ICANN DNSSEC Workshop

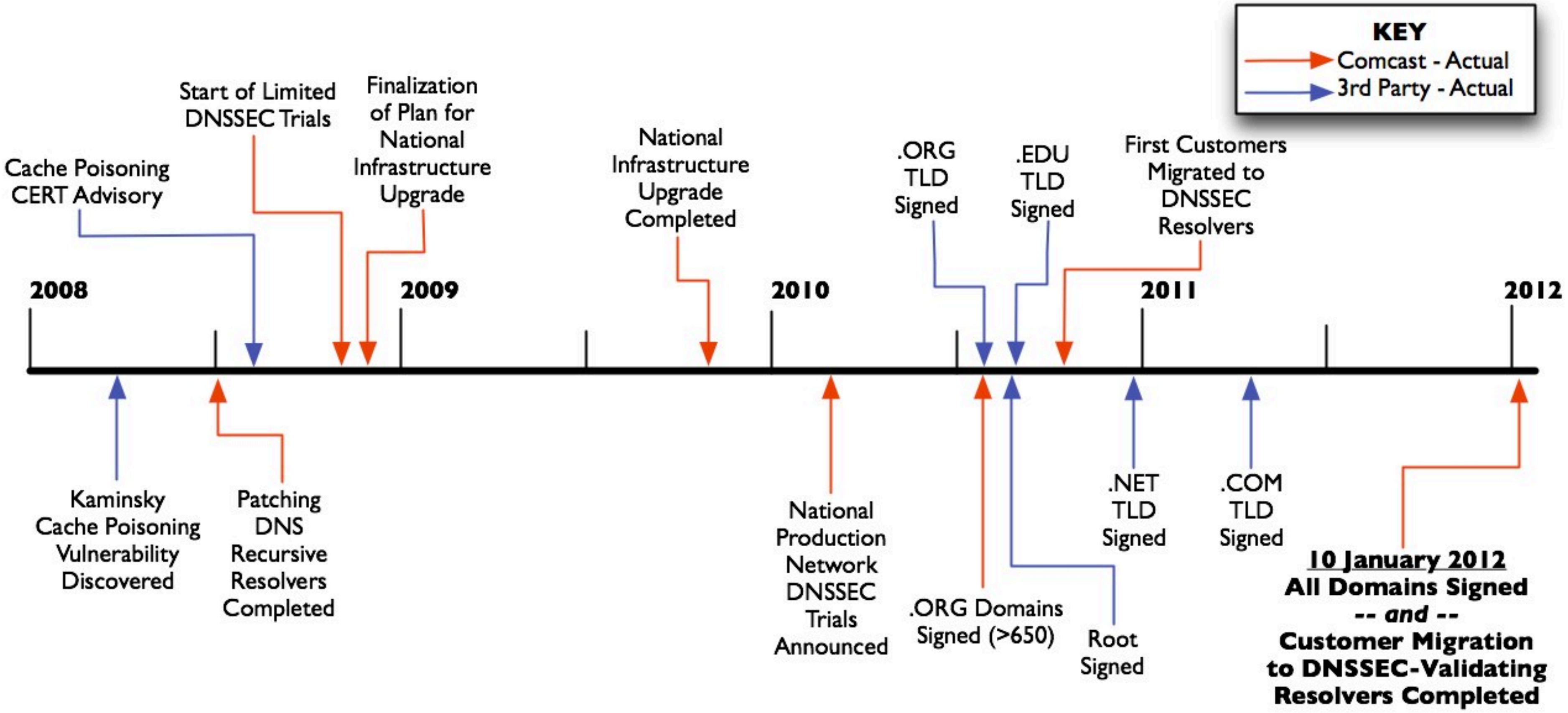
Comcast’s Operational Experiences

14 March 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)



Cache Poisoning CERT Advisory

Start of Limited DNSSEC Trials

Finalization of Plan for National Infrastructure Upgrade

National Infrastructure Upgrade Completed

.ORG TLD Signed

.EDU TLD Signed

First Customers Migrated to DNSSEC Resolvers

Kaminsky Cache Poisoning Vulnerability Discovered

Patching DNS Recursive Resolvers Completed

National Production Network DNSSEC Trials Announced

.ORG Domains Signed (>650)

Root Signed

.NET TLD Signed

.COM TLD Signed

10 January 2012
All Domains Signed
-- and --
Customer Migration to DNSSEC-Validating Resolvers Completed

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

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, they 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

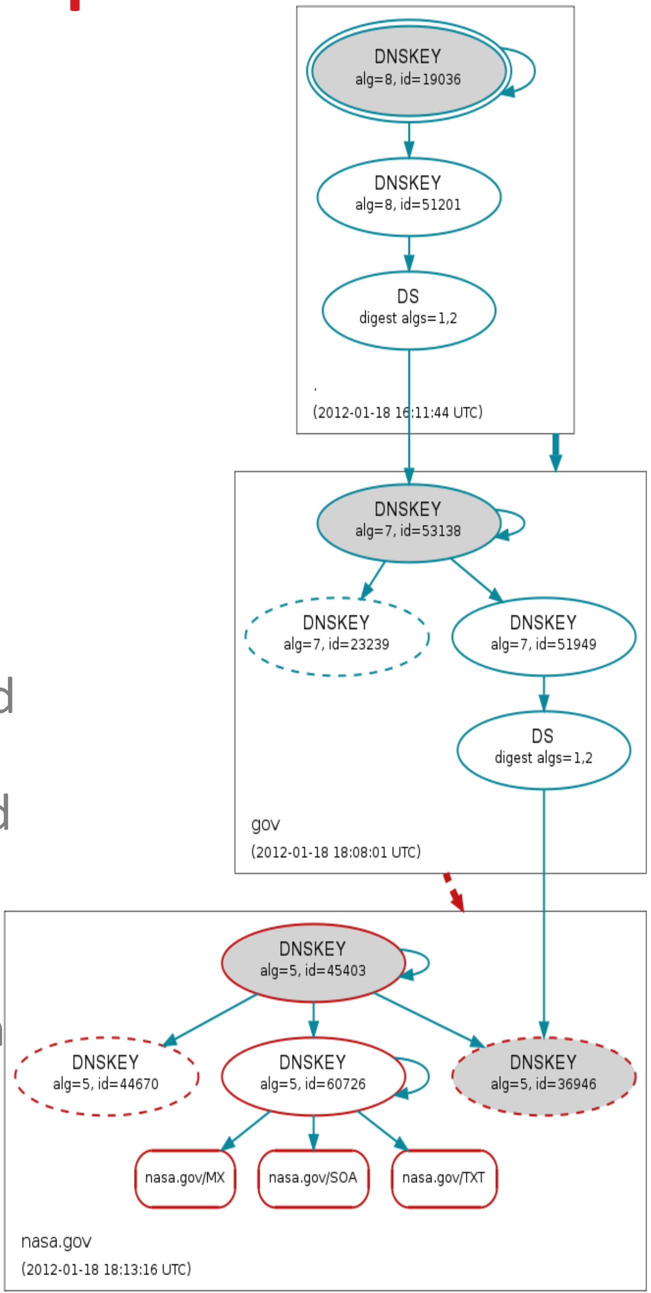
- Different software vendors interpret the RFCs differently, causing irregular validation results
    - CNAME at the zone apex, pointing to another zone
        - mail.comcast.net in CNAME mail.g.comcast.net (a GSLB)
        - Worked if you used BIND, but not Vantio (SERVFAIL = ☹)
    - So after signing 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 = ☹)
- 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

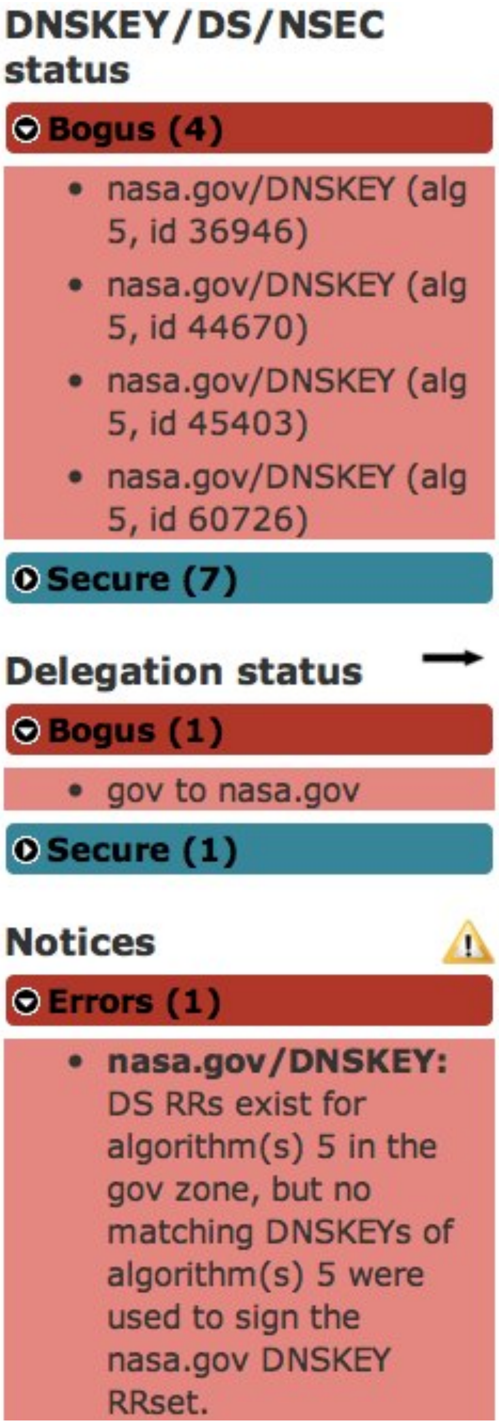
More Recent Lessons Learned at Scale

- 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 (mostly in the .GOV TLD)
- 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!

Validation Failure Example – NASA.GOV

- 18 January 2012: Domain performed a Key Signing Key (KSK) rollover
  - Created new key & signed domain with new key
  - Updated DS record in .GOV TLD
  - But did not double sign with old key, which would have ensured both the old and new keys worked simultaneously
  - So the new DS record pointed to the old KSK, which was no longer in the zone
  - Chain of trust broken = validation failure = SERVFAIL





DNSKEY/DS/NSEC status

Bogus (4)

- nasa.gov/DNSKEY (alg 5, id 36946)
- nasa.gov/DNSKEY (alg 5, id 44670)
- nasa.gov/DNSKEY (alg 5, id 45403)
- nasa.gov/DNSKEY (alg 5, id 60726)

Secure (7)

Delegation status

Bogus (1)

- gov to nasa.gov

Secure (1)

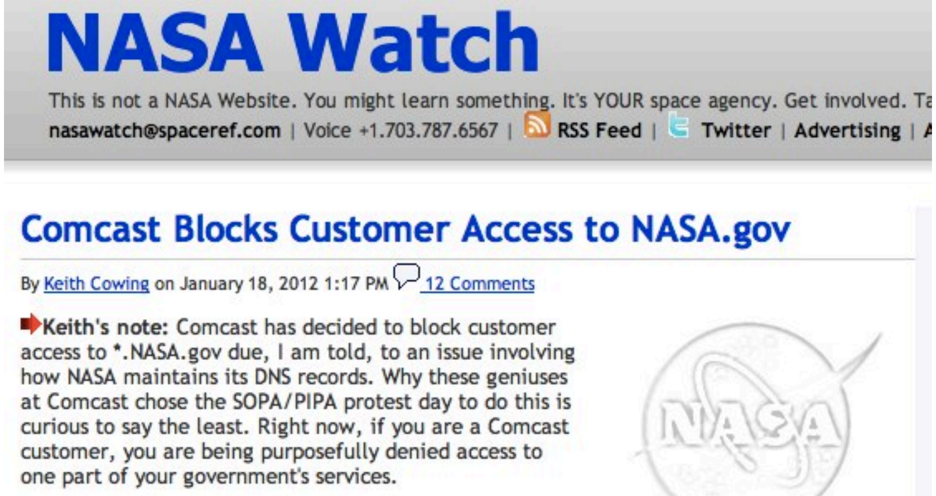
Notices

Errors (1)

- **nasa.gov/DNSKEY:** DS RRs exist for algorithm(s) 5 in the gov zone, but no matching DNSKEYs of algorithm(s) 5 were used to sign the nasa.gov DNSKEY RRset.

Validation Failure Example – NASA.GOV

- Customers interpreted this as us "blocking" access to the site, some recommended switching to non-validating resolvers
- "Fixed" temporarily with a Negative Trust Anchor
- In parallel, the domain administrator repaired their zone



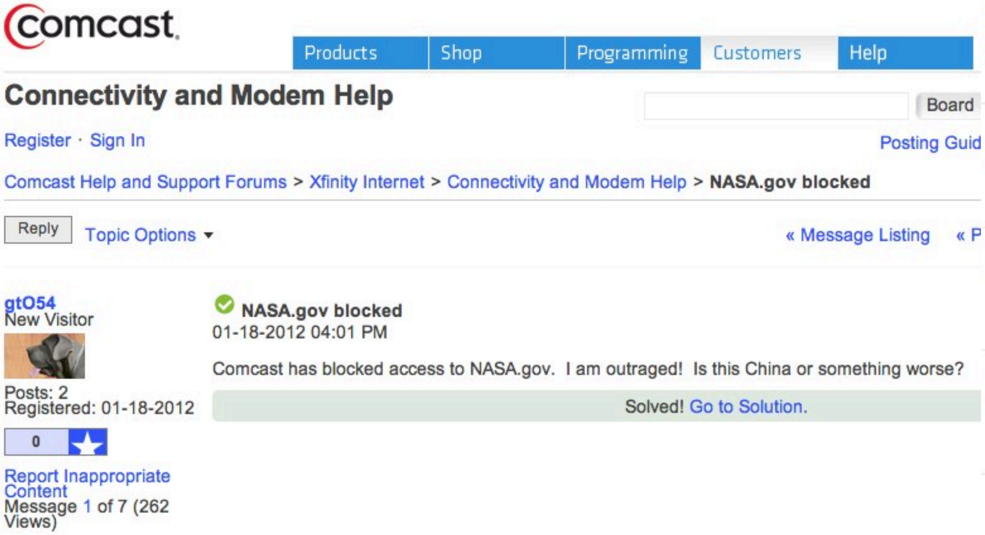
NASA Watch

This is not a NASA Website. You might learn something. It's YOUR space agency. Get involved. Ta
nasawatch@spaceref.com | Voice +1.703.787.6567 | RSS Feed | Twitter | Advertising | A

Comcast Blocks Customer Access to NASA.gov

By Keith Cowing on January 18, 2012 1:17 PM 12 Comments

Keith's note: Comcast has decided to block customer access to *.NASA.gov due, I am told, to an issue involving how NASA maintains its DNS records. Why these geniuses at Comcast chose the SOPA/PIPA protest day to do this is curious to say the least. Right now, if you are a Comcast customer, you are being purposefully denied access to one part of your government's services.



Connectivity and Modem Help

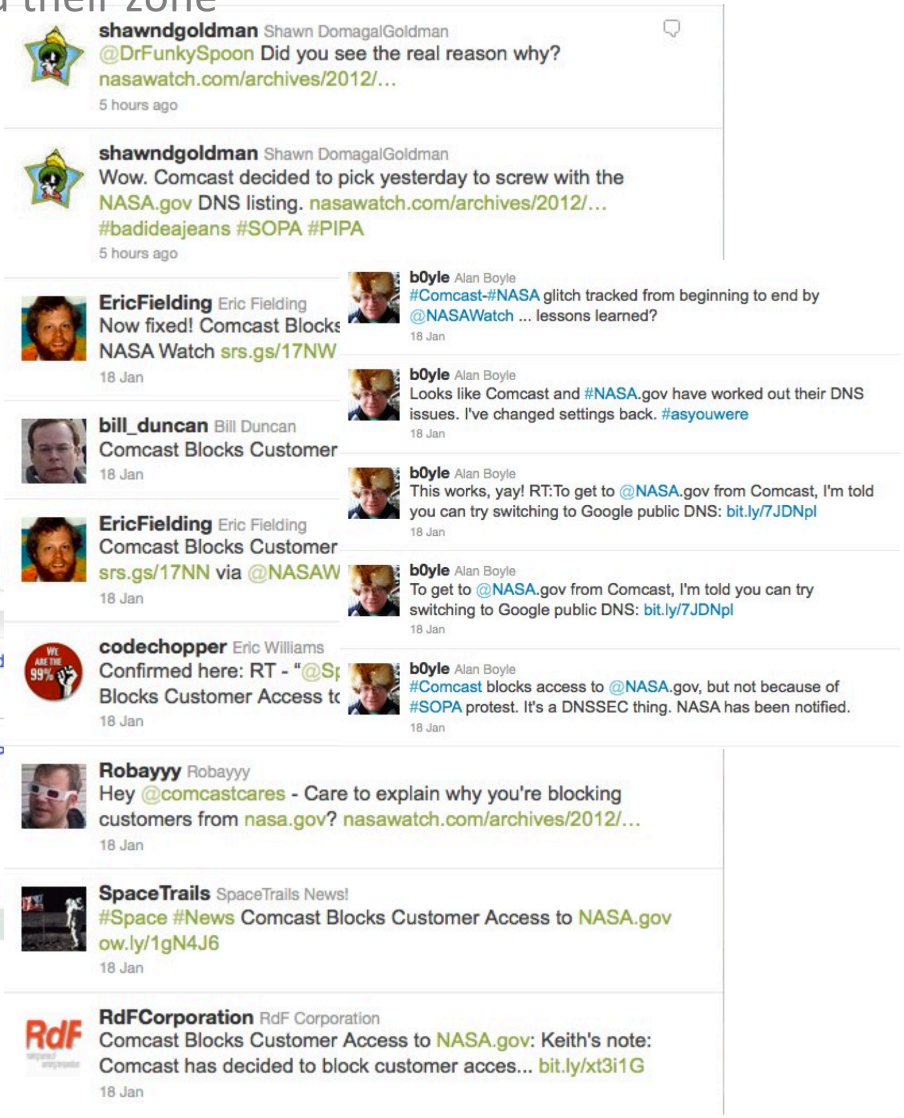
Comcast Help and Support Forums > Xfinity Internet > Connectivity and Modem Help > **NASA.gov blocked**

gt054
New Visitor
Posts: 2
Registered: 01-18-2012
0
Report Inappropriate Content
Message 1 of 7 (262 Views)

NASA.gov blocked
01-18-2012 04:01 PM

Comcast has blocked access to NASA.gov. I am outraged! Is this China or something worse?

Solved! Go to Solution.



shawndgoldman Shawn DomagalGoldman
@DrFunkySpoon Did you see the real reason why? nasawatch.com/archives/2012/…
5 hours ago

shawndgoldman Shawn DomagalGoldman
Wow. Comcast decided to pick yesterday to screw with the NASA.gov DNS listing. nasawatch.com/archives/2012/… #badideajeans #SOPA #PIPA
5 hours ago

EricFielding Eric Fielding
Now fixed! Comcast Blocks
NASA Watch srs.gs/17NW
18 Jan

bill_duncan Bill Duncan
Comcast Blocks Customer
18 Jan

EricFielding Eric Fielding
Comcast Blocks Customer
srs.gs/17NN via @NASAW
18 Jan

codechopper Eric Williams
Confirmed here: RT - "@S
Blocks Customer Access t
18 Jan

b0yle Alan Boyle
#Comcast-#NASA glitch tracked from beginning to end by @NASAWatch ... lessons learned?
18 Jan

b0yle Alan Boyle
Looks like Comcast and #NASA.gov have worked out their DNS issues. I've changed settings back. #asyouwere
18 Jan

b0yle Alan Boyle
This works, yay! RT:To get to @NASA.gov from Comcast, I'm told you can try switching to Google public DNS: bit.ly/7JDNpl
18 Jan

b0yle Alan Boyle
To get to @NASA.gov from Comcast, I'm told you can try switching to Google public DNS: bit.ly/7JDNpl
18 Jan

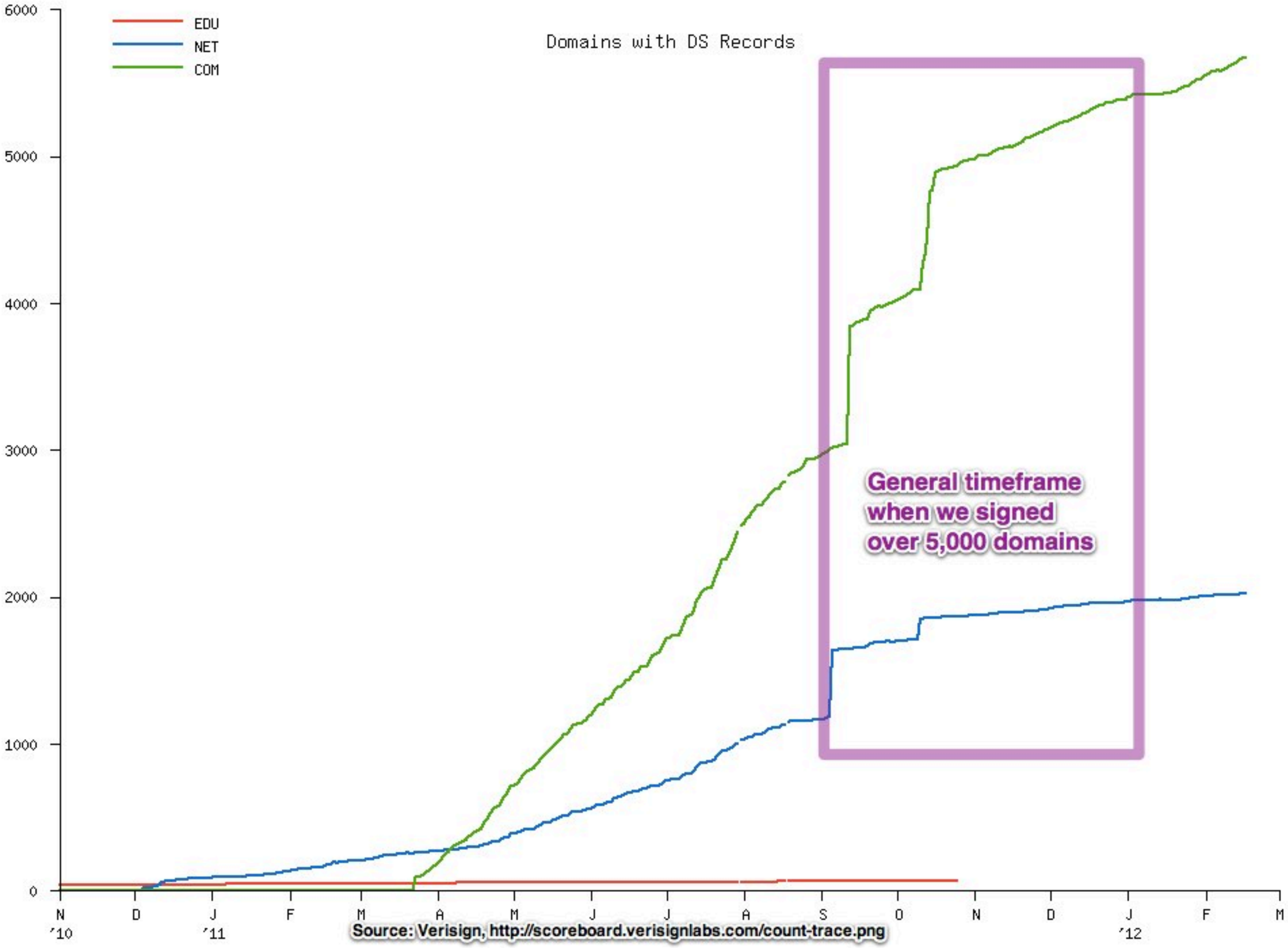
b0yle Alan Boyle
#Comcast blocks access to @NASA.gov, but not because of #SOPA protest. It's a DNSSEC thing. NASA has been notified.
18 Jan

Robayyy Robayyy
Hey @comcastcares - Care to explain why you're blocking customers from nasa.gov? nasawatch.com/archives/2012/…
18 Jan

SpaceTrails SpaceTrails News!
#Space #News Comcast Blocks Customer Access to NASA.gov ow.ly/1gN4J6
18 Jan

RdFCorporation RdF Corporation
Comcast Blocks Customer Access to NASA.gov: Keith's note: Comcast has decided to block customer acces... bit.ly/xt3i1G
18 Jan

Some Measurement Data



General timeframe when we signed over 5,000 domains

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

Thank You!

For more information:

http://www.dnssec.comcast.net
http://dns.comcast.net

NATIONAL ENGINEERING & TECHNICAL OPERATIONS