

## **Documentación Técnica**

### **Envío de muestras de SPAM a TrendMicro.**

VERSIÓN  
**1.0**

DIRIGIDO A

---

**DIPUTACIÓN PROVINCIAL DE TERUEL – USUARIOS DE SERVICIOS TIC**

## Datos de Control

**Proyecto:** Sistemas  
**Entidad de destino:** Uso Interno  
**Título:** Envío de muestras de SPAM a TrendMicro  
**Referencia oferta:** Sin Ref.  
**Versión:** 1.0  
**Fecha edición:** 25/06/2010  
**Fichero:** Envio\_SPAM\_TrendMicro.doc  
**Autor(es):** José Antonio Magallón Civera

## Control de firmas

**Autor**

**Revisado**



**Firma**  
**Nombre**  
**Cargo**  
**Entidad**  
**Fecha**

José Antonio Magallón Civera  
 Ing. Técnico Telecomunicaciones  
 Diputación Provincial de Teruel  
 25/06/2010

**Firma**  
**Nombre**  
**Cargo**  
**Entidad**  
**Fecha**

DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>	Envío de muestras de SPAM a TrendMicro	
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 2 de 14

## Control de modificaciones por cambio de versión

<i>Versión</i>	<i>Autor</i>	<i>Descripción</i>	<i>Fecha</i>
1	J.A. Magallón	Documentación Técnica	25/06/2010

## Declaración de confidencialidad

La presente documentación es propiedad de Diputación Provincial de Teruel, tiene carácter confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de Diputación Provincial de Teruel, titular del Copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a la ley.

DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>	Envío de muestras de SPAM a TrendMicro	
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 3 de 14

## Índice

1) Objetivo .....	5
2) Ámbito de aplicación .....	5
3) Procedimiento. ....	5
3.1. Captura de correos .....	6
3.2. Compresión de archivos.....	11
3.3. Envío a TrendMicro .....	14

DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 4 de 14

## 1) **Objetivo**

Es objeto de este informe describir la forma de enviar una muestra de spam a TrendMicro. Cubre tanto el envío de falsos positivos (correo legítimo detectado como spam) como el de falsos negativos (spam no detectado).

## 2) **Ámbito de aplicación**

Este documento está dirigido a todos los usuarios de servicios TIC de la Diputación Provincial de Teruel como documento interno de consulta técnica.

## 3) **Procedimiento.**

Cuando a nuestro buzón de correo entra algún mensaje que puede ser considerado como correo no deseado (o SPAM) y que los filtros antispam no han detectado como tal, debemos realizar los pasos que se detallan a continuación con el objeto de proporcionar información al prestador del servicio para que actualice sus bases de datos de SPAM.

Hay que tener en cuenta que:

- La muestra de SPAM debe estar en formato “.msg” o “..eml”.
- La muestra de SPAM debe provenir del correo original, no de correos reenviados, ya que en el reenvío se pierde la información de las cabeceras del mensaje.

El procedimiento resumido para envío de correos es:

1. Meter los correos en una carpeta, en formato .eml o .msg
2. Comprimir los ficheros en un fichero .zip, protegido por contraseña, usando como password “**novirus**”<sup>1</sup>
3. Crear un correo y adjuntar el fichero .zip  
Enviar el mensaje a :

- [Spam@support.trendmicro.com](mailto:Spam@support.trendmicro.com)  
→ Para falsos negativos (spam no detectado).
- [False@support.trendmicro.com](mailto:False@support.trendmicro.com)  
→ Para falsos positivos (correo legítimo detectado como spam)

<sup>1</sup> Sin las comillas

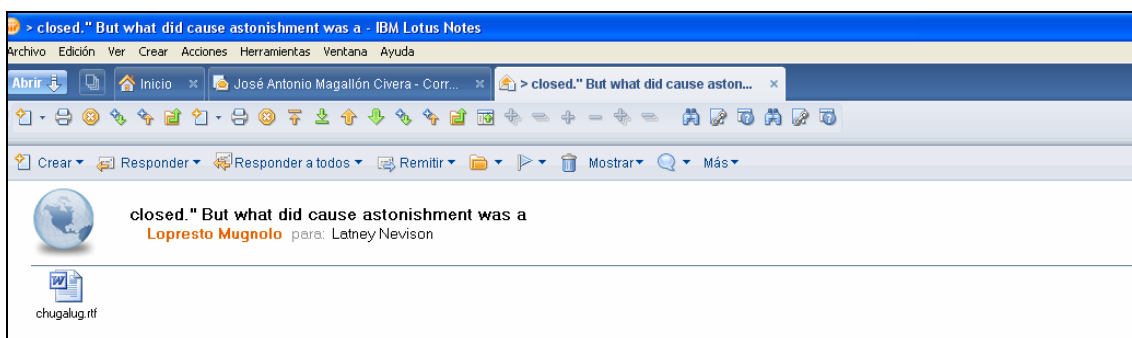
DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>	Envío de muestras de SPAM a TrendMicro	
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 5 de 14

### 3.1. Captura de correos

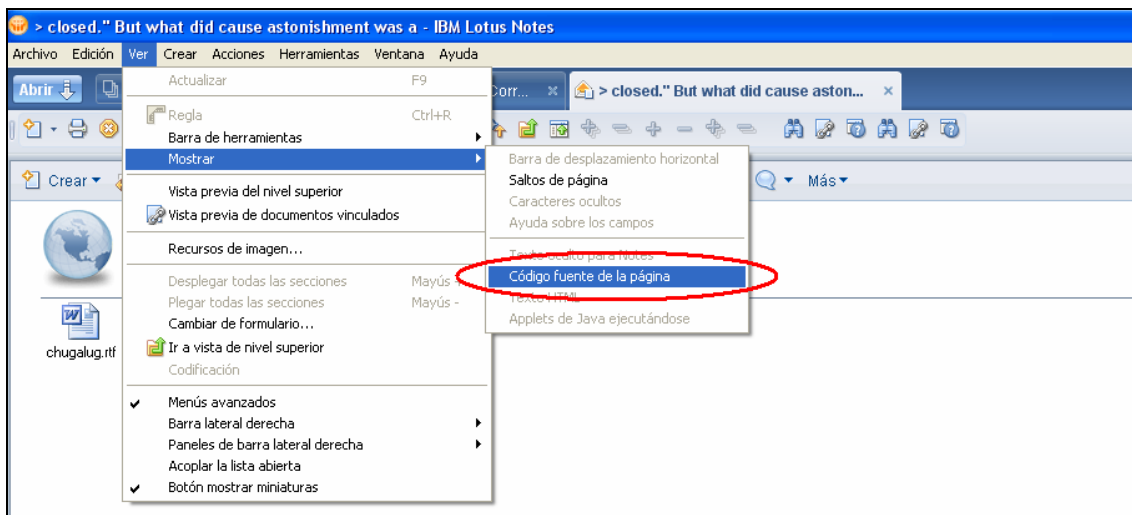
1) Seleccionamos el correo que clasificamos como SPAM



2) Abrimos el correo

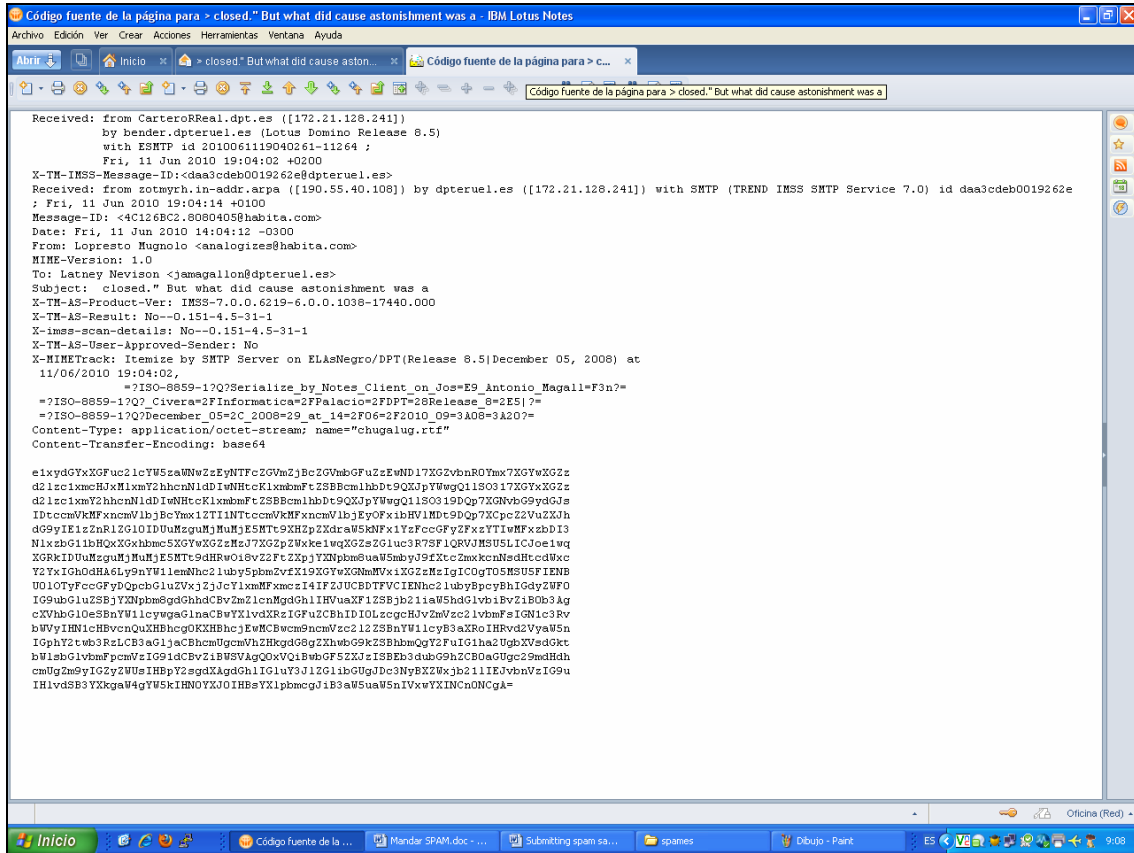


3) Seleccionamos el menú **Ver** → **Mostrar** → **Código fuente de la página**:



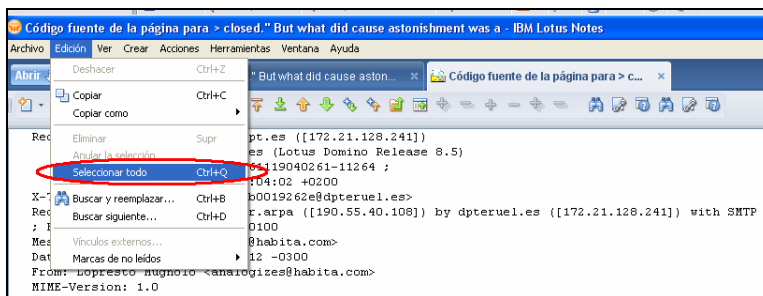
Nos aparecerá algo como:

DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 6 de 14



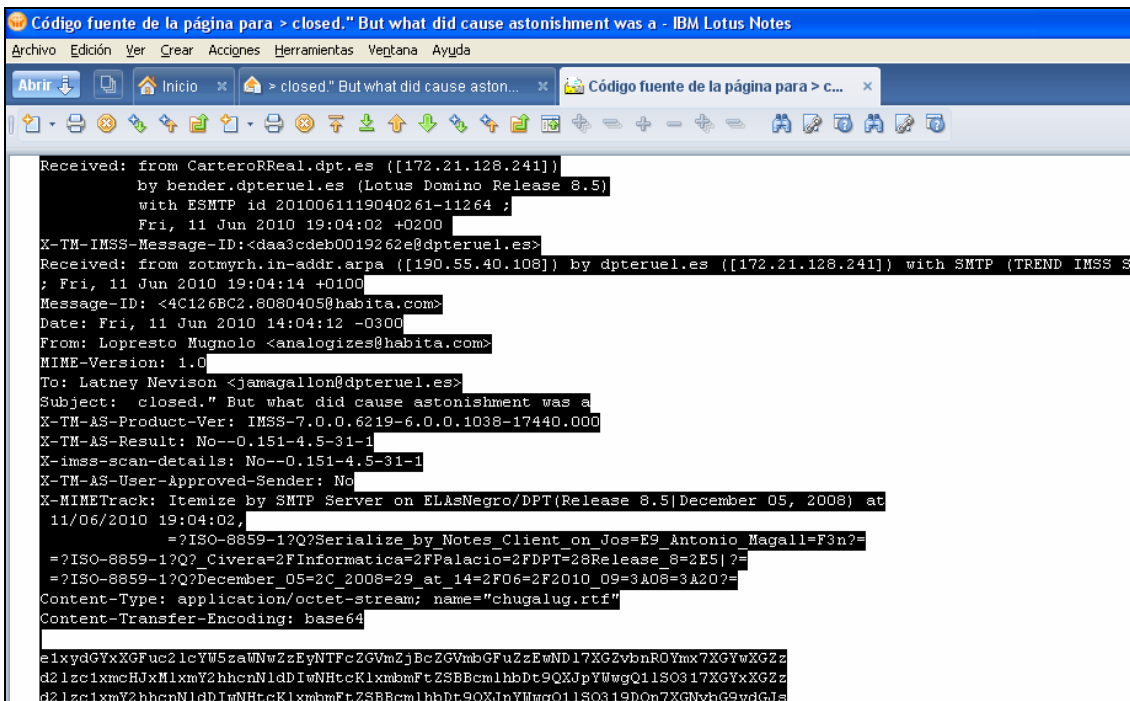
- 4) El contenido de esa ventana es lo que hay que guardar en un archivo en formato “.msg” o “.eml”.

Para ello, seleccionamos el menú Edición → Seleccionar todo:



Cuyo resultado es:

DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 7 de 14

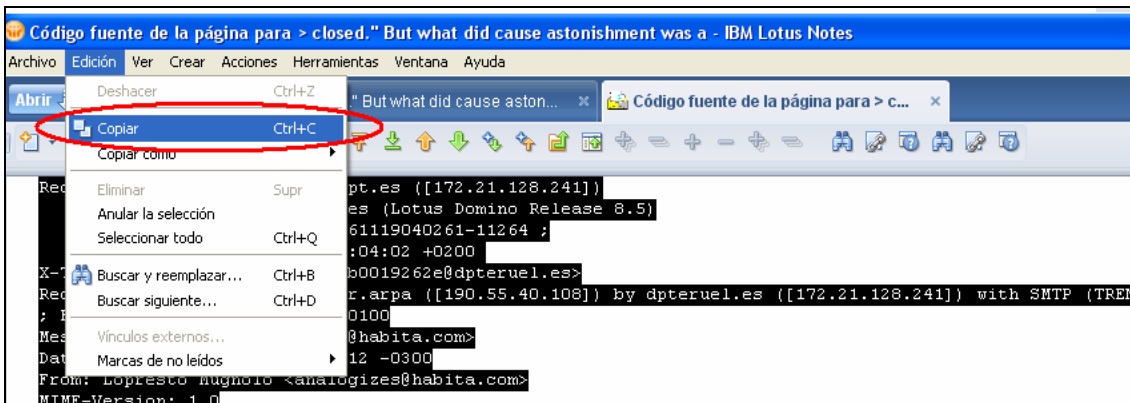


```

Código fuente de la página para > closed." But what did cause astonishment was a - IBM Lotus Notes
Archivo Edición Ver Crear Acciones Herramientas Ventana Ayuda
Abrir Inicio > closed." But what did cause aston... Código fuente de la página para > c...
Received: from CarteroRReal.dpt.es ([172.21.128.241])
  by bender.dpteruel.es (Lotus Domino Release 8.5)
  with ESMTMP id 2010061119040261-11264 ;
  Fri, 11 Jun 2010 19:04:02 +0200
X-TM-IMSS-Message-ID: <daa3cdeb0019262e@dpteruel.es>
Received: from zotmyrh.in-addr.arpa ([190.55.40.108]) by dpteruel.es ([172.21.128.241]) with SMTP (TREND IMSS SP
; Fri, 11 Jun 2010 19:04:14 +0100
Message-ID: <4C126BC2.8080405@habita.com>
Date: Fri, 11 Jun 2010 14:04:12 -0300
From: Lopresto Mugnolo <analogizes@habita.com>
MIME-Version: 1.0
To: Latney Nevison <jamagallon@dpteruel.es>
Subject: closed." But what did cause astonishment was a
X-TM-AS-Product-Ver: IMSS-7.0.0.6219-6.0.0.1038-17440.000
X-TM-AS-Result: No--0.151-4.5-31-1
X-ims-scan-details: No--0.151-4.5-31-1
X-TM-AS-User-Approved-Sender: No
X-MIMETrack: Itemize by SMTP Server on ELAsNegro/DPT(Release 8.5|December 05, 2008) at
11/06/2010 19:04:02,
  =?ISO-8859-1?Q?Serialize by Notes_Client on Jos=E9 Antonio Magall=F3n?F
  =?ISO-8859-1?Q?Civera=2FInformativa=2FPalacio=2FDPT=28Release_8=2E5|?F
  =?ISO-8859-1?Q?December_05=2C_2008=29_at_14=2F06=2F2010_09=3A06=3A20?F=
Content-Type: application/octet-stream; name="chugalug.rtf"
Content-Transfer-Encoding: base64

elxydGYxXGFuc2lcYW5zaWwZzE5NTFfc2VmbGZjBc2GVmbGFuZzEwND17XGZvbnoR0Ymx7XGYwXGZz
d2lze1xmcHJxMlxmY2hhcnNldDlWnHtcKlxbmFtZSBBCmlhbDt9QXJpYUwgQ11S0317XGYwXGZz
d2lze1xmcHJxMlxmY2hhcnNldDlWnHtcKlxbmFtZSBBCmlhbDt9QXJpYUwgQ11S0319DQp7XGNvbG9ydGJ5
  
```

5) Seleccionamos el menú **Edición** → **Copiar**:



```

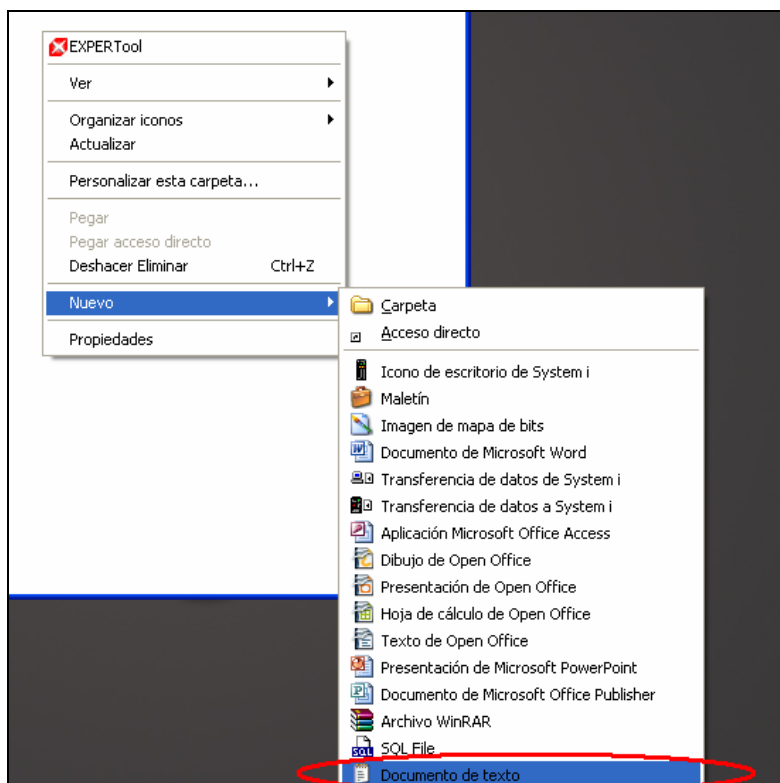
Código fuente de la página para > closed." But what did cause astonishment was a - IBM Lotus Notes
Archivo Edición Ver Crear Acciones Herramientas Ventana Ayuda
Abrir Deshacer Ctrl+Z " But what did cause aston... Código fuente de la página para > c...
Copiar Ctrl+C
Copiar como
Eliminar Supr
Anular la selección
Seleccionar todo Ctrl+Q
X-? Buscar y reemplazar... Ctrl+B
Buscar siguiente... Ctrl+D
Mes Vínculos externos...
Date Marcas de no leídos
MIME-Version: 1.0
  
```

Abrimos el “notepad” o el procesador de textos que estemos acostumbrados a usar (que no sea el Word o el swriter del OpenOffice)

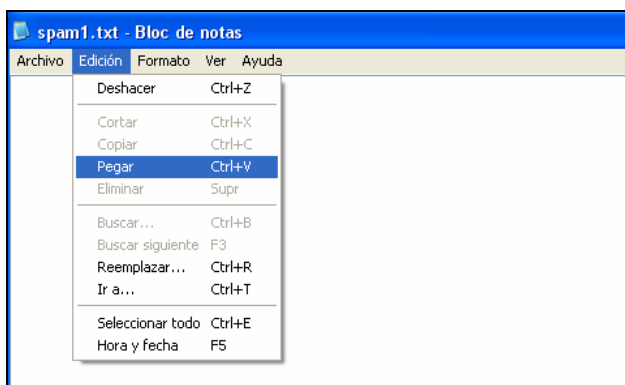
Por ejemplo, podemos crear un “nuevo documento de texto”, dentro de la carpeta donde queramos guardar el SPAM

DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 8 de 14



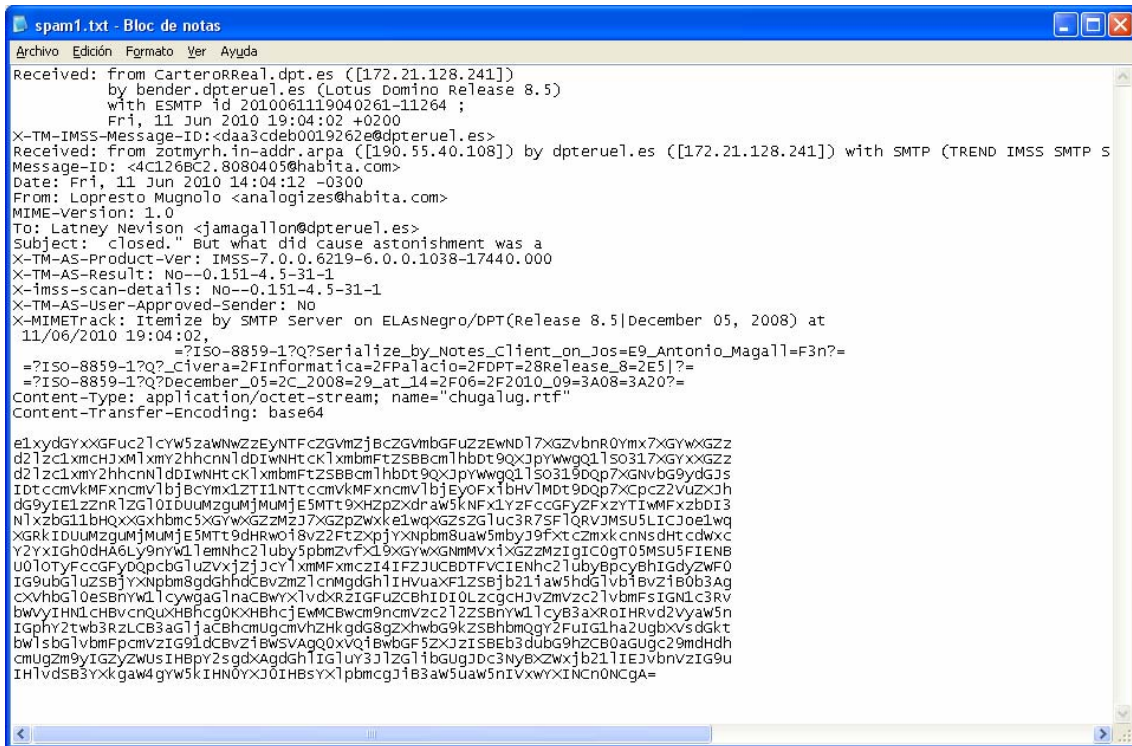


6) Una vez abierto, seleccionamos el menú **Edición** → **Pegar**:

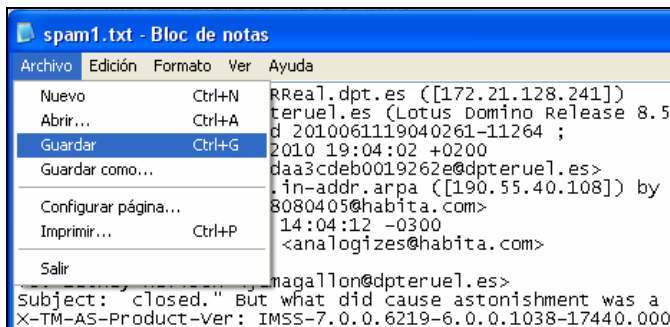


Esto pegará el código fuente del mensaje de spam, que habíamos seleccionado previamente, en el fichero abierto.

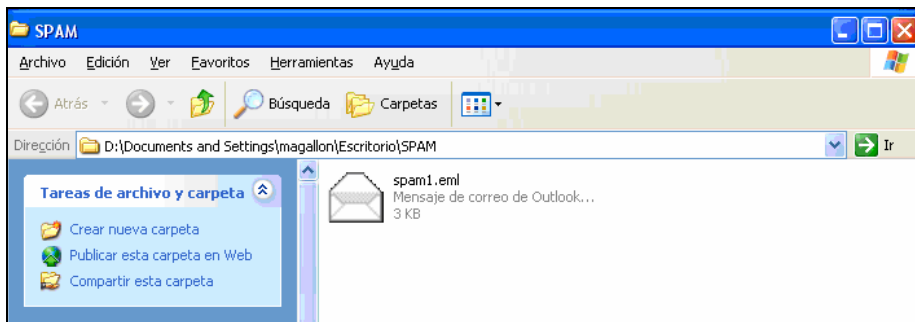
DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>	Envío de muestras de SPAM a TrendMicro	
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 9 de 14



7) Seleccionamos el menú **Archivo → Guardar:**



8) Ahora cambiaremos la extensión del fichero recién creado a .eml (o .msg)

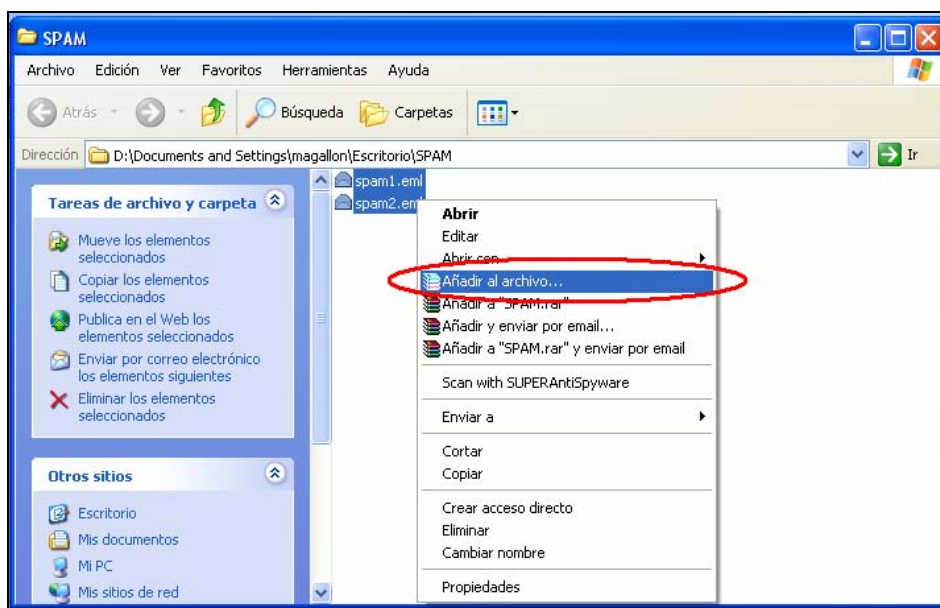


DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 10 de 14

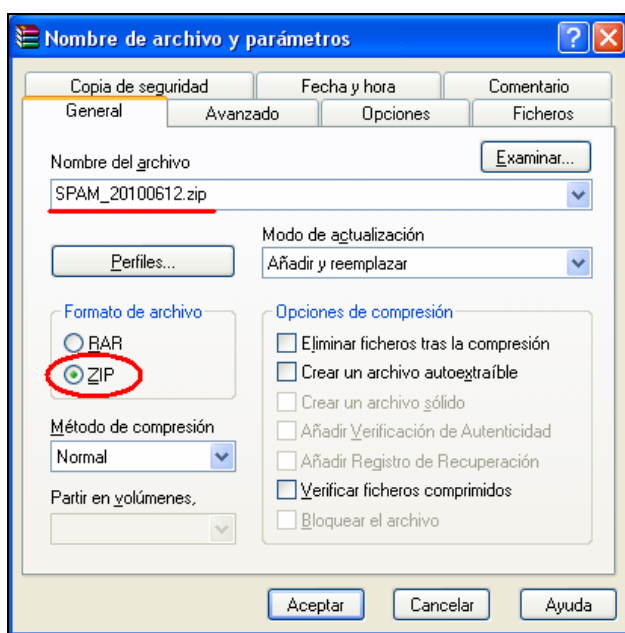
### 3.2. Compresión de archivos.

Una vez hayamos generado todos los ficheros .eml (o .msg) con el spam que nos haya entrado, deberemos comprimirlos en un fichero .zip, protegido por contraseña, usando como password “**novirus**”, sin las comillas.

- 1) Para ello, seleccionamos todos los ficheros a comprimir, pulsamos el botón derecho del ratón y seleccionamos “Añadir al archivo”



- 2) Esto nos abre el winrar, donde seleccionamos la compresión en formato ZIP:



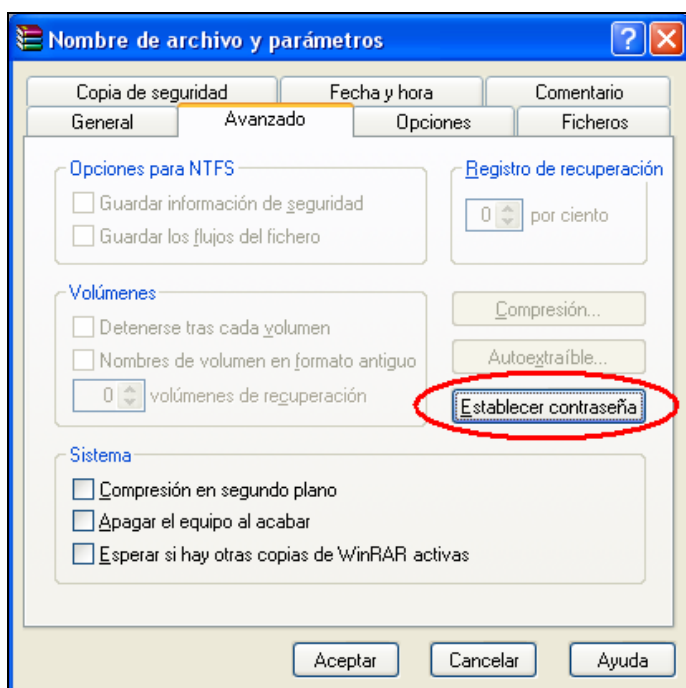
DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 11 de 14

Además de seleccionar el formato, le daremos un nombre al fichero, por ejemplo: SPAM\_AAAAMMDD.zip

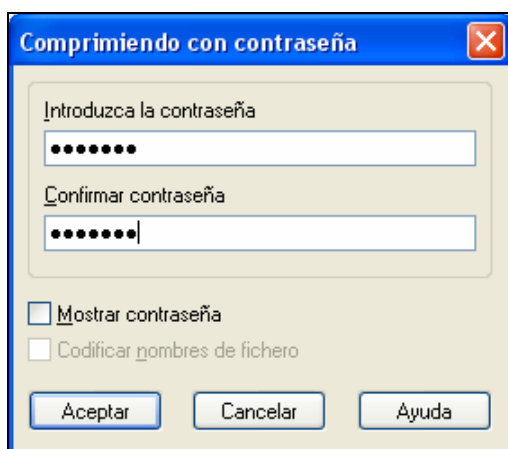
Con:

- AAAA= año [4 cifras]
- MM=Mes [2 cifras]
- DD=Día [2 cifras]

3) Una vez hecho esto, iremos a la pestaña “avanzado”, donde seleccionaremos “Establecer contraseña”

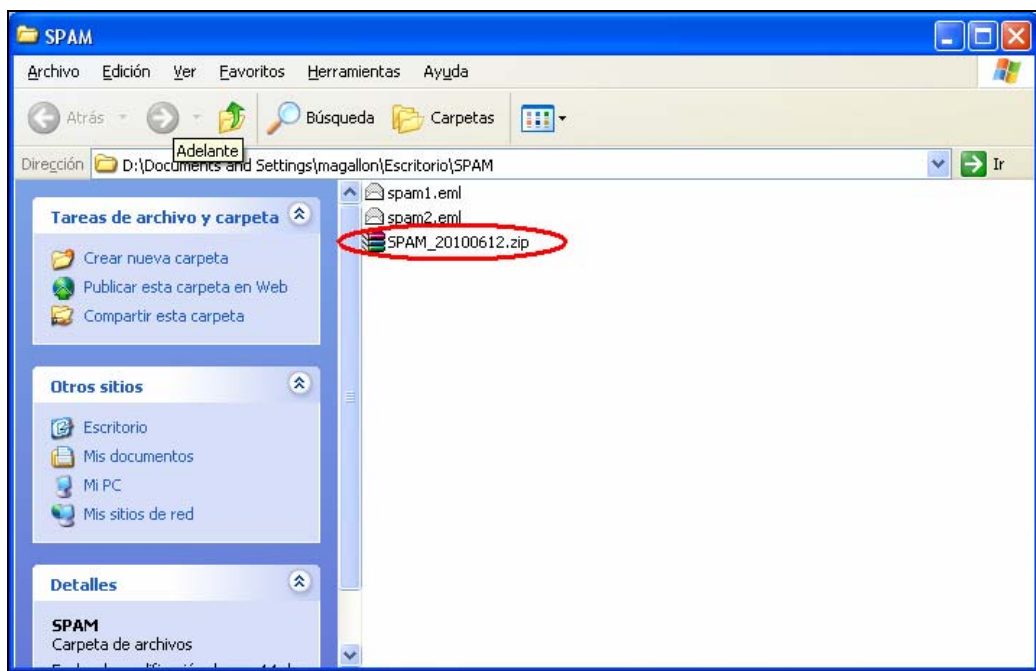


4) Establecemos la contraseña:



DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 12 de 14

Aceptamos y nos creará un fichero comprimido, en formato ZIP, con el nombre elegido, protegido con contraseña:



Este es el fichero que deberemos enviar a TrendMicro, de la forma que se describe a continuación

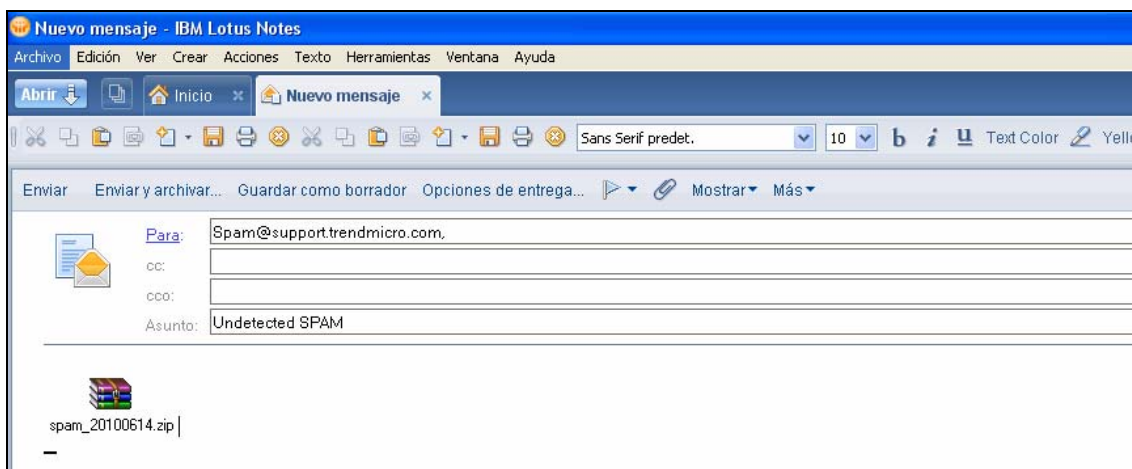
DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>		Envío de muestras de SPAM a TrendMicro
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 13 de 14

### 3.3. Envío de muestras de SPAM a TrendMicro

Con el fichero .zip generado anteriormente se manda el mensaje a:

- [Spam@support.trendmicro.com](mailto:Spam@support.trendmicro.com)  
→ Para falsos negativos (spam no detectado).
- [False@support.trendmicro.com](mailto:False@support.trendmicro.com)  
→ Para falsos positivos (correo legítimo detectado como spam)

Por ejemplo, si reportasemos un correo de spam que nos ha entrado a nuestro correo (falso negativo), enviaríamos el zip a [spam@support.trendmicro.com](mailto:spam@support.trendmicro.com), según imagen adjunta:



DOCUMENTACIÓN TÉCNICA		
<b>Título:</b>	Envío de muestras de SPAM a TrendMicro	
<b>Referencia:</b>	Sin Ref.	
<b>Modificación:</b>	25/06/2010 13:13	Página 14 de 14