

Nos llega un mail un tanto sospechoso con fichero adjunto

Analizamos el correo en formato eml con la herramienta mailparser, obtenemos la información de la cabecera del correo:

```
# mailparser -r -o -f "Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg"
```

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -r -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA
NUMERO 3259.msg'
{
  "Date": "31 Aug 2022 09:40:42 +0200",
  "MIME-Version": "1.0",
  "Content-Type": "multipart/alternative; boundary=\"17165454650.3643da9.1795\"",
  "Content-Transfer-Encoding": "7bit",
  "Subject": "Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL\n SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259",
  "From": "NO-REPLY.JDEcoffee@gpsema.ihost.com",
  "To": "remnux@remnux.com",
  "Message-Id": "<OFBE488E3F.03CFDB67-0N002588AF.002A2DCE@gpsema.ihost.com>",
  "Return-Path": "<NO-REPLY.JDEcoffee@gpsema.ihost.com>",
  "X-Spam-Checker-Version": "SpamAssassin 3.3.1 (2010-03-16) on\n s17583606.onlinehome-server.info",
  "X-Spam-Level": "**",
  "X-Spam-Status": "No, score=1.8 required=7.0 tests=DEAR_SOMETHING,HTML_MESSAGE,\n MIME_HTML_ONLY,SPF_PASS,T_SCC_BODY_TEXT_LINE,URIBL_BLOCKED a
utolearn=no\n version=3.3.1",
  "X-Spam-ASN": "AS36351 169.54.128.0/19",
  "X-Original-To": "remnux@remnux.com",
  "Delivered-To": "remnux@remnux.com",
  "Received": "from plkraping07p1 ([10.48.106.253]) by krdominop1.emea.ibm.net\n (IBM Domino Release 10.0.1FP6) with ESMTP id 2022083107404237-8
26936 ; Wed, 31 Aug 2022 07:40:42 +0000",
  "X-MIMETrack": "Itemize by SMTP Server on plkrmail23p1/SVR/PROD/GPSEMEA(Release\n 10.0.1FP6)September 24, 2020) at 08/31/2022 07:40:42 AM, Ser
ialize by Router\n on plkrmail23p1/SVR/PROD/GPSEMEA(Release 10.0.1FP6)September 24, 2020) at\n 08/31/2022 07:40:44 AM, Serialize complete at 08/
31/2022 07:40:44 AM",
  "X-TNEFEvaluated": "1",
  "X-Proofpoint-GUID": "FmSG0LLAHcoTtKgms1_lgSoAu1EZ4ft1",
  "X-Proofpoint-ORIG-GUID": "FmSG0LLAHcoTtKgms1_lgSoAu1EZ4ft1"
}
```

Leemos el cuerpo del mensaje

```
# mailparser -b -o -f "Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg"
```

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -b -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merch
anservis Canarias S.L. NUMERO 3259.msg'
- Automatically generated e-mail. Please DO NOT respond! -

Dear Sir, Madam,

Thank you for your email, we will process it as soon as possible.

Did you know, JDE mandates e-invoicing per January 1st 2020, and is connected with Tradeshift and Basware, being our e-invoicing platforms.

The usage of these platforms is for free, and as easy to use as the PDF e-mail you are sending today.

To connect with Tradeshift, an invite is sent by Tradeshift once you've onboarded to JDE's Supplier base. In case you did not yet receive an act
ivation link, please request one at: https://jde.support.tradeshift.com/. Until you are actively submitting invoices through Tradeshift, you can
still use the email box. However, we inspire you to start using Tradeshift today!

If you are a supplier to one of the "Basware" countries, you will find the proper email box on our purchase orders (pdf form).

Please keep in mind following considerations when using our current e-mail box:

* Please be aware E-invoice@JDEcoffee.com<mailto:E-invoice@JDEcoffee.com> is a fully automated mailbox, messages in the email body will NOT
be read.
* Please submit your invoices in PDF-format to E-invoice@JDEcoffee.com<mailto:E-invoice@JDEcoffee.com> (each invoice should be submitted in
a separate PDF-file).
* Invoices sent in any other file type (such as .xlsx, .docx, .zip, .msg, .jpeg, .html etc) will NOT be processed.
* If your invoice has an appendix (e.g. a delivery note), then please include the invoice + appendix in the same PDF-file.
* Emails containing a digital signature will NOT be processed.
* The total size of your email to E-invoice@JDEcoffee.com<mailto:E-invoice@JDEcoffee.com> should not exceed 9MB.
* For Payment Reminders, Statements of Account and invoice-related queries please contact GTC.FrontOffice@JDEcoffee.com<mailto:GTC.FrontOffi
ce@JDEcoffee.com>.
* For Remittance Advises (Payment Specifications) of our payments (to you) please contact GTC.CashManagement@JDEcoffee.com<mailto:GTC.CashMa
nagement@JDEcoffee.com>.
```

Leemos el destinatario del correo

```
# mailparser -t -o -f "Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg"
```

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -t -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merch
anservis Canarias S.L. NUMERO 3259.msg'
[["", "webmaster@remnux.com"]]
```

Leemos el remitente del correo

```
# mailparser -m -o -f "Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL
SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg"
```

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -m -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merch
anservis Canarias S.L. NUMERO 3259.msg'
[["", "NO-REPLY.JDEcoffee@gpsema.ihost.com"]]
```

Vemos el asunto del correo

```
# mailparser -u -o -f "Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL
SUBJECT- FACTURA XXXXXXXX S.L. NUMERO 3259.msg"
```

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -u -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merch
anservis Canarias S.L. NUMERO 3259.msg'
Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL
SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259
```

Exportamos todos los ficheros adjuntos en el correo

```
# mailparser -sa -ap ./ -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL
SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259.msg'
```

```
remnux@remnux:~/Documents/e-mail/005$ mailparser -sa -ap ./ -o -f 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTU
RA Merchanservis Canarias S.L. NUMERO 3259.msg'
remnux@remnux:~/Documents/e-mail/005$ ls -al
total 72
drwxrwxr-x 2 remnux remnux 4096 may 24 07:15 .
drwxrwxr-x 7 remnux remnux 4096 may 24 06:07 ..
-rw-rw-r-- 1 remnux remnux 10853 may 24 07:15 eozoaxvyza.rtf
-rwxrwxrwx 1 remnux remnux 53248 may 21 02:48 'Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merchanservis Can
arias S.L. NUMERO 3259.msg'
```

Vemos que se ha generado un document en formato rtf

Analizamos el tipo de fichero

```
# file eozoaxvyza.rtf
```

```
remnux@remnux:~/Documents/e-mail/005$ file eozoaxvyza.rtf
eozoaxvyza.rtf: Rich Text Format data, version 1, ANSI
```

Analizamos el fichero por si tiene algún documento incrustado

```
# rtfobj eozoaxvyza.rtf
```

```
remnux@remnux:~/Documents/e-mail/005$ rtfobj eozoaxvyza.rtf
rtfobj 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

=====
File: 'eozoaxvyza.rtf' - size: 10853 bytes
---+-----+-----
id |index      |OLE Object
---+-----+-----
```

No contiene ningún objeto incrustado malicioso

Mostramos el contenido del fichero rtf

```
# rtfDump.py -s 1 eozoaxvyza.rtf
```

```
remnux@remnux:~/Documents/e-mail/005$ rtfDump.py -s 1 eozoaxvyza.rtf | more
00000000: 5C 61 6E 73 69 5C 66 62 69 64 69 73 5C 61 6E 73 \ansi\fbidis\ans
00000010: 69 63 70 67 31 32 35 32 5C 64 65 66 66 30 5C 66 icpgl252\deff0\f
00000020: 72 6F 6D 68 74 6D 6C 31 7B 5C 66 6F 6E 74 74 62 romhtml1{\fonttb
00000030: 6C 7B 5C 66 30 5C 66 73 77 69 73 73 5C 66 63 68 l{\f0\fswiss\fch
00000040: 61 72 73 65 74 30 20 54 69 6D 65 73 20 4E 65 77 arset0 Times New
00000050: 20 52 6F 6D 61 6E 3B 7D 7B 5C 66 31 5C 66 73 77 Roman;}{\f1\fsw
00000060: 69 73 73 5C 66 63 68 61 72 73 65 74 32 20 53 79 iss\fccharset2 Sy
00000070: 6D 62 6F 6C 3B 7D 7D 0A 0D 7B 5C 63 6F 6C 6F 72 mbol;}}..\{color
00000080: 74 62 6C 3B 5C 72 65 64 31 39 32 5C 67 72 65 65 tbl;\red192\gree
00000090: 6E 31 39 32 5C 62 6C 75 65 31 39 32 3B 5C 72 65 n192\blue192\re
000000A0: 64 30 5C 67 72 65 65 6E 30 5C 62 6C 75 65 32 35 d0\green0\blue25
000000B0: 35 3B 7D 0A 0D 7B 5C 2A 5C 67 65 6E 65 72 61 74 5;}}..\{*\generat
000000C0: 6F 72 20 4D 69 63 72 6F 73 6F 66 74 20 45 78 63 or Microsoft Exc
000000D0: 68 61 6E 67 65 20 53 65 72 76 65 72 3B 7D 0A 0D hange Server;}}..
000000E0: 7B 5C 2A 5C 66 6F 72 6D 61 74 43 6F 6E 76 65 72 {\*\formatConver
000000F0: 74 65 72 20 63 6F 6E 76 65 72 74 65 64 20 66 72 ter converted fr
00000100: 6F 6D 20 68 74 6D 6C 3B 7D 0A 0D 5C 76 69 65 77 om html;}}..\view
00000110: 6B 69 6E 64 35 5C 76 69 65 77 73 63 61 6C 65 31 kind5\viewscale1
00000120: 30 30 0A 0D 5C 68 74 6D 6C 72 74 66 7B 5C 2A 5C 00..\htmlrtf{\*\
00000130: 62 6B 6D 6B 73 74 61 72 74 20 42 4D 5F 42 45 47 bkmkstart BM_BEG
00000140: 49 4E 7D 5C 68 74 6D 6C 72 74 66 30 7B 5C 2A 5C IN}\htmlrtf0{\*\
00000150: 68 74 6D 6C 74 61 67 36 34 7D 7B 5C 2A 5C 68 74 htmltag64}{\*\ht
00000160: 6D 6C 74 61 67 30 20 3C 68 74 6D 6C 3E 3C 68 65 mltag0 <html><he
00000170: 61 64 3E 3C 6D 65 74 61 20 68 74 74 70 2D 65 71 ad><meta http-eq
00000180: 75 69 76 3D 22 43 6F 6E 74 65 6E 74 2D 54 79 70 uiv="Content-Typ
00000190: 65 22 20 63 6F 6E 74 65 6E 74 3D 22 74 65 78 74 e" content="text
000001A0: 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74 3D 75 /html; charset=u
000001B0: 74 66 2D 38 22 3E 3C 2F 48 65 61 64 3E 3C 62 6F tf-8"></Head><bo
000001C0: 64 79 3E 3C 70 3E 7D 7B 5C 2A 5C 68 74 6D 6C 74 dy><p>}{\*\htmlt
000001D0: 61 67 30 20 3C 62 3E 7D 5C 70 61 72 64 0A 0D 5C ag0 <b>}\pard..\
000001E0: 70 6C 61 69 6E 5C 66 30 5C 68 74 6D 6C 72 74 66 plain\f0\htmlrtf
000001F0: 7B 5C 62 5C 68 74 6D 6C 72 74 66 30 20 2D 20 41 {\b\htmlrtf0 - A
00000200: 75 74 6F 6D 61 74 69 63 61 6C 6C 79 20 67 65 6E utomatically gen
00000210: 65 72 61 74 65 64 20 65 2D 6D 61 69 6C 2E 20 50 erated e-mail. P
```

Abrimos el fichero con un visor de texto

```

eozoaxvyza.rtf - SciTE
File Edit Search View Tools Options Language Buffers Help

1 eozoaxvyza.rtf
{\rtf1\ansi\fbidis\ansicpg1252\deff0\fromhtml1{\fonttbl{\f0\fswiss\fcharset0 Times New Roman;}{\f1\fswiss\fcharset2 Symbol;}}
{\colortbl;\red192\green192\blue192;\red0\green0\blue255;}
{\*\generator Microsoft Exchange Server;}
{\*\formatConverter converted from html;}
\viewkind5\viewscale100
\htmlrtf{\*\bkmkstart BM BEGIN}\htmlrtf0{\*\htmltag64}{\*\htmltag0 <html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><
\plainf0\htmlrtf{\b\htmlrtf0 - Automatically generated e-mail. Please {\*\htmltag0 <u>}\htmlrtf{\b\ul\htmlrtf0 DO NOT{\*\htmltag0 </U>}\htmlrtf
}{\b\htmlrtf0 respond! \96 {\*\htmltag0 </B>}\htmlrtf}\htmlrtf0{\*\htmltag0 </P>}\htmlrtf\par
\htmlrtf0{\*\htmltag0 <p>}\pard\sb280\plainf0\htmlrtf{\htmlrtf0 Dear Sir, Madam,{\*\htmltag0 </P>}\htmlrtf}\htmlrtf0{\*\htmltag0 }\htmlrtf
\par
\htmlrtf0{\*\htmltag0 <p style="margin: 1px 1px 1px 1px;">}\pard\li12\ri12\sb280\plainf0\htmlrtf{\htmlrtf0 Thank you for your email, we will process it as soon
}\htmlrtf0{\*\htmltag0 }\htmlrtf\par
\htmlrtf0{\*\htmltag0 <p style="margin: 1px 1px 1px 1px;">}\pard\li12\ri12\sb12\plainf0\htmlrtf{\htmlrtf0 Did you know, JDE mandates e-invoicing per January
}\htmlrtf0{\*\htmltag0 }\htmlrtf\par
\htmlrtf0{\*\htmltag0 <p style="margin: 1px 1px 1px 1px;">}\pard\li12\ri12\sb12\plainf0\htmlrtf{\htmlrtf0 The usage of these platforms {\*\htmltag0 <u>}\ht
}{\ul\htmlrtf0 is for free{\*\htmltag0 </U>}\htmlrtf}{\htmlrtf0 , and as easy to use as the PDF e-mail you are sending today.{\*\htmltag0 </P>}\htmlrtf
}\htmlrtf0{\*\htmltag0 }\htmlrtf\par
\htmlrtf0{\*\htmltag0 <p>}\pard\sb280\plainf0\htmlrtf{\htmlrtf0 To connect with Tradeshift, an invite is sent by Tradeshift once you've onboarded to JDE\92
}{\field{\*\fidinst HYPERLINK "https://jde.support.tradeshift.com/"}{\fldrslt{\cf2\ul\htmlrtf0 https://jde.support.tradeshift.com/{\*\htmltag0 </A>}\htmlrtf
}}}\htmlrtf0 . Until you are actively submitting invoices through Tradeshift, you can still use the email box. However, we inspire you to start using Tradeshift tod
}\htmlrtf0{\*\htmltag0 }\htmlrtf\par
\htmlrtf0{\*\htmltag0 <p>}\pard\sb280\plainf0\htmlrtf{\htmlrtf0 If you are a supplier to one of the \93Basware\94 countries, you will find the proper email box
}\htmlrtf0{\*\htmltag0 }\htmlrtf\par

```

Software:

Remmex

Aplicación:

emlAnalyzer

Mailparser

Rtfdump

Rtfobj

Fuente:

Thank you for your email to E-invoice@JDEcoffee.com - ORIGINAL SUBJECT- FACTURA Merchanservis Canarias S.L. NUMERO 3259.zip