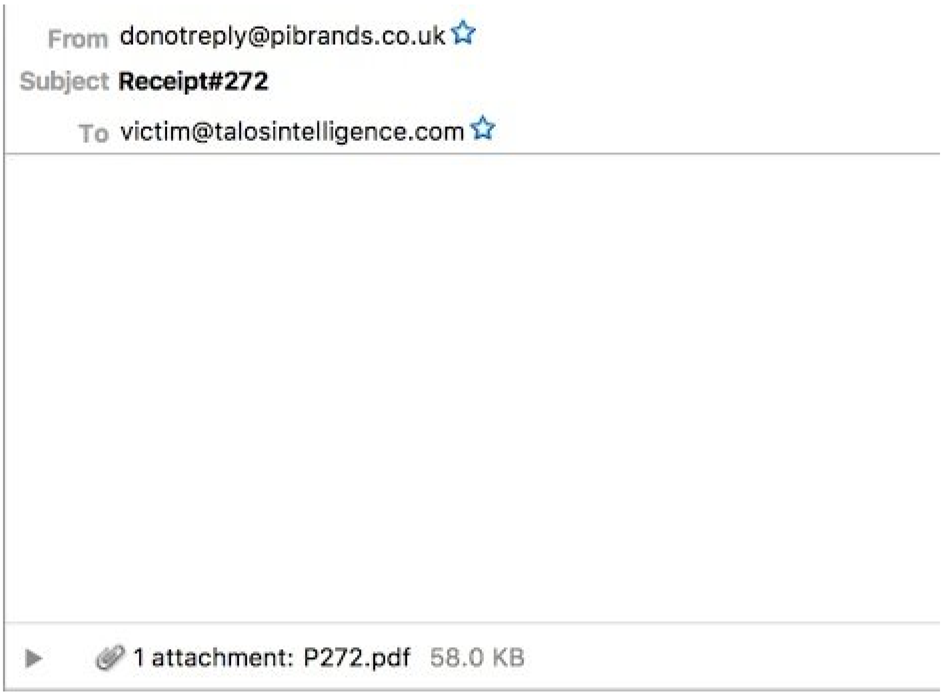
[illegible] Locky [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]. [illegible] [illegible] [illegible] [illegible] [illegible] 2017 [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]. [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] Necurs [illegible] [illegible]. Necurs [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] 1.7 [illegible] [illegible] [illegible] [illegible] [illegible].

[illegible]

[illegible]

[illegible]

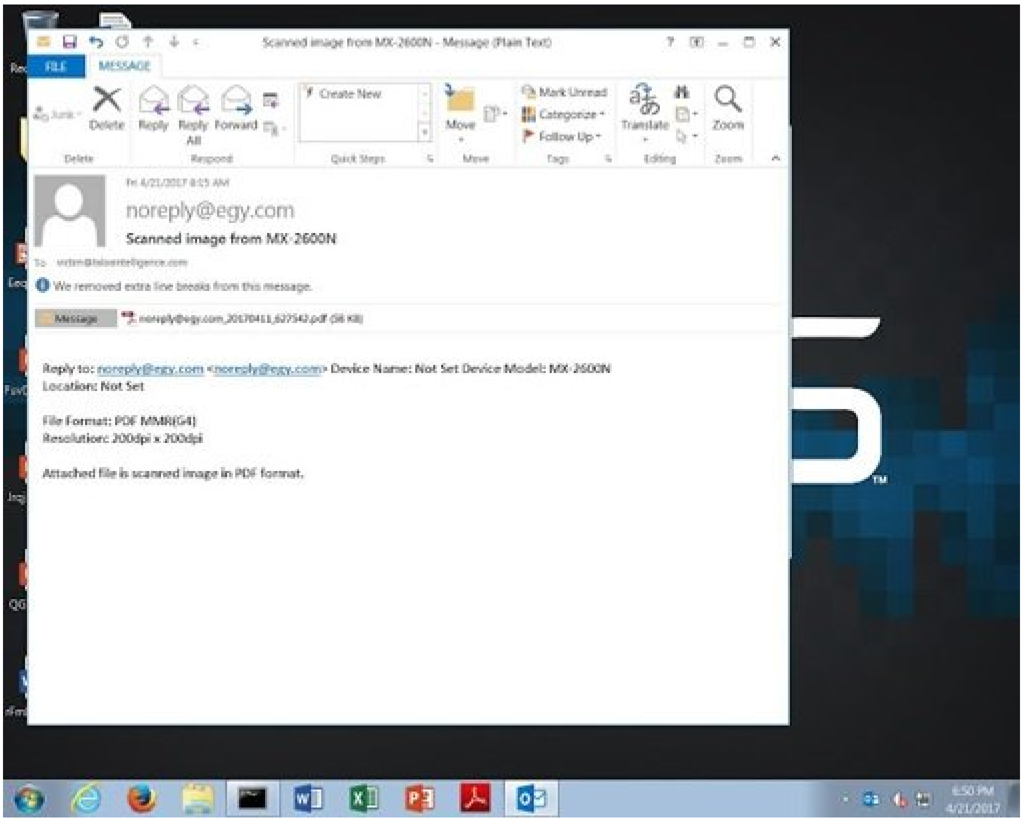
[illegible] SophosLab [illegible]. [illegible]. [illegible]: «[illegible] Necurs [illegible]. [illegible] 21 [illegible] 5 [illegible]. [illegible] Necurs [illegible].»



From donotreply@pibrands.co.uk
Subject **Receipt#272**
To victim@talosintelligence.com

1 attachment: P272.pdf 58.0 KB

[illegible]: «[illegible]. [illegible]. [illegible] pump-and-dump [illegible].» [illegible].



Scanned image from MX-2600N - Message (Plain Text)

Fri 4/21/2017 8:15 AM

noreply@egy.com

Scanned image from MX-2600N

We removed extra line breaks from this message.

noreply@egy.com_20170411_627542.pdf (58 KB)

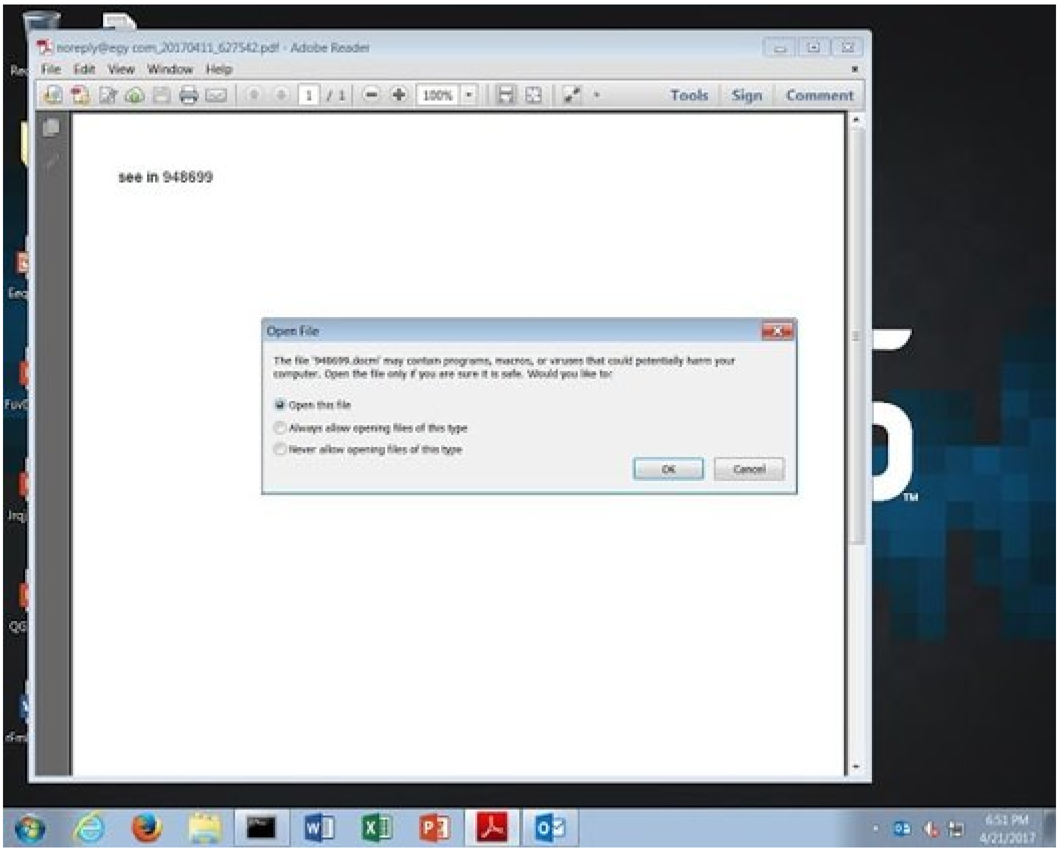
Reply to: noreply@egy.com <noreply@egy.com> Device Name: Not Set Device Model: MX-2600N
Location: Not Set

File Format: PDF MMR(G4)
Resolution: 200dpi x 200dpi

Attached file is scanned image in PDF format.

[illegible]

[illegible] « [illegible] : [illegible]
[illegible] 35 [illegible] . [illegible]
[illegible] . [illegible] «. [illegible]
[illegible] . [illegible]
[illegible] 'Receipt#272 [illegible]
. [illegible] P272.pdf [illegible] PDF [illegible] . [illegible]



see in 948699

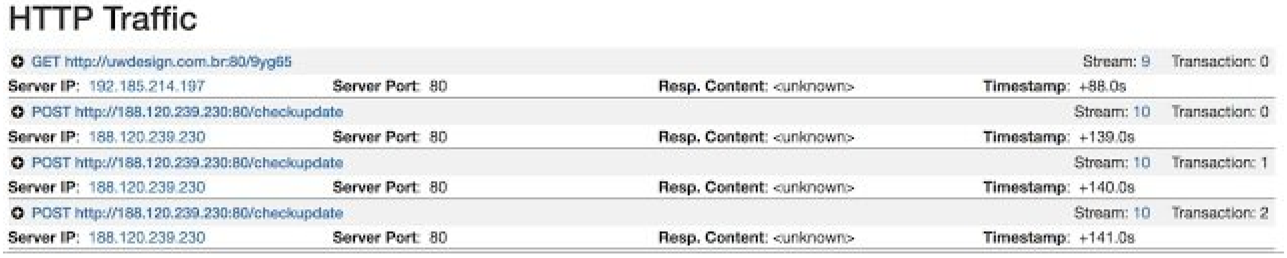
Open File

The file '948699.docm' may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to:

● Open this file
○ Always allow opening files of this type
○ Never allow opening files of this type

OK Cancel

[illegible] Dirdex [illegible] PDF [illegible] DOCM. [illegible].



HTTP Traffic

GET http://uwdesign.com.br:80/9yg65 Stream: 9 Transaction: 0
Server IP: 192.185.214.197 Server Port: 80 Resp. Content: <unknown> Timestamp: +88.0s
POST http://188.120.239.230:80/checkupdate Stream: 10 Transaction: 0
Server IP: 188.120.239.230 Server Port: 80 Resp. Content: <unknown> Timestamp: +139.0s
POST http://188.120.239.230:80/checkupdate Stream: 10 Transaction: 1
Server IP: 188.120.239.230 Server Port: 80 Resp. Content: <unknown> Timestamp: +140.0s
POST http://188.120.239.230:80/checkupdate Stream: 10 Transaction: 2
Server IP: 188.120.239.230 Server Port: 80 Resp. Content: <unknown> Timestamp: +141.0s

[illegible] «[illegible].»

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
10:40 - 12/02/1396

[illegible]:

[illegible] - [illegible] - Locky - [illegible] - Necurs - [illegible] - [illegible]

[illegible]

[illegible]: https://www.shabakeh-mag.com/security/7657/%DA%A9%D8%A7%D9%85%D9%84%D8%A7-%D8%A7%D8%AD%D8%AA%DB%8C%D8%A7%D8%B7-%DA%A9%D9%86%DB%8C%D8%AF%D8%9B-%D8%A8%D8%A7%D8%AC-%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-locky-%D8%AF%D9%88%D9%85%D8%B1%D8%AA%D8%A8%D9%87-%D9%81%D8%B9%D8%A7%D9%84-%D8%B4%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA