

Re: Growing SMTP queue to random domains

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2004-04/3561.html>

From: Peter Murray (*anonymous_at_discussions.microsoft.com*)

Date: 04/22/04

Date: Thu, 22 Apr 2004 14:41:45 -0400

Hello,

Use Notepad to open the messages in your out bound queue and find out what machine is sending these messages. You can tell by the first "Received" line in the header.

If most messages are coming from an internal machine, unplug it from the network and run anti-virus software on it.

I'd also recommend using a third party software for anti-spam such as Spam Marshall. Besides, read the following article on Intrusion Detection.

<http://www.spammarshall.com/SpamMarshallWeb/SMTPIntrusionDetection.jsp>

Regards.

Peter

Plee wrote:

- > *We have seen this issue where the SMTP queue on an Exchange 2000 Server*
- > *begins to grow. The domains are valid but the email addresses seem suspect*
- > *(i.e. kxkevgrlw@domain.com). However, the domains are not known to the*
- > *business and generally appear to be completely random. If we enumerate the*
- > *messages they all are sent from the postmaster with the subject "Delivery*
- > *Status Notification (Failure)."*
- >
- > *The only knowledge base article I could find (324958) describes this problem*
- > *only if the mail server is open for relay or is on a black list of some*
- > *sort. The servers that are experiencing this issue are not open for relay*
- > *and are not blacklisted.*
- >
- > *Does anyone know what is the cause of this and the fix? Has a machine on*
- > *the LAN been compromised and is being used to send out SPAM? We have seen*
- > *this in several of the enviroments we support and we are eager to get to the*
- > *bottom of this.*
- >
- > *Thanks.*
- >

microsoft.public.exchange.admin: Re: Growing SMTP queue to random domains

>