Subject: No more China mail please!
Posted by RandallRash on Tue, 27 Dec 2005 17:20:57 GMT
View Forum Message <> Reply to Message

I am wondering how the following message got through. I am trying to use the zz-nerd database to filter e-mail from China. The following is the headers in the mail as stored from the Mail storage filter: (between the **********)
****
Return-Path:
Received: from 192.168.0.14 by mail.mycompany.com ([192.168.0.4] running VPOP3) with SMTP for ; Mon, 26 Dec 2005 13:25:36 -0600
X-Spam-Checker-Version: SpamAssassin 3.1.0 (2005-09-13) on SpamCheck.mycompany.local.com
X-Spam-Level: *****
X-Spam-Status: No, score=5.6 required=6.0 tests=BAYES_99,DATE_IN_PAST_12_24 autolearn=no version=3.1.0
Received: from cooltoad.com ([61.173.23.188]) by SpamCheck.mycompany.local.com ([192.168.0.14], envelope-sender=) with No Spam Today! Service V2.3.3.3 100 Recipients for 192.168.0.4; Mon, 26 Dec 2005 13:25:22 -0600
Message-ID:
Date: Mon, 26 Dec 2005 07:31:28 +0200
Reply-To: "lenita reyes"
From: "lenita reyes"
User-Agent: Rodriquezmail v9.8
MIME-Version: 1.0
To: "Katelyn Reed"
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: 7bit
X-NoSpamToday-FileID: SpamCheck_0002D8B5.msg
Subject: {Mon-Incoming} Abolish all that you owe without sending an other
dime
X-Monitor-Recipient: john.doe
****

The filter rule looks like this:
header NERD_DK eval:check_rbl('nerd', 'zz.countries.nerd.dk.')
tflags NERD_DK net
score NERD_DK 0.1

header NERD_CHINA eval:check_rbl_sub('nerd', '127.0.0.156')
describe NERD_CHINA CHINA
tflags NERD_CHINA net
score NERD_CHINA 3.0
****

I've seen a few messages that have been filtered by zz.countries.nerd.dk but most are not. I am assuming this one should because if I look up the "Received from" IP address above (61.173.23.188) using dnsstuff.com it says it's from China.

Subject: Re: No more China mail please!

Posted by support on Thu, 29 Dec 2005 12:17:19 GMT
View Forum Message <> Reply to Message

[...]

> I've seen a few messages that have been filtered by
> zz.countries.nerd.dk but most are not. I am assuming this one
> should because if I look up the "Received from" IP address
> above (61.173.23.188) using dnsstuff.com it says it's from
> China.
> Am I using the filter correctly?

The fact that some mails were filtered with this new rule indicates that all is well. Perhaps the server in question was not yet in the database.
Even without the nerd rule contributing to the score it was a close call, 5.6 points out of six.