NZRS
an InternetNZ company

Two years of zone scans

Daniel Griggs, NZRS
Prepared by Sebastian Castro, NZRS
Registrar Conference 2015

Introduction

- Zone scan started on Aug 2013
- Runs monthly
- Governed by policy https://nzrs.net.nz/dns/zone-and-web-scanning
- Based on a fork from dnscheck https://github.com/NZRS/dnscheck
- DNS tests for configuration correctness and data gathering

Overview

- Notable examples

  Domain is broken, has lame delegation, has mail server
- Name server status

  Answers UDP, TCP, provides recursion, provides zone transfers
- DNSSEC

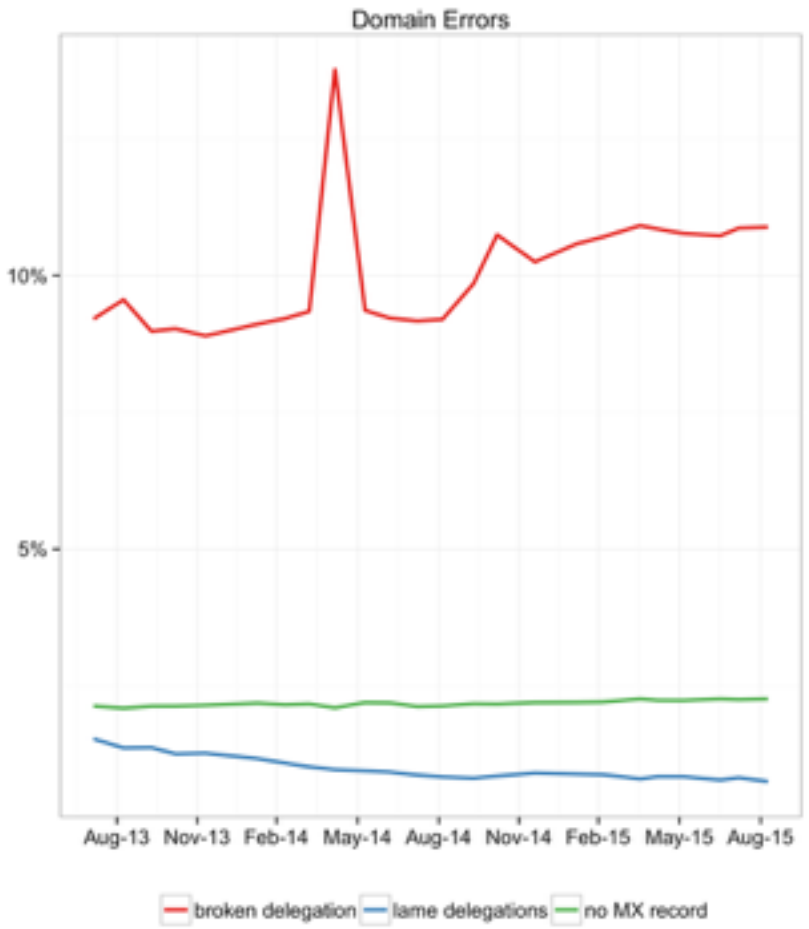
  Detect signed domains, signed delegations, DNSKEY algorithms

Overview

- Servers (web, mail, DNS) addresses
  Enabling topological and geographic redundancy analysis
- TTL distribution by function
  DNS (NS records), Mail (MX records), Web (A, AAAA for ‘www’)
- Other interesting stuff
  Cloud mail servers market share

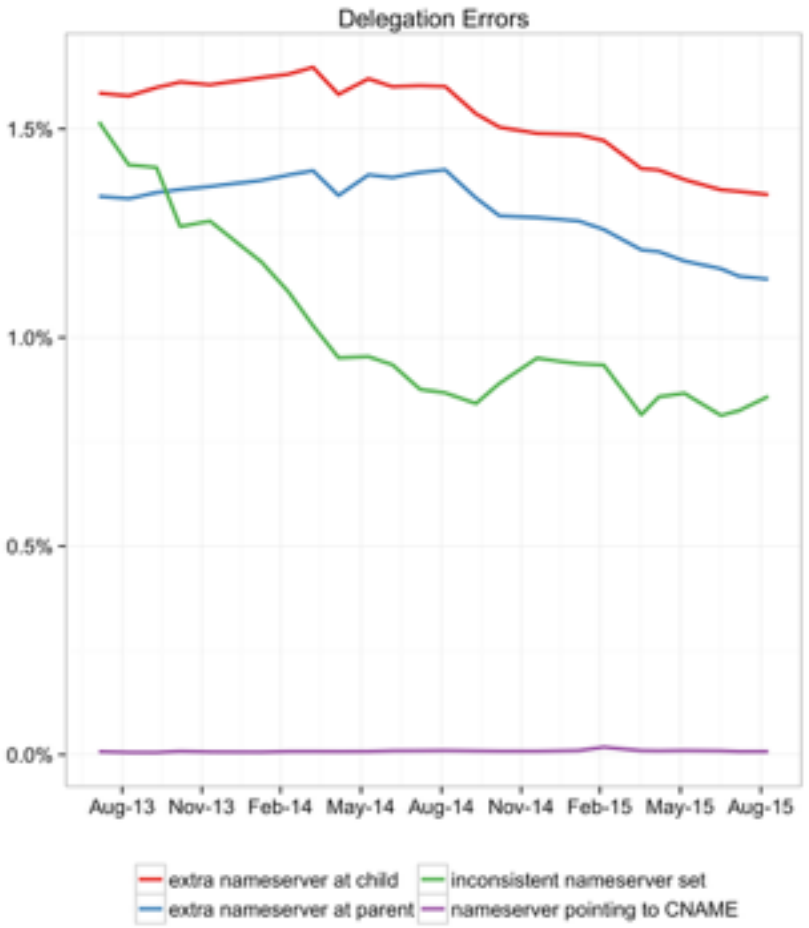
High Level domain errors

- ~10% of active domains are broken
- Lame delegations gradually reduced from 1.5 to 0.8%
- 2% of domains don't have a mail server



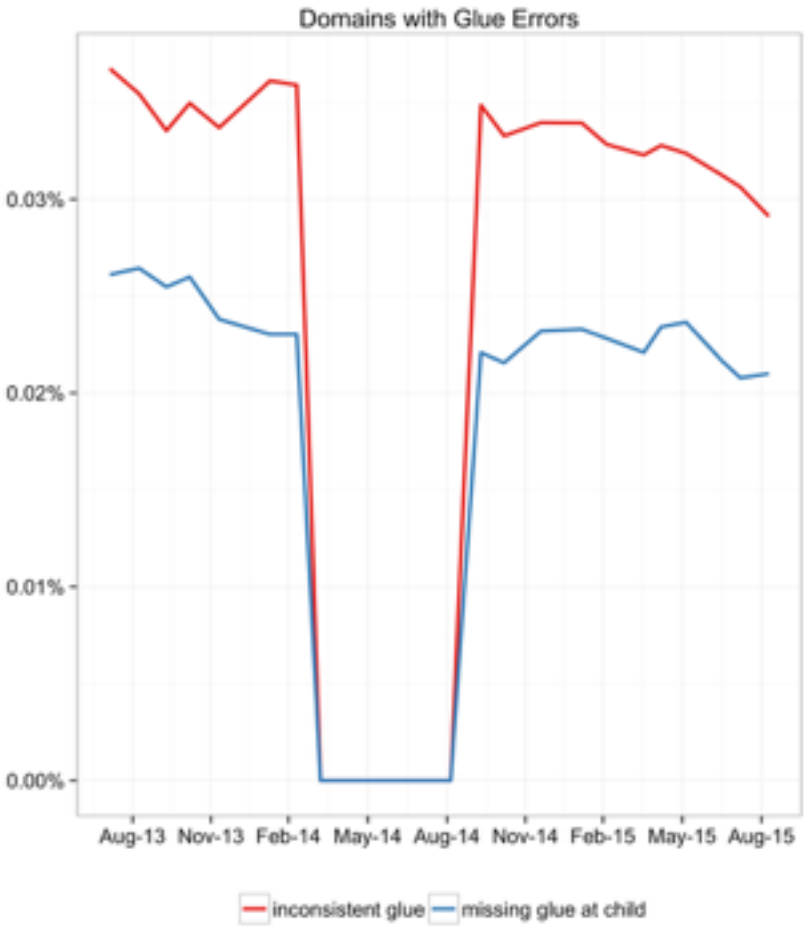
Delegation errors

- Inconsistencies where the NS set at the parent != at the child
  - Extra NS at parent
  - Extra NS at child
  - No match at all
- NS pointing to CNAME
  - Against RFC 1912 2.4



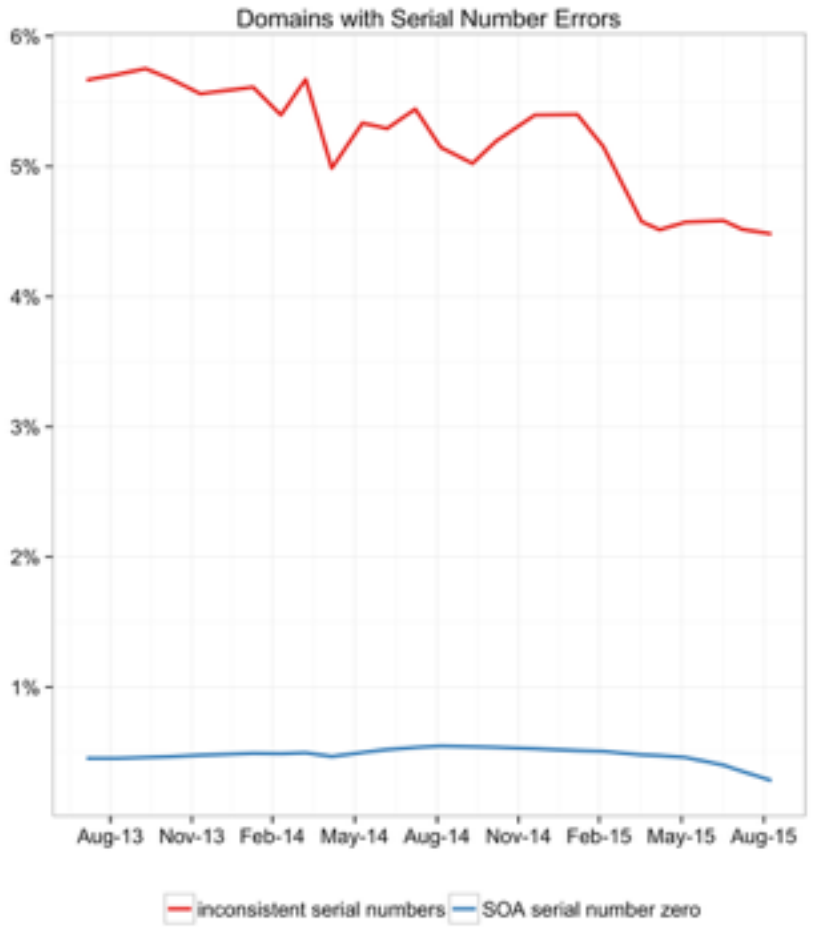
Glue errors

- Glue records
  - A/AAAA records that help untangle the resolution process
- Inconsistent glue
  - Glue at parent != glue at child
- Missing glue
  - Server should return an address, but it didn't



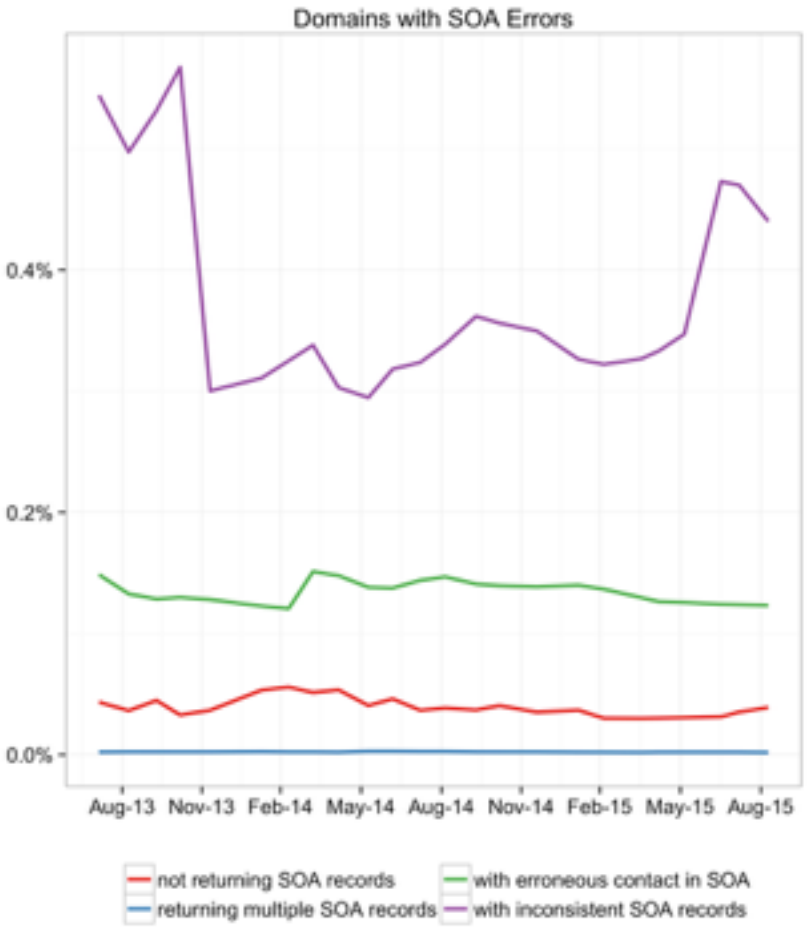
Serial Number Errors

- Serial inconsistency
  - Different nameservers for a domain report different serials
- Serial number zero
  - Self-explanatory
  - It may have an special meaning for BIND



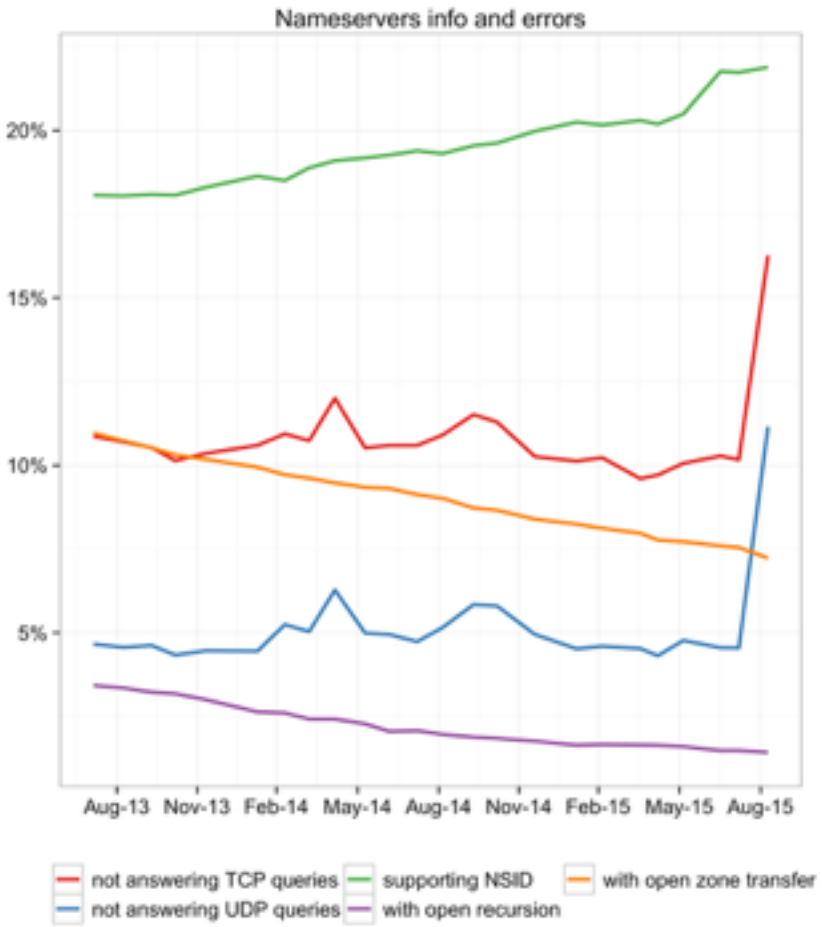
SOA errors

- Not returning SOA
  - No reply to SOA query
- Multiple SOA
  - A query for SOA returns >1 record
- Erroneous contact
  - Written in bad format
- Inconsistent SOA
  - Different servers, different SOA



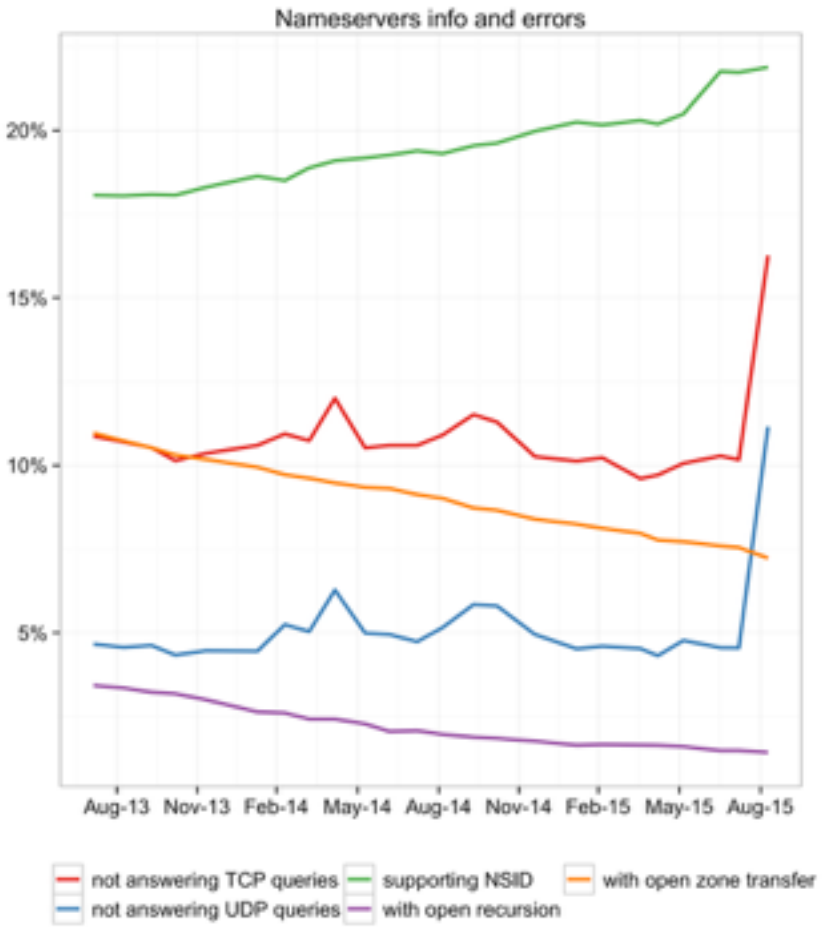
Nameserver errors

- NSID
  - RFC 5001
  - Identification of servers, useful for anycast
  - dig soa nz @ns2.dns.net.nz +nsid
- no TCP
  - Not only for zone transfers!



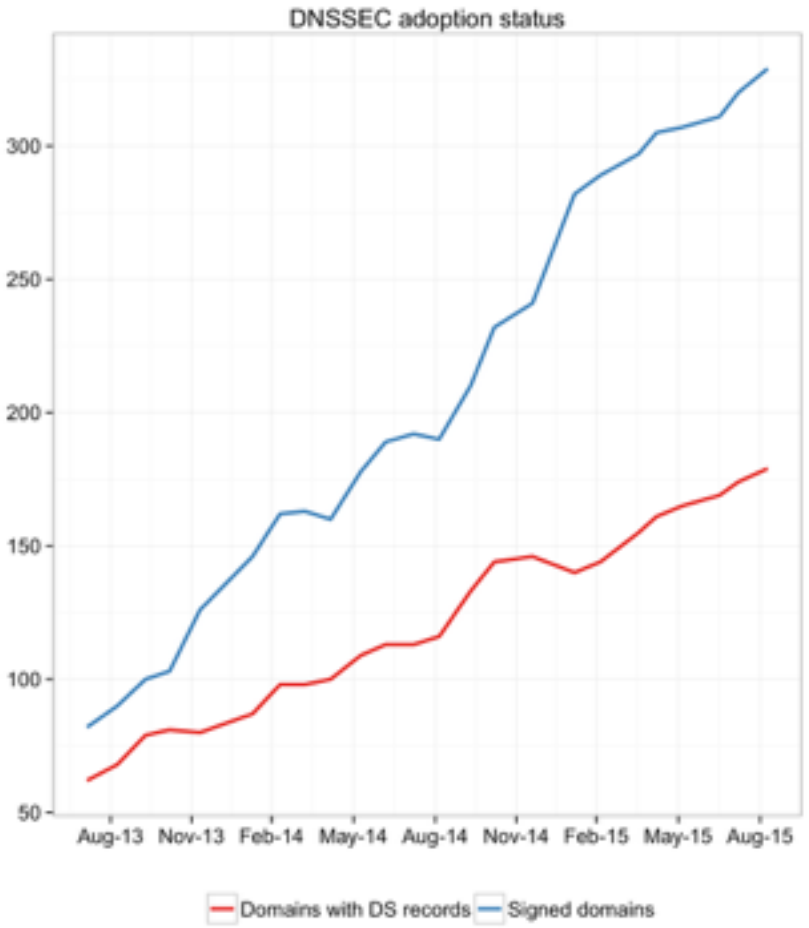
Nameserver errors

- Open recursion
  - Answering queries with RD=1
  - Bad bad idea!
- Open zone transfer
  - Exposing zone data
  - We don't keep it while testing



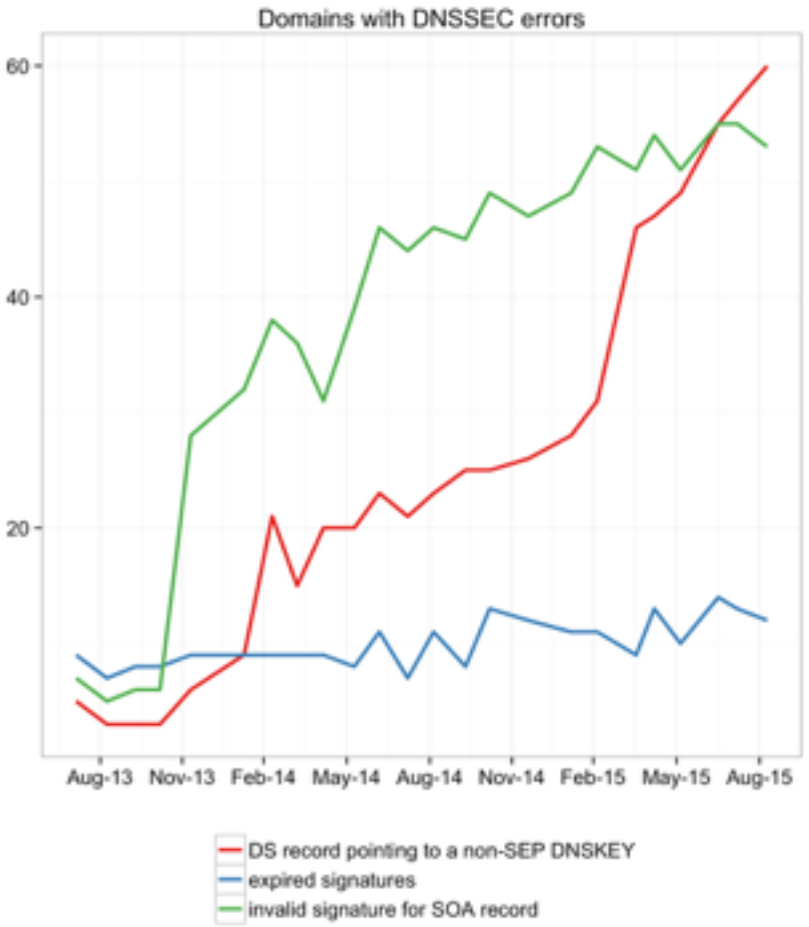
DNSSEC adoption status

- Secure delegation
  - DS record in the parent
  - Requires a registrar with DS support
- Signed domains
  - Has a DNSKEY and signed data for the zone
- Signed is growing faster than secure delegations



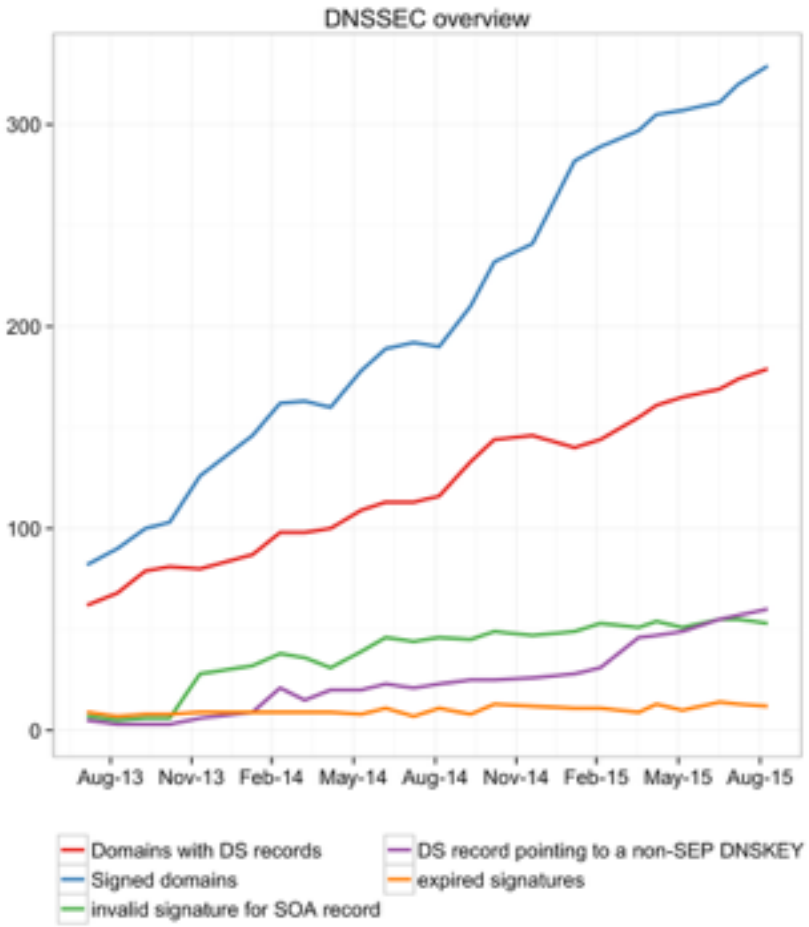
DNSSEC errors

- DNSSEC: Two types of keys
  - KSK
  - ZSK
- DS should point to KSK
- Expired signatures
  - RRSIG has inception and expiration
- Invalid signature
  - Signature fails to validate



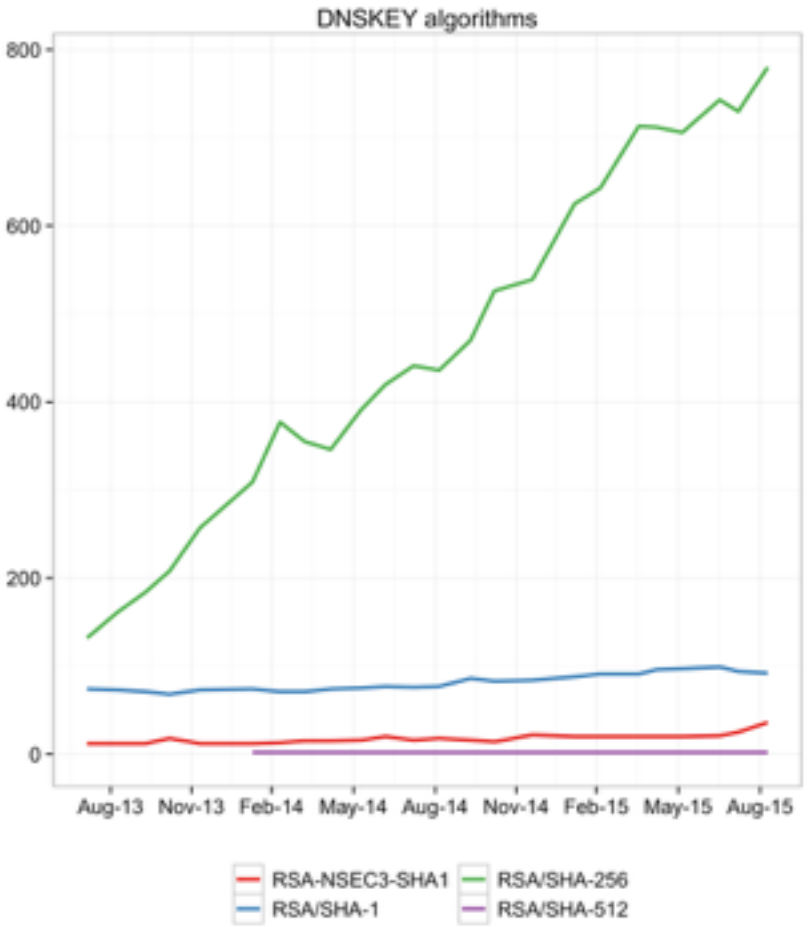
DNSSEC overview

- Errors grow with signed domains
- Very sketchy, we are not doing good
- Secure delegations not growing as fast



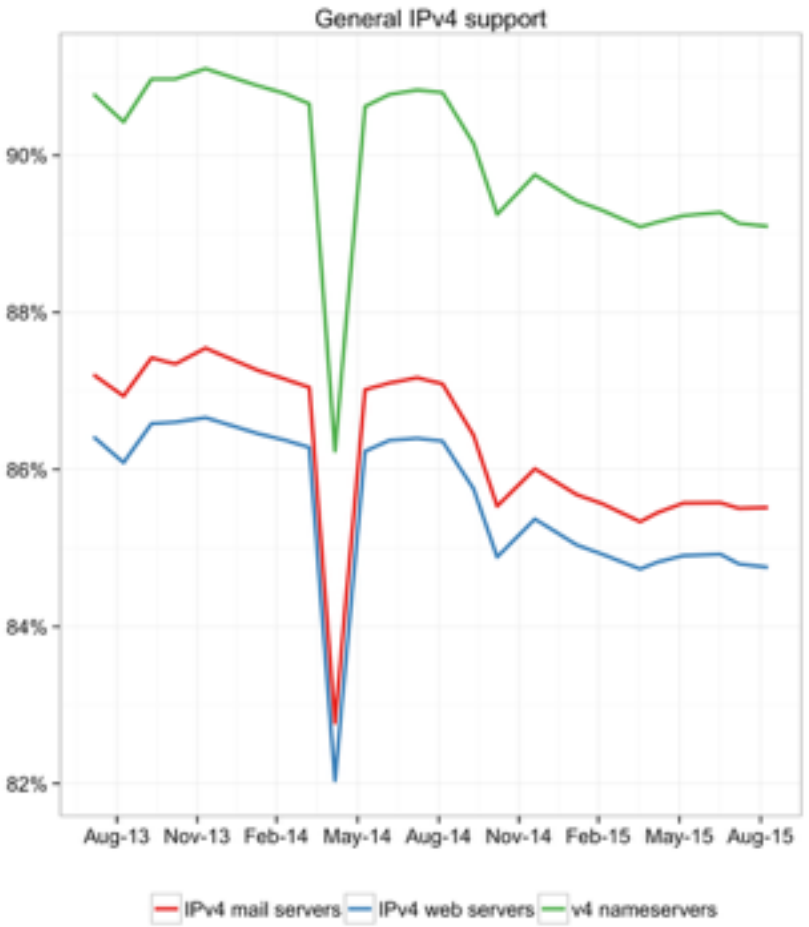
DNSKEY algorithms

- Expected to see new SHA-512
- Reasonable grow of RSA/SHA-256
- No ECDSA or GOST
  - Expected, no surprises
- Missing the key lengths
  - Will be added in the future



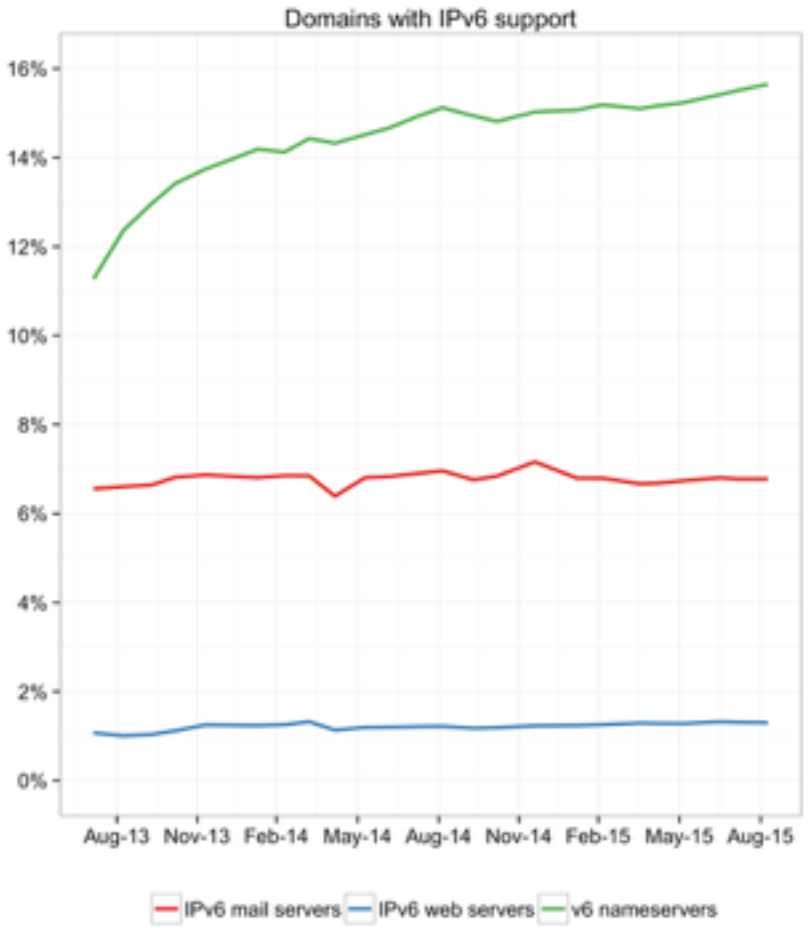
IPv4

- Drop in April 2014 due to collection issue
- Not all domains have v4 NS?
  - Broken domains!
- General decrease of support
  - More protective registrations



IPv6

- Flat as a pancake
- Organic growth at the DNS level due to providers making changes
- Further analysis needed to find where change is produced.

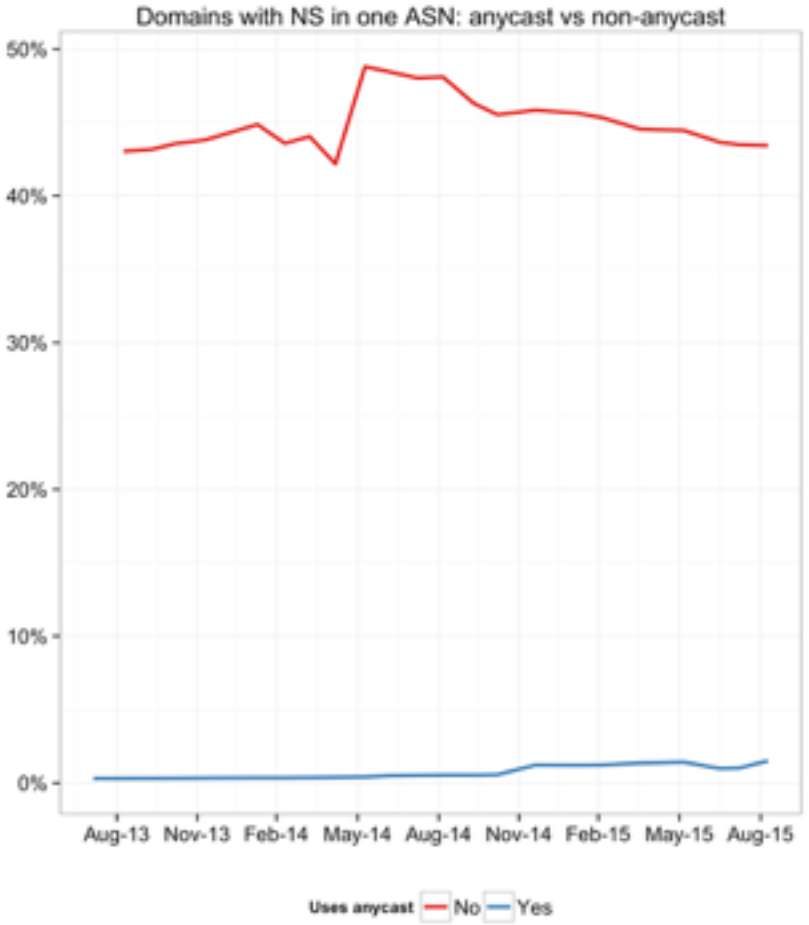


DNS resilience

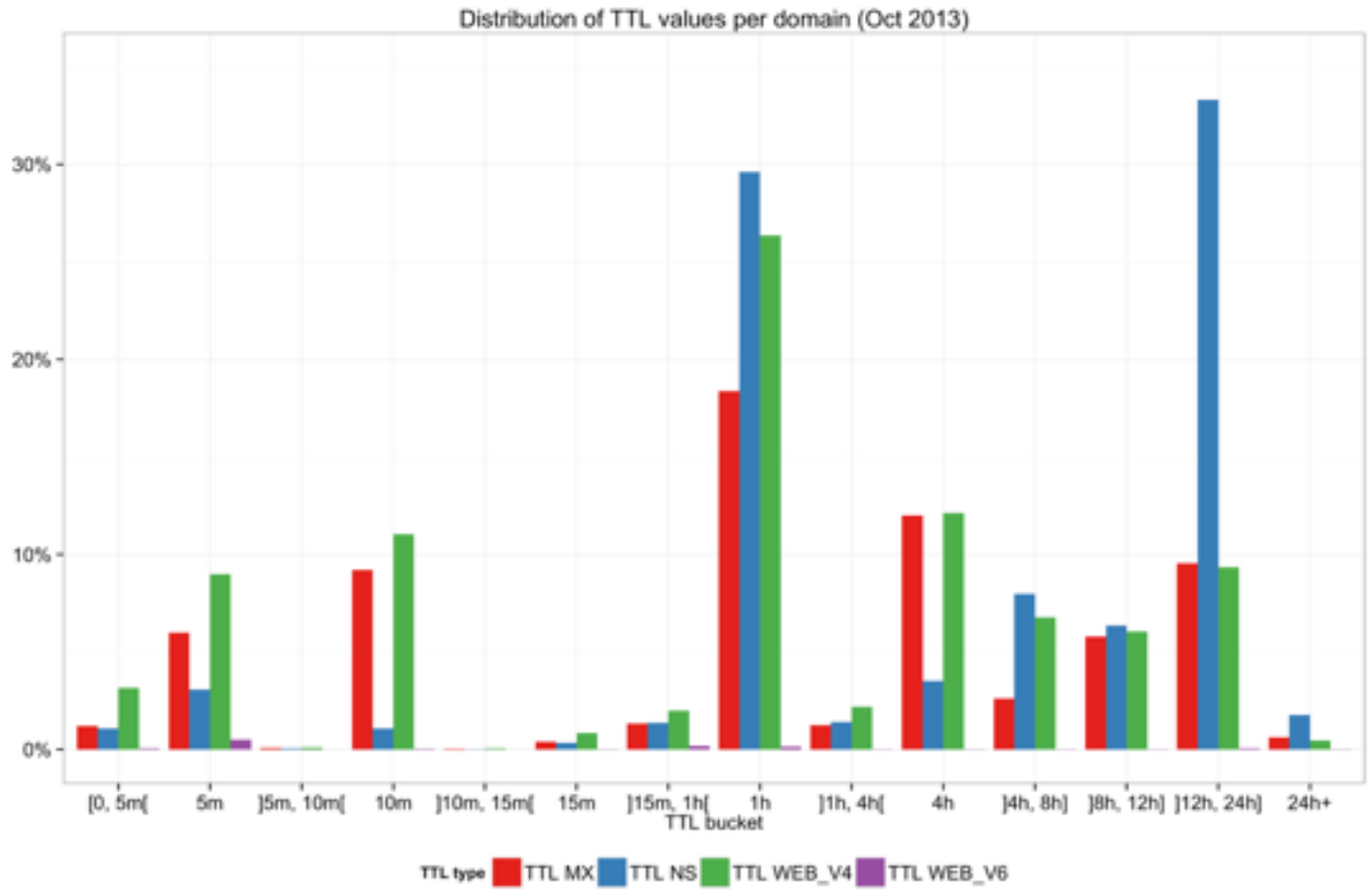
- Most providers have all nameservers in the same AS
- Need to explore network prefix
  - Same prefix as well?
- Nearly half of the registry has poor redundancy
  - Use of anycast?

DNS resilience: anycast

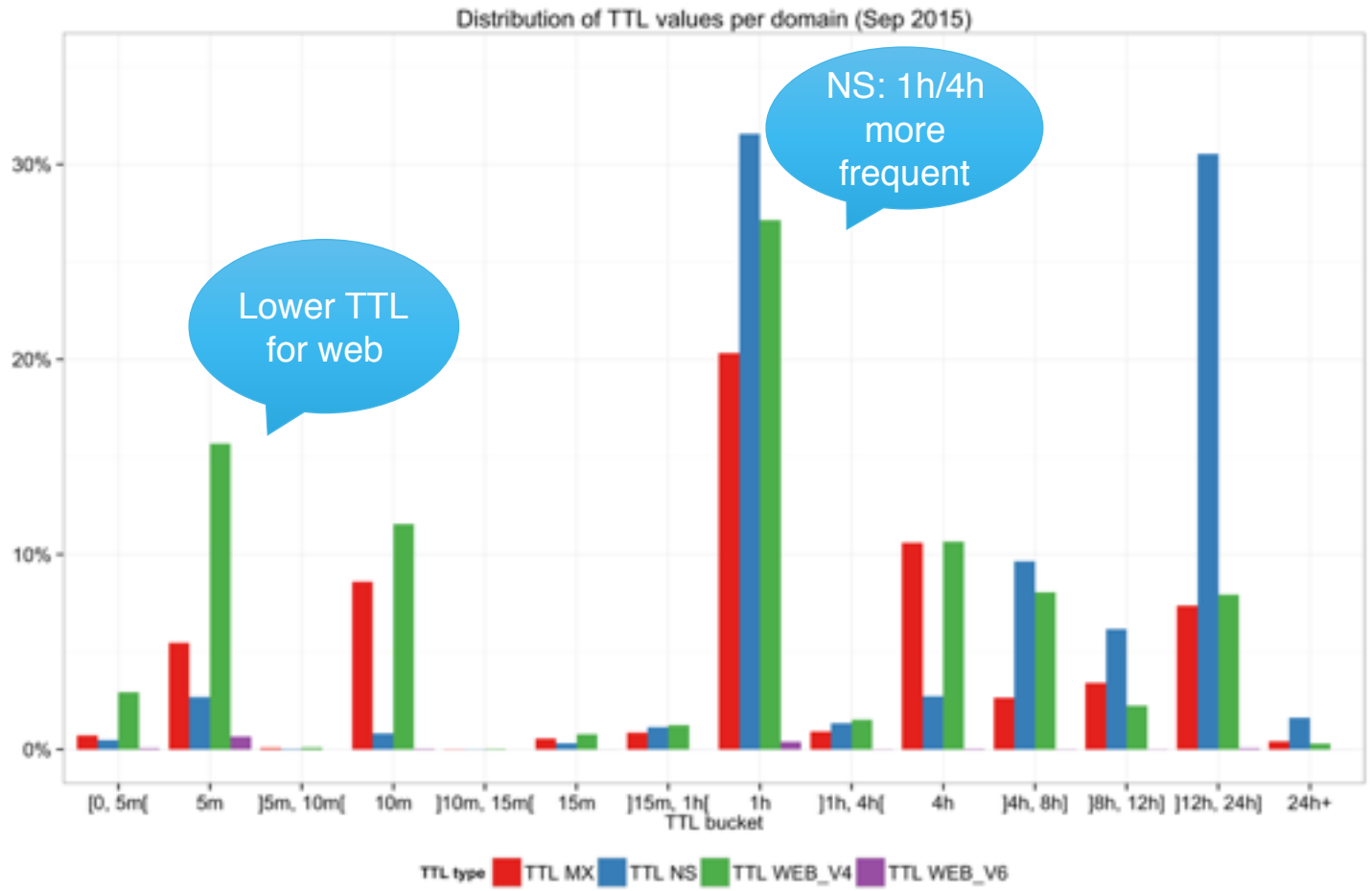
- Does anycast explains lack of redundancy?
  - Mostly no
- Some growth in the past year
- Anycast detection not exhaustive
  - Few hand picked providers



TTL distribution

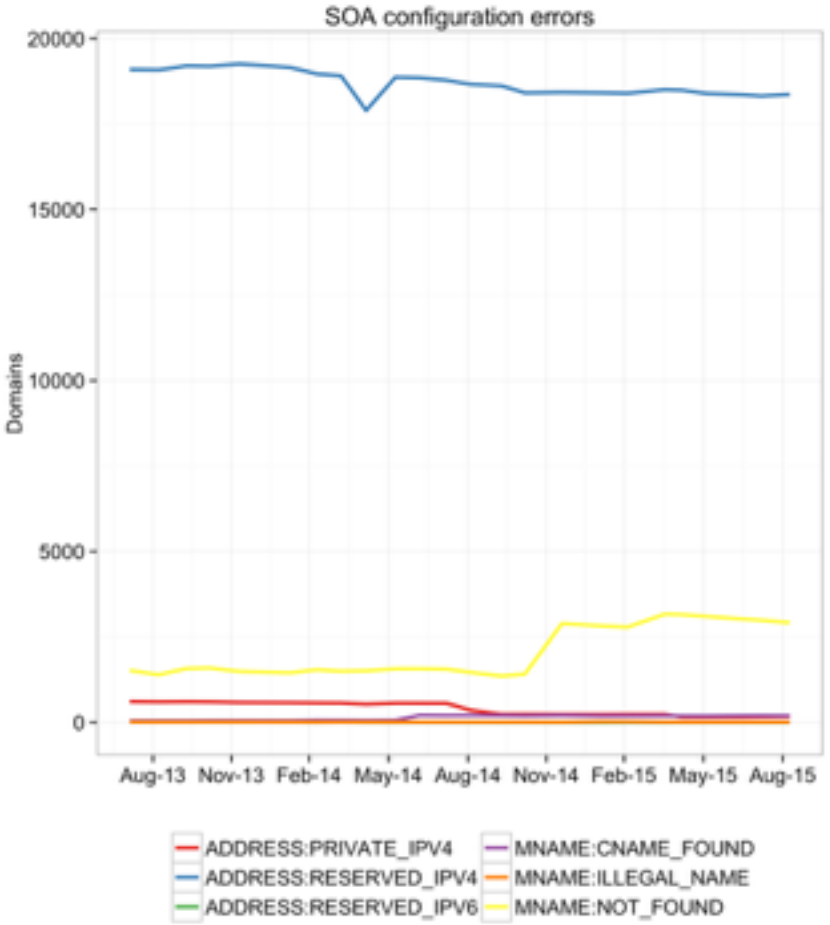


TTL distribution



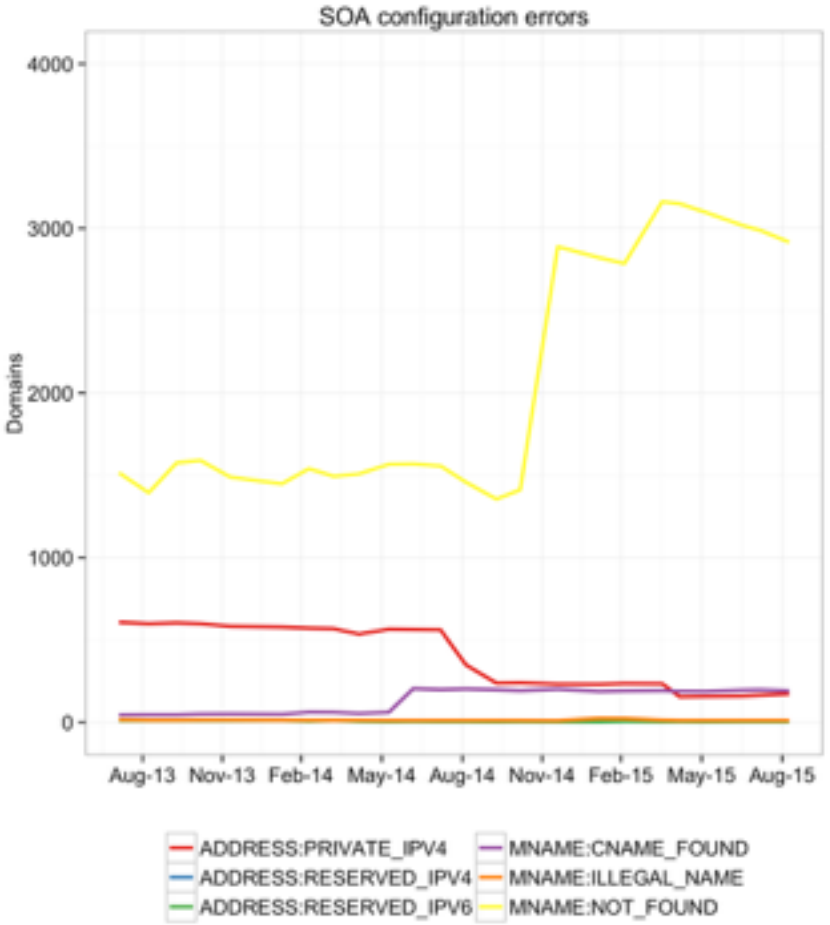
SOA Host/address errors

- SOA record has a MNAME
  - Primary source of data – RFC 1035
  - Relevant for DDNS
- MNAME points to invalid address
- MNAME points to unresolvable host



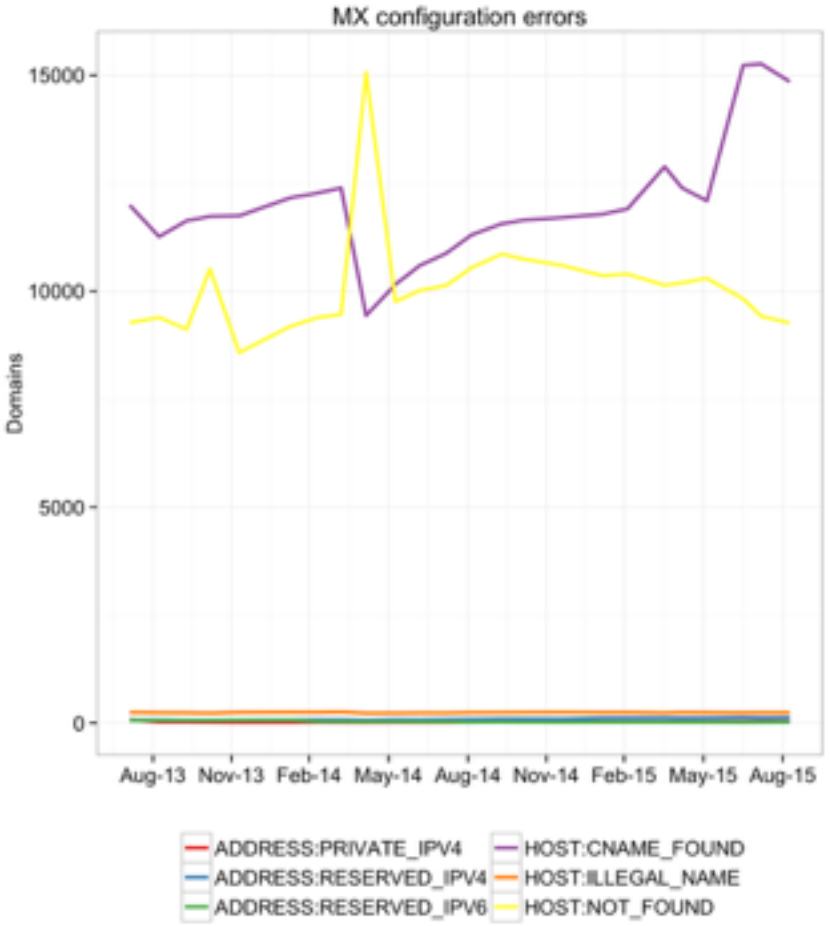
SOA Host/address errors

- Closer view of the least frequent errors



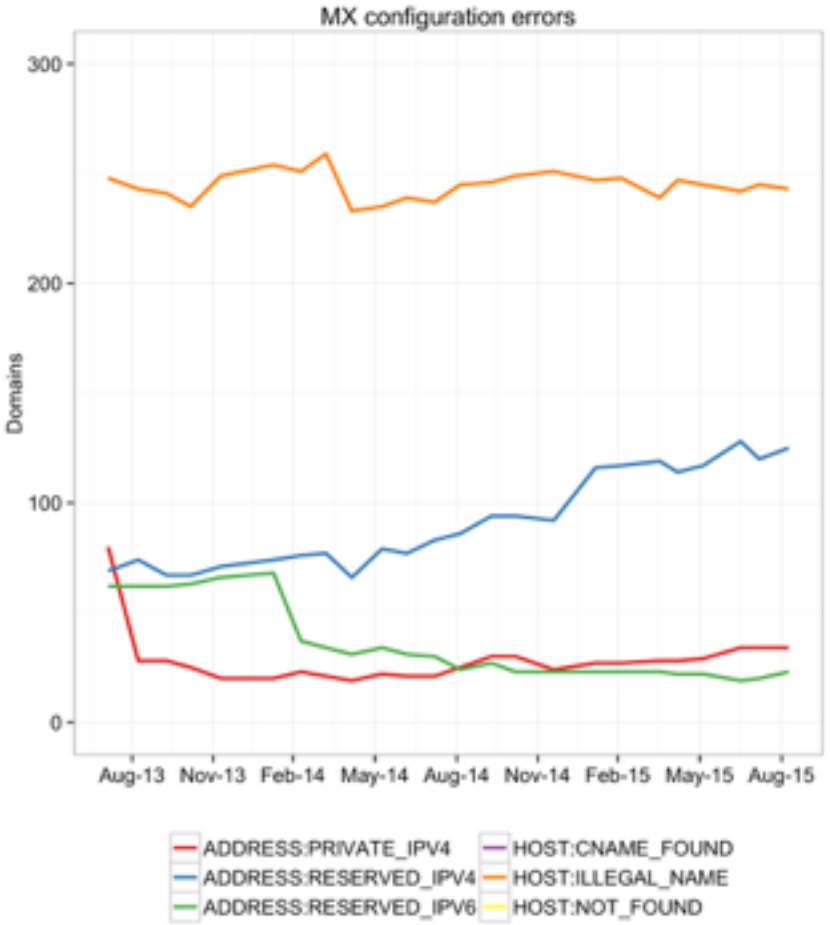
MX Host/Address errors

- Same definition as before
- Mostly misspelled/ invalid hosts
- Data at the child, nothing we can do



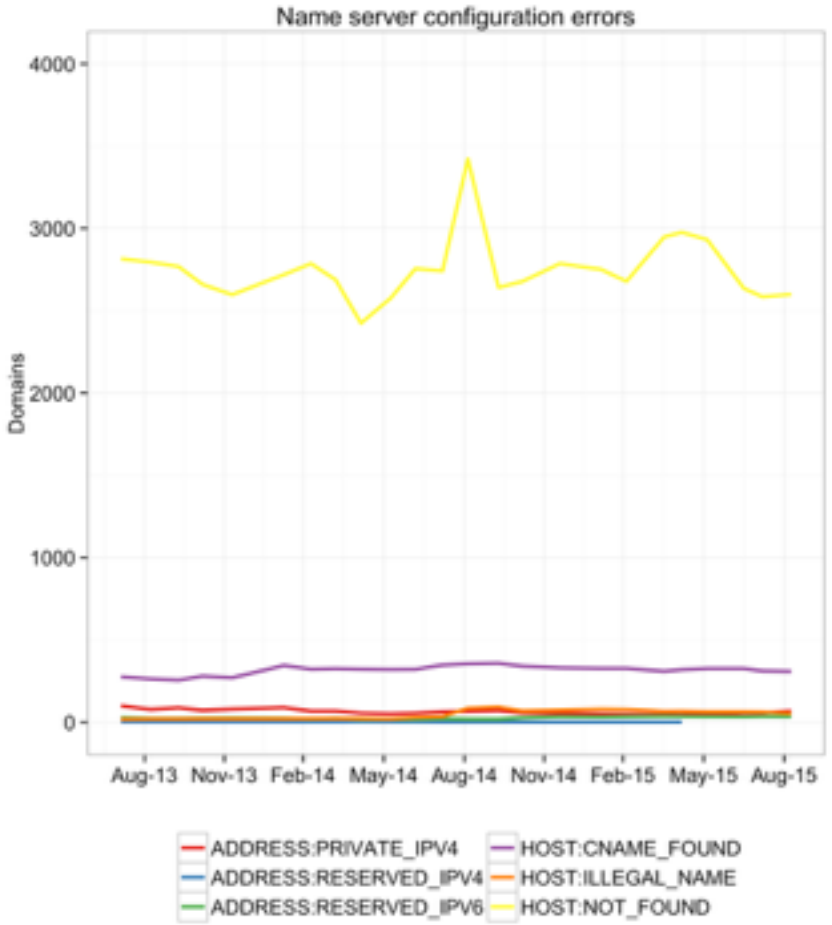
MX Host/Address errors

- Few errors, not wide spread
- Allowed by not strict checking of zone content
  - named-checkzone



NS Host/Address errors

- Yes, nameservers using CNAMEs
- Nameservers with invalid addresses
- Great source of brokeness



Wrap-up

- Most of this data available currently in the IDP (Internet Data Portal)
  Aggregated at the registry level
  https://idp.nz/Domain-Names/-nz-Zone-Scan/ep35-2s5u
- The Registrar Portal will have detailed errors per registrar!
  So you can have a clean configuration
- Possibly in the future a correctness score per registrar
  Using some of these errors
- We want a better and solid .nz namespace
  Hopefully you too!

Contact: Daniel Griggs / daniel@nzrs.net.nz
www.nzrs.net.nz

NZRS
an InternetNZ company