

Re: Help! Being Used As A Relay

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2004-09/0787.html>

From: Deji Akomolafe (*deji_at_REMOVEPADDINGakomolafedotcom*)

Date: 09/06/04

Date: Sun, 5 Sep 2004 20:08:29 -0700

One of the documented vectors for this type of attack/abuse is the use of the Guest account. Make sure that your Guest account is disabled.

Make sure there are not "soft" passwords. This is easier said than done, but you've seen one of the reasons to adhere to this mantra.

Make sure that your servers remain patched all the time. Follow normal security practices.

Having said all that, I have to point out that much of what you can do actually depends on WHICH account was actually being misused. If the account is your administrator's account, there is no telling what other thing the spammer may have done in the meantime besides using you for SPAM. IF I were the SPAMmer and I had admin access to the server, I would have made preparation for the day I would be discovered. This would very likely be along the lines of creating more dummy accounts that could still be used for authentication. Installing malwares on the server that could enable me to get back into the server and undo whatever you have done. Running scripts/tasks that can auto-create as many accounts as I want any time I want them and add them to any group I desire.

I am not trying to make you paranoid, I'm just saying your mile may vary when it comes to telling you how to recover from this.

Oh, remove Relay completely. It's hard to accept, but even allowing relay from authenticated users/computers is something I don't recommend. As I mentioned in my previous response to you, IF the localpart (@domainname.whatever) of an email matches either the SENDER or RECIPIENT address that exists in your org, your Exchange will deliver the mail. Allowing relay is only supposed to be used in special limited cases, and I like to think that if you have a case that falls into this category, you'd know. Disable it anyways and see what breaks :)

--

Sincerely,
Dèjì Akómóláfé, MCSE MCSA MCP+I
Microsoft MVP - Directory Services
www.readymaids.com - COMPLETE SPAM Protection

microsoft.public.exchange.admin: Re: Help! Being Used As A Relay

www.akomolafe.com

Do you now realize that Today is the Tomorrow you were worried about
Yesterday? -anon

<anonymous@discussions.microsoft.com> wrote in message
news:66e401c493aa\$89105990\$a501280a@phx.gbl...

I can and I can't believe it. I know of a couple of soft
passwords and I bet that they're the ones that got us into
this mess. I appreciate all of your hard work in helping
me. So, once I get the password issues resolved, from
what I've supplied to you from the log, do you think that
my problems will be solved? After I've changed ALL the
passwords, is there anything else I should do?

Thanks

Gerry

>-----Original Message-----

>Sorry. Had to take a break :)

>

>Quite an interesting thing you have in that list. To
answer the original

>question, you are NOT open relay. However, I think you
have a problem worse

>that Open Relay. It appears that you are the target of
direct spam-relay

>exploit. This is where a spammer gets hold of an account
on your SMTP server

>and uses that account to supply authentication
credentials to your SMTP

>server and therefore use it to relay his/her spam. For
all intent and

>purposes, YOU are the one sending the SPAM now and you
could be subject to

>blocking/RBL.

>

>You need to have your users change their passwords nad
you need to change

>the passwords on all the service/admin accounts you have
in your domain. I

>don't mean to scare you, but it appears to me that you
have more issues now

>than relay.

>

>I have been known to be wrong before, so someone else may
come around

>shortly and shoot this theory down with more reasonable
explanations.

>

>--

>Sincerely,

>

>Dèjì Akómóláfé, MCSE MCSA MCP+I

>Microsoft MVP - Directory Services

>www.readymaids.com - COMPLETE SPAM Protection

>www.akomolafe.com

>Do you now realize that Today is the Tomorrow you were
worried about

>Yesterday? -anon

>

>

><anonymous@discussions.microsoft.com> wrote in message
>news:67d901c4939e\$25151130\$a301280a@phx.gbl...

>Hi Deji,

>

Re: Help! Being Used As A Relay

microsoft.public.exchange.admin: Re: Help! Being Used As A Relay

> I've posted the info you've requested in an earlier
>post. Just thought you should know.
>
>Thanks
>Gerry
>
>>-----Original Message-----
>>I should clarify something here:
>>"You mention that Open Relay occurs when my Exchange
>server accepts emails
>>where NEITHER the SENDER nor the RECIPIENT is verified to
>belong to my
>>domain."
>>
>>That is not completely correct. Even though your server
>should NOT accept
>>mails where neither the SENDER nor the RECIPIENT "domain"
>is LOCAL to your
>>exchange org, merely doing so does not constitute an Open
>Relay. IF your
>>server then proceeds to send that mail to the non-local
>address, then it is
>>decidedly an open relay.
>>
>>We will be able to tell you definitely when we see what
>you are looking at.
>>
>>--
>>Sincerely,
>>
>>Dèjì Akómóláfé, MCSE MCSA MCP+I
>>Microsoft MVP - Directory Services
>>www.readymaids.com - COMPLETE SPAM Protection
>>www.akomolafe.com
>>Do you now realize that Today is the Tomorrow you were
>worried about
>>Yesterday? -anon
>>
>>
>><anonymous@discussions.microsoft.com> wrote in message
>>news:64aa01c49314\$ca933310\$a301280a@phx.gbl...
>>Hi Deji,
>>
>> I can't thank you enough for that great explanation.
>>There is, however, a couple of things that I am having a
>>hard time understanding. You mention that Open Relay
>>occurs when my Exchange server accepts emails where
>>NEITHER the SENDER nor the RECIPIENT is verified to
belong
>>to my domain. When I check the "SMTP Protocol Log", that
>>is what I am seeing....an unknown sender AND an unknown
>>recipient NOT on my domain. Most messages get transfered
>>out of my server, while some get the "Relaying is
>>Prohibited" message. In fact, it is very rare that I see
>>a SPAM addressed to my domain. This is where I get
>>confused. Am I missing your point? Maybe I am....I have
>>been dealing with this for the last 48 hours and my mind
>>has turned to mush. Can you please help explain this, I
>>feel that with your help, I may be able to finally get
>>this thing resolved. Thanks once again for all of your
>>time and your great explanation.
>>

microsoft.public.exchange.admin: Re: Help! Being Used As A Relay

>>Sincerely,
>>Gerry
>>>-----Original Message-----
>>>Most SMTP server implementations are RELAY servers.
There
>>is more to this,
>>>but I don't think this is useful for this discussion.
>>>
>>>I mentioned that just so that you can understand that
>>there is a difference
>>>between being a relay and being an OPEN relay.
>>>
>>>Your Exchange server will accept mails FROM anyone FOR
>>any user in the
>>>domain for which it is responsible. Before Exchange
2003,
>>there's no
>>>built-in mechanism for Exchange to check and verify that
>>the address exists
>>>in your domain. All that is needed for your Exchange to
>>accept the mails is
>>>for the TO address to end in @yourdomain.whatever
>>>
>>>Also, your Exchange will accept mails FROM your users
FOR
>>anyone in the
>>>world by default. All that is needed is for the Exchange
>>server to verify
>>>that the message is actually being sent by a legitimate
>>(authenticated) user
>>>within your domain. IF this verification is done,
>>exchange will attempt to
>>>deliver the message.
>>>
>>>OPEN relay comes into play where NEITHER the SENDER nor
>>the RECIPIENT is
>>>verified to belong to your domain. IF I (deji@nowhere)
>>send an email THROUGH
>>>your exchange server (e.g. by telnetting to port 25 on
>>your server) to
>>>foo@foobar and foobar is not a local domain on your
>>exchange server, an OPEN
>>>RELAY situation will occur IF your Exchange server
>>delivers that message to
>>>foo@foobar.
>>>
>>>There is a long-standing and unresolved argument as to
>>where the Open Relay
>>>actually occurs. Some people argue that, just by
>>accepting the mail in the
>>>first place, you are consider open relay. Some RBL
>>operators will block your
>>>server for this. Others argue that a relay race (as in
>>Tracks and Fields)
>>>does not take place until one runner has handed of the
>>baton to the next
>>>runner nad that race is not complete until the last
>>runner has crossed the
>>>finish line WITH THE baton in hand. So, even if your
>>server accepts the
>>>mail, unless and until you sent it onwards to the non-
>>local final recipient,

microsoft.public.exchange.admin: Re: Help! Being Used As A Relay

>>>you can't be judged an Open Relay.
>>>
>>>Some MTAs were actually written to accept everything
sent
>>to them and then
>>>silently drop whatever is not local.
>>>
>>>Have I digressed?
>>>
>>>Anyways, in your situation, the fact that you got an
>>affirmative "550
>>>Relaying Prohibited" is proof that you are not Open
>>Relay. The problem you
>>>are experiencing is that spammers sent emails to
randomly
>>generated SMTP
>>>addresses ending in @yourdomainname. The mails got to
>>your Exchange server
>>>and your server saw the @yourdomainname part and happily
>>accepted them - as
>>>it is designed to do. If you had been using Exchange
2003
>>AND had enabled
>>>Recipient Filtering, your Exchange would have accepted
>>ONLY the SPAMs that
>>>were addressed to SMTP addresses that ACTUALLY exist in
>>your organization. I
>>>digress again.
>>>
>>>Now that your exchange had accepted all these mails, it
>>has to do something
>>>with them. It tries to deliver them and found out that
>>those addresses do
>>>not exist. So, now it has to return an NDR to the
>>original sender (or
>>>purported sender) of the undeliverable mails.
>>Unfortunately for you (and
>>>your Exchange server), the SPAMMER had forged the sender
>>address. To make
>>>matters worse, the spammer may have forged an address
>>that does not exist at
>>>another domain as the sender. So, your Exchange sends an
>>NDR to a
>>>non-existent address at wigglewaggle.whatever. The SMTP
>>server at
>>>wigglewaggle.whatever then replies back to your Exchange
>>server that that
>>>address does not exist, etc, etc.
>>>
>>>Now, the moral of the above story? Upgrade to Exchange
>>2003 or get a proven
>>>effective Anti-SPAM solution (hint.... hint). For a
>>really good
>>>solution get both. If you can't do both my Anti-SPAM
>>solution is cheaper
>>>than E2K3 license fee and way better than Exchange IMF.
>>>
>>>--
>>>Sincerely,
>>>
>>>Dèjì Akómóláfé, MCSE MCSA MCP+I
>>>Microsoft MVP - Directory Services

microsoft.public.exchange.admin: Re: Help! Being Used As A Relay

>>>www.readymaids.com - COMPLETE SPAM Protection
>>>www.akomolafe.com
>>>Do you now realize that Today is the Tomorrow you were
>>>worried about
>>>Yesterday? -anon
>>>
>>>
>>><anonymous@discussions.microsoft.com> wrote in message
>>>news:01e201c492e2\$b73fc350\$a401280a@phx.gbl...
>>>Hi Deji,
>>>
>>> Thank you for your reply. Excuse my ignorance, but
>>>why would my server accept the mail and try to deliver
>>>it? Is this not what relaying is? I would have thought
>>>that the SPAM would be dropped because it wants my
server
>>>to relay the mail. I noticed that some of the mail does
>>>get delivered to its intended targets while others get
>>>NDRs. Can you please explain this to me a little
better.
>>>Again, sorry for my ignorance and I appreciate all the
>>>help I've been receiving on this.
>>>
>>>Sincerely,
>>>Gerry
>>>
>>>-----Original Message-----
>>>>You are confusing SPAM attack with open relay. Someone
>is
>>>blasting SPAM into
>>>>your server, your server accepts the mails but can't
>>>deliver it, then your
>>>>server tries to return them (NDR) but can't either
>>>because the source
>>>>addresses are spoofed.
>>>>
>>>>This is where you need an Anti-SPAM filter like mine.
>>>>
>>>>--
>>>>Sincerely,
>>>>
>>>>Dèjì Akómöláfé, MCSE MCSA MCP+I
>>>>Microsoft MVP - Directory Services
>>>>www.readymaids.com - COMPLETE SPAM Protection
>>>>www.akomolafe.com
>>>>Do you now realize that Today is the Tomorrow you were
>>>>worried about
>>>>Yesterday? -anon
>>>>
>>>>
>>>><anonymous@discussions.microsoft.com> wrote in message
>>>>news:601601c4929f\$c8d8e710\$a601280a@phx.gbl...
>>>>
>>>>>-----Original Message-----
>>>>> >
>>>>> >"Gerry" <anonymous@discussions.microsoft.com> wrote
>in
>>>>> message
>>>>> >news:600b01c4929a\$8260b010\$a501280a@phx.gbl...
>>>>> >>I am running Exchange 5.5 and I've noticed that I
>>>>>have a
>>>>> >> ton of mail messages in my IMS Queue waiting to be

microsoft.public.exchange.admin: Re: Help! Being Used As A Relay

```
>>>> >> delivered. They are all unknown senders and
>>>recipients.
>>>> >> I've followed Microsoft's instructions to prohibit
>>>> >> relaying, but I still get messages coming through.
>>>> When I
>>>> >> telnet my server and type in RCPT TO: xx@xx.xx I
>>>> get "550
>>>> >> Relaying Prohibited". When I check
the "Diagnostic
>>>> >> Logging" file created by the "SMTP Protocol Log",
I
>>>can
>>>> >> see the RCPT TO: xx@xx.xx and it is followed
>>>with "350
>>>> Go
>>>> >> Ahead". I would have thought to see "Relaying
>>>> >> Prohibited". Any help would greatly be
>appreciated.
>>>> >
>>>> >Why don't you delete them from the queue?
>>>> >
>>>> >
>>>> >.
>>>> >I have deleted them from the queue. Once I re-
enable
>>>the
>>>> IMS Service, the messages start piling up again.
>>>>
>>>> Thanks,
>>>> Gerry
>>>>
>>>>
>>>>.
>>>>
>>>
>>>
>>>.
>>>
>>
>>
>>.
>>
>
>
>.
>
```