
Subject: report of Spam by email address

Posted by [clarke-pj](#) on Tue, 22 Feb 2005 10:12:56 GMT

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

We have a number of users on our domain who are part of multiple groups and some of these users are getting 3-400 spam mails a day.

I would like to be able to see which of the groups are receiving the most spam mails so that I can handle the worst offenders differently.

Is there a report available to show the number of spam mails per smtp address?
Or has anyone been able to generate a report like this from the log files?

Thanks
Peter Clarke

Subject: Re: report of Spam by email address

Posted by [themarcel](#) on Wed, 23 Feb 2005 20:48:33 GMT

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

Here is a little VB-script I wrote to Parse the log file that is generated by NOSPAMTODAY v1.2.5.2

This is for v1.2.5.2 but could easily be modified for the current version of No Spam Today.

Code is a little rough but it does the job.

<http://www.twinsburgh.com/nospamtoday/>

I then import these into MS Excel and create pivot tables to get counts for each of the three parsed logs. Sort by high count. I then add top known offenders from FROM and HELO/EHLO lists by adding them to my local.cf file.

Marcel

Subject: Re: report of Spam by email address

Posted by [clarke-pj](#) on Thu, 24 Feb 2005 10:32:41 GMT

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

Thanks for that marcel, it makes very interesting reading.

What I was actually looking for though was the number of spam per mailbox, rather than the number of mails.

However I would say that they should map pretty closely together.

Also I'm using 2.0.3.1 and it seems to work fine.

Peter

Subject: Re: report of Spam by email address

Posted by [themarcel](#) on Thu, 24 Feb 2005 17:25:36 GMT

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

"As per the spam per mail box" - I was thinking the same thing.

i.e. Who gets the most SPAM and which person in my organization is receiving it.

I just haven't had the chance to spend some time on adding the additional code.

I will repost code when I get that done.

Marcel

Subject: Re: report of Spam by email address

Posted by [Kpauley](#) on Sat, 11 Feb 2006 16:50:16 GMT

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

This code is not available anymore on that website it looks like.

I am looking for a SPAM/HAM p/user email address report. I am trying to use a SpamAssassin log parser on the nospamtoday.log file but so far I am not having much luck.

Does anyone have a reporting tool like this for NST? I'd like to be able to look at this data before I purchase so I can get my email addresses trimmed down (trying to get it to under 10).

Ken

Subject: Re: report of Spam by email address

Posted by [Heidner](#) on Sun, 12 Feb 2006 19:19:44 GMT

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

I wrote a tool that is in the NST third party contribution area.

<http://www.byteplant.com/support/nospamtoday/contrib.html>

The tool spamlogs reads the NST logfiles and builds a line that can either be read by we humans, or saved as a comma separated variable file (csv). You then import the csv file into a spreadsheet, sort by group receiving the most, the spammer sending the most, etc.

The information written for each e-mail includes (but not limited to), status (accept/reject), spam assassin score, timestamps, sender, receiver, subject, etc.

I break the report down and send a list of rejected e-mails to each recipient (small network) so they can see what was rejected. I also look at the scores and the biggest senders to decide if I want to block domains.

Subject: Re: report of Spam by email address

Posted by [RandallRash](#) on Mon, 10 Apr 2006 20:33:05 GMT

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

If I run SPAMLOGS with no options it scrolls a list of e-mail info on the screen as expected. But if I enter SPAMLOGS --csv I get "Can't open Spamlogs for reading:No such file or directory at spamlogs.pl line 64". What am I missing? Thanks for your help.

Subject: Re: report of Spam by email address

Posted by [RandallRash](#) on Mon, 10 Apr 2006 20:37:49 GMT

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

Oh, just got it: -csv=filename

Subject: Re: report of Spam by email address

Posted by [Heidner](#) on Thu, 13 Apr 2006 21:21:26 GMT

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

For some of the heavy e-mail users (or administrators) you might also just want to send an e-mail report of the rejected mails. I do that with script that looks like:

```
del dennis.txt
spamlogs.exe --file="nospamtoday.log" --rcpt=dennis --score=9 --remark="delete" --days=1 >
dennis.txt
if %errorlevel% GTR 0 e:\bork\exchange\mapisend.exe -u username -p password -r "Dennis
Heidner" -s "Deleted e-mail log" -m "Deleted e-mail log for Dennis included" -v -f "Dennis.txt"
```

mapisend was available on the MS Backoffice resource CD's. There are other ways to also send mail back into your server... that is... mapisend .exe isn't your only choice.

The spamlogs options I used were to select only e-mails that were deleted, in the last 24 hours, and had a score of 9 (your threshold might vary).

You could repeat the spamlogs extraction step multiple times -- each time it would append the info to the text file... this way you could look at email being rejected for a group of people.

Subject: Re: report of Spam by email address

Posted by [thisbejoe7](#) on Tue, 24 Oct 2006 16:09:56 GMT

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

Anyone else have problems running this? I execute the program from the command line and it creates my output csv file but its always 0kb. I don't see any output in the dos box as it runs either even without arguments. My log files are over 70MB and more lines than excel can handle. Any others having this problem?

Subject: Re: report of Spam by email address

Posted by [Heidner](#) on Sat, 28 Oct 2006 04:59:17 GMT

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

Joe, I know you got it going... we've been corresponding. But I think I will include your observation that spamlogs wants both the logfile that ends with ".log" and ".log~". Plus detailed logging must be enabled.
