Using BGP for realtime import and export of spam whitelist/blacklist entries

after 2 years

Peter Hessler
phessler@openbsd.org

OpenBSD

14 March, 2015

bgp-spamd.net

network-based spam fighting:

- bypass and trap lists from spamd(8)
- use BGP-4 and BGP communities (RFC 4271 & RFC 1997) for distribution and labeling

bgp-spamd.net

- Publically launched at AsiaBSDCon 2013 on March 17
- 3 upstream sources
- 4 users

bgp-spamd.net

- A year ago (16 May 2014)
- 5 upstream sources
- 28 users

bgp-spamd.net

- Today (14 March 2015)
- 5 upstream sources
- 55 users
- 2 route servers

bgp-spamd.net

- available at `http://www.bgp-spamd.net`
- all configurations and scripts are available
- I am interested in additional “spamd-source” servers, please contact me
- and of course, more users are always welcome

spamd-source

- only list the specific IP addresses that exhibited a specific behaviour
- do *NOT* penalize/reward network neighbors
- really simplistic, we just want to catch the low-hanging-fruit
- don't open your mail server to the world
- don't block the world from seeing your mail server
- greylisting is powerful, when it still applies!

spamd-source trap list

- generated from source server's spamd trap list
- addresses are listed if their first delivery attempt is to a spamtrap
- expires in 24 hours from last delivery attempt

spamd-source bypass list

- spamd has a very low bar to be added to the whitelist
- ...redelivery within 4 hours
- ...kept in the whitelist for 36 days.
- semi-trusted email server list used to bypass spamd
- higher entry bar than normal spamd whitelist
- in the whitelist for 75 days, and sent more than 10 emails
- ...we “think” it’s a real mail server
- again, do not be overly aggressive

why is this useful

- use the bypass and trap lists from 3rd parties
- ...they are much larger than you
- ...semi-trusted servers are usually semi-trusted elsewhere
- ...ditto for attackers
- shared bypass lists help the “gmail sender” problem

statistics - also known as 'blatent lies'

- 1,675,203,296 Events

traplist statistics - also known as 'blatent lies'

Unique Unroutable IP Addresses

- 44 entries from 0.0.0.0/8 ('this' network)
- 128 entries from 10.0.0.0/8 (RFC 1918)
- 6 entry from CGN Shared network
- 21 entries from localhost (127.0.0.0/8)
- 3 entry from 169.254.0.0/16 (link local)
- 73 entries from 172.16.0.0/12 (RFC 1918)
- 70 entry is 192.168.0.0/16 (RFC 1918)
- 390 entries are "Multicast" (224.0.0.0/4)
- 318 entries are "reserved" (240.0.0.0/4)
- total of 845,310 additions

traplist statistics - also known as 'blatent lies'

Top 10

- 1 193,382 65.98.68.250/32 fortressitx.com.
- 2 171,500 69.56.148.14/32 gateway05.websitewelcome.com.
- 3 170,929 69.56.224.20/32 gateway02.websitewelcome.com
- 4 169,687 69.15.35.10/32 mail.inviewvision.com
- 5 168,632 67.18.94.7/32 gateway14.websitewelcome.com.
- 6 168,609 67.241.130.149/32 cpe-67-241-130-149.buffalo.res.rr.com.
- 7 167,514 72.10.20.37/32 mail.pascoprocessing.com.
- 8 167,145 74.125.83.50/32 google.com.
- 9 167,145 74.125.83.42/32 google.com.
- 10 167,145 74.125.83.41/32 google.com.

results

SUCCESS

lessons learned

- overall, a success
- generally positive reactions from users

the good

- European mirror!
- available at `eu.bgp-spamd.net`
- ... just use the IP address it resolves to
- ... web page and documentation will be updated today

the good

- many sources sharing information
- block lists are supurb

the good

- 3rd parties are making this work with non-OpenBSD users!
- Mark Martinec made it work with FreeBSD, rbldnsd, and SpamAssassin
- Anonymous using Quagga and their Propritary infrastructure
- (thank you!)

the good

- very fast to update
- 7 seconds to download the full bypass and trap lists over crappy home dsl
- 2 seconds to propagate changes to all members
- ... can be even faster, needs more work

the bad

- bypass list has too many spammers on it
- ... several users have mentioned they had to stop using it
- ... we need to spend more time adjusting the heuristics

the bad

- server crash, causing 5 day outage
- ...while I was on vacation (in New Zealand)
- ...and during long holiday weekend

the ugly

- I have not been as responsive as I should have been
- have not had a lot of time to dedicate to improving
- ... code
- ... sources
- ... client usage

the ugly

- still no IPv6 support
- ... well, the distribution mechanism works perfectly fine
- ... “just” needs spamd(8) support

future work

- fix the heuristics for addition to the bypass list
- ... a bit *too* relaxed
- (still) add IPv6 support to spamd
- 36 hour days

future work - spamd-source

- easier processing of spamd(8) on spamd-source systems
- can spamd differentiate how it received the data
- more spamd-sources from different and new countries
- ... University students in CA do not send a lot of email to JP

future work - brainstorming

- voting
- ... “two upstreams think an IP is X, then make it X”
- ... somewhat tricky, as BGP doesn’t support this
- deeper level of integration between bgpd and spamd
- ... partial syncs of spamd databases
- ... spamd use pf tables for all the things?
- ... for now, only thoughts with both upsides and downsides

Acknowledgements

Many thanks to
my coauthor Bob Beck,

- the University of Alberta at `ualberta.ca`
- Bob Beck of `obtuse.com`,
- Henning Brauer of `bsws.de`
- Peter N.M. Hansteen of `BSDly.net`,

for being sources of `spamdb` information.

- `Sonic`

for hosting the reference implementation `rs.bgp-spamd.net` and

- `Hostserver.de`

for hosting the European implementation `eu.bgp-spamd.net`

Questions?