Diputación de Teruel
Servicio TIC

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
Titulo:	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	José Antonio Magallón Civera	
Cargo	Ing. Técnico Telecomunicaciones	
Entidad	Diputación Provincial de Teruel	
Fecha	25/06/2010	

Firma	
Nombre	
Cargo	
Entidad	
Fecha	

Control de modificaciones por cambio de versión

Versión	*Autor*	*Descripción*	*Fecha*
1	J.A. Magallón	Documentación Técnica	25/06/2010

Declaración de confidencialidad

Índice

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 :

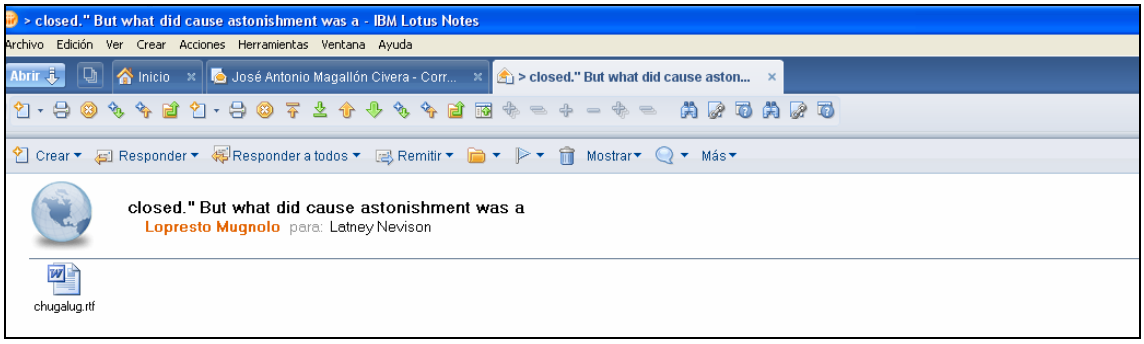
   - Spam@support.trendmicro.com
     → Para falsos negativos (spam no detectado).
   - False@support.trendmicro.com
     → Para falsos positivos (correo legítimo detectado como spam)

[1] Sin las comillas

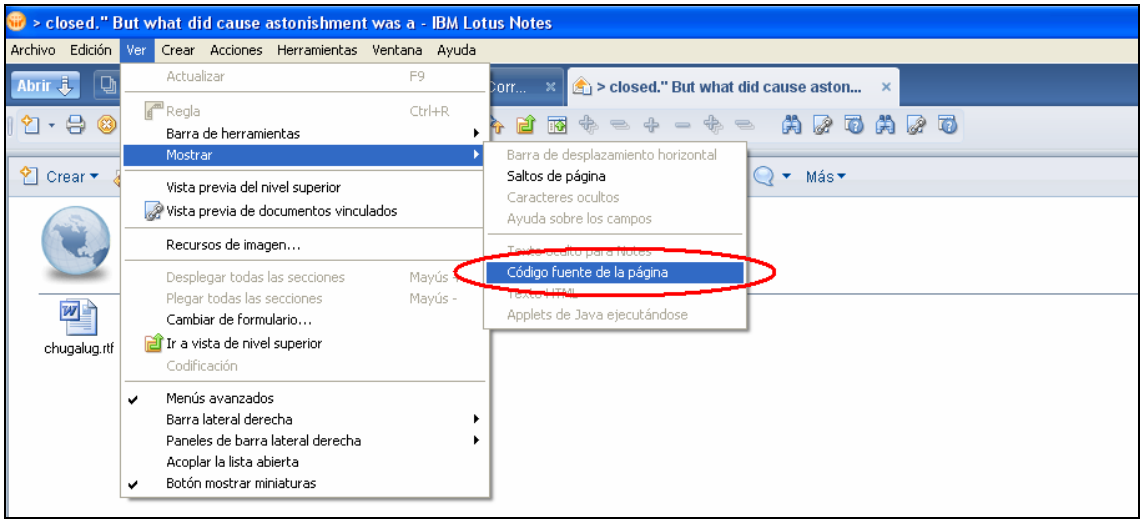
3.1. Captura de correos

1) Seleccionamos el correo que clasificamos como SPAM

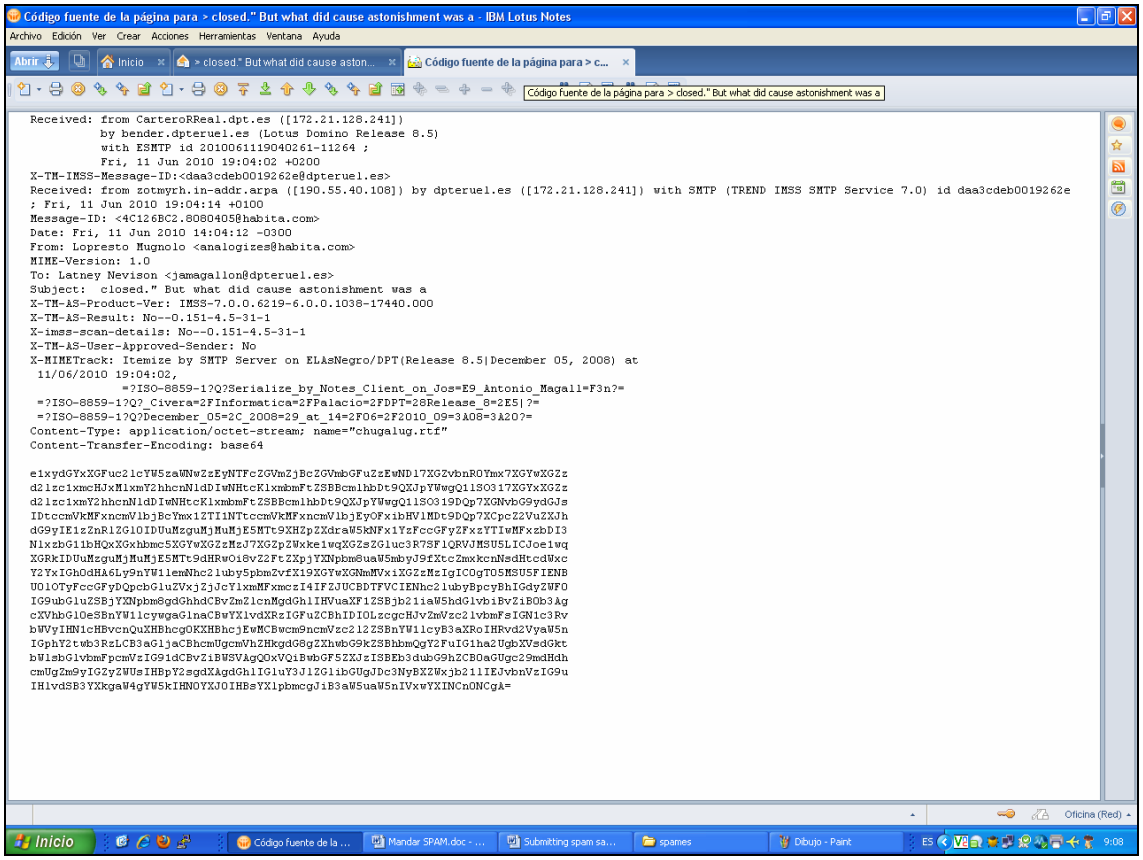
2) Abrimos el correo



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

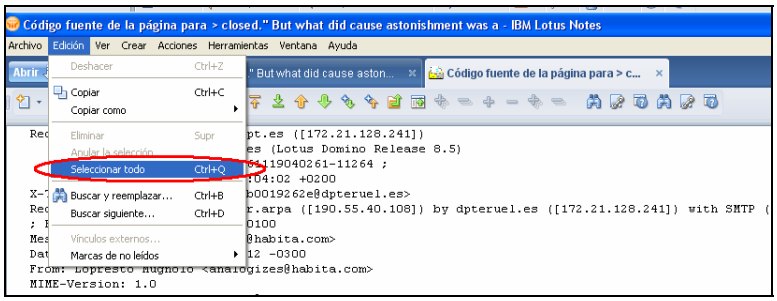


Nos aparecerá algo como:

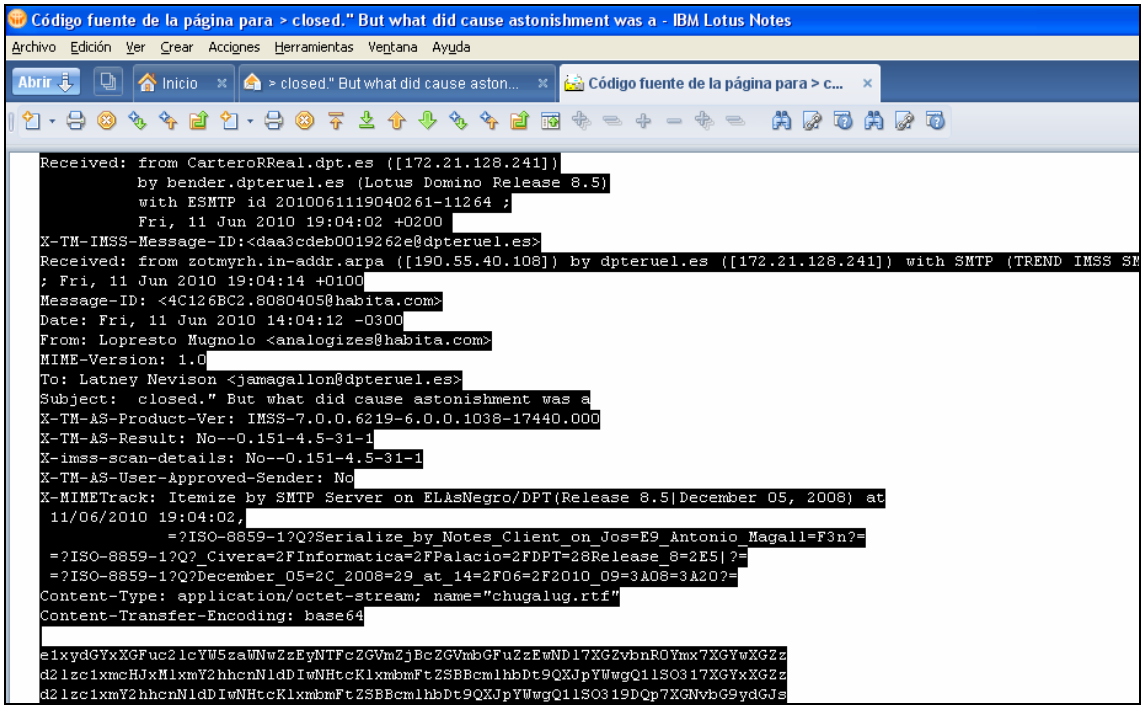


4) El contenido de esa ventana es lo que hay que guardar en un archivo en formato ".msg" o "..eml".

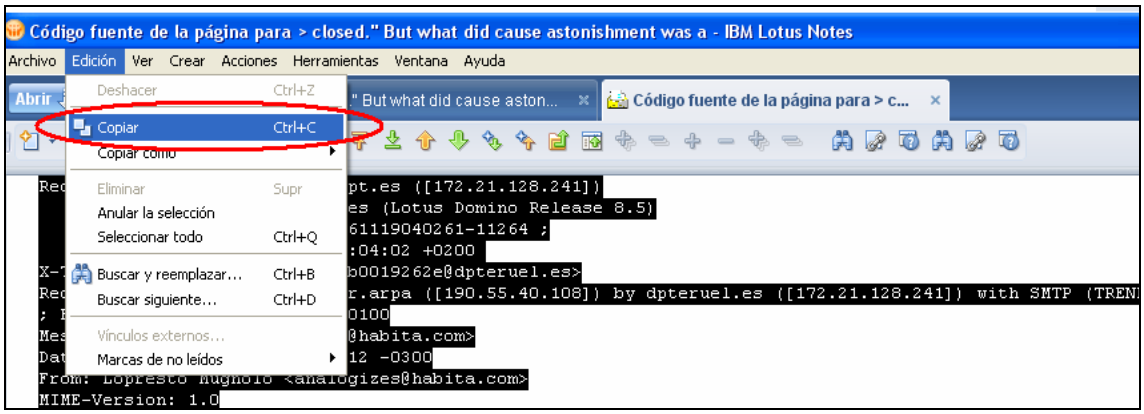
   Para ello, seleccionamos el menú Edición → Seleccionar todo:



   Cuyo resultado es:

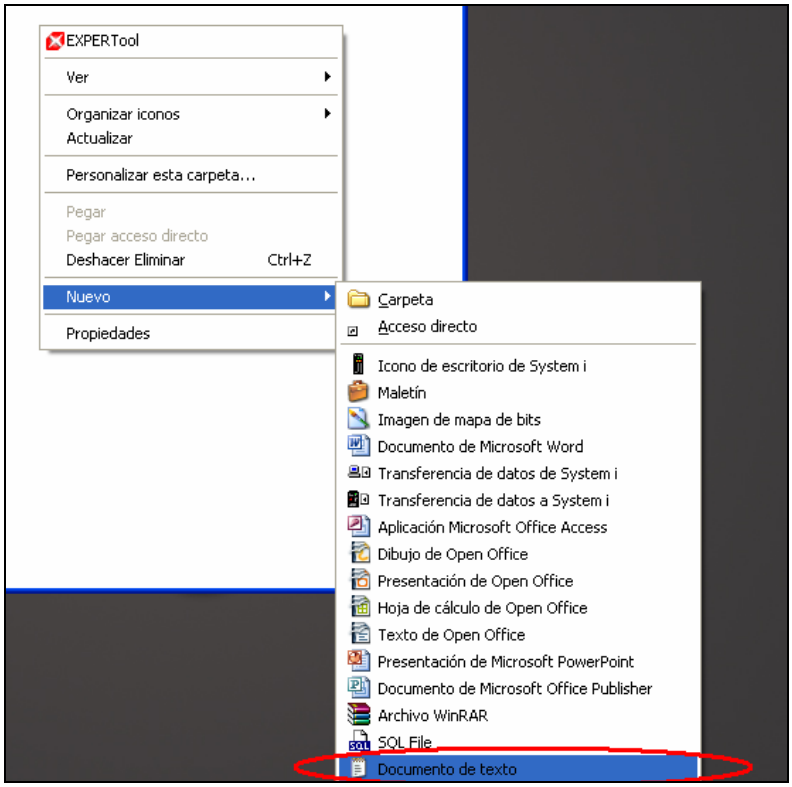


5) Seleccionamos el menú Edición → Copiar:

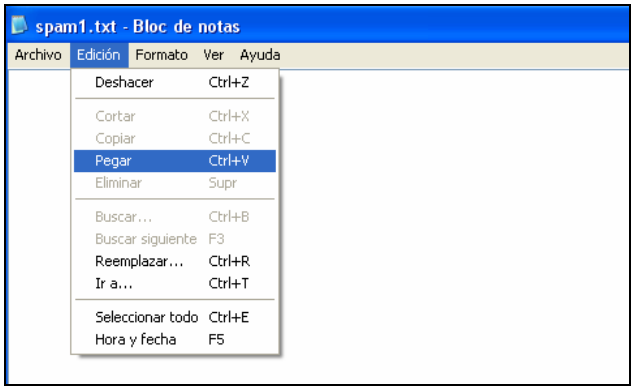


Abrimos el “notepad” o el procesador de textos que estemos acostumbrados a usar (que no sea el Word o el swritter del OpenOffice)

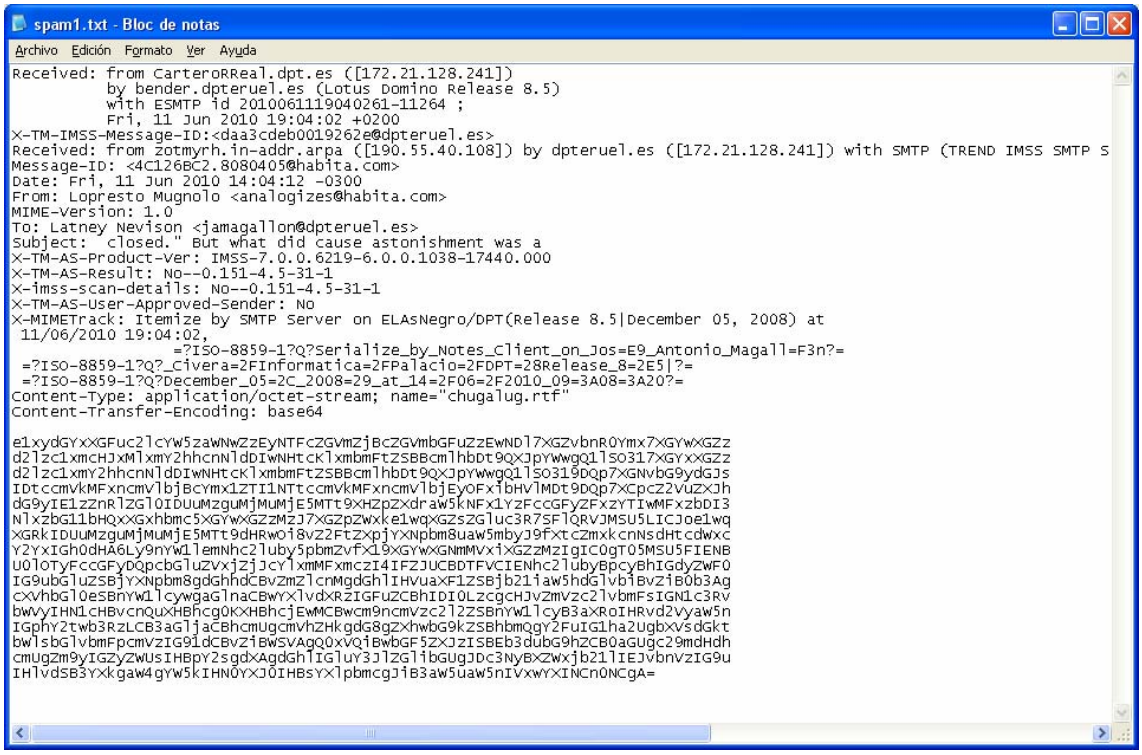
Por ejemplo, podemos crear un “nuevo documento de texto”, dentro de la carpeta donde queramos guardar el SPAM



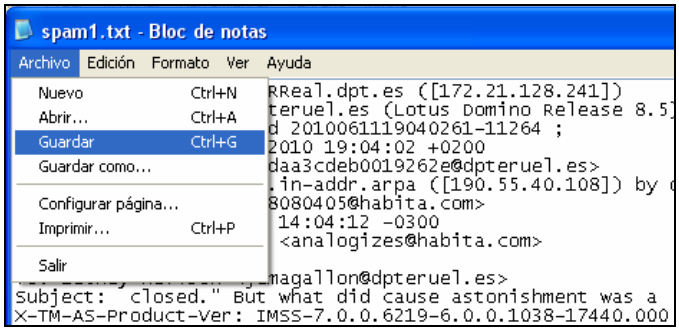
6) Una vez abierto, seleccionamos el menú Edición → Pegar:



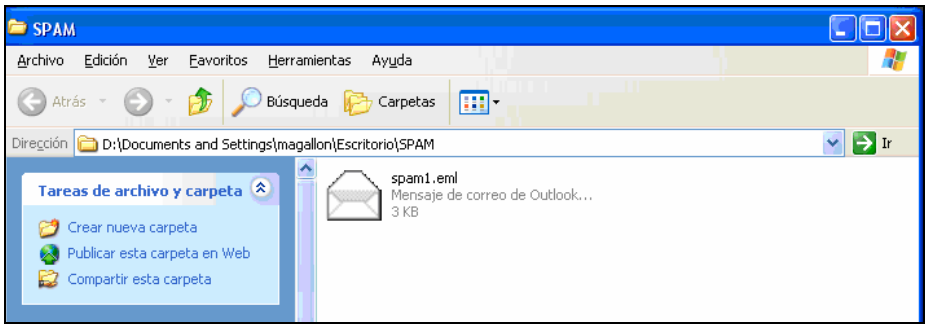
Esto pegará el código fuente del mensaje de spam, que habíamos seleccionado previamente, en el fichero abierto.



7) Seleccionamos el menú Archivo → Guardar:



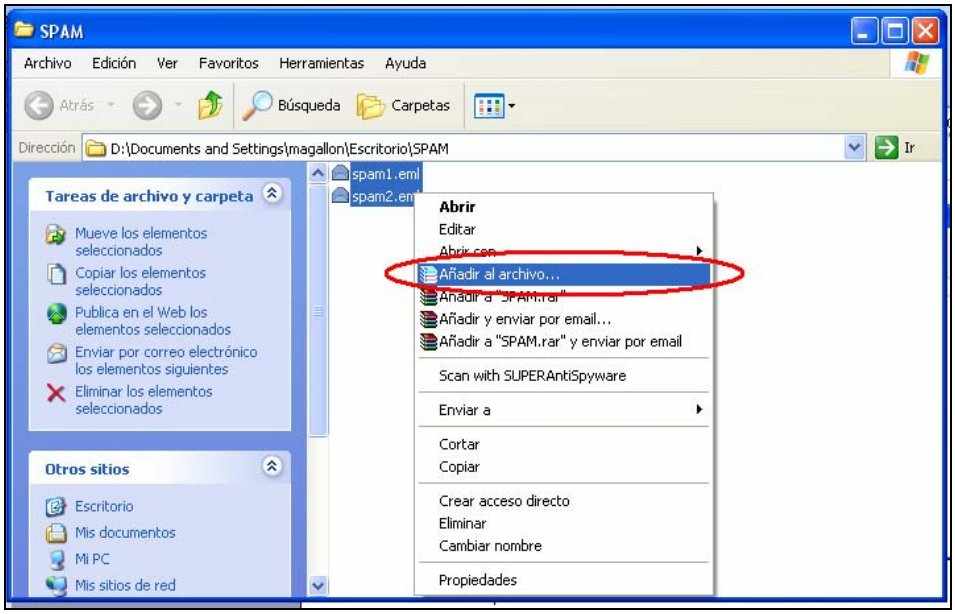
8) Ahora cambiaremos la extensión del fichero recién creado a .eml (o .msg)



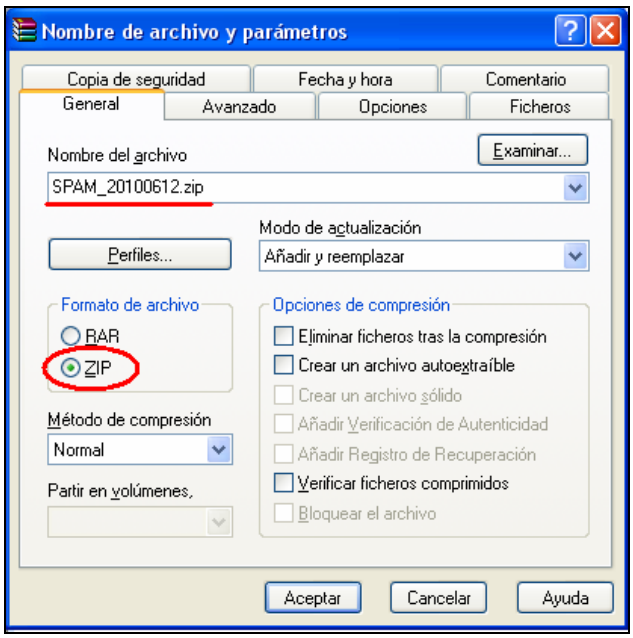
3.2. Compresión de archivos.

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:

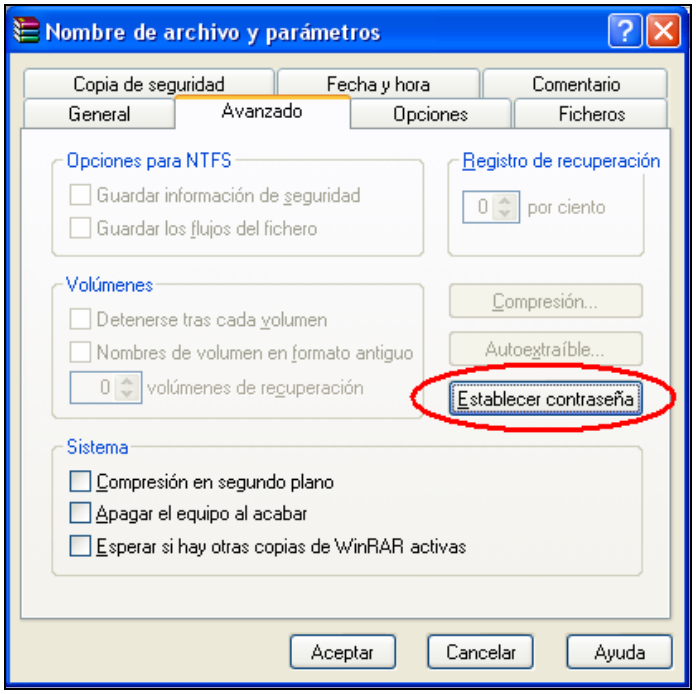


Además de seleccionar el formato, le daremos un nombre al fichero, por ejemplo: SPAM_AAAAMMDD.zip

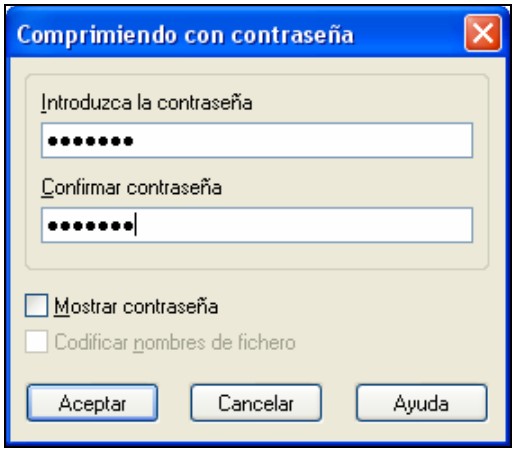
Con:

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

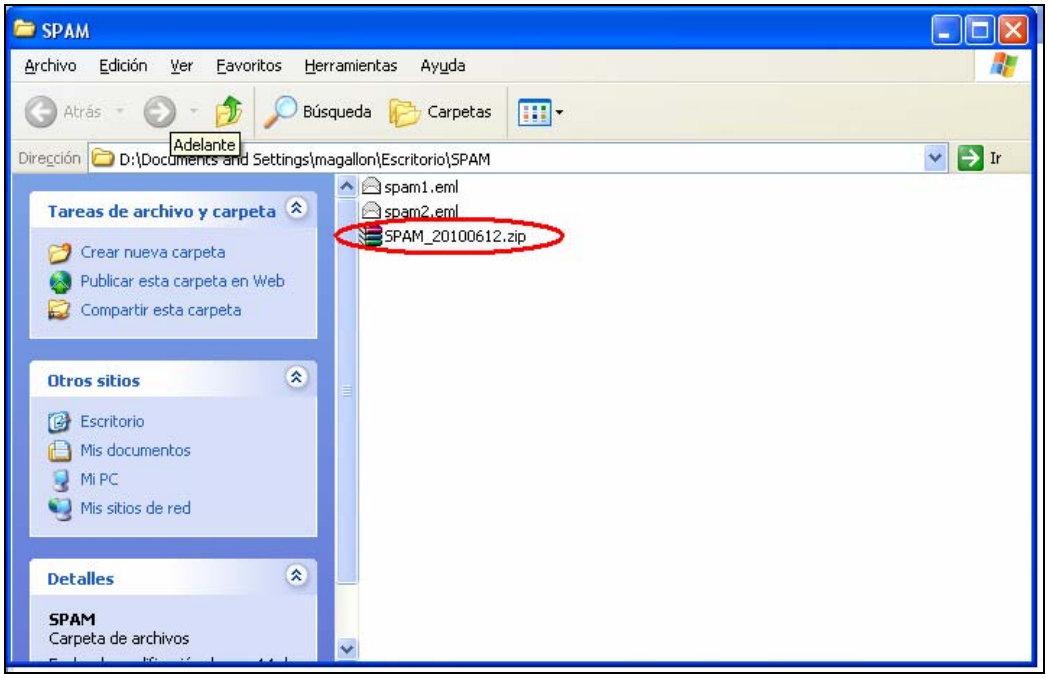
3) Una vez hecho esto, iremos a la pestaña “avanzado”, donde seleccionaremos “Establecer contraseña”



4) Establecemos la contraseña:



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

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: