

## Re: Mass emails

**Source:**

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.admin/2004-12/0456.html>

---

**From:** Francis ([francis\\_at\\_chl.net.au](mailto:francis_at_chl.net.au))

**Date:** 12/11/04

Date: Sun, 12 Dec 2004 01:31:49 +0800

Thank you very much Anthony. I am sure that is what happened. There are 3 transmitting sites in some headers that we recieved.

Francis

"Anthony Edwards" <[anthony.edwards@uk.easynet.net](mailto:anthony.edwards@uk.easynet.net)> wrote in message news:10rkko1heqe4s51@news.supernews.com...

> On Sat, 11 Dec 2004 07:27:08 +0800, Francis <[francis@chl.net.au](mailto:francis@chl.net.au)> wrote:

>> Hi,

>>

>> We had a strange and very unpleasant event happen when one of our users

>> sent

>> an email using a large distribution list in the cc: box instead of bcc:

>> Emails were sent repeatedly to the recipients as though we were spamming

>> or

>> infected with a virus.

>> When we checked the headers of some of those emails received, it was not

>> sent repeatedly from our server but through some of the recipients in the

>> list although the from: address is the originator.

>> We just cannot figure out what had happened as the same list was used

>> frequently in the bcc: box and nothing like that happened.

>> Has anyone experienced this or have any knowledge of it. Please help.

>> Thank

>> you.

>

> You have almost certainly (innocently) been bitten by the increasingly

> problematic Microsoft Small Business Server 2003 POP3 connector issue.

>

> There is a particular problem on the Internet at present where sites

> are using Microsoft Small Business Server 2003 and are collecting their

> mail using that product's included POP3 connector to retrieve mail

> from a POP3 mailbox or mailboxes, rather than receiving mail by SMTP.

> The aforementioned POP3 connector contains a bug which causes it to

> re-send all messages that it receives to all email addresses in the

> "To" and Cc" fields of the messages concerned.

>

> This issue is explained at the following URL:

Re: Mass emails

>  
> <http://support.microsoft.com/?kbid=835734>  
>  
> As you can see, there is a downloadable update which resolves this  
> issue, which is simple and easy to apply.  
>  
> I imagine that two or more of the original recipients of the email  
> in question are using SBS 2003 and an unpatched version of its POP3  
> connector to collect their mail. As a result, a continuous mail loop  
> will be in existence and that will be the reason why all original  
> recipients continue to receive copies.  
>  
> If you can, attempt to obtain copies of the emails which are being  
> retransmitted due to this bug, and analyse their SMTP headers in order  
> to identify the retransmitting sites (there will be at least two).  
> You should then by means of SMTP header analysis be able to identify  
> either the actual transmitting sites, or the ISPs to whose networks  
> the sites are connected, or both. Then, contact those sites and  
> the abuse departments at the ISPs concerned with a request that the  
> retransmitting sites download and apply the patch available at the  
> URL referenced above.  
>  
> A recent high profile incident of this type here in the UK:  
>  
> <http://www.theregister.co.uk/2004/11/30/email-outbreak/>  
> <http://www.mcmillan-scott.plc.uk/news/?pid=2967&lsid=3002&edname=16710.htm&ped=16710>  
> <http://www.mcmillan-scott.plc.uk/news/?pid=2967&lsid=3002&edname=16713.htm&ped=16713>  
> <http://www.mcmillan-scott.plc.uk/news/?pid=2967&lsid=3002&edname=16814.htm&ped=16814>  
>  
> ISPs' abuse desks are finding that complaints related to this issue  
> are increasingly common, and will no doubt continue to increase in  
> volume as more copies of SBS 2003 are sold and deployed.  
>  
> In view of the above, senders of any particular mailing or mailshot,  
> particularly one likely to be received by small business customers  
> within the target market for Microsoft Small Business Server 2003,  
> should take care to ensure that just one email address is included in  
> "To" (and "Cc") and that all other recipients are added to the "Bcc"  
> field (this is generally good policy on privacy grounds also since  
> exposing the email address of all recipients of a mailing to all  
> other recipients of the mailing is usually not a good idea, since it  
> can result in one or more rogue recipients of the mailing deciding  
> to subsequently use or resell the resultant list of email addresses  
> for spamming purposes).  
>  
> I hope this helps.  
>  
> --  
> Anthony Edwards \* [anthony.edwards@uk.easynet.net](mailto:anthony.edwards@uk.easynet.net)  
> Abuse Team Manager \* Tel: 0800 053 0588  
> Easynet Ltd \* DDI: 0161 227 0707

microsoft.public.exchange2000.admin: Re: Mass emails

> <http://www.uk.easynet.net> \* Fax: 0845 333 4503