Spam, Spam, Spam: Cómo evitarlo y combatirlo

Javier Fernández-Sanguino
jfernandez@germinus.com
Germinus XXI, S.A., Avenida de Manoteras 44, 2ª planta, Madrid, España.
Tel: +34 91 2961234, Fax: +34 91 2961230

RESUMEN: El envío de correo no autorizado ha pasado recientemente de ser un problema "molesto" a ser un problema grave para el correcto funcionamiento del servicio de correo en Internet.

Por un lado, muchas organizaciones ven como el rendimiento de sus empleados disminuye debido a que una herramienta, como es el correo electrónico de la que dependían para su negocio, reducía su valor al llenarse sus buzones corporativos de solicitudes para renovar una hipoteca, comprar un reloj o beneficiarse de píldoras milagrosas. Pero también los usuarios domésticos se ven ya afectados por un problema que llena sus buzones de cantidades enormes de correo que no tiene para ellos interés alguno.

Para intentar evitar y combatir este problema es necesario conocer tanto el origen del mismo como su evolución, así como alguna de las tácticas utilizadas para evitarlo y combatirlo.

1 Introducción

El envío de mensajes no solicitados (también llamado *spam* [1]) es un problema muy importante asociado al servicio de correo electrónico en Internet y que afecta a todos los usuarios que lo usan cuando éstos, además de intercambiar correo interno (si forman parte de una organización) intercambian correo con otros usuarios de este servicio en Internet.

Este tipo de correo, habitualmente enviado de forma masiva, es lo que se denominaría también correo basura (por la inutilidad de su contenido), pero, en general, el contenido del correo en sí no es lo importante, sino el hecho de que la persona que lo recibe no lo ha solicitado. El correo basura suele ser *spam*, pero no todo el *spam* es correo basura para todas las personas que lo reciben. Esto lo demuestra el hecho de que un número muy pequeño de estas personas llegan a interesarse por lo que reciben y tomarán alguna acción como pueda ser comprar un producto, participar en una estafa que parece lucrativa, contratar un servicio determinado, etc.

No todas las personas con correo electrónico ni organizaciones conectadas a Internet lo sufren al mismo nivel. En el caso de las organizaciones, su impacto dependerá en gran medida de las políticas que hayan definido: tanto internas de utilización del correo electrónico (quién puede usar correo electrónico, quién puede intercambiar correo electrónico con Internet...) como las de utilización de Internet en general y también las de seguridad: esto es, de lo "protegidos" que están sus usuarios frente a ataques maliciosos del exterior.

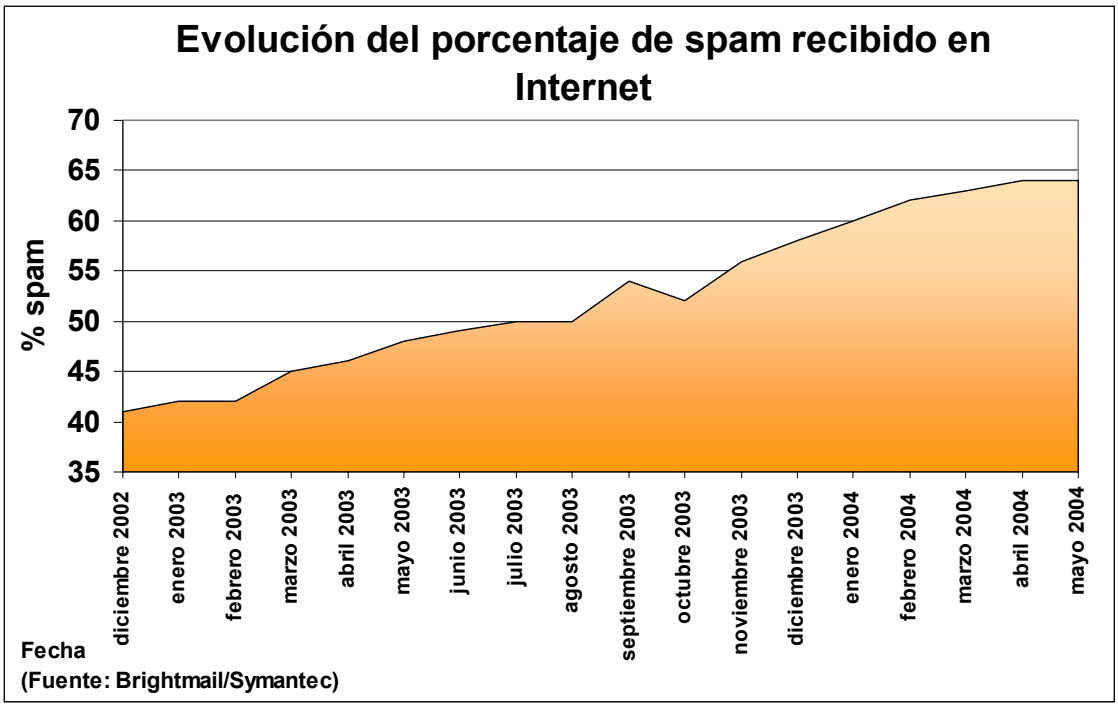
En el caso de los usuarios domésticos, dependerá del uso que le den al correo electrónico y la facilidad con la que publiciten sus direcciones de correo al utilizar otros servicios (foros, chats...)

1.1 Evolución del spam en Internet

Existen fuentes que citan el comienzo del *spam* en el año 1994. El 12 de Abril de dicho año un abogado estadounidense, Laurence Canter y su mujer, Martha Siegel, utilizaron un programa informático para ofrecer los servicios de su bufete a seis mil foros de Internet (grupos de USENET) algo que molestó a varios millones de usuarios y tuvo como consecuencia (por los ataques en respuesta que sufrieron) su desconexión de Internet y, posteriormente, la pérdida de su licencia de abogados [2].

En realidad, es posible que el primer *spam* generado lo fuera en 1978, cuando Gary Thuerk un comercial de la empresa DEC, envió un mensaje anunciando sus nuevos sistemas informáticos. Entonces Internet era aún Arpanet, y el envío de un mensaje [3] a casi seiscientas personas también causó malestar generalizado si bien éste tenía interés para algunos de los que lo recibieron.

El uso del término *spam* para relacionarlo con la recepción de información no deseada surge probablemente [4] en Internet en los años 80 dentro de un tipo de juegos de rol en línea llamados MUDs (*Multi-User Dungeons*). Proviene de un famoso *sketch* del grupo cómico inglés Monty Python en el que unos vikingos dentro en una tienda acompaña con una molesta canción la insistencia del propietario de que toda la comida que proporciona está hecha con



spam[1]. En los años 90 se empieza a utilizar este término para asociarlo a los mensajes no solicitados, que ya empezaba a inundar a los grupos de noticias trasladándose rápidamente a otro servicio de Internet: el correo electrónico.

El correo no solicitado, aún sin existir estadísticas muy fiables, se estima que ha ido creciendo de forma exponencial, siendo, hoy en día un problema acuciante para muchas personas y organizaciones. Algunas personas que empezaron a enviar de forma masiva, tras ser reprendidos, se dieron cuenta de su error, otras se han acabado convirtiendo en profesionales del método, conocidos como *spammer*, que hacen uso de todo tipo de tácticas para asegurar que son capaces de enviar correo a todos los puntos del planeta. Estos "profesionales" incluso ofertan sus servicios a compañías privadas.

Actualmente se calcula que entre el 65% y el 75% [5] [6] del correo recibido en Internet en el año 2004 ha sido *spam* y la situación no hace sino agravarse con el paso del tiempo (como se muestra en la figura).

El *spam* en Internet se trata de un problema global ya que tanto los sistemas que generan el correo basura como los responsables de su envío están distribuidos por todo el mundo.

No existen aún medidas capaces de eliminarlo por completo, aunque ya fuera un problema reconocido desde 1975 [7] por Jon Postel, co-creador del correo electrónico.

1.2 Evolución del spam en España

No existen datos muy concretos que permitan determinar el crecimiento real del problema del correo no solicitado en España ya que sólo recientemente han surgido iniciativas paliativas con relación al correo basura.

El proyecto Sísifo [8], realizado por la Universidad de Zaragoza y Rediris junto con otras cuatro universidades españolas, ha instalado múltiples sondas para analizar la incidencia del *spam* en las redes universitarias.

En base a la información extraída por estas sondas se estima[2] que entre el 45% y el 50% del correo recibido por estas cinco universidades españolas es no solicitado (de 120.000 correos diarios) y que, aproximadamente, el 50% de las conexiones recibidas por los servidores de correo de dichas universidades son de otros sistemas que sólo envían este tipo de correo.

De la información estadística ofrecida por el proyecto es fácil observar como, del correo no solicitado generado desde España, tiene su origen, fundamentalmente, en equipos ubicados en conexiones de banda ancha como las proporcionadas por Auna, Telefónica, Ono y otros proveedores de Internet.

Estos equipos, controlados de forma remota por los *spammers*, son habitualmente sistemas de usuarios que, sin su conocimiento, están siendo utilizados para enviar este tipo de correos. Habitualmente se les conoce como

[1] *SPAM* (en mayúsculas) es una marca registrada de la compañía norteamericana Hormel Foods Corporation y se refiere a un tipo de carne procesada (el acrónimo oficial es *Specially Processed Assorted Meat*, anteriormente *Spiced Ham*)

[2] Hay que hacer hincapié en que es detectado, puede incluir tanto falsos positivos como negativos.

equipos zombis, por el hecho de que están a las órdenes (sin conocimiento de su propietario) de terceras entidades para llevar a cabo sus actividades.

Es más, esta es la misma tendencia que se ha producido ya anteriormente en otros países, como Estados Unidos, en el que las fuentes de correo no solicitado son millones de ordenadores contaminados y utilizados para enviarlo. Claramente, el nivel de población y de penetración de Internet en España afecta a la participación de sistemas españoles en esta actividad. Sin embargo, numerosos informes [5] [9] indican que España se sitúa entre los veinte países que más sistemas tiene que envían correo no solicitado, un 1-2% del total de sistemas en el mundo. Muy por detrás[3], en cualquier caso de Estados Unidos (por encima del 40%), Corea del Sur (en torno al 19%) y China (en torno al 11%) que ocupan los primeros puestos en número de sistemas.

1.3 Los objetivos del spam

Si bien algunos mensajes no deseados tienen como objetivo la difusión de mensajes filosóficos, políticos o incluso religiosos enviados por personas comprometidas con una causa. Éstos suponen hoy en día una pequeña parte del correo no deseado, ya que la gran mayoría del spam tiene fines lucrativos.

Según un estudio realizado por la empresa Brightmail [5], aproximadamente un 14% del *spam* a lo largo del 2004 está asociado a fraudes, y un 80% a la oferta de servicios o compra de productos.

Claramente, son los fines lucrativos los que mueven a los *spammers* a enviar cantidades ingentes de correo, pero ¿realmente merece la pena? La respuesta es que sí, sólo basta hacer unos cálculos muy sencillos. El coste de enviar un correo no solicitado para el *spammer* es muy bajo (casi nulo si se usan técnicas ilegales) y la venta de un producto que le interesa a un porcentaje muy pequeño (digamos, un 0.1%) de la población puede dejar un determinado margen (digamos que dos euros). Más aún si lo que se venden son productos comunes (como por ejemplo, una aspirina) como si fueran productos milagrosos a precios elevados. Si el *spam* se envía a un millón de personas los beneficios de un sólo envío indiscriminado serán de dos mil euros. Parece razonable pensar que, a más direcciones, más lucro, hasta llegar al sueño de muchos *spammers*, disponer de todas las direcciones de los usuarios de Internet del planeta.

En una entrevista publicada en Internet [10] un *spammer* holandés detalla pormenorizadamente el gasto que le supuso el envío indiscriminado de correo y los réditos que éste le supusieron. Después de enviar correo de forma indiscriminada durante 25 días, utilizando la información de una base de datos de direcciones de correo que previamente había adquirido, el *spammer* calcula haber ganado entre dos mil y tres mil euros. Ciertamente, una actividad suficientemente lucrativa.

Sin embargo, estas mismas direcciones de correo y las mismas tácticas del *spammer* pueden ser utilizadas para llevar a cabo ataques aún más lucrativos si estos son fraudulentos o tienen fines ilegales. Por esto recientemente se han empezado a observar ataques dirigidos a usuarios de entidades bancarias con el afán de engañarles y obtener las contraseñas de acceso a sus cuentas para así poder transferir su dinero a otras cuentas. Estos ataques, conocidos como *phishing*, han afectado a un elevado número de entidades conocidas, incluyendo[4] servicios en Internet (American Online, Amazon, eBay, MSN, Paypal, Yahoo!), bancos norteamericanos (Bank of America , Barclays, Citibank, SunTrust, U.S. Bank), alemanes (Deutsche Bank, Postbank), españoles (Banesto, Banco Pastor, BBVA, BBK, Caja Madrid), e ingleses (NatWest), entre otros.

La táctica para llevar a cabo estos ataques es similar, enviar correo no solicitado a millones de direcciones, esperar que alguno de éstos usen los servicios bancarios que se están suplantando y que caigan en la trampa. El crecimiento de este tipo de ataques a lo largo del año 2004 ha sido gigantesco, en su estudio [6], la compañía MessageLabs indica que ha detectado 18 millones de correos asociados a ataques de *phishing* en 2004.

1.4 Tácticas para la recolección de direcciones de correo

Los *spammers* hacen uso de distintas técnicas para obtener las direcciones de correo a las que luego envían correo de forma indiscriminada. Algunas de estas técnicas utilizan información pública y otras pueden

[3] Según las estadísticas proporcionadas por la compañía Commtouch

[4] Pueden encontrar más información y ejemplos de ataques de phishing en http://www.antiphishing.org/phishing_archive.html y http://www.fraudwatchinternational.com/internetfraud/phishing/phishing_index.htm

llegar a considerarse un delito en mucho países. Las utilizadas más frecuentemente son:

- Recogida de información publicada en grupos de noticias (USENET), servidores web, salas de chat y listas de correo (incluso suscribiéndose a las mismas). De éstos extraen no sólo direcciones de correo de usuarios (de las cabeceras de los mensajes) sino también servidores de correo o pasarelas existentes en Internet.
- La utilización de diccionarios de palabras y nombres comunes contra servidores de correo para identificar direcciones válidas en éstos.
- El ataque a sistemas informáticos, bien a través de intrusiones remotas (habitualmente a líneas con conexión a Internet doméstica), o bien a través del envío de virus o troyanos. El objetivo es hacerse con el control del ordenador personal de un usuario para recoger información de las direcciones de correo que éste almacena en su equipo (libreta de direcciones, correos enviados y recibidos, etc.)

Se han realizado varias pruebas [11] [12] para evaluar la capacidad de los *spammers* para obtener direcciones de correo. Estas pruebas muestran que de las direcciones publicadas en servidores web conocidos, un 86% al 97% son recogidas y utilizadas en un plazo inferior a un mes por los *spammers*. El porcentaje para el caso de direcciones de correo utilizadas para publicar información en foros de USENET es cercano al 85%. Si bien el porcentaje se reduce en el caso de direcciones publicadas en servidores web poco publicitados (un 50% de las direcciones publicadas en páginas personales) o en otros servicios (como las bases de datos de *whois*) que aún no están siendo aprovechados.

Algunas veces los *spammers* utilizan distintos mecanismos para comprobar si las direcciones así obtenidas son válidas. Por ejemplo, una táctica habitual consiste en enviar un correo a la dirección y comprobar si el correo se recibe o "rebota" o bien se envían correos con imágenes incrustadas (que muchos programas de correo mostrarán de forma automática) cuyos nombres incluyen marcas identificativas y están disponibles en servidores en Internet. Una vez enviado el mensaje, el *spammer* analiza los registros de acceso al servidor de donde el usuario intenta recoger la imagen. Así, puede identificar fácilmente si el correo utilizado está siendo o no leído realmente. Igualmente, muchos mensajes de correo basura incluyen indicaciones del procedimiento que debe seguirse para darse de baja de la listas de correo en la que el usuario ha sido incluido. En realidad, cuando el usuario sigue estas indicaciones, lejos de borrar su dirección, ayuda a confirmar al *spammer* que una persona efectivamente está leyendo esa dirección de correo.

Los grupos que se dedican a este oscuro negocio se intercambian estas listas de direcciones. Además, las ponen a la venta (muchas veces haciendo sus ofertas a través de más correos basura), distribuyéndolas en CD-ROMs. No se han realizado muchos análisis de estos CD-ROMs, pero Rejo Zenger, investigador holandés miembro de una fundación anti-spam, ha publicado un análisis [13] que indica que, tras eliminar direcciones sintácticamente incorrectas, direcciones genéricas y duplicadas, el CD-ROM contenía alrededor de seis millones de direcciones de correo válidas. Menos direcciones de las que prometía el vendedor (poco más de la mitad) pero aún así un número muy elevado.

En la actualidad algunas de las formas utilizadas por los *spammers* para obtener direcciones de correo pueden ser evitadas:

- Mediante una correcta configuración o supervisión de los sistemas de correo, si se evita enviar información a usuarios externos de direcciones de correo legítimas con respuestas automáticas o si se controla el envío y recepción de "cadenas de mensajes" a y desde Internet.
- Con un correcto control de los ordenadores personales (o corporativos), para evitar la infección de troyanos o virus.
- Con una correcta configuración del programa utilizado por un usuario como su cliente de correo para evitar enviar información que pueda ayudar a un *spammer* incluyendo: evitar la carga automática de imágenes (u otros contenidos) de servidores remotos, no enviar respuestas automáticas a correos (incluyendo los acuses de recibo, los mensajes de vacaciones o ausencias temporales), etc.

También es necesario concienciar a los usuarios finales de aquellas actividades que pueden convertirles en objetivo del *spam*, incluyendo la instalación de software ilegal, la introducción de información personal en servidores no confiables, o la compra de productos anunciados a través del *spam*.

1.5 Consecuencias del spam en Internet

Las consecuencias del *spam* en Internet son nefastas. Atacan a un servicio "estrella" de Internet: el correo electrónico, haciendo que su usabilidad se vea reducida, y obliga a los usuarios de éste a lidiar con el correo no

solicitado que reciben, discriminando qué correo es legítimo, cuál no lo es y borrándolo de sus buzones. Al final, cuando el volumen de *spam* es insoportable, el usuario se ve forzado a abandonar la dirección de correo y utilizar otras direcciones como sus direcciones personales.

El hecho de que los *spammers* dispongan de un elevado número de direcciones de correo válidas también hace posible que aquellos individuos que tengan la intención de difundir un ataque, como pueda ser un nuevo virus, un troyano o algún otro ataque especializado (como los ataques de *phishing*) pueda extender más fácilmente el contenido malicioso a muchas más víctimas potenciales. La difusión inicial y la propagación de estos ataques es consecuentemente mucho mayor.

Esto lleva, al final, a una pérdida de confianza de los usuarios en la propia tecnología, con consecuencias sobre los servicios electrónicos, incluido el comercio, y va directamente en contra de los esfuerzos que realizan los organismos y empresas para desplazar servicios tradicionales (desde la compra de entradas de cine a la oferta de servicios de la administración pública) a Internet.

2 Cómo abordar el problema

El problema del *spam* se debe abordar desde distintos frentes. Desde un punto de vista local, las organizaciones que sufren el problema del *spam* tienen que implementar soluciones para evitar que éste alcance dimensiones poco manejables para sus usuarios y deberán tratar el problema como un riesgo más asociado a la utilización del correo electrónico en Internet. Más adelante se detallarán algunas estrategias que se pueden seguir para intentar abordar el problema del *spam* dentro de una organización (empresa, institución, etc.).

Las soluciones en el ámbito local, sin embargo, deben considerarse soluciones a corto o medio plazo ya que, si bien pueden evitar la aparición, o reducir la incidencia del correo no solicitado, se hace a costa de recursos de la organización (ya sean personales o materiales) y, a medida que aumente el fenómeno del *spam* en Internet, también lo harán los recursos que este fenómeno consume.

Las soluciones en el ámbito global para este problema son más complejas. Por un lado, se debe llevar a cabo cambios en los sistemas de intercambio de correo electrónico para intentar reducir la incidencia del *spam* o hacer más fácil su detección y eliminación. Por otro, se deben abordar cambios en la seguridad de los sistemas informáticos (tanto en los sistemas finales de los usuarios o de las empresas como en los sistemas de los proveedores de acceso a Internet) para hacer más difícil que los sistemas informáticos sean utilizados para estos envíos indiscriminados y para que, en caso de detectarse un envío de correo masivo, se pueda determinar su fuente con exactitud y atajar el problema. Esto, claro está, sin perder de vista que el problema del *spam*, hoy en día asociado al correo electrónico, puede extenderse con facilidad a otras tecnologías y que puede ser necesario, por tanto, adaptar las soluciones adoptadas para este servicio a otras tecnologías en Internet o diseñar las nuevas tecnologías teniendo presente esta amenaza.

2.1 Estrategias globales contra el spam

No existen aún soluciones, ni técnicas ni políticas, para hacer que el *spam* desaparezca, o reduzca su incidencia de forma significativa, en Internet.

Tampoco existe aún, desafortunadamente, un consenso en las modificaciones que deben realizarse al sistema de intercambio de correo electrónico (el protocolo SMTP o la infraestructura utilizada en Internet para transmitir correos) para reducir la incidencia de éstos.

2.1.1 Asegurar la identidad del remitente

Una de las razones que impiden que sea posible determinar el origen de un envío masivo de correo, y, por tanto, permitir tomar medidas al respecto, es la arquitectura actual de correo en Internet. El protocolo SMTP, descrito en el RFC 2821 [14], define el estándar de intercambio de correo electrónico entre clientes de correo y servidores y de servidores entre sí. Este protocolo está basado en una confianza implícita entre los servidores de correo y en, cierta medida, también en la confianza de que los remitentes son quienes dicen ser.

Un número muy elevado del correo no solicitado enviado hoy en día utiliza, sin embargo, direcciones de correo inexistentes. En algunos casos, se utilizan direcciones de correo válidas (extraídas de las mismas bases de datos utilizadas para el envío) pero que nada tienen que ver con el *spammer*. Esto hace muy difícil trazar el correo no solicitado [15]

¿Cómo vende un *spammer* sus productos entonces? Sencillamente dirigiendo a los compradores interesados en los correos no solicitados a direcciones de servidores web en los que se puede llevar a cabo la transacción comercial.

Por esto los usuarios normales, no acostumbrados al problema, responden con sus quejas al usuario original que, o bien no existe, o bien nada tiene que ver con el *spammer*. Generando intercambios de correos inútiles que o serán devueltos (porque el remitente no existe) o serán respondidos con sorpresa por parte del remitente. Además, para rizar el rizo, dado que, como se ha visto antes, las direcciones utilizadas por los *spammers* pueden no existir o ser inválidas, los servidores que reciben el correo para el dominio de dicha dirección responden con un mensaje de error automático a la dirección de origen, con la generación de un nuevo ruido producido por el intercambio de correos.

Esto tiene como consecuencia reciente el hecho de que los usuarios puedan llegar a hacer caso omiso de las respuestas automáticas de errores de usuarios inexistentes, por llegarles éstas con la misma periodicidad que el *spam*. O que, sencillamente, muchos administradores hayan configurado sus pasarelas de correo de forma que no respondan automáticamente cuando se producen estos errores y descarten de forma silenciosa correos enviados a usuarios inexistentes. Esto hace que a veces un remitente (legítimo, y no un *spammer*) asuma que un correo ha llegado a su destino cuando en realidad ha enviado un correo a una dirección equivocada y este ha sido descartado.

La única forma efectiva de identificar la fuente del *spam* es a través de un análisis detallado de las cabeceras del correo recibido. Algunas de estas cabeceras, generadas por sistemas intermedios que el *spammer* no controla, ayudan a determinar el sistema real que ha originado el envío (su dirección IP). Sin embargo, este sistema no está, en muchos casos, relacionado con el *spammer* sino que está siendo utilizado por éste para el envío del correo, puede ser un ordenador doméstico, o un servidor proxy o una pasarela de correo mal configurada. Lo único que se puede hacer en estos casos es reportar el problema al responsable del sistema (o con el responsable administrativo del rango de direcciones IP en las que está ubicado, generalmente el proveedor de acceso) y esperar a que éste lo resuelva.

2.1.1.1 Certificación digital de remitente

Sólo es posible garantizar con seguridad la corrección del remitente (el valor del campo *From:* en un mensaje) cuando el correo ha sido firmado, utilizando para ello certificados públicos digitales con una cadena de confianza suficiente.

Ésta puede ser una práctica útil dentro de una organización, o en el ámbito estatal (si los ciudadanos de un país tienen certificados digitales y saben utilizarlos), y es ya una realidad para los usuarios de correo que hacen uso de certificados PGP ó GPG de manera informal.

Sin embargo, la extensión de esta práctica a nivel global es difícil, por la propia dificultad de extender sistemas de criptografía de clave pública a nivel mundial. Cabe recordar que aún no existen autoridades de certificación a ese nivel y es posible que no existan en mucho tiempo

Dejando de lado (pero no olvidando) la posibilidad de la certificación del remitente con mecanismos criptográficos, no existe un mecanismo para asegurar que el remitente del correo es quien dice ser.

Sin embargo, sí se están desarrollando mecanismos para que se pueda determinar qué pasarelas de correo son las que deberían enviar mensajes asociados a un determinado dominio de correo. Si bien aún no existe un estándar concreto.

El objetivo de estos sistemas es que los propietarios de un dominio concreto puedan decir: "éstos son los servidores de correo que están autorizados a enviar correo diciendo que viene de mi dominio". En este caso se trata de certificar el dominio en el *From* del "sobre" de un correo electrónico (como se define en el RFC2821 [8]), no de verificar el remitente indicado en el cuerpo del mensaje, que es la dirección de correo electrónico origen del mismo (definido en el RFC2822 [16]).

Han surgido múltiples iniciativas compitiendo entre sí, y la gran mayoría de ellas usa el servicio de nombres (DNS) para que los responsables de los dominios almacenen información indicativa de los servidores de correo reconocidos para el dominio. Básicamente, un servidor de correo que reciba una conexión de otro sistema, contrastaría la dirección IP de éste con las direcciones IP publicadas por los administradores del dominio en la información del DNS. Si esta dirección se encuentra dentro de las direcciones (o redes) indicadas, se permitiría el envío de correo, en caso contrario, se rechazaría.

La solución técnica que parece haber cobrado más fuerza es SPF (*Sender Policy Framework*) [17], una solución para la que ya existen implementaciones para los programas de transporte de correo más utilizados (Courier, Exim, Microsoft Exchange, Postfix, Qmail, y

Sendmail). La propuesta inicial promulgada por Microsoft (Caller-ID) ha terminado fusionándose con SPF para constituir una nueva propuesta (Sender-ID [18]) que intenta ofrecer autenticación del remitente final (no del sistema que envía el correo).

Casualmente, el afán de Microsoft por patentar estas técnicas ha llevado a que el grupo de trabajo de la *Internet Engineering Task Force* (IETF) que las desarrollaba (MARID [19]) tuviera que disolverse en agosto de 2004.

Aunque aún está por ver el grado de implementación de esta última propuesta, SPF ya está siendo utilizada por un elevado número de dominios.

Este tipo de soluciones no tiene como objetivo solucionar el problema del *spam*, sí pueden ayudar a determinar si el dominio de un correo ha sido falseado (porque lo envía una pasarela no reconocida por los administradores del dominio), algo que puede ser indicativo¡ del intento de envío de *spam*.

En el caso de que los *spammers* utilicen también ellos mismos este mecanismo, como ya está sucediendo con SPF, no se podría utilizar la comprobación para identificar *spam*. Sin embargo, esto permitiría asociar el correo no solicitado a una serie de dominios concreto, y así facilitar la capacidad de reportar el incidente y de intervenir en contra del responsable administrativo del dominio, los servidores de correo de éste o el proveedor de acceso a Internet que le proporciona la conectividad.

Además, de llegar el caso en que todos (*spammers* y remitentes legítimos) utilizaran registros SPF, se podrían entonces introducir esquemas de reputación de dominios de forma que, por ejemplo, un dominio reconocido y suficientemente acreditado dispusiera de mayor credibilidad que un dominio recién creado o de un dominio que se sabe está siendo utilizado para enviar correo no solicitado. Este esquema de reputación facilitaría, consecuentemente, el que los administradores de los sistemas de correo decidieran retardar el envío (o descartar) mensajes asociados a dominios de mala reputación algo que, hoy en día, no es posible debido a la falsificación de cabeceras que utilizan los *spammers* para ocultar su identidad. Igualmente, se reduciría el ruido que genera en el sistema de correo en la actualidad los correos de error devueltos a usuarios legítimos cuando se falsean sus direcciones para enviar correos no solicitados.

2.1.1.2 Eliminación de las pasarelas de reenvío

Los mecanismos de envío de mensajes basado en almacenamiento y reenvío (*store & forward*) dan pie a la utilización de pasarelas intermedias (o *relays*) que pueden utilizar tanto clientes como servidores para enviar correo dirigido a otros servidores distintos. Supuestamente estas pasarelas han de incluir identificación del servidor previo, pero en algunos casos (debido a una mala configuración) esto no es así.

La mala utilización de estas pasarelas de correo por parte de los *spammers* hace que baste tener un sistema de correo conectado a Internet mal configurado, es decir, que permita el reenvío de correo desde cualquier sistema en Internet, para que una organización se incluya en algunas de las listas negras utilizadas para el control de *spam* (algunas de las denominadas RBLs o *Real-Time Block List* [20]).

De hecho, en la actualidad, la gran mayoría de las conexiones de envío de correo se realizan contra los sistemas encargados de gestionar un dominio (identificados por los registros MX, de *Mail eXchange*, en el DNS) sin utilizar pasarelas de reenvío.

2.1.2 Mayor seguridad de los equipos en Internet

Actualmente los *spammers* hacen uso de sistemas conectados a conexiones de banda ancha y con conexión permanente a Internet como "plataforma" no sólo para enviar correos electrónicos de forma masiva sino para otro tipo de ataques en Internet (como pueden ser ataques de denegación de servicio).

Muchos grupos de *spammers* tienen bajo su control redes enteras con centenares de ordenadores dispuestos a enviar correo por ellos cuando así se lo solicitan. Se estima [21] que cerca de un millón de ordenadores pueden formar parte de estas redes de control y que son responsables del envío del 90% del correo no solicitado.

Esto no sólo hace más difícil trazar el origen de este tipo de ataques, sino que además facilita a los *spammers,* como ya se ha descrito, la recogida de direcciones de correo legítimas a través de la inspección de los ordenadores domésticos y de sus buzones de correo.

También muchos *spammers* hacen uso de servidores conectados a Internet mal configurados y que pueden ser utilizados como pasarelas para enviar correo no solicitado al mismo tiempo que ocultan el origen real del correo. Muchos de estos equipos residen en

países tecnológicamente poco avanzados, pero también se da en países desarrollados cuando la instalación de los equipos la realiza personal no especializado.

Es posible que parte de la responsabilidad de resida en aquellos que desarrollan sistemas operativos o aplicaciones que utilizan configuraciones "por omisión" poco seguras para su conexión a Internet.

La inseguridad latente en los ordenadores personales de usuarios domésticos es evidente, ya un análisis [22] realizado en 2001 demostraba que un equipo doméstico recién instalado con Windows 98 y conectado a Internet era comprometido en menos de 24 horas, el mismo experimento [23] en el año 2004 el tiempo de vida de un equipo con Windows XP con SP1 antes de ser comprometido es de cuatro minutos y de menos de ocho horas para un equipo con Windows Small Business Server 2003[5]. Basándose en los ataques recibidos por sus sensores, el *Internet Storm Center* estima [24] que el tiempo en que un sistema con Windows XP SP1 puede infectarse de forma automática ha bajado de alrededor de 40 minutos en junio de 2003 a menos de 20 minutos en noviembre de 2004. Un tiempo muy por debajo del que se tarda en descargar los últimos parches del fabricante desde Internet.

2.1.3 La batalla legal contra el spam

En muchos países se ha abogado por una solución legislativa nacional contra el *spam*. La Directiva de la Unión Europea 2002/58/EC, del 12 de julio de 2002 [25] ya hace referencia (en su artículo 40) a la necesidad de un consentimiento previo de la persona para el caso de las comunicaciones enviadas para el marketing directo (independientemente del método utilizado, ya sea fax, correo electrónico o SMS)

En concreto, en España, la Ley de servicios de la sociedad de la información y del comercio electrónico [26] (habitualmente denominada LSSI) prohíbe el envío de comunicaciones comerciales sin consentimiento previo, dejando un tratamiento en mayor profundidad a los códigos de conducta de corporaciones, asociaciones y organizaciones comerciales, profesionales y consumidores. Además, independientemente de la utilización, comercial o no, del correo electrónico la Ley Orgánica de Protección de Datos de carácter personal española especifica los actos permitidos para la recogida de información personal, como pudiera ser el correo electrónico y castiga el mal uso de la información personal. Otras legislaciones comunitarias, como la legislación francesa, belga, austriaca, danesa, finlandesa, italiana y del reino unido contienen medidas similares.

Existen leyes más tardías contra el envío no solicitado como puede ser la ley 108-187 (conocida como CAN-SPAM ACT) norteamericana de diciembre de 2003 [27]. Esta ley no criminaliza el envío de correo no solicitado, por lo que ha tenido muchos detractores, pero sí criminaliza la utilización de pasarelas para ocultar el remitente y el hecho de no responder a las solicitudes del usuario de excluirse de la lista de correo. En cierta medida la ley estadounidense debería obligar a los *spammers* a utilizar sus propios servidores con lo que debería ser posible trazar su actividad.

La ley contra los mensajes electrónicos no solicitados con fines comerciales (*Spam Act*) australiana [28], aprobada también en diciembre de 2003, exige consentimiento previo, la inclusión de información válida del remitente, y la respuesta obligada del remitente a las solicitudes de eliminación de la lista, imponiendo sanciones muy elevadas en caso de incumplimiento. Además, al igual que la legislación española, la ley de protección de datos australiana (*Privacy Act*) ilegaliza la recogida indiscriminada de direcciones de correo sin consentimiento del usuario final.

Sin embargo las leyes contra el *spam* ven reducida su eficacia al tratarse de un problema que, como muchos otros relacionados con redes telemáticas mundiales, tiene un ámbito que supera al nacional. Así, existe un gran número de países sin legislación específica que se pueden convertir en países utilizados por los *spammers* para ocultar sus verdaderas identidades y mantener su negocio en marcha.

Hay que tener en cuenta que, según la lista ROKSO [29] de Spamhaus, un proyecto dedicado a combatir el *spam* en Internet, sólo son doscientas organizaciones o personas individuales las responsables del envío del 80% del *spam* que se genera en Internet. Un efecto inmediato de estas legislaciones ha sido la detención de algunos *spammers* reconocidos o una reducción (o abandono) de su actividad al considerarse ilegal en el país en el que estos residen. Conviene recalcar que casi un 77% de

[5] Otros sistemas: Windows XP SP1 con un cortafuegos personal, Windows XP SP2, Linspire (Linux) y MacOS X no fueron comprometidos durante el experimento que duró dos semanas.

las organizaciones listadas en el índice ROKSO tienen sede en Estados Unidos.

Estas leyes están siendo utilizadas para detener y juzgar a *spammers* por su incumplimiento. Aún siendo Estados Unidos, como se ha indicado, la mayor fuente de *spam*, no se ha notado aún el efecto del *CAN-SPAM Act* a lo largo del año 2004. Por ello está aún por ver un efecto importante de estas legislaciones en el nivel de *spam* que se genera en Internet.

2.2 Estrategias locales contra el *spam*

Una organización que quiera evitar los problemas que el correo no solicitado genera en su propia infraestructura y en sus usuarios debe desarrollar soluciones con distintos enfoques. Por un lado se pueden plantear soluciones técnicas al problema y, por otro, también son necesarias soluciones de tipo organizativo y social.

En cualquier caso, las soluciones reducirán el riesgo asociado con una conexión a Internet, pero no lo eliminarán por completo. Realmente, la única solución que puede evitar que el problema del *spam* desaparezca de forma irremisible es el no intercambiar correo electrónico con Internet, una solución algo drástica y, en muchos casos, inviable. Así pues, habrá que asumir que cualquier solución introducida podrá paliar el problema, en mayor o menor medida, pero no lo resolverá por completo. Generalmente una combinación adecuada de distintas soluciones puede ayudar a reducir el problema en mayor medida que una solución en exclusiva, por muy bien que ésta se lleve a cabo.

Algunas soluciones organizativas serían:

- La definición de una política corporativa en cuanto a la utilización del correo electrónico en la organización, que especifique tanto las actividades permitidas como las no permitidas en relación con el uso del servicio de correo.
- La formación del personal técnico para que éstos realicen una correcta configuración y supervisión de los sistemas de correo, de forma que sean capaces de reaccionar ante un incidente asociado al envío masivo de correo no solicitado.
- Proporcionar información a los usuarios sobre la política de uso definida por la organización, los problemas del correo no solicitado, los mecanismos para evitar el problema, así como las actuaciones recomendadas en el caso de detectar un problema relacionado con el correo no solicitado.

Las soluciones técnicas al spam son muy variadas y podrán implementarse unas u otras en función de los requisitos de la organización. Es decir, no adaptará la misma solución un proveedor de acceso a Internet que una organización. El primero debe ofrecer un sistema de filtrado de correo como medida de protección a un elevado número de usuarios dispares, el segundo debe introducir un sistema de filtrado que implemente las políticas de uso internas, obligando su cumplimiento.

En general suelen consistir en la instalación de sistemas de filtro de *spam* (mediante sistemas específicos de filtrado) y en la instalación de sistemas para reducir el impacto del *spam* a través del control de las comunicaciones a nivel de red de la organización (implementando sistemas de gestión de ancho de banda).

2.2.1 Sistemas de filtrado

Los sistemas de filtrado disponibles en la actualidad se pueden dividir en función de su ubicación y en función de la tecnología que utilizan. En la mayor parte de los casos es recomendable combinar los distintos sistemas de filtrado disponibles ya que son complementarios entre sí.

2.2.1.1 Ubicación de los sistemas de filtrado

En función de su ubicación se puede hablar, al igual que en el caso de tecnologías de anti-virus, de filtrado en la pasarela de la organización (se aplican habitualmente los mismos filtros a todos los usuarios), es decir, en los MTAs (*Mail Transport Agent*), o de filtrado en el cliente de correo, es decir, en los MUA (*Mail User Agent*).

Los sistemas de filtrado de pasarela tienden, por tener que aplicarse a un conjunto mayor de usuarios, a ser menos adaptables y a tener políticas de filtrado relativamente permisivas, es decir, no se pueden permitir falsos positivos (mensajes reconocidos como *spam* cuando en realidad no lo son). En este último caso el usuario deseará recuperar el correo y los mecanismos para ello pueden no estar disponibles o ser de utilización compleja (puede ser necesario proporcionar acceso a la pasarela). Esto obliga a que los mensajes descartados en la pasarela tengan que ser revisados manualmente por los administradores en caso de que se desee su recuperación.

Sin embargo, es en la pasarela donde una organización es capaz de aplicar aquellos filtros que más se adecuen a la política de uso que haya definido.

Estas pasarelas podrán estar instaladas como primera punto de entrada de correo a la organización (directamente expuesta a Internet) o tras la pasarela de primer nivel de la organización, que realizaría un almacenamiento temporal del correo entrante.

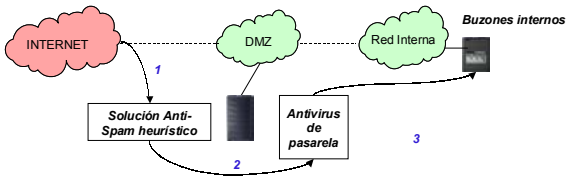


Ilustración 1: Instalación habitual de una solución anti-spam en pasarela

En el caso de que exista una pasarela con capacidad de detección y eliminación de virus, su instalación podrá ser anterior (como se muestra en la Ilustración 1) o posterior a la misma. No existe realmente una configuración óptima ya que la instalación dependerá, del nivel de virus y spam que reciba la organización y de los recursos que consuman las soluciones utilizadas anti-virus y anti-spam.

En general las pasarelas de correo entrante podrían:

- Rechazar el correo y generar un rebote (*bounce*) al remitente cuando se detecta que es spam. Si bien esto era aceptado hace algunos años ya no lo es ya que, como se ha comentado previamente, la gran mayoría de las direcciones origen son falseadas rutinariamente y, de enviarse un rebote, se enviaría a un tercero que en realidad no ha enviado el correo.
- Aceptar el correo e introducirlo en una cuarentena cuando se determina que es basura. La cuarentena se convierte en un elemento adicional a gestionar, ya que los usuarios querrán extraer de la misma correos legítimos mal identificados.
- Aceptar el correo, marcarlo como correo no solicitado (añadiendo cabeceras específicas o cambiando alguna cabecera, habitualmente el asunto del mensaje) y tramitarlo, dejando al cliente de correo que decida qué hacer con él.
- Rechazar el correo dentro de la comunicación SMTP (generando errores 5xx o 4xx) cuando se determina que es basura basándose en el análisis dado por las reglas o filtros implementados.

Esta última forma evita el *spam* generado por sistemas zombi ya que éstos habitualmente no reintentan el envío, algo que sí harán las pasarelas de correo legítimas bien configuradas. También se puede implementar una solución denominada *greylisting* [29] en la que se bloquean temporalmente los sistemas no conocidos, anotando su acceso en una base de datos. Posteriormente, si se realiza una nueva conexión del mismo sistema se acepta el correo si el remitente y receptor coinciden con el intento de envío anterior. Esto reduce el correo basura a costa de introducir un retardo en el correo recibido de servidores desconocidos, ya que se fuerza un reenvío para éstos. Como ventaja adicional, un sistema no podrá introducir correo si falsean (utiliza de forma aleatoria) las direcciones de remitente o destinatario.

Los filtros de *spam*, especialmente cuando se basan en filtrado de contenidos (análisis de mensaje) suponen un importante esfuerzo computacional con lo que su tasa de entrada (o salida) de mensajes será inferior a la soluciones de pasarela de correo tradicionales (sendmail, postfix, etc.). Así, puede ser recomendable una pasarela previa que almacene el correo entrante (o saliente). De hecho, éste es el diseño que algunos fabricantes de productos anti-spam han escogido para poder garantizar el almacenamiento de correo en situaciones de alta carga.

Sin embargo, en este caso, no será posible rechazar el correo antes de que éste entre en la organización, teniendo que descartarse, por tanto, la última de las posibilidades para el tratamiento del correo basura descritas anteriormente.

Al margen de las pasarelas, también es posible implementar el filtrado en los agentes de correo de usuario. Muchos de los productos de correo más populares, como Mozilla (desde la versión 1.4), o Outlook (desde la versión 2003), implementan ya características de filtrado de correo no solicitado. Además, existen productos comerciales que puedan servir como complemento incorporando funciones adicionales. La ventaja de utilizar el filtrado en el agente de correo es que el usuario final tiene un mayor control sobre la política de filtrado.

Otra opción es utilizar tecnologías basadas en aprendizaje estadístico. Éstas permiten que los usuarios ayuden a "aprender" al sistema utilizando para ello el correo no solicitado que reciben (que no tiene por qué ser igual para todos los miembros de una organización). Igualmente, es más fácil para los usuarios recuperar correos marcados como *spam* ya que el correo está disponible en un buzón al efecto.

2.2.1.2 Tecnologías de filtrado

En función de la tecnología se distinguen los sistemas de filtrado basados en heurísticos, que implementan un conjunto de reglas específicas para detectar el *spam*, y los sistemas de filtrado adaptativos, basados en aprendizaje estadístico y generalmente implementados con filtros bayesianos [31].

La tecnología de filtrado basada en heurísticos analiza los correos e intenta determinar si es o no *spam* en función de si cumple o no unas características predefinidas. Algunas de estas comprobaciones son aplicables a un funcionamiento en pasarela y otras pueden utilizarse indistintamente de la ubicación. Algunos de los elementos habitualmente utilizados en análisis son: palabras clave en el cuerpo o cabecera, composición del mensaje (como pueda ser la forma en que se utiliza el lenguaje HTML), origen específico del correo (direcciones IP que lo han generado y comprobaciones con listas negras, RBLs o DNSBLs), configuración asociada al DNS del sistema remoto que envía el correo, comprobaciones de los servidores de correo asociados a un dominio (utilizando SPF ó Sender-ID), etc.

Generalmente la tasa de falsos positivos (correos rechazados que son legítimos) dependerá de cada chequeo realizado, pudiéndose producir bloqueos de correos deseados. Además, los *spammers* tiene como objetivo encontrar mecanismos para esquivar estas reglas y modifican constantemente los contenidos de sus correos, lo que hace necesario revisar las reglas utilizadas e introducir nuevas reglas a medida que los contenidos varían y éstas dejan de ser válidas.

SpamAssassin [32], por ejemplo, es un sistema de filtrado de *spam* de software libre, muy utilizado, y posiblemente uno de los primeros de filtrado desarrollados para combatir el *spam*. Esta aplicación dispone en su última versión (3.0, publicada en octubre de 2004) de alrededor de seiscientas comprobaciones distintas sobre los mensajes, de las cuales un 54% son de información del cuerpo del mensaje y un 39% de las cabeceras.

El aprendizaje estadístico, por otro lado, se basa en la generación automática de reglas mediante un sistema al que se le "enseña" qué es *spam* y qué no lo es, de forma que éste genera reglas para detectarlo de forma automática. Las reglas se generan analizando el mensaje completo (cabeceras y cuerpo) y sirven para crear clasificaciones (grupos) de correo no solicitado de forma que sea posible determinar, con un cierto grado de confianza, si un correo nuevo efectuadas comparando si tiene características comunes. Esta tecnología es útil para extraer reglas no evidentes del *spam* y es capaz de adaptarse a los nuevos tipos de correo no solicitado que van surgiendo, siendo necesario, sin embargo, un aprendizaje permanente.

Estos sistemas de aprendizaje se implementan habitualmente en los agentes de correo del usuario final, dado que el usuario puede ir "enseñando" al sistema marcando el correo que recibe como *spam*. También es posible implementarlos en sistemas de pasarela pero para ello es necesario utilizando direcciones falsas, que se publican con el objeto de que las utilicen los *spammers*, y cuyos buzones alimentan constantemente a la herramienta de aprendizaje.

2.2.2 Gestión del ancho de banda

Es importante recalcar que, si bien una solución de filtrado puede ayudar mucho a reducir el problema del *spam*, el simple hecho de recibir correo (para posteriormente descartarlo) supone un consumo importante de recursos para la organización. Aún en el caso de que tenga una efectividad del 100%, se estarán gastando además, recursos que dependen directamente del volumen de correo manejado.

En el caso de sufrir una oleada de intentos de envío de *spam*, no sólo sería necesario ser capaz de absorberlo (disco suficiente en las pasarelas para almacenarlo) sino que sería necesario tratarlo con celeridad para que éste no afecte al correo legítimo. Al incrementarse la entrada de correo no solicitado (y su tamaño) se incrementan también las necesidades de disco y CPU de los sistemas que lo tratan de forma equivalente.

Un ejemplo muy claro de este problema es la situación de muchos proveedores de acceso a Internet que están sufriendo, día a día, los embistes de los *spammers* y tienen que revisar e incrementar el número de sistemas que dedican para tratar el correo de sus usuarios y ser capaz de absorber, al mismo tiempo, el correo no solicitado que les llega. La implementación de sistemas de filtrado puede aliviar el problema a corto plazo, pero a largo plazo es necesario implementar otras soluciones para controlar el volumen del correo.

Por esto es necesario complementar los sistemas de filtrado con sistemas de gestión del ancho de banda que permitan, por un lado, controlar y ralentizar la entrada de correo basura y, por otro, garantizar que otros servicios que

hagan uso de la misma línea de conexión a Internet no se vean afectados en caso de sufrir un envío masivo de correo. Al mismo tiempo debe garantizarse que los intercambios de correo con servidores de correo de confianza (servidores de correo corporativos en oficinas remotos, clientes prioritarios o proveedores de Internet locales) es priorizado frente al intercambio con servidores de correo desconocidos.

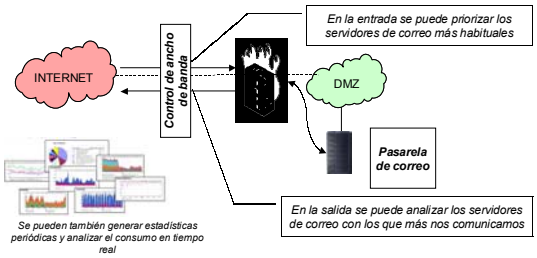


Ilustración 2: Solución de gestión de ancho de banda para control del spam

Para ello se pueden utilizar sistemas genéricos de gestión de ancho de banda existentes en el mercado y capaces de gestionar múltiples protocolos de Internet. Estos sistemas pueden utilizarse para implementar criterios de gestión de ancho de banda para los servicios que una organización utiliza o provee en Internet aplicando su política corporativa, si la hubiera.

También es posible utilizar programas servidores de correo que sean capaces de imponer un cierto control del ancho de banda [33]. Estos servidores de correo modificados realizan también comprobaciones del correo entrante que recibe (origen de la conexión, identificación del remitente en el "sobre" del correo, etc.) para intentar determinar si puede tratarse de un correo no solicitado, en caso de serlo, ralentizan la conexión del sistema remoto, por ejemplo, respondiendo a las órdenes que éste envía en la conversación SMTP más despacio de lo habitual.

3 Evolución a largo plazo

La evolución del *spam* a largo plazo es desalentadora, a pesar de los esfuerzos realizados, en vista de la evolución de estos últimos años. Por un lado, el volumen de *spam* recibido no hace sino aumentar, por otro lado, se detectan cada vez más las vinculaciones entre grupos dedicados al *spam* y grupos dedicados a otras actividades ilegales [34] como son la propagación de contenidos maliciosos o la realización de fraudes a través de Internet.

Además, el fenómeno del *spam* está traspasando las barreras de Internet y está empezando a llegar a otros servicios. La telefonía móvil sufre también el envío de *spam* a través de SMS, si bien es posible que el coste de dichos mensajes, y la inexistencia de pasarelas gratuitas de mensajería a móviles desde Internet, haya influido en que este fenómeno no haya cobrado aún las mismas proporciones.

Otros servicios que han sufrido (o sufren) el azote del *spam* son la mensajería instantánea, los diarios en línea (*blogs*), los foros de noticias vía web y los servicios de edición colaborativa en línea vía web (*wikis*). El efecto del *spam* no es muy acusado aún en la mensajería instantánea debido a que en muchas de estas redes no es posible enviar mensajes de forma indiscriminada a usuarios que no han "aceptado" al remitente dentro de su grupo de "amigos". Si bien es posible que los *spammers* se aprovechen de vulnerabilidades en estos protocolos (o en equipos controlados remotamente) para llevar a cabo este tipo de envío de mensajes, como ya ha sucedido con virus que han afectado a algunos sistemas de mensajería instantánea[6]. Los otros servicios en línea mencionados han sufrido en mayor o menor medida este tipo de ataques, siendo mayor cuando para estos servicios se han utilizado programas muy difundidos y conocidos, lo que ha facilitado la generación de herramientas automáticas para esta tarea. Este efecto se ha venido reduciéndose en dichos servicios en cuanto se introducía la obligación de los usuarios de registrarse a los mismos.

Un último servicio en Internet que ha empezado a sufrir también el *spam* es el servicio telefónico a través de Internet (Voz sobre IP, o VoIP). Si bien la incidencia del *spam*, denominado en estos casos *spit*, ha sido inferior debido al menor número de usuarios. Sin embargo es posible que los mecanismos de control sobre el protocolo sean insuficientes para evitar este problema cuando sea utilizado por un mayor volumen de usuarios.

4 Conclusiones

Desgraciadamente, el fenómeno del *spam* en Internet y, específicamente, el del envío de correo no solicitado seguirá existiendo en tanto en cuanto siga siendo un negocio lucrativo para unos pocos y seguirá extendiéndose a servicios y protocolos que no incluyan las medidas suficientes para garantizar su mala utilización.

[6] El primer virus en hacerlo (W32/Hello o W32.FunnyFiles.Worm) apareción en abril de 2001.

El crecimiento del correo no solicitado estos últimos años supone un enorme esfuerzo para los proveedores de acceso y para todos los usuarios de Internet, independientemente de que sean organizaciones conectadas o usuarios domésticos. Todos tienen que soportar una entrada cada vez mayor de correo no solicitado aunque sólo sea para borrarlo en última instancia en algunos casos, incluso, de forma automática. Los gastos asociados a este problema demuestran que, aunque los costes puedan ser despreciables para los que lo generan, supone un coste importante para los que lo reciben.

No existen medidas únicas para resolver este problema, aunque algunas que pudieran ayudar están en desarrollo (y no lejos de una implantación a gran escala), por lo que todas aquellas organizaciones que se conectan a Internet, y las que ofrecen conexión, deberán seguir introduciendo medidas que mitiguen el problema, por lo menos a corto y medio plazo. Estas medidas no deberán ser exclusivamente técnicas sino que deben ser también sociales: es necesaria también una mayor formación y concienciación de los usuarios de Internet en este grave problema.

5 Referencias

[1] Entrada del término *Spam* asociado al correo electrónico, en la enciclopedia libre Wikipedia, disponible en Internet: http://en.wikipedia.org/wiki/E-mail_spam

[2] Entrada de Canter y Siegel, en la enciclopedia libre Wikipedia, disponible en Internet: http://en.wikipedia.org/wiki/Canter_&_Siegel

[3] *Reaction to the DEC Spam of 1978*, Brad Templeton, disponible en Internet: http://www.templetons.com/brad/spamreact.html

[4] *Origin of the term "spam" to mean net abuse*, Brad Templeton, disponible en Internet: http://www.templetons.com/brad/spamterm.html)

[5] *Spam Statistics,* Brightmail Logistics and Operations Center (BLOC).

[6] *MessageLabs Intelligence Annual E-mail Security Report*, MessageLabs Intelligence, noviembre 2004.

[7] *RFC 706: On the Junk Mail Problem*, Jon Postel, noviembre 1975.

[8] Proyecto Sísifo, Universidad de Zaragoza, http://sanet.unizar.es/

[9] *Virus and spam activity in Europe, monthly report*, Comendo A/S, noviembre 2004 http://www.comendo.dk/

[10] *Confession for two: a spammer spills it all*, Rejo Zenger, disponible en http://rejo.zenger.nl/abuse/1085493870.php

[11] *Email Address Harvesting: How Spammers Reap What You Sow*, Comisión Federal de comercio estadounidense, noviembre 2002, disponible en http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.html

[12] *Why Am I Getting All This Spam:Unsolicited Commercial E-mail Research Six Month Report*, Center for Democracy & Technology, marzo 2003, disponible en http://www.cdt.org/speech/spam/030319spamreport.shtml

[13] *What do you get when you buy a spam CD*, Rejo Zenger, mayo 2004, publicado en http://rejo.zenger.nl/abuse/emailcd.php

[14] *RFC 2821: Simple Mail Transfer Protocol,* publicado por el IETF, abril 2001.

[15] *The Difficulties of Tracing Spam Email*, Dan Boneh, Department of Computer Science Stanford University, septiembre 2004.

[16] *RFC 2822: Internet Message Format,* publicado por el IETF, abril 2001.

[17] *SPF FAQ* (preguntas frecuentes sobre SPF), disponible en Internet en http://spf.pobox.com/faq.html

[18] Sender-ID, Microsoft, disponible en Internet en http://www.microsoft.com/senderid

[19] *MTA Authorization Records in DNS* (marid), grupo de trabajo de la IETF: http://www.ietf.org/html.charters/OLD/marid-charter.html

[20] Entrada de DNSBL, en la enciclopedia libre Wikipedia, disponible en Internet: http://en.wikipedia.org/wiki/DNSBL

[21] *Bot Software Spreads, Causes New Worries*, Laurianne McLaughin, IEEE Distributed Systems Online, volumen 5, número 6, junio 2004.

[22] *Know Your Enemy: Statistics*, proyecto Honeynet, 22 julio 2001.

[23] *Time to live on the network*, Avantgarde, noviembre 2004.

[24] *Survival Time History*, Internet Storm Center, SANS, disponible en http://isc.sans.org/survivalhistory.php

[25] *Directive 2002/58/EC of the European Parliament and of the Council*, 12 de julio 2002.

[26] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, Ministerio de Industria y Comercio español.

[27] *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)*, Senado norteamericano, 16 diciembre 2003, disponible en Internet en http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

[28] *An Act about spam, and for related purposes (Spam Act 2003),* Gobierno Australiano, 12 diciembre 2003 http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

[29] *Register of Known Spam Operations (ROKSO)*, Proyecto Spamhaus, http://www.spamhaus.org/rokso/index.lasso

[30] *Greylisting*, Evan Harris, disponible en http://projects.puremagic.com/greylisting/index.html

[31] *A Bayesian Approach to Filtering Junk E-Mail*, Mehran Sahami, Susan Dumais, David Heckerman y Eric Horvitz, Standford University y Microsoft Research, 1998.

[32] SpamAssassin, disponible en http://spamassassin.apache.org/

[33] *Email Prioritization: reducing delays on legitimate mail caused by junk mail*, Dan Twining, Matthew M. Williamson, Miranda J. F. Mowbray y Maher Rahmouni, HP Labs, abril 2004.

[34] *Criminals Become Tech Savy*, Elias Levy, IEEE Security & Privacy, volumen 2, número 2, marzo-abril 2004.

6 Reseña curricular

Javier Fernández-Sanguino, Ingeniero de Telecomunicación por la ETSIT-UPM, es miembro de la división de Seguridad Lógica de Germinus XXI S.A. en la que ejerce tareas de consultoría y jefatura de proyecto, desarrollando auditorías y pruebas de intrusión, despliegues de arquitecturas de seguridad perimetral, securización de sistemas, etc. Es miembro del proyecto de software libre Debian, del comité internacional de definición de vulnerabilidades OVAL, del grupo español de investigación de redes trampa, y de los grupos de desarrollo de diversas herramientas de seguridad de software libre (Tiger, Nessus, y Bastille).