



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

Regla (simple) del spamassassin para el gusano Swen (14432 lectures)

Per Ricardo Galli Granada, [gallir](http://mnm.uib.es/gallir/) (<http://mnm.uib.es/gallir/>)

Creado el 26/09/2003 16:21 modificado el 26/09/2003 16:21

A pesar de que pasé más de doscientos mensajes del gusano por el `sa-learn -spam`, esta mañana me encontré con más de cincuenta mensajes que dieron falsos negativos. Así que hice una pequeña regla para marcarlo como spam para liberarme de él de una vez por todas.

Antes de nada, la regla que muestro no funcionaba en la versión 2.55 del spamassassin que estaba en Debian Sarge. Después de perder más de dos horas sin entender el fallo probé de hacer el upgrade a la 2.60 disponible en Sid y funcionó perfectamente a la primera.

La siguiente regla la pondremos en `/etc/spamassassin/local.cf`, aunque también se puede poner en el fichero de configuración de cada usuario, habitualmente `$HOME/.spamassassin/user_prefs`:

```
body SWEN /latest version of
security.{1,10}update.{1,200}explorer.{1,50}outlook/i
describe SWEN 'Swen worm'
score SWEN 7.0
```

Para probarlo es mejor grabar en un fichero uno de los mensajes con el gusano y probarlo con:

```
spamassassin -t <mensaje_guardado
```

Si al final véis algo como lo siguiente es porque funciona correctamente:

```
Content analysis details: (13.5 points, 5.0 required)
```

```
pts rule name description
```

```
-----
```

```
7.0 SWEN BODY: 'Swen worm'
```

```
0.1 HTML_MESSAGE BODY: HTML included in message
```

```
...
```

Ahora sólo falta reiniciar el `spamd` para que lea nuevamente el fichero. Por supuesto, podéis cambiar el `score` de 7 y ajustar a vuestro gusto los puntos asignados.

E-mail del autor: gallir_ARROBA_uib.es

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=1879>