# Negative Trust Anchors

ICANN 48

DNSSEC Workshop

20 November 2013

Presented by
Jason Livingood
Vice President, Internet & Communications Engineering
Comcast

ICANN 48 • 17-21 Nov 2013
Buenos Aires
ICANN

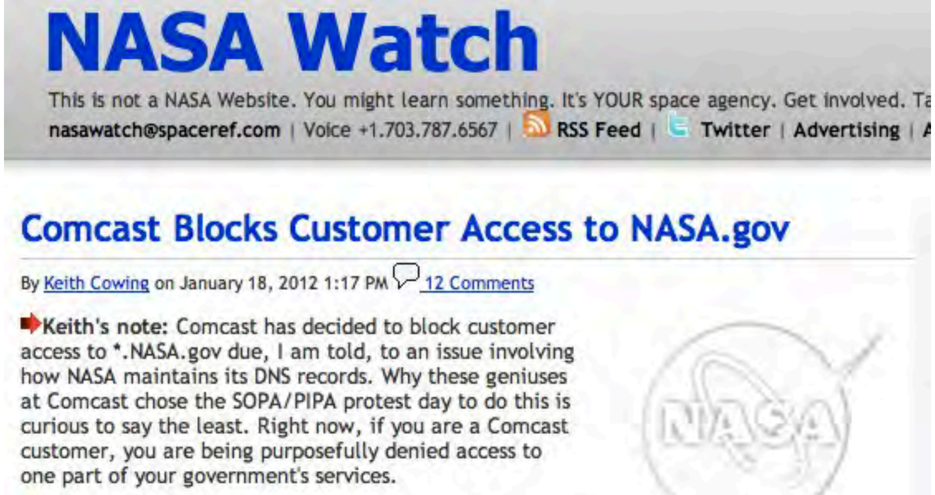
COMCAST

# DNSSEC Validation Is Good

Except when it fails.

– Customers have sometimes interpreted this as us “blocking” access to the site, and some have recommended switching to non-validating resolvers

- “Fixed” temporarily with a Negative Trust Anchor while their domain administrator repaired their zone



NASA Watch

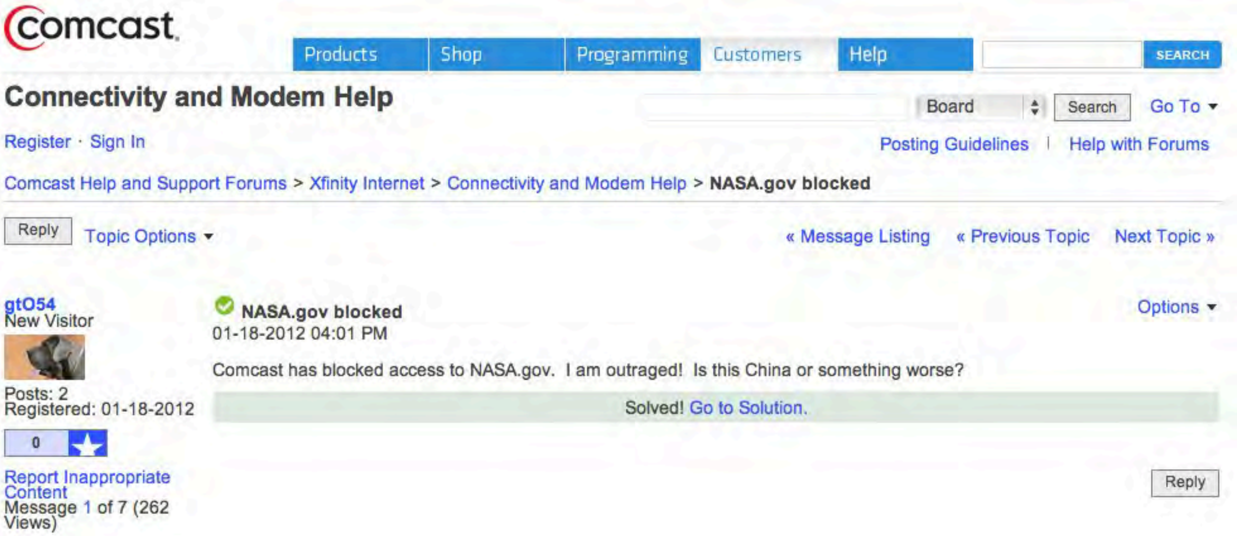
This is not a NASA Website. You might learn something. It's YOUR space agency. Get involved. Ta

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**

gtO54
New Visitor

Posts: 2
Registered: 01-18-2012

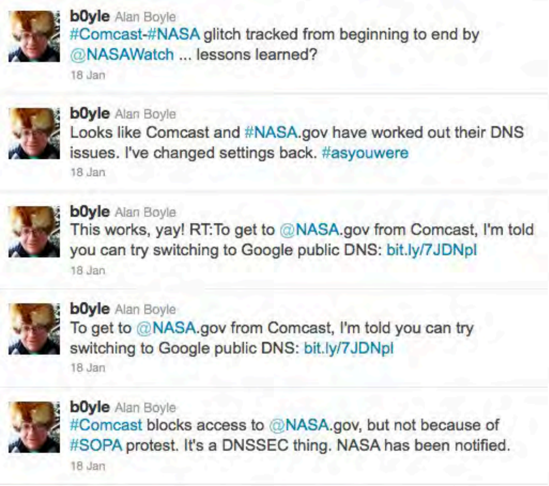
0

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.



**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

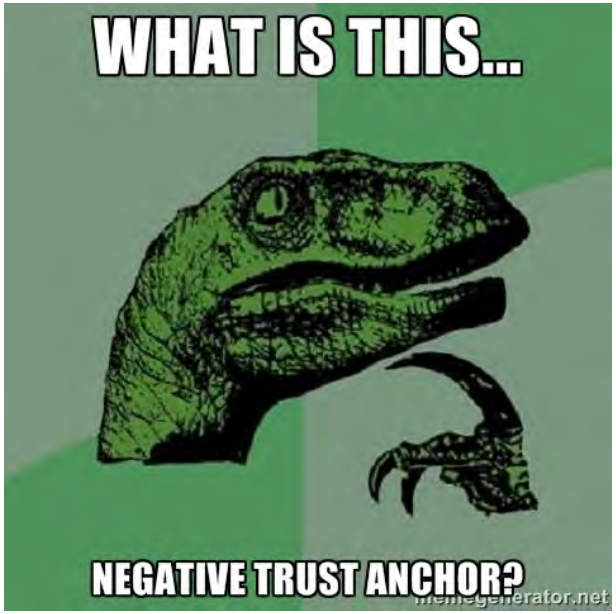
**b0yle** Alan Boyle
#Comcast blocks access to @NASA.gov, but not because of #SOPA protest. It's a DNSSEC thing. NASA has been notified.
18 Jan

# Negative Trust Anchor?

- Sometimes DNSSEC signing domains mess things up a bit operationally…
- Some blame the validators, and have a hard time understanding it’s an authoritative issue.
  - “It resolves just fine with ShinyCloudFreeDNS+ but not with you guys!”
  - “I’m switching to a non-validating resolver. DNSSEC stinks! No security for me!”

# What is a Negative Trust Anchor?

- If a major domain fails DNSSEC validation it is likely either:
  1. A real security issue
  2. An operational / process / technical error



- At the current stage of deployment, #2 seems more likely based on what we have observed

- So a validator can either
  1. Do nothing
  2. Turn off ALL validation
  3. Turn off validation for ONE domain – which is done using a Negative Trust Anchor

- If the customer complaints and/or associated pain is great enough, #1 is not realistic.
- Undertaking #2 seems excessive
- So #3 seems the most targeted temporary solution

# NTAs in Practice

- We’re still using them and will continue to do so for the foreseeable future, but the frequency is no longer increasing
- When we do it we note it at http://dns.comcast.net
- We don’t always do it, especially for “repeat offenders”
- We continue to encourage more domains to sign & for signing domains to have reliable signing practices

# Open Questions at the IETF

- Negative Trust Anchors are being used in practice, but should the IETF's DNSOP document this in any manner?

- If so, should we recommend that an individual NTA be time limited?
  - "Reasonably short period of time"
  - 1 month or less
  - 1 week or less
  - 1 day or less
  - Is this a MUST or a SHOULD?

- How do we (or should we) assess when critical DNSSEC deployment mass has been achieved so that this is no longer a common practice?

# Plan to Update Related IETF Docs

- Consensus is hard to build – some strongly support it and some do not
- Now on draft-livingood-negative-trust-anchors-06 but still not full consensus
- Backed up a step to try to build consensus on more basic issues:
  - draft-livingood-auth-dnssec-mistakes-01
  - draft-livingood-dont-switch-resolvers-01

# draft-livingood-auth-dnssec-mistakes-01

- “Responsibility for Authoritative DNSSEC Mistakes”
- Intended to explain that authoritative entities are ultimately responsible for authoritative DNS misconfigurations

# draft-livingood-dont-switch-resolvers-01

- “In Case of DNSSEC Validation Failures, Do Not Change Resolvers”

- Intended to discourage changing to non-validating resolvers to “route around” DNSSEC failures

# The end