Filter messages in Qmail with unwanted words, get rid of the Viagra annoying spam with Qtrap

Author : admin

Recently the annoying **Viagra** spam has emerged again. Therefore I decided to clean up some of the mails received to one of the qmail servers to protect users emailbox from this viagra peril.

To do so I've remember about an old script which used to be part of *qmailrocks.org* qmail install, the script is called qtrap and is able to filter emails based on list of specific mail contained words.
Since *qmailrocks.org* is gone (down) for some time and its still available only on few mirrored locations which by the way are not too easy to find I decided to write a little post on how **qtrap.sh** could be integrated quick & easy with any **Qmail + Vpopmail** install out there.

Hereby I include the description for **qtrap.sh** given by the script author:

"qtrap.sh script is applied on a per domain basis and serves as a "bad word" scanner to catch any spam that Spamassassin may have missed. This filter serves as the last defense against SPAM before it arrived in your inbox. I like this filter because it helps to get rid of any SPAM that happens to make it by Spamassassin. Without any protection at all, my mailbox gets a shit ton of SPAM every day. Within the first 3 months I enacted the Qtrap filter, Qtrap logged over 9,000 deleted SPAM messages, none of which were legitimate e-mails. My keyboard's delete key was very appreciated the extra rest.

Any emails that are scanned and contain a banned word will be automatically deleted and logged by the qtrap script. A whitelist feature now exists so that individual addresses or domains can be exempt from the qtrap scan."

Now as one might have general idea on what the script does. Here is the step by step qtrap.sh integration;

1. Create necessery qtrap directory and logs and set proper permissions

If the vpopmail is installed in **/home/vpopmail** , issue the following commands.

```
debian:~# cd /home/vpopmail
debian:~# mkdir -p qtrap/logs
debian:/home/vpopmail/qtrap# cd qtrap
debian:/home/vpopmail/qtrap# wget http://www.pc-freak.net/files/qtrap.sh
...
debian:/home/vpopmail/qtrap# cd ~
debian:~# touch /home/vpopmail/qtrap/logs/qtrap.logdebian:~# chown -R vpopmail:vchkpw
/home/vpopmail/qtrapdebian:~# chmod -R 755 /home/vpopmail/qtrap
```

On older qmail installations it could be vpopmail is installed in **/var/vpopmail** if that's the case, link **/var/vpopmail** to **/home/vpopmail** and go back to step 1. To link:

```
debian:~# ln -sf /var/vpopmail/ /home/vpopmail
```

2. Edit qtrap.sh to whitelist email addresses and build a ban words list

a) Include the email addresses mail arriving from which would not be checked by qtrap.sh

Inside **qtrap.sh** in line 63, there is a shell function *whitelist_check()*, the function looks like so:

```
whitelist_check () {
case $WHITELIST in
address@somewhere.com|address@somewhereelse.com)
echo $SENDER found in whitelist on `date "+%D %H:%M:%S"` >>
/home/vpopmail/qtrap/logs/qtrap.log
exit 0;;
*)
;;
esac
}
```

By default the script has just two sample mails which gets whitelisted this is the line reading:

address@somewhere.com|address@somewhereelse.com

The whitelisted emails should be separated with a pipe, thus to add two more sample emails to get whitelisted by script the line should be changed like:

address@somewhere.com|address@somewhereelse.com|hipod@mymailserver.com|hipo@gmail.com

In order to whitelist an entire domain let's say yahoo.com add a line to the above code like:

address@somewhere.com|address@somewhereelse.com|hipod@mymailserver.com|hipo@gmail.com|*yahoo.com

b) Defining the bad words ban list, mails containing them should not be delivery by qmail

The function that does check for the ban word list inside the script is **checkall();**, below is a paste from the script function:

```
checkall () {
case $BANNED_WORDS in
porn|PORN|Sex|SEX)
printout $BANNED_WORDS
echo MESSAGE DROPPED from $SENDER because of $BANNED_WORDS on `date "+%D %H:%M:%S"` >> /home/vpopmail/qtrap/logs/qtrap.log
exit 99;;
*)
;;
esac
}
```

checkall(); is located on line 74 in **qtrap.sh**, the exact list of banned words which the script should look for is *located on line 76*, the default qtrap.sh filters only mails containing just 4 words, e.g.:

porn|PORN|Sex|SEX)

To add the **Viagra** and **VIAGRA** common spam words to the list, modify it and expand like so:

porn|PORN|Sex|SEX|viagra|Viagra)

The delimiter is again **|** , so proceed further and add any unwanted spam words that are not common for any legit mails.

3. Install qtrap.sh to process all emails delivered to vpopmail

If its necessery to install the dropping of mails based on word filtering only to a single vpopmail virtualdomain do it with cmd:

```
debian:~# cd /home/vpopmail/domains/yourdomain.com
debian:/home/vpopmail/domains/yourdomain.com# touch .qmail-default.new
debian:/home/vpopmail/domains/yourdomain.com# echo '| /home/vpopmail/qtrap/qtrap.sh' >> .qmail-default.new
debian:/home/vpopmail/domains/yourdomain.com# echo "| /home/vpopmail/bin/vdelivermail " bounce-no-mailbox" >> .qmail-default.new
debian:/home/vpopmail/domains/yourdomain.com# chown vpopmail:vchkpw .qmail-default.new
```

debian:/home/vpopmail/domains/yourdomain.com# cp -rpf .qmail-default .qmail-default.bak; mv .qmail-default.new .qmail-default
If however *qtrap.sh* needs to get installed for all existing vpopmail virtualdomains on the qmail server, issue a one liner bash script:

debian:~# cd /home/vpopmail/domains
debian:/var/vpopmail/domains# for i in *; do cd $i; echo "| /home/vpopmail/qtrap/qtrap.sh" >> $i/.qmail-default.new; \
echo "| /home/vpopmail/bin/vdelivermail " bounce-no-mailbox" >> $i/.qmail-default.new; \
chown vpopmail:vchkpw .qmail-default.new; mv .qmail-default .qmail-default.old; mv .qmail-default.new .qmail-default; cd ..; done

This for loop will add '| /home/vpopmail/qtrap/qtrap.sh' to all **.qmail-default** for all vpopmail domains.

Afterwards the **.qmail-default** file should contain the following two lines:

| /home/vpopmail/qtrap/qtrap.sh
| /home/vpopmail/bin/vdelivermail " delete

A very important thing here you should consider that adding some common words, as let's say **hello** or **mail** etc. could easily drop almost all the emails the qmail hands in to vpopmail.

Caution!! Never ever implement common words in the list of words !!
Always make sure the banned words added to qtrap.sh are words that are never enter an everyday legit email.

Another thing to keep in mind is that *qtrap.sh* doesn't make a copy of the received message ,though it can easily be modified to complete this task.
Any mail that matches the banned words list will be dropped and lost forever.

4. Check if qtrap.sh is working

To check, if qtrap is working send mail to some mailbox located on the qmail server containing inside subject or mail message body the unwanted word defined inside **qtrap.sh**.

The mail should not be received in the mailbox to which its sent, if qtrap is working moreover qtrap.sh should log it inside it's log file:

debian:~# cat /home/vpopmail/qtrap/logs/qtrap.log
MESSAGE DROPPED from hipo@mytestmail.com because of viagra on 09/03/11 11:34:19
MESSAGE DROPPED from support@mymailserver.com because of Viagra on 09/03/11 11:39:29

If the **qtrap.log** contains records similar to the one above, and the mail matching the banned word is not delivered, qtrap.sh is properly configured. If any issues check in qmail logs, they should have a good

pointer on what went wrong with qtrap.sh invokation.

Note that I've integrated **qtrap.sh** to custom qmail install running on Debian Lenny 5.0 GNU/Linux.
If I have time I'll soon test if its working fine on the latest stable Debian Squeeze and will report here in comments.
If however someone is willing to test if the script works on Debian Squeeze 6.0 or have tested it already please drop a comment to report if it works fine.
qtrap.sh, is a bit oldish and is not written to work too optimal therefore on some heavy loaded mail servers it can create some extra load and a bit delay the mail delivery. Thus when implementang one needs to consider the downsides of putting it in.

Also I was thinking tt might be nice if the script is rewritten to read the **ban words** and **whitelist mails** from files instead of as it is now as the words are hard coded in the script.
If I have some free time, I'll probably do this, though I'm not sure if this is a too good idea as this might have a negative performance impact on the script execution time, as each instance of the script invoked should do one more operation of reading a file storing the ban words.

Well that's pretty much it, enjoy ;)