

Tecnologías de filtrado en Symantec Brightmail AntiSpam™ 6.0

CONTENIDO

- › Resumen ejecutivo
- › La condición del spam
- › Criterio de evaluación para una solución antispam
- › La solución Symantec
- › Conclusiones

> **Contenido**

Resumen ejecutivo	1
La condición del spam	2
Definición de spam	2
El ciclo de vida y la evolución del spam	3
Tácticas de los creadores de spam: creación y diseminación del spam	4
Criterio de evaluación para una solución antispam	7
Efectividad	7
Precisión: evitar falsos positivos a toda costa	8
Proactividad y sensibilidad	8
Administración mínima	9
La solución Symantec	10
El BLOC™: análisis del spam y operaciones	10
Tecnología de filtrado de varios niveles	11
Administración de filtro y actualización de motores	16
Conclusiones	17

> Resumen ejecutivo

Además de ganar dinero, la obsesión principal de un creador de spam es evadir los filtros antispam. El juego del gato y el ratón entre los creadores de spam y los proveedores de antispam continúa desde hace más de una década. Las primeras generaciones de spam fueron basadas en ASCII y de alguna manera aleatorias –manejadas fácilmente por acercamientos de filtros hechos por uno mismo y estáticos de palabras claves. Pero el juego ha evolucionado. La última generación de spam incorpora tácticas sofisticadas como el cálculo aleatorio extremo, encubrimiento de origen y evasión de filtros utilizando HTML. Los creadores de spam continúan aumentando las jugadas inventando maneras de escapar de los filtros y nuevas formas de beneficiarse de sus acciones. Este compendio de tecnología describe cómo los grupos de investigación y desarrollo de Symantec adaptan continuamente técnicas de filtrado para desafiar a los creadores de spam y bloquear los ataques de spam.

El arsenal antispam de gran adaptación de Symantec incluye una colección de poderosas tecnologías de filtrado proactivas y sensibles respaldadas por una infraestructura completa del análisis de spam. Juntos, estos elementos fortalecen su organización con una sólida protección antispam a la vez que proporcionan la mejor tasa de precisión disponible en la industria (99.9999%)¹.

Este documento abarca lo siguiente:

- **La condición del spam** Un vistazo de las armas preferidas de los creadores de spam, incluyendo evasión de filtros y tácticas de diseminación.
- **Características esenciales de una solución antispam.** Un panorama general de las pautas que se deben considerar cuando se evalúan productos antispam de capacidad para empresas.
- **La solución Symantec.** Un resumen de las tecnologías de filtrado, infraestructura y recursos de antispam que Symantec utiliza. Los temas incluyen tecnologías de filtrado completas proactivas y sensibles de Symantec, sus características únicas de análisis de spam y sus centros de operaciones que trabajan las 24 horas, los 7 días de la semana.

Symantec Brightmail AntiSpam 6.0 es la oferta antispam que utiliza tecnología de Brightmail, la cual se ha enfocado exclusivamente en el mercado antispam durante más de seis años. El software Symantec Brightmail AntiSpam protege a más de 2,500 de las empresas líderes en el mundo, incluyendo Avaya, eBay, Bechtel, Booz Allen Hamilton, Cypress Semiconductor, Deutsche Bank, Lucent Technologies y Terra Lycos. Como la solución antispam comercial más implementada, Symantec Brightmail AntiSpam ahora protege a más de 300 millones de buzones en todo el mundo, incluyendo más de 5 millones de bases empresariales. Estos clientes dependen de Symantec por su experiencia en filtrado de spam, su acercamiento lógico y flexible para combatir el spam en el sitio de la estación de trabajo y su compromiso continuo para oponerse a las tácticas de los creadores de spam.

NOVEDADES DE LA VERSIÓN 6.0

Symantec ha aumentado el galardonado trabajo de ediciones previas de Brightmail AntiSpam. Éstas son algunas características de filtrado del motor que se han añadido o mejorado en esta versión:

- **Brightmail Reputation Service™ integrado.** El Brightmail Reputation Service mide la reputación de un transmisor de correo electrónico por enviar correo electrónico legítimo vs. spam.
- **Tecnologías avanzadas para combatir el spam en idiomas diferentes al inglés.** Con las nuevas capacidades de identificación de idiomas y herramientas del usuario, Symantec ha fortalecido sus defensas contra el spam en idiomas diferentes al inglés.
- **URL de la siguiente generación y tecnologías de firma.** Los filtros URL únicos de Symantec se han actualizado para mantener el paso con los nuevos intentos para evadir el filtrado. Entre otras mejoras, los filtros URL ahora examinan enlaces de correo electrónico incrustados. Las firmas anexas son la respuesta de Symantec a anexos en MIME indeseables o peligrosos.

¹ "Anti-Spam Services for SMBs and Middle-Market End-Users", 25 de febrero de 2003
Nota de investigación de J.P. Gownder de Yankee Group

> La condición del spam

Esta sección abarca lo siguiente:

- Definición de spam
- El ciclo de vida y la evolución del spam
- Tácticas de los creadores de spam

Definición de spam

La persona media, cuando se le pide definir spam, puede responder citando tipos específicos de solicitudes de correo electrónico ofensivos o fraudulentos –la implacable corriente de anuncios de Viagra o los mensajes electrónicos scam nigerianos creativamente puntuados. Otras pueden incluir boletines o cartas en cadena, que hace mucho tiempo perdieron interés. Otras podrán considerar cualquier tipo de publicidad de cualquier fuente, legítima o no, como spam. En efecto, para tal modalidad subjetiva de comunicación, una definición autoritaria de cada receptor puede ser difícil de encontrar. Sin embargo, sigue siendo imperativo distinguir el spam enviado por creadores de spam maliciosos del correo legítimo.

Symantec utiliza las pautas que se destacan en la Figura 1 para distinguir el spam de la comunicación electrónica legítima.

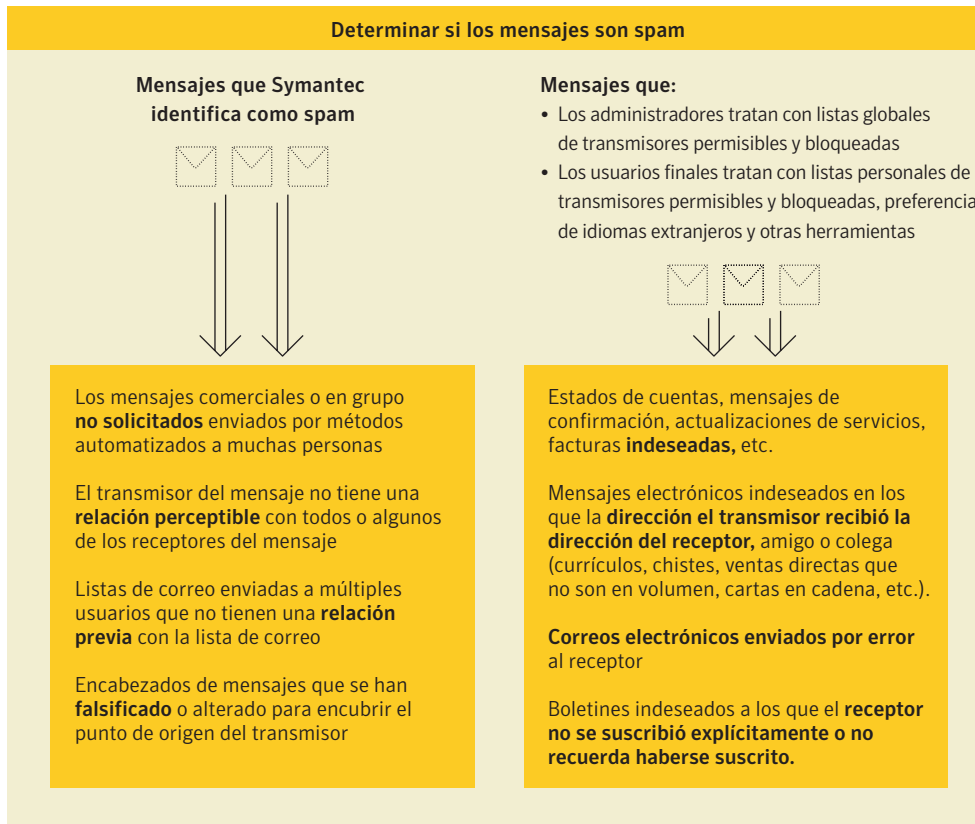


Figura 1. Determinar si los mensajes son spam

Los mensajes spam desperdician los recursos corporativos. Los correos electrónicos al azar, sin un objetivo fijo, enviados por métodos automatizados tienen un impacto cuantificable en las empresas. Dicho spam consume directamente el tiempo de los administradores de tecnología de información, junto con los recursos del servidor de correo y almacenamiento de la compañía. Además, ya que grandes compañías estiman que sus empleados dedican hasta 15 minutos del día leyendo, borrando y respondiendo a estos mensajes, el spam roba a los empleados tiempo preciado y costosa productividad².

El ciclo de vida y la evolución del spam

El spam ha sido un efecto secundario del Internet por más de una década. En ese tiempo ha madurado para seguir un ciclo de vida predecible con tres circunscripciones claves (vea la Figura 2).

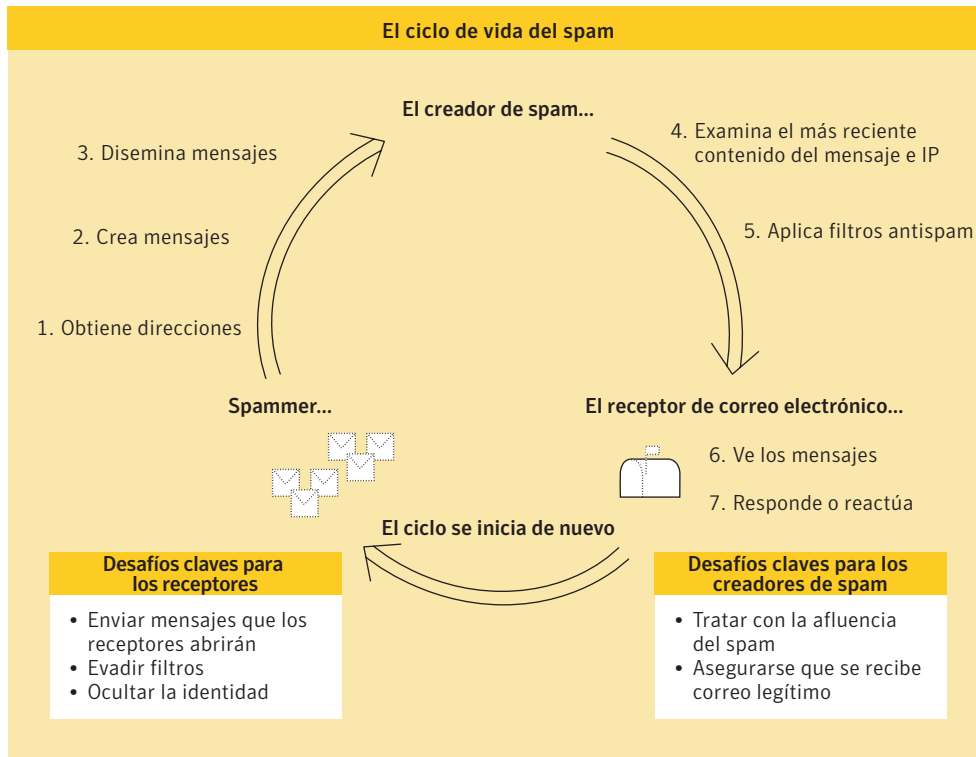


Figura 2. El ciclo de vida del spam

El ciclo de vida continuo impulsa la evolución del spam, tanto en su forma como en sus implicaciones. Como resultado de un aumento de filtrado antispam, junto con la llegada de nuevas tecnologías y oportunidades a disposición de los creadores de spam, el spam está evolucionando rápidamente en un fenómeno todavía más peligroso.

El aumento constante de spam es sólo parte de la ecuación; así como los problemas son la forma que están tomando muchos ataques de spam (vea la Figura 3). Los días en que los creadores de spam simplemente enviaban sus lanzamientos de ventas nada sofisticados de sus cuentas de ISP son cosa del pasado. El spam resistente a los filtros de transmisores ocultos se está convirtiendo rápidamente en el mecanismo de diseminación preferente para los costosos ataques de virus o intentos de fraude por correo electrónico.

²"El costo de los falsos positivos del spam", de Ferris Research, agosto de 2003.

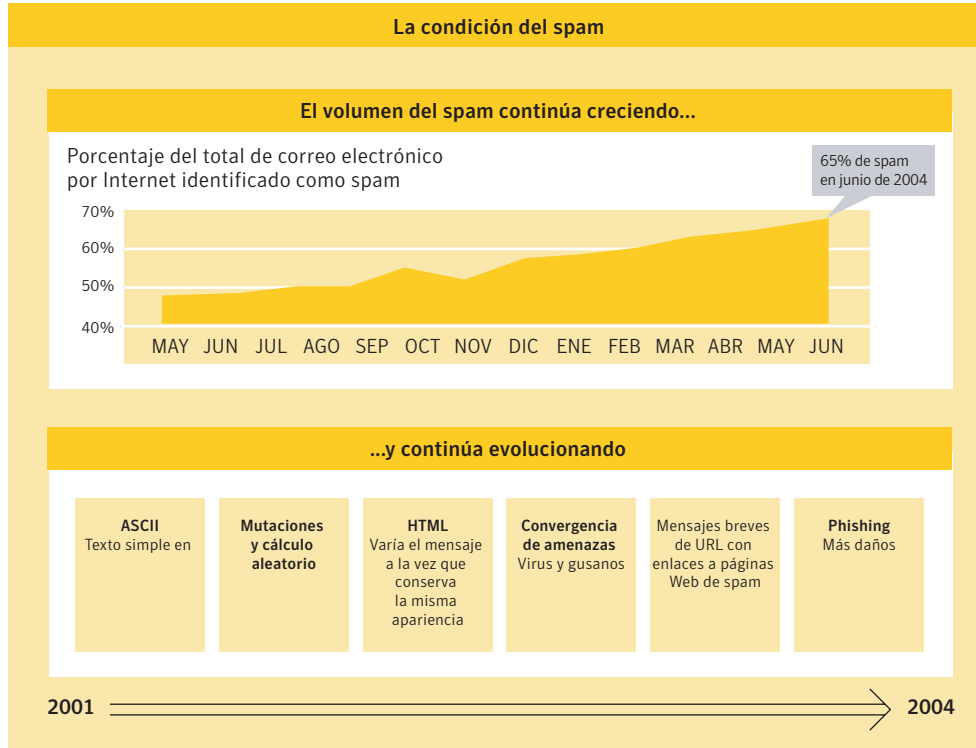


Figura 3. La condición del spam

La siguiente sección abarca los aspectos principales del ciclo de vida desde la perspectiva del creador de spam.

Tácticas de los creadores de spam: creación y diseminación del spam

De acuerdo a la revista *Business 2.0*, para que algunos creadores de spam obtengan \$1 millón al mes, todo lo que se necesita es una compra con valor de \$20 de una de cada 2.000 personas engañadas –una tasa de respuesta del 0,05%. La economía del spam es difícil de igualar: por casi nada, los creadores de spam pueden obtener listas de millones direcciones electrónicas producidas. La barrera para estos recursos son los filtros antispam. Esta sección resume algunas de las tácticas utilizadas por los creadores de spam para evadir el filtrado.

EVASIÓN DE FILTROS CON MODIFICACIONES DE CONTENIDO EN BASE HTML

Los creadores de spam a gran escala son cada vez más adaptables y sofisticados. Estas personas u organizaciones pueden ciclar a través de nombres de dominio falsos y alterar los renglones de asuntos de manera tan precisa y eficiente que para cuando las viejas tácticas antispam pueden discernir un patrón, el daño está hecho y ya se ha lanzado un nuevo ataque con características diferentes. El software de correo masivo inclusive permite a los creadores de spam correr el correo en listas preprogramadas, evaluando si los filtros de spam podrían bloquear el correo.

Modificación del contenido usando HTML es la más reciente y poderosa técnica antifiltrado del creador de spam efectivo.

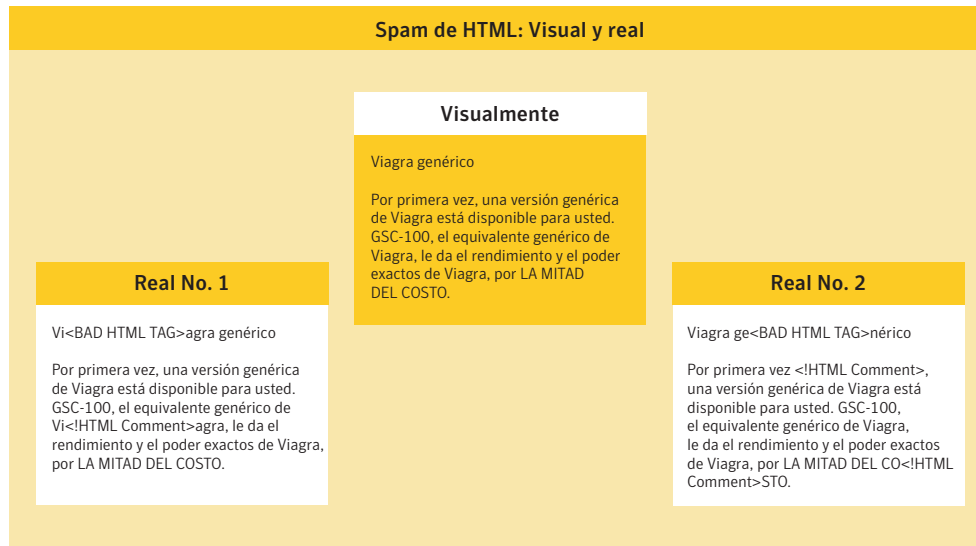


Figura 4. Spam de HTML: visual y real

Hay muchas razones por las que los creadores de spam seleccionan HTML:

- **Atrae la atención.** Utilizando medios opulentos, los creadores de spam pueden añadir mensajes llamativos y provocativos sin aumentar significativamente sus costos o el tamaño de los archivos.
- **Permite el rastreo.** Con dispositivos de rastreo incrustados que se activan tan pronto como se descargan las imágenes, los creadores de spam pueden verificar si la dirección electrónica blanco es una dirección *activa o válida*.
- **Permite el spam aleatorio o polimórfico.** Debido a que el texto fundamental del mensaje es único, este tipo de spam es muy difícil de filtrar. La inserción de texto blanco sobre un fondo blando, las etiquetas falsas de HTML, o las tablas de HTML son sólo algunos de los trucos antifiltrado basados en HTML.

Debido a las infinitas variaciones y cálculos aleatorios, formatear el spam en HTML ofrece a los creadores de spam una manera poderosa de evadir el filtrado.

EVASIÓN DE FILTROS CON OFUSCACIÓN DE URL

Los creadores de spam con frecuencia usan técnicas antifiltrado basadas en URL, solicitando a los receptores que realicen una acción adicional además de simplemente leer el mensaje. En la mayoría de los casos, el creador de spam quiere que el receptor compre un producto o se registre para un servicio. Para añadir a la transacción, los creadores de spam con frecuencia incluyen un URL que señala una página Web. El spam que anima a los receptores hacer clic en un URL es con frecuencia problemático para los filtros antispam. En primer lugar, los creadores de spam pueden introducir una cantidad excesiva de personalización, incluyendo texto inofensivo y aparentemente legítimo en el enlace objetivo. Este texto no sólo hace que el mensaje electrónico parezca legítimo, sino que también permite a los creadores de spam crear más mensajes substancialmente diferentes donde sólo el URL fundamental es el mismo. Existe también un exceso de ofuscación y tácticas de retransmisión de URL que los creadores de spam pueden emplear para ocultar el URL objetivo.

También se ha comprobado que los creadores de spam son partidarios de enmascarar la apariencia externa de los URL, de manera que los receptores piensan que los URL pertenecen a una organización legítima. El éxito reciente de los ataques de correo electrónico de “trampas de marcas” son testimonio del poder de esta táctica. En dichos ataques, los creadores de spam crean correos electrónicos fraudulentos y enmascaran los URL, declarando que originan de organizaciones legítimas, tentado a los receptores para que proporcionen información financiera y privada.

DISEMINACIÓN USANDO RETRANSMISIONES CON IDENTIFICACIÓN ENMASCARADA

Enviar físicamente correos electrónicos en volumen es un asunto trivial. Los appliances de los servidores de correo electrónico con propósitos especiales pueden enviar hasta un millón de mensajes electrónicos por hora. Sin embargo, para evitar repercusiones legales o bloqueo de la fuente vía dirección IP, los creadores de spam necesitan un mecanismo para ocultar sus identidades.

Una forma común en que los creadores de spam tratan con el asunto de disimulo es utilizando *mensajes con identificación enmascarada*. Una aplicación de tal técnica es el mal uso de los servidores con proxy abierto. Los servidores con proxy abierto son computadoras mal configuradas o infectadas con virus que permiten que el tráfico de virtualmente cualquier servicio de red se canalice a través de una computadora host. La siguiente tabla muestra cómo los servidores con proxy abierto utilizados de esta manera difieren de los mensajes SMTP abiertos, los cuales realmente no se utilizan para enmascarar identidades.

	Mensaje SMTP abierto	Proxy abierto
Descripción	El servidor de correo que procesa el correo donde ni el transmisor ni el receptor es un usuario local.	Computadora host insegura que acepta peticiones de cualquier computadora aleatoria para compartir conexión al Internet. También se conoce como software legítimo mal configurado o virus malicioso de caballo de Troya que permite que una computadora se use de tal manera.
Cómo los usan los creadores de spam	Conecta al servidor de correo con un mensaje abierto y pasa el correo a la fuerza. El origen del spam parece ser el servidor intermedio.	Se conecta al puerto 25 del servidor de correo como un servicio http a través del proxy abierto, envía una petición POST y esconde el contenido SMTP en el cuerpo de los datos publicados. El servidor del correo ignora los encabezados de http y acepta el mando de SMTP en el cuerpo del correo electrónico.
Identidad enmascarada	Bajo. No oculta la fuente del spam porque la mayoría de los agentes transmisores de correo (MTA) añaden un encabezado de Recibido: antes de enviar el correo.	Alto. Los proxy envían conexiones TCP/IP crudas, sin dejar encabezados. Ya que los servidores proxy permiten que una computadora se enmascare de otra, es imposible identificar la dirección de origen real del IP.
¿Se utilizan para enviar correo legítimo?	Ocasionalmente. Algunas veces los administradores usan mensajes abiertos para seguir la ruta de un problema de servidor. Otras veces pueden olvidar apagar los mensajes de correo abiertos.	No. No hay razones válidas para enviar correo a través de un servidor proxy.
Popularidad como recurso del spam	Disminuyendo. La mayoría de los administradores bloquean sus mensajes para mantenerse fuera de las listas negras.	Método de opción. La mayoría de los spam no se envía a través de un puerto de correo convencional. Casi siempre se envía usando proxy. Gracias al software mal configurado y a los caballos de Troya, los servidores proxy vulnerables abundan.

Los creadores de spam rutinariamente identifican y se apoderan de servidores proxy inseguros. Sin que los dueños de las computadoras malversas se enteren, los creadores de spam usan las computadoras como vehículos para enviar grandes volúmenes de correo no solicitado. Dos tercios de todos los mensajes de correo electrónico no deseado emanan de estos servidores inseguros. La Figura 5 muestra cómo los servidores proxy abiertos son una manera ideal de ocultar la identidad del servidor.

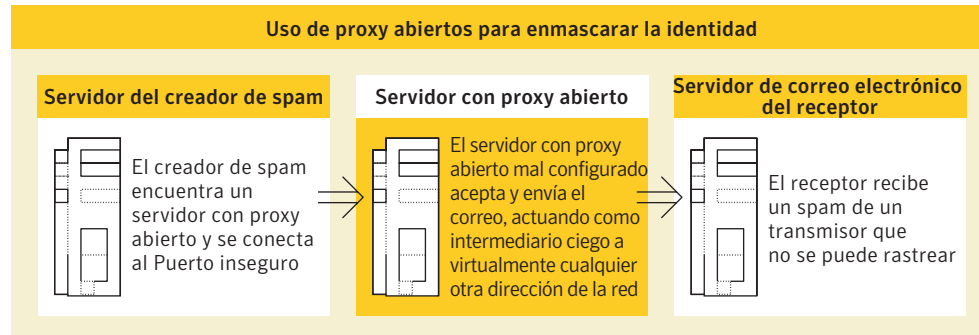


Figura 5. Uso de proxy abiertos para enmascarar la identidad

Una vez que los creadores de spam descubren un proxy abierto, continuarán enviando spam a través de éste, hasta que el proxy abierto se cierre. Los creadores de spam también están inventando nuevas maneras de apoderarse de computadoras para enviar spam, como evidencia de los recientes gusanos computacionales de correo masivo, como Sasser, Netsky y SoBig. El análisis inicial sugiere que, aunque no tuvo una carga útil especialmente maliciosa, el virus sí instaló un programa de correo en las computadoras de las víctimas, estableciendo el escenario para una inmensa red de conductos de enmascarado de identidad a través de los cuales se podría enviar.

Para obtener más información sobre proxy abiertos y otras tácticas de evasión de filtros, visite las siguientes fuentes:

- www.infosecwriters.com/texts.php?op=display&id=54
- www.nanae.org/links.html
- www.spam.abuse.net
- www.mail-abuse.com

Criterio de evaluación para una solución antispam

Esta sección resume el criterio más importante para evaluar una solución antispam. Los puntos principales son efectividad, precisión y facilidad de administración. Las soluciones más importantes ofrecen una combinación de tecnologías y liberan al administrador de tareas de implantación y mantenimiento continuo.

Efectividad

Aunque hay muchas formas de medir la utilidad de una solución antispam, el punto fundamental es la alta efectividad de bloqueo de spam. La efectividad es el porcentaje de mensajes de spam que se filtran correctamente como spam. Los términos *capturar* o *atrapar* también se utilizan para describir esta medida.

Mantener la alta efectividad es desafiante por muchas razones. Primeramente, el “spam” que constituye los pocos puntos finales de porcentaje con frecuente puede ser muy subjetivo, difícil de tratar en una base global de todo el servidor. Los filtros del cliente pueden ser una opción en tales casos. A continuación, acciones muy agresivas para conseguir efectividad aumenta las posibilidades de que el correo legítimo se bloquee. Por último, a medida que aumentan los porcentajes de bloqueo de spam, los creadores de spam tienen un incentivo para aumentar su volumen total para mantener el status quo. Y dada la adaptabilidad de los creadores de spam, las defensas de hoy pueden volverse rápidamente obsoletas a medida que los creadores de spam encuentran otros caminos. Como tal, los proveedores deben supervisar y refinar sus filtros continuamente. Cuando se evalúan las declaraciones de efectividad, es importante asegurarse de que los proveedores demuestren un compromiso y una infraestructura necesarios para mantener el paso de los creadores de spam.

Precisión: evitar falsos positivos a toda costa

Las soluciones antispam deben tener la más alta precisión posible –la capacidad del software antispam para distinguir los mensajes legítimos de los no deseados. Más de uno o dos falsos positivos –correos electrónicos legítimos que diseñaron mal filtros antispam se clasifican erróneamente como spam pueden representar el fracaso de un producto para un usuario. Cuando los usuarios no pueden depender de la precisión de filtrado antispam, se ven forzados a pasar por sus cuarentenas manualmente y borrar el spam, una actividad peligrosa y frustrante.

Por éstas y otras razones, Ferris Research³ fija el costo total del negocio de falsos positivos en \$3.5 mil millones de dólares anualmente en Estados Unidos. Los proveedores que se enfocan primeramente en eliminar los falsos positivos –el daño colateral de los filtros muy agresivos- y sólo entonces mejorar poco a poco la efectividad de bloque de spam tomaron la decisión correcta. Muchos proveedores decidieron seguir una ruta inicialmente agresiva, ofreciendo soluciones con un bloqueo de spam muy alto. A medida que las implicaciones comerciales de falsos positivos se han vuelto aparentes, estos proveedores se han visto forzados a retroceder, tratando un efecto colateral. Sus clientes empezaron a cuestionar el valor de una herramienta que rutinariamente complementaría una comunicación comercial de misión crítica.

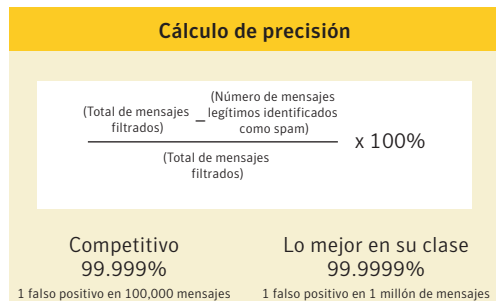
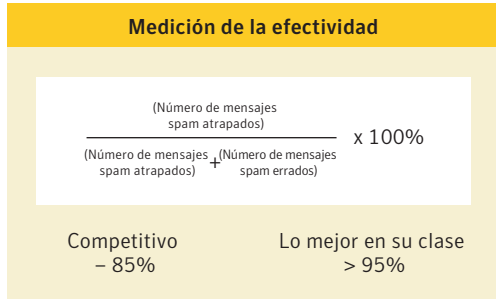
Proactividad y sensibilidad

De manera ideal, una solución antispam sería 100% exacta y 100% efectiva. Muchos proveedores se ven forzados a manejar un cambio por otra cosa. Para bloquear suficiente spam, la solución debe ser agresiva. Si la solución es demasiado agresiva, es probable que cause falsos positivos.

La alta precisión y efectividad en los filtros antispam son impulsados por dos acercamientos generales: sensible y proactivo.

Acercamiento	Descripción	Ejemplos	Notas
Sensible	Los filtros influyen en la investigación del spam real. El correo muy preciso y legítimo raras veces se bloquea.	<ul style="list-style-type: none"> Filtros con base en firmas Filtros impulsados por ataques 	Se requiere una infraestructura de análisis de spam extensa y bien administrada para lograr la efectividad
Proactivo	Los filtros examinan el spam en busca de una variedad de características de spam. Muy efectivos para bloquear los nuevos spam.	<ul style="list-style-type: none"> Filtros adaptables / bayesianos Filtros heurísticos Listas de filtrado basadas en recursos 	Los filtros necesitan afinarse o capacitarse constantemente, o la efectividad disminuye; susceptible a falsos positivos

³“El costo de los falsos positivos del spam”, de Ferris Research, agosto de 2003.



Dado el peligro del sobrebloqueo inherente a acercamientos más proactivos, las soluciones antispam deben combinar cuidadosamente técnicas de filtrado proactivas y sensibles. Los filtros sensibles ofrecen un resguardo importante contra los falsos positivos, complementando la efectividad de los filtros proactivos.

Administración mínima

Aunque muchas soluciones antispam apoyan el trabajo fuera de la caja, realmente liberan gran parte de la carga para combatir el spam del administrador y los usuarios finales. Por ejemplo, muchos filtros proactivos requieren capacitación importante por parte de administradores para la efectividad antispam inicial y continua. Algunas soluciones también tratan con falsos positivos recomendando que los administradores mantengan listas blancas. Aunque otras soluciones, bajo la apariencia de “administración individual de spam”, hacen que el usuario final haga el trabajo.

Como administrador que evalúa un producto antispam, la pregunta que debe hacer es: ¿Cuánto tiempo quiero dedicar para combatir y administrar el spam? La Figura 6 demuestra qué tan complejo se puede volver el proceso de capacitación de filtrado continuo.

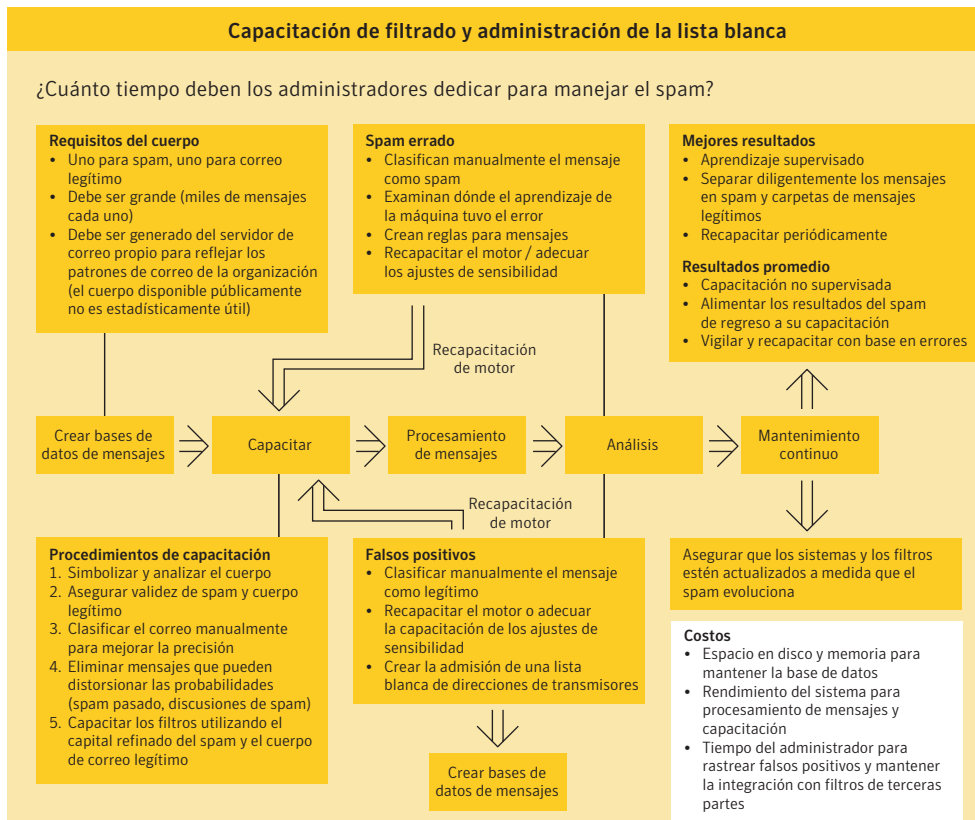


Figura 6. Capacitación de filtros y administración de la lista blanca

> **La solución Symantec**

El BLOC: análisis del spam y operaciones

La alta efectividad y precisión de los filtros Symantec es posible gracias a BLOC (iniciales en inglés de Centro de logística y operaciones Brightmail). BLOC consiste de diversos centros que trabajan en cooperativa en tres continentes, los cuales comprenden una red de protección continua que abarca el mundo entero. Estos centros de operaciones antispam son responsables de toda la afinación de tiempo real y los ajustes detrás de los filtros Symantec.

Las herramientas automáticas sofisticadas, asistidas y supervisadas por técnicos de BLOC, evalúan el correo en busca de nuevas variaciones de spam, y luego emiten filtros para identificar y capturar mensajes similares. BLOC ofrece continuamente filtros actualizados para filtrar software en funcionamiento en las instalaciones de los clientes. Los técnicos de BLOC desempeñan un papel importante para confirmar la identificación de posible spam. Esta combinación de automatización e intervención humana permite a Symantec Brightmail AntiSpam adaptarse en tiempo real a las técnicas de spam siempre cambiantes, dándoles una flexibilidad y precisión sin precedentes como filtro de spam.

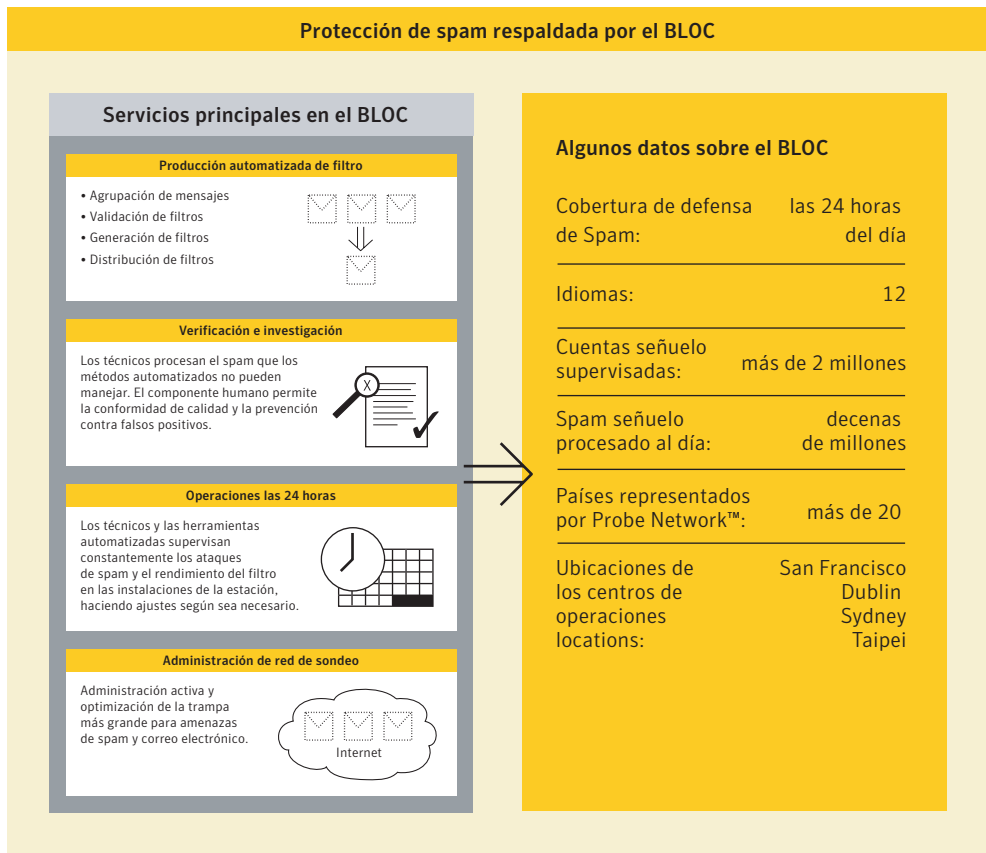


Figura 7. Protección de spam respaldada por el BLOC

El análisis de spam en el BLOC empieza con la red patentada Probe Network, una extensa gama de más de 2 millones de direcciones y dominios de correo electrónico señuelos, conocidos también como “trampas de spam”. Cuando se extiende con envíos de correo basura de los clientes, la Probe Network es estadísticamente representativa de más de 300 millones de bandejas de entrada de correo electrónico. La red mundial de cuentas de correo electrónico atrae y reúne grandes cantidades de spam –decenas de millones de mensajes spam pasan a través de la Probe Network cada mes. Conforme los mensajes entran al BLOC, los procesos automatizados y los técnicos expertos entran en acción, analizando el spam entrante y desarrollando contramedidas efectivas.

Esta infraestructura para atrapar el spam da a Symantec el conocimiento sobre los ataques de spam en el momento en que ocurren, haciendo posible que Symantec proteja automáticamente a sus clientes contra los ataques reales a la vez que rastrea la distribución y el contenido de los ataques de spam de todo el mundo. A diferencia de otros acercamientos donde los filtros necesitan capacitarse de tres a seis meses antes de ser efectivos, Probe Network de Symantec es *tiempo real*. Además, cuenta con más de seis años de antecedentes rastreando spam y escribiendo filtros antispam.

El tráfico de spam de tiempo real que fluye a través de la Probe Network impulsa los filtros sensibles y precisos de Symantec, como el BrightSig2™. Probe Network también ofrece un valioso recurso e información de URL de spam para el Brightmail Reputation Service y los filtros URL, respectivamente.

El otro componente esencial del proceso de análisis de spam de Symantec es el equipo de Business Intelligence. La misión del grupo de Business Intelligence es mantener a Symantec al frente en la guerra contra el spam. Entre sus actividades están:

- Analizar constantemente el tráfico de spam en busca de nuevas amenazas y nuevas defensas
- Analizar los sitios Web y el software de correo masivo que los creadores de spam usan con frecuencia
- Supervisar foros y las salas de charla frecuentados por los creadores de spam
- Mantenerse al corriente con la evolución de técnicas de los creadores de spam de manera que las defensas se puedan incorporar en publicaciones futuras

Tecnología de filtrado de varios niveles

No hay ningún método infalible contra el spam. Symantec tiene un acercamiento completo y de varios niveles para el filtrado del spam, empleando una variedad de técnicas de filtrado para mantener a los creadores de spam a raya. Algunos de los filtros examinan la fuente del correo electrónico, mientras que otros separan el contenido del mensaje, aventajando los datos de spam de tiempo real y las técnicas proactivas como el filtrado heurístico.

Tecnologías y arquitectura de Symantec Brightmail AntiSpam		
<p>Filtrado de reputación</p> <ul style="list-style-type: none"> • Fuentes Troyanas • Fuentes de spam de alto volumen • Fuentes seguras 	<p>Filtros URL</p> <ul style="list-style-type: none"> • URL fraudulentos • URL de correo • URL de HTTP • URL de adultos 	<p>Heurística</p> <ul style="list-style-type: none"> • Análisis de encabezados • Idioma foráneo • Análisis de contenido • Análisis estructural
<p>Firmas</p> <ul style="list-style-type: none"> • Confusión del cuerpo • Firmas borrosas del cuerpo • Firmas anexas 	<p>Arquitectura antispam</p> <ul style="list-style-type: none"> • Probe Network • Técnicos de BLOC • Arquitectura redundante • Filtrado en tiempo real • Detección de fraude • QA automatizado 	<p>Filtros definidos para el consumidor</p> <ul style="list-style-type: none"> • Lista personal de permiso • Lista personal de bloqueo • Filtros personales de idioma • Filtros de contenido • Lista de transmisores permitidos • Lista de transmisores bloqueados

Figura 8. Tecnologías y arquitectura de Symantec Brightmail AntiSpam

Symantec Brightmail AntiSpam incorpora 17 tecnologías diferentes de filtrado de antispam. Symantec evalúa continuamente nuevas técnicas de filtrado y añade nuevas tecnologías a su arsenal. Cada nuevo acercamiento se evalúa para asegurar que no comprometa la rigurosa tasa de precisión de Symantec –la cual actualmente es de un falso positivo en un millón de mensajes, una tasa de precisión de 99.9999%.

BRIGHTMAIL REPUTATION SERVICE

El bloqueo basado en la reputación es una poderosa técnica de filtrado que examina la calidad o reputación del origen de envío o servidor de correo electrónico. Hasta este punto, Symantec supervisa cientos de miles de fuentes de correo electrónico para determinar cuánto correo electrónico enviado de estas direcciones es legítimo y cuánto es spam. Estos datos se incorporan en el Brightmail Reputation Service. Al rastrear datos como patrones de correo, la presencia de proxy abierto o servidores de correo no seguros, volúmenes de mensajes enviados y quejas, el Brightmail Reputation Service puede determinar un valor de reputación para un determinado transmisor de correo electrónico o dirección de IP. En algunos casos, este valor se usa para permitir o bloquear transmisores. En otros casos se utiliza en conjunto con otros filtros.

El Brightmail Reputation Service incluye actualmente las siguientes listas de direcciones de IP, que se compilan y actualizan continuamente:

- **Lista de proxy abierto.** Direcciones de IP que son proxy abiertos usados por creadores de spam.
- **Lista segura.** Direcciones de IP de las que virtualmente ningún correo electrónico de salida recibe spam.
- **Lista sospechosa.** Direcciones de IP de las que virtualmente todo el correo electrónico de salida recibe spam.

A diferencia de otras colecciones de listas de origen, el Brightmail Reputation Service es:

- **De gran alcance.** Dado que Symantec filtra más del 15% del correo electrónico de Internet del mundo (más de 100 mil millones de mensajes al mes) y protege a más de 300 millones de bandejas de entrada de usuarios, Symantec está en una posición única para evaluar la reputación de los orígenes del correo electrónico. Con acceso a estos datos, el Brightmail Reputation Service representa un filtro importante de actividad de servidor de correo.
- **Automatizado e impulsado por datos.** La inclusión y eliminación de las listas se basa completamente en los patrones de tráfico de los servidores de correo. Las organizaciones o los individuos no pueden solicitar ni pagar para ser añadidos o eliminados de ninguna lista en el Brightmail Reputation Service.
- **Proactivo y preciso.** Otras listas tienen personal malo y simplemente agregan información, dando como resultado sitios con listas negras inadecuadas. Por otro lado, el Brightmail Reputation Service genera con regularidad su base de datos buscando proactivamente servidores inseguros y transmisores de altos volúmenes, permitiendo actualizaciones rápidas y automáticas a la lista. Por ejemplo, en el caso de la lista de proxy abierto, una vez que un servidor de proxy abierto identificado por el Brightmail Reputation Service es asegurado por el propietario, la dirección de IP del servidor se eliminará automáticamente cuando las listas se regeneren nuevamente (cada hora).
- **Automáticamente incorporado.** Al igual que otros filtros usados por Symantec Brightmail AntiSpam, no se requiere ninguna administración continua.

Filtros de reputación

Táctica: las ventajas alcanzan Probe Network y las capacidades analíticas del BLOC para crear un perfil de reputación de fuentes de correo electrónico

Efectivo contra: creadores de spam de gran escala que usan grandes redes con muchos dominios y direcciones de IP

Filtros disponibles: listas de direcciones de IP actualizadas dinámicamente de servidores proxy abiertos, servidores seguros y servidores sospechosos

Único para Symantec

FILTROS HEURÍSTICOS

La tecnología heurística proporciona una estructura muy proactiva para combatir el spam. Los filtros heurísticos analizan el encabezado, el cuerpo y la información del sobre de los mensajes de entrada, revisando la presencia de distintas características de spam. Por ejemplo, el exceso de signos de exclamación o mayúsculas aumentaría la *calificación de spam* de un mensaje. A cada mensaje se le asigna una calificación total, la cual se compara con un umbral que determina si el mensaje es spam o no. Los filtros heurísticos, una vez que están *capacitados* para determinar qué apariencia tiene un spam y un correo legítimo, puede ser muy efectivo para identificar nuevo spam.

La desventaja de muchos filtros heurísticos es que pueden crear una carga administrativa sustancial. Lo peor, si no se capacita adecuadamente y se mide la precisión, pueden producir números significativos de falsos positivos.

En Symantec Brightmail AntiSpam, se utilizan pruebas de análisis heurístico para determinar la probabilidad de que un mensaje sea spam. Cada prueba se mide para reducir falsos positivos. La probabilidad total de que un mensaje es spam se examina para determinar una calificación total.

La heurística de Symantec se afina y actualiza para dar la precisión estándar⁴ de 99.9999% de Symantec Brightmail AntiSpam. A diferencia de otras soluciones, el filtrado heurístico no es la única herramienta que utiliza Symantec contra todos los ataques de spam. Asimismo, antes de que los filtros se implantan en las instalaciones del cliente, Symantec optimiza los filtros, midiendo cada heurística con base a qué tanto representa una característica de spam. Los filtros heurísticos de poca medición –por ejemplo, puntuación incorrecta- resguardan contra los falsos positivos. Los filtros de mayor medición, como aquellos que coinciden un intervalo conocido de una dirección de IP de un creador de spam, son muy efectivos para diferenciar el spam de los mensajes legítimos.

Los filtros heurísticos de Symantec no tienen un impacto en los recursos del administrador. No se requiere afinación ni capacitación del cliente, ya que Symantec reduce constantemente los filtros inefectivos o demasiado agresivos antes de implantar automáticamente los filtros en las instalaciones del cliente. Además, los filtros no dependen de un idioma interpretado, como Perl, el cual puede ser un servidor un recurso intensivo, obstruyendo el rendimiento del servidor conforme los mensajes se analizan.

FILTROS DE ENCABEZADOS

Los filtros de encabezados de Symantec son una combinación de acercamientos proactivos y sensibles. Para identificar proactivamente el *spam de primera vez*, los filtros de encabezados consisten de reglas de filtrado basadas en expresión que hacen uso de características comunes o tendencias que están presentes en los mensajes de spam. Ejemplos de características indicadoras de spam que un filtro de encabezados analizaría incluyen:

- **Filigranas o herramientas de creador de spam.** Rastros de información dejados en mensajes por algunas herramientas de creador de spam, por ejemplo, el nombre del programa utilizado para enviar el mensaje.
- **Zonas de tiempo modificadas.** Por ejemplo, si la zona de tiempo está apagada durante más de 12 horas.
- **Líneas con trampa recibidas.** Por ejemplo, si el mensaje declara que proviene de un MTA en una organización que el BLOC conoce.

Los filtros de encabezados también se dirigen a mensajes de spam específicos que han pasado por el sistema de análisis de spam. Estos filtros específicos de ataque son muy efectivos, aprovechando Symantec Probe Network y el sistema de filtro.

Filtros heurísticos

Táctica: Busca proactivamente características comunes de spam en todas las partes del mensaje y asigna una calificación; si la calificación rebasa el umbral, el mensaje es spam

Efectivo contra: Nuevo spam

Exactitud y rendimiento probados de la tecnología heurística de Symantec

Filtros de encabezados

Táctica: atrapa el spam con filtros con objetivo basado en encabezados

Efectivo contra: mensajes con características indicadoras de spam en los encabezados

⁴Anti-Spam Services for SMBs and Middle-Market End-Users
Nota de investigación por J.P. Gownder de Yankee Group del 25 de febrero de 2003

FILTROS BRIGHTSIG2

La tecnología firma de Symantec es el catalizador para la tasa de precisión líder en la industria de Symantec. En general, las firmas de spam trabajan destilando un ataque específico de spam hasta una cadena única de bits, o una *firma*. Esta huella esencial de un ataque de spam se puede usar para identificar variantes del ataque. La precisión se conserva porque las firmas se basan en el spam real.

Los creadores de spam respondieron a la tecnología de firma de primera generación introduciendo grandes cantidades de personalización y ofuscación de HTML. Symantec, a su vez, respondió con su tecnología patentada BrightSig2. La tecnología BrightSig2 es la piedra angular de la tecnología de firma de Symantec. La tecnología caracteriza ataques de spam utilizando algoritmos patentados, los cuales se añaden a una base de datos de spam conocidos. BrightSig2 coincide mensajes aparentemente al azar que originan un solo ataque, lo cual acelera y reestructura la creación e implantación del filtro. Este proceso permite a Symantec crear filtros de objetivos estrechos sin tener que escribir numerosos filtros contra un solo ataque. Al destilar un ataque complejo y cambiante de su ADN, se pueden desviar más spam con un solo filtro.

BrightSig2 tiene ahora defensas específicas contra el spam de HTML, específicamente combatiendo ruido de HTML y cálculo aleatorio (comentarios, constantes, malas etiquetas) que los creadores de spam insertan para evadir filtros.

FIRMAS ANEXAS

Los anexos de mensajes han sido por mucho tiempo una herramienta favorita de los creadores de spam. Al atacar a un archivo o imagen con nombre engañoso a un correo electrónico, los creadores de spam tientan a los receptores a hacer clic y abrir el archivo. Con frecuencia, el resultado es molesto: el receptor se enfrenta a una imagen explícitamente ofensiva. Otras veces, el anexo puede tener contenido malicioso, como un caballo de Troya, gusano o un archivo ejecutable que hace estragos en la computadora del receptor. En respuesta, muchas organizaciones simplemente borran todos los tipos de anexos de cierto tipo (por ejemplo, exe o zip) que han causado problemas, incluso si un anexo de entrada particular es una comunicación comercial legítima.

Las firmas anexas, que tienen objetivo específico en anexos MIME, son el más reciente ejemplo de la tecnología de firma de Symantec. Con algoritmos borrosos similares a BrightSig2, las firmas anexas permiten a Symantec crear filtros basados en un anexo MIME particular (por ejemplo, una imagen pornográfica específica usada en un ataque de spam de tiempo real) e impiden que ese anexo llegue a los clientes. Las firmas de anexos hacen innecesario bloquear categorías completas de ciertos anexos.

Filtros BrightSig2

Táctica: Despoja HTML al azar de spam y utiliza lógica borrosa para agrupar mensajes

Efectivo contra: Ataques de spam basados en HTML altamente aleatorizados

Único para Symantec

Firmas anexas

Táctica: extrae una firma precisa de anexos indeseables o maliciosos en mensajes de spam (por ejemplo, imagen pornográfica o gusano)

Efectivo contra: Imágenes incrustadas, ejecutables, archivos zip, etc.

Único para Symantec

FILTROS URL

Esta versión de Symantec Brightmail AntiSpam continúa la innovación en tecnologías de filtrado basadas en URL. Los filtros URL ahora tratan enlaces URL *mailto*, impidiendo que los usuarios finales respondan a los creadores de spam vía electrónica. Esta nueva generación de filtros URL también mejora la capacidad de Symantec para invertir nuevos métodos de enmascaramiento de URL y técnicas de ofuscación desarrolladas por los creadores de spam en meses recientes.

Esta tecnología de filtro URL, con patente pendiente, aprovecha los elementos de infraestructura que son únicos para Symantec. Mediante el uso de datos de spam de tiempo real, Symantec desarrolla una lista de sitios Web de creadores de spam. En las instalaciones de la estación, los filtros URL comparan enlaces incrustados en mensajes con la lista de URL de spam que se mantienen en Symantec. Esta lista se crea utilizando una combinación de procesos fuera de línea y en tiempo real, incorporando los URL de las siguientes fuentes:

- **Datos de Probe Network.** La mayoría de los URL de spam se extraen de spam entrante y datos históricos de Probe Network.
- **Listas confiables de terceras partes.** Las listas de URL que mantienen otros proveedores y socios también se verifican minuciosamente, se revisan en forma cruzada y se incorporan en la lista de URL de spam de Symantec.

Los filtros URL son especialmente efectivos contra:

- **URL enmascarados.** Los filtros URL invierten los intentos de los creadores de spam para cifrar los URL con caracteres extraños. Esta versión más reciente de filtros URL cuenta con defensas ampliadas contra la ofuscación de URL y tácticas de evasión de filtros.
- **Cálculo aleatorio extremo.** Los filtros URL pueden identificar un mensaje de spam incluso si los creadores de spam ponen muchos cálculos aleatorios en un mensaje que otros filtros no son efectivos.
- **Mensajes muy cortos.** Si un mensaje consiste en texto HTML inocuo o simplemente un enlace URL a una página Web de spam, los filtros URL identificarían y bloquearían el mensaje.

TECNOLOGÍA ANTISPAM DE IDIOMAS FORÁNEOS

Symantec estima que entre el 10 y el 20% de todo el spam mundial está escrito en idiomas que no son inglés, haciendo el spam que no es inglés un problema crítico para cualquier compañía que tiene negocios fuera de Estados Unidos. Conforme el spam multilingüe se convierte en un problema mayor para las organizaciones, las soluciones antispam deben tomar en cuenta el idioma en el cual se escriben los mensajes. Con los nuevos centros de operaciones antispam en Taipei y Sydney, Symantec aumentó su presencia mundial y base multilingüe para ayudar a impedir que el spam enviado de países foráneos pase desapercibido.

Symantec Brightmail AntiSpam 6.0 tiene capacidades de identificación de idiomas y una nueva serie de heurística que aplica sólo a ese idioma. Al identificar el idioma de un mensaje si está escrito en una variedad (11) de idiomas, Symantec Brightmail AntiSpam puede activar sólo los filtros que aplican al idioma del mensaje, dando como resultado un mejor rendimiento. Además, utilizando el Brightmail Plug-In for Outlook, los usuarios finales pueden ahora definir los idiomas en los que desean recibir mensajes.

Aunque las características de identificación de idioma siempre se implantan en los filtros heurísticos de Symantec, las acciones por idioma están apoyadas actualmente sólo cuando la conexión se implantan las computadoras. La conexión es una barra de herramientas que permite a los usuarios personalizar los aspectos de filtrado de Symantec.

Filtros URL

Táctica: identifica URL de spam en los mensajes. Elimina caracteres que ocultan una dirección de un sitio Web en un mensaje

Efectivo contra: ataques de spam de llamada de acción, ataque de spam con URL comunes y cuerpos radicalmente diferentes

Único para Symantec

Defensas contra spam que no es en inglés

Táctica: tratar spam en un idioma que no es inglés con una combinación de tecnología e infraestructura

- ✓ Tecnología de filtrado agnóstica de idioma
- ✓ Identificación de idioma
- ✓ Heurística específica al idioma
- ✓ Técnicos multilingües de BLOC
- ✓ Preferencias de idioma por usuario

FILTRADO DE CONTENIDO Y OTRAS HERRAMIENTAS DEL ADMINISTRADOR

Aunque los administradores de Symantec Brightmail AntiSpam nunca necesitan crear filtros personalizados, el software ofrece herramientas de personalización gráfica para permitir a los administradores ser más ágiles para enfocarse en el correo no deseado.

Con el uso del Custom Filters Editor, parte de la interfase del Centro de Control, los administradores pueden crear filtros de contenido para bloquear o manejar proactivamente el correo que no cumple con los criterios del spam.

Con esta interfase gráfica, los administradores pueden:

- Filtrar correo electrónico de listas de mercadotecnia que generan quejas del usuario o usan ancho de banda excesivo
- Controlar el volumen de mensajes y proteger el ancho de banda filtrando mensajes de tamaño excesivo
- Bloquear tipos específicos de contenido adulto
- Bloquear cartas de cadena
- Bloquear un virus particular transmitido por correo electrónico

Symantec también ofrece administradores con un host de otros métodos para personalizar el filtrado, por ejemplo, utilizando listas de transmisores permitidos y bloqueados, umbrales de spam, etc.

Administración de filtro y actualización de motores

Cada minuto, el software de Symantec implantado en las instalaciones de las estaciones inicia una conexión HTTPS segura con BLOC. Utilizando esta conexión, las actualizaciones de los filtros fluyen de BLOC a las instalaciones de la estación. Con el uso de un mecanismo similar, las estadísticas de filtrado de spam de las instalaciones de los clientes se transmiten a BLOC, permitiendo al BLOC calibrar el rendimiento y la efectividad de los filtros implantados.

Este proceso mundial de actualización de filtros de spam tiene muchas ventajas:

- **Fácil administración.** Las reglas y los filtros se descargan e instalan automáticamente y de forma segura. Los filtros heurísticos se actualizan automáticamente cada cierto tiempo. Las nuevas firmas de spam y filtros se extraen de Symantec automáticamente, en tiempo real, siempre que hay un nuevo suceso de spam. A menos que seleccionen filtros de aumento que utilizan el Custom Filters Editor, los administradores nunca necesitan escribir manualmente, capacitar o actualizar reglas o filtros existentes.
- **Protección antispam.** El software de Symantec en las instalaciones del cliente siempre tiene los filtros antispam más actualizados, y BLOC tiene visibilidad constante para determinar la efectividad de esos filtros.
- **Seguridad y privacidad.** La validación de dos direcciones garantiza que las reglas de filtrado provienen de Symantec y ninguna otra entidad puede hacer trampa con ellas. Además, ninguna información confidencial del cliente se transmite a Symantec durante la recopilación del paquete de estadísticas agregadas de reglas.
- **Disponibilidad.** El software de filtrado nunca se detiene durante el proceso de actualización. Esta capacidad impide que pasen mensajes durante el proceso de actualización, lo cual dejaría al servidor de correo desprotegido.

> Conclusiones

El ciclo de vida del spam continúa evolucionando. Los creadores de spam están escalando la batalla con nuevas técnicas de evasión y diseminación de filtros.

En respuesta, Symantec ha fortalecido su motor de filtrado y su acercamiento al problema de spam. Tecnologías patentadas como BrightSig2 y el Brightmail Reputation Service se han actualizado para tratar el spam más complejo y voraz: spam aleatorizado y spam retransmitido a través de servidores de proxy abierto desprevenidos. Otros filtros, como los filtros heurísticos, evalúan proactivamente la probabilidad de que un mensaje sea spam. Los filtros URL actualizados combaten el spam con URL, una categoría de spam nueva y de gran crecimiento.

Éstos y otros filtros antispam que utiliza Symantec Brightmail AntiSpam están respaldados por los recursos para combatir spam más grandes y más completos. Probe Network patentada y la infraestructura BLOC de Symantec distribuida mundialmente son niveles adicionales de defensa, completando una respuesta precisa, efectiva y única al problema del spam.

Para obtener más información sobre los productos y servicios de Symantec, visite <http://www.symantec.com.mx/>.

WORLD HEADQUARTERS

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1 800 441-7234
1 541 334-6054**

www.symantec.com

SYMANTEC AMÉRICA LATINA

**9155 South Dadeland Blvd., Suite 1100
Miami, FL 33156
Teléfono: 305-671-2300
Fax: 305-671-2350**

**<http://www.symantec.com/la/>
<http://www.symantec.com.mx/>**

Symantec opera a nivel mundial en más de 35 países. Para más información sobre las oficinas y los números de contacto en los diferentes países, consulte nuestro sitio Web: www.symantec.com.