Using BGP for realtime import and export of OpenBSD spamd entries

Peter Hessler
phessler@openbsd.org

OpenBSD

17 March, 2013
spamd uses IP host entries, to whitelist, blacklist or greylist hosts
spamd can import and export these lists
trivia: IP host entries can be represented as a route
bgp is used to distribute IP route lists
tie the two together, to simplify distributing these addresses
spamd

- written by Bob Beck
- included in OpenBSD since 3.3, greylisting added in 3.5
- uses greylisting to force unknown senders to retry delivery
  (very effective against bot-nets sending spam)
- uses blacklisting to reject mail from “known bad” senders
- fetches blacklists at the top of the hour from a web server
bgp is the glue that holds the internet together
used to distribute the 400k+ IPv4 routes of the Global Routing Table
scales incredibly high, and incredibly fast
very minor feature called “communities” that we will exploit
**bgp communities**

- allows you to mark a route with optional site-specific attributes
- bgp peers can use this to make arbitrary decisions on received routes
- route: 192.0.2.55/32 community: 65066:42
- this is our “secret sauce”
openbgpd

- written by Henning Brauer and Claudio Jeker
- included in OpenBSD since 3.5
- software based, so we can use the power of a general purpose OS
- ...like scripting. or cron.
everything we use is already built-in to both spamd and bgpd, or are our custom scripts.

...the ability to use “long” pf table names will be in the 5.3 release
tying them together

- so, let's start to tie them together
- export IP address lists
- import IP address lists
tying them together

- exporting IP addresses happens on the “spamd-source” systems.
- only list the specific IP addresses that exhibited a specific behaviour
- do \textit{NOT} penalize network neighbors
“spamd-source” systems insert IP addresses to our feed

really simplistic, we just want to catch the low-hanging-fruit
first, select known good upstream sources
be conservative
don’t whitelist the world
don’t blacklist the world
greylisting is powerful, when it still applies!
spamd-source blacklist

- listed IP address sent mail to a “spam trap” address
- blacklist timeout of 24 hours
- do not be overly aggressive

bgpctl network add 192.0.2.20/32 community 65066:666
spamd-source whitelist

- semi-trusted email servers
- higher entry bar than normal spamd whitelist
- in the whitelist for 75 days, and sent more than 10 emails
- again, do not be overly aggressive

bgpctl network add 192.0.2.55/32 community 65066:42
route server

- the center of our universe
- receives routes and communities from the spamd-source systems
- redistributes them to client/peers
route server

- only accept addresses from trusted spamd-source systems
- only accept host routes (/32)
- mark with our AS and community, for easy filtering

match from group BS community neighbor-as:42 set community $myAS:42
match from group BS community neighbor-as:666 set community $myAS:666
receives the black and white lists
separates them out, and applies the local configuration
client whitelist

- adds whitelist entries to a pf table
- allows whitelisted entries to bypass spamd
- receive emails faster from servers that are semi-trusted elsewhere
$ cat /etc/pf.conf

table <bgp-spamd-bypass> persist
table <spamd-white> persist

pass in proto tcp from any to any port smtp \ 
rdr-to 127.0.0.1 port spamd

pass in proto tcp from <bgp-spamd-bypass> to any port smtp

pass in proto tcp from <spamd-white> to any port smtp

pass out out proto tcp to any port smtp
why not simply use pf to block blacklist hosts?

your ceo is expecting an email from a blacklisted system

tell sending servers that they are being blacklisted on purpose
warning: Work In Progress ahead!
$ cat /usr/local/sbin/bgp-spamd.black.sh

#!/bin/sh
AS=65066

bgpctl show rib community ${AS}:666 | awk '{print $1}' | \ sed 's/\.*$//' > /var/db/spamd.black

/usr/libexec/spamd-setup

# EOF
$ cat /etc/mail/spamd.conf

all:
    :bgp-spamd:

bgp-spamd:
    :black:
    :msg="Your address %A has sent mail to a spamtrap\nwithin the last 24 hours":\n    :method=file:\n    :file=/var/db/spamd.black:

# EOF
security concerns

- where do we get the IP addresses from?
- what is the criteria for adding an IP address to a black or white list?
- how do we prevent random clients from inserting information?
- how does this tie in with the Global BGP Routing Table?
- wait, will this adjust the routes on my system/network?
this sounds interesting, can I use it?

available today, at http://www.bgp-spamd.net

I will run the above reference implementation for the entirety of 2013

all configurations and scripts will be available.

48457 blacklist entries

124527 whitelist entries
future work

- accelerate adding addresses to the bgp feed
- import/export of data between bgpd and spamd
- network aggregation
Acknowledgements

Many thanks to my coauthor Bob Beck,

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

for being sources of spamdb information.

- Sonic.net

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