Subject: Antivirus Filtering
Posted by mhcomp on Tue, 15 Jan 2008 20:24:33 GMT
View Forum Message <> Reply to Message

We have our NoSpamToday for Servers set to reject/redirect to a Spam account within Exchange 2003. This account is then checked by someone from a Workstation. Somehow viruses are getting past the Antivirus check the NoSpamToday should be doing causing much concern on the Workstation when her antivirus program scans the email and finds a virus!!!

What could be the problem. I have checked everything and even sent the eicar test string which got deleted by NoSpamToday is instructed to do so. I have got the latest version installed 3.0.5.1

Subject: Re: Antivirus Filtering
Posted by support on Wed, 16 Jan 2008 17:48:21 GMT
View Forum Message <> Reply to Message

Virus checkers in NST are configured to scan messages only, so if you just reject/redirect the message, it will be forwarded to the spam account with the virus still intact.

If you have a virus checker that supports an option to sanitize messages, you can experiment with the AV filter settings, but it is probably much simpler to just reject/delete virus messages.

False positives with virus filters are far less common than with spam filters.

Subject: Re: Antivirus Filtering
Posted by mhcomp on Tue, 22 Jan 2008 01:49:09 GMT
View Forum Message <> Reply to Message

I think you may of misunderstood.

To clarify, Antivirus checking in NST is indeed set to reject/delete. If an incoming message gets marked as Spam by the DNSBL filter which is set to reject/redirect surely the Antivirus should still check the message for viruses before redirecting it to the Spam account.

Subject: Re: Antivirus Filtering
Posted by support on Wed, 23 Jan 2008 13:51:26 GMT
View Forum Message <> Reply to Message

OK, I see your point, and you're right, this is not expected behaviour.

Please send your noSPAMtoday.cf file to nstsupport@byteplant.com so we can have a look at what's going on. Please add examples of this thing happening (ie. log file snippets), OS version

information, and NoSpamToday! version information.

Subject: Re: Antivirus Filtering
Posted by mhcomp on Thu, 24 Jan 2008 10:43:38 GMT
View Forum Message <> Reply to Message

Unfortunately the lady who handles the Spam only clears them every few days. The log file for NST only goes back to the previous day and I therefore can't get my hands on it.

Is there any way of extending the number of old log files that NST keeps to say 5 instead of 1 ?

Subject: Re: Antivirus Filtering
Posted by support on Fri, 25 Jan 2008 10:40:46 GMT
View Forum Message <> Reply to Message

mhcomp wrote:

> Unfortunately the lady who handles the Spam only clears them
> every few days. The log file for NST only goes back to the
> previous day and I therefore can't get my hands on it.
>
> Is there any way of extending the number of old log files that
> NST keeps to say 5 instead of 1 ?

You can use the task scheduler to rename log files, or change the logging settings so that a log file lasts more than one day.

Subject: Re: Antivirus Filtering
Posted by mhcomp on Tue, 06 May 2008 20:26:19 GMT
View Forum Message <> Reply to Message

My apologies for not getting back to you before.

Another customer of mine has had a similar occurance where the email marked as Spam by SpamAssassin has not been virus checked until it reached the clients Microsoft Outlook program where it was duly Quarantined.

I noted this time that the email had an attachment which was another email. That attached email contained an attachment which was an executable (exe) which was a trojan.

The antivirus on the SBS Server 2003 is Nod32 and appears not to be checking deep enough into the message.

Is there a way to change just how deep the antivirus scanner checks ?

Subject: Re: Antivirus Filtering
Posted by support on Wed, 07 May 2008 09:25:05 GMT
View Forum Message <> Reply to Message

> Another customer of mine has had a similar occurance where the
> email marked as Spam by SpamAssassin has not been virus checked
> until it reached the clients Microsoft Outlook program where it
> was duly Quarantined.
>
> I noted this time that the email had an attachment which was
> another email. That attached email contained an attachment
> which was an executable (exe) which was a trojan.
>
> The antivirus on the SBS Server 2003 is Nod32 and appears not
> to be checking deep enough into the message.
>
> Is there a way to change just how deep the antivirus scanner
> checks ?

Please check the manuals of your antivirus software to find out more about the scanning options.