

Re: Anyone successfully stopped Reverse NDR Attacks in exchange 2000?

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.admin/2006-02/msg00065.html>

- *From:* "John Oliver, Jr. [MVP]" <jcoliverjr@xxxxxxxxxxx>
 - *Date:* Tue, 7 Feb 2006 16:15:41 -0500
-

I have been recommending to outsource the Antispam controls. I prefer either Spam Soap, www.spamsoap.com or Postini at www.postini.com. Basically, you end up changing your MX Record to point to their filtering servers and the Spam stops filling your Exchange Queues with Reverse DNS Attacks, Dictionary Attacks, etc. Spam Soap seems to have the best price per mailbox and is very effective.

—

John Oliver, Jr
MCSE, MCT, CCNA
Exchange MVP 2006
Microsoft Certified Partner

<pdarisse@xxxxxxxx> wrote in message
news:1139339597.259670.266420@xx

What it is :
imagine a spammer that want to spam 123@xxxxxxx The spammer connects to your SMTP server, sends a spam mail claiming to be from 123@xxxxxxx and destined to an non existing address on your server. What happens then is that the server can't deliver, since the address doesn't exist so it issues a NDR(non delivery response) to the sender(123@xxxxxxx) and joins the original(spam) message to this NDR. Basically, the spammer got to send an email to his victim, even if your server is not configured as an open relay.

Symptoms :
Way more SMTP queues than usual
Many queues are in retry state
The content of these queues all come from postmaster
Outgoing mail takes time to reach destination

I originally wrote a post in this group for a problem that ended in me discovering that the root of my problem was a Reverse NDR attack(about 3600 per day). So, since the original post is way down and that the subject is not accurate, I judged it would be better to start a new thread, since it seems a lot of people deal with this problem

Re: Anyone successfully stopped Reverse NDR Attacks in exchange 2000?

(knowingly or unknowingly)

So here is my basic question :

Can I block this kind of attacks without losing the genuine mail in the process?

I found a couple of solution, but I didnt find out that let me keep the genuinely lost mails :

1-I can stop all NDR from being delivered (Global settings-->Internet Messages Format-->Advance tab-->NDR) but this means that if someone made a spelling error for my name, I will not receive it, nor will the sender know. To counter this, I send myself a copy of the NDR(SMTP Virtual Server-->Properties-->Send Copy Of NDR To). Still, I dont get a copy of the original message. I tried to forward all mail send to an unresolved address but wasn't able to do it(found several places that said you couldn't do it out of the box)

2-Exchange 2003 has a feature that can be used to do this. You can reject all mail destined to unresolved users, which leaves the burden of sending the bounce notice to the sending server, which any legit server will do. Sadly this feature is not available in exchange 2000.

3-I could block the spam senders at the firewall or via "SMTP Virtual Server-->properties-->Access-->Connection", but after I killed 2 addresses that were always connected, there seems to be as much connecting addresses as there are spam sent. I figure there are many zombie machines out there that are used for this particular purpose so that I have no chance of banning them all.

4-I could refuse connections from servers whose PTR resolution differs from the ip being connected from(SMTP Virtual Server-->properties-->Delivery-->Advanced-->Perform Reverse DNS Lookup on incoming...), but I fear I might refuse minor servers that are OK but don't know the PTR thing (I just learned it myself, resolving this issue) and moreover, most zombie DSL and Cable line have a correct IP vs PTR Resolve match so that all zombie botnets would continue to pound my server

As you can see, all of these methods have their drawbacks. I'm trying to find a solutions that would work on our system. I'm actually forced into doing number 1 because if let the NDRs out again, my server can not keep with the pace of emails to send, with our limited bandwidth.

As I see it, the second solution is the best one for our problem but we have exchange 2000 and dont want to upgrade right now.

So, anyone has had this particular problem? How did you manage to solve it? Do you know of any fixes that microsoft might have released that would add the exchange 2003 feature I want to exchange 2000?

Re: Anyone succesfully stopped Reverse NDR Attacks in exchange 2000?

Many thanks to all

Pierre Darisse