
Subject: negative scores

Posted by [Chad](#) on Fri, 16 Mar 2007 16:15:44 GMT

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

It seems that my DB was corrupted as the NST stopped learning new emails and would not allow me to expire tokens. I have removed the DB to start over, relearned a variety of spam email, but all inbound scores seem to be in the negative scores...like -67.5 so I am getting a lot of spam traffic right now. Any thoughts?

Thanks in advance.

Subject: Re: negative scores

Posted by [support](#) on Fri, 16 Mar 2007 18:02:13 GMT

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

Check the X-Spam headers of the mails in question, and see which rules contributed to the score.

Negative scores that high usually are caused by whitelisting. AFAIK whitelisting has scores up to -100.0. So check your whitelist.

If this doesn't help, consider removing the auto-whitelist (the awl file in the sa\db subdirectory), though AWL scores are never that high.

Subject: Re: negative scores

Posted by [Chad](#) on Sat, 17 Mar 2007 06:13:05 GMT

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

X-Spam-Status: No, score=-70.1 required=4.0 tests=BP_STOCK_SPAM_1, EXTRA_MPART_TYPE,HTML_IMAGE_ONLY_20,HTML_MESSAGE,MY_CID_AND_ARIAL2, MY_CID_AND_CLOSING,MY_CID_AND_STYLE,MY_CID_ARIAL2_CLOSING, MY_CID_ARIAL_STYLE,RCVD_IN_BL_SPAMCOP_NET,RCVD_IN_NJABL_DUL, RCVD_IN_XBL,SARE_GIF_ATTACH,SARE_GIF_STOX,USER_IN_WHITELIST autolearn=no version=3.1.7

I did delete the Awl file....but some how it keeps getting populated ????. This is what is the problem for sure. How do I turn off the the AWL ?

Thanks again.

Subject: Re: negative scores

Posted by [support](#) on Mon, 19 Mar 2007 08:41:47 GMT

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

> X-Spam-Status: No, score=-70.1 required=4.0
> tests=BP_STOCK_SPAM_1,
> EXTRA_MPART_TYPE,HTML_IMAGE_ONLY_20,HTML_MESSAGE,MY_CID_AND_ARIAL2,
> MY_CID_AND_CLOSING,MY_CID_AND_STYLE,MY_CID_ARIAL2_CLOSING,
> MY_CID_ARIAL_STYLE,RCVD_IN_BL_SPAMCOP_NET,RCVD_IN_NJABL_DUL,
> RCVD_IN_XBL,SARE_GIF_ATTACH,SARE_GIF_STOX,USER_IN_WHITELIST
> autolearn=no version=3.1.7
>
> I did delete the Awl file....but some how it keeps getting
> populated???? This is what is the problem for sure. How do I
> turn off the the AWL ?

Obviously the sender of this email is whitelisted (USER_IN_WHITELIST, see above), so please check your whitelist.

Subject: Re: negative scores
Posted by [Cognivore](#) on Sun, 28 Oct 2007 18:05:24 GMT
[View Forum Message](#) <> [Reply to Message](#)

I have seen this behavior before also, but it's been because the return email address is the same as the recipient address. It's as though the recipient email address is automatically whitelisted as a sender address. Is this correct?

Subject: Re: negative scores
Posted by [support](#) on Tue, 30 Oct 2007 14:50:01 GMT
[View Forum Message](#) <> [Reply to Message](#)

Cognivore wrote:

> I have seen this behavior before also, but it's been because
> the return email address is the same as the recipient address.
> It's as though the recipient email address is automatically
> whitelisted as a sender address. Is this correct?

Not quite.

SpamAssassin has a feature called "auto-whitelist", which adds a bias to the overall mail score towards spam or non-spam, depending on the history of messages received earlier with the same sender address.

But as a result, spam scores may well be negative as well.

<http://wiki.apache.org/spamassassin/AutoWhitelist>

Subject: Re: negative scores

Posted by [James Wilkinson](#) on Wed, 31 Oct 2007 13:54:08 GMT

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

Note that the auto-whitelist also takes the first two bytes of the sender's IP address into consideration, which makes it very difficult for a random spammer to benefit from a known correspondent's AWL listing. (If you get an e-mail allegedly from support at byteplant, but from a completely different part of the Internet, SpamAssassin will treat it as a different sender).

As support mentioned a few posts back, this doesn't apply to manual SpamAssassin whitelist_from entries (NoSpamToday users may still have these in their configuration files if they've upgraded from version 2).

Users who configure their *own* domain in whitelist_from will see spammers taking advantage of it, which is why it's not recommended (e-mail from your own domain probably shouldn't be going through NoSpamToday at all).
