

microsoft.public.exchange.admin: Re: Exchange Server may be hacked...Please help.

Re: Exchange Server may be hacked...Please help.

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2005-03/0429.html>

From: you know who maybe (*nguser2u_at_spamnotAOL.com*)

Date: 03/02/05

Date: Wed, 2 Mar 2005 08:20:36 -0800

Are you sure someone isn't just forging your email address to send spam and you are getting the responses? This is quite common.

"Stephen Zachmann" <StephenZachmann@discussions.microsoft.com> wrote in message news:F78A87EA-CE04-43CA-A44D-26B8FCEB81A4@microsoft.com...

> I posted a message before about my exchange server possibly being hacked
> but

> I have still not figured it out. Here is as detailed a rundown as I can
> provide.

>

> 1. server is sending me lots of messages saying the following:

> The original message was received at Mon, 28 Feb 2005 14:23:30 -0800 from
> mydomain.com [196.41.180.99]

>

> ----- The following addresses had permanent fatal errors -----

> szachmann@mydomain.com

>

> ----- Transcript of session follows -----

> ... while talking to server mydomian.com.:

>>>> MAIL From: "Returned mail" <noreply@mydomain.com>

> <<< 506 "Returned mail" <noreply@mydomain.com>... Access denied

>

>

> OR

>

>

> Dear user of mydomain.com, administration of mydomain.com would like to
> inform you

>

> Your email account has been used to send a large amount of junk email
> during

> the recent week.

> Most likely your computer was infected and now contains a hidden proxy
> server.

>

> Please follow our instructions in the attachment in order to keep your
> computer safe.

Re: Exchange Server may be hacked...Please help.

microsoft.public.exchange.admin: Re: Exchange Server may be hacked...Please help.

>
> *Best regards,*
> *The mydomain.com team.*
>
>
> *2. They come from noreply@mydomain.com, mailer-daemon@mydomain.com, or*
> *postmaster@mydomain.com*
>
> *3. They all have attachments that my server is regarding as viruses and*
> *replaces with a simple text file. The file it replaces is usually*
> *'myusername@mydomain.com.zip'.*
>
> *4. I actually recieved message the other day claiming to be from the fbi*
> *(it came from police@fbi.gov). It also had a supposed virus attachment.*
>
> *5. my server is claiming that store.exe is allocating more memory than*
> *usual and an I also get alerts (that I set up) stating that the queue is*
> *sending out more than 15 messages a minute (which is the threshold I set).*
> *We are a very small organization so the send queue is probably (at best)*
> *50*
> *messages for the entire day.*
>
> *6. logged emails and checked the logs as best as i could and did not find*
> *a*
> *copious amount of outgoing mail (hardly any)*
>
> *7. checked the queue in system manager and found nothing in it. We had*
> *been hacked before (about a year ago) and th queue was huge then.*
>
> *8. I could send a message to a yahoo address so I don't think we've been*
> *blacklisted.*
>
> *9. I ran our virus scan client (trendmicro client/server messaging suite*
> *officescan) and it claimed the system was clean*
>
>
> *So, some things make me think we've been hacked and some don't. I*
> *honestly don't know what to do. I kind of think we've been hacked, but*
> *it's*
> *really not terribly obvious so I'm not completely sure.*

Re: Exchange Server may be hacked...Please help.