



# DNS?

**Paul Ebersman**

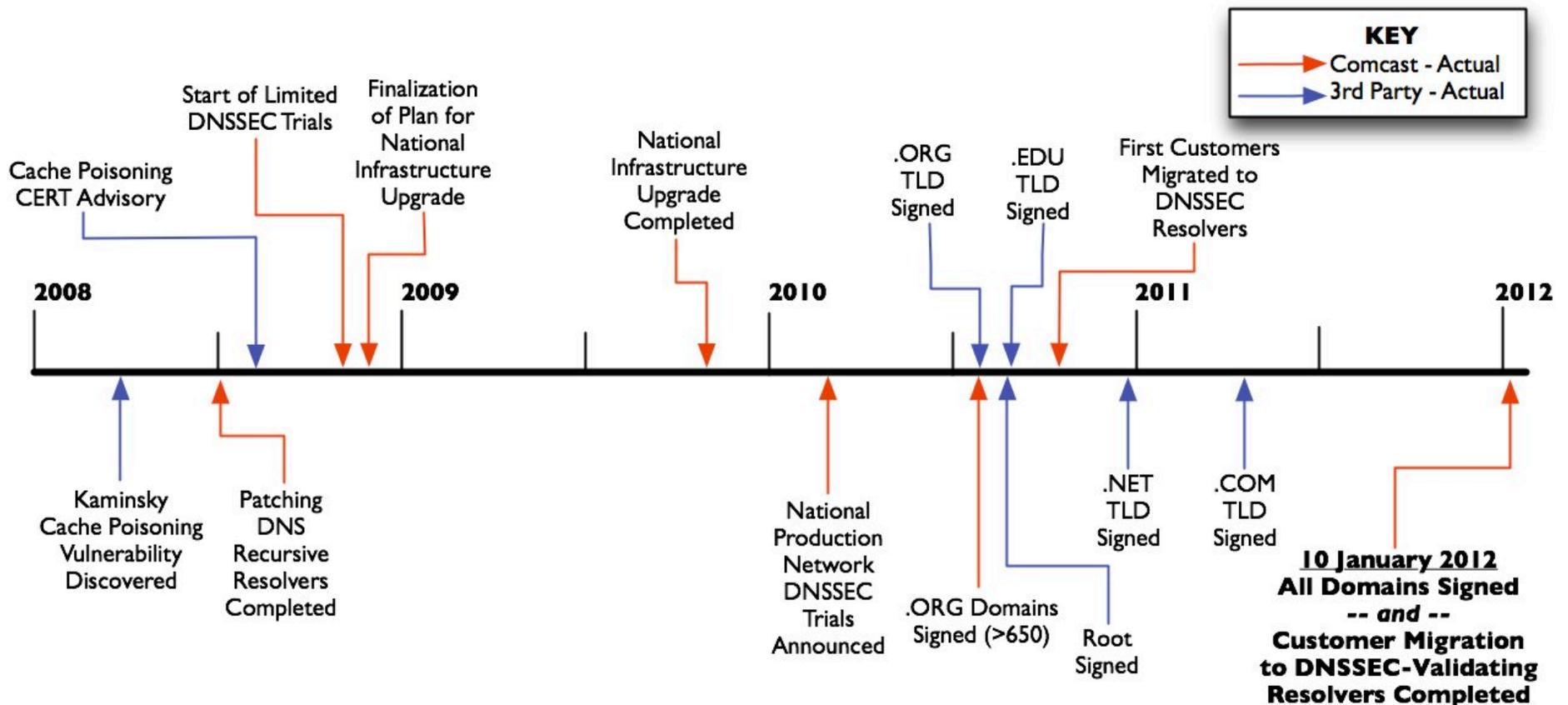
**Paul\_Ebersman@cable.comcast.com, @paul\_ipv6**

**Bucknell Meet & Greet, 10 Jun 2014**

# The Initial Rollout

## DNSSEC Initial Deployment

- We began working on this in 2008 (see timeline)
- We completed our DNSSEC deployment in January 2012
  - All customers use our validating resolvers (>18.1M homes)
  - All Comcast domain names signed (>6,000)



## Lessons Learned in Testing & Early Deployment

- Upgrade/test hardware/software
- Network equipment may need to be updated
  - Permit both UDP and TCP traffic on port 53?
  - Handle EDNS0
  - Handle fragmentation?
- Beef up Authoritative infrastructure
  - Zone signing can be resource intensive
  - Many sub-zones can be complex

## Lessons Learned in Testing & Early Deployment

- If you plan this at the same time as your IPv6 upgrade, the incremental cost and work is more modest than it otherwise would be.
- Update operational processes for debugging (1<sup>st</sup> Tier)
- Add new Key Performance Indicators (KPIs) or metrics, such as:
  - # of SERVFAILs (set an alarm threshold)
  - SERVFAILs as a % of all RCODEs (set an alarm threshold)
  - When top-10 domains sign, ad hoc temporary monitors?
- Try to find registrar with automated DS update method

# More Recent Experience

## What have we seen?

- Most common problems relate to key rollovers or key expirations.
- NTAs (Negative Trust Anchors) a must for now
- <http://dnsviz.net> is your friend

## Our current process

- Failure is noticed
- Use “dig +cd” to verify DNSSEC is the issue
- Use dnsviz to isolate actual failure
- Escalate from 1<sup>st</sup> tier to engineering
- Contact zone owner and attempt to get zone fixed
- If not (or if high value zone), insert NTA
- When zone is fixed, validate with “dig +dns”
- Remove NTA