USO DE LISTAS BLANCAS DE REDIRIS EN MILTER-GREYLIST

Autor: Jorge Revuelta Saiz (Vicegerencia de las TIC de la UPV/EHU)

Introducción:

La técnica llamada greylisting consiste en rechazar temporalmente un correo la primera vez que se recibe, notificando un código de error temporal a la estafeta emisora, con el objeto de forzar a que reenvie el correo más tarde. Si el la estafeta emisora cumple el RFC y está correctamente configurada, intentará enviar de nuevo el correo en un plazo razonable de tiempo configurado por el administrador. En este segundo envío, greylist entenderá que el emisor se comporta correctamente y dejará pasar este correo, guardando la tupla de IP origen, from y rcpt en una lista blanca gestionada dinámicamente para que a partir de ese momento, los mensajes enviados desde esa IP origen, from y rcpt no sufran retrasos.

La clave está en que muchos de los spammers no cumplen la RFC y no intentan reenviar un correo rechazado temporalmente, por lo que este tipo de correo llegará a depositarse en los buzones de los usuario.

Por otra parte, milter-greylist permite establecer una serie de Ips en las que confiamos con el objetivo de no hacerlas pasar por el proceso de greylisting. Esto es lo que llamamos incluir una IP en la lista blanca o hacer whitelisting. La idea que quiere transmitir este documento es cómo incorporar el listado de Ips de las listas ESWL y MTAWL que recoge RedIRIS a milter-greylist.

Procedimiento:

La idea es hacer que el fichero de configuración de milter-greylist (greylist.conf) se actualice automáticamente, incorporando regularmente el fichero actualizado de las listas ESWL o MTAWL en función de nuestras preferencias. Esta documentación y los propios ficheros ESWL y MTAWL están pensados para funcionar en versiones 2.X y 3.X de milter-greylist.

Pare ello dividiremos la configuración de greylist en 3 ficheros que posteriormente concatenaremos para generan el greylist.conf definitivo. Estos ficheros podrían ser:

- greylist_base.conf: recogería la configuración básica de greylist, como parámetros de configuración típicos de tiempos y demás. En nuestro caso particular:

```
acl whitelist addr 127.0.0.0/8
acl whitelist addr 158.227.0.0/16
acl whitelist addr 10.0.0.0/8
acl whitelist domain rediris.es
acl whitelist rcpt /postmaster@.*ehu\.es/
delayedreject
greylist 10m
timeout 2d
autowhite 36d
dumpfreq 5m
subnetmatch /24
pidfile "/var/run/milter-greylist.pid"
socket "/var/milter-greylist/milter-greylist.sock"
dumpfile "/var/milter-greylist/greylist.db"
user "smmsp"
```

- lista blanca de RedIRIS: programaremos en el cron la bajada desde RedIRIS de este fichero con wget acorde con la frecuencia con la que queramos actualizar la lista blanca. El listado de Ips podemos bajarlo

desde una de las siguientes URLs en función de cuál queramos utilizar:

http://www.rediris.es/abuses/eswl/data/eswl.greylist
http://www.rediris.es/abuses/eswl/data/mtawl.greylist

- greylist_restos.conf: este fichero recogería el resto de acls que queramos incorporar a nuestra configuración: listas de Ips a las que queramos añadir la lista blanca a nivel particular, acls de greylisting, política por defecto, etc. Hay que tener en cuenta que las acls se leen y ejecutan recorriendo el fichero definitivo de arriba abajo. En nuestro caso particular:

```
acl whitelist addr 12.5.136.141/32    # Southwest Airlines (unique sender)
acl whitelist addr 12.5.136.142/32    # Southwest Airlines
acl whitelist addr 12.5.136.143/32    # Southwest Airlines
.....
acl whitelist addr 207.171.168.0/24   # Amazon.com
acl whitelist addr 207.171.190.0/24   # Amazon.com
acl whitelist addr 211.29.132.0/24    # optusnet.com.au (wierd retry pattern)
acl whitelist addr 213.136.52.31/32   # Mysql.com (unique sender)
acl whitelist addr 216.33.244.0/24    # Ebay
acl whitelist addr 217.158.50.178/32  # AXKit mailing list (unique sender)
#a probar con milter-greylist 3.0
#dnsrbl "SORBS DUN" dnsbl.sorbs.net 127.100.100.100
#acl greylist dnsrbl "SORBS DUN" delay 6h
acl greylist default
```

Sólo queda programar un script en el cron que concatene estos 3 ficheros en el nuevo greylist.conf y que reinicie el proceso milter-greylist. En lineas generales, la idea es la siguiente, a falta de controles de chequeo sobre los ficheros que se manejan y demás comprobaciones:

```
#!/bin/bash
FECHA=`date +%Y%m%d`
WGET="/usr/bin/wget"
GBASE="/etc/mail/greylist_base.conf"
GRESTOS="/etc/mail/greylist_restos.conf"
GBUENO="/etc/mail/greylist.conf"
GBACKUP="/etc/mail/backup/greylist.conf.${FECHA}"
MTAWL="/tmp/mtawl.greylist"
URLWL=" http://www.rediris.es/abuses/eswl/data/mtawl.greylist "

$WGET $URLWL -O $MTAWL
cp $GBUENO $GBACKUP
cat $GBASE $MTAWL $GRESTOS > $GBUENO
/etc/init.d/greymilter restart
rm $MTAWL
```

Un detalle a tener en cuenta es la frecuencia con la que programemos este proceso en el cron, ya que milter-greylist vuelca en los logs del sistema toda la base de datos cada vez que se reinicia. Si la base de datos de milter-greylist es muy grande, los logs crecen considerablemente y puede convertirse en un problema, por lo que antes de programar todo esto para que se haga, por ejemplo, varias veces al día, hay que considerar este posible efecto.