

Re: Ok, strange thing

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.admin/2004-02/0024.html>

From: Lanwench [MVP – Exchange] (lanwench_at_heybuddy.donotsendme.unsolicitedmail.atyahoo.com)

Date: 02/04/04

Date: Wed, 4 Feb 2004 09:26:27 -0500

What AV software are you using for Exchange, your server's file system, your workstations? Do you allow non-Exchange e-mail into your network anywhere? Anyone allowed to relay, even via authenticated relay?

Vassilis Contogeorgos wrote:

> guys,
>
> i know that the virus spoofs the sender but i think that you miss the
> point. I don't get NDRs from other domains saying that i send an
> email with a virus. I get an NDR from MY administrator box of
> exchange with the virus as an attachment. Their is no trace of SMTP
> connection whatsoever. Here is an example:
>
> our message did not reach some or all of the intended recipients.
>
> Subject: Error
> Sent: 3/2/2004 13:27
>
> The following recipient(s) could not be reached:
>
> george@otherdomain.com on 3/2/2004 13:25
> The e-mail account does not exist at the organization this
> message was sent to. Check the e-mail address, or contact the
> recipient directly to find out the correct address.
> < aserver.dot #5.1.1 SMTP; 550-machine (server.dot) [an
> ip] is currently not permitted to relay>
>
> I have a few of this NDRs with different erros, no user found, no host
> found, wrong mailbox etc.
>
>
>
> "Vassilis Contogeorgos" <vcon@hate_spam_hol.gr> wrote in message
> news:#Sv#LOj6DHA.3008@TK2MSFTNGP09.phx.gbl...
>> Here is the issue.
>>
>> Since the Mydoom.A virus, a few users are starting to get reports

microsoft.public.exchange2000.admin: Re: Ok, strange thing

>> *from the exchange administrator (the local NDRs) saying that error*
>> *in transmission, no host found, unable to relay etc etc. All this*
>> *NDRs comes with attachement! the attachement contains the actual*
>> *virus which my AV software deletes the attachement. The strange thing*
>> *is that it seems to come from my actual exchange (the icon of the*
>> *message in outlook has the normal NDR icon (the red one) and there*
>> *is no SMTP trace from the options to view a header. There is no way*
>> *that the server has the virus or that any other computer in my*
>> *network has the virus.*
>>
>> *Is this some variant that tricks the user to think that it came from*
>> *the server itself ?*
>>
>> *I'm not an open relay.*
>>
>> *Anyone has this symptom ?*
>>
>> *Thank you,*