Subject: SPAM, random scores - but similar emails

Posted by nickvn on Tue, 24 Oct 2006 15:03:30 GMT
View Forum Message <> Reply to Message

The only thing I can see that seems to be consistant with these emails;

---

subjects:

Very important note. You require to read.
Weighty note. You have to read.

---

gets scores anywhere from 5.4 - up

and on another note - another set of emails getting through, but I haven't found a pattern yet. The emails have GIFs attached to them similar to;

http://www.e-tek.com.au/other/annoying.gif
(I've noticed other email addresses I have, from a couple ISPs also scoring spam with similar emails of the above link)

anyone else getting emails with subjects above (and ones with the linked image) going through the filters?

I have the server threshold set to 9.2, because anything less and it rejects certain emails coming from OUTLOOK or emails with those stupid emoticons (smiley faces) in them.
Essentially, SA is relying on rules and blocking out majority of spam that comes above the 9 rating.

Subject: Re: SPAM, random scores - but similar emails

Posted by support on Wed, 25 Oct 2006 15:23:51 GMT
View Forum Message <> Reply to Message

> Very important note. You require to read.
> Weighty note. You have to read.

Yes, those mails are quite hilarious, we get plenty of them.

> I have the server threshold set to 9.2, because anything less
> and it rejects certain emails coming from OUTLOOK or emails
> with those stupid emoticons (smiley faces) in them.
> Essentially, SA is relying on rules and blocking out majority
> of spam that comes above the 9 rating.

9.2 is very cautious, we are using 4.8 on our servers. The problems with the Outlook rules have been fixed in the later versions of SpamAssassin.

Subject: Re: SPAM, random scores - but similar emails

Posted by nickvn on Wed, 25 Oct 2006 15:53:42 GMT
View Forum Message <> Reply to Message

what about incredimail? (this was the one I was thinking of, with the emoticons).

I've seen incredimail emails come in as high as 9.0

Since setting the threshold to 9.2, I've updated the server program a couple times. First update was roughly around 1/3 through this year. I was getting bad feedback from people saying emails were being denied (from 9.2, I dropped it down to 7).
When the feedback came in, I then upped it back to 9.2

I recently updated the server to V2.3.5.3 and haven't been game enough to drop it down.

Initially, when the server was freshly installed, I had it set to the default 5.0
Then I had the outlook problems. So I had to up it all the way to 8.0

Then I got incredimail problems, which resulted to setting it to 9.2

Now I have spam problems - and have now resorted to just collecting them all and getting SA to learn from them.

After having another look at the log file, I just noticed a government agency (Australian tax department - email address, legit) scoring 7.1

What do you suggest I do?

at the moment, I'm thinking just leaving it at 9.2 - collect the spam and feed it to the SA-learn program.

Subject: Re: SPAM, random scores - but similar emails

Posted by support on Thu, 26 Oct 2006 15:36:11 GMT
View Forum Message <> Reply to Message

> What do you suggest I do?
>
> at the moment, I'm thinking just leaving it at 9.2 - collect
> the spam and feed it to the SA-learn program.

Look at the spamassassin report of the false positives. Maybe you can identify the rules that most commonly trigger for these mails, and reduce the score of these rules.

Subject: Re: SPAM, random scores - but similar emails

Posted by nickvn on Fri, 27 Oct 2006 06:46:03 GMT
View Forum Message <> Reply to Message

ok, yeh I've been doing that the past few days.

Some emails were dated 12-24 hours infront somehow and 'that' rule (I've deleted it since) was giving some legit emails a higher than normal score.

I've been redirecting emails to have a look at manually as of recent. Prior to that, I've been just relying on NST updates and adjusting the score limit...

Subject: Re: SPAM, random scores - but similar emails

Posted by support on Fri, 27 Oct 2006 07:44:50 GMT
View Forum Message <> Reply to Message

legit mails older than 12 hours are extremely rare. Check the mail headers and make sure all mail gateways and servers that you have access to report the correct time.

Subject: Re: SPAM, random scores - but similar emails

Posted by nickvn on Fri, 27 Oct 2006 12:57:07 GMT
View Forum Message <> Reply to Message

I checked the emails, and they were a full day ahead - after being received.

A few emails all came from the same person (they were definately legit emails though).

Of the entire dates CF rule file, I just removed the lines for the 12-24 hour check and left the rest.

The problem I have is I am trying to find a perfect solution to the spam problem - if I set the score to default (5.0), I get roasted when 'important people' get rejected emails.
And if I set it too high, then I get complaints with people having to deal with more than 3-4 spam emails per day.

I currently only filter one domain (soon to be more) and there seem to be just 2 - 3 email addresses that just get targeted for a lot of spam. The rest, no so much attention...

Subject: Re: SPAM, random scores - but similar emails

Posted by Heidner on Sat, 28 Oct 2006 05:21:03 GMT
View Forum Message <> Reply to Message

I also have set the rejection scoring higher. But I also changed the points assigned by spamassassin for various offenses.

It doesn't take a lot of tuning... and you can stop a higher percentage of the spammers

My values are:

score YAHOO_RD_REDIR 1.237 1.083 1.366 3.642
score RCVD_IN_SORBS_ZOMBIE 0 0.819 0 1.0
score RCVD_IN_BL_SPAMCOP_NET 0 3.050 0 5.107
score RCVD_IN_NJABL_DUL 0 4.655 0 4.088
score RCVD_IN_NJABL_PROXY 0 3.026 0 3.438
score RCVD_IN_NJABL_RELAY 0 4.934 0 4.397
score RCVD_IN_NJABL_SPAM 0 2.051 0 2.841
score RCVD_IN_SBL 0 3.050 0 5.107
score RCVD_IN_XBL 0 2.511 0 5.076
score URIBL_SBL 0 3.629 0 5.996
score BAYES_00 0 0 -1.665 -2.599
score BAYES_05 0 0 -0.925 -2.413
score BAYES_20 0 0 -0.730 -1.951
score BAYES_40 0 0 -0.276 -1.096
score BAYES_50 0 0 1.567 0.001
score BAYES_60 0 0 3.515 1.372
score BAYES_80 0 0 3.608 3.087
score BAYES_95 0 0 4.514 4.063
score BAYES_99 0 0 5.070 5.886
score SPF_PASS -.501
score SPF_FAIL 0 0 0 2.875
score SPF_SOFTFAIL 0.500 0.842 0.500 0.500

score UNPARSEABLE_RELAY 4.001

I have a small net work -- so it is easier for me to monitor the mail. But my basic process for tuning the filters is still the same..

1) I enabled the message store filter. It is stores e-mails AFTER virus checking and before MIME and spamassassin checking.

2) I enabled the detailed logging in NST

3) I use spamlogs to consolidate the NST logs each night and forward the summary to my self and other important people. It has the time stamps, sender, subject, etc. on one line.

4) If an e-mail was bounced by NST (but stored) and it is critical, then I bring it from the mailstorage area back into the mail stream. I also feed the mail back into spam assassin with the learn option so it will learn the mail as "good"

5) I set the reject/delete e-mail at 11, mark as spam but send it to recepient at 9.0

6) I created a global HAM and SPAM mailbox that spam can be dropped into... and HAM can be copied into. The mail receipents do that themselves. Then I setup a job that runs a couple of times a day to learn both the good and the bad.

7) I review the mail that I receive that is in the range of 9 to 11 and make adjustments to the spamassassin scores to catch the most common problems (like the bad date/time problem you've mentioned).

8) I also setup some spamtrap addressess. I don't have a sales organization.. so I spam trap on "sales"... other good ones are "root" and "admin" I have about five spam trap addresses setup and they trap about 10% of the inbound spam. Spam trapping is good because the spam is fed into spam assassin with the learn option.

End result is that the spam filter rate is quite high.... about 95 - 97% accurate with only occassional false positives.

Oh yeah, I also made an effort to look at mail identified as possible spam - that comes from friends, relatives, businesses that I want -- and add them to a whitelist.

Subject: Re: SPAM, random scores - but similar emails

Posted by nickvn on Mon, 30 Oct 2006 00:08:12 GMT
View Forum Message <> Reply to Message

after reinstalling NST on a different server (uninstalling the old one), I copied the configuration files and the bayes database (backed up the new one)...

New install is set to 4.8 reject/redirect and 9 reject/delete

the bayes database was rating 3/4 of legit emails with an auto spam score of 4.4 - and then if someone had (for example) no subject, or all capitals in their subject, it would reject the emails and send to spam folder.

So I copied the backup of the new bayes DB into the the new install directory again and now emails are coming through properly again, with a few spam here and there.

What causes the bayes database to get corrupted like that?
Nothing is usually done to the (NST) server for months - and the "expire" bat file is scheduled to run 4am every morning...
