DNS Amplification – Are YOU Part of the Problem?

(RIPE66 – Dublin, Ireland - May 13, 2013)

Merike Kaeo

Security Evangelist, Internet Identity

merike@internetidentity.com

INTRO

- Statistics on DNS Amplification Attacks in 2012/2013
- March / April Measurements on Open Recursive Resolvers
- How To Close Open Recursive Resolvers
- What Other Basic Network Hygiene Can Help?

DNS AMPLIFICATION ATTACK – WHAT IS IT?

Attacker sends a small request with the expectation of invoking a much larger response

Open Resolver

Unfortunate Target

(4) Open resolvers send DNS response to target name server

(1) Attack traffic sends DNS query for record “malicious record” in domain “bad.<tld>” to open recursive servers and set source IP to <target IP address>

(2) Open resolver asks authoritative bad.<tld> for record “malicious record”

Authoritative bad.<tld>

(3) Authoritative bad.<tld> responds with record “malicious record”

GROWING TRENDS

- Reflective DDoS attacks use IP addresses of legitimate users
- Combining spoofed addresses with legitimate protocol use makes mitigation extremely difficult – what do you block and where?
- Recent trends have been utilizing DNS as attack vector since it is a fundamentally used Internet technology
  - Exploit unmanaged open recursive resolvers
  - Exploit large response profile to some standard queries (DNSSEC)
- Utilize resources of large hosting providers for added attack bandwidth
- Many other Internet protocols also susceptible

HOW BAD IS THE PROBLEM?

Largest in 2012

Event Time Start: Aug 1, 2012 00:33:00 UTC

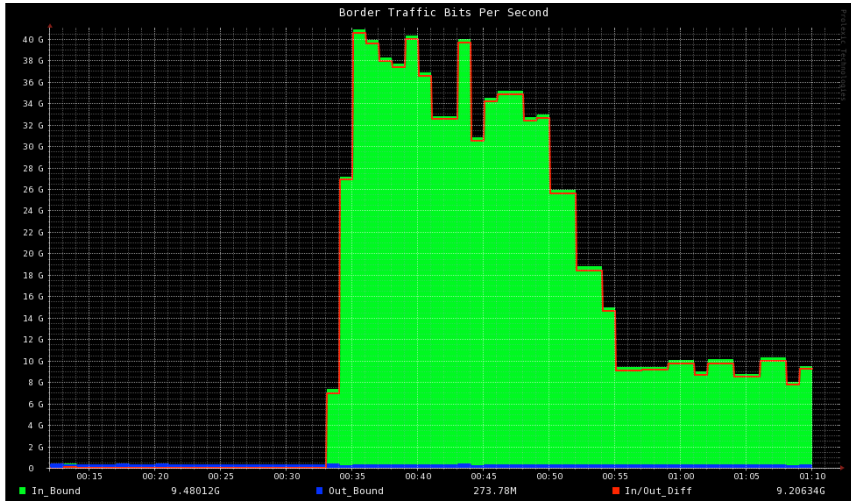
Attack Types: DNS Flood, GET Flood, UDP Fragment Flood, ICMP Flood

Destination Ports: 80,443,53

Industry Vertical: Financial

Peak Bandwidth: **42.2 Gbps**

Peak pps: **2.1 Mpps**



Source: Prolexic

"Trending data points to an increase of DNS attacks that can be observed in the comparison of Q1 2012 (2.50 percent), Q4 2012 (4.67 percent), and Q1 2013 (6.97 percent). This represents an increase of over 200 percent in the last year."

Source: Prolexic Quarterly Global DDoS Attack Report Q1 2013

WHY DOES THE DNS AMPLIFICATION WORK SO WELL?

- Victims cannot see actual originator of attack
  - Lots of DNS packets from a wide variety of ‘real’ DNS servers
  - Victims cannot block the BotNet making the spoofed queries
- DNS servers are answering seemingly normal requests
- Originating ISPs aren’t impacted
- Originating ISPs only see small amounts of traffic
- Filtering attack traffic is difficult in practice
  - The open resolvers are themselves not infected not malicious
  - Depending on architecture, may block legitimate traffic

WHY WOULD PEOPLE RUN OPEN RESOLVERS?

- Deliberate Services
  - Google, OpenDNS, DynDNS, Amazon Route53
  - Ensure reliability and stability
- Many are not deliberate – why do they exist?
  - Evil DNS servers run by criminals on bulletproof hosts
  - Everyone else

    Hosting companies

    Small/medium ISPs

    Enterprises, SMBs

    Default device configuration

WHAT NEEDS TO BE DONE

- Ensure no **unmanaged** open recursive resolvers exist
  - Equipment vendors need ship default as CLOSED
  - BCPs should **not** show recursive resolver configurations as open
- Get everyone to participate in stopping ability to spoof IP addresses
  - ISPs need to do ingress filtering (BCP38/BCP84)
  - Enterprises/SMBs need to implement egress filters
  - Equipment vendors need to have better defaults for helping alleviate spoofing
- Sponsoring research/studies to get definitive data on where IP address spoofing is possible may help
  - MIT Spoofer Project (http://spoofer.csail.mit.edu)

PROJECTS THAT HELP DETERMINE OPEN RESOLVERS

- Measurement Factory
  - http://dns.measurement-factory.com/surveys/openresolvers.html
  - has been running tests for open recursive resolvers since 2006
  - have daily reports of open resolvers per AS number
  - send DNS query to a target IP address for a name in test.openresolver.org domain (target IP addresses tested no more than once every three days)
- The Open Resolver project
  - http://openresolverproject.org
  - started in March 2013
  - active scans run on a weekly basis that get some added information

THE MEASUREMENT FACTORY

DNS SURVEY: OPEN RESOLVERS

ABOUT

We have an ongoing survey that looks for open DNS resolvers. A DNS resolver is *open* if it provides recursive name resolution for clients outside of its administrative domain. Open DNS resolvers are a bad idea for a few reasons:

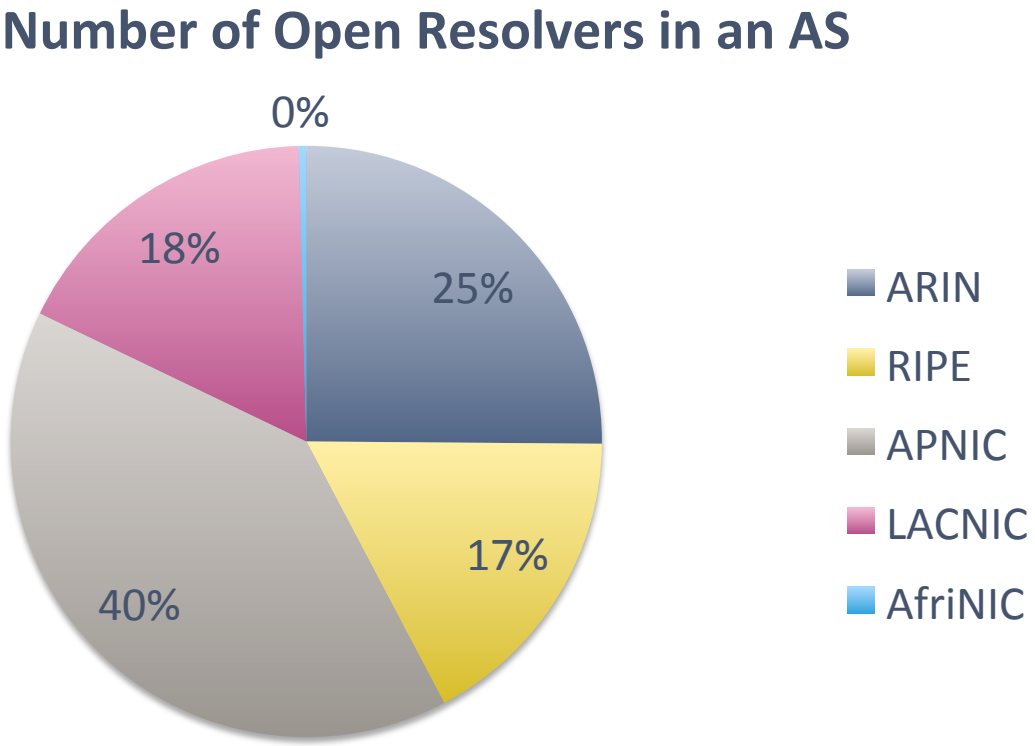
- They allow outsiders to consume resources that do not belong to them.
- Attackers may be able to poison the cache of an open resolver.
- Open resolvers are being used in widespread DDoS attacks with spoofed source addresses and large DNS reply messages.

As with open SMTP relays, open DNS resolvers are now being abused by miscreants to further pollute the Internet.

[On main page go to 'Results' then 'DNS survey results' and finally 'Open Resolvers']

MEASUREMENT FACTORY DATA

- Data from May 7, 2013 that show worst offenders of open recursive resolvers from measurement factory.
- Summary of data that listed open resolvers per AS – the first 100 with the most open resolvers listed



http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/

Open DNS Resolver Project

Open Recursive Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from Smurf attacks commonly seen in the late 1990s.

We have collected a list of 27,200,613 resolvers that respond to queries in some fashion. 25.2 million of these pose a significant threat (as of 07-APR-2013). Detailed History and Breakdown

Check my IP space

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /24 will be rejected): 199.106.166.22

hilbert curve heatmap of 20130414 data heatmap archive

What can I do?

If you operate a DNS server, please check the settings.

Recursive servers should be restricted to your enterprise or customer IP ranges to prevent abuse. Directions on securing BIND and Microsoft nameservers can be found on the Team CYMRU Website

Authoritative servers should not offer recursion, but can still be used in an attack. Configure your Authoritative DNS servers to use DNS RRL [Response Rate Limiting] Knot DNS and NLNetLabs NSD include this as a standard option now. BIND requires a patch.

Prevent spoofing on your network!

Configure BCP-38 on all CPE and Datacenter equipment edges that have fixed IP ranges. This could be as simple as setting ip verify unicast source reachable-via rx on a router interface. Any staticly routed customer should receive this setting by default.

If you are in the security community:

Please contact dns-scan /at/ puck.nether.net or if you know the host owner, engage him for access to raw data.

Additional Information

Informações em Português

We can provide you a List of Open Resolvers by ASN if you e-mail dns-scan /at/ puck.nether.net

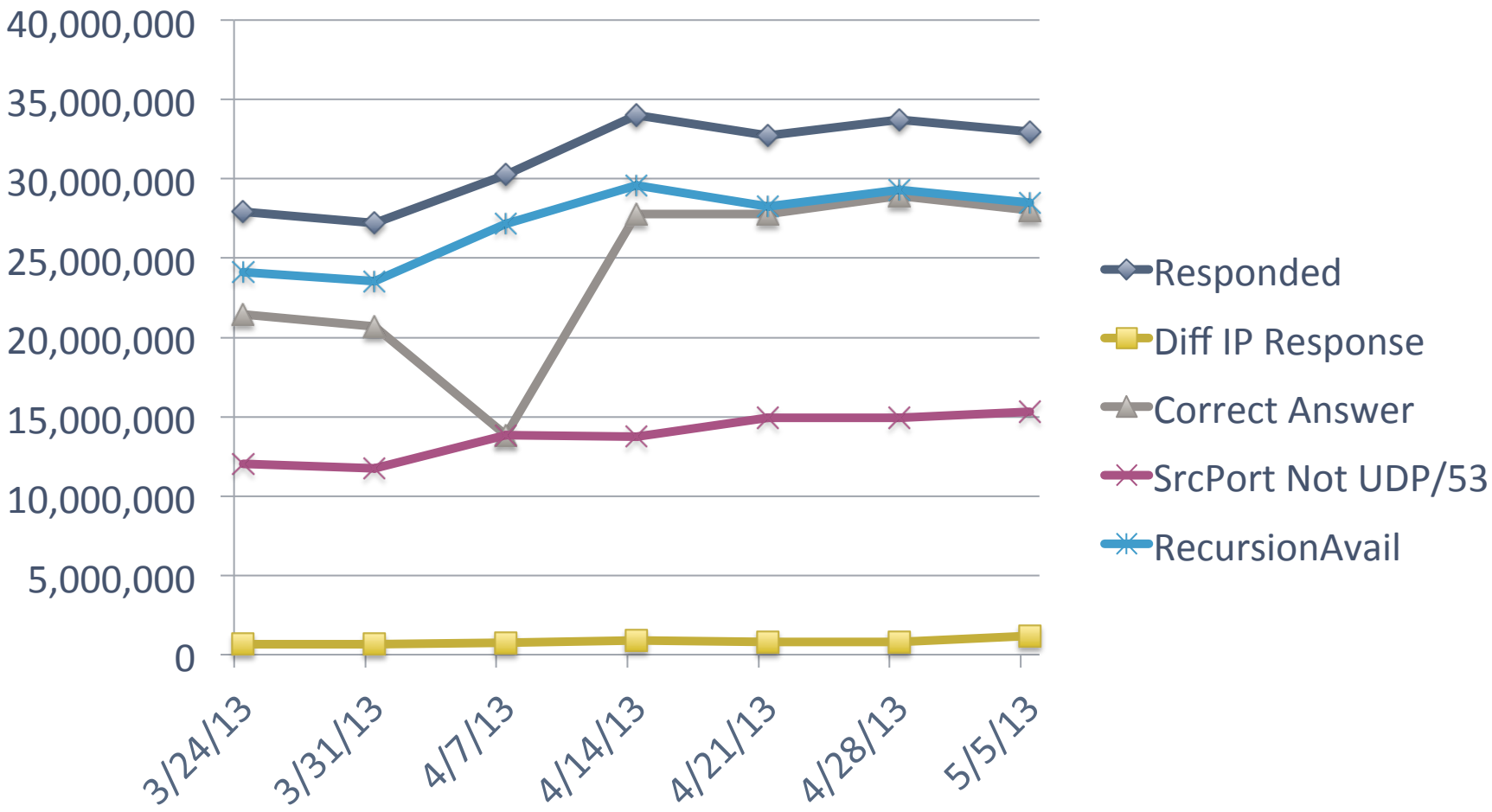
Test your IP Now!

DNS DDoS and Security in the News

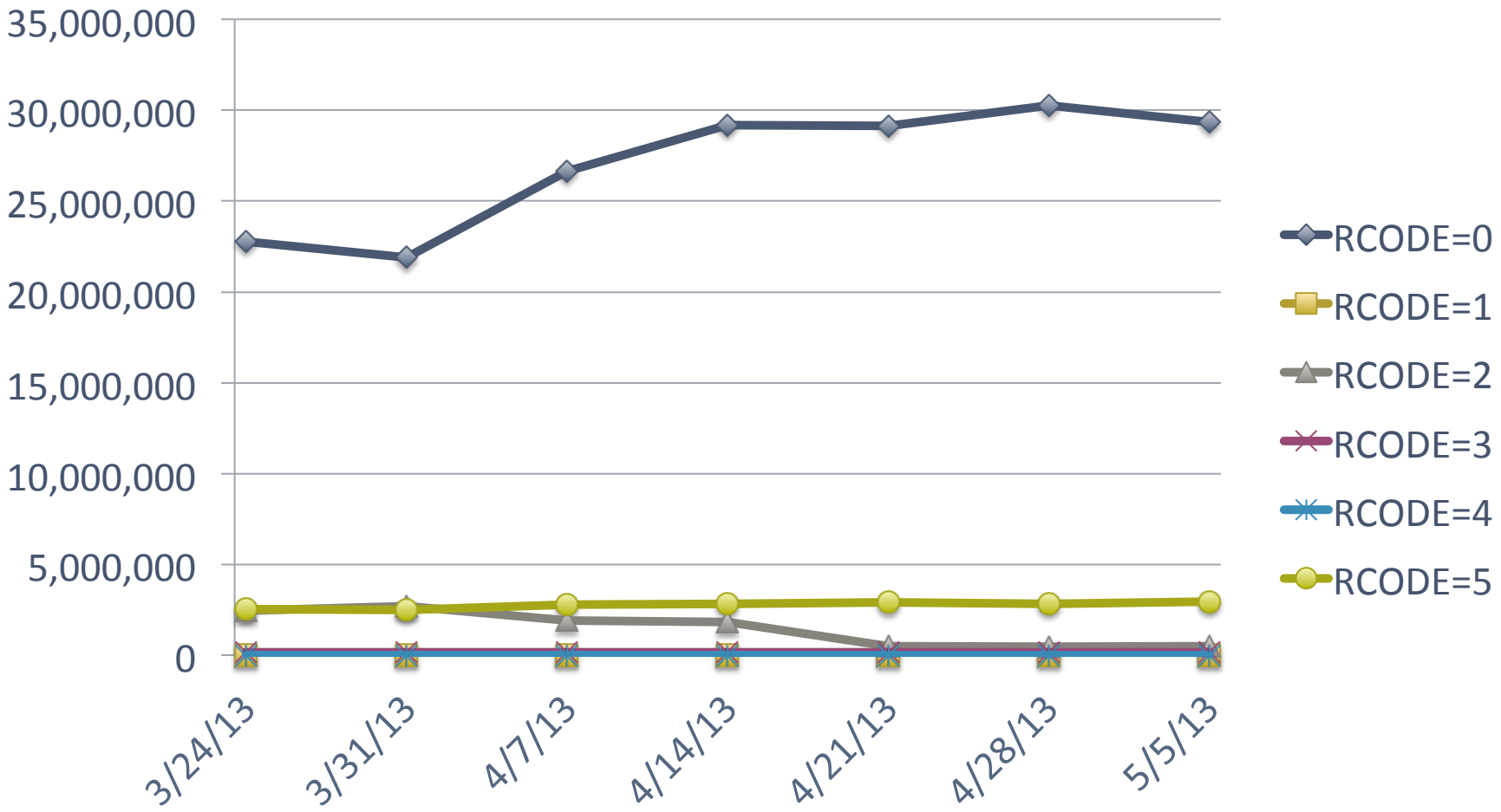
- 04-APR-2013 Spamhaus DDoS was just a warning shot
- 30-MAR-2013 How the Cyberattack on Spamhaus Unfolded
- 28-MAR-2013 Is Your DNS Server part of a criminal conspiracy?
- 20-MAR-2013 75Gb/s DDoS against Cloudflare

We hope to present the data at a future conference, and share it with the broader security community.

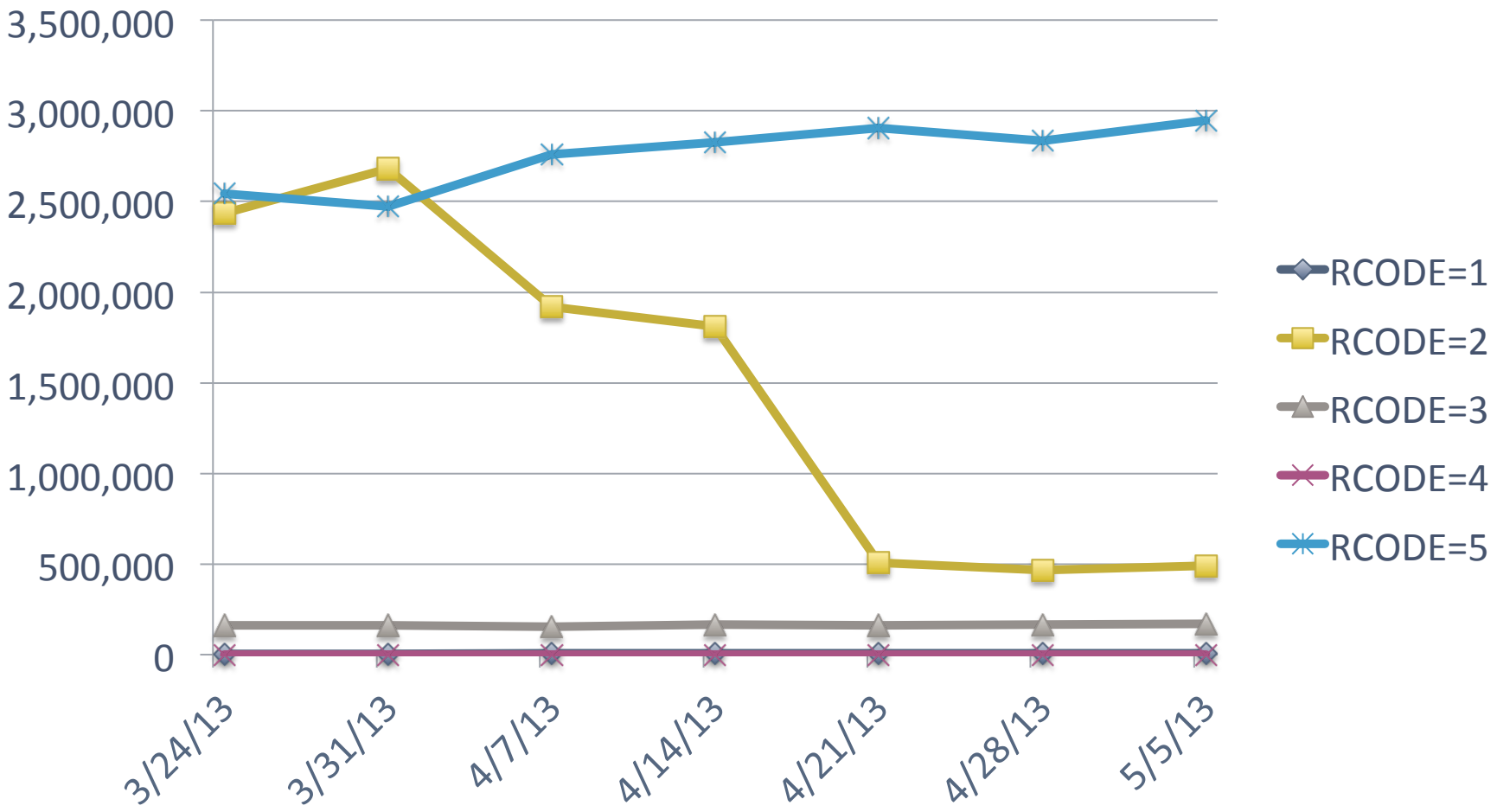
OPEN RECURSIVE RESOLVER PROJECT STATS



OPEN RECURSIVE RESOLVER PROJECT RCODE STATS



OPEN RECURSIVE RESOLVER PROJECT RCODE STATS(2)



CLOSING RECURSIVE RESOLVERS

- RFC 5358 (BCP 140): Preventing Use of Recursive Nameservers in Reflector Attacks
  - http://www.ietf.org/rfc/rfc5358.txt
- BIND
  - http://www.zytrax.com/books/dns/ch9/close.html
- Team CYMRU
  - Pointers to BIND implementations and Microsoft
  - http://www.team-cymru.org/Services/Resolvers/instructions.html

DNS RESPONSE RATE LIMITING (DBS RRL)

Red Barn

Blogs

Home

Navigation

- Recent posts

User login

Username: *

Password: *

Log in

Request new password

Response Rate Limiting in the Domain Name System (DNS RRL)

This page describes DNS Response Rate Limiting (DNS RRL) which is an experimental feature for domain name servers including CZ-NIC Knot DNS, NLNetLabs NSD, and ISC BIND9.

These patches and instructions pertain to authority name servers or authoritative views. Use of this kind of rate limiting for recursive or hybrid servers or views is currently unspecified.

Note Well: This is DNS RRL, meant to be implemented in many different name servers, it is not a BIND specific feature even though BIND was the first name server for which DNS RRL was implemented. DNS RRL will eventually be submitted to the IETF for standardization work. The need for DNS RRL is immediate and pressing, and the IETF processing of this work was therefore planned to come last rather than first.

References:

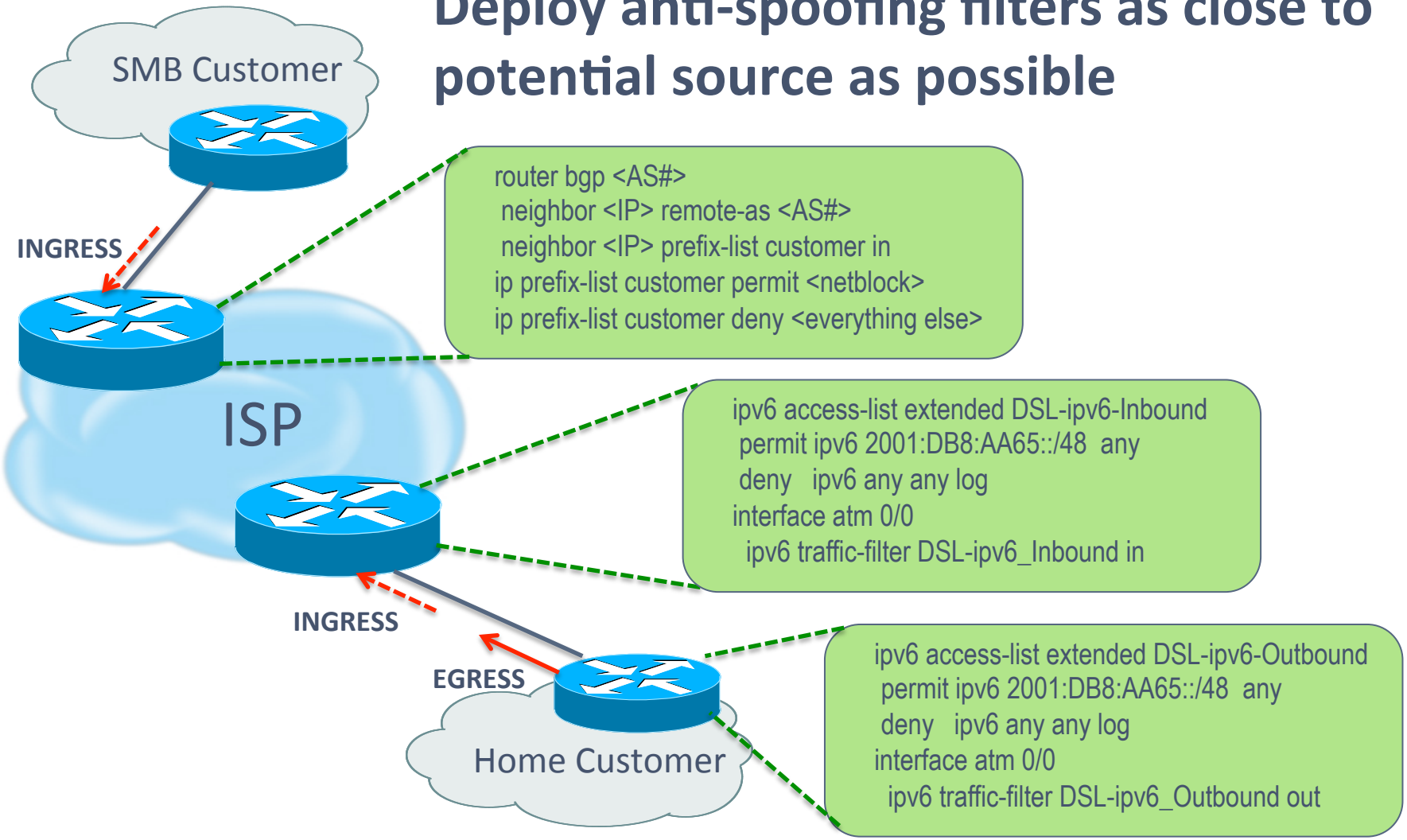
- **Red Hat Enterprise Linux update for RRL in BIND**
- **Release notes** for **CZ-NIC Knot DNS**, available as a standard Knot feature as of Version 1.2-RC3, released 2013-03-01

http://www.redbarn.org/dns/ratelimits

WHAT OTHER BASIC NETWORK HYGIENE HELPS?

- Ingress Filtering (BCP38/BCP84)
  - Using simple filters
  - Using uRPF
    - http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_unicast_rpf.html
    - http://www.juniper.net/techpubs/en_US/junos9.4/topics/concept/unicast-rpf-ex-series.html
    - https://tools.ietf.org/html/draft-savola-bcp84-urpf-experiences-03
- Transit Route Filters
- Peering Route Filters
- IX Specific
  - Set next-hop self on border routers
  - Do not redistribute connected routes into IGP/BGP

Deploy anti-spoofing filters as close to potential source as possible



DON'T BE PART OF THE PROBLEM (PLEASE)

- Test to determine whether you have unmanaged open resolvers in your environment
  - http://www.thinkbroadband.com/tools/dnscheck.html
  - http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl
- Ensure that you are helping stop spoofed traffic as close to the source as possible
  - You don't need to use uRPF – simple filters work
- Added References:
  - http://www.cisco.com/web/about/security/intelligence/dns-bcp.html
  - https://devcentral.f5.com/tech-tips/articles/building-a-resilient-secure-dns-infrastructure#.UYij55USM_U

Questions ?