

Re: Undeliverable Mail showing up from my domain postmaster (exchange 2)

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-07/msg03419.html>

- *From:* v-jerryz@xxxxxxxxxxxxxxxxxxxxxx (Jerry zhao (MSFT))
 - *Date:* Fri, 15 Jul 2005 03:48:03 GMT
-

Hi Kevin,

Thank you for the post. And thank our MVP for the answer.

>From the description, it seems that you may under the RNDR attack or the sender just flood the spam to random recipients.

For your information:

Spammers have a new means to avoid filters built into many systems. They take advantage of a mail systems sending of a non-delivery report (NDR) when a message cannot be delivered as addressed and returns the original contents. Since this follows the RFC standard, most all mail servers will function this way. This is what is called a "Reverse NDR attack" (RNDR). This form of attack is becoming increasingly widespread. Some users get it so badly that over 33% of their Internet messages are attributed to this type of spam. The end result is the spammer has attained a new form of mail relaying. Your server's resources are being stolen to deliver spam.

How does a "Reverse NDR" attack work?

Step 1 Spam email is created with the intended spam victim's address in the sender field and a random, fictitious recipient, at your domain, in the To: field.

Step 2 Your mail server cannot deliver the message and sends an NDR email back to what appears to be the sender of the original message, the spam victim.

Step 3 The return email carries the non-delivery report and possibly the original spam message. Thinking it is email they sent, the spam victim reads the NDR and the included spam.

What are the symptoms of a RNDR attack?

1. Sluggish email delivery
2. Outbound queues full of non-delivery notices
3. Excessive admin time to clear outbound queues

If you are experiencing any of the above, chances are good your mail server is under attack.

Re: Undeliverable Mail showing up from my domain postmaster (exchange 2

Those NDR spam can be resolved with two simple checkboxes on Recipient Filtering of the Message Delivery section of Global Settings.

For your information:

Exchange queues fill with many non-delivery reports from the postmaster account in Small Business Server 2003

<http://support.microsoft.com/default.aspx?scid=kb;en-us;886208>

If it is not your case or it dose not work, please help me collect the following information:

1. Are you using POP3 mailbox to receive mail?
2. What are the senders' addresses for those emails? Are they same?

If you have any questions please do not hesitate to let me know. I am glad to be of assistance.

Best regards,

Jerry Zhao (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.
=====

This posting is provided "AS IS" with no warranties, and confers no rights.

• **Follow-Ups:**

- ◆ **Re: Undeliverable Mail showing up from my domain postmaster (exchan**
◇ From: Kevin

• **References:**

- ◆ **Undeliverable Mail showing up from my domain postmaster (exchange 2**
◇ From: Kevin

- Prev by Date: **RE: SQL 2000 Question**
- Next by Date: **RE: Exchange 2003 and timeout errors on XP machines**
- Previous by thread: **Undeliverable Mail showing up from my domain postmaster (exchange 2**
- Next by thread: **Re: Undeliverable Mail showing up from my domain postmaster (exchan**

Re: Undeliverable Mail showing up from my domain postmaster (exchange 2

Re: Undeliverable Mail showing up from my domain postmaster (exchange 2

- Index(es):

- ◆ *Date*

- ◆ *Thread*