

Re: SBS 2003 – Exchange: email address hijack?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2009-02/msg00415.html>

- *From:* "SteveB" <newsgroup@xxxxxxxxxxx>
 - *Date:* Thu, 5 Feb 2009 19:42:11 –0800
-

In addition do you have SBS 2003 PE with ISA 2004? If so you can block all SMTP traffic being sent from IP addresses in China and Russia. I believe Leythos also does that with the hardware firewalls he recommends.

"Les Connor [SBS MVP]" <les.connor@xxxxxxxxxxxxx> wrote in message news:eDLDxIAiJHA.2384@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Use zen.spamhaus.org to reject them.

In Exchange System Manager | Global Settings Message Delivery Properties > connection filtering

Add a Block List Service Configuration

Display Name: zen.spamhaus.org

DNS Suffix of Provider: zen.spamhaus.org

Custom Error Message: Connection refused – zen.spamhaus.org

OK your way out.

Expand <servername> | Protocols | SMTP, and r-click default smtp virtual server >properties

General Tab > Advanced button

Edit button

Ensure you have Apply Connection Filter selected

OK your way out.

R-click the default smtp virtual server, and select 'stop'

r-click the default smtp virtual server, and select 'start'

That should get you out of immediate trouble.

There's a fair bit more you can do (and should do) to control spam as well, both within the Exchange configuration, and with 3rd party applications.

--

Les Connor [SBS MVP]

"Thomas Kroljic" <tkroljic@xxxxxxxxxxx> wrote in message

Re: SBS 2003 – Exchange: email address hijack?

news:ewMKC2\$hJHA.3380@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

All,

Currently running SBS 2003 R2. I have an high level user whose email address may have been hijacked. This user is receiving thousand of emails per hour. It appears that someone is sending out emails using my user's email address and all the bounce backs are coming into his email box. It is mostly from China and Russia.

Not being an expert in Exchange Server, is there a way to determine if the emails are a) being sent out from our server to begin with, or b) are they sent from another location and we are receiving the Undeliverable notices?

All the emails (thousands of them) are address as System Administrator (Undeliverable) or Mail Delivery Subsystem (Could not send message.)

Not sure how to handle this problem. Also, I hope this is the proper forum since it exists on a SBS server. If not, let me know which forum would be more appropriate.

Thank you,

Thomas J. Kroljic