

## RE: OMA and Outgoing Spam

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-09/msg03445.html>

---

- *From:* Doc <[Doc@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Doc@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 21 Sep 2006 10:17:02 -0700
- 

Chace,

Thanks so much for all of the info.. I will work through it and see if this fixes the problem... This is very helpful!!

Doc

"chace zhang" wrote:

Hi,

Thank you for your update!

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

1. Someone hacked a user account and use it to spam emails;
2. Your Exchange server is open relaying emails;( You have checked it already)
3. A virus or spyware inside your network is sending emails;
4. Your server is under RNDR Attack.

I would like to suggest you try the following suggestions:

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:

RE: OMA and Outgoing Spam

324958 How To Block Open SMTP Relaying and Clean Up Exchange Server SMTP Queues

<http://support.microsoft.com/?id=324958>

After performing the above suggestions, check if everything is OK. If you still see many unsolicited emails in the SMTP queues, you can try the suggestions below:

C. If you are using POP3 Connector for incoming emails, make sure POP3 Connector is not relaying emails. You should install the update described in the following KB article:

835734 Many unexpected outbound e-mail messages appear in the SMTP queue in  
<http://support.microsoft.com/?id=835734>

D. If you are using SMTP for incoming emails, you can install IMF (Intelligent Message Filter):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=C1B08F7B-8CAF-4147-B074-8C9C8F277071&displaylang=en>

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.msp>

However if you are using POP3 Connector for incoming emails, IMF will not work and you can ignore this suggestion.

E. You can install SBS 2003 compatible antivirus or anti-spam software on your server to kill viruses. You can go to the following web page and download the spyware removal tool to scan and remove any spyware on the server and the problematic client computers:

<http://www.firewallguide.com/spyware.htm>

F. 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. 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.

## RE: OMA and Outgoing Spam

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.

– 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".

## RE: OMA and Outgoing Spam

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:

[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/](http://www.mapilab.com/exchange/mail_guard/)

F. 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:

RE: OMA and Outgoing Spam

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.

Regarding your questions:

1. This is possible.
2. You can use message tracking against a SMTP queue to check for the message trace:

821910 How to troubleshoot for Exchange Server 2003 transport issues  
<http://support.microsoft.com/?id=821910>

3. Spammers have several methods to hide the original sender to spam emails and it's hard to track the original sender. You can implement the above suggestions to block spam and unsolicited emails.
4. See above suggestions.

Please do not hesitate to let me know if you have any further concerns

Best Regards,

Chace Zhang (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – [www.microsoft.com/security](http://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. 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

RE: OMA and Outgoing Spam

"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.

---

| Thread-Topic: OMA and Outgoing Spam  
| thread-index: Acbb/vAKI3kd5nkCSYatOSX8yZV7sA==  
| X-WBNR-Posting-Host: 63.150.7.130  
| From: =?Utf-8?B?RG9j?= <Doc@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
| References: <FB2173A3-9E78-47F0-B2A9-31E74E150F8B@xxxxxxxxxxxx>  
<aB8CSE72GHA.3440@xxxxxxxxxxxxxxxxxxxxxxxx>  
| Subject: RE: OMA and Outgoing Spam  
| Date: Tue, 19 Sep 2006 08:19:02 -0700  
| Lines: 164  
| Message-ID: <DD618CF4-DEF7-4CF5-9CA6-278C989EA41D@xxxxxxxxxxxx>  
| MIME-Version: 1.0  
| Content-Type: text/plain;  
| charset="Utf-8"  
| Content-Transfer-Encoding: 7bit  
| X-Newsreader: Microsoft CDO for Windows 2000  
| Content-Class: urn:content-classes:message  
| Importance: normal  
| Priority: normal  
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830  
| Newsgroups: microsoft.public.windows.server.sbs  
| Path: TK2MSFTNGXA01.phx.gbl  
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.windows.server.sbs:298636  
| NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250  
| X-Tomcat-NG: microsoft.public.windows.server.sbs  
|  
| Chace,  
| Thanks so much for the response! The outgoing SPAM was discovered using  
the  
| message tracking tool and noting a great deal of activity after-hours. I  
| really have no way of seeing the actual email message as the SPAM appears

RE: OMA and Outgoing Spam

to  
| be spoofing the user in question, i.e., the "from" and "to" fields are  
the  
| same yet the message is being sent via SMTP to njbrwigsp2-13 (can be any  
| server with this name from 2 to 13). I've got recipient filtering  
established  
| and I also have the relay option turned off. Additionally I'm running the  
IMF  
| on all inbound mail...  
|  
| Thanks again!  
| Doc  
|  
| "chace zhang" wrote:  
|