

Re: Improvements in TCP/IP Services anti-spam features

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2003-04/2953.html>

From: Don Sykes (*anonymous_at_pacbell.net*)

Date: 04/30/03

Date: Tue, 29 Apr 2003 23:38:44 GMT

John Johnstone wrote:

>
> *There really should be a way to configure the handling of non-existent
> addresses with HP's TCP/IP Services. Mail to non-existent addresses has
> reached an intolerable level here. Of all the email addresses that we
> have, the ones that get the most spam are old addresses that are no
> longer valid. And it's incredibly ironic that the volume of mail being
> sent to them is still on the increase. There has even been a big
> increase to one email address that has never existed.*

I've noticed the same thing. I bet someone with a big pipe (so to speak) got a hold of one of those old 100M email address lists and is now offering "spam services" to customers.

The way things are going, I expect spam to account for 99% of all IP communications by the end of this year!

> *The spam to it
> started coming from a few consistent IP addresses. Since that's been
> filtered, all of the mail to this address come from random IPs with
> random return-paths that are completely unfilterable.*

I really don't want to throw the baby out with the bath water, but I took Michael Austin's suggestion to add :

Bad-Clients: 210.0.0.0/8,211.0.0.0/8,202.0.0.0/8,203.0.0.0/8

as he says, "Add these as well, these are entire Asia/Pacific! (China) entire networks."

I think it helped a little, but I could be loosing business from some good folks in Asia, so I'm keeping as a temporary measure only.

>
> *Since 85% of our spam that isn't blocked has an invalid return address,
> that means all of those messages will be generating a bounce to
> Postmaster. As Don Sykes noted, the side-effect of clogging up the mail
> queues with hopeless retries is also quite a drain.*

comp.os.vms: Re: Improvements in TCP/IP Services anti-spam features

>
> *It was great that they added anti-spam features to TCP/IP Services but
> going just a little bit further would have a huge payoff. How about
> another field name such as Reject-Rcpt-To?*
>
> *Reject-Rcpt-To: old-email-address@domain-name*
>
> *With spam, looking for a signature to match on the mail message (i.e.
> Mail-From, source IP address, etc.) is always a moving target. If
> specific non-existent addresses could be configured for a reject, that
> would block 100% of the spam sent to those addresses. A reject message
> Reject-Rcpt-To-Text could be tailored as desired if feedback for valid
> mail was a concern. In my case, if email is sent any of these
> particular old addresses, there's a 99.999% chance that it's spam.*
>
<snip>

Excellent idea! I think not too difficult to include either. It would solve 99% of my problem too. I wonder why it wasn't included already? (HP response???)

--
Have VMS, Will Travel
Wire paladin, San Francisco
(paladinATalphaseDOTcom)