The curse of the Open Recursor

Tom Paseka
Network Engineer
tom@cloudflare.com

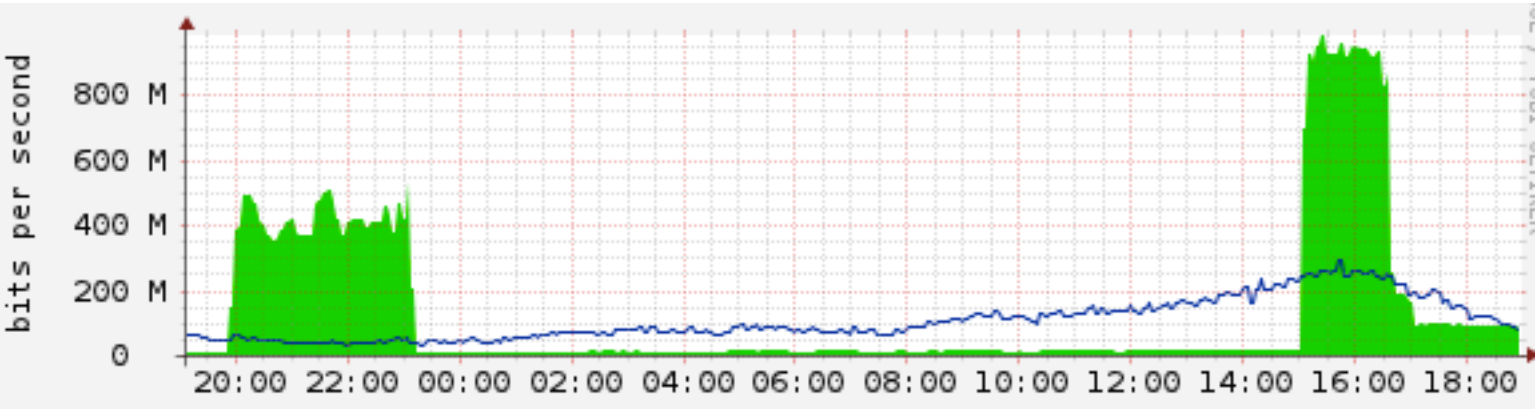
Recursors

Why?

- Exist to aggregate and cache queries
  - Not every computer run its own recursive resolver.
- ISPs, Large Enterprises run these
- Query through the root servers and DNS tree to resolve domains
- Cache results
- Deliver cached results to clients.

Recursors

The Problem!



- Example of DNS Based reflection attack from a Peer in Hong Kong.

Recursors

Open / Unsecured Recursors ?

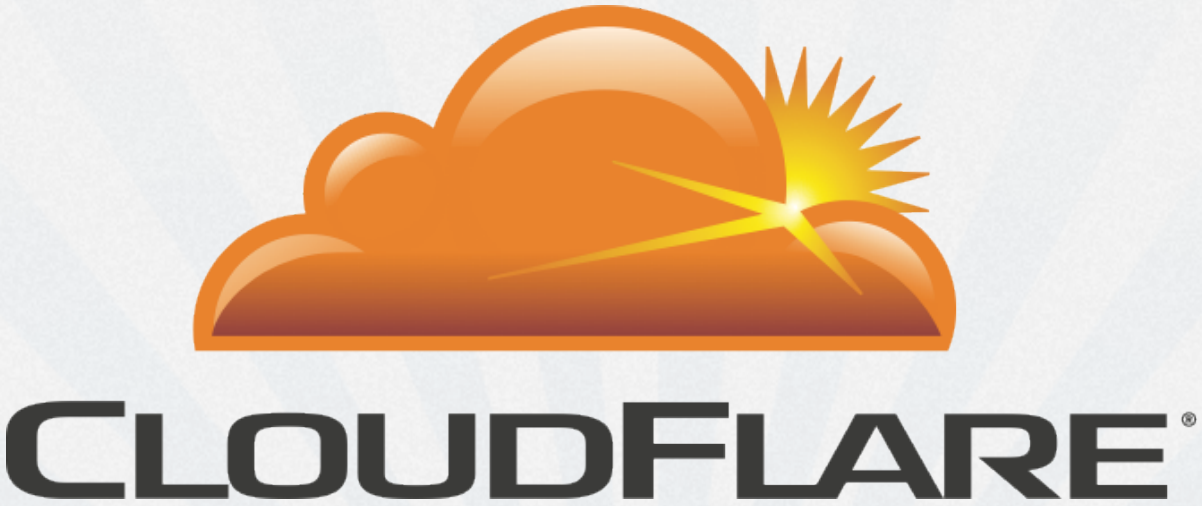
- DNS server set up for recursion
  - ie. non-authoritative
  - Will answer for zones it is not authoritative for
  - Recursive lookups
  - Will answer queries for anyone
- Some Public Services:

  Google, OpenDNS, Level 3, etc.
  - These are “special” set-ups and secured.

Recursors

Say Again?

- There are hundreds of thousands of DNS Recursors.
- Many of these are not secured.
- Non secured DNS Recursors can and will be abused
- CloudFlare has seen DNS reflection attacks hit 100Gbit traffic globally.



What is a Reflection Attack?

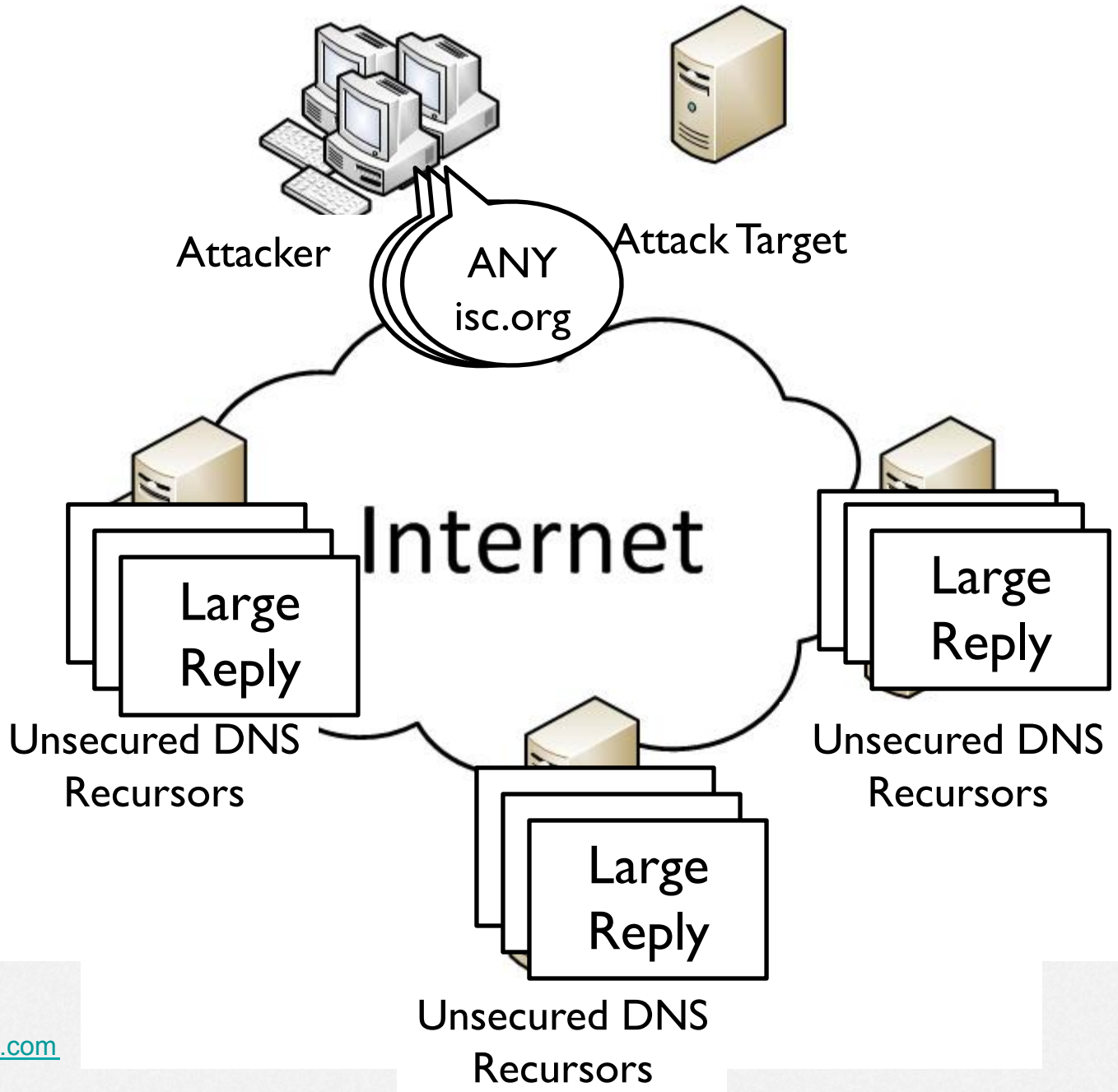
Reflection Attack

- UDP Query
- Spoofed source
  - Using the address of the person you want to attack
  - DNS Server used to attack the victim (sourced address)

- Amplification used
  - Querying domains like ripe.net or isc.org
  - ~64 byte query (from attacker)
  - ~3233 byte reply (from unsecured DNS Server)
  - 50x amplification!

- Running an unsecured DNS server helps attackers!

Reflection Attack

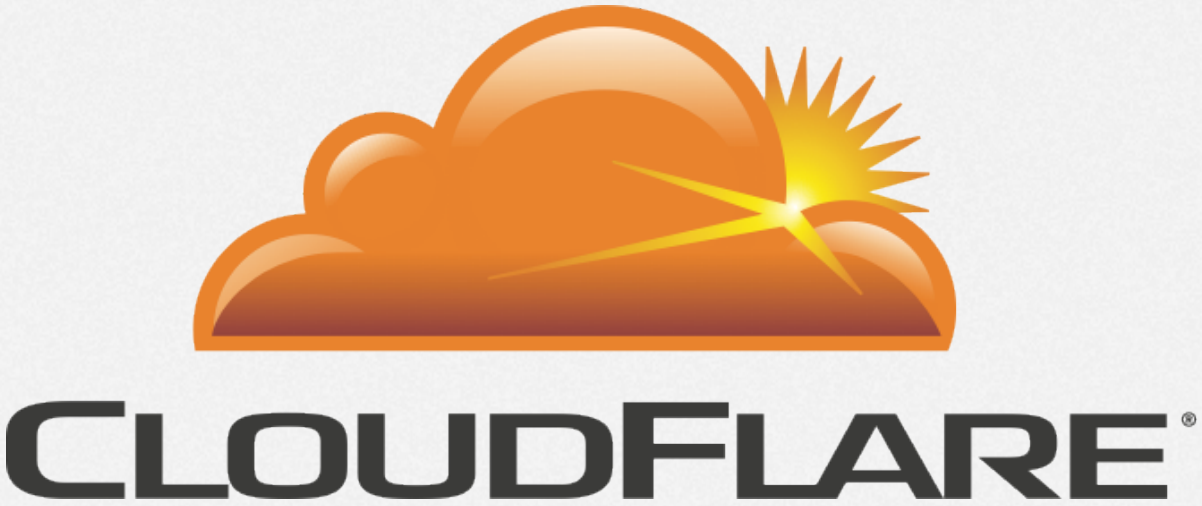


Reflection Attack

- With 50x amplification:
  - 1Gbit uplink from attacker (eg: Dedicated Servers)
  - 50Gbit attack
  - Enough to bring most services offline!

- Prevention is the best remedy.

- In recent attacks, we've seen around 80,000 open/ unsecured DNS Resolvers being used.
- At just 1Mbit each, that's 80Gbit!
  - 1mbit of traffic may not be noticed by most operators.
  - 80Gbit at target is easily noticed!



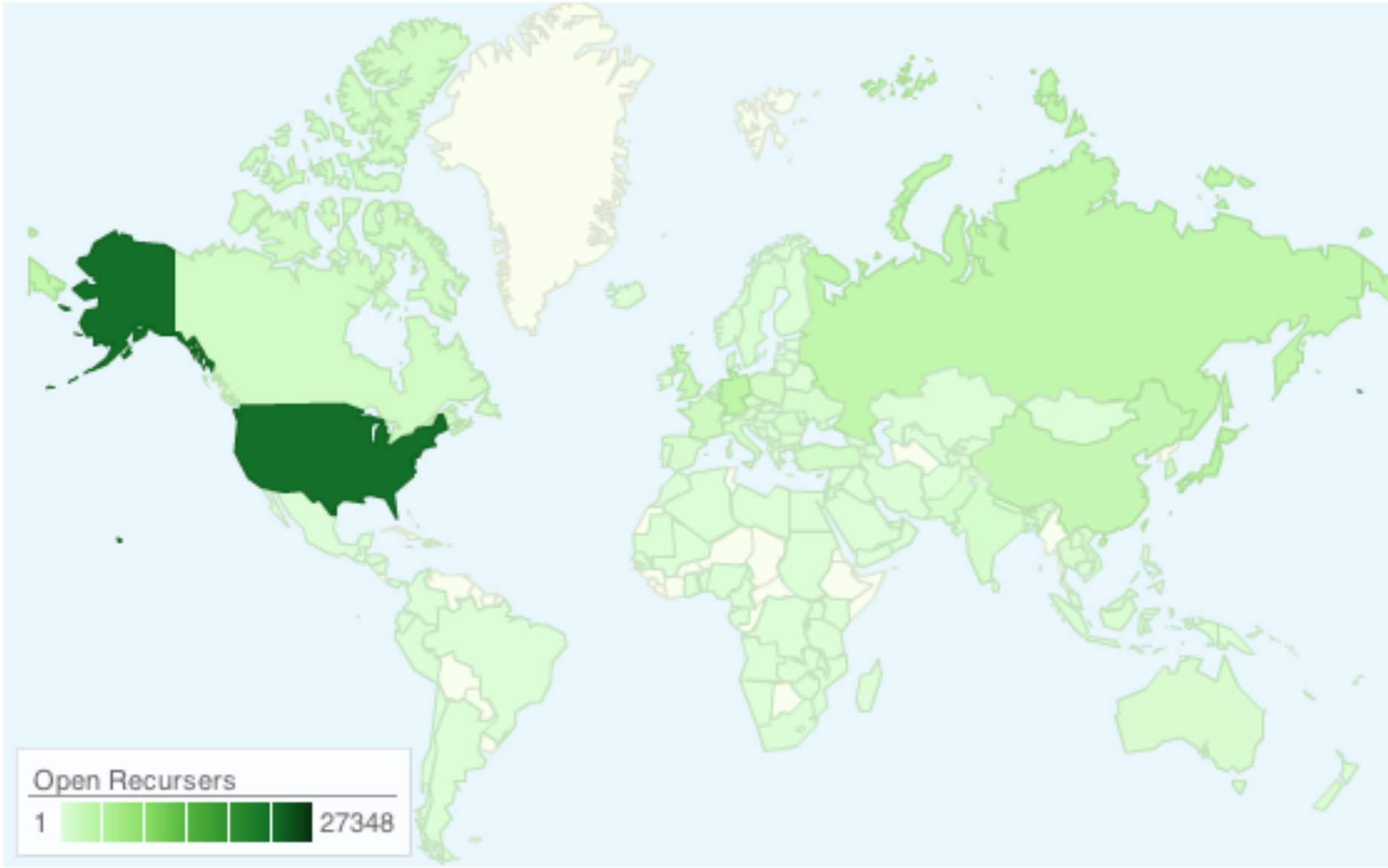
Where are they coming from?

Where are the open Recursors?

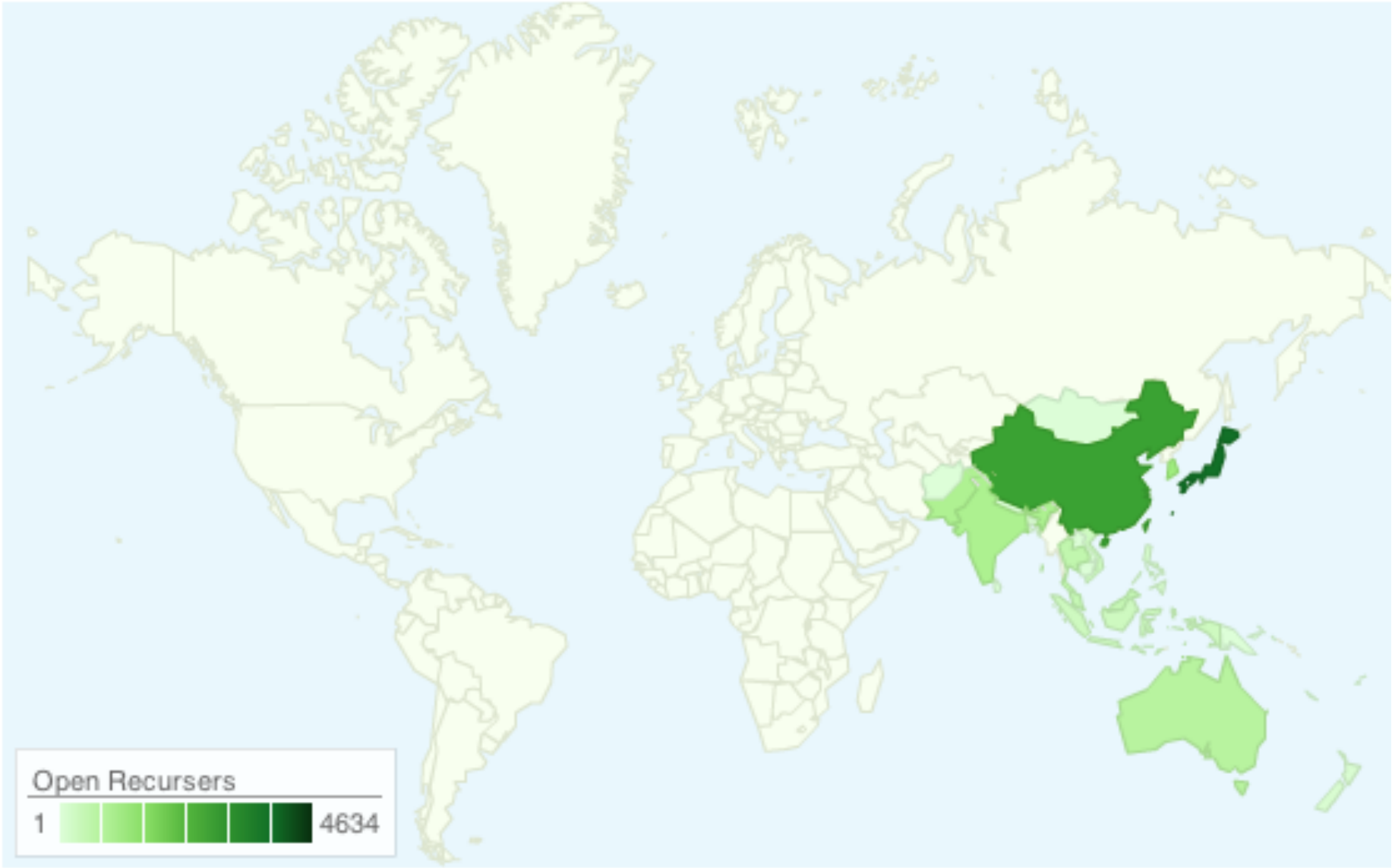
- Nearly Everywhere!

- CloudFlare has seen DNS Reflected attack traffic from:
  - 27 out of 56 Economies in APNIC Region
  - More attacks from higher populated economies.

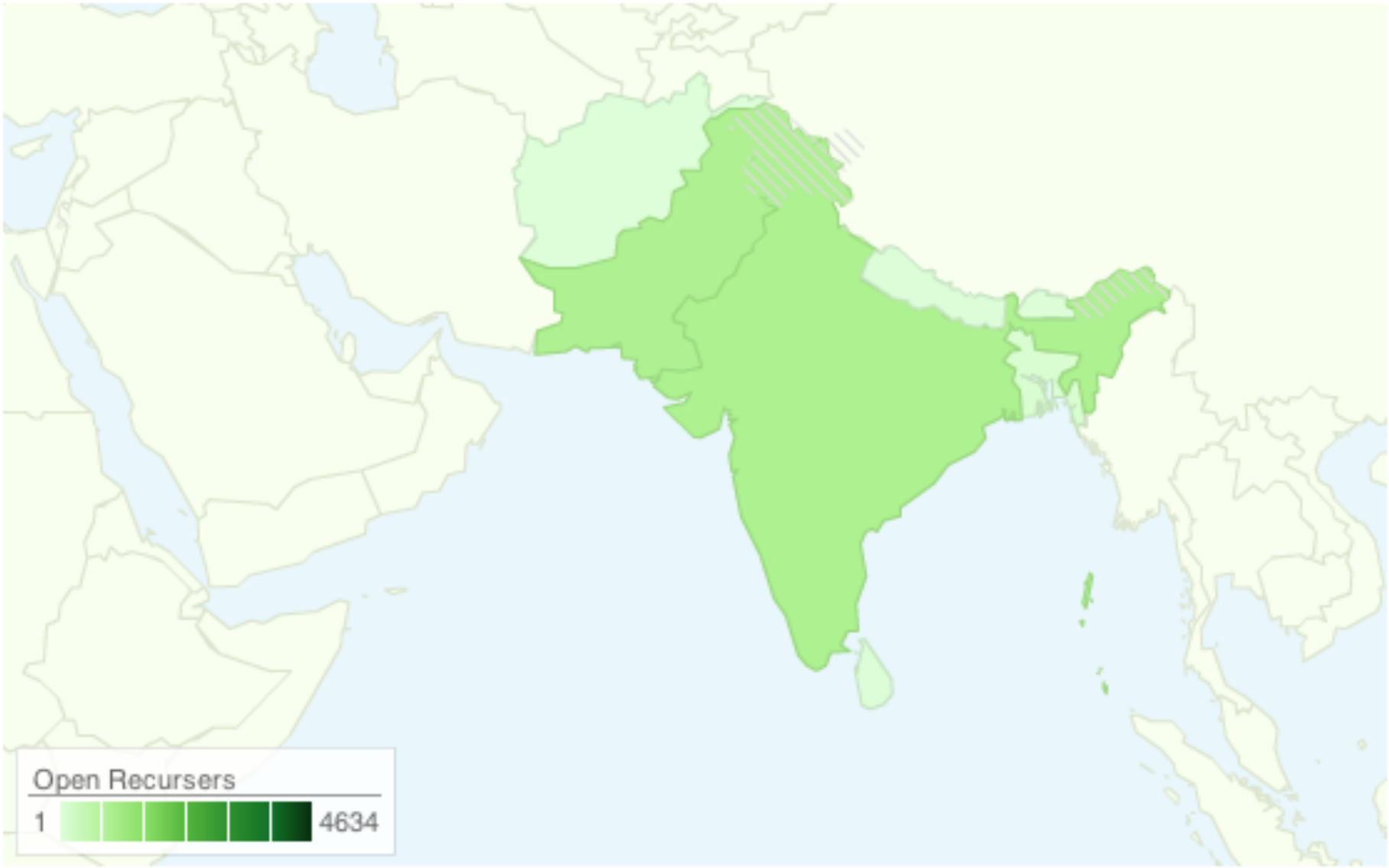
Where are the open Recursors?



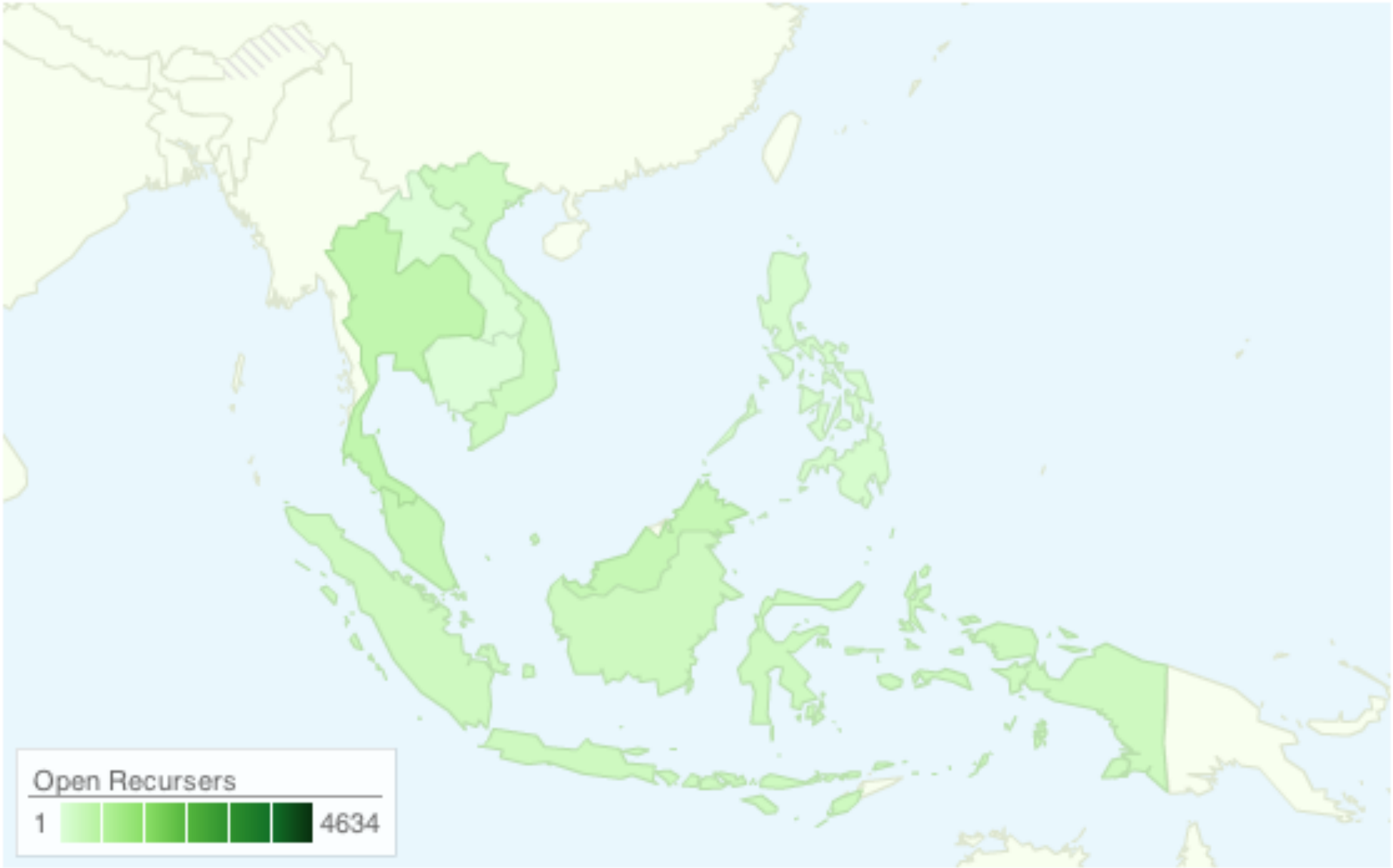
Where are the open Recursors?



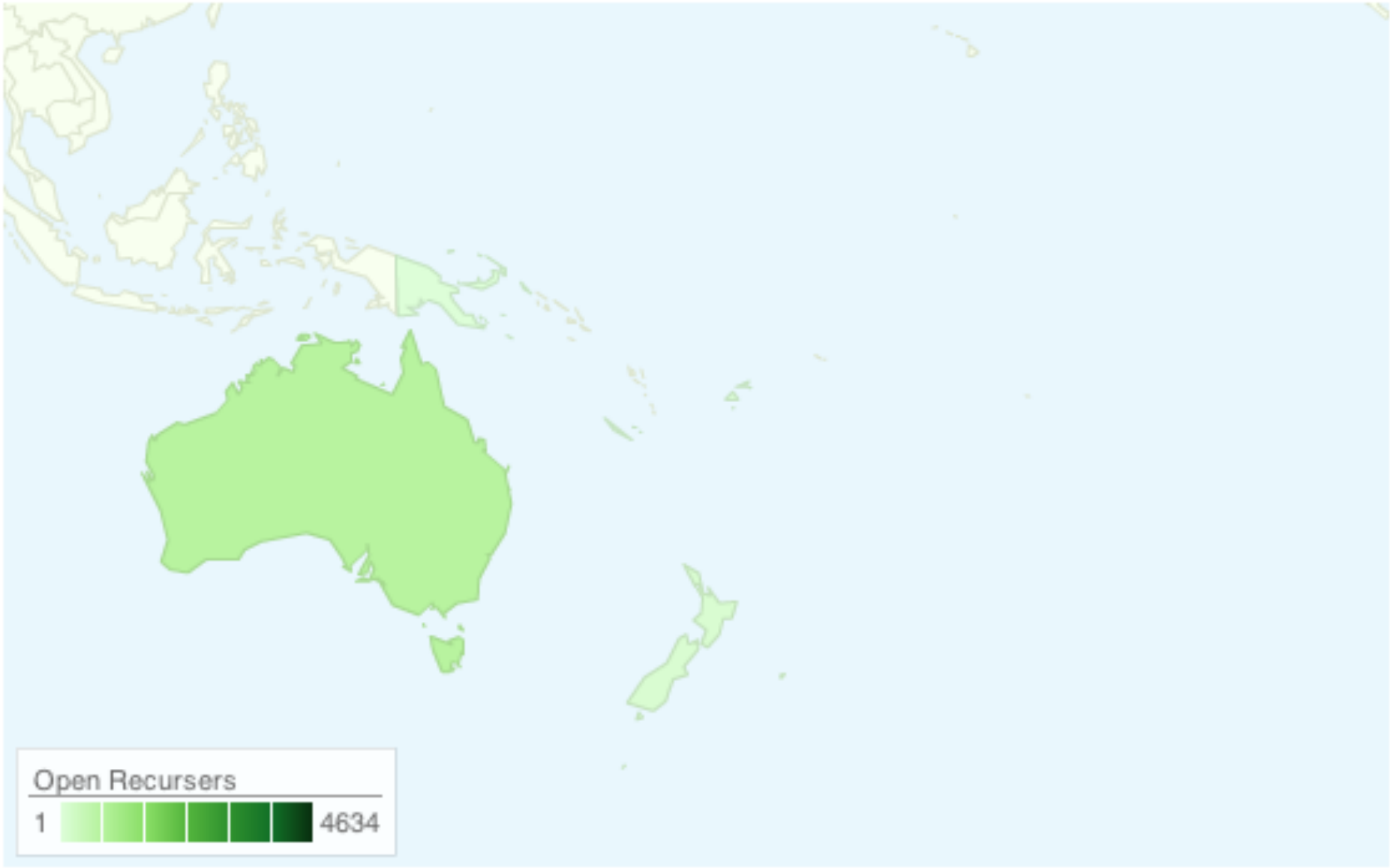
Where are the open Recursors?



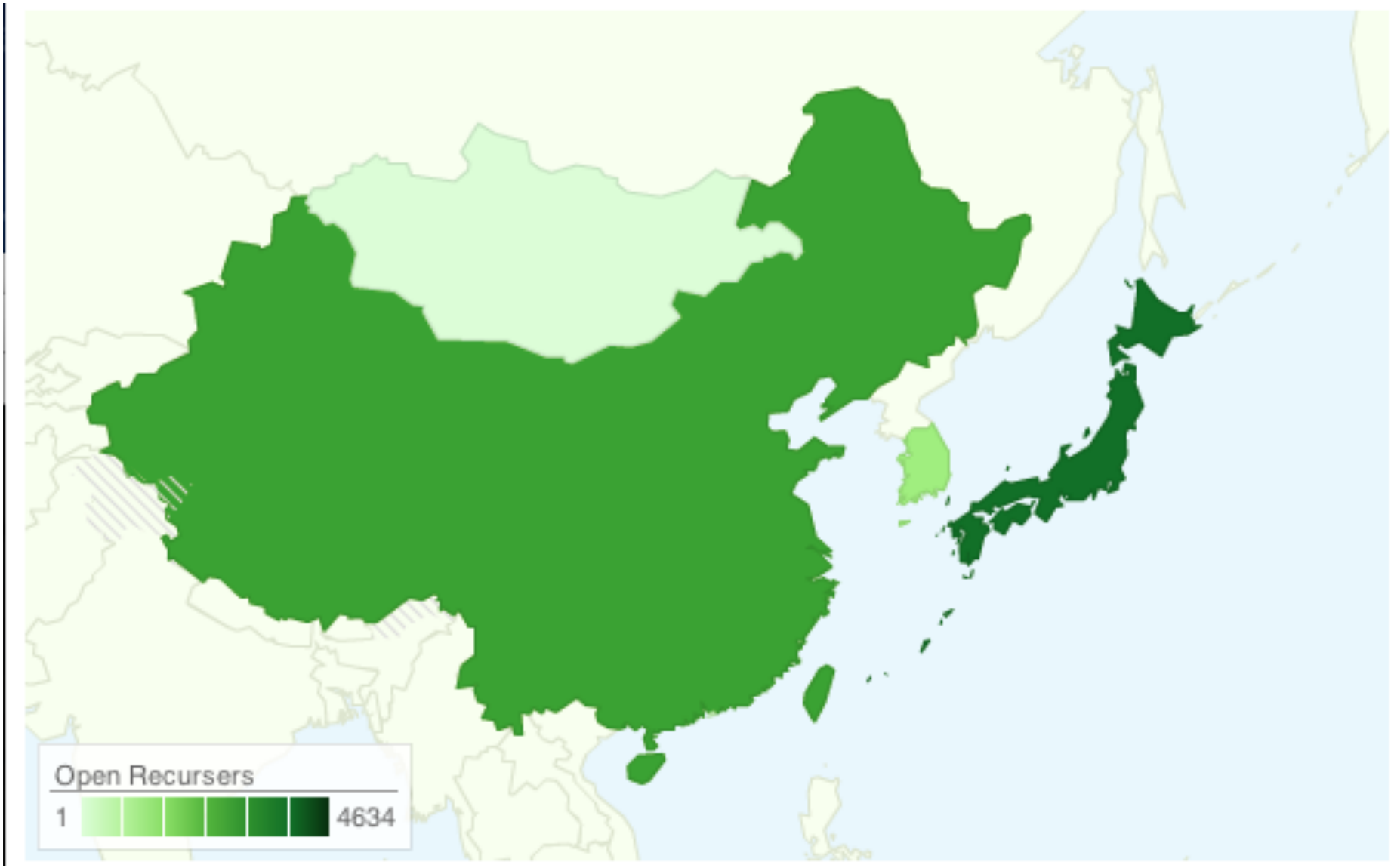
Where are the open Recursors?



Where are the open Recursors?



Where are the open Recursors?



Where are the open Recursors?

Country	Open Recursors		Country	Open Recursors
Japan	4625		Bangladesh	103
China	3123		New Zealand	98
Taiwan	3074		Cambodia	13
South Korea	1410		Sri Lanka	7
India	1119		Nepal	7
Pakistan	1099		Mongolia	5
Australia	761		Laos	4
Thailand	656		Bhutan	2
Malaysia	529		New Caledonia	2
Hong Kong	435		Fiji	2
Indonesia	349		Maldives	2
Vietnam	342		Papua New Guinea	1
Philippines	151		Afghanistan	1
Singapore	118			

Where are the open Recursors?

Some Networks:

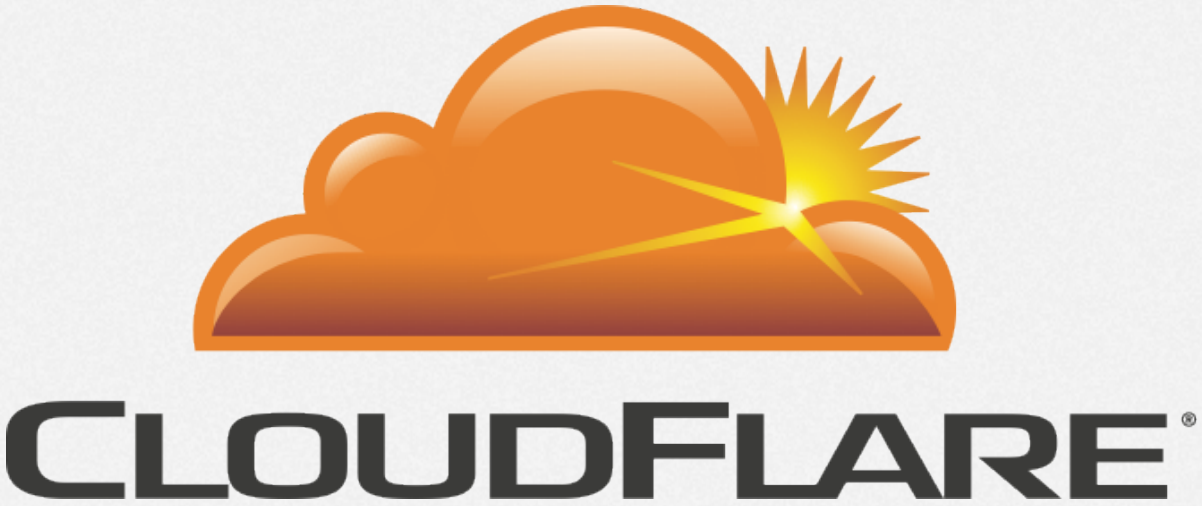
Country	ASN	Network Name	Open Recursors
TW	3462	HINET Data Communication Business Group	2416
CN	9394	CRNET CHINA RAILWAY Internet(CRNET)	1052
JP	4713	OCN NTT Communications Corporation	1044
PK	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	1030
CN	4134	CHINANET-BACKBONE No.31,Jin-rong Street	851
JP	2514	INFOSPHERE NTT PC Communications, Inc.	542
JP	17506	UCOM UCOM Corp.	378

Where are the open Recursors?

- Where are they running?

Mostly on Servers.

~11,000	Servers profiled from Asia-Pac Networks.
~7,500	BIND
~1600	unknown / undetermined
~900	Microsoft DNS Server
~500	dnsmasq
~200	ZyWALL DNS (a consumer internet router)



How to fix this?

Fixing this?

Preventative Measures!

- BCP-38
  - Source Filtering.
  - You shouldn't be able to spoof addresses.
  - Needs to be done in hosting and ISP environments.
  - If the victim's IP can't be spoofed the attack will stop
  - Will also help stop other attack types
    - (eg: Spoofed Syn Flood).

Fixing this?

Preventative Measures!

- DNS Server Maintenance
  - Secure the servers!
    - Lock down recursion to your own IP addresses
  - Disable recursion
    - If the servers only purpose is authoritative DNS, disable recursion
  - Turn them off!
    - Some Packages (eg, Plesk, cPanel) have included a recursive DNS server on by default.

Fixing this?

Consumer Internet Routers / Modems

- Update firmware.
  - Some older firmware has security bugs
    - Allows administration from WAN (including DNS, SNMP)

- Does the feature need to be on?
    - Make sure its set up properly

Fixing this?

Information

- BCP-38:

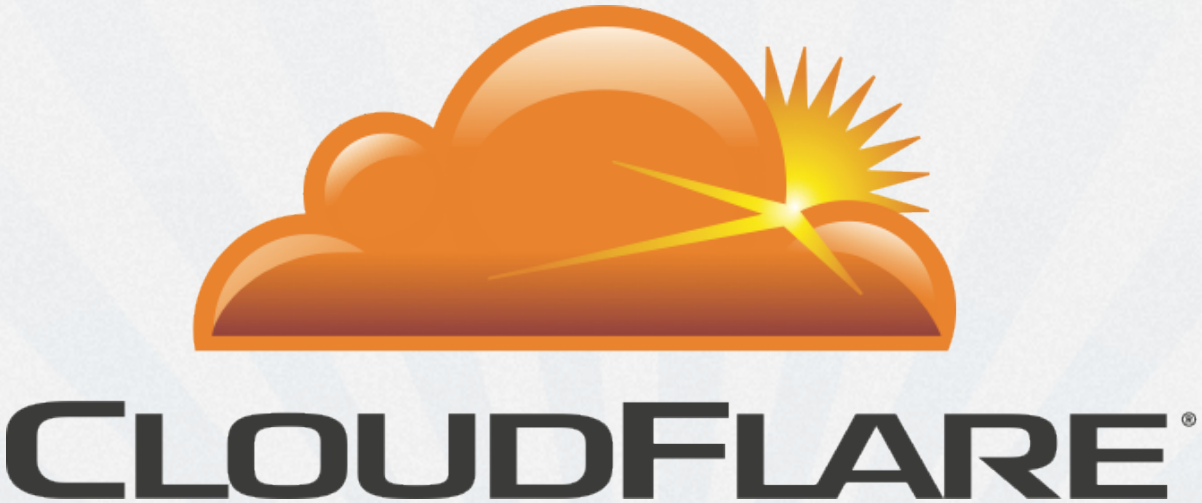
http://tools.ietf.org/html/bcp38

- BIND:

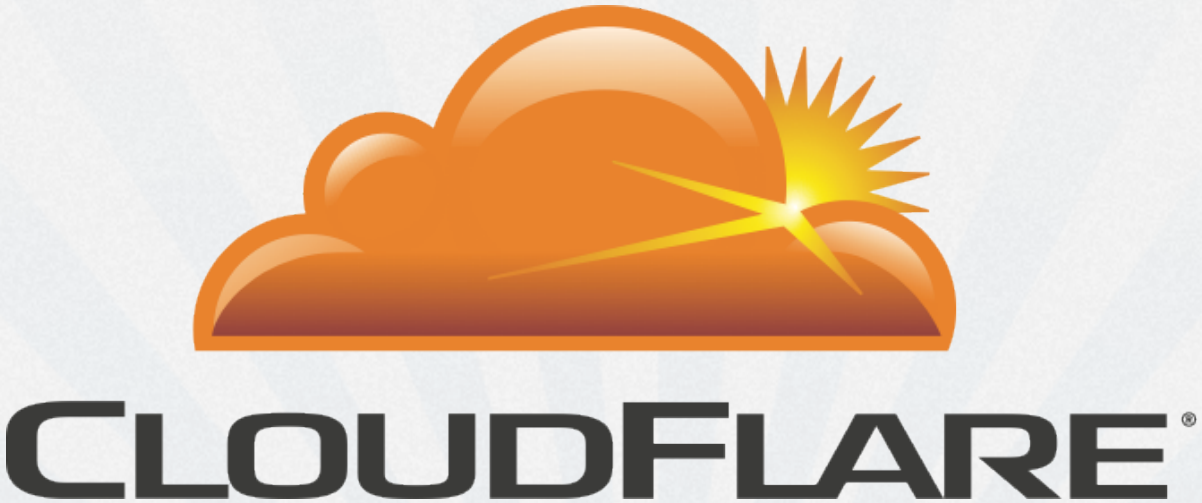
http://www.team-cymru.org/Services/Resolvers/instructions.html

- Microsoft:

http://technet.microsoft.com/en-us/library/cc770432.aspx



Questions?



Thank You