



SpamKiller Whitepaper

Versión 2.3

Greg Day
Arquitecto de Soluciones

<u>1. PRÓLOGO</u>	3
<u>2. TECNOLOGÍAS ANTI-SPAM</u>	3
<u>2.1 FILTRADO DE CONTENIDO</u>	3
<u>2.1.1 FALSOS</u>	4
<u>2.2 LISTAS NEGRAS</u>	4
<u>3. LA NECESIDAD DE LAS EMPRESAS HOY DÍA</u>	5
<u>3.1 LAS SOLUCIONES ANTI-SPAM DE MCAFEE</u>	5
<u>3.2 LA LÍNEA DE PRODUCTOS SPAMKILLER</u>	6
<i>Microsoft Exchange 2000 Small Business</i>	<i>6</i>
<i>SpamKiller 2.1 for WebShield Appliances 2.7</i>	<i>7</i>
<i>SpamKiller 2.1</i>	<i>7</i>
<i>SpamKiller 2.1 for Lotus Domino</i>	<i>7</i>
<u>4. ¿CÓMO FUNCIONAN LOS PRODUCTOS SPAMKILLER?</u>	8
<u>4.1 ¿CÓMO RECIBE CADA REGLA SU PUNTUACIÓN PREDEFINIDA?</u>	8
<u>4.2 REGLAS DEL SPAMASSASSIN</u>	9
<i>Reglas de Encabezamiento</i>	<i>9</i>
<i>Reglas de cuerpo de mensaje</i>	<i>9</i>
<i>Reglas de cuerpo de mensaje en formato crudo</i>	<i>10</i>
<i>Reglas de cuerpo de mensaje Integral</i>	<i>11</i>
<i>Reglas URI</i>	<i>11</i>
<i>Meta-Reglas</i>	<i>11</i>
<u>4.3 ¿QUÉ OCURRE CUANDO UN MENSAJE ES CLASIFICADO COMO SPAM?</u>	12
<i>Opciones comunes de filtrado de servidor de archivos y gateway</i>	<i>12</i>
<i>Opciones exclusivas de SpamKiller for WebShield for Appliances</i>	<i>13</i>
<i>Enrutando spam a través del SpamKiller for WebShield Appliances</i>	<i>13</i>
<i>Opciones exclusivas de SpamKiller for Exchange Small Business</i>	<i>14</i>
<i>Enrutando spam a través del SpamKiller for Microsoft Exchange Small Business</i>	<i>14</i>
<u>4.4 EDICIÓN DE REGLAS Y PUNTUACIONES</u>	14
<u>4.5 ACTUALIZACIÓN DEL SPAMKILLER</u>	16

1. Prólogo

Hoy día, el correo electrónico es reconocido como la herramienta de comunicación más importante en los negocios. En una reciente investigación conducida por el META Group, un 80 por ciento de los usuarios prefieren el correo electrónico al teléfono como herramienta de comunicación de negocios, pues permite una comunicación rápida con varias personas, además de generar un registro escrito de la interacción.

No causa sorpresa que los usuarios estén empezando a encontrar dificultades con el volumen de mensajes de correo recibido diariamente, y algunos reciben más de 200 mensajes, los cuales pueden consumir varias horas para su gestión.

En un informe reciente de IDC, se relató que más de 20.000 millones de mensajes de correo eran enviados diariamente en el 2002, y hay previsiones de que dicho número alcanzará los 60.000 millones hasta 2006. Con el creciente uso del correo, los administradores y usuarios finales están buscando métodos de optimizar el tiempo de gestión de mensajes de correo.

Uno de los puntos de concentración son los mensajes de spam, que la industria define como **UCE** (Mensajes Comerciales No-solicitados) o **UBE** (Mensajes en Masa No-solicitados). Los más comunes son mensajes de spam enviados públicamente a usuarios que ni los han solicitado ni los quieren realmente.

Debido a que el correo electrónico resultó ser una forma común de comunicación tanto profesional como personal, los vendedores de productos y/o servicios aprovecharon la oportunidad para usar el correo electrónico como una forma de poner sus mensajes ante nosotros.

Financieramente, el marketing por correo electrónico es muy sensato, ya que el precio de las listas de distribución empieza en \$10 (direcciones electrónicas sin filtrado) y alcanza a cerca de \$500 por mil direcciones altamente dirigidas de clientes. Con las direcciones electrónicas de contacto, los costos de producción del marketing por correo electrónico son mínimos. Enviar el mismo mensaje de marketing por el correo tradicional (correo directo) acarrearía costos de material y postales.

Uno de los primeros incidentes de spam ocurrió en abril de 1994, cuando dos abogados de Canter & Siegel (C&S) bombardearon más de 6.000 grupos en foros de discusión de Usenet en menos de 90 minutos. El contenido era una propaganda de la "Lotería del 'Green Card' Norteamericano – una oportunidad para que los no-Americanos participen en un sorteo de visado de trabajo en EE.UU., con posibilidades muy remotas". C&S se ofrecía para rellenar formularios por sólo \$95 por persona o \$145 por pareja (detalle: los formularios del "green card" son gratis). Ellos y su proveedor de acceso a Internet fueron echados al olvido debido a quejas provenientes de todas partes del mundo. El proveedor "Internet direct" cerró la cuenta de C&S y los abogados lo amenazaron con un proceso de \$250.000 si no reactivaban la cuenta. La amenaza no resultó en nada, pero publicaron, tras el incidente, un libro titulado "How to Make a Fortune on the Information Superhighway" (*Cómo hacer fortuna en la Autopista de la Información*), con consejos sobre esquemas para ganar dinero utilizando Internet.

Desde entonces, los usuarios y las organizaciones empezaron a adoptar técnicas existentes y nuevas para bloquear los mensajes no-solicitados.

2. Tecnologías Anti-spam

2.1 Filtrado de contenido

Muchos bloqueadores de spam de la primera generación estaban basados en el uso de la tecnología existente de filtrado de contenido para detectar y eliminar mensajes de correo electrónico según palabras-claves o frases conocidas por su relación con mensajes no-solicitados. Esta es, todavía, una parte fundamental de muchas de las soluciones de hoy.

Por ejemplo, si un mensaje contuviera la palabra Viagra, probablemente sería una propaganda, que es considerada spam. Por lo tanto, se debería eliminarlo. El problema es que dicha regla no es adecuada para todas las personas. Por ejemplo, si usted trabaja en el ramo farmacéutico, "Viagra" sería una palabra válida usada en los mensajes diarios que necesitaría recibir.

Los proveedores de anti-spam también mencionan la analogía de la "pechuga de pollo". Una regla común para bloquear mensajes con contenido sexual sería filtrar la palabra "pechuga". Sin embargo, dicha regla acarrearía el bloqueo de mensajes legítimos tales como los que se refirieran al ingrediente "pechuga de pollo" en una receta culinaria.

2.1.1 Falsos

Falsos Positivos. Esto representa cuál es el aspecto más importante de las tecnologías anti-spam. Aunque quisiéramos limpiar de nuestros buzones los mensajes no-solicitados, no queremos que los mensajes legítimos sean excluidos, ni filtrados, ni que sufran ningún retraso hasta llegar a nosotros, pues las implicaciones de costo serían mucho mayores. Imagínese en una situación delicada y que el cliente no quiere recibir su cotización por haberla filtrado como spam, y la competencia, entonces, se gana el negocio. Este es el concepto de falsos positivos: mensajes legítimos que son detectados como spam.

Falsos Negativos. Los productos anti-spam son generalmente evaluados según el número de mensajes de spam detectados. Los que no son detectados, pero constituyen mensajes no-solicitados, son conocidos como "falsos negativos". La realidad para cualquier empresa es que el costo de los falsos positivos puede ser mucho más alto que el costo de los falsos negativos.

2.2 Listas Negras

En abril de 2003, AOL Time Warner procesó a cinco grandes fuentes de spam. AOL, el mayor proveedor de acceso a Internet de EE.UU., cree que spammers enviaron a sus suscriptores cerca de mil millones de mensajes de spam, generando más de ocho millones de quejas. El spam consistía en pornografía, productos "milagrosos" para mejorar la forma física, productos para reducción de peso y esquemas financieros. Las acciones, que reclaman un total de \$10 millones en daños, además de la interrupción de los spammers en sus actividades de envío de mensajes, fueron interpuestas contra cinco spammers (dos supuestamente identificados y los otros tres no identificados hasta que se puedan confirmar sus identidades)

Todo eso indica que hay un gran número de fuentes conocidas de spam, contra las cuales surgió el segundo y, asimismo, uno de los métodos más comunes de prevención de spam: las listas negras de tiempo real (RBL). Generalmente, se las ofrece bajo suscripción.

El objetivo de las RBL es bloquear mensajes según el host del mensaje o la cuenta de correo electrónico del remitente. El valor de dicha metodología es que usted no necesita examinar la validez del mensaje a través de filtrado de contenido o alguna otra técnica. Todos los mensajes provenientes de sitios Web o de usuarios listados en una RBL son manejados como spam.

Como el filtrado, las RBL no son la solución perfecta. Las RBL son dinámicas y muchas utilizan un método de embudo de fuentes de spam, empezando por el bloqueo del sitio Web identificado hasta que se pueda refinar dicho parámetro hasta llegar a una fuente específica.

Esconderse entre usuarios legítimos de correo electrónico es una táctica común de las fuentes de spam para esquivarse de la detección. Así, por un pequeño período de tiempo, los que no son fuentes de spam pueden tener el mismo destino de la fuente, hasta que el proveedor de la RBL pueda refinarla con la información exacta de la fuente de spam.

3. La necesidad de las Empresas hoy día

Desde la década de los ochenta, hemos visto un número cada vez mayor de métodos de disfrazar mensajes no-solicitados como mensajes legítimos, y contramedidas utilizadas para detectar y eliminar dichos mensajes.

Se calcula que, hoy, el spam cuesta a las empresas norteamericanas \$8.900 millones, \$2.500 millones a las empresas europeas y otros \$500 millones a proveedores de servicios norteamericanos y europeos, según una investigación de Ferris Research.

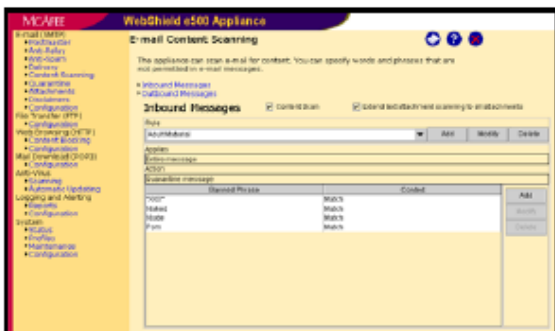
Ferris sugiere que los ISP norteamericanos clasifican como spam a un 30% de todos los mensajes recibidos, mientras el spam es responsable del 15% al 20% de los mensajes recibidos por grandes empresas con oficina principal en EE.UU. Eso es debido al hecho de que una parte de los mensajes corporativos de correo electrónico son internos.

En el Reino Unido, BT Openworld destacó, en una nota de prensa, que, al monitorear mensajes de correo electrónico durante una semana de marzo de 2003, más del 40% de los mensajes enviados a usuarios en el país eran spam, y uno a cada 220 estaba infectado por virus.

Para que una solución anti-spam sea eficiente hoy día, debe caminar por la tenue línea que divide la eliminación de mensajes no-solicitados y la garantía de que los mensajes legítimos puedan ser enviados y recibidos por los usuarios sin interrupción.

3.1 Las soluciones anti-spam de McAfee

La protección contra spam siempre integró las soluciones ofrecidas por McAfee desde 2001, cuando el dispositivo WebShield e500 fue lanzado.



El dispositivo, instalado en su gateway, monitorea los protocolos comunes de Internet (SMTP/HTTP/FTP y POP3) en búsqueda de códigos maliciosos, además de ofrecer gestión de seguridad de Web / correo electrónico que incluye métodos comunes de filtrado de mensajes no-solicitados.

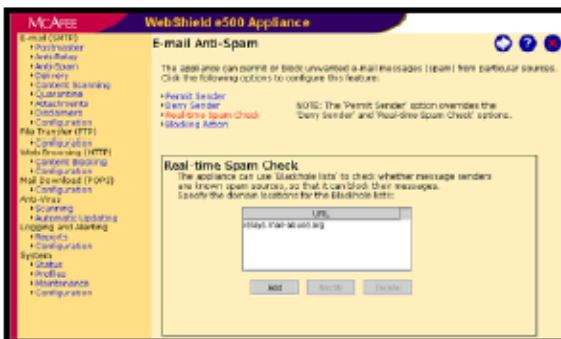
Dichos métodos son los siguientes:

- Filtrado de contenido del tráfico SMTP, en búsqueda de palabras-claves y frases utilizadas normalmente en mensajes no-solicitados.

- Opciones anti-spam –

(1) Capacidad de utilizar listas bajo suscripción (conocidas como "listas negras") de direcciones electrónicas y dominios conocidos por enviar mensajes no-solicitados.

(2) Filtrado de mensajes de correo electrónico según la dirección electrónica.



Hoy día, ofrecemos los dispositivos con varias especificaciones de hardware distintas, según sus necesidades. Todos los dispositivos poseen

el mismo software.

Los productos GroupShield también ofrecen filtrado de spam a través de la verificación de líneas de asunto y del texto de los mensajes, y pueden eliminar mensajes no-solicitados según palabras-claves y frases.

Con el crecimiento global de los mensajes no-solicitados, McAfee adquirió la tecnología de scan SpamAssassin, de Deersoft, en el inicio de 2002, y hoy día, es la tecnología central utilizada en los productos corporativos SpamKiller, de McAfee.

Ambos son productos que se pueden usar independientemente, además de ser integrados al antivirus GroupShield y a los dispositivos WebShield para aumentar su capacidad de gestión de correo electrónico.

Más detalles sobre los productos disponibles y las plataformas soportadas pueden ser encontrados en el sitio Web corporativo de McAfee.

<http://www.networkassociates.com/us/products/mcafee/antivirus/antispam/category.htm>

3.2 La línea de productos SpamKiller

En este documento, usted encontrará referencias al engine SpamAssassin, que es la tecnología de scan utilizada.

SpamKiller es la marca de productos creada por McAfee para utilizar este engine. A lo largo de 2003, McAfee lanzará el SpamKiller para varias plataformas. El objetivo es brindar una cobertura flexible y completa para su red.

El primer producto lanzado en el mercado fue:

SpamKiller 2.0 for Microsoft Exchange 2000 Small Business

Limitado al scan de hasta 500 buzones en instalaciones del Microsoft Exchange 2000, "escucha" a la API OnSyncSave, que es responsable de guardar nuevos mensajes en el Buzón del usuario. Dicha API permite que el SpamKiller intercepte el mensaje y lo transmita al engine SpamAssassin para que lo verifique.

Debido a que este producto funciona en el entorno Exchange 2000, posee algunas opciones específicas de la plataforma:

- Capacidad de encaminar mensajes de spam a las Carpetas de Basura Electrónica del Buzón de los usuarios o a una carpeta pública. Como el producto es integrado al entorno Exchange, tiene el permiso de crear carpetas de Basura Electrónica en el buzón del usuario y encaminar mensajes a dicho buzón.
- Incluye la lista personal de contactos de los usuarios en la "lista blanca" (lista de remitentes confiables). Los usuarios pueden editar sus listas negras y blancas a través de una interfaz de Web que acompaña al producto.
- Debido a que es basada en el entorno Microsoft 2000, la versión para pequeñas empresas permite el scan de todos los buzones o de un grupo específico de buzones de usuarios del Active Directory.

Lanzado en agosto de 2003:

SpamKiller 2.1 for WebShield Appliances 2.7

El SpamKiller for WebShield Appliances utiliza los filtros existentes en los dispositivos, los cuales interceptan el tráfico de SMTP para buscar virus y filtrar el contenido. A medida que los filtros capturan los mensajes de SMTP, los transmiten al engine SpamAssassin para que los someta al scan antes que se los decompongan para el scan antivirus.

La versión 2.7 del software de los dispositivos WebShield posee una versión de prueba del SpamKiller válida por 30 días.

Si quiere utilizarla tras el período de prueba de 30 días, usted necesitará adquirir una licencia contáctese a su ejecutivo de ventas. Entonces, Network Associates le enviará un CD de actualización, que convierte la licencia provisional en la licencia permanente que usted adquirió.

Nota: NO es necesario que se reinstale el software del dispositivo WebShield.

Los dispositivos WebShield ya ofrecen algunas opciones básicas de bloqueo de spam, tales como filtrado de contenido, creación de listas blancas o negras propias y suscripción a listas de tiempo real. La inclusión de la tecnología SpamAssassin hace que los dispositivos se conviertan en una solución completa antivirus y anti-spam.

Lanzamiento previsto para el final de 2003:

SpamKiller 2.1 for Microsoft Exchange

Estará disponible con el antivirus GroupShield y como un producto separado. El producto podrá ser instalado como un módulo externo a la consola del GroupShield o como un producto autónomo.

Su operación será muy semejante a la de la Small Business Edition anterior, salvo por el hecho de que no habrá ninguna limitación al número de buzones en que el producto podrá realizar el scan. Se espera que el producto soporte al Microsoft Exchange 2000 y 2003.

SpamKiller 2.1 for Lotus Domino

Su operación será semejante a la de la versión para el Microsoft Exchange mencionada arriba. Se espera que su soporte incluya las versiones 5.0 y 6.0 del Domino.

Información más detallada sobre dichas versiones estará disponible en el sitio Web de McAfee a medida que se libere cada producto.

Soporte de la localización

Hasta el presente momento, las reglas del engine SpamAssassin son predominantemente dirigidas a la detección de spam con contenido de texto en inglés.

Para explicar esto, veamos el ejemplo de las reglas de encabezamiento. Una regla de encabezamiento que busca el historial de enrutamiento del mensaje independientemente del idioma, por ejemplo, verificando si existe en la línea de asunto una palabra-clave como "teen", que es específica de la lengua inglesa. En este ejemplo, la palabra usada es universalmente reconocida, así como muchas otras palabras o giros usados normalmente en mensajes de spam. Por ejemplo, "Viagra" es una marca común al producto en la mayoría de los idiomas.

En el futuro, consideraremos la posibilidad de incluir reglas localizadas de contenido textual. Sin embargo, según la experiencia acumulada en el ramo, un buen porcentaje del spam recibido en todos los países hoy día se escribe en inglés norteamericano.

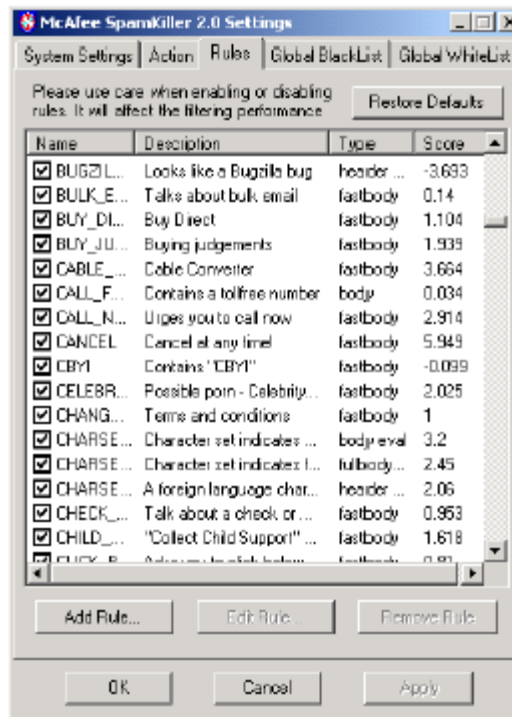
4. ¿Cómo funcionan los productos SpamKiller?

El engine SpamAssassin, de Network Associates, considera acumulativamente cada mensaje de correo electrónico sometido al scan, utilizando todas las técnicas comunes de detección de spam (llegan a más de 650 reglas) y atribuyendo una puntuación ponderada a cada regla.

Eso permite que el engine emita una opinión general sobre el mensaje con respecto a su validez.

Normalmente, es necesaria la coincidencia con tres o más reglas para que el mensaje sea clasificado como spam. Eso es mucho más preciso que los abordajes tradicionales, que tratan el mensaje como spam si se encuentra una coincidencia con cualquiera de las reglas.

El engine SpamAssassin posee una puntuación predefinida para cada regla. Por defecto, si un mensaje recibe una puntuación general superior a cinco, el engine SpamAssassin lo clasificará como spam.



Usted percibirá que algunas de las reglas llevan una puntuación negativa. Dichas reglas se concentran en la exclusión de falsos positivos (es decir, mensajes que parecen spam, pero que no lo son).

4.1 ¿Cómo recibe cada regla su puntuación predefinida?

Network Associates mantiene una base de datos con más de 300.000 mensajes, y cada uno fue manualmente clasificado por una persona como: spam, legítimo o en la zona intermedia entre los dos extremos del espectro.

El equipo de desarrollo de Network Associates utiliza un algoritmo genético, que es una forma reconocida de Inteligencia Artificial (IA).

Si busca en la Web, encontrará algunas explicaciones profundamente científicas sobre qué son algoritmos genéticos. Sin embargo, en términos muy sencillos, podemos decir que es un modelo de enseñanza por computadora basado en el comportamiento evolutivo humano.

Por ejemplo, a cada generación/iteración, él aprende y se adapta basado en las experiencias de la generación/iteración anterior.

En términos del SpamAssassin, dicha técnica es utilizada para optimizar la ponderación de puntuaciones de cada regla. Empezando por una puntuación atribuida por una persona a cada regla creada, las reglas del engine SpamAssassin son probadas en contraste con los 300.000 mensajes conocidos.

Entonces, la tecnología de IA verifica la eficiencia del filtrado de spam según la puntuación por las reglas actuales, con respecto a las cuáles se deben obtener los resultados (no podemos olvidarnos de que todos los mensajes de prueba han sido clasificados manualmente).

Enseguida, el engine ajusta las puntuaciones en una plantilla para aumentar la tasa de detección y reducir los falsos. En efecto, cada vez que se cambian las puntuaciones de las reglas y se re-ejecutan las pruebas, se puede pensar en un ciclo de generación.

El algoritmo genético puede atravesar millones de generaciones hasta alcanzar las combinaciones ideales de puntuación para el conjunto de reglas definido con respecto a los resultados conocidos.

4.2 Reglas del SpamAssassin

El engine SpamAssassin utilizado en los productos McAfee SpamKiller posee más de 650 reglas predefinidas utilizadas para verificar si los mensajes de correo electrónico recibidos han sido solicitados o no.

En la interfaz del SpamKiller, el administrador puede activar/desactivar cualquier regla existente según las necesidades específicas de su empresa, donde varían del standard. Por ejemplo, una empresa farmacéutica puede querer permitir que los usuarios reciban mensajes que contengan palabras tales como "Viagra", mientras que una institución financiera como un banco puede no permitirlo. SpamKiller le brinda la flexibilidad de personalizar su tecnología a su entorno. Más información sobre personalización será discutida más adelante en esta guía.

Véanse a continuación los principales tipos de reglas usadas por el engine SpamAssassin para detectar spam en los productos SpamKiller y ejemplos de cómo funcionan dichas reglas.

Reglas de Encabezamiento

El encabezamiento del mensaje contiene la siguiente información:

- Para
- De
- Asunto
- Fecha de Envío
- Encabezamiento recibido (a cada etapa por la cual el mensaje es retransmitido, se añade al encabezamiento información sobre la retransmisión)
- Encabezamiento de aplicación (por ejemplo, encabezamientos de clientes de correo electrónico Exchange o AOL)
- X-Header

Estos son algunos ejemplos de reglas utilizadas para verificar el encabezamiento del mensaje e identificar si es legítimo o es spam:

- **Reglas de Contenido** – Verifica la línea de asunto en búsqueda de giros normalmente utilizados en spams, tales como "\$\$\$" o "FOR FREE".
- **Autenticidad del Mensaje** – Un mensaje puede afirmar que es proveniente de una cuenta de AOL, pero cuando se verifica el encabezamiento de aplicación, le falta el encabezamiento del cliente de correo electrónico de AOL.
- **Validación de Fecha** – Un truco común utilizado por las fuentes de spam es modificar la fecha de envío para una fecha futura. Esto sirve para asegurar que el mensaje permanezca en la parte superior de su buzón, pues, normalmente, muchos clientes de correo electrónico clasifican los mensajes según la fecha de recibimiento en orden decreciente.
- **Información de Enrutamiento** – El host de correo electrónico puede ser capaz de modificar la dirección electrónica del remitente, pero el encabezamiento del mensaje recibido es creado a medida que el mensaje es enrutado a través de retransmisiones hasta llegar a su destino. Debido a que dichos datos son escritos tras el envío del mensaje, no pueden disfrazar el historial. Por lo tanto, esta es una buena fuente para saber si el mensaje es proveniente de una fuente conocida en las RBL (listas negras de tiempo real).

Reglas de Cuerpo de mensaje

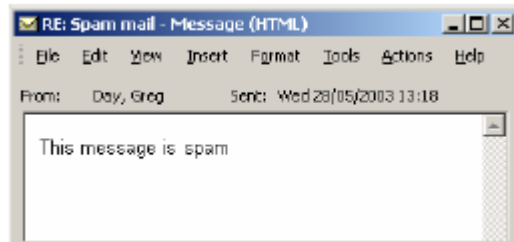
La forma más sencilla de describir el cuerpo de un mensaje de correo electrónico es la siguiente: "lo que el usuario observa al abrir el mensaje en el cliente de correo electrónico". Eso, normalmente, es la línea de asunto y el cuerpo del texto.

Una técnica común usada por las fuentes de spam es añadir otros códigos al mensaje para disfrazar el contenido del mensaje crudo.

Por ejemplo, en mensajes escritos en HTML, pueden añadir otros códigos HTML que no alteran el texto real exhibido al usuario, pero, en el nivel del código, añaden un "ruido" para confundir un mecanismo de scan de spam. El mensaje exhibido a continuación contiene, en verdad, el siguiente código HTML:

```
<FONT face=Arial size=2>This message is s<U></U>pa<STRONG></STRONG>m</FONT>
```

El mensaje contiene códigos HTML para definir el tipo de caracteres, activando y desactivando el subrayado "<U>" y el texto en negrita "". Ni las opciones de texto subrayado o negrita son exhibidas al usuario, pues se las activan y desactivan al mismo tiempo, anulando el efecto.



Si usted estuviera utilizando reglas de contenido para buscar en el mensaje HTML crudo la palabra "spam", los códigos HTML camuflarían dicha palabra. El engine SpamAssassin posee la tecnología para interpretar el mensaje, muy semejante a lo que haría el cliente de correo electrónico del destinatario, con lo cual es capaz de efectuar el scan del cuerpo del mensaje de la forma como sería exhibido al usuario.

Al efectuar el scan aplicando reglas al cuerpo del mensaje, el engine SpamAssassin utiliza una tecnología propia para optimizar la velocidad del scan. Esencialmente, eso permite que termine el scan rápido de las reglas de cuerpo de mensaje de alto nivel, y enseguida, rehace el scan de forma profundizada, utilizando las reglas que han sido accionadas de alto nivel anteriormente.

Entre las reglas de cuerpo de mensaje están las siguientes:

- Verificación de frases tales como "Make money fast" (*Gane dinero rápido*).
- Verificación del porcentaje de palabras obscenas en el mensaje de correo electrónico.
- Detección de los varios ejemplos de mensajes de spam nigerianos.

Verificando el patrón del mensaje en vez de palabras-claves específicas, los productos SpamKiller pueden detectar nuevas variaciones de spam basado en temas existentes.

Reglas de cuerpo de mensaje en formato crudo

Las reglas de cuerpo de mensaje en formato crudo son lo opuesto de las reglas de cuerpo de mensaje, examinando el mensaje en su formato crudo, otra vez en búsqueda de técnicas usadas por fuentes de spam para camuflar (ocultar) el spam a través de la inclusión de ruido para impedir que las reglas de contenido logren ubicar palabras-claves o frases.

Las reglas de cuerpo de mensaje en formato crudo buscan camuflajes, señalando que el mensaje no es muy legítimo porque intenta esconder el mensaje verdadero dentro de los datos adicionales incluidos.

Se puede lograr ocultar a través de varias técnicas, tales como:

- **HMTL** – Inclusión de código HTML y de palabras, tales como el ejemplo mostrado más arriba para la Regla de Cuerpo de mensaje.
- **Codificación del Texto** – Como, por ejemplo, la codificación Base64, usada para convertir adjuntos en un formato que pueda ser enviado por correo electrónico SMTP. Los textos no necesitan codificación para el envío. Sin embargo, al codificar el texto, la fuente de spam lo convierte en un formato que parezca distinto, siendo por lo tanto, ignorado por las reglas de contenido crudo. En otros términos, el spam es cifrado. Cuando el usuario abre el mensaje, el cliente de correo electrónico decodifica automáticamente el texto para que se pueda leer el mensaje de spam.

En términos del engine SpamAssassin, podemos decodificar patrones comunes, tales como el

Base64. Así, las reglas de cuerpo de mensaje pueden detectar el verdadero contenido del spam. Sin embargo, las reglas de cuerpo de mensaje en formato crudo también destacan el mensaje como un spam potencial, debido a que él intenta ocultar su contenido. La combinación de ambas genera una indicación más positiva de que el mensaje es un spam, a diferencia del uso de una u otra técnica aisladamente.

- **Texto Blanco** – En mensajes compuestos en HTML, los creadores de spam pueden incluir intencionalmente un texto legítimo utilizando el mismo texto como color de fondo, para que el usuario no vea el texto. El objetivo es burlar reglas Bayesianas y de contenido, haciendo que el mensaje parezca más legítimo que sospechoso. Otra vez, debido a que éste no es un comportamiento común, el engine SpamAssassin maneja la táctica como semejante a spam, ayudando a clasificar el mensaje como no-solicitado.

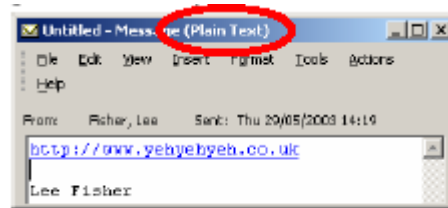
Reglas de Cuerpo de mensaje integral

Estas reglas consideran todo el mensaje no-codificado como una unidad única. Este método funciona de manera muy semejante a los productos antivirus tradicionales, buscando propiedades conocidas de spam. Normalmente, eso puede utilizar técnicas de *hashing* (como, por ejemplo, las creadas por DCC o Pysor) para crear una base de datos de mensajes identificados como spam a través de las sumas de verificación de *hash* del mensaje.

Reglas URI

Las reglas URI son reglas especiales de cuerpo de mensaje creadas para examinar el cuerpo del mensaje en búsqueda de cualquier Identificador Universal de Recursos (URI) incorporado, como por ejemplo, hipervínculo o Localizadores Universales de Recursos (URL). Al examinar los URI, el engine SpamAssassin busca:

- Explotaciones que se puedan utilizar por la fuente del spam, como por ejemplo, apertura de una página Web o concesión de derechos donde no se deben conceder.
- Palabras-claves o giros en los URI incorporados que puedan indicar que el mensaje es un spam. Ejemplos de esto son la verificación de cualquier URI en búsqueda de palabras-claves tales como "sex" o "teen", que puedan ser enlaces a imágenes o sitios Web.
- URL que contengan direcciones IP, no el nombre del *host*, una técnica común para enmascarar el nombre del sitio anunciado en el mensaje.
- Mensajes de texto simple no soportan las URI. Sin embargo, algunos clientes de correo electrónico (como el Outlook) pueden interpretar el texto del mensaje como un URI debido a su formato. Por ejemplo, al recibir un mensaje de texto simple con el texto "http://www.nai.com", muchos clientes de correo electrónico lo manejan dinámicamente como un hipervínculo que pulsado, abre el navegador en la URL, aunque el mensaje de texto simple no fuera originalmente un hipervínculo. Véase el ejemplo al lado.



Muchos de los ejemplos mencionados arriba pueden estar presentes en mensajes legítimos. Es por esta razón que la tecnología SpamAssassin considera el mensaje acumuladamente, sin depender de una regla aislada para identificar el mensaje como spam.

Meta-Reglas

A menudo, cuando la combinación de dos o más reglas es accionada, la oportunidad real de que el mensaje sea un spam es mayor que el peso sumado de la puntuación de cada una de dichas reglas.

Meta-reglas permiten la atribución de puntos en combinaciones booleanas de reglas (por ejemplo, si las reglas son la 12 y la 17, entonces el mensaje definitivamente se asemeja a un spam. Entonces,

sume más puntos a la puntuación general del mensaje). Las meta-reglas pueden buscar combinaciones que contengan reglas de puntuación positivas así como negativas, de spam.

4.3 ¿Qué ocurre cuando un mensaje es clasificado como Spam?

Por Defecto, cuando un mensaje recibe una puntuación igual o superior a cinco, el SpamKiller supone que es un mensaje no-solicitado.

Todos los productos SpamKiller (servidor de correo y gateway) tienen las mismas opciones de filtrado, pero son implementados de forma un poco diferente, según el entorno donde el producto es instalado.

Opciones comunes de filtrado para correo electrónico y gateway

- **Inclusión de un prefijo en el Asunto** – La capacidad de añadir texto (“SPAM”, por defecto) en la línea de asunto. Eso puede ser especialmente útil cuando usted quiere usar el servidor o el cliente de correo electrónico para gestionar mensajes con sospecha de spam.
 1. La inserción de un prefijo común en la línea de asunto del mensaje permite que los administradores y/o usuarios finales creen reglas de correo para filtrar el mensaje sospechoso y enviarlo a una carpeta o a una base de datos definidas, centrales o locales del usuario. Esto garantiza que el mensaje sospechoso no obstruya el buzón de los usuarios, permitiendo que se verifique si es o no es un caso de spam.
 2. Las reglas de manejo de mensajes de correo electrónico incorporadas a la mayoría de los servidores o clientes de correo pueden ser usadas para gestionar la exclusión de mensajes sospechosos y cuando el usuario tenga tiempo pueda acceder al mensaje, si fuese necesario. Una práctica común de gestión de spam es mantener el mensaje por algunos días (lejos del buzón de los usuarios) y enseguida excluirlo. Por ejemplo, una regla de correo que verifique la edad del mensaje y la marca de la línea de asunto, excluyendo así, el spam cuando permanezca almacenado por un intervalo definido.
- **Añadir puntos de spam al mensaje** – En el producto SpamKiller for Exchange SMB, esta opción es denominada “Spam Level header”. Esto identifica la puntuación de spam recibida por el mensaje. Como se demostró arriba, usted puede utilizar reglas de servidor o cliente de correo para filtrar mensajes de spam y enviarlos a distintas carpetas o bases de datos, dependiendo de la puntuación recibida.
- **Añadir al X-header del mensaje una lista de reglas de spam accionadas** – En el producto SpamKiller for Exchange SMB, esta opción es denominada “Spam Report”, que brinda una lista de las reglas que identificaron al mensaje como spam. Esto es crucial cuando usted quiere optimizar la detección en su entorno, pues le permite que vea las reglas utilizadas cuando sean accionadas en cada mensaje.

Opciones exclusivas del SpamKiller for WebShield Appliances

La solución de gateway (un módulo externo de los dispositivos WebShield) mostrada al lado ofrece el filtrado de spams enviados y recibidos, según un abordaje de dos fases.

(1) Marcar el mensaje como spam – según lo descrito en la sección común arriba.

(2) Bloquear/Encaminar el mensaje – debido a que el scan de spam está en el gateway, usted puede ahorrar el ancho de banda de la red al impedir que el spam entre en su red.

El control fue simplificado para ser basado en una clasificación alta, media o baja, mostrada en la tabla dada a continuación, correlacionada a la puntuación del engine SpamAssassin.

Clasificación	Puntuación
BAJA	5 – 9,99
MEDIA	10 – 14,999
ALTA	15 o más

Si no se define nada en contrario, los intervalos de puntuación no pueden ser alterados a través de la GUI. Sin embargo, cuando sea necesario, los administradores con conocimiento avanzado pueden alterar la puntuación a través de la modificación de los valores en el archivo XML de configuración de sistema del WebShield.

Enrutando spam con el SpamKiller for WebShield Appliances

Consideramos que el enrutamiento hecho por SpamKiller for WebShield Appliances puede ser configurado de la siguiente forma:

(1) Si el mensaje está cerca de la frontera entre “no-solicitado” y “legítimo”, (por ejemplo, baja clasificación de spam), es probable que usted opte por enrutarlo al usuario para permitir que se haga la verificación final.

Marcar el mensaje como spam permite que el usuario lo ignore inicialmente y se dedique a sus mensajes legítimos. ¡Ojo! Las reglas del cliente pueden ser usadas para transferir mensajes marcados como spam para otras carpetas/bases de datos locales de correo.

Según la necesidad, el usuario puede verificar cualquier mensaje sospecho si busca un mensaje que cree haber recibido (es decir, quiere estar seguro de que el filtrado de spam no lo capturó equivocadamente).

Cuando tiene tiempo, el usuario puede verificar todos los mensajes marcados como sospechosos.

(2) Si el mensaje es definitivamente un spam (por ejemplo, clasificación media o alta), rechace el mensaje o enrútelo a un local definido.

Opciones exclusivas del SpamKiller for Exchange Small Business

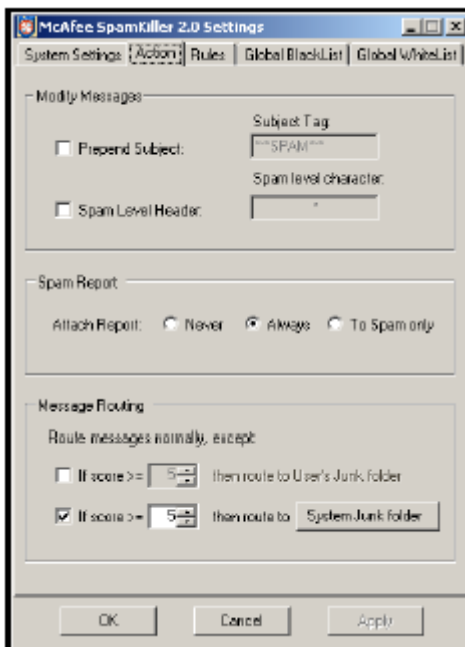
Así como en la solución para gateway, existen dos niveles de filtrado posibles.

Sin embargo, debido a que el producto SpamKiller opera directamente en el sistema de correo, tiene el permiso de redirigir los mensajes a carpetas o bases de datos en el entorno del servidor de correo.

Eso significa que usted puede enrutar los mensajes a una carpeta/ base de datos central o a una carpeta específica de correo Basura creada por SpamKiller en el buzón de cada usuario; en la primera oportunidad que un mensaje es filtrado como spam, se lo enruta a los usuarios y es transferido a la carpeta específica de Basura Electrónica.

El producto SpamKiller Small Business Edition for Exchange 2000 mostrado al lado tiene la opción de efectuar el scan de los spams recibidos y enrutarlos a los buzones de los usuarios o a un grupo específico del Active Directory, creado durante la instalación del producto.

El enrutamiento está basado directamente en la puntuación atribuida por el engine SpamAssassin, que puede ser personalizado (según fue mostrado arriba) a través de la interfaz de configuración de la guía "Action".



Enrutando spam a través del SpamKiller for Microsoft Exchange Small Business

Consideramos que el enrutamiento de su SpamKiller for Exchange 2000 Small Business debe ser configurado de la siguiente forma:

- (1) Si un mensaje recibe una puntuación igual o superior a cinco, entonces está cerca de la frontera entre "legítimo" y "no-solicitado". Por lo tanto, el mensaje debe ser enrutado a la carpeta de Basura Electrónica del usuario. Eso garantiza que no obstruirá el buzón, permitiendo, cuando sea necesario, que se acceda a la carpeta de correo Basura en su tiempo libre para verificar si los mensajes que allí están son realmente spam.
- (2) Si el mensaje recibe una puntuación igual o superior a 15, definitivamente es un spam. Si no hay nada definido en contrario, se enrutará a una carpeta central del sistema. Eso permite que el administrador almacene el mensaje durante algunos días si los usuarios quisiera validarlos.

4.4 Edición de Reglas y Puntuaciones

En todos los productos SpamKiller, las reglas han sido previamente configuradas para proporcionar una detección de spam ideal para los usuarios en general. Sin embargo, usted puede personalizar el conjunto de reglas según sus necesidades personales.

Existen varias razones por las cuales usted puede querer personalizar las reglas:

- (1) Incluir detección de mensajes específicos que usted cree que deben ser manejados como spam y que no están en el conjunto principal de reglas. Ellos son conocidos como "falsos negativos".
- (2) Permitir que pasen mensajes que habitualmente son tratados como spam. Por ejemplo, si usted trabaja en una empresa del ramo farmacéutico, puede tener un motivo legítimo para enviar y recibir mensajes que contengan la palabra "Viagra". Nos referimos a este caso como "falsos positivos".

Cuando se configure el conjunto de reglas del SpamAssassin en cualquiera de los productos SpamKiller, el aspecto más importante que se debe tener en cuenta es que las reglas ya han recibido una puntuación basada en el algoritmo genético. Alterar la puntuación o desactivar cualquiera de las reglas tendrá un "efecto dominó" sobre todas las otras.

Si usted quiere modificar la detección de spam del SpamKiller, el primer método debe ser el uso de las opciones de listas negras y listas blancas, que permiten el bloqueo o la liberación implícitos de mensajes sin cambiar el conjunto de reglas. La solución SpamKiller que usted utiliza definirá cuáles tipos de artículos podrán ser incluidos en la lista.

Por ejemplo, la solución SpamKiller for Exchange 2000 SMB permite agregar entradas en las listas blancas y negras según la dirección SMTP del remitente, incluso soporta comodines para que usted pueda bloquear dominios de correo completamente.

Debido a que la solución es instalada en el entorno Exchange, también permite que las listas blancas y negras sean relacionadas a las cuentas de correo electrónico de cada usuario. Por defecto cuando esta opción es utilizada, la lista de contacto para del usuario es agregada a la lista blanca.

Al usar el SpamKiller for WebShield Appliances en el gateway, las listas blancas y negras se pueden usar más ampliamente, ya que el dispositivo examina el tráfico de SMTP y no sólo el objeto del mensaje (como en el caso de la solución Exchange SMB).

En este caso, las listas negra y blanca pueden recibir direcciones electrónicas, dominios o direcciones/intervalos de red.

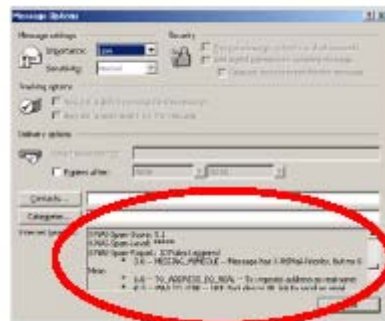
Si necesita más personalización aún, usted percibirá que todos los productos SpamKiller permiten la activación o desactivación de las reglas existentes, pero no permiten que sus puntuaciones sean alteradas.

Eso es debido a las implicaciones de que una regla tiene un "efecto dominó" sobre las otras, pues el algoritmo genético ha optimizado la puntuación de cada regla para el trabajo conjunto de las reglas.

Cuando usted realmente tiene necesidad de alterar las reglas, le sugerimos lo siguiente:

1. Utilice la opción del SpamKiller de exhibir la puntuación y la lista de reglas activadas en todos los mensajes de correo electrónico. Eso permitirá que usted vea cuáles reglas fueron activadas por el mensaje y la puntuación atribuida al mensaje.

El ejemplo al lado muestra el X-header del mensaje con la puntuación y las reglas accionadas en el scan realizado por el SpamKiller 2.7 for WebShield Appliances.



2. Encuentre la regla que usted cree que está causando la detección incorrecta del spam. Por ejemplo, los mensajes de su abuela con la famosa receta de pastel de pollo están siendo detectadas como spam porque la lista de ingredientes incluye "pechuga de pollo", que está activando el filtro de contenido para la palabra "pechuga". Desactive la regla.

Nota: cuando usted actualiza la lista de reglas de spam, todas las reglas desactivadas quedarán desactivadas.

Una personalización más detallada de las reglas es posible con la tecnología SpamAssassin, que incluye la creación de nuevas reglas y permite alterar la puntuación de las nuevas reglas.

Debido a una comprensión **en profundidad** del conjunto de reglas **requeridas** para lograr esto sin **desajustar** las reglas existentes, la mayoría de los productos SpamKiller no **ofrece esta funcionalidad a través de la** interfaz de usuario.

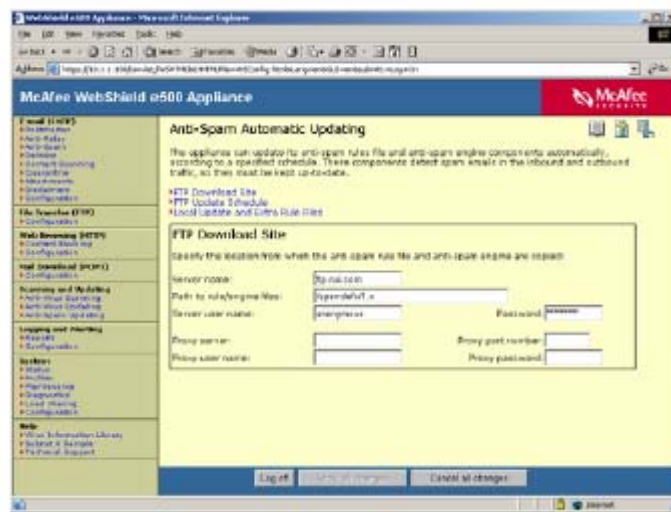
Las reglas están escritas en lenguaje Perl y deben ser editadas manualmente sólo por expertos experimentados. Si usted tiene la necesidad de crear o editar reglas con dicho nivel de detalle, el equipo de consultoría Network Associates Expert Services puede brindarle el conocimiento necesario.

4.5 Actualización del SpamKiller

Todas las soluciones SpamKiller permiten la actualización de los conjuntos de reglas y del engine de scan de spam desde nuestro sitio FTP de actualización.

Esto es necesario para mantener la eficiencia de la detección de spam.

Según nuestra experiencia, hoy día usted necesita efectuar las actualizaciones sólo en intervalos de algunos meses. Sin embargo, eso puede cambiar según los cambios en las técnicas de los autores de spams.



La tecnología de actualización que acompaña a los productos SpamKiller posee un programador que, si no se define lo contrario, verifica nuevas actualizaciones todos los días. Eso le permite tener siempre lista la protección más reciente.

Cuando es ejecutado, el actualizador descarga en su equipo el archivo SPAMUPD.INI para verificar cuáles versiones de las reglas de spam y del scan engine están disponibles en el sitio FTP. Si es necesario, el actualizador descargará y aplicará las nuevas reglas y el nuevo scan engine. Las actualizaciones recientes de reglas y del engine poseen menos de 300 Kb.

Para garantizar que todas las reglas personalizadas que usted creó, no sean sobrescritas durante una actualización, los productos SpamKiller permiten el uso de archivos de reglas extras, separados para almacenar sus reglas personalizadas.