Subject: SpamCopURI
Posted by InforMed Direct on Mon, 19 Jul 2004 08:49:33 GMT
View Forum Message <> Reply to Message

How do we tell if SpamCopURI is installed and working?

Thanks, Rob.

Subject: Re: SpamCopURI
Posted by support on Mon, 19 Jul 2004 11:56:00 GMT
View Forum Message <> Reply to Message

Please check your spamassassin reports and/or your X-Spam headers. You should find the SPAMCOP_URI_RBL test now and then adding some points to the overall spam score.

Or take a look at the spamassassin debug output:

cd [InstallationDirectory]
sa\spamassassin -x -D -c sa\ruleset < sa\sample-spam2.txt > out

Subject: Re: SpamCopURI
Posted by InforMed Direct on Tue, 20 Jul 2004 12:03:10 GMT
View Forum Message <> Reply to Message

> Please check your spamassassin reports and/or your X-Spam
> headers. You should find the SPAMCOP_URI_RBL test now and then
> adding some points to the overall spam score.

Hmm, doesn't look like it's trapping anything here. I collect the last two weeks of trapped SPAM messages in a separate folder. I've just searched for SPAMCOP_URI_RBL and none of the headers have this text string.

> Or take a look at the spamassassin debug output:
>
> cd [InstallationDirectory]
> sa\spamassassin -x -D -c sa\ruleset < sa\sample-spam2.txt >
> out

What is this supposed to do? As far as I can tell, sample-spam2.txt doesn't contain any links so wouldn't be trapped by SPAMCOP anyway.

What should I check next?

Thanks, Rob.

Subject: Re: SpamCopURI
Posted by InforMed Direct on Tue, 20 Jul 2004 12:53:26 GMT
View Forum Message <> Reply to Message

> What should I check next?

Later... I've just installed the latest version and made sure the checkbox for SpamCopyURI was checked.

I sent an email from Yahoo with the following link:

http://www.hollywoodshemales.com

This was taken from the blacklist and therefore should have been trapped - it wasn't. I believe the score is 3.0 and we have our level set to 2.0

Regards, Rob.

Subject: Re: SpamCopURI
Posted by support on Thu, 22 Jul 2004 08:47:33 GMT
View Forum Message <> Reply to Message

Instead of sample-spam2.txt, use any other mail for the test. When SPAMCOP_URI triggers, you will find evidence in the output file.

Subject: Re: SpamCopURI
Posted by support on Mon, 26 Jul 2004 09:58:51 GMT
View Forum Message <> Reply to Message

support wrote:

> Instead of sample-spam2.txt, use any other mail for the test.
> When SPAMCOP_URI triggers, you will find evidence in the output
> file.

Make sure to use the current URI entries on http://www.spamcop.net when testing
the SpamCopURI feature. You can define additional SURBL lists by adding these lines to the spamcop_uri.cf file in the sa\ruleset subdirectory (see also http://www.surbl.org):

```
uri       WS_URI_RBL  eval:check_spamcop_uri_rbl('ws.surbl.org','127.0.0.2')
describe  WS_URI_RBL  URI's domain appears in sa-blacklist
tflags    WS_URI_RBL  net
score     WS_URI_RBL  3.0

uri       OB_URI_RBL  eval:check_spamcop_uri_rbl('ob.surbl.org','127.0.0.2')
describe  OB_URI_RBL  URI's domain appears in ob.surbl.org
tflags    OB_URI_RBL  net
score     OB_URI_RBL  4.0

uri       AB_URI_RBL  eval:check_spamcop_uri_rbl('ab.surbl.org','127.0.0.2')
describe  AB_URI_RBL  URI's domain appears in ab.surbl.org
tflags    AB_URI_RBL  net
score     AB_URI_RBL  5.0
```

Subject: Re: SpamCopURI
Posted by Shinare on Tue, 27 Jul 2004 18:41:57 GMT
View Forum Message <> Reply to Message

I just upgraded from 1.2.4.1 to 1.2.4.4 with high hopes of implementing this SpamCopURI functionality. I followed the FAQ and simply installed the new version over the old version. When I ran the Admin program, it correctly shows that the version is 1.2.4.4 but no where in the admin process was a Check-Box asking if I wanted to enable/disable the SpamCopURI functionality as mentioned above.

(Quote InforMed: "Later... I've just installed the latest version and made sure the checkbox for SpamCopyURI was checked. ")

Did I miss something? Also, I am unable to find the document "spamcop_uri.cf" anywhere in my installation directory.

Subject: Re: SpamCopURI
Posted by InforMed Direct on Tue, 27 Jul 2004 20:00:04 GMT
View Forum Message <> Reply to Message

> version is 1.2.4.4 but no where in the admin process was a
> Check-Box asking if I wanted to enable/disable the SpamCopURI
> functionality as mentioned above.

It's not in the admin process - it's an install option (NOTE: shouldn't it be in the admin program as well?).

> Did I miss something? Also, I am unable to find the document
> "spamcop_uri.cf" anywhere in my installation directory.

Maybe a re-install is in order. However, I had to make two further changes to get it to pickup our test spam:

1. Uncheck "Skip RBL checks" (i.e. enable it) and enter DNS IP address
2. Change the SPAMCOP_URI_RBL score in sa\ruleset\spamcop_uri.cf) to 10.0

The later isn't strictly needed but we found that in a simple spam test with a link to http://bigbonus-casino.com slipped through. The reason being is that it was scored correctly with 3.0 (the default) but the Bayes learner (for some reason) reduced the score by -4.9 thus taking it our threshold of 2.0

Before enabling RBL (off by default), SpamCopURI was in effect disabled. Turning it on, and it started scoring.

Cheers, Rob.

Subject: Re: SpamCopURI
Posted by InforMed Direct on Tue, 27 Jul 2004 20:10:13 GMT
View Forum Message <> Reply to Message

InforMed Direct wrote:

> Before enabling RBL (off by default), SpamCopURI was in
> effect disabled. Turning it on, and it started scoring.

PS. Since enabling SpamCopURI yesterday, it's caught an extra 8 spam emails. Compared to my average before, this is a ~20% improvement in trap rate which is most welcome.

Cheers, Rob.

Subject: Re: SpamCopURI
Posted by Shinare on Wed, 28 Jul 2004 13:45:22 GMT
View Forum Message <> Reply to Message

OK, re-installed and it looks like its all there now. I did not notice the checkbox when installing the upgrade the first time. I dont know if it was checked by default that first time but it was this second time. Once finished, I looked for spamcop_uri.cf and it was there. Looks like it should be working. I copied and pasted the above aditional SURBL lists to the end of the .cf file as suggested in the

eariler post. Hopefully that will help with our false negatives. :) I also changed the score to 10 as suggested. Personally, that seems to be a good policy because if it contains these URL's then I would say with %100 confidence that its spam.

What kind of upkeep am I going to need to give the SpamCopURI? Should I be looking out for new entries to place in the .cf file like the new entries above?

Subject: Re: SpamCopURI
Posted by support on Wed, 28 Jul 2004 15:09:24 GMT
View Forum Message <> Reply to Message

The changes to the spamcop_uri.cf file earlier in this thread will be part of the next release of NoSpamToday!, so there is nothing for you to do.

Changes we do in the local.cf file are not automatically applied to your installation, because we don't want to overwrite your settings. You can view our default settings in the file local.cf.sample. This file is updated each time you update NoSpamToday!.

Subject: Re: SpamCopURI
Posted by Shinare on Wed, 28 Jul 2004 19:32:09 GMT
View Forum Message <> Reply to Message

I'm not sure how this will look on the forums, but here is a sample of SPAMCOP_URI_RBL in action, so I know its working. This is from a spam message I just now received:

Content preview: Windows Update XP.ME.2000.NT [...]

Content analysis details: (15.9 points, 5.0 required)

```
 pts rule name              description
---- ---------------------- --------------------------------------------------
 0.1 HTML_50_60             BODY: Message is 50% to 60% HTML
 0.3 MIME_HTML_ONLY         BODY: Message only has text/html MIME parts
 0.1 HTML_MESSAGE           BODY: HTML included in message
 0.3 HTML_FONT_BIG          BODY: HTML has a big font
  10 SPAMCOP_URI_RBL        URI's domain appears in spamcop database at sc.surbl.org
                            [Benito.kbsbwj.info is blacklisted in URI RBL at]
                            [sc.surbl.org]
 4.0 OB_URI_RBL             URI's domain appears in ob.surbl.org
                            [Benito.kbsbwj.info is blacklisted in URI RBL at]
                            [ob.surbl.org]
```

1.1 MIME_HTML_ONLY_MULTI Multipart message only has text/html MIME parts

Subject: Re: SpamCopURI
Posted by InforMed Direct on Wed, 28 Jul 2004 22:32:55 GMT
View Forum Message <> Reply to Message

> I'm not sure how this will look on the forums, but here is a
> sample of SPAMCOP_URI_RBL in action, so I know its working.

It's working well for us now after a) enable RBL with DNS and b) increasing the score from 3.0 to 10.0. The lower figure does work it's just that I'm pretty happy that if a URL to a blocked site is found, then it gets scored pretty highly.

Block URLs are now getting included in about 30% of blocked spam with the rest getting trapped by the other rules.

Cheers, Rob.