

Re: Need automatic spam reporting tool

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.sco.misc/2008-03/msg00040.html>

- *From:* "Steve M. Fabac, Jr." <smfabac@xxxxxxx>
 - *Date:* Wed, 05 Mar 2008 13:57:08 -0600
-

Bill Campbell wrote:

On Wed, Mar 05, 2008, Steve M. Fabac, Jr. wrote:

I'm flooded with returned messages from e-mail servers bouncing spam messages where the spammer uses fake "From:" tags with random names on my 24by7webstores.com site: "From: "Mort tikkanen" <Mort-vorhies@xxxxxxxxxxxxxxxxxxxxxx>"

You should be able to build the current version of whois on SCO systems without much problem.

Is there a command string to whois that will accept an IP address and return something that looks like this?:

(Asked whois.apnic.net:43 about 117.11.60.63)

```
inetnum: 117.8.0.0 - 117.15.255.255
netname: CNCGROUP-TJ
descr: CNC Group Tianjin province network
descr: China Network Communications Group Corporation
descr: No.156 Fu-Xing-Men-Nei Street
descr: Beijing 100031
country: CN
admin-c: CH455-AP
tech-c: HZ19-AP
remarks: service provider
mnt-by: APNIC-HM
mnt-lower: MAINT-CNCGROUP-TJ
mnt-routes: MAINT-CNCGROUP-RR
status: ALLOCATED PORTABLE
remarks: -----
remarks: This object can only be updated by APNIC hostmasters.
remarks: To update this object please contact APNIC
remarks: hostmasters and include your organisation's account
remarks: name in the subject line.
remarks: -----
```

Re: Need automatic spam reporting tool

changed: hm-changed@xxxxxxxxxx 20070525
source: APNIC
route: 117.8.0.0/13
descr: CNC Group CHINA169 Tianjin Province Network
country: CN
origin: AS4837
mnt-by: MAINT-CNCGROUP-RR
changed: abuse@xxxxxxxxxx 20070525
source: APNIC
role: CNCGroup Hostmaster
e-mail: abuse@xxxxxxxxxx

On the other hand, dealing with idiots who don't control the blowback resulting from forge From and Sender in spam, is generally a waste of your time and effort (a good bit of what I see here if from Barracuda boxes, and I don't know whether that's the default setting on current Barracudas).

Bill, I welcome the bounced messages. It give me a chance to submit them to the ISP's where the open relays or spammer's lurk.

As I indicated to Boyd, I am angered by someone cloaking their spam as from my domain. Unstopped, they will eventually result in my domain being added to rbl so I'll have to take action to have my site removed from the black list.

Is it possible that your web site has a vulnerable formail.pl script (are there any non-vulnerable ones :-)) so the messages are actually being sent through the web server?

No, examination of the bounced messages headers show the originating IP addresses of the spam. I collect all messages identified by originating IP address and then submit them to the ISP for the IP address.

...
Bill

—

INTERNET: bill@xxxxxxxxxxxxx Bill Campbell; Celestial Software LLC
URL: <http://www.celestial.com/> PO Box 820; 6641 E. Mercer Way
FAX: (206) 232-9186 Mercer Island, WA 98040-0820; (206) 236-1676

Re: Need automatic spam reporting tool

Liberals love to say things like, 'We're just asking everyone to pay their fair share.' But government is not about asking. It is about telling. The difference is fundamental. It is the difference between making love and being raped, between working for a living and being a slave.
Dr. Thomas Sowell, Forbes, July 1994

—
Steve Fabac
S.M. Fabac & Associates
816/765-1670
.