



Published on hacktimes.com (<http://www.hacktimes.com>)

SOLUCIONES ANTI-SPAM Y SEGURIDAD

By freed0m

Creado 19 Nov 2005 - 19:43

Presentamos una interesante traducción de un documento de investigación sobre distintos métodos y técnicas destinadas a frenar la gran plaga que representa el spam, hemos escogido este artículo por considerarlo una completa y exhaustiva disección de las diferentes soluciones. El documento original puede leerse [aquí](#). [1]

1. INTRODUCCIÓN

En una reciente encuesta, el 93% de los encuestados afirmaron su grado de insatisfacción con el elevado volumen de correo no solicitado (spam) que reciben.[ref 1]

El problema ha crecido hasta el punto de que cerca del 50% del correo que se envía en el mundo es spam [ref 2], aunque solo unos pocos grupos son los responsables.[ref 3]

Muchas soluciones anti-spam has sido propuestas y algunas han sido implementadas. Desafortunadamente, la prevención que aportan estas soluciones no ayudan a prevenir el spam tanto como interfieren en las comunicaciones diarias a través de email.

El problema que representa el spam ha crecido desde simples molestias a significativos problemas de seguridad.

El diluvio del spam provoca aproximadamente unos 20 millones de dólares en pérdida de productividad al año, de acuerdo con el mismo documento, el spam dentro de una compañía puede costar entre 600 y mil dólares por año y por usuario. [ref 4]

1.1. RIESGOS DE SEGURIDAD

Además del tiempo empleado para ver y borrar los mensajes de spam, supone diferentes riesgos de seguridad como son:

- **Robo de identidad:** El phishing y el scam distribuido como spam, va dirigido principalmente al robo de identidades y al fraude. De acuerdo con el Anti-Phishing Working Group, el phishing enviado como spam aumento un 52% en enero. [ref5]

- **Virus:** Nuevos virus, gusanos y malware, como el Melissa, Love Bug, y MyDoom han usado técnicas de spam para propagarse una vez ejecutados por el usuario.
- **Combinaciones de spam y exploits.** La diferencia entre un hacker malicioso y un spammer es, a día de hoy menos evidente. Muchos spammers han incorporado código HTML y Javascript manipulado para aprovechar las vulnerabilidades de los navegadores. Por ejemplo, el 31 de diciembre de 2002, un grupo de hackers de Brasil, enviaron mensajes de spam que contenían código Javascript a millones de usuarios. Las personas que recibieron este mensaje desde Hotmail comprometieron sus cuentas de correo sin saberlo. Como otro ejemplo, el problema de Internet Explorer relativo a la forma en que se muestran las URLS, donde la cadena de caracteres "%01" antes del nombre del host podían ser usadas para ocultar el verdadero nombre del host [ref 6], también fue incorporado en los mensajes de spam.
- **Combinaciones de virus y spam.** La creencia de que los virus están diseñados para ayudar a los spammers. Por ejemplo, el gusano SoBig instala proxys abiertos que se usan como relay por los spammers. A medida que el spam se vuelve más frecuente, el uso de malware y spyware para dar soporte al spam es probable que aumente.

Las soluciones y propuestas anti-spam existentes intentan mitigar el problema del spam y los problemas de seguridad. Identificando correctamente el spam, el impacto de virus de correo electrónico exploits y robo de identidad puede ser reducido. Estas soluciones implementan varios tipos de seguridad en un esfuerzo para frustrar el spam.

Las soluciones anti-spam presentan fallos que se pueden clasificar en cuatro categorías principales: filtros, búsqueda inversa, desafíos y criptografía. Cada una de estas soluciones ofrece algún tipo de alivio para el problema del spam, pero tienen limitación bastante significativas. La primera parte de este documento de dos partes, examina los filtros y las búsquedas inversas. La segunda parte se centra en varios tipos de desafíos, como desafío-respuesta y desafíos computacionales además de las soluciones criptográficas. Hay muchos aspectos diferentes en estas soluciones, este documento sólo trata sobre los problemas y preocupaciones más frecuentes, no pretende ser una lista completa de implementaciones, opciones, y versiones.

1.2. TERMINOLOGÍA

- **Emisor:** La persona o proceso que es responsable de la generación del mensaje de correo electrónico.
- **Receptor:** Cualquier dirección de correo electrónico que recibe el mensaje. Este puede ser especificado en el email como "To:", "CC:" o "BCC:".

1.2. FILTROS

Los filtros se usan en los sistemas que reciben los mensajes para identificar y organizar el spam. Hay muchos tipos diferentes de sistemas de filtrado incluyendo:

- **Listas de palabras:** simples y complejas listas de palabras que se asocian con el spam. Por ejemplo, “viagra”.
- **Listas negras y listas blancas.** Estas listas contiene direcciones IP conocidas de spam y legítimos respectivamente.
- **Tablas con hash.** Estos sistemas resumen los emails en valores casi únicos. La presencia de valores repetidos son síntomas de mensajes masivos.
- **Inteligencia artificial y sistemas probabilísticos.** Sistemas como las redes Bayesianas se usan para aprender frecuencias de palabras y patrones que son habitualmente asociados con mensajes de spam y legítimos.

Los filtros son valorados en función de los resultados frente a falsos positivos y falsos negativos. Un falso negativo indica que un mensaje de spam ha conseguido pasar el filtro. En contraste, un falso positivo indica que un mensaje legítimo ha sido clasificado incorrectamente como spam. Un filtro de spam ideal no debería generar falsos positivos y muy pocos falsos negativos.

La solución anti-spam basada en filtros tiene tres limitaciones significativas:

- **Evitar el filtro.** Aquellos que envían spam y las aplicaciones de envío masivo de correo no son estaticas, se adaptan rapidamente entorno a los filtros. Por ejemplo, para evitar la identificación de las palabras, los spammers cambian de forma aleatoria las letras que componen la palabra (“viagra”, “V1agra”, “Viaagra”). Los hashbusters (secuencias de caracteres aleatorios que difieren en cada mensaje) están elaborados para evitar los filtros basados en tablas con hash. Y los famosos métodos Bayesianos están siendo eludidos mediante el uso de frases o palabras aleatorias. La mayoría de los filtros son efectivos únicamente durante unas pocas semanas en el mejor de los casos. Para mantener la viabilidad de los sistemas anti-spam, el conjunto de reglas tiene que ser constantemente actualizado, habitualmente diaria o semanalmente.
- **Falsos positivos.** Cuanto más efectivo es un filtro de spam, mayor es la posibilidad de clasificar equivocadamente un correo legítimo como spam. Por ejemplo, un mensaje que contenga la palabra “viagra” (p.e. , el texto de spam “Free viagra” o un texto que no sea de spam como “¿Viste que gracioso era el anuncio de viagra que emitieron durante la superbowl?”) seguramente será marcado como spam a pesar del contenido. De forma similar el correo que provenga de la subred 24.8.0.0/15 de Comcast es bloqueado de forma automática por las listas negras de SORBS porque está asociado con direcciones DHCP y no porque el emisor esté relacionado con spam. Inversamente, los filtros de spam que teóricamente no generan falsos positivos es posible que generen una gran cantidad de falsos negativos.
- **Revisión de filtros.** Debido a la existencia de los falsos positivos, los mensajes marcados como spam no son borrados de forma inmediata. Por lo contrario, son ubicados en buzones de spam para revisarlo posteriormente. Desafortunadamente, esto significa que los usuarios tendrán que ver el spam, aunque sea solo el asunto, para buscar mensajes mal clasificados. Esencialmente, los filtros ayudan únicamente en la organización del correo entrante.

Mas importante que las limitaciones de los filtros de spam es el mito sobre el éxito de los mismos, hay una creencia muy extendida que dice que los filtros eliminan el spam.

Los filtros no paran el spam . En todos los casos, el spam sigue generándose, sigue atravesando la red, y sigue entregándose. Si al usuario no le importa perder ocasionalmente algún mensaje clasificado por error como spam, el spam sigue siendo revisado. Mientras que los filtros ayudan a organizar y separar los mensajes de correo electrónico en grupos de correo legítimo y correo spam, los filtros no previenen el spam.

1.4. BÚSQUEDAS INVERSAS

Casi todo el spam utiliza direcciones falsificadas en el campo (“From:”); muy pocos mensajes de spam utilizan la dirección real. Además, la mayoría de los mensajes de spam parecen provenir de dominios confiables. Por ejemplo, en 15 meses nuestro archivo de spam recogió 9300 emails que parecían provenir de 2400 dominios únicos. El dominio “yahoo.com” acumulaba el 20% de las direcciones del archivo, pero el spam que venía de “yahoo.com” era menor del 1%. De forma similar, “aol.com” y “hotmail.com” acumularon un 5% cada uno, y “msn.com” acumuló un 3% de spam, originado desde esos dominios, considerándose menor del 1% de todo el spam recibido.

Los spammers falsifican la dirección de remite por numerosas razones.

- **Ilegalidad.** Muchos mensajes de spam son ilegales en la mayoría de los países. Falsificando la dirección de remite, el remitente puede permanecer anónimo y evitar que se persiga el delito.
- **No deseable.** La mayoría de los spammers saben que sus mensajes no son deseados. Modificando los remitentes, se puede reducir la repercusión de mandar millones de mensajes a millones de destinatarios molestos.
- **Limitaciones en el ISP.** La mayoría de los proveedores de servicios de Internet tienen cláusulas contractuales que previenen el spam. Falsificando las direcciones de origen reducen la probabilidad de que sus ISP anulen sus accesos a Internet.

Tratando el problema de la falsificación de direcciones, los spammers perderían la posibilidad de permanecer anónimos. Sin la posibilidad de operar de forma anónima, las leyes podrían actuar contra los spammers.

En un esfuerzo para limitar las posibilidades de falsificación de direcciones, han surgido un número de sistemas para verificar la dirección del remitente. Estos sistemas incluyen:

- Reverse Mail Exchanger (RMX) [2]
- Sender Permitted From (SPF) [3]
- Designated Mailers Protocol(DMP) [4]

Estas aproximaciones son muy similares entre si y en muchos aspectos son idénticas. El servicio DNS, es un servicio de red global que se utiliza para establecer la relación entre una dirección IP y su nombre de host y viceversa. En 1986 el servicio DNS se extendió para asociarlo con los registros MX de correo.[ref 7]. Cuando se distribuye el correo, un servidor de correo determina hacia donde se ha de enviar el mensaje basándose en el registro MX asociado al nombre de dominio del destinatario.

De forma similar a los registros MX, la búsqueda inversa define los registros MX inversos (“RMX” para RMX, “SPF” para SPF, Y “DMP” para DMP) para determinar cuando un email de un determinado dominio se puede originar desde determinada IP. La idea básica es que el correo con remitentes falsificados no se puedan originar desde rangos de direcciones con registros RMX (o SPF o DMP) correctos y sean identificados inmediatamente como falsificados.

Aunque estas situaciones son viables en determinadas situaciones, comparten limitaciones significativas.

1.4.1 DOMINIOS SIN HOST O DOMINIOS "POR VANIDAD"

La aproximación de la resolución inversa requiere que el mensaje de correo electrónico se origine desde un servidor conocido y confiable localizado en una dirección IP conocida (el registro inverso MX). Desafortunadamente, la mayoría de los nombres de dominios no están asociados con direcciones IP estáticas. Omitiendo a los “cyber squatters”, el caso general incluye a usuarios y pequeñas compañías que quieren usar su propio dominio en lugar del de su ISP, pero no pueden costearse adquirir su propio direccionamiento IP estático y un servidor de correo. Los host de registros de DNS, como “GoDaddy”, proveen de redirectores gratuitos de correo a gente que registra dominios sin tener host, o dominios destinados a la vanidad. Aunque estos servicios de redirección de correo pueden gestionar correo entrante, no ofrecen la posibilidad de correo saliente gratuito.

Las soluciones de búsqueda inversa causan pocos problemas para los usuarios de dominios sin host o dominios "por vanidad":

- **No hay registros Inversos MX.** La gente que envía mensajes desde dominios sin maquina o dominios por vanidad configuran sus aplicaciones de correo para enviar mensajes de correo electrónico desde su nombre de dominio registrado. Desafortunadamente, la búsqueda de la dirección IP no coincidirá con el dominio del remitente, y una búsqueda del dominio del remitente no encontrará el registro MX inverso correcto. Este caso es particularmente común en conexiones móviles, dial-up, y otros usuarios que cambian frecuentemente de dirección IP.
- **No hay correo saliente.** Una posible solución requiere confiar todo el correo saliente en el servidor SMTP del ISP. Esta opción proveería de un registro inverso MX valido para el envío de mensajes. Desafortunadamente, muchos ISP's no permiten el envío de correo cuando el dominio del remitente no es el mismo que el dominio del ISP.

En ambos casos, alguien puede usar dominios por vanidad, o un dominio que no tiene su propio servidor de correo, y será bloqueado por los sistemas de búsqueda inversa.

1.4.2 COMPUTACIÓN MOVIL

La computación móvil es una practica muy común. La gente lleva sus portátiles a conferencias, reuniones fuera de la oficina, y a sus casas para trabajar fuera del trabajo o

en una ubicación diferente.

Hoteles, aeropuertos e incluso cafeterías se llevan de una multitud de personas con sistemas móviles de computación. Desafortunadamente, el sistema de búsqueda inversa evitará que muchos usuarios móviles puedan enviar emails.

- **Envío directo.** Hay dos formas de enviar mensajes de correo electrónico. Un usuario se conecta a su sistema de correo usando una cuenta externa POP / IMAP / SMTP, webmail o un servicio similar, o realiza el envío directamente. La mayoría de las empresas no permiten acceso externo a sus sistemas de correo; los usuarios móviles configuran sus portátiles para enviar el correo directamente. Desafortunadamente, los problemas con el envío directo de correo electrónico son exactamente los mismos problemas que se tienen en los dominios que no tienen host, una búsqueda inversa del dominio no incluirá la dirección IP emisor del mensaje, y una búsqueda inversa de la IP del emisor no identificará el dominio.
- **Mail relaying.** La alternativa al envío directo requiere que todas las compañías y sistemas de dominios provean de servicios de correo externo para sus usuarios móviles y externos. En muchas situaciones, esto no es ni práctico ni deseable. Como ejemplo, desde un punto de vista estricto de seguridad de red, el servicio POP3 transmite los usuarios y contraseñas en texto claro. Así, cualquier ataque que capture el tráfico de la red, obtendrá credenciales válidas. Podría usarse IMAP con soporte SSL y con autenticación segura, pero no todos los servidores lo soportan. El protocolo SMTP también soporta SSL o TLS pero nuevamente, muchos servidores de organizaciones no dan este soporte, o usan certificados en la parte del servidor (server-side). Correo web a través de HTTPS es tan seguro como los certificados de cliente. Como la mayoría de los sitios utilizan certificados de servidor, HTTPS ofrece poca protección frente a los ataques de hombre en el medio.

Mientras que las soluciones de búsqueda inversa son viables en redes internas, no son prácticas a nivel global o en redes externas. Las compañías que quieren dar soporte a dominios sin host, dominios por vanidad, y usuarios móviles o externos pueden reconsiderar el uso tecnologías anti-spam basadas en mecanismos de búsqueda inversa.

2. RESUMEN

El spam ha alcanzado proporciones de epidemia y se están buscando soluciones rápidas de cualquier tipo.

Los filtros anti-spam representan la solución más adecuada hasta la fecha, los filtros que intentan identificar el spam y limitar su llegada al buzón del usuario. Pero los filtros no previenen el spam más que el equivalente a grabar con un video un programa de TV para evitar los anuncios.

Los sistemas de búsqueda inversa intentan solucionar el problema de la falsificación de direcciones de remite. Mientras que las resoluciones inversas son viables en entornos cerrados, como una red corporativa interna, estas soluciones no son suficientes para que se acepten por todo el mundo.

La segunda parte de esta investigación, se centrará sistemas de desafío respuesta y en las soluciones criptográficas propuestas.

Sobre el autor.

Neal Krawetz Doctor en Informática con más de 15 años de experiencia en el campo de la seguridad informática. Dr. Krawetz está considerado uno de los expertos que lideran la investigación frente al spam, dirige el "Equipo de tratamiento de riesgos externos" (ETAT) en la empresa Secure Science, una compañía de software y servicios profesionales que desarrolla tecnologías avanzadas dedicadas a la protección de activos online.

Referencias

[ref 1]

Majority in Favor of Making Mass-Spamming Illegal Rises to 79% of Those Online. [5] The Harris Poll @ #38. July 16, 2003.

[ref 2]

"Spam On Course to Be Over Half of All Email This Summer [6] Brightmail press release. July 1, 2003.

[ref 3] According to SpamHaus, a spam content tracking organization, less than 200 spam groups generate more than 90% of spam messages. SpamHaus ROKSO [7], September 22, 2003.

[ref 4] Source: "Spam Costs \$20 Billion Each Year in Lost Productivity [8], by Jay Lyman. December 29, 2003.

[ref 5] Source: Phishing e-mail fraud rises 52% in January, report says [9], February 18, 2004.

[ref 6] Reference: Multiple Browser URI Display Obfuscation Weakness [10]

[ref 7] Source: "Domain System Changes and Observations", RFC973 by Paul Mockapetris. January 1986.

Traducido por: Juan de la Fuente Costa

Source URL:

<http://www.hacktimes.com/?q=node/26>

Links:

[1] <http://www.securityfocus.com/infocus/1763>

[2] <http://www.ietf.org/internet-drafts/draft-danisch-dns-rr-sntp-03.txt>

[3] <http://spf.pobox.com>

[4] <http://www.pan-am.ca/dmp/>

[5] http://www.harrisinteractive.com/harris_poll/index.asp?PID=387

[6] http://www.brightmail.com/pressreleases/070103_uk_spam_summit.html

[7] <http://www.spamhaus.org/rokso/index.lasso>

[8] <http://www.linuxinsider.com/perl/story/32478.html>

[9] <http://www.internetretailer.com/dailyNews.asp?id=11317>

[10] <http://www.securityfocus.com/bid/9182>