

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		
Título:	Envío de muestras de SPAM a TrendMicro	
Referencia:	Sin Ref.	
Modificación:	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		
Título:	Envío de muestras de SPAM a TrendMicro	
Referencia:	Sin Ref.	
Modificación:	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		
Título:		Envío de muestras de SPAM a TrendMicro
Referencia:	Sin Ref.	
Modificación:	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**”¹
3. Crear un correo y adjuntar el fichero .zip
Enviar el mensaje a :

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

¹ Sin las comillas

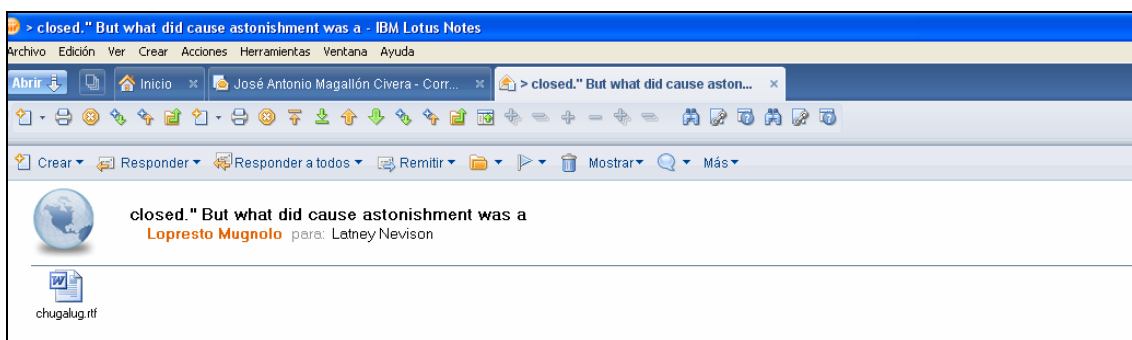
DOCUMENTACIÓN TÉCNICA		
Título:	Envío de muestras de SPAM a TrendMicro	
Referencia:	Sin Ref.	
Modificación:	25/06/2010 13:13	Página 5 de 14

3.1. Captura de correos

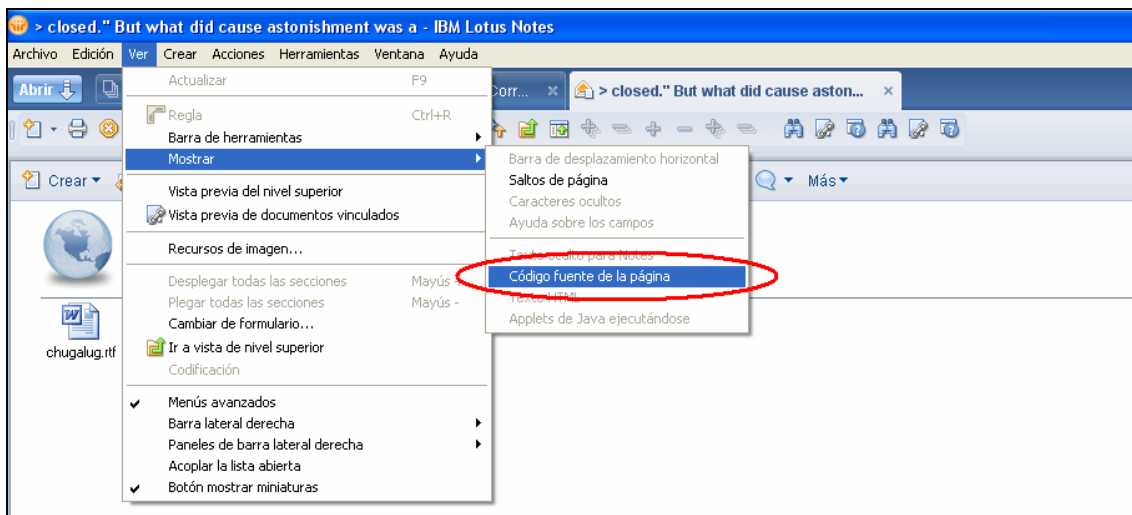
1) Seleccionamos el correo que clasificamos como SPAM



2) Abrimos el correo

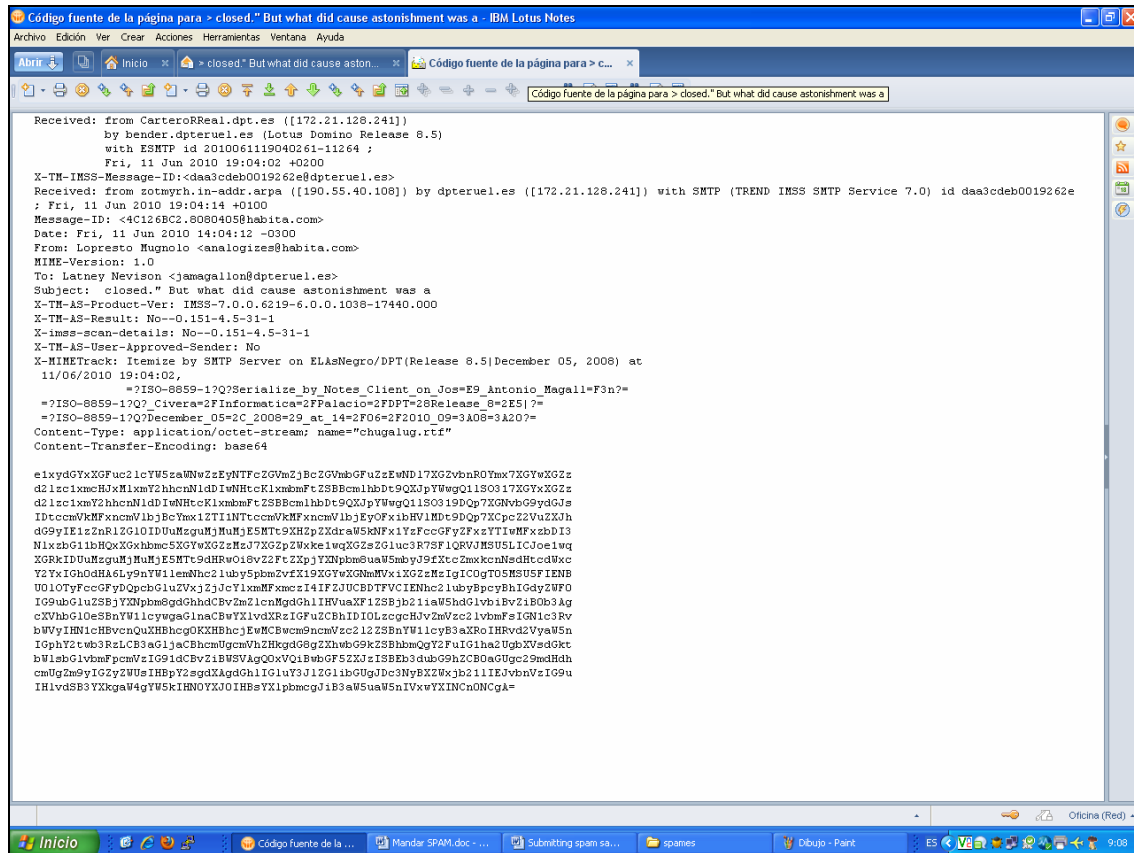


3) Seleccionamos el menú **Ver** → **Mostrar** → **Código fuente de la página**:



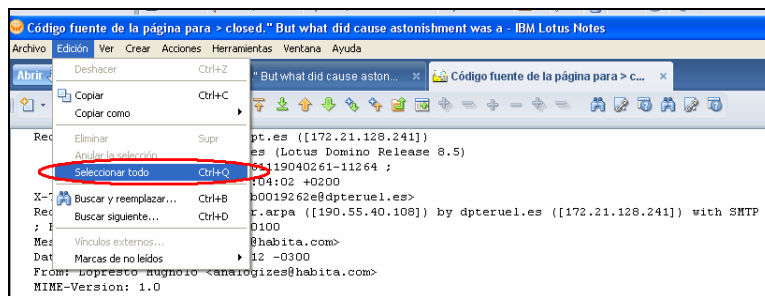
Nos aparecerá algo como:

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



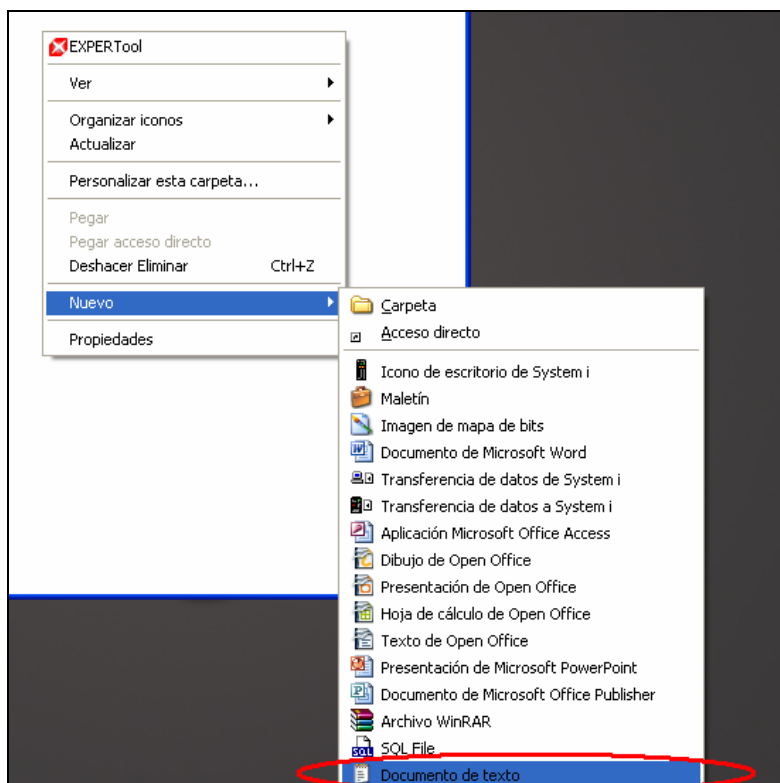
- 4) El contenido de esa ventana es lo que hay que guardar en un archivo en formato “.msg” o “.eml”.

Para ello, seleccionamos el menú Edición → Seleccionar todo:

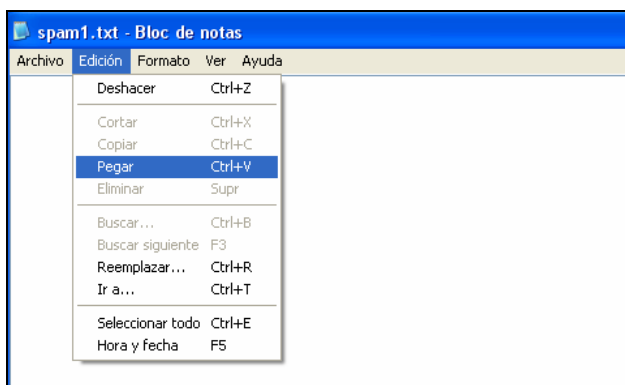


Cuyo resultado es:

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

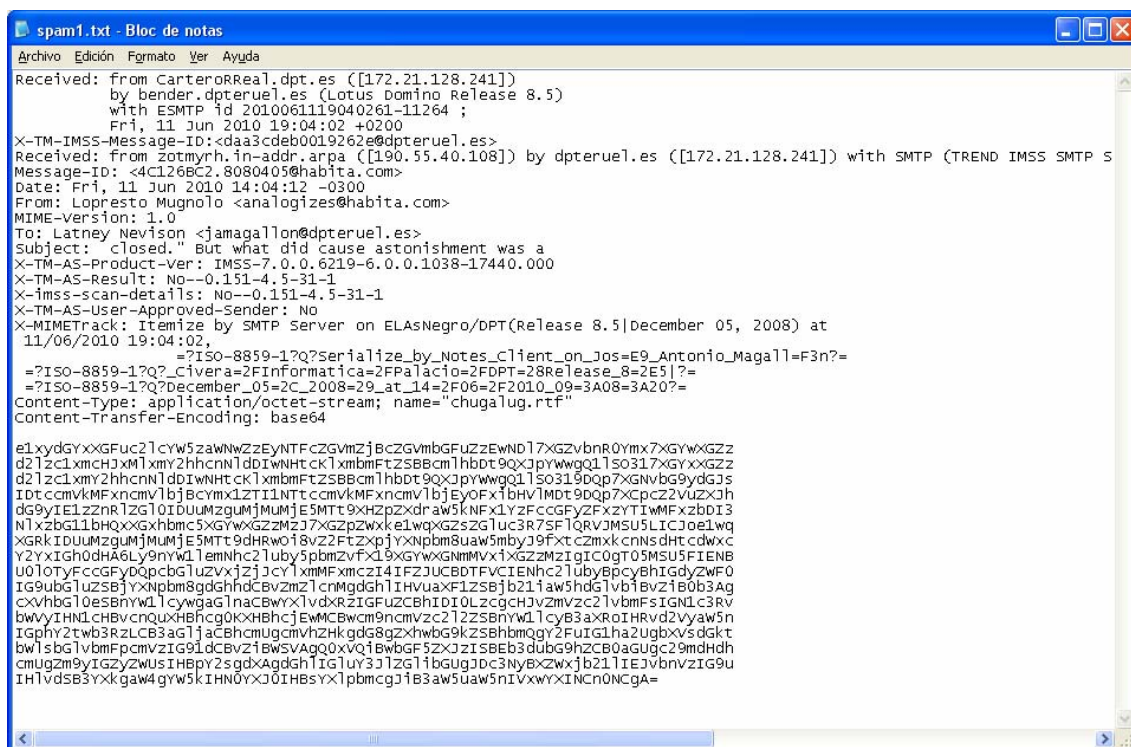


6) Una vez abierto, seleccionamos el menú **Edición** → **Pegar**:

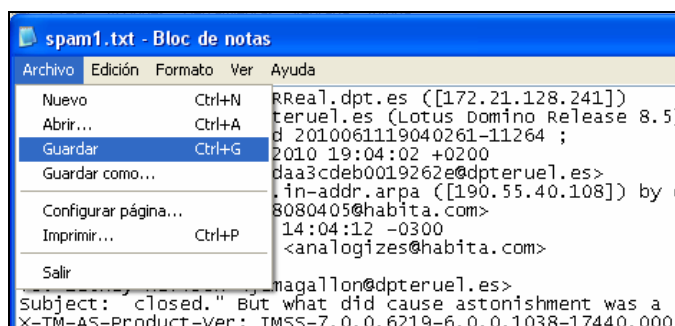


Esto pegará el código fuente del mensaje de spam, que habíamos seleccionado previamente, en el fichero abierto.

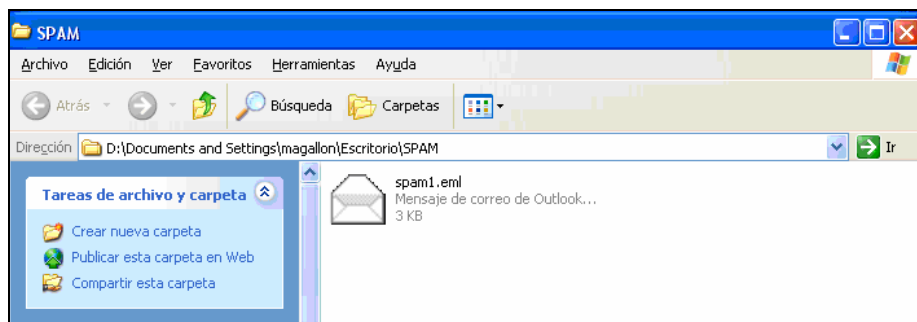
DOCUMENTACIÓN TÉCNICA		
Título:		Envío de muestras de SPAM a TrendMicro
Referencia:	Sin Ref.	
Modificación:	25/06/2010 13:13	Página 9 de 14



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



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

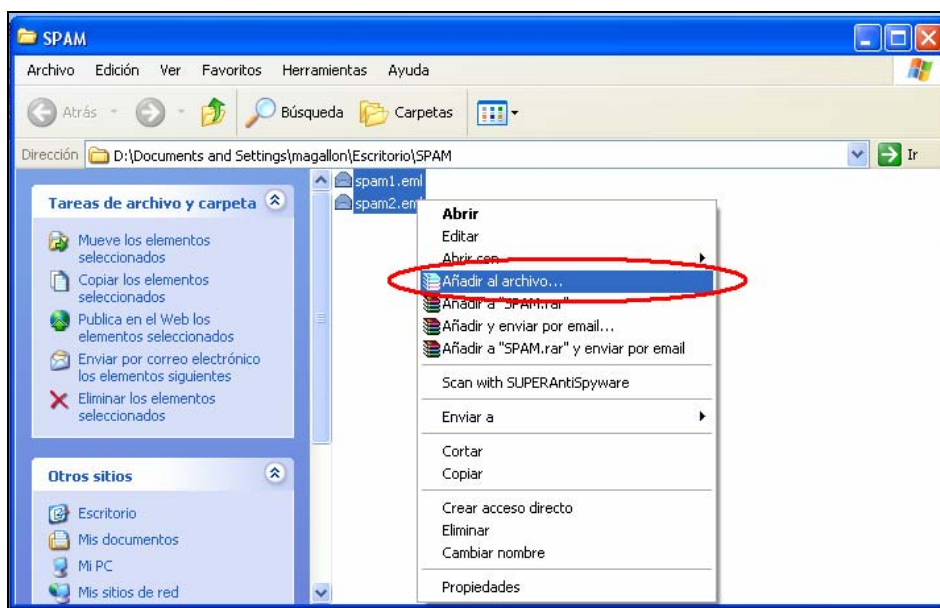


DOCUMENTACIÓN TÉCNICA		
Título:		Envío de muestras de SPAM a TrendMicro
Referencia:	Sin Ref.	
Modificación:	25/06/2010 13:13	Página 10 de 14

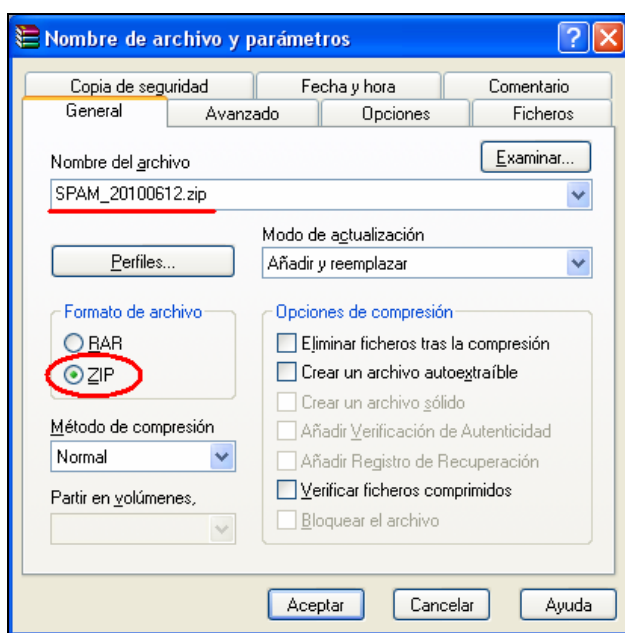
3.2. Compresión de archivos.

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:



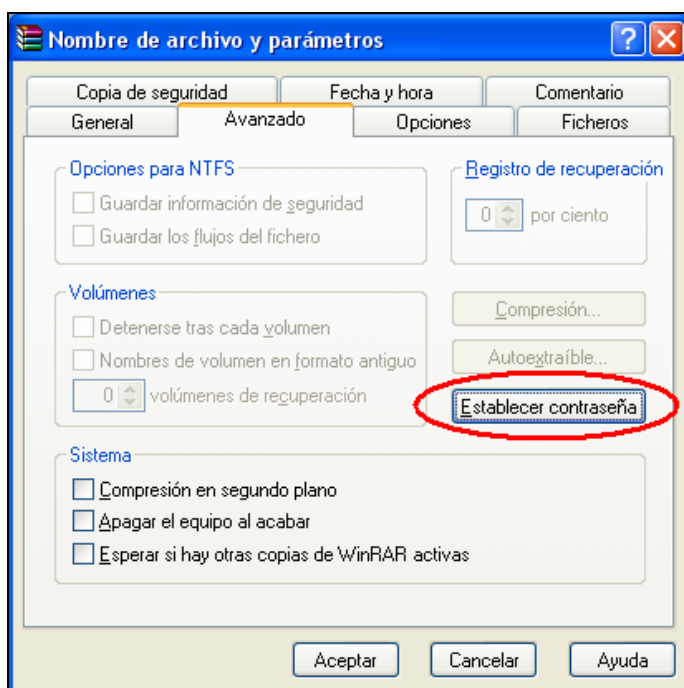
DOCUMENTACIÓN TÉCNICA		
Título:		Envío de muestras de SPAM a TrendMicro
Referencia:	Sin Ref.	
Modificación:	25/06/2010 13:13	Página 11 de 14

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

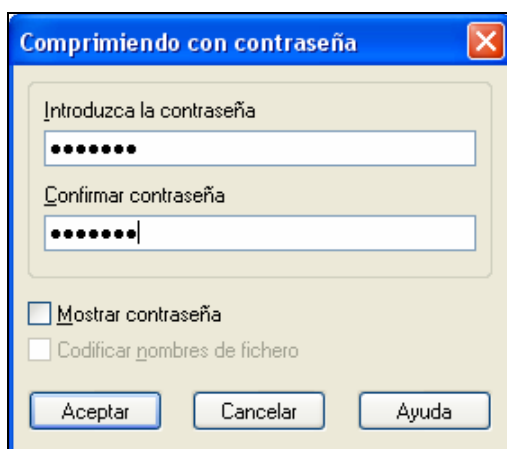
Con:

- 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”

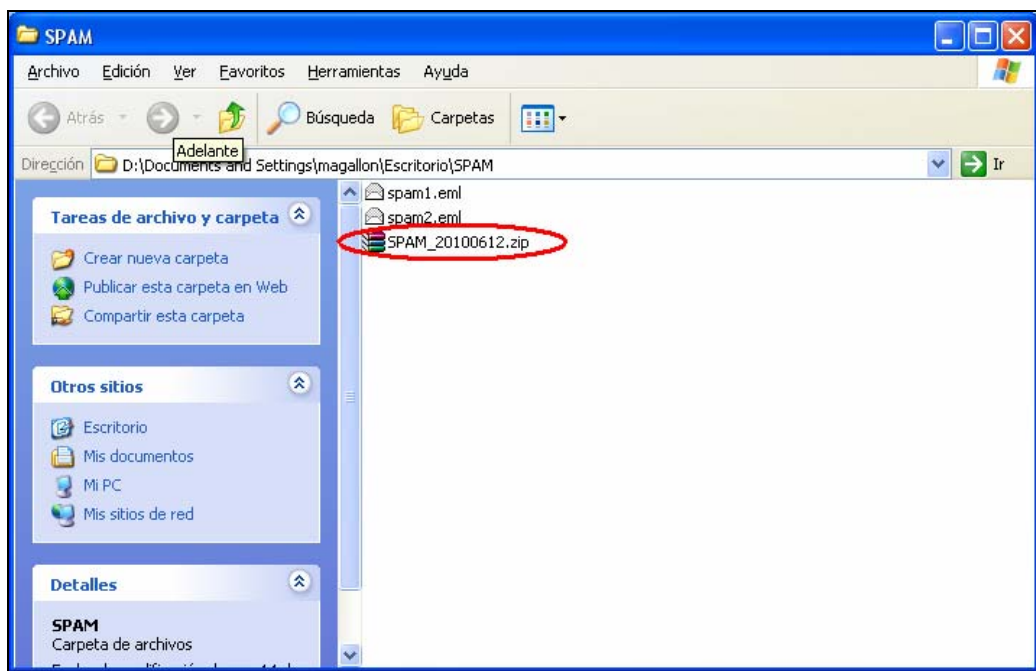


4) Establecemos la contraseña:



DOCUMENTACIÓN TÉCNICA		
Título:		Envío de muestras de SPAM a TrendMicro
Referencia:	Sin Ref.	
Modificación:	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

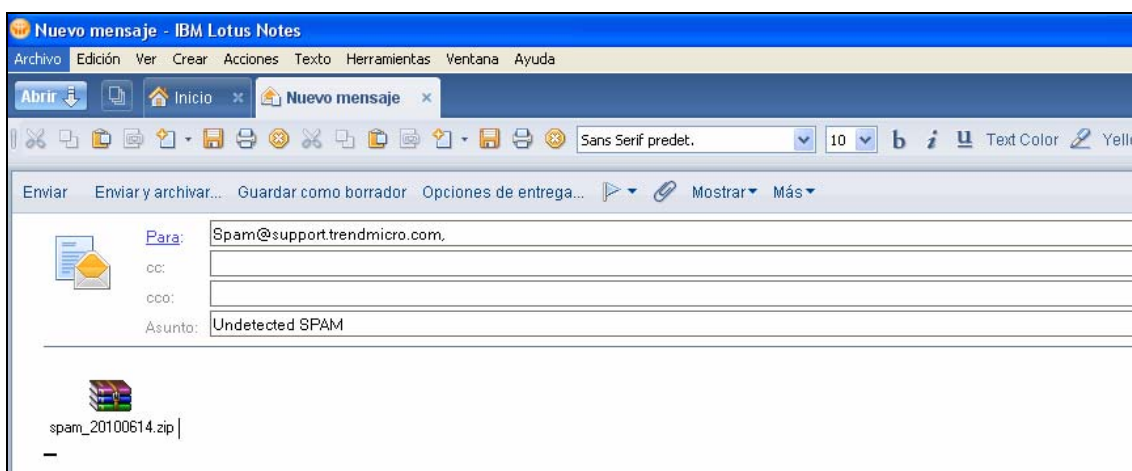
DOCUMENTACIÓN TÉCNICA		
Título:		Envío de muestras de SPAM a TrendMicro
Referencia:	Sin Ref.	
Modificación:	25/06/2010 13:13	Página 13 de 14

3.3. Envío de muestras de SPAM a TrendMicro

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

- Spam@support.trendmicro.com
→ Para falsos negativos (spam no detectado).
- 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, según imagen adjunta:



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