Subject: auto blacklist
Posted by macjung on Fri, 27 Feb 2009 09:21:53 GMT
View Forum Message <> Reply to Message

Hi,

is there a way to disable the new feature, which auto blacklists a host for 20 minutes.

We are sitting behind a mail relay from our provider, so all mail that nospamtoday gets will be from that server. After a few seconds, nospamtoday stops accepting mails from the mail relay server since it got enough spam.

By the way it would be great if the DNSBL Filter would have an additional setting where we could specify which host in the chain should be tested. In our case we wouldn't need to the last one but the one before that.

Subject: Re: auto blacklist
Posted by support on Fri, 27 Feb 2009 10:28:47 GMT
View Forum Message <> Reply to Message

> is there a way to disable the new feature, which auto
> blacklists a host for 20 minutes.
>
> We are sitting behind a mail relay from our provider, so all
> mail that nospamtoday gets will be from that server. After a
> few seconds, nospamtoday stops accepting mails from the mail
> relay server since it got enough spam.
>
> By the way it would be great if the DNSBL Filter would have an
> additional setting where we could specify which host in the
> chain should be tested. In our case we wouldn't need to the
> last one but the one before that.

In a store & forward setup like yours, NoSpamToday's directory harvesting protection does not make any sense because your provider's mail relay has already accepted all incoming mails and you'll not be able to reject any of them.

You should disable the directory harvesting protection in NST by leaving the "Max. Rejected Recipients" setting in the traffic limiting section of the SMTP port wizard empty.

Post Edited (02-27-09 11:29)

Subject: Re: auto blacklist

Posted by macjung on Fri, 27 Feb 2009 11:18:26 GMT
View Forum Message <> Reply to Message

leaving the "Max. Rejected Recipients" empty will worsen the spam filter alot, since the provider mail filter does not filter out unknown recipients. They will forward every mail that is addressed to one of our domains.

From the 30.000 to 40.000 mails we are receiving less than 5% are addressed to valid addresses. Without the "Max. Rejected Recipients" in place my Domino Server behind the nospamtoday server would be swamped.

Any other suggestion?

Subject: Re: auto blacklist
Posted by James Wilkinson on Fri, 27 Feb 2009 17:02:48 GMT
View Forum Message <> Reply to Message

As for your last question -- which Received lines can be trusted -- this is what the SpamAssassin internal_networks directive does. Obviously, it only works if you get SpamAssassin to do DNSBL lookups.

In this case, you'd want to list your local network, and the IP addresses of all mail relays. Find the sa\ruleset\local.cf file, and add something like:
trusted networks 192.168.1.0/24 10.5.3.4 10.266.5.0/24
assuming that your local network is 192.168.1.x, and your ISP has a mail relay at 10.5.3.4 and others at 10.266.5.y.

Run sa-lint.bat to check you've got everything right, then restart NoSpamToday. (You can just double-click on sa-lint.bat.) Make sure there's nothing between these two lines:
C:\Program Files\No Spam Today!>sa\spamassassin -x --siteconfigpath="sa\ruleset" --lint

C:\Program Files\No Spam Today!>pause

(I prefer to get SpamAssassin to do DNSBL lookup because we have correspondents in places like India, China and Turkey. They tend to do weird things and/or use dodgy ISPs and get on one list or another. The SpamAssassin AWL can "rescue" their mail, especially since we have custom SpamAssassin rules looking for our standard company signature and message-IDs. That means anyone who replies to one of our emails is likely to get a SpamAssassin score of less than -10, and is very unlikely to get blocked even if they do end up on a DNSBL).

Hope this helps,

James.

Subject: Re: auto blacklist
Posted by support on Fri, 27 Feb 2009 17:40:27 GMT

macjung wrote:

> leaving the "Max. Rejected Recipients" empty will worsen the
> spam filter alot, since the provider mail filter does not
> filter out unknown recipients. They will forward every mail
> that is addressed to one of our domains.
>
> From the 30.000 to 40.000 mails we are receiving less than 5%
> are addressed to valid addresses. Without the "Max. Rejected
> Recipients" in place my Domino Server behind the nospamtoday
> server would be swamped.
>
> Any other suggestion?

Hold your horses! Setting "Max. Rejected Recipients" to empty does not change which mails will be accepted by your setup. It just disables the part that disconnects and blocks offending remote hosts.