

El Día a Día del Administrador de Sistemas

NUEVO ORDEN

SA-Update ayuda a los administradores en apuros a enfrentarse a los ataques de los spammers. **POR CHARLY KÜHNAST**

Los spammers tienen que ser creativos con la estructura y el contenido de sus correos basura si desean garantizar el disgusto de cualquier usuario de PCs del mundo. Como a mi me gusta combatir a los spammers en igualdad de condiciones, las reglas de mi filtro SpamAssassin requieren actualizaciones regulares. Afortunadamente, dispongo de múltiples canales para obtener munición.

SA-Update

La herramienta que obtiene actualizaciones y luego las copia en los puntos adecuados recibe el nombre de SA-Update [1].

Una clave GPG impide diversas técnicas de manipulación tales como DNS spoofing. Para rejuvenecer el canal por defecto, *updates.spamassassin.org*, necesito primero la clave pública correspondiente:

```
wget http://spamassassin.apache.org/updates/GPG.KEY
gpg --import GPG.KEY
sa-update --import GPG.KEY
```

Ficheros Creados

A continuación creo dos ficheros en la carpeta SpamAssassin. Uno de ellos, *channels.text*, lista los canales de

actualización. El segundo, *keys.text*, contiene los IDs de las claves GPG que necesito para acceder de forma segura. Una llamada a

```
sa-update -D --channelfile
/etc/spamassassin/
channels.text --pgpkeyfile
/etc/spamassassin/
keys.text
```

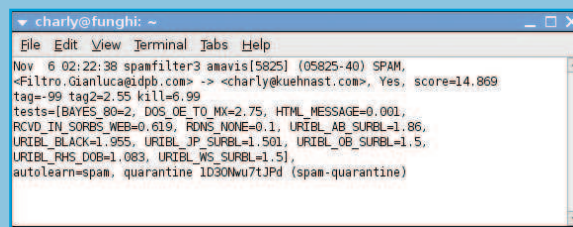


Figura 1: Una rápida inspección del registro del correo revela lo que no le gusta a SpamAssassin acerca de un determinado mensaje y qué conjunto de reglas ha utilizado.

inicia la actualización. El parámetro *-D* le indica a SA-Update que muestre la información de depuración. Sin este parámetro *-* SA-Update es tan taciturno como el personaje de la armónica de Charles Bronson [2] *-* no existe un modo detallado intermedio.

¡Filtros, Por Favor!

El valor de retorno ofrece un procedimiento sencillo para comprobar una actualización satisfactoria. Un valor de retorno de *0* significa que SA-Update ha añadido nuevas reglas de filtrado. Un valor de *1*, que el conjunto de reglas está actualizado hasta la fecha. Un valor de *4* o superior indica un error, y eso significa que hay que comprobar la salida de depuración más detenidamente.

Para mejorar la tasa de detección de spam me gusta añadir canales como OpenProtect [3] o Daryl O'Shea [4]. Un resumen útil de las reglas del SARE (SpamAssassin Rules Emporium) se encuentra en línea en [5], y el conjunto de reglas por defecto se explica en detalle en [6]. Las formas abreviadas de las reglas de filtrado aparecen en los registros del correo; de este modo, se puede decir de un vistazo lo que a SpamAssassin no le gusta acerca de un mensaje y qué conjunto de reglas ha utilizado la herramienta (Figura 1).

La pregunta más importante es ¿vale la pena? ¡Por supuesto! La tasa de detección de mi filtro de spam se beneficia considerablemente extendiendo el conjunto de reglas. De todos modos, me gusta echarle un ojo a los ficheros de registros: El peligro de falsos positivos crece con cada nueva regla de filtrado que se añade.

RECURSOS

- [1] SA-Update: <http://wiki.apache.org/spamassassin/RuleUpdates>
- [2] "Hasta que llegó su hora" ("C'era una Volta il West"), 1968: <http://www.imdb.com/title/tt0064116/>
- [3] OpenProtect: <http://saupdates.openprotect.com>
- [4] Daryl O'Shea: <http://daryl.dostech.ca/sa-update/sare/sare-sa-update-howto.txt>
- [5] SARE: <http://www.rulesemporium.com/rules.htm>
- [6] Conjunto de reglas por defecto: http://spamassassin.apache.org/tests_3_2_x.html

SYSADMIN

Los Fantasmas de NFS366
La autenticación basada en hosts es sencilla de configurar, pero no es muy eficaz contra visitantes indeseados.