

Re: IP ranges used in North America, Hawaii, and Alaska?

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2005-12/msg00345.html>

- *From:* "prg" <rdgentry1@xxxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2005 14:42:39 -0800
-

Cameron L. Spitzer wrote:

- > In article <1135022984.734741.90890@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, prg wrote:
- >>
- >> If you are trying to cut down on spam, try SpamAssassin.
- >> <http://spamassassin.apache.org/>
- >
- > Filtering is nice for cleaning up the stragglers that
- > get past the source-IP block list checking.
- > But there's no reason for most places to accept email
- > from IP ranges owned by spam houses. I don't care
- > if it's Python Video or Hanaro.net. If they sent it,
- > I'm absolutely sure my users don't want it, and there's
- > no reason to give it further CPU time.
- > *Filtering* all that crap would cost a lot more.

You obviously did not note that I suggested the use of (dns)RBLs.

If only email (or a special use web server, eg.) is being firewalled (ie., MTA sits on its own box and has its own IP), I have no problem with the idea of blocking "overseas" IP blocks wholesale as part of a larger, layered, deeper security system. In fact, with a drop policy and a list/range of "good" (per your needs) IP blocks it can help to filter on source IPs. Also, I don't mind dedicating boxes to single purposes if possible.

Besides, SpamAssassin has a number of plugins that will handle dnsbls, country codes (from each relay used in the delivery path -- not just the IP source address), Razor, Spamcop. Ah, but Alan said it was "Not reliable and a hassle". Now `_his_` solution is ... hmmm.

- >> The list you have might be somewhat useful (for something) if
- >> `_everyone_` conformed to its intent. The ones you are trying to keep
- >> out are the ones who don't.
- >
- > The `sbl-xbl.spamhaus.org` list (for example) is more than
- > "somewhat" useful. I don't care if "`_everyone_` conformed"
- > (whatever that means), just that it meets my organizations'
- > needs.

Re: IP ranges used in North America, Hawaii, and Alaska?

See above.

Is it the "everyone" or "conformed" part you don't get. Perhaps the dropped "intent"? Yep, it's pretty fuzzy and senseless taken out of the context of the thread preceding it.

And what does the sbl-xbl.spamhaus.org list have to do with IANA's IP block list of allocated IP space? I would much rather make use of the spamhouse list.

>> Packets are routed by destination and not_by_source addresses.
>> Spam will 99.9999999999% of the time have a bogus IP return address
>
> I'm not sure what you're talking about there. The source IP
> is, as far as I know, the most difficult thing for the spammer
> to forge.

Patently false, since most ISPs do not perform effective egress filtering nor do most private stub nets.

> (Well, he can forge it, but he's got to be able to
> collect your responses to the forged addresses, or he can't send
> spam that way.)

Now you know why spammers include a "return" link in the body of the email. There does not have to be any connection between the IP source address of the spam and the IP the link goes to.

> He's got to do some kind of asymmetric routing
> trick. Rumor has it Alan Ralsky was doing that for a while.
> His crap would seem to come from a throwaway dialup account,
> but there was way too much of it for that to be true.
> That trick became useless when lists of dynamically-assigned
> IP ranges became available in DNSBL form. It's no use
> pretending to be a dial-up if everybody's blocking those.

You might be surprised how often source_routed packets (from any kind of IP) are allowed into a network. Spammers work on volume, not precise aiming. They use any and all tricks. Open relays, source routed packets, zombies and drones, even MS_Windows:-0

>> Your "solution" has been proposed and tried by countless numbers of
>> those unknowledgeable in the ways of routing across the net.
>
> Blocking by source-IP is one of the most important techniques
> for keeping spam out.

Maybe yes, maybe no, depending on where you expect your email to originate.

If you can limit your expected origins and accept the side effects,

Re: IP ranges used in North America, Hawaii, and Alaska?

Re: IP ranges used in North America, Hawaii, and Alaska?

great. However, it's much easier to have a denial `_policy_` at the firewall and allow the `_expected_` through. Then if/when you need to allow someone in from, say overseas like UK, it's easier and less error prone than explicitly denying certain blocks, then coding `_exceptions_`.

- > I doubt there are many networks with more
- > than a few thousand mailboxes that **don't** do it, at least a
- > little, if only to reduce the load on their filtering machines.

The larger the network --- and presumably the more likely employees will work/travel around the globe writing email back to the main office --- the `_less_` likely (IMO) that IP `_block_` filtering by `_country_codes_` is to be used. It's been my experience, anyway. BTW, it's a similar reason the ISPs give for not more aggressively filtering on source IP of incoming mail.

Smaller networks (with fewer email users) can likely be more easily accommodated `_and_` have IP `_block_` addresses denied.

Anyway, without a clearer statement of what Alan J. wanted, I was being purposefully dramatic to make sure he did not think that by this (seemingly) simple technique he had cured his woes. With more info and better understanding of `_his_` needs (and willingness to accept the effects) I have no particular reason to poo-poo his efforts (I'll certainly not live with the consequences). Less knowledgeable folk who find this in the archives will hopefully be better informed what issues are involved and what they can expect by adopting a similar approach (or whether they should do so for `_their_` needs).

But I will wager that neither Alan nor you will work your way through (any?) of the links I provided, though you might find the exercise informative if not necessarily immediately applicable. Not even this eg.:

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/AE-cidr.txt>
UAE

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/AF-cidr.txt>
Afghanistan

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/IR-cidr.txt>
Iran

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/CL-cidr.txt>
Chile

[Note the 24.152.0.0/17 block ;-(]

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/CN-cidr.txt>
China

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/CU-cidr.txt>
Cuba

<http://www.completewhois.com/statistics/data/ips-bycountry/rirstats/CX-cidr.txt>
Christmas I.

[Could not resist]

cheers,

Re: IP ranges used in North America, Hawaii, and Alaska?

prg

• **References:**

- ◆ **[IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* Alan Jones
 - ◆ **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* Felix Tilley
 - ◆ **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* Alan Jones
 - ◆ **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* Wayne
 - ◆ **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* Alan Jones
 - ◆ **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* prg
 - ◆ **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - ◇ *From:* Cameron L. Spitzer
- Prev by Date: **[Hiding directory contents from HTTP](#)**
 - Next by Date: **[Re: Hiding directory contents from HTTP](#)**
 - Previous by thread: **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - Next by thread: **[Re: IP ranges used in North America, Hawaii, and Alaska?](#)**
 - Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**