

Combatimos a los cerebros del correo no deseado en Internet

EL NEGOCIO DEL SPAM

Los spammers cobran dinero real por sus dudosos servicios, y cientos de anunciantes están deseando pagar. Os mostramos algunas técnicas innovadoras para controlar y contener el spam, incluyendo estrategias para ralentizar spambots, impedir que los spammers consigan nuestra dirección y separar el spam del correo legítimo. **POR JOE CASAD, ULRICH BANTLE Y TOBIAS EGGENDORFER**

De acuerdo con el proveedor de correo electrónico Postini [1], de 524 millones de correos que pasaron por este proveedor en todo el mundo en un periodo de 24 horas, el 88 por ciento era spam (345 millones de correos), incluyendo 2 millones de “ofertas especiales”, 650.000 planes para hacerse rico y 2 millones de correos con contenido sexual. Sólo 46 millones de correos legítimos llegaron a su destino.

A pesar de los esfuerzos de los mejores expertos, el problema del spam no remite. La mayoría de las organizaciones se centran en contener el problema para evitar pérdidas en tiempo de administración y productividad del usuario final. En el tema de portada de este mes os mostramos algunas de las últimas estrategias para luchar contra el spam. Comenzamos examinando algunas técnicas para evitar que los spammers consigan nuestra dirección de correo, como primera medida. A continuación veremos cómo podemos alejar a los spammers de nuestro camino con un tarpit. Revisamos también algunas aplicaciones y servicios anti-spam, y describimos una solución a medida consistente en un filtro entrenable por el usuario que opera desde el lado servidor.

Conocer al Enemigo

El origen del término “spam” no está completamente claro. El término se acuñó originalmente en Usenet, donde hacía referencia a publicidad no solicitada. Cuando el fenómeno golpeó al correo electrónico, los usua-

EN PORTADA

Protección de direcciones.....	18
Tarpits.....	23
Aplicaciones anti-spam.....	25
Filtro Spam con IMAP.....	31

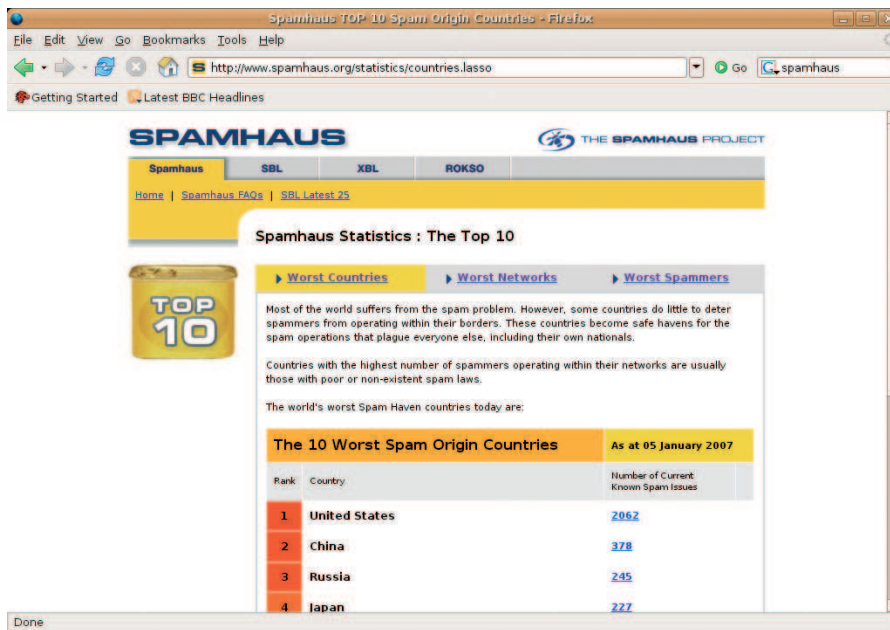


Figura 1: Spamhaus mantiene una lista de los peores países en cuanto a spam, las peores redes y los mayores spammers del mundo.

rios comenzaron a denominarlo UCE (Unsolicited Commercial Email) spam. Hoy día, la mayoría de la gente denomina a cualquier tipo de correo no solicitado simplemente spam.

El proyecto anti-spam Spamhaus [2] estima que 200 spammers generan el 80 por ciento de todo el spam en los EEUU y Europa. Como las organizaciones spammers son generalmente grupos en lugar de personas, Spamhaus supone que campan por algún lado 600 profesionales del spam. Podemos encontrar el top ten de los spammers mundiales en la página de Spamhaus [3].

Aunque la mayoría de los usuarios desprecian al spam, muchas empresas aún recurren a él. Una de las razones de que siga existiendo es que los directores de marketing no pueden resistirse a su extremo bajo coste. Los spammers cobran usualmente entre 100 y 200 dólares (80 a 160 euros) por envío masivo. El coste es tan bajo que las compañías pueden asumirlo sin afectar a sus presupuestos. Los spammers tienen un flujo constante de clientes, incluso si los correos se envían a direcciones desconocidas de manera indiscriminada.

Los spammers operan bordeando los límites de la legalidad, a veces haciéndose pasar por negocios legítimos, incluso cuando usan herramientas como gusanos y virus para generar redes de ordenadores secuestrados para sus sucios propósitos. Como dice Spamhaus,

“...algunos países hacen poco por impedir que los spammers operen dentro de sus fronteras. Estos países se convierten en paraísos seguros para las operaciones de spam que afectan a todo el mundo, incluyendo a sus propios compatriotas. Los países con el mayor número de spammers operando en sus redes suelen ser aquellos con poca o ninguna legislación referente al spam”.

Spamhaus sitúa a EEUU como el país con la mayor población de spammers con mucha diferencia, aunque de acuerdo al top ten de Spamhaus, se aprecia que países como China o Rusia son también grandes centros de distribución de spam. Según una

investigación del laboratorio de la empresa anti-malware Kaspersky, los spammers rusos ofrecen gran variedad de paquetes en función del número de direcciones, desde 100 a 3,7 millones, sin ningún tipo de restricciones de grupos objetivo. La mayoría de los anunciantes optan por el número máximo de direcciones, sin importar la audiencia.

Las empresas implicadas en actividades de spam no se preocupan de si sus acciones generan los resultados deseados. En una encuesta de Kaspersky, ninguna de las empresas encuestadas medía realmente la efectividad de su inversión en spam. Algunos encuestados suponían un impacto de sus actividades spammers en torno a un 0,01 a 0,05 por ciento de su facturación.

La Mejor Defensa

La industria informática ha desarrollado todo un arsenal de estrategias para luchar contra el problema del spam. Las fuerzas anti-spam se basan en herramientas como:

- **Listas negras y listas blancas:** Estas listas contienen las direcciones de correo de spammers conocidos (listas negras), y de remitentes legítimos y conocidos (listas blancas). Las listas blancas reducen la aparición de falsos positivos. Las listas negras suelen ser poco efectivas, ya que los spammers suelen falsificar las direcciones del remitente.
- **Listas negras y listas blancas basadas en la IP:** usan un método similar. Estas listas catalogan a los spammers a partir de su IP. Esta técnica fue útil cuando los relays abiertos eran los principales distribuidores de spam. Hoy día, las listas

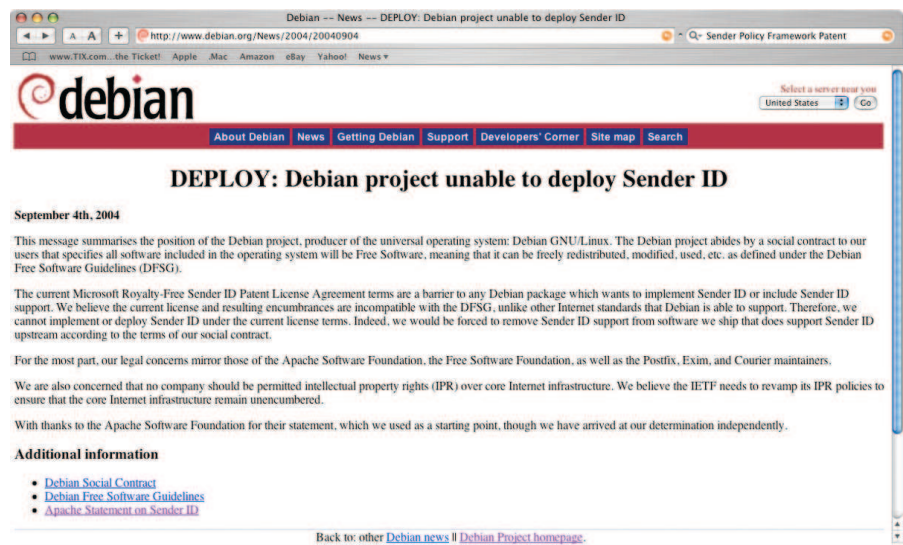


Figura 2: Los intentos de engañar a los filtros anti-spam no son siempre tan obvios como en este caso.

negras son demasiado agresivas, han llegado a bloquear todas las IP dinámicas e incluso países asiáticos enteros. Desafortunadamente, esto deja fuera de combate a muchas fuentes legítimas.

- **Listas negras basadas en URL:** Muchos correos spam anuncian páginas Web específicas. Si una URL sospechosa aparece en un correo, se puede suponer que es spam.
- **Filtros de contenido:** estos filtros analizan el contenido y tratan de separar el spam del ham mediante la detección de frases típicas de spam. Las expresiones favoritas son “pulse aquí” y “suscríbete”, así como “Viagra”. Las estrategias de combate tratan de detectar palabras clave.
- **Lazy HTML / Webbug:** se trata de un tipo especial de filtro de contenido que busca en los correos imágenes que se supone que ha de descargar el cliente de correo desde Internet. Las imágenes se sirven desde un script del lado servidor que evalúa un parámetro GET específico al mismo tiempo. Los spammers usan esta técnica para detectar si un mensaje se ha leído, verificando de esta manera sus listas de direcciones.
- **Filtros bayesianos:** al contrario que los filtros de contenido configurados manualmente, que incluyen una lista estática de palabras apropiadas, el filtro bayesiano intenta generar una lista basándose en la teoría de probabilidades. Para ello, analiza correos spam y ham y basa la probabilidad de que un correo sea publicidad no solicitada en función de la frecuencia de expresiones específicas. Los spammers tratan de confundir a estos filtros añadiendo listas de palabras aleatorias a los correos. Esta es la razón de la maraña de palabras sin sentido que acompañan frecuentemente al spam de hoy día.
- **Filtros de imágenes:** estos filtros intentan analizar el contenido de las imágenes. Los primeros filtros se limitaban a la detección del color de tonos de piel comunes en pornografía.
- **Filtros de checksum y filtros colaborativos:** los filtros colaborativos comparan los correos que llegan a muchas cuentas e intentan descubrir similitudes. La lógica es aplastantemente simple: si muchos usuarios reciben el mismo correo, probablemente sea spam. Por supuesto, esta técnica amenaza a los boletines legítimos, aunque las listas

blancas ayudan a evitar clasificaciones incorrectas. Los filtros más cautos esperan a que el usuario clasifique el correo como spam. Estos filtros aplican otros criterios adicionales para distinguir entre spam y ham. Para cumplir con la legislación de protección de datos, el filtro central sólo recibe checksums de correos recientes. El algoritmo de checksum tiene que ser a prueba de cambios menores en el contenido de los correos, ya que el método es perfectamente conocido por los spammers, quienes añaden texto aleatorio a su correo basura.

- **Listas grises:** la estrategia basada en listas grises retarda la aceptación de correo entrante, fingiendo un error temporal en las comunicaciones SMTP. En ese momento, el remitente ya habrá enviado su IP, junto con las direcciones de correo del remitente y del destinatario. El servidor de correo guarda esta información y acepta el correo si el remitente vuelve a intentarlo. La idea es que los gusanos que usan los spammers no tienen motores SMTP completos y entienden el error temporal como un error permanente. Desafortunadamente, los spammers de hoy día ya conocen este sistema y saben sortear las listas grises.
- **SPF, Sender ID, DK:** el Sender Permitted From, o Sender Policy Framework, así como el Sender ID, o la clave de dominio de Yahoo, crean un registro de DNS definiendo las fuentes desde donde un dominio específico podrá recibir email. Además de la situación incierta sobre las patentes, todos estos métodos tienen un inconveniente importante: la mayor parte del spam de hoy día se envía desde ordenadores identificados por los registros DNS como responsables del dominio. Registrar dominios y crear registros de DNS es parte del trabajo diario del spammer. Después de todo, los spammers están constantemente mejorando para sortear los filtros URL y los reportes de abusos.

Podemos esperar la aparición de más técnicas anti-spam conforme los sistemas informáticos vayan cambiando, y la historia del spam seguirá su curso.

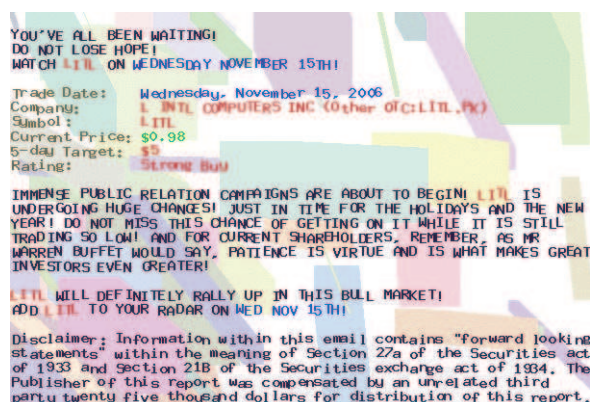


Figura 3: La propuesta Sender ID de Microsoft recibió una fría acogida desde el Proyecto Debian.

Lo Que Viene

A pesar del gran arsenal de estrategias, el spam continúa inundando los buzones por todo el mundo. Los spammers se han vuelto muy sofisticados, y son tan ingeniosos y creativos como los chicos buenos. Las campañas del pasado verano mostraron lo agresivo y sofisticados que se han vuelto sus métodos.

Los spammers han adoptado nuevas técnicas para evitar las tecnologías de huellas empleadas por los filtros anti-spam, por ejemplo, incluyendo GIFs animados a sus creaciones. Una vez que el filtro ha reconocido los patrones en el correo spam y creado su huella digital, la imagen integrada cambia de tamaño, color o posición para evitar la detección. Pequeños cambios que el receptor no notará nunca al leer el correo, ya que cambiar el color a un solo pixel puede evitar su detección.

Por tanto, la guerra armamentística continúa. No es de esperar una solución final a corto plazo. La batalla seguirá mientras los anunciantes sigan queriendo pagar por hacer spam y la infraestructura de correo electrónico mundial sea incapaz de contenerlo. Lo mejor que podemos hacer es filtrar lo que podamos e intentar evitar que nuestra dirección caiga en manos de los spammers. Siga leyendo para saber cómo puede sumarse a esta lucha. ■

RECURSOS

- [1] Estadísticas de Postini: <http://www.postini.com/stats/>
- [2] Spamhaus: <http://www.spamhaus.org>
- [3] Top ten de spammers: <http://www.spamhaus.org/statistics/spammers.lasso>
- [4] Kaspersky Lab: <http://www.aspersky.com/de/>