Subject: Open Relay Protection
Posted by chrisso101 on Fri, 30 Jun 2006 09:47:22 GMT
View Forum Message <> Reply to Message

Hi,

I'm using NoSpamToday v2.3.4.3 on one PC and forwarding mail to our smtp mailserver which is running on another PC.

Our mailserver is old (Infinite Interchange) and does not appear to support SMTP-AUTH so I configure the NoSpamToday proxy using the wizard to limit recipients to

 *@ourdomain.co.uk

so that only mail to our domain is accepted and forwarded to our mailserver.

However, when I run an open relay check like the one at:

http://www.mob.net/~ted/tools/relaytester.php3

I appear to have an open relay.

Subject: Re: Open Relay Protection
Posted by richardhall on Tue, 04 Jul 2006 10:01:01 GMT
View Forum Message <> Reply to Message

Yes, I think our problem is similar.

(a) NoSpamToday seems to only accept recipients from one domain in our list of domain names (there are a good number)

(b) Our server is also an open relay according to that website and after running manual tests I can identify that whilst it will accept any sender address, because it restricts on the recipient addresses to only those within our domain names (obviously only one at the moment but in theory should be all of them), its not effective as an open relay because people can only spoof mail or send spam to individuals within our organisation - they can't send mail to people who don't have local mailbox accounts on our mail server. I suspect your setup is similar.

My questions are as follows:

(1) Why is it ignoring the majority of our domains in the recipient acceptance criteria?

(2) Why does NoSpamToday not require a 'MAIL FROM:' command prior to accepting a 'RCPT TO:' command? Sure it should return a message something like "503 5.5.1 Need MAIL before RCPT" in accordance with RFC2821/821?

(3) Would it not make a lot more sense to restrict the acceptance of the sender to local mailbox account holders rather than the recipients?

Regards,

Richard Hall LRSM BSc MBCS
Software Developer
Source Software Ltd

Subject: Re: Open Relay Protection
Posted by support on Tue, 04 Jul 2006 11:58:55 GMT
View Forum Message <> Reply to Message

> Yes, I think our problem is similar.
>
> (a) NoSpamToday seems to only accept recipients from one domain
> in our list of domain names (there are a good number)
>
> (b) Our server is also an open relay according to that website
> and after running manual tests I can identify that whilst it
> will accept any sender address, because it restricts on the
> recipient addresses to only those within our domain names
> (obviously only one at the moment but in theory should be all
> of them), its not effective as an open relay because people can
> only spoof mail or send spam to individuals within our
> organisation - they can't send mail to people who don't have
> local mailbox accounts on our mail server. I suspect your setup
> is similar.
>
> My questions are as follows:
>
> (1) Why is it ignoring the majority of our domains in the
> recipient acceptance criteria?

Please make sure that the domain entries in NoSpamToday!'s Open Relay Protection list
are separated by blanks.

> (2) Why does NoSpamToday not require a 'MAIL FROM:' command
> prior to accepting a 'RCPT TO:' command? Sure it should return
> a message something like "503 5.5.1 Need MAIL before RCPT" in
> accordance with RFC2821/821?

Please note that NoSpamToday! works as a transparent SMTP proxy.
This means that incoming SMTP sessions are accomplished by the sending

MTA (mail transfer agent) and your mail server.

> (3) Would it not make a lot more sense to restrict the
> acceptance of the sender to local mailbox account holders
> rather than the recipients?

Again, as NoSpamToday! works as a transparent SMTP proxy and does not accept mails
on its behalf, it cannot tell which recipient address maps to a local mailbox and which is merely an
alias.

If you need any further assistance, please turn on detailed logging and send your
nospamtoday.log and nospamtoday.cf files to nstsupport@byteplant.com.