Subject: HELO domain (reject?)
Posted by Patrick Buresh on Tue, 21 Dec 2004 17:39:06 GMT
View Forum Message <> Reply to Message

I'm having a bit of trouble with the Reject by HELO domain feature.
We constantly get spam from multiple IP addresses which appear to claim to be from a machine calling itself 64.69.111.211.
(i.e. Received: from 64.69.111.211 ([207.69.35.247])).
I assumed by placing 64.69.111.211 in the "Reject by HELO domain" list, that it would block these messages, but it does not.
Do I not understand how this lists works?
We also get many spam messages where the sending servers' name ends in a country designator such as .jp for Japan.
(I.e. Received: from smtp.email.spamalot.jp ([209.114.7.1]) or mail.greatoffers.com.jp ([66.54.92.44])).
If I enter *.jp in the domain list, it appears to do nothing as well. I thought that the wildcard * would include any domain prefix as long as it ended with .jp ?

Can anyone offer any suggestions?

Thanks.

Post Edited (12-21-04 18:41)

Subject: Re: HELO domain (reject?)
Posted by support on Thu, 23 Dec 2004 13:19:26 GMT
View Forum Message <> Reply to Message

> I'm having a bit of trouble with the Reject by HELO domain
> feature.
> We constantly get spam from multiple IP addresses which
> appear to claim to be from a machine calling itself
> 64.69.111.211.
> (i.e. Received: from 64.69.111.211 ([207.69.35.247])).
> I assumed by placing 64.69.111.211 in the "Reject by HELO
> domain" list, that it would block these messages, but it does
> not.
> Do I not understand how this lists works?

NoSpamToday! puts the HELO name into the Received header, so you are right, it should have been working. But are you sure this is the Received header added by NoSpamToday?

Another sure way to find the HELO name is to enable detailed logging, and to look for the parameter of the HELO or EHLO commands used by the sending mail server in the log.

> We also get many spam messages where the sending servers'
> name ends in a country designator such as .jp for Japan.
> (I.e. Received: from smtp.email.spamalot.jp ([209.114.7.1])
> or mail.greatoffers.com.jp ([66.54.92.44])).
> If I enter *.jp in the domain list, it appears to do nothing
> as well. I thought that the wildcard * would include any domain
> prefix as long as it ended with .jp ?

Yes, but again only the HELO name used in the SMTP session counts, so I suppose the .jp header is either faked or was added by an earlier mail relay.

You can add the following rule to local.cf to filter all mails relayed by a *.jp server:

```
header RELAYED_JAPAN received =~ /.*\.jp/i
describe RELAYED_JAPAN Mail was relayed by some Japanese server
score RELAYED_JAPAN 5.0
```

Post Edited (12-23-04 14:28)