

## Re: Possible worm...please help

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2007-10/msg01740.html>

---

- *From:* "Rich Matheisen [MVP]" <[richnews@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:richnews@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 17 Oct 2007 14:27:46 -0400
- 

"Matthew Laping" <[mlaping@xxxxxxxxxxxxxxxxxxxxxxxxx](mailto:mlaping@xxxxxxxxxxxxxxxxxxxxxxxxx)> wrote:

Not sure if this is the proper place for this, but since it is Exchange related let's start here. I had started to notice that out bound emails were not getting delivered. When I checked the Event Viewer I came across the following message:

The inbound SMTP queue currently exceeds 4000 items. The Internet Mail Service will not accept inbound connections until the inbound content conversion queue has dropped below 3000 items

I also noticed that the Outbound Message Awaiting Delivery queue was filled with emails awaiting delivery. For the most part the Originator is the same. So I started to think my server was infected with a worm. I disconnected the network cable and after deleting all the messages in the queue, they kept coming back...about a thousand a minute!

Probably queued up NDRs.

I have scanned the server with Norton Anti-Virus and with Spybot, neither found anything. What else can I try? Is there a way to see the emails and see where they are coming from?

My first guess would be that they're NDRs from messages sent to non-existent addresses in your domain. Have a look at a few of them in the outbound directory and see what they are.

Exchange 5.5 should never be connected directly to the Internet. It was bad enough in 1997 but today it's subject being overwhelmed by spam (even more so than it was back then). Stand up a Windows 2003 server (or Linux/FreeDSB) as a SMTP relay and start refusing to accept messages sent to addresses you can't deliver mail to. You can, if you like, also use a DNSBL on the relay to reduce the number of inbound

Re: Possible worm...please help

connections to your Exchange server.

--

Rich Matheisen

MCSE+I, Exchange MVP

MS Exchange FAQ at [http://www.swinc.com/resource/exch\\_faq.htm](http://www.swinc.com/resource/exch_faq.htm)

Don't send mail to this address <mailto:h.pott@xxxxxxxxxxxxxx>

Or to these, either: <mailto:h.pott@xxxxxxxxxxxxxx> <mailto:melvin.mcphucknuckle@xxxxxxxxxxxxxx>

<mailto:melvin.mcphucknuckle@xxxxxxxxxxxxxx>

.