

Re: Followup to reject: spam site

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-09/msg00579.html>

- *From:* ngan <ngan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 6 Sep 2006 15:04:01 -0700
-

FYI: For #1, there is nothing listed in the Connection Filter tab in the Message Delivery properties

"ngan" wrote:

Hope the answers below help.

1. I don't know. Where can I find out if there are any RBLs?
3. We only have they Symantec anti-spam and I have disabled it.
2. Our MX records are housed with an ISP. If you do a MX record search for asila.org, you get the following. So it would go to horizonsite.com and see that the mail.asila.org is at 38.118.210.9 (our exchange server).

Searching for asila.org MX record at m.root-servers.net [202.12.27.33]: Got referral to TLD6.ULTRADNS.CO.UK. (zone: org.) [took 84 ms]
Searching for asila.org MX record at TLD6.ULTRADNS.CO.UK. [198.133.199.11]: Got referral to NS2.HORIZONSITE.COM. (zone: ASILA.ORG.) [took 6 ms]
Searching for asila.org MX record at NS2.HORIZONSITE.COM. [63.228.179.141]: Timed out. Trying again.
Searching for asila.org MX record at NS2.HORIZONSITE.COM. [63.228.179.141]: Timed out. Trying again.
Searching for asila.org MX record at NS2.HORIZONSITE.COM. [63.228.179.141]: Timed out. Trying again.
Searching for asila.org MX record at NS1.HORIZONSITE.COM. [209.161.21.3]: Reports mail.asila.org. [took 75 ms]

Answer:

```
Domain Type Class TTL Answer
asila.org. MX IN 10800 mail.asila.org. [Preference = 10]
asila.org. MX IN 10800 mail2.asila.org. [Preference = 20]
asila.org. NS IN 10800 ns2.horizonsite.com.
asila.org. NS IN 10800 ns1.horizonsite.com.
mail.asila.org. A IN 10800 38.118.210.9
ns1.horizonsite.com. A IN 10800 209.161.21.3
```

Re: Followup to reject: spam site

ns2.horizonsite.com. A IN 10800 63.228.179.141

"Ben Winzenz [Exchange MVP]" wrote:

IMF doesn't reject messages. It either marks them as spam, or quarantines or deletes them, but it doesn't reject them. your permissions issues are also not likely to be causing this problem.

You need to look at:

- 1) do you have Exchange configured to use any RBL's?
- 2) is Exchange your first point of entry for e-mail?
- 3) do you have any other anti-spam products installed?

Answer those questions and you should be in a better place to figure out the cause.

--

Ben Winzenz
Exchange MVP
MessageOne
Read my blog!
<http://winzenz.blogspot.com>
<http://feeds.feedburner.com/winzenz> (RSS Feed)

"ngan" <ngan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:7A6E74E3-968E-4770-8165-7A37FB2F02F5@xxxxxxxxxxxxxxxxxxxx>

Summary: We have exchange 2003 sp2

Since last Tuesday, alot of emails sent to our organization are being rejected with the error message:

38.118.210.9 does not like recipient.
Remote host said: 550 5.2.1 Mail from 68.142.199.118
refused: spam site.
Giving up on 38.118.210.9.

Before Tuesday, we never had emails be rejected for the above reason. I have already turned off the symantec heurastic (sp?) spam detection. I changed the IMF to SCL > 9 and no action.

I just did all the MS updates so the IMF has the latest updates.

We are still rejecting emails.

Re: Followup to reject: spam site

funny thing: Company A could email us back and forth in the morning (4–5 emails) and then all of a sudden, Company A would get a rejection message and can not email us again, unless we whitelist their IP.

this has happened to a few domains in the past week.

What can I look into to see what is causing these rejections?

About the ExBPA, I do have that tool, ran the reports and received these critical issues:

Permission:

Permissions inheritance block on Exchange server object:
Access control list inheritance is blocked for the exchange server object (CN=sextus, CN=servers,CN=first Admin group, cn=admin groups, cn=access services, cn=MS exchange, cn=services,cn=configuration,dc=tower,dc=as)

Health:

Permissions inheritance block on Exchange server object
Volume shadow copy service update available

Can you explain the two issues? I read the details of the permissions issue and didn't understand what I needed to do.