Subject: Trying to stop the German Racist Spam

Posted by BradlayLaw on Wed, 23 Jun 2004 08:26:22 GMT
View Forum Message <> Reply to Message

I'm trying to write a rule to prevent the hundreds of mails we get a day generated by the Sober.G virus (the racist german spewing one). I looked through the headers and they all have one thing in common :

Message-ID:

eg. Message-ID:

So I created a rule like so :

header LOCAL_GERMANSPAM Message-ID =~ //
describe LOCAL_GERMANSPAM Captures German Racist Spam
score LOCAL_GERMANSPAM 5.1

I tried the regular expression with my text editors find function and it found the message-ID fine enough.

This text was put in a file called germanspam.cf and placed in the folder with our other sa rulesets and config files and I restarted the NST service.

The german email is still getting through. I checked the headers and my rule appears to be picking up on it but the score is not changing. Here is part of a header after my rule was installed :

X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on NETPILOT
X-Spam-Status: No, hits=2.6 required=5.0 tests=BAYES_00,FROM_ENDS_IN_NUMS,
 LOCAL_GERMANSPAM,NO_REAL_NAME,PRIORITY_NO_NAME autolearn=no
 version=2.63
X-Spam-Level: **

Do you have any idea on where I am going wrong and if there is a better way to stop this spam.

Thanks

Post Edited (06-23-04 11:03)

Subject: Re: Trying to stop the German Racist Spam

Posted by lebig on Wed, 23 Jun 2004 08:52:07 GMT
View Forum Message <> Reply to Message

+1

http://www.byteplant.com/forum/read.php?f=3&i=25&t=25#reply_25

Subject: Re: Trying to stop the German Racist Spam

Posted by BradlayLaw on Wed, 23 Jun 2004 09:00:51 GMT
View Forum Message <> Reply to Message

There is no solution there though.

Subject: Re: Trying to stop the German Racist Spam

Posted by support on Wed, 23 Jun 2004 09:14:50 GMT
View Forum Message <> Reply to Message

BradlayLaw wrote:

> header LOCAL_GERMANSPAM Message-ID =~ //
> describe LOCAL_GERMANSPAM Captures German Racist Spam
> score LOCAL_GERMANSPAM 5.1

> X-Spam-Status: No, hits=2.6 required=5.0
> tests=BAYES_00,FROM_ENDS_IN_NUMS,
> LOCAL_GERMANSPAM,NO_REAL_NAME,PRIORITY_NO_NAME autolearn=no
>
> version=2.63
> X-Spam-Level: **

The score is too low. The BAYES_00 test has a negative score, and it all adds up to only 2.x spam points (X-Spam-Level: **). Try a score of at least 8, and you should feed an example of these mails to sa-learn for good measure.

Subject: Re: Trying to stop the German Racist Spam

Posted by BradlayLaw on Wed, 23 Jun 2004 09:24:32 GMT
View Forum Message <> Reply to Message

Ah, thats where I'm going wrong. I have already used sa-learn on about 1500 of these, but most of them seem identical so it only learnt from 30 or so of them.