

---

Subject: inconsistent header info

Posted by [tiger1vic](#) on Thu, 04 Nov 2004 15:33:56 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

I just upgraded yesterday to NSTfree v2.0.1.1 and since then my spam checking is barely working. I say 'barely' because most of the emails coming through now have no X-Spam header info at all, so at first I thought it wasn't checking at all. However, the headers do contain the "received by NST fw v2.0.1.1...." tags. Last night a handful of spams WERE flagged and DID contain the X-Spam header info (?) while most of the others still did not. It doesn't appear to be a case of messages simply not scoring high enough, because the complete lack of X-Spam info seems to indicate there is no spamassassin checking at all. Needless to say, my spam filtering is hosed and I am now being flooded with spam in my inbox again, after "enjoying" a relatively low amount for quite some time, thanks to NST.

The headers also indicate that SA v3.0 is being used, while there is a new bugfix release of SA (v3.0.1) that came out on Oct 22nd. I just downloaded NST yesterday (Nov 3rd) - does anyone know if this is incorporated into the new NST already?

As for the problem I'm having, if anyone can suggest what may be at fault, I would really appreciate it. I am using free version NST on a win2k/exchange server with 10 specific email addresses being checked, and it always worked with the earlier version. I installed NST over top of the v1.2.5.2 as suggested by the upgrade docs. All of the config looks ok. The logs at first showed the license quota being exceeded but I think I figured that one out. The addition of the new filter chain with the ability to check for viruses first, seems to have caused that. I had 10 addresses specified in the SA filter but nothing in the earlier virus (attachment) filter. By putting my addresses in the first filter and then choosing "use previous filter" in the SA filter settings, this seems to have resolved the license overrun. But no change to the original problem -- H..E..L..P..!!

---

---

Subject: Re: inconsistent header info

Posted by [support](#) on Fri, 05 Nov 2004 13:01:16 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Check the log of NoSpamToday!. The new version prints much more interesting info to the log, and maybe you will find a hint what happens in the log.

Be sure to enable extended logging (this prints subject, to and from headers to the log, and also the spam score). Also you should enable detailed logging, until your problem is resolved.

---

---

Subject: Re: inconsistent header info

Posted by [tiger1vic](#) on Fri, 05 Nov 2004 18:40:43 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Let me preface this post by saying that I think it's great that you take time to at least once a day

answer these posts. I realize this is the free version and is not technically entitled to support, but finding answers here will help all paid and free users. And just for the record, I've been using the free version for awhile on my own small mail server, but I've recommended the paid version to many clients since I began using it. I've seen several of my earlier suggestions incorporated into the software as it has developed and it seems to be maturing nicely. So, thanks for a great product!

-----  
Now for my continuing saga...

I turned on all logging this morning and let it run for awhile like that. Apart from bogging down the server, it really didn't do much for me, so I turned it off again after I thought I had obtained a large enough sample. There's lots of detail all right and I can certainly see the spammers at work, but nothing that I can see which might indicate a problem with SA or NST. I can email you the log if you like.

The log shows 125 accepted connections in that short time, but only 7 instances where it said "executing spamassassin".

I don't know if this is really what's happening, but it almost seems like the messages that are undetected spam are most often the ones missing the X-Spam-status etc. Thus far this morning, all legitimate messages seem to contain the X-Spam-status. How can that be? Or is it just coincidence?

FYI, here is a small snippet of the log (domain names have been changed to protect the innocent). This session contained lots of "suspect" smtp commands and it did execute SA as far as I can tell, but most sessions do not have that info.

```
Nov 5, 2004, 09:14:55 Session 0: Connection from 69.6.18.111 accepted on 192.168.1.11:25
Nov 5, 2004, 09:14:55 Session 0: 220 mail.mydomain.com Microsoft ESMTP MAIL Service,
Version: 5.0.2195.6713 ready at Fri, 5 Nov 2004 09:14:55 -0800
Nov 5, 2004, 09:14:55 Session 0: EHLO mx18111.ss03.com
Nov 5, 2004, 09:14:55 Session 0: 250-mail.mydomain.com Hello [192.168.1.11]
Nov 5, 2004, 09:14:55 Session 0: 250-TURN
Nov 5, 2004, 09:14:55 Session 0: 250-ATRN
Nov 5, 2004, 09:14:55 Session 0: 250-SIZE
Nov 5, 2004, 09:14:55 Session 0: 250-ETRN
Nov 5, 2004, 09:14:55 Session 0: 250-DSN
Nov 5, 2004, 09:14:55 Session 0: 250-ENHANCEDSTATUSCODES
Nov 5, 2004, 09:14:55 Session 0: 250-8bitmime
Nov 5, 2004, 09:14:55 Session 0: 250-VRFY
Nov 5, 2004, 09:14:55 Session 0: 250-X-EXPS GSSAPI NTLM LOGIN
Nov 5, 2004, 09:14:55 Session 0: 250-X-EXPS=LOGIN
Nov 5, 2004, 09:14:55 Session 0: 250-AUTH GSSAPI NTLM LOGIN
Nov 5, 2004, 09:14:55 Session 0: 250-AUTH=LOGIN
Nov 5, 2004, 09:14:55 Session 0: 250-X-LINK2STATE
Nov 5, 2004, 09:14:55 Session 0: 250 OK
Nov 5, 2004, 09:14:55 Session 0: MAIL From: SIZE=7824
Nov 5, 2004, 09:14:55 Session 0: 250 2.1.0
```

b.funemails2.0-44588f0-10a4.mydomain.com.-fbennett@mx18111.ss03.com....Sender OK  
Nov 5, 2004, 09:14:55 Session 0: RCPT To: NOTIFY=FAILURE  
Nov 5, 2004, 09:14:55 Session 0: 250 2.1.5 fbennett@mydomain.com  
Nov 5, 2004, 09:14:55 Session 0: DATA  
Nov 5, 2004, 09:14:55 Session 0: 354 Start mail input; end with .  
Nov 5, 2004, 09:14:55 Session 0: (Attachment Filter) From: Consumer Feedback  
Nov 5, 2004, 09:14:55 Session 0: (Attachment Filter) To: fbennett@mydomain.com  
Nov 5, 2004, 09:14:55 Session 0: (Attachment Filter) Subject: Get a Gateway Laptop Free!  
Nov 5, 2004, 09:14:55 Session 0: Received end of data, mail size 5kB  
Nov 5, 2004, 09:14:55 Session 0: (Attachment Filter) Filter result is accept/deliver  
Nov 5, 2004, 09:14:55 Session 0: (SpamAssassin) Executing: sa\spamassassin.exe -x -c  
"sa\ruleset" -e 255

By the way, I'm still wondering whether the bug fixes in the new SA (v3.0.1) have been incorporated into NST yet? Thx.

---

---

Subject: Re: inconsistent header info  
Posted by [tiger1vic](#) on Mon, 08 Nov 2004 16:20:57 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

No answers here, so uninstalled and did a clean install - same problem... still only the occasional message has X-Spam-status and other spamcheck related stuff in its header. Only one of about 200 spam messages last night was actually flagged as spam. Giving up... can't stand sorting through all the spam... going back to v1.2.5.2 now.....

---

---

Subject: Re: inconsistent header info  
Posted by [support](#) on Mon, 08 Nov 2004 17:38:40 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

As to your log snippet above, it would be interesting how the story continues. From the subject, it looks like spam. Find the next line reading

Nov 5, 2004, ... Session 0: (SpamAssassin) ...

and tell us what you see. Maybe send us the log file by mail, and for good measure your config file(nospamtoday.cf), too.

Also, as an upgrader from version 2.0, be sure to upgrade the SpamAssassin Bayes DB upon installation. This job takes a few minutes, and if you don't do it during installation, it may cause problems later.

SpamAssassin 3.0.1 did not offer any important bug fixes, and it did not address any bug we would like to have fixed, so we decided to wait a little for the next bugfix, which will probably be out soon.

---

---

Subject: Re: inconsistent header info

Posted by [tiger1vic](#) on Mon, 08 Nov 2004 21:57:39 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

I already replied to your email which you sent to me directly. With that I included the full logfile and .cf file. But for your additional info, I did upgrade the bayes db and it appeared to upgrade without problems. However, as noted in that other email and above, I've now uninstalled and reverted back to the old version until a fix can be found. Thanks for the clarification about the rev of SA.

---