

Re: Relaying nightmare

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.transport/2004-12/0077.html>

From: Jeff Thibodeau [MS] (jeffthi_at_online.microsoft.com)

Date: 12/30/04

Date: Thu, 30 Dec 2004 16:00:44 GMT

I was not able to relay from that server so it sounds like someone is authenticating and relaying.

Determine Whether an Authenticated User is Relaying

Enables logging in the Windows Event Viewer such that any authentication attempts against the SMTP service (successful or failures) are logged in the application log.

1. Start Exchange Administrator.
2. Double-click "Servers".
3. Under "Servers", right-click <ServerName>, and then click "Properties".
4. Click the "Diagnostic Logging" tab.
5. Click "MSExchangeTransport" on the left.
6. On the right, click "SMTP Protocol".
7. Under "Logging Level", click "Maximum".
8. Click "OK" to close "Server Properties".

Check the application log to see what accounts are being authenticated. Then disable or change the password for that account.

Jeff Thibodeau
Microsoft

--

Get Secure! - www.microsoft.com/security

--

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.

--

This posting is provided "AS IS" with no warranties, and confers no rights.

=====

From: "GAZ" <contact@asd-bl.com>

Subject: Re: Relaying nightmare

Date: Wed, 29 Dec 2004 15:11:55 +0100

Yes, that's the only domain, and the mail server is mail.asd-bl.com (at least for the internet).

And I wish that relaying would be impossible, however here is a part of the smtp log showing what is actually happening. I just haven't got a single idea how to stop this.

2004-12-29 00:57:36 218.150.8.199 w8jqtmrrhlbf721 SMTPSVC1 PARTHENON

Re: Relaying nightmare

microsoft.public.exchange2000.transport: Re: Relaying nightmare

```
10.0.0.16 0 HELO - +w8jqtmrrhlbf72l 250 0 61 20 2293 SMTP - - - -
2004-12-29 00:57:36 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 MAIL - +From:+t183003@atmail.com 250 0 43 29 0 SMTP - - - -
2004-12-29 00:57:36 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 RCPT - +To:+koccip@hanmail.net 550 0 50 27 0 SMTP - - - -
2004-12-29 00:57:37 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 QUIT - w8jqtmrrhlbf72l 240 3756 50 27 371 SMTP - - - -
2004-12-29 02:11:32 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 HELO - +w8jqtmrrhlbf72l 250 0 61 20 2283 SMTP - - - -
2004-12-29 02:11:32 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 MAIL - +From:+h503373@com.ne.kr 250 0 42 28 0 SMTP - - - -
2004-12-29 02:11:32 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 RCPT - +To:+koccip@hanmail.net 550 0 50 27 0 SMTP - - - -
2004-12-29 02:11:33 218.150.8.199 w8jqtmrrhlbf72l SMTPSVC1 PARTHENON
10.0.0.16 0 QUIT - w8jqtmrrhlbf72l 240 3806 50 27 351 SMTP - - - -
Unfortunate as it is, this actually goes through. Would appreciate any help.
Thanks.
```

GAZ

"Jeff Thibodeau [MS]" <jeffthi@online.microsoft.com> wrote in message news:%23YbrJWT7EHA.2600@cpmsftngxa10.phx.gbl...

```
> Is asd-bl.com the correct domain for the mail server with the relaying
> issue?
> I did some testing to the Exchange server hosting this domain and I was
> not
> able to relay anything. Relaying Denied
>
>
> Jeff Thibodeau
> Microsoft
> --
> Get Secure! - www.microsoft.com/security
> --
> When responding to posts, please "Reply to Group" via your newsreader so
> that others may learn and benefit from your issue.
> --
> This posting is provided "AS IS" with no warranties, and confers no
> rights.
> =====
>
> -----
> From: "GAZ" <contact@asd-bl.com>
> Subject: Re: Relaying nightmare
> Date: Tue, 28 Dec 2004 16:14:42 +0100
>
> God, I wish it was SPAM. Unfortunately, it is relaying. When I said all
> over
> the shop I actually ment from a whole range of IP addresses. Sorry, I do
> get
> carried off sometimes.
>
> We have an anti- SPAM module from BitDefender and it works great, but
> realying is another issue. So far we are blocking ranges of IP addresses
> that used for relaying, but little buggers just change the IP address and
> the next morning come another full SMTP log.
>
> Is there a way in Exchange 2000 (or Ex2K3 as we are soon changing) to
> actually prevent relaying and allow only e-mails addressed to our domain
> to
> enter the system?
>
> Thanks,
```

microsoft.public.exchange2000.transport: Re: Relaying nightmare

> GAZ
>
>
>
> "Rich Matheisen [MVP]" <richnews@rmcons.com.NOSPAM.COM> wrote in message
> news:pvh0t0doc7o7pr077mk88aiq2ioslrurb@4ax.com...
>> "GAZ" <contact@asd-bl.com> wrote:
>>
>>>I would be most grateful if you could help me with a 'small' relaying
>>>problem.
>>>
>>>We have the Exchange 2000 enterprise server with the SMTP virtual server
>>>behind the ISA 2000 firewall.
>>>
>>>Basically, several days ago we 'started' relaying messages all over the
>>>shop. The Relay tab is set to 'Only listed below' with nothing in the
>>>list
>>>and the 'Allow all computers...' is unchecked. However, spam still passes
>>>through.
>>
>> Spam and relaying are not the same problem. "All over the shop" sounds
>> like the problem is spam and no relaying.
>>
>>>We started putting whole ranges of IP address in the banned list on
>>>the connection tab. The problem is that the spammers change ip addresses
>>>constantly and we have to extend the list almost on a daily basis. Never
>>>mind the bandwidth gone to waste, but we definitely do not want to end up
>>>on
>>>a black list.
>>
>> If you need a quick fix, one that relies only on DNS RBL's and limited
>> checking on the message body, try Open Relay Filter fro Vamsoft
>> (<http://www.vamsoft.com/orf>). Other inexpensive software might be GFI.
>> More expensive software is available, as are e-mail appliances that
>> are much more capable of dealing with SMTP and the Internet than
>> Exchange will ever be.
>>
>>>Is there a one time 'kill all' solution that would prevent spammers from
>>>using our server?
>>
>> If you find one, the world will be eternally grateful.
>>
>> --
>> Rich Matheisen
>> MCSE+I, Exchange MVP
>> MS Exchange FAQ at http://www.swinc.com/resource/exch_faq.htm
>
>
>