

# The signing of dotUS ("US.")

NANOG 44

Lightening Talks

Edward Lewis/Neustar

# US. is signed

- Since December 2009
- DNSSEC with NSEC records
  - If you want to "walk the zone" we recommend you ask for a FTP dump instead
- No DS records yet
- We haven't changed any keys yet
- We haven't changed name servers (yet)

# What does that mean?

- The US zone mostly refers DNS queries to other servers
  - There's not much DNSSEC in today's referrals
- You will see DNSSEC records only if you ask
  - And you probably do without knowing it
- Lookups for non-existent names do include DNSSEC records
  - (Non-existent means not active in DNS)

# Somebody noticed...

- "We received a call from *\$somebody* concerning a flood of fragments coming from b.gtld.biz.... Upon further investigation, networking team saw fragments ... isolated down to NXDOMAIN when querying with DNSSEC requested. "
- Heard this once, at the start, not since.

# A plug for a DNS-OARC test

- <https://www.dns-oarc.net/oarc/services/replysizetest>
- OARC's DNS Reply Size Test Server
  - Recent increases in DNSSEC deployment are exposing problems with DNS resolvers that cannot receive large responses...
  - DNS-OARC built the DNS Reply Size Test Server to help users identify resolvers that cannot receive large DNS replies.

# What's ahead

- Soon, soon, Early Adoption program
  - A few invited "guests" will begin to exercise DNSSEC
  - It's not so much a test of the registry as a test of the production impact on the 'net
- Looking forward to the signing of the root this summer

# The "Zone Key"

- We believe that the best way for folks to get the US zone key is via the signed root zone
  - Not in DLV, not in ITAR
- In the interim, and into the future as a backup plan
  - The US zone keys (trust anchors) are available with PGP signatures from
  - <http://www.neustarregistry.biz/dnssec/publickeys/us/>

# What else to look out for

- Operators - here's another way you can become an innocent victim of DNSSEC
  - An enterprise signs their zone, registers in a TLD
  - You protect your caches by having the Root key
  - \*Then someone messes up\* (enterprise, TLD,...)
  - Your subscribers will get DNS errors and make calls to your help desk
- No one wants that to happen to you

# Summary

- dotUS has changed
  - Adding NSEC records
  - Larger negative answers
- More changes are coming
  - Signed delegation information (larger positives)
  - New server constellation