Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Asesinando spams (28531 lectures)

Per **Ricardo Galli Granada**, ***gallir*** (http://mnm.uib.es/gallir/)

Creado el 24/06/2002 15:40 modificado el 24/06/2002 15:40

> *Estaba cansado de recibir tantos spams cada día, desde que instalé el **spamassassin**[1] es casi como si no existiesen. Llevo varios meses probándolo, sólo me ha dado un par de "falsos positivos" (aunque ninguno con la última versión de Debian Sid) y muy pocos "falsos negativos". Os recomiendo, sobre todo para MX de empresas, si vuestros colegas están de acuerdo (temas legales de por medio...).*

El spamassassin[1] es un filtro basado en scripts en Perl que procesan los mensajes y detectan, en base a una reglas bastantes complejas, si el mensajes es un spam. El resultado de filtrar los mensajes es un puntaje, que si supera determinado valor (5.0 por defecto) es considerado un spam.

La mejor manera de hacerlo funcionar es arrancar el demonio `spamd` y comunicarse con él a través del spamc. De esta forma nos ahorramos varios ciclos de CPU arrancando el Perl.

La instalación en Debian es muy sencilla:

```
apt-get install spamassassin spamc
```

El paquete spamassassin instala los script de Perl y el demonio spamd. Por otro lado, el spamc provee el cliente (spamc) que se comunica con el spamd. Éste último paquete lo acaban de separar en Debian Sid, así que probeblemente en Woody esté todavía incluido en el paquete original spamassassin.

Una vez instalado ambos y arrancado el spamd, sólo hay que hacer que el spamc filtre todos los mensajes para detectar si es spam. Luego podéis hacer con ellos lo que queráis a través del .procmailrc.

El spamd agrega unas cabeceras para indicar los resultados:

```
X-Spam-Prev-Content-Type: text/html; charset="us-ascii"
X-Spam-Prev-Content-Transfer-Encoding: 7bit
X-Spam-Status: Yes, hits=11.7 required=5.0
tests=NO_REAL_NAME,MSG_ID_ADDED_BY_MTA,INVALID_MSGID,SUBJ_REMOVE,
UPPERCASE_25_50,MAILTO_WITH_SUBJ,MAILTO_TO_REMOVE,
MAILTO_WITH_SUBJ_REMOVE,BIG_FONT,MAILTO_LINK,
FROM_AND_TO_SAME
version=2.30
X-Spam-Flag: YES
X-Spam-Level: ***********
X-Spam-Checker-Version: SpamAssassin 2.30 (devel $Id: SpamAssassin.pm,v 1.94
2002/06/14 23:17:15 hughescr Exp $)
```

También un mensaje de spam en el *Subject*:

```
Subject: *****SPAM***** Say Goodbye to YELLOW, STAINED Teeth!
```

Y las siguientes líneas en el texto para describir las reglas aplicadas

```
SPAM: -------------------- Start SpamAssassin results ----------------------
SPAM: This mail is probably spam. The original message has been altered
SPAM: so you can recognise or block similar unwanted mail in future.
SPAM: See http://spamassassin.org/tag/ for more details.
SPAM:
SPAM: Content analysis details: (25.5 hits, 5 required)
SPAM: NO_REAL_NAME (-1.1 points) From: does not include a real name
SPAM: INVALID_DATE_TZ_ABSURD (4.4 points) Invalid Date: header (timezone does
not exist)
SPAM: FAKED_UNDISC_RECIPS (3.5 points) Faked To "Undisclosed-Recipients"
SPAM: PLING (0.1 points) Subject has an exclamation mark
SPAM: DOUBLE_CAPSWORD (1.1 points) BODY: A word in all caps repeated on the line
SPAM: CLICK_BELOW (1.5 points) BODY: Asks you to click below
SPAM: CALL_FREE (0.7 points) BODY: Contains a tollfree number
SPAM: NORMAL_HTTP_TO_IP (3.3 points) URI: Uses a dotted-decimal IP address in
URL
SPAM: REMOVE_PAGE (2.2 points) URI: URL of page called "remove"
SPAM: MAILTO_WITH_SUBJ (1.9 points) URI: Includes a link to send a mail with a
subject
SPAM: CLICK_HERE_LINK (0.8 points) BODY: Tells you to click on a URL
SPAM: MAILTO_LINK (0.8 points) BODY: Includes a URL link to send an email
SPAM: FREQ_SPAM_PHRASE (2.4 points) Contains phrases frequently found in spam
SPAM: [score: 14, hits: click here, email address,]
SPAM: [enter your, list please, please click, this]
SPAM: [message, you wish, your email, your]
SPAM: [name]
SPAM: DATE_IN_FUTURE_06_12 (2.4 points) Date: is 6 to 12 hours after Received:
date
SPAM: FORGED_YAHOO_RCVD (1.5 points) 'From' yahoo.com does not match 'Received'
headers
SPAM:
SPAM: -------------------- End of SpamAssassin results ---------------------
```

Configuración con el procmail

Con toda la información descrita previamente se pueden aplicar filtros en el procmail del usuario, en el genérico para todo el sistema (CUIDADO: puede ser ilegal modificar o borrar el mensaje de terceros sin su aprobación) o en el propio cliente (MUA) de correo electrónico.

En mi caso yo llamo al spamc desde el **/etc/procmailrc** para hacerlo de forma global:

```
DROPPRIVS=yes

:0fw
| /usr/bin/spamc -f
```

Luego en mi **$HOME/.procmailrc** filtro los spams a una carpeta especial para que no me moleste al recoger correo:

```
:0:
* ^X-Spam-Status: Yes
mail/spams
```

Como véis, envío los spams al fichero $HOME/mail/spams, pero si os fiáis de sus resultados y no os importa perder algún que otro mail "válido" [*] podéis enviarlo a /dev/null.

[*] Los dos únicos "falsos positivos" que tuve fueron de un amigo que envió unos mensajes desde Outlook a una lista con "Undisclosed recipients" en la cabecera. Pero no eché mucho de menos al mensaje, porque era a una lista y desde el Outlook, posiblemente con virus :-)

Lista de enlaces de este artículo:

1. http://spamassassin.org/

E-mail del autor: gallir _ARROBA_ uib.es