



## MASBYTES: DESARROLLO DE UNA SOLUCIÓN ANTYSBAM

Nombre de la empresa: MASBYTES

Sector: Telecomunicaciones, Hosting, Housing, ISP

Ubicación: Calle Pablo Sarasate 9, 31500, Tudela

Nº de empleados: 8

Fecha de creación:

Persona de contacto: Álvaro Alonso

Ante la problemática actual surgida en relación a los Virus y Spam que se introducen a diario a través de los correos electrónicos MASBYTES ha desarrollado una solución tecnológica que permita el filtrado de correo.

La **problemática y objetivos** perseguidos eran:

- 1.- Identificación de mensajes de correo con Virus en su contenido, y de aquellos que el texto del mismo pudiese ser identificado como SPAM.
- 2.- Limitación de acceso SMTP a las IP con un masivo envío de mensajes con las características anteriores para salvaguarda de recursos, tanto en máquinas (CPU en procesos de identificación) como ancho de banda en la recepción de los mensajes.
- 3.- Limitación de envíos de mensajes con diccionario.

Para la consecución de esos objetivos se planteo la siguiente **solución**:

El software antivirus, debido a las limitaciones de actualizaciones de las firmas de Antivirus, hizo que se tuviera que realizar el escaneo de los mensajes con 2 programas diferentes de Antivirus, permitiendo una mejora en los tiempos de respuestas ante nuevos virus. El desarrollo permite la adición de nuevos antivirus, pero debido a la carga de CPU, se ha acabado limitando a 2 programas, que cubren el 100% de los virus identificados. No se ha considerado necesario identificación heurística.

El software antiSpam, marca con una identificación aquellos mensajes que puedan ser considerados SPAM, para que luego el usuario pueda, mediante reglas, filtrar a una carpeta en su programa de correo.

En una segunda fase, en la cual no se envían aquellos mensajes que el umbral de detección considera exclusivamente SPAM, pero ante el riesgo de ser mensajes validos, al final del día se envía un mensaje informativo con un texto informando del remitente, asunto y tamaño del mensaje, así como un Link para que puedan recuperar ellos mismo aquellos mensajes que puedan considerar interesantes.

Todos los sistemas anteriores, suponen que el mensaje ha sido recibido, con lo que el tráfico de bytes se ha tenido que asumir como un aumento del ancho de banda.

Casi todos los software de correo, inicialmente reciben todo el mensaje, y luego intentan la entrega del mismo de forma local. Se ha modificado el software SMTP, para que identifique la existencia del buzón de correo, antes de que aceptase el cuerpo del mensaje, evitando los ataques de diccionario y recepción de tráfico inútil. Adicción del filtro GreyList, para reducir intentos de envíos indiscriminados a cuentas reales.



En una tercera fase del proyecto, se busca la identificación de las IP de quien envía el mensaje con Virus o SPAM, bloqueando el acceso a los SMTP, durante un periodo de tiempo, evitando el consumo de tráfico y reduciendo carga en los servidores al procesar los mensajes, la penalización se basa en información estadística recogida en la cual se ha detectado que los envíos de mensajes problemáticos, son reincidentes en un muy breve plazo de tiempo desde una misma IP.

Finalmente en una cuarta fase, se va a generar administradores para facilitar a los clientes la parametrización del software AntiSpan.

Como consecuencia del desarrollo del proyecto, se alcanzaron los siguientes **resultados**:

1.- *VIRUS*: Reducción casi completa del envío/recepción de mensajes con Virus, mejora en la velocidad de descarga de correo por parte de los usuarios, no tienen "basura" que descargar y luego procesar con su aplicación antivirus, aunque se les recomienda que lo mantengan.

2.- *SPAM*: El Greylist ha resultado de una eficacia sorprendente en cuanto a coste/resultados. La detección y marcado ha permitido a los usuarios reducir el tiempo empleado en procesar sus mensajes, y el mensaje de informe a final de día de mensajes retenidos evita el problema de "falsos positivos".

3.- *ANCHO DE BANDA*: Nuestras necesidades de ancho de banda se han contenido, tanto para envío/recepción, aunque el tráfico aumenta. La estadística demuestra que se ha reducido el número de mensajes enviados/recibidos, y si que aumenta el total de Mbytes de los mensajes, debido en gran parte también al aumento de la banda ancha de los clientes.

4.- *MAQUINAS*: Se ha logrado estabilizar el consumo de CPU en los servidores de correo, ya que en el momento que se llega a detectar un aumento excesivo de envío de mensajes problemáticos, se disparan los umbrales de detección y se termina bloqueando el acceso a las IP consideradas ofensivas del servicio SMTP, limitándose el impacto en los procesos.

5.- *INFORMES*: Informes en tiempo real, tanto para uso interno de análisis e identificación, como externos a los clientes para información del servicio y situación de estado de la red.

Como **innovaciones** en la solución planteada por Masbytes destacan las siguientes:

- 1.- Retención de los mensajes de SPAM, con notificación al usuario al final del día para que se pueda recuperarlos.
- 2.- Administración por parte del usuario de los parámetros de funcionamiento del software AntiSpam.



La valoración de este producto por parte de las empresas **clientes** en general es positiva. Ha habido casos de rechazo de la solución antiSpam, pero cuando se ha desactivado el servicio, en un plazo breve de tiempo han vuelto a solicitarlo debido a la problemática que les planteaba la cantidad de mensajes que recibían, que tenían que procesar bien con otras soluciones o bien realizando una revisión manual de los mismos.