Trucos comerciales de los spammers

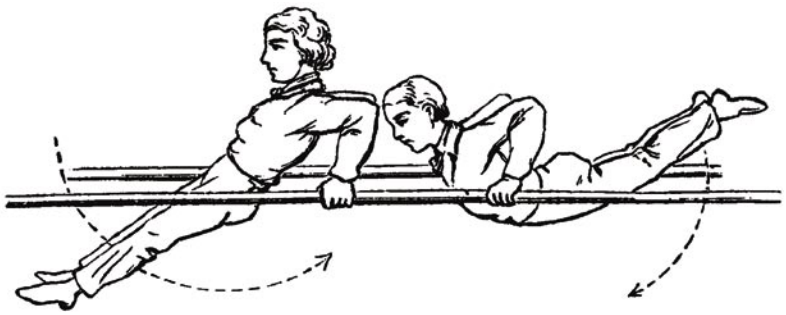
John Graham-Cumming

Artículo publicado en el número 3/2004 de la revista *Hakin9*

Revista *Hakin9*, Wydawnictwo Software, ul. Lewartowskiego 6, 00-190 Warszawa, hakin9@hakin9.org

Trucos comerciales de los spammers

John Graham-Cumming



A pesar de los filtros, los spammers intentan enviar sus mensajes valiéndose de ciertos trucos. Vamos a ver cómo funcionan esos trucos y cómo actualizar los filtros para que los reconozcan y sean más eficientes.

Los spammers usan principalmente un tipo de trucos. Tratan de ocultar palabras claves (tales como *Viagra*) de tal forma que el filtro no las vea; incluyen palabras buenas o inocentes de tal manera que los filtros las vean mientras que el lector no. De este modo los filtros creen que el mensaje es legítimo y, puesto que las URLs de sus páginas son muy a menudo indicadoras, tratan de ocultar cualquier URL usada.

Ocultaremos palabras claves

Lo primero que los spammers tratan de hacer es ocultar las palabras que califican el mensaje como spam. Usan una colección de técnicas que están diseñadas para que las palabras como *Viagra* sean ilegibles para el filtro de spam, aunque sean perfectamente legibles para el destinatario.

Perdido en el espacio

El truco más simple de todos es tomar una palabra sospechosa como *Viagra* y dividirla con espacios.

```
V I A G R A
```

Esto engaña a filtros muy simples que buscan la palabra *Viagra*; naturalmente, en los más sofisticados, se puede buscar el modelo `<letra><espacio><letra><espacio>...` y reconstruir la palabra buscada. Igual que los spammers, usan variedad de otros caracteres para dividir la palabra:

```
V'I'A'G'R'A
V.I.A.G.R.A
V*I*A*G*R*A
V-I-A-G-R-A
```

el listado puede seguir y seguir. Desgraciadamente, para los spammers es muy fácil buscar diferentes modelos en los filtros de spam y hacer llegar su mensaje hablando de Viagra. Sin embargo, esta simple técnica no dificulta el pro-

En este artículo aprenderás...

- lo que hacen los spammers para evitar los filtros bayesianos y heurísticos.

Lo que deberías saber...

- bases de los filtros bayesianos heurísticos (véase la edición anterior de nuestra revista),
- bases de HTML y de Javascript.

blema para cualquiera que considere comprar un filtro antispam: no compres nada que tengas que actualizar con los últimos cambios; cómprate algo que tenga servicio de actualización automática. Incluso cuando estás al corriente, esta simple forma de ocultar la palabra requerirá un gran esfuerzo por tu parte.

Los spammers, por supuesto, analizan su correo tanto contra aplicaciones libres como contra aplicaciones comerciales antispam y si se dan cuenta de que este truco no funciona bien, suelen cambiar las letras de *Viagra*. Un correo conocido ha seguido la dirección opuesta y ha eliminado todos los espacios del mensaje, sustituyendo los espacios con letras aleatorias:

```
DidAyouFknowNyouMcanBget
VprescriptionVmedications
prescribedTonlineTwith
NORPRIORRPRESCRIPTIONRREQUIRED!
```

Esto no parece una técnica muy eficaz, puesto que el mensaje es casi ilegible.

Acento extranjero

Una rápida ojeada a la tabla ASCII revelará la presencia de un montón de vocales acentuadas, que pueden ser usadas por los spammers para tomar palabras sospechosas, y camuflarlas, sustituyendo las vocales con sus equivalentes acentuadas:

- a: à á â ã ä å,
- e: è é ê ë,
- i: ì í î ï,
- o: ò ó ô õ ö,
- u: ù ú û ü.

Tan sólo al mezclar y poner diferentes acentos a las vocales *a* e *i* los spammers disponen de 144 diferentes formas de escribir *Viagra*, tales como *Víagra*, *Viâgra*, *Vîãgrä*. El lector simplemente ignorará los acentos y leerá la palabra, sin embargo, es suficiente para entorpecer el filtro antispam.

Está claro que un filtro antispam que está programado para reconocer los trucos de spam puede capturar cualquier vocal acentuada, convertirla en la vocal original y reconstruir la palabra original. Hoy día los dos trucos – éste y el anterior – son presas fáciles para los filtros antispam actuales, ya que los spammers se han especializado en HTML y en las formas inventivas para terminar en nuestras carpetas.

Juego de números

Otra forma de ocultar la palabra *Viagra* es usar una propiedad especial de HTML, diseñada especialmente para introducir caracteres especiales o caracteres no ingleses. Estas entidades HTML están escritas empezando por `&#` y terminando con `;`. Por ejemplo, para escribir el carácter acentuado francés *é* en HTML, tienes que introducir `&#233;`, para escribir la letra griega ∑, tienes que introducir `&#917;`.

Por supuesto, todos los caracteres, incluyendo el alfabeto inglés estándar, tienen entidades equivalentes. La letra *A,* por ejemplo, puede escribirse `&#65;` y, por lo tanto, un spammer astuto puede reescribir la palabra entera *Viagra* en entidades: `&#86;&#105;&#97;&#103;&#114;&#97;`.

Otra vez un filtro antispam actualizado entenderá estas entidades HTML y las convertirá en la palabra original. Hay formas mucho más sofisticadas de ocultar la palabra *Viagra* si analizamos muy detalladamente las propiedades del formateo del HTML.

Hypertextus Interruptus

La información HTML sobre el formateo está especificada con el uso de lo que conocemos como etiquetas HTML: instrucciones escritas entre `<` `>` signos "menor que" y "mayor que".

Por ejemplo, para tomar la palabra *Hola* y especificar que debería aparecer en negrita, tienes que escribir: `<b>Hola</b>`. La `<b>` significa *empezar texto en negrita* y la `</b>` *terminar texto en negrita*. El texto puesto entre estas dos etiquetas aparecerá en negrita cuando lo veamos con un navegador web o con un cliente de correo que soporte HTML.

Como la mayoría de los lenguajes informáticos, HTML también tiene un mecanismo con el cual el creador de la página o del mensaje puede introducir una nota. Estas notas están allí para ser leídas por otras personas, sin embargo, se ignoran completamente cuando se muestra HTML. Una nota empieza por `<!--` y termina con una `-->`; cualquier cosa escrita entre estas dos etiquetas es ignorada completamente por las aplicaciones que muestran HTML.

Los spammers usan notas HTML para fragmentar la palabra sospechosa, intercalando notas en el medio de la palabra. Por ejemplo, *Viagra* puede fragmentarse de la siguiente forma:

```
V<!--anon-->i<!--dinosaur-->
a<!--hexagon-->g<!--two-->r
<!--mouse-->a
```

Este listado que parece texto mostrará *Viagra* en cualquier cliente de correo que soporta HTML. Muchos filtros antispam serán burlados con estas técnicas, ya que no soportan HTML y no son capaces de ver la palabra *Viagra;* o mucho peor, podrán leer las palabras entre las notas y considerar el mensaje como legítimo.

Este es el truco más popular con HTML usado por los spammers y actualmente los buenos filtros antispam incluyen un código que simplemente quita las notas HTML antes de que se considere si el mensaje es spam o no. Una buena tarea para la aplicación es buscar `<!--` seguido por `-->` y, simplemente eliminarlo, con lo que el cliente de correo muestra el mensaje.

Además, un filtro antispam puede considerar la presencia de muchas notas HTML como sospechosas: al fin y al cabo ¿quién envía este tipo de mensajes legítimos? Los spammers también usan etiquetas HTML no válidas, tan sólo inventan un nombre para las etiquetas, debido a que todos los navegadores van a rechazarlas. Únicamente funciona la introducción de palabras aleatorias entre `<` y `>`, así como las notas HTML:

```
V<anon>i</dinosaur>a<hexagon>g
<two>r</mouse>a
```

El agujero negro

La increíble popularidad del truco anterior fue la causa de su ocaso:

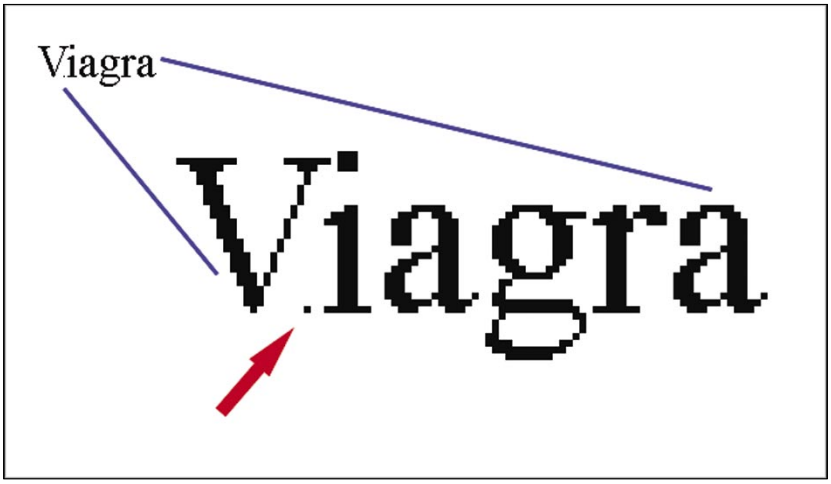


Figura 1. *Microdot*

actualmente la mayoría de los filtros antispam eliminan las notas HTML. Sin embargo, la fragmentación de palabras con bits de HTML sigue siendo el método preferido de los spammers. *El agujero negro* envuelve la fragmentación de la palabra sospechosa con espacios que no tienen ancho.

Para especificar el tamaño de una parte del texto en HTML tienes que escribir `<font size=X>`, donde `X` puede ser un valor de 1 a 7 (7 será el tamaño más grande y 1 el más pequeño). Por ejemplo, para decir *Hola* en la fuente accesible más pequeña, tendrás que escribir:

```
<font size=1>Hola</font>
```

Las aplicaciones como Microsoft Internet Explorer o los clientes de correo de Microsoft Outlook y Outlook Express aceptan también la fuente de tamaño 0, es decir, el texto no tiene tamaño. Por lo tanto, algunos spammers agregarán el espacio para obtener uno que no tenga ancho:

```
<font size=0> </font>
```

y, luego, lo usan para fragmentar *Viagra* de la siguiente forma:

```
V<font size=0> </font>i
<font size=0> </font>a
<font size=0> </font>g
<font size=0> </font>r
<font size=0> </font>a
```

La competición entre las armas de los spammers y anti-spammers significa que la actualización de los filtros antispam requiere no sólo el soporte de las notas HTML (véase los trucos anteriores), sino también cómo están especificados los tamaños de las fuentes HTML. Esto obliga a los spammers a emplear trucos mucho más inteligentes: si el tamaño de la fuente 0 ya está quemado ¿qué tal con el tamaño 1?

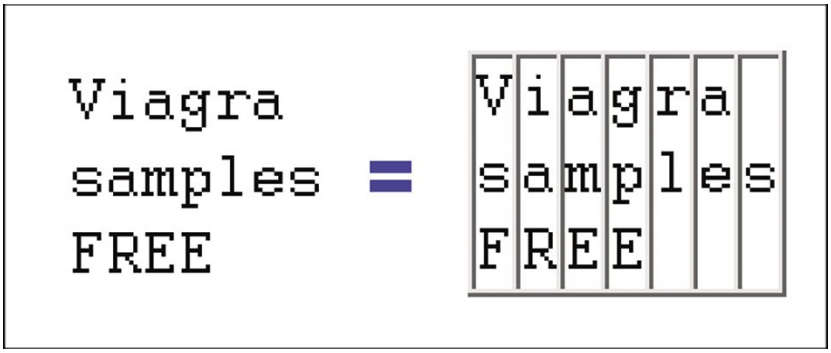


Figura 2. *Cortar y partir*

Microdot

Esta reciente innovación de los spammers les permite introducir letras al azar en el medio de la palabra (de tal forma que el filtro antispam que descompone HTML lea *Viagra* como *Vziagra* por ejemplo) y hacer estas letras tan pequeñas que apenas sean legibles. Bienvenidos al mundo de microdot o de la fuente de tamaño 1.

```
V<font size=1>z</font>iagra
```

la cual, al visualizarse en el cliente de correo que soporta HTML, resulta similar a la de la Figura 1. Como podemos ver, la letra `z` ha sido reducida a un punto muy pequeño, apenas visible.

Cortar y partir

Es la forma más inteligente de dividir una palabra en uso. Requiere una combinación del ancho fijo de la fuente y de las tablas HTML. Un spammer inteligente primero escribirá el texto, usando la mezcla del ancho fijo de la fuente de tal forma que tenga definidas las columnas de letras:

```
Viagra
samples
FREE
```

Luego, con ayuda de una tabla con una columna para cada columna de letras, el spammer envía las columnas en orden (véase el Listado 1 y la Figura 2).

Los filtros antispam que fragmentan las etiquetas HTML son engañados totalmente por esta técnica, ya que terminan viendo una secuencia de letras aparentemente aleatorias para analizar, dado que el filtro lee el texto de arriba abajo en columnas y no de izquierda a derecha.

```
Vsf iaR ame gpe rl ae s
```

Actualmente el proceso de reconstrucción de palabras en el mensaje requiere que el filtro antispam incluya algunas formas del mecanismo del esquema HTML. En la práctica esto no es necesario, ya que el carácter de spam del mensaje se deja aparte,

Listado 1. *Cortar y partir*

```
<table border=0 cellpadding=0 cellspacing=0><tr valign=top>
    <td><font face=Courier>V<br>s<br>F</font></td>
    <td><font face=Courier>i<br>a<br>R</font></td>
    <td><font face=Courier>a<br>m<br>E</font></td>
    <td><font face=Courier>g<br>p<br>E</font></td>
    <td><font face=Courier>r<br>l</font></td>
    <td><font face=Courier>a<br>e</font></td>
    <td><font face=Courier> <br>s</font></td>
</tr></table>
```

gracias al uso de una tabla completa y un tamaño fijo de fuentes. Las palabras naturales que contiene no son tan importantes como el esquema.

Introducimos buenas palabras ocultas

Cuando ya se han ocultado las palabras malas, los spammers añaden las que consideran inocentes. Dado que algunos filtros antispam tienen listas de buenas palabras que permiten pasar los mensajes, las esperanzas de los spammers que añaden algunas palabras que no sean spam harán que sus mensajes sean suministrados. Si el spammer no quiere que el destinatario vea estas palabras (¡se considera que el destinatario se centrará en la oferta de Viagra!), el spammer verá la forma de esconder las buenas palabras al lector, que al mismo tiempo serán legibles para el filtro antispam.

Listado 2. *Tinta invisible*

```
<body bgcolor=white>
  Viagra
  <font color=white>
     Hi, Johnny! It was
     really nice to have
     dinner with you
     last night. See
     you soon, love Mom.
  </font>
</body>
```

Listado 3. *Camuflaje*

```
<body bgcolor=#113333>
  <font color=yellow>
    Viagra
  </font>
  <font color=#123939>
    unas palabras inocentes
  </font>
</body>
```

Tinta invisible

Probablemente la forma más habitual de añadir palabras buenas a los correos consiste en escribir algún texto en el fondo blanco (o cualquier otro color con tal de que el color del fondo y del primer plano sean los mismos): véase el Listado 2. A los spammers les gusta esto, puesto que la gente es capaz de leer dicho texto, mientras que un ordenador que ignora la información de color va hacia adelante y lee el texto inocente. Algunos filtros antispam han quedado burlados con eso y cuando el spammer es bastante inteligente como para reagrupar las palabras respectivas, el spam pasa.

Los buenos filtros antispam soportan colores de HTML y reconocen el truco, al identificar el correo que se supone como spam. Debido a que estos trucos prevalecen y al hecho de que los filtros antispam luchan contra ellos, los spammers han creado una forma parecida de esconder texto coloreado, usando colores que son casi iguales.

Camuflaje

En vez de escribir un texto blanco sobre el fondo blanco, un spammer puede optar por usar colores de HTML que se parecen mucho (por ejemplo, un gris muy claro en el fondo blanco): véase el Listado 3 y la Figura 3. Desde que los colores pueden especificarse, usando el formato hexadecimal RGB, los spammers tienen más de 16 millones de colores a seleccionar, lo cual permite ajustar los colores individualmente para cada spam enviado.

El spammer recoge el color del fondo (en el ejemplo abajo `#113333`) y luego el color del primer plano que se parece mucho a este (por ejemplo `#123939`). El texto actual, que los spammers quieren que leas, usan un color que se difiere del fondo.

Así las palabras inocentes son casi invisibles y el producto que se ofrece se lee fácilmente. Esto atonta a los filtros antispam que soportan el truco de la tinta invisible, ya que los colores no son iguales, sin embargo, el ojo humano rápidamente se centrará en el texto, que se puede leer fácilmente.

Los buenos filtros antispam soportan también este truco y calculan la similitud entre los colores del primer plano y del fondo, usando la distancia de Euclides para reconocer el texto que es apenas visible para el ojo humano.

MIME es dinero

La mayoría de los clientes de correo soporta la codificación MIME de mensajes que permiten que el mensaje se envíe a muchas partes, donde cada una de las partes especifique su tipo (por ejemplo, texto plano, HTML, documento de

Figura 3. *Camuflaje*

Ms Word) y automáticamente mostrará la versión HTML del mensaje e ignorará cualquier versión del texto plano.

Los spammers lo utilizan, enviando el texto inocente en la parte plana del mensaje y el mensaje de spam en HTML (véase el Listado 4). El mensaje de spam se muestra y la parte plana se esconde de la vista. Un filtro antispam que lee el mensaje entero terminará leyendo tanto la versión HTML como la plana.

Listado 4. *MIME es dinero*

```
------=_NextPart_01C29D73.26716240
Content-Type: text/plain;
The modes of letting vacant farms, the duty of supplying buildings
and permanent improvements, and the form in which rent is to be
received, have all been carefully discussed in the older financial
treatises. Most of these questions belong to practical administration,
and are, moreover, not of great interest in modern times.
------=_NextPart_01C29D73.26716240
Content-Type: text/html;
<p><b><font color=red>Viagra</font></b></p>
```

Noticias diarias

Otra forma preferida de los spammers es recoger las noticias de una página en línea, sacar el texto de ella y añadirlo a su spam en espera de que la inclusión de los asuntos corrientes en el mensaje les permita pasar por un filtro.

```
<Despite statements last week from
chief U.N. inspector Hans Blix that
full cooperation was expected from
Iraq, Iraqi Foreign Minister Naji
Sabri lashed out at the United
Nations in a 19-page letter to
Secretary-General Kofi Annan
written in Arabic>
```

Obviamente, los spammers no quieren que leas las noticias en vez de su mensaje, por lo tanto, envuelven el texto en los caracteres < y > del código HTML. Tanto las aplicaciones que soportan HTML, como los clientes de correo ignoran las etiquetas que no soportan el texto entre los signos de *menor que* y *mayor que* no mostrado y hace que se ignore (la aplicación no sabe lo que es la etiqueta `<despite>` en el ejemplo de arriba).

Título honorífico

HTML entrega la etiqueta `<title>`, la cual se usa para fijar el título mostrado en el navegador a la hora de ver la página. Cuando el HTML se incluye en un e-mail, el contenido de la etiqueta `<title>` se suele ignorar y no se muestra en ninguna parte (el título del correo suele ser la línea del sujeto).

```
<title>dinosaur reptile ghueej
egrjerijg gerrg</title>
```

Por tanto, esto da a los spammers otra forma de incluir palabras inocentes que nunca serán vistas por el destinatario.

Esto es Mini Marquee

El rótulo *marquee* enrollado da al spammer la oportunidad de introducir una cantidad arbitraria de buen texto y, luego, especificar que aparezca en un espacio pequeño. En el ejemplo real que sigue el texto real entero, encierra en un cajón de 8 pixeles por 8 pixeles y, por tanto, el lector del correo apenas lo nota (véase la Figura 4).

```
<marquee bgcolor="white"
height="8" width="8">
  Did you ever play that game
  when you were a kid where the
  little plastic hippo tries to
  gobble up all your marbles?
</marquee>
```

Cariño, he encogido la fuente

El último truco habitual para esconder el texto inocente es usar una fuente muy pequeña, de tamaño de 1 (véase también el truco de *Microdot* arriba). En el siguiente ejemplo, el spammer ha especificado el tamaño de fuente 1 (y, también el color blanco, pues a lo mejor usa también *Tinta invisible*) para una parte de texto bueno, sin embargo, parece que ha fallado en seguir las direcciones en sus aplicaciones de spam:

```
<font size="1" color="#FFFFFF">
  Palabras aleatorias en MAYUSCULAS
  con largo de 1 a 22
  TSUTHRXJKVUVBECP
</font>
```

Ocultando las direcciones URL

Otra forma de tender una trampa contra el spam por los filtros antispam es examinar las direcciones URL, presentes en el mensaje. Muchos correos no deseados poseen por lo menos un enlace a la página web, en la cual el spammer vende sus productos. Al construir un listado negro de estas páginas es posible eliminar el spam basado en los enlaces a las páginas de los spammers. Por eso

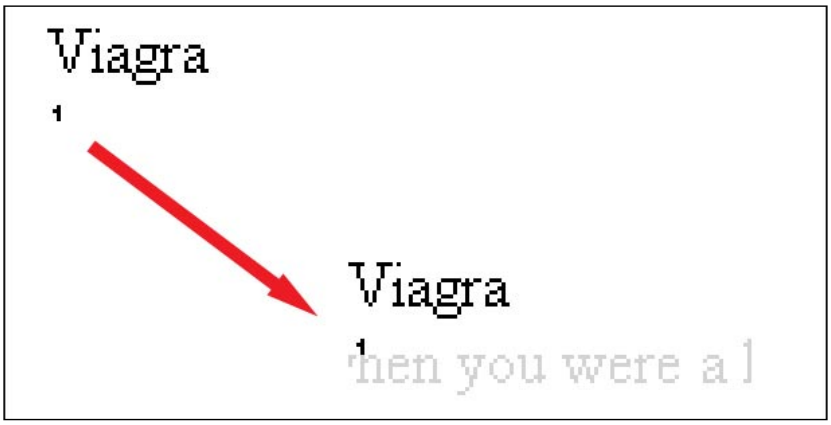


Figura 4. *Mini Marquee*

los spammers tratan de oscurecer las direcciones URL presentes de tal forma que los filtros fallan y no introducen las direcciones URL en la lista negra; al mismo tiempo el spammer tiene que asegurarse de que la dirección URL sigue funcionando.

Enigma y Ultra

Las direcciones URL suelen especificarse de forma legible, con las direcciones de las páginas (por ejemplo, *http://www.sophos.com*), sin embargo, el HTML es bastante flexible al permitir muchas otras formas. La siguiente tabla presenta estas formas: las primeras tres emplean la dirección IP de la página (*www.yahoo.com*), codificada primero como un número decimal separado, luego como uno hexadecimal y, finalmente, en forma de puntos usando el octagonal. La cuarta forma de URL emplea la codificación de `%` que marca cada letra (o carácter) con su equivalente hexadecimal.

```
http://3631052355/
http://0xD86D7643/
http://0330.0155.0166.0103/
http://%77%77%77%2E%79%61%68
%6F%6F%2E%63%6F%6D/
```

Un buen filtro antispam debería soportar varias codificaciones e invertir las accesibles y luego revertirlas antes de realizar cualquier comparación.

Falso Login

Una propiedad poco usada de URL (por lo menos para HTTP) es la sintaxis `http://nombre de usuario@host/` (el uso más habitual es la simple `http://host/`). Los spammers lo utilizan con los nombres de usuarios seleccionados al azar para que la dirección URL sospechada parezca inocente. En este ejemplo, la página visitada no es *www.microsoft.com,* sino la página con la dirección IP especificada por `3631052355` (la cual es oculta, gracias a los mencionados trucos para lograr el efecto máximo).

```
http://www.microsoft.com@3631052355/
```

El usuario asignado a la página es *www.microsoft.com* y, sin duda, será totalmente ignorado.

Internet Exploiter

Un bug en el popular navegador Internet Explorer de Microsoft (para el cual existe la ruta: *http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-004.asp*) permite a un poderoso spammer (o scammer) ir más adelante de los dos trucos anteriores, no sólo haciendo que las URL aparezcan como páginas legales, sino que también se vea en la barra de estado de Internet Explorer que aparecen legalmente:

```
<a href=http://www.microsoft.com
=01%01%00@3631052355>
www.microsoft.com</a>
```

Otra vez esta dirección URL te redirige ahora a `http://3631052355/`, sin embargo, aparecerá en un cliente de correo como *www.microsoft.com*, e incluso la barra de estado lo mostrará como *www.microsoft.com* debido al `%00`, situado delante de la señal `@` para la impresión del resto de la dirección URL. ¡En este truco se encuentra una página oculta por el spammer, el nombre falso del usuario y la utilización de un bug!

Listado 5. *Escritor de scripts*

```
<HTML><HEAD><SCRIPT LANGUAGE="Javascript">
  <!-- var Words="%3CHTML%3E%0D%0A%3CHEAD%3E%0D%0A%3CTITLE%3E%3C/TITLE%3E%0D
  %0A%3CMETA%20HTTP-EQUIV%3D%22Content-Type%22%20CONTENT%3D%22text/html%3B
  %20charset%3DBig5%22%3E%0D%0A%3CMETA%20HTTP-EQUIV%3D%22Expires%22%20
  CONTENT%3D%22Sat%2C%201%20Jan%202000%2000%3A00%3A00%20GMT%22%3E%0D%0A%3C
  META%20HTTP-EQUIV%3D%22Pragma%22%20CONTENT%3D%22no-cache%22%3E%0D%0A
  %3C/HEAD%3E%0D%0A%3CFRAMESET%20ROWS%3D%22100%25%2C0%2220FRAMEBORDER%3D
  NO%20BORDER%3D%220% function SetNewWords(){ var NewWords; NewWords =
  unescape(Words);document.write(NewWords);} SetNewWords();
// --></SCRIPT></HEAD><BODY></BODY></HTML>
```

Trucos de Javascript

Como si todos estos trucos no fueran suficientes, los spammers emplean a veces Javascript para hacer sus mensajes más difíciles para descodificar.

Escritor de scripts

Cuando empleamos este método, el mensaje entero que se muestra es realmente codificado dentro de una simple variable (véase el Listado 5), la cual no se descodificará hasta que el mensaje permanezca abierto. El spammer espera que el filtro no se dé cuenta de que el mensaje incluye spam y seguirá por el Javascript.

WYSI_not_WYG

Otro truco de Javascript está relacionado con ocultar las direcciones URL. Aquí la dirección real se la esconde para cambiar el texto que aparecerá en la barra de estado, cuando el ratón se mueva por el texto `ClickHere` (véase el Listado 6).

Los remitentes quedan atónitos al pensar que van a una página cuando, de hecho, están dirigidos a un lugar totalmente diferente.

Ironía final

La ironía consiste en que cuanto más trata de ocultar el spammer su mensaje, más fácil se lo identifica como spam y elimina. Además, ¿quién envía mensajes reales con trucos de tipo *Agujero Negro, Tinta invisible* o *Microdot*? ■

Listado 6. *WYSI_not_WYG*

```
Remove My e-mail from my Friends Contact
<a href="http://sex.com/bPqjOL09yGCHw/"
onmouseover= "window.status='http://%77%77%77%77.3%65%653--%69%6c11%6c%69
  --3%6c%69%6c%6c.%6f%72%67/bPqjOL09yGCHw/remove.htm';return true;"
onmouseout= "window.status=' ';return true;">ClickHere</a>
```