

Re: Exchange Weird Issue

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-07/msg00434.html>

- *From:* "ChickenMan" <spam@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 5 Jul 2006 17:32:52 +1200
-

Thanks for your reply :

Emails are from different external users, that aren't spam as they're involved in a conversation with the intended recipient.

No – not NDR's but the actual message that was intended for the person they were sending too. I.e. the user it's addressed to (A) is in the to box, but person B is getting the message.

Just one user having the problem, and whenever it happens it goes through to the same user each time.

So I don't think it's a spam or open relay issue...

Further ideas?

Thanks
Marek

"chace zhang" <v-chacez@xxxxxxxxxxxxxxxx> wrote in message [news:d0HcgI\\$GHA.4612@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:d0HcgI$GHA.4612@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi,

Thank you for posting here.

According to your description, I understand one of your internal users receives a lot of unknown recipients' emails. If I have misunderstood your concern, please do not hesitate to let me know.

In order to clarify your issue, please help me to gather following info:

- Are these emails from internal user or external user?
- Are these emails from specific domain or random domain?
- Are these emails NDR reports?
- Does this issue occur on specific user or all users?

Based on my experience, this issue can be any or a combined of the following situations:

1. You under spam attack

Re: Exchange Weird Issue

2. Your server is open relaying emails.
3. Your server are under RNDR attack.

I would like to suggest you try the following suggestions:

Suggestion 1:

Add a name to the Blocked Senders List on the Outlook 2003 client:

1. Open Outlook.
 2. On the Tools menu, click Options.
 3. Click Junk E-mail.
 4. Click the Blocked Senders tab.
 5. Click Add.
 6. In the Enter an e-mail address or Internet domain name to be added to the list box, enter the name or address you want added, and then click OK. For example, you can add @*.cn
- Note: You can remove and re-add it to check.
7. Repeat steps 4 and 5 for each name or address that you want to add.

NOTE: Please make sure the above lists do not listed in the Safe Sender.

Suggestion 2:

A. Disable the Guest account in your SBS 2003 server and enable Stronge Password Protection. You can also have your users change their passwords. Everytime when you run CEICW you will be asked for enabling password policies after it ends. I suggest you enable it. You can also do that in Server Management\Users->Configure Password Policies. For more information, see:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx>

B. Block open relay and clean up the SMTP queues by referring to the following KB article:

324958 How To Block Open SMTP Relaying and Clean Up Exchange Server SMTP Queues
<http://support.microsoft.com/?id=324958>

If you find many emails are NDR emails generated by postmaster or administrator of your server, your server should be under Reverse DNS Attack. Nowadays 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.

Re: Exchange Weird Issue

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. You may observe the following symptoms:

1. Exchange mailboxes are receiving NDR's for mail that they did not send.
2. Non delivery reports are filling the SMTP queues. Messages appear from Postmaster or "<>".
3. There are hundreds (sometimes thousands) of SMTP queues where there are normally just a few.

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.

To stop the RNDR from happening, you can try either of the following solutions based on your configuration:

If you use SMTP to receive inbound emails

– Configure Recipient Filtering

When you enable recipient filtering on the SMTP virtual server, e-mail messages that are received from anyone on the recipient filter are not accepted. Recipient filtering is set globally, but you enable it on a per-Virtual Server basis on each SMTP virtual server.

Re: Exchange Weird Issue

– Create a recipient filter:

1. Click "Start", point to "Programs", point to "Microsoft Exchange", and then click "System Manager".
2. Expand "Global Settings", right-click "Message Delivery", and then click "Properties".
3. Click the "Recipient Filtering" tab, and then click the checkbox at the bottom (Filter recipients who are not in the directory).
4. Specify any additional filter options that you want to configure, Select Apply, and then click "OK".

To enable recipient filtering on the SMTP virtual server:

1. Click "Start", point to "Programs", point to "Microsoft Exchange", and then click "System Manager".
2. Expand "Servers", expand "<ServerName>", and then expand "Protocols".
3. Expand "SMTP", right-click "Default SMTP Virtual Server", and then click "Properties".
4. Click the "General" tab, and then click "Advanced".
5. In the "Address" list, click the IP address where you want to apply the recipient filter, and then click "Edit".
6. Click to select the "Apply Recipient Filter" check box, click "OK", and then click "OK".

Note: Recipient filter rules apply only to anonymous connections. Authenticated users and Exchange servers bypass these validations.

If you are using POP3 Connector to receive inbound emails

In this scenario, we cannot use recipient filters to stop the attack. You will have to contact your ISP to help you stop the NDR attack. Or you will need to disable the NDR feature. To do so, please refer to the following KB article:

294757 How to control non-delivery reports when you use Exchange 2000 or <http://support.microsoft.com/?id=294757>

We can also use third party tools to block NDR attack:

Re: Exchange Weird Issue

[http://www.cmsconnect.com/Praetor/WebHelp/zAppendix_B - Message tests/Thwarting_reverse_NDR_attacks.htm](http://www.cmsconnect.com/Praetor/WebHelp/zAppendix_B_-_Message_tests/Thwarting_reverse_NDR_attacks.htm)

http://www.mapilab.com/exchange/mail_guard/

Suggestion 3:

You can also install third party anti-spam and antivirus software however you should make sure they are fully compatible with Windows Server 2003 and

Exchange Server 2003. Otherwise they may cause instability to the server.

If you install antivirus software, you should exclude the SYSVOL and Exchange installation folder exchsrvr from being scanned. For more information, see:

823166 Overview of Exchange Server 2003 and antivirus software

<http://support.microsoft.com/?id=823166>

822158 Virus Scanning Recommendations on a Windows 2000 Domain Controller

<http://support.microsoft.com/?id=822158>

NOTE: This response contains a reference to a third party World Wide Web site. Microsoft is providing this information as a convenience to you.

Microsoft does not control these sites and has not tested any software or information found on these sites; therefore, Microsoft cannot make any representations regarding the quality, safety, or suitability of any software or information found there. There are inherent dangers in the use of any software found on the Internet, and Microsoft cautions you to make sure that you completely understand the risk before retrieving any software from the Internet.

Hope this helps.If you have other concerns on this issue, please feel free to let me know.

Have a nice day!

Best Regards,

Chace Zhang (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! - www.microsoft.com/security

=====
This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner.

Re: Exchange Weird Issue

You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the

"Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

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

| From: "ChickenMan" <spam@xxxxxxxxxxxxxx>
| Newsgroups: microsoft.public.windows.server.sbs
| Subject: Exchange Weird Issue
| Date: Tue, 4 Jul 2006 18:34:15 +1200
| Organization: Slingshot Internet
| Lines: 13
| Message-ID: <1151994752.698676@ftpsrv1>
| NNTP-Posting-Host: news.tranzpeer.net
| X-Trace: lust.ihug.co.nz 1151994917 17467 202.180.64.19 (4 Jul 2006
06:35:17 GMT)
| X-Complaints-To: abuse@xxxxxxxxxx
| NNTP-Posting-Date: Tue, 4 Jul 2006 06:35:17 +0000 (UTC)
| X-Priority: 3
| X-MSMail-Priority: Normal
| X-Newsreader: Microsoft Outlook Express 6.00.3790.2663
| X-RFC2646: Format=Flowed; Original
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.2663
| Cache-Post-Path: ftpsrv1!unknown@xxxxxxxxxxxxxx
| X-Cache: nntpcache 2.3.3 (see <http://www.nntpcache.org/>)
| Path:
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTFEEDS01.phx.gbl!newsfeed00
.sul.t-online.de!t-online.de!newshub.sdsu.edu!logbridge.uoregon.edu!newsfeed
s.ihug.co.nz!lust.ihug.co.nz!ihug.co.nz!not-for-mail
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.windows.server.sbs:279006
| X-Tomcat-NG: microsoft.public.windows.server.sbs

Re: Exchange Weird Issue

|
| Hey,
|
| I have an issue on SBS Premium where one user every now and then
receives
| another users email. It's not coming from the same sender each time, and
| some of the time it's in the middle of a conversation (i.e. had been
| replying back and forth).
| I can't figure it out!?
|
| Any ideas?
|
| Thanks
|
|
|