VBounceRuleset

The "Virus Bounce Ruleset" is a SpamAssassin ruleset to catch "backscatter".

Backscatter is mail you didn't ask to receive, generated by legitimate, non-spam-sending systems in response to spam. Here are some examples, courtesy of Al Iverson:

- Misdirected "undeliverable email" bounce messages from spam runs, from mail servers who "accept then bounce" instead of rejecting mail during the SMTP transaction.
- Misdirected virus/worm "OMG your mail was infected!" email notifications from virus scanners.
- Misdirected "please confirm your subscription" requests from mailing lists that allow email-based signup requests.
- Out of office or vacation autoreplies and autoresponders.
- Challenge requests from "Challenge/Response" anti-spam software. Maybe C/R software works great for you, but it generates significant backscatter to people you don't know.

It used to be OK to send some of these types of mail – but no longer. Nowadays, due to the rise in backscatter caused by spammer/malware abuse, it is no longer considered good practice to "accept then bounce" mail from an SMTP session, or in any other way respond by mail to an unauthorized address of the mail's senders.

How do I block it?

There's a ruleset to block joe-job, virus-blowback, and spam-blowback bounce messages (a.k.a. "backscatter"), which is included in SpamAssassin 3.2.0. It provides the following rules:

- {{__}}MY_SERVERS_FOUND: a whitelisted relay a la "whitelist_bounce_relays" was found
- BOUNCE_MESSAGE: an MTA-generated bounce from a non-whitelisted relay, "message was undeliverable" etc.
- CRBOUNCE_MESSAGE: Challenge-response bounce message from a non-whitelisted relay, eg. "please confirm your message was not spam"
- VBOUNCE_MESSAGE: a virus-scanner-generated bounce from a non-whitelisted relay, e.g. "You sent a virus"

- ANY_BOUNCE_MESSAGE: any of the *BOUNCE_MESSAGE types above will also trigger this

{{__}}MY_SERVERS_FOUND inhibits the other 4 rules from firing.

Setup

If you are using SA 3.2.x, just enable the `loadplugin Mail::SpamAssassin::Plugin::VBounce` line in `/etc/mail/spamassassin/v320.pre`, and skip to the 'whitelist_bounce_relays' line in step 3 below.

If you are using SA 3.1.x, you can install the ruleset as follows:

1. Download 20_vbounce.cf and VBounce.pm. (Note: download was disabled for 20_vbounce.cf when I tried this - "Checkout view is disabled" - you can get it from here with by copying, pasting into an editor with good rectangle support, and getting rid of the line numbers.)

2. Save both files to your **/etc/mail/spamassassin** directory.

3. Edit your **local.cf** and add a line like the following:

```
  whitelist_bounce_relays myrelay.mydomain.net
```

Replace **myrelay.mydomain.net** with the hostname of the relay (or relays) that you send your outbound mail through.

This is used to 'rescue' legitimate bounce messages that were generated in response to mail you really *did* send. If a bounce message is found, and it contains one of these hostnames in a 'Received' header in the bounced message, it will not be marked as a blowback virus-bounce.

Note that if you do not add this line, the *BOUNCE_MESSAGE rules will never fire! You have to specify at least one whitelisted relay for it to operate.

4. Run **spamassassin --lint** and ensure it works.

5. Check a 'sample vbounce' mail, to ensure it marks blowback bounces as such:

```
spamassassin -Lt < sample-vbounce.txt
[...]
Content analysis details:   (2.6 points, 5.0 required)

 pts rule name              description
---- ---------------------- --------------------------------------------------
 0.0 NO_REAL_NAME           From: does not include a real name
 0.0 FORGED_RCVD_HELO       Received: contains a forged HELO
[...]
 0.1 BOUNCE_MESSAGE       MTA bounce message
 0.1 ANY_BOUNCE_MESSAGE   Message is some kind of bounce message
```

You should see the tests *BOUNCE_MESSAGE* and *ANY_BOUNCE_MESSAGE* appearing in the "Content analysis details" section.

6. Restart spamd, as usual, so that the ruleset is loaded.

7. Edit your procmailrc (or similar) to move messages that contain "ANY_BOUNCE_MESSAGE" in the "X-Spam-Status" header, to a "bounces" folder.

If upgrading from 3.1.x to 3.2.0, you need to delete **VBounce.pm** and **20_vbounce.cf** from **/etc/mail/spamassassin**, so that it doesn't clash with the released version.

Further Steps

If you're using Postfix, and volumes of backscatter at your mailserver are very high, you can also block incoming backscatter during the SMTP transaction. This blog post describes how to do it.

What About My Own Bounces?

You might be worried that the VBounce ruleset will block bounces sent in response to your own mail. As long as the error conditions are flagged during the SMTP transaction (as they should be nowadays), and you've specified your own mailserver(s) in 'whitelist_bounce_relays', you're fine.