



# DNSSEC and Infrastructure Providers

FOSE 2012 DNSSEC Session

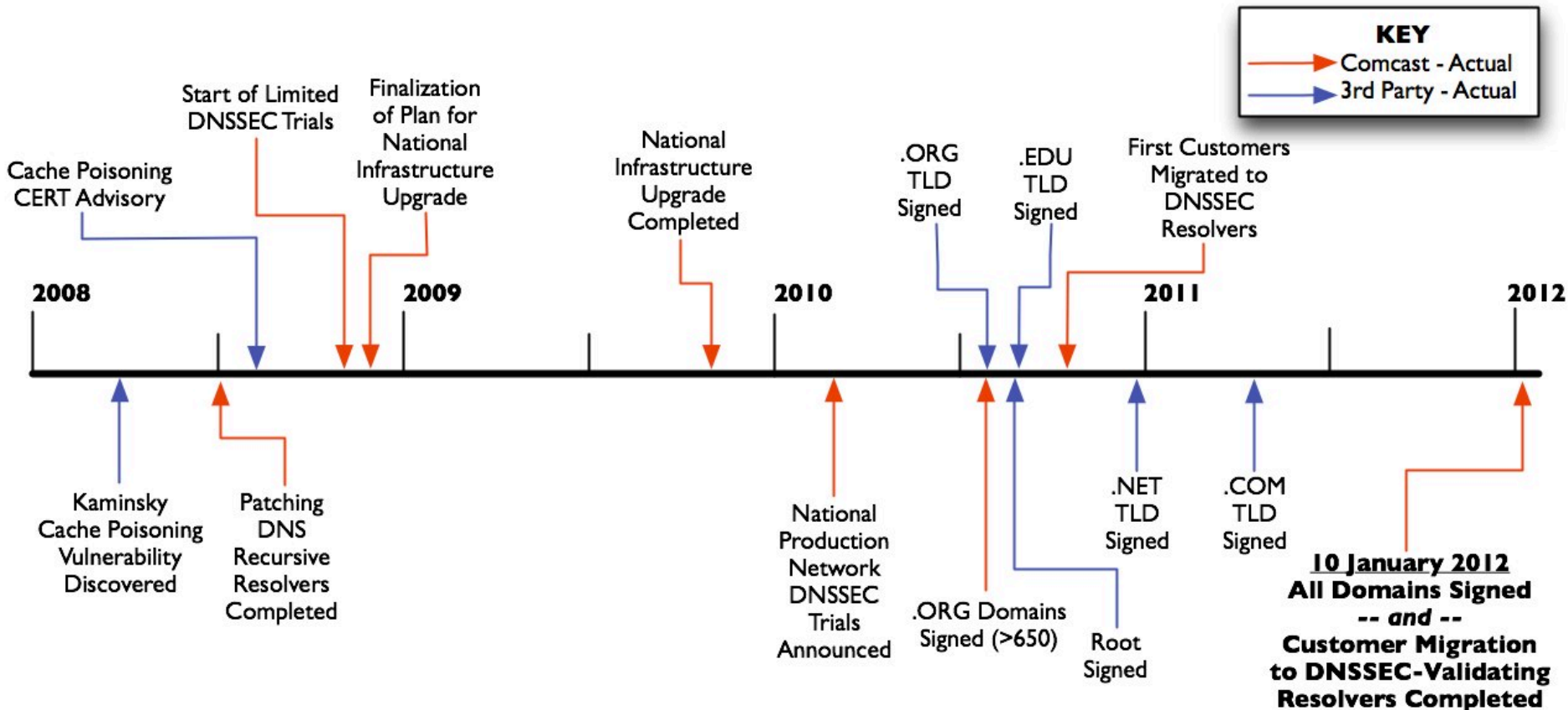
April 3, 2012



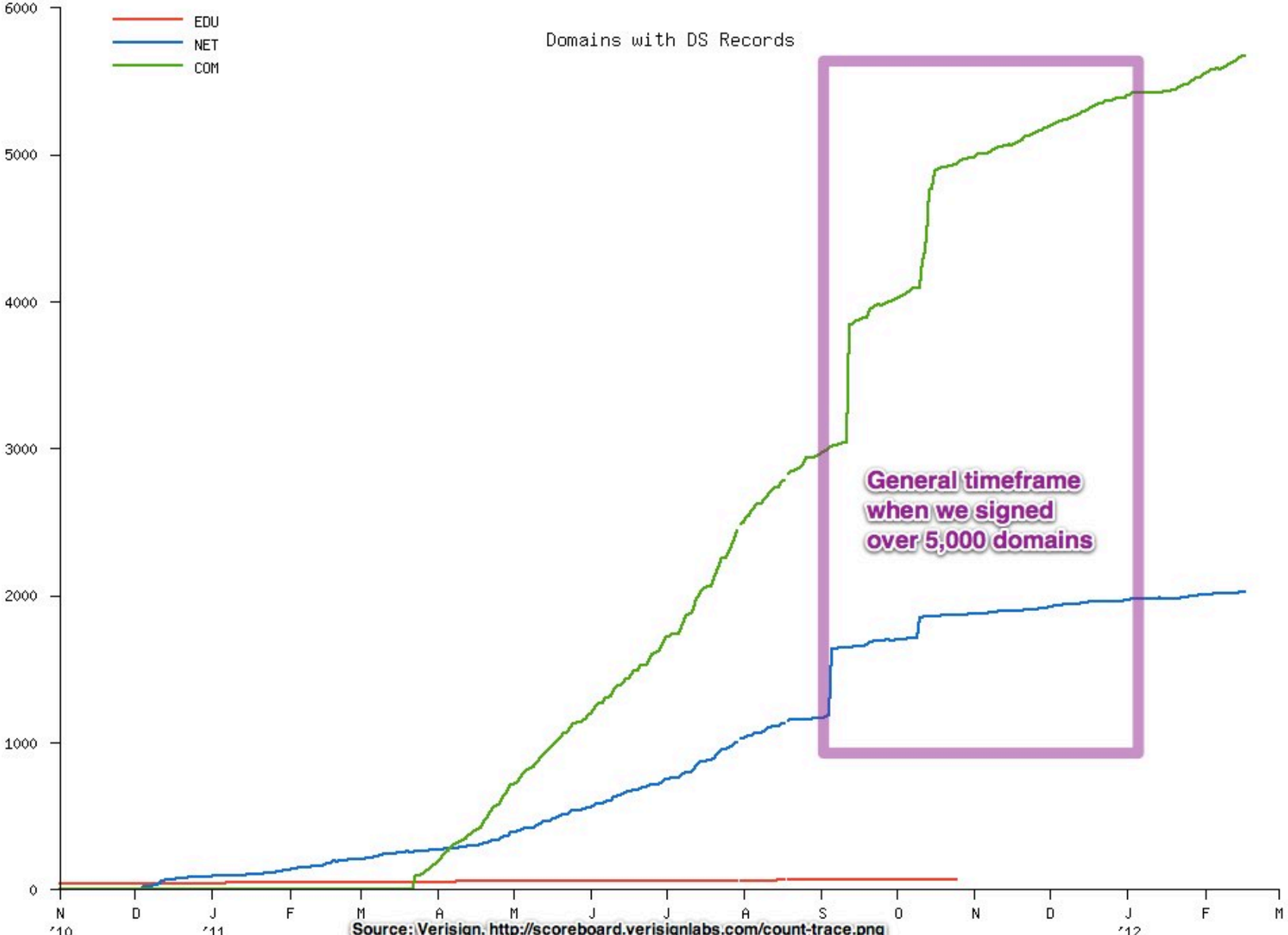
NATIONAL ENGINEERING & TECHNICAL OPERATIONS

# DNSSEC Deployment Status

- 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)



# Some Measurement Data



Source: Verisign, <http://scoreboard.verisignlabs.com/count-trace.png>

# Validation and Customer Perceptions

There is still much work needed to make validation for name resolution stable

- There have been several high profile sites in the .GOV TLD that have had operational issues reported recently
- Many of which immediately cause people to claim that an ISP is blocking services
- Customers are overtly aware when a site stops working...
  - Twitter, Facebook, Blogs are the new way of alerting that a website is down. Social media is the new alerting mechanism.
- How do we help customers identify when there is a site down due to DNSSEC validation?
  - Either because of error or maliciousness
  - Should this be done in web browsers and applications?

# Validation and Customer Perceptions

- In the end, customers are not going to have patience trying to decipher a DNS problem, DNSSEC signing problem, or just that they cannot get to a site due to any number of problems
  - We need better tools and alerting mechanisms for zone operators to know their zone is not operating
  - There needs to be better coordination across all zone operators
  - Could we use organizations like DNS-OARC or something else to help coordinate and provide tools for zone operators to assist with signing validation and operational deployment?

# Lessons Learned in Testing & Early Deployment

- Is a software upgrade required?
- Can the servers handle incremental CPU load?
- Network equipment may need to be updated
  - Will they permit both UDP and TCP traffic on port 53?
  - Can they properly handle larger DNS responses? (with EDNS0, response may go from 512 bytes to 4,000 bytes)
  - Can they handle fragmentation?
- Authoritative infrastructure may need to be augmented to support signing your zones
  - Zone signing can be resource intensive
  - This can be complex if you have many sub-zones
  - Delegations to platforms like GLSB and CDN which are not yet supporting DNSSEC signing will stop validation and in some cases break

# Lessons Learned in Testing & Early Deployment

- Best way to figure this out is to test in the lab and validate with production traffic under close observation and measurement
- 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.
- Look for operational processes that may need to be adjusted to support DNSSEC validation (i.e. troubleshooting, customer FAQs)
- 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?
- For signing your zones, be sure your registrar has an automated process for updating / inserting DS records

## More Recent Lessons Learned at Scale

- Different software vendors interpret the RFCs differently, causing irregular validation results
  - CNAME at the zone apex, pointing to another zone
    - mail.comcast.net in CNAME mail.g.comcast.net (a GSLB)
    - Worked if you used BIND, but not Vantio (SERVFAIL = ☹)
  - So after signing a complex domain, we recommend you validate using different resolvers
- We've observed registries doing 'interesting' things. Such as:
  - One big registrar has a "Premium" service that automatically includes DNSSEC (DNSKEY, RRSIGs, DS inserted in the TLD)
  - If you downgrade from this service, your DNSKEY and RRSIGs are deleted – BUT the DS record is not removed from the TLD
  - This causes the domain to fail validation (SERVFAIL = ☹)



## More Recent Lessons Learned at Scale

- On our authoritative servers, not many DNSSEC-related RR queries as of yet (expected based on the state of validation)
- Of the top 2,000 domains:
  - 1.75% signed – which is oddly close to the % with AAAA RRs
- As with any new technology or deployment there will be problems
  - Prepare in advance (scripts, processes, testing, practice)
- Most common issue is incorrectly signed zones, usually related to key rollovers

## More Recent Lessons Learned at Scale

- One solution is a “Negative Trust Anchor” to temporarily skip validation for a given domain
  - Only when an engineer has personally verified the failure is due to DNSSEC misconfiguration and, preferably, communicated with the affected domain
  - Can temporarily restore end user access while the domain fixes their problem
  - Does NOT scale, but can be helpful for high traffic and other key domains
  - Probably useful for the next 1 – 2 years as domains mature and master their signing and key rollover processes
  - Ultimately, this is the responsibility of the domain owner or administrator to get right!

# Increasing Adoption

There is still much work needed to make validation for name resolution stable

- More ISPs should move towards enabling DNSSEC validation on their resolvers in their network. They should also sign domains if they manage their authoritative zones.
  - Get started as soon as possible, there is a lot of planning needed to do it right.
  - Setting up a test bed and/or beta program is fairly low impact and will provide time to work through planning for eventual roll out.
  - Securing DNS answers is a value add for your customers.
- Enterprises should also look to trial DNSSEC validation in their network.
  - Setup for DNSSEC validation has become much easier with applications and tools.
  - Enterprises need security for the DNS as well.

## Next Steps

- Managing customer escalations VS zone operator issues and how to we get in front of this problem
- We need to solve the current problems for DNS Global Load Balancing (GSLB) and Content Distribution Networks (CDN)
  - We are evaluating solutions now, but suggestions are welcome
  - Multiple points points of presence for the same authoritative signed answers
- Commercial Services
  - We have many commercial services customers who we would like to offer services like signed domains
  - Legacy platforms that need to be upgraded to support signing
  - Solve the DS key upload to many registrar problem

**Thank You!**



**For more information on the Comcast  
DNSSEC and IPv6 deployments:**

**<http://www.dnssec.comcast.net>**

**<http://www.comcast6.net>**

**<http://dns.comcast.net>**



**NATIONAL ENGINEERING & TECHNICAL OPERATIONS**