.org advance your mission

# .ORG & DNSSEC

## Jim Galvin

*July 2009*

# Why?

# Our Brand & Reputation

» Top five perceptions of the .ORG Brand

- **Informative**
- **Well-Intentioned**
- **Trustworthy**
- **Valuable Information**
- **Reliable**


## We expect to keep it that way!

# Our Mission

» **.ORG signed with DNSSEC on June 2, 2009**

– *Our mission is to serve in the public interest, so securing our TLD with DNSSEC became a top priority for our organization.*

# Because the threat is real

» *In March-April 2005, users of an ISP had specific spyware, spam and pay-per-click trojans, from redirection sites*

– The ISP's cache had hundreds of DNS names spoofed…

- AmericanExpress.com
- FedEx.com
- CitiCards.com
- DHL-USA.com
- Sabre.com

Source: Allison Mankin http://www.psg.com/~mankin/vita.txt

# Because the threat is real

» *July 2009:* Irish internet service provider (ISP) Eircom says that it was targeted by a cache poisoning attack that redirected customers to sites they did not intend to visit twice within the last few weeks.

Source:
http://www.siliconrepublic.com/news/article/13448/cio/eircom-reveals-cache-poisoning-attack-by-hacker-led-to-outages

# Because so many critical applications rely on DNS

» *DNSSEC isn't just about "man in the middle" attacks. It's also about all of the applications that rely on DNS to work. For example, why in the year 2008 is email not secure?* - Dan Kaminsky

» DNSSEC isn't a magic bullet, but it is a very important starting point that allows us to start evaluating how to secure the many applications that are intertwined with DNS.

» DNSSEC is a new tool for Internet security. So new that we do not know yet how developers will leverage a secure DNS for new applications, but rest assured, they will…

## Because there are opportunities that surface from a more secure and authenticated internet

Online health records?

Spam?

?

?

Cost Savings?

Secure email?


?

Trusted online transactions?

# .ORG DNSSEC Update

Where We Are Today

&

Lessons Learned

# Timeline

» .ORG signed on 2 June 2009
  – SOA, DNSKEY, RRSIG TTL SET TO 0
» SOA TTL changed to 900 on 13 June 2009
» DNSKEY TTL = 900 on 17 June 2009
» First ZSK roll and resign completed 10 July 2009
» No KSK roll (yet)

# Aspects of the .ORG Zone

» Over 7.5 million delegations

» Nearly 18 million Resource Records

» Continuously Updated

» Using NSEC3 for both policy and technical reasons.

# .ORG Lessons Learned

» A Technology Implementation

– Let the readiness of your technology drive your launch date and nothing else (not marketing, PR, management etc).

» Collaborate

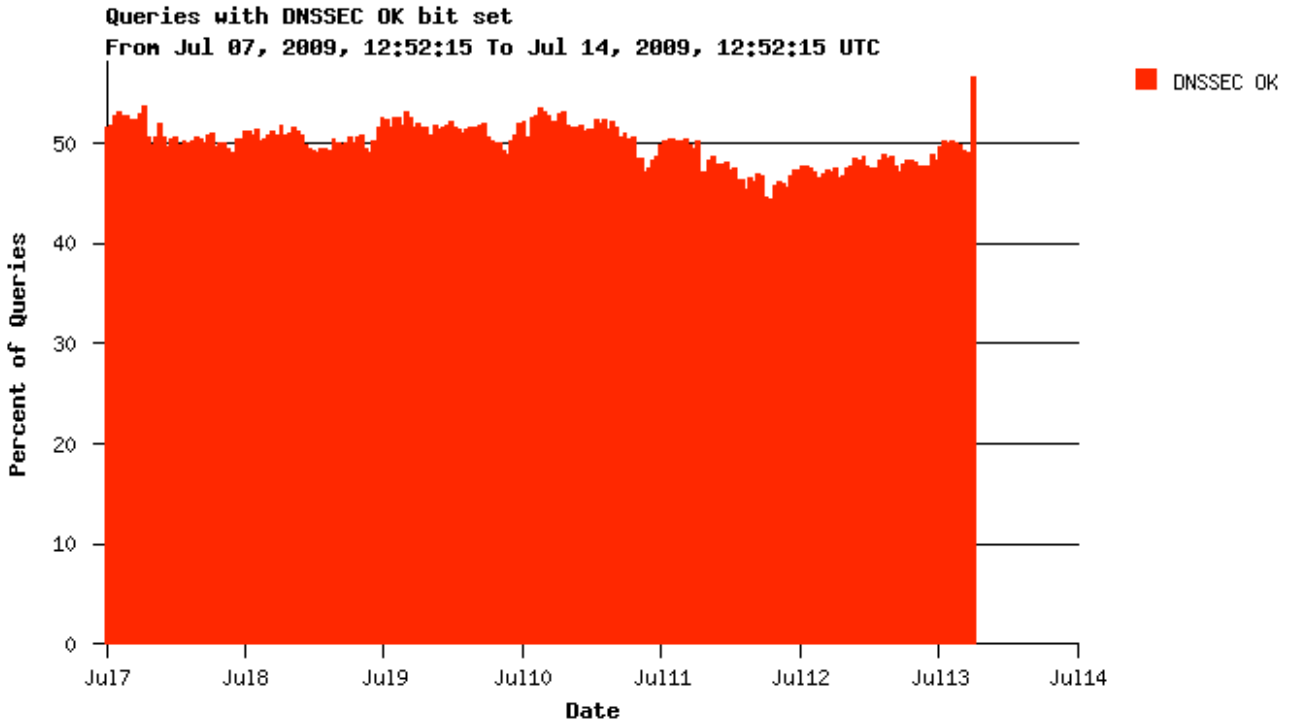
– It takes a village

• There are many DNSSEC experts willing to assist in industry wide adoption. Let them help you!

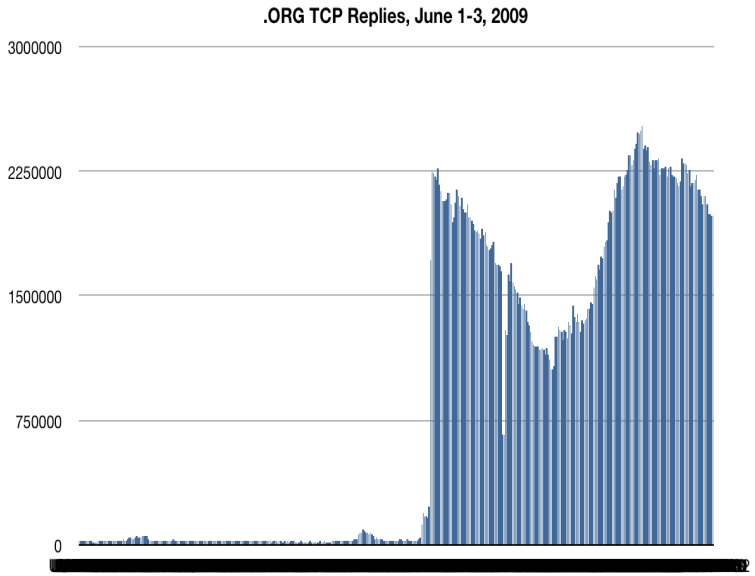
» A Phased Approach

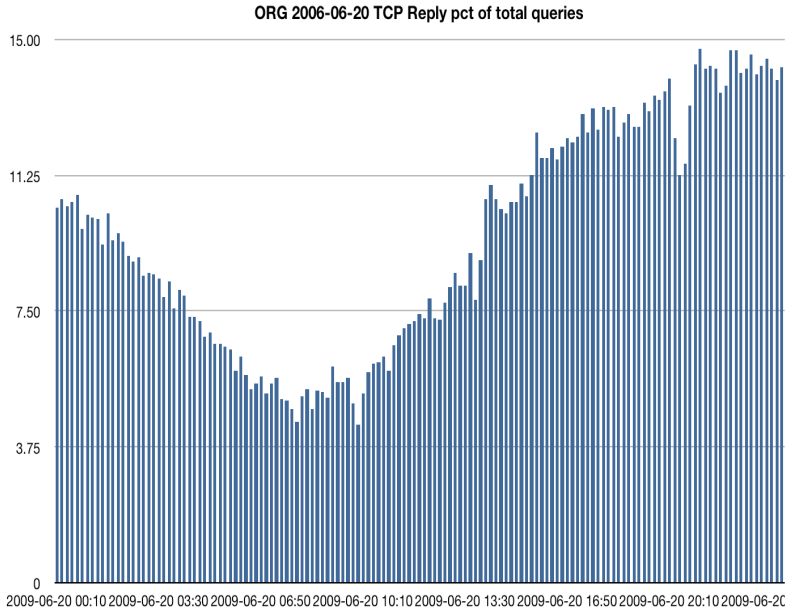
– Phase your launch to provide an environment that allows for proper planning, risk mitigation and readiness assessments.

Nearly half of all queries are DNSSEC ready:



# TCP Replies increased ***two orders of magnitude!***




# Thank you!