Analysis of DNSSEC Validation Failure
Comcast – DNS Engineering

Affected Domain: NASA.GOV
Date of Incident: 18 January 2012
Report Released: 24 January 2012

What is DNS Security Extensions (DNSSEC)?
DNSSEC is an enhanced level of Internet security that allows websites and Internet Service Providers (ISPs) to validate domain names (e.g. example.com) to ensure they are correct and have not been tampered with. This prevents hackers from injecting false information (i.e. DNS cache 'poisoning'), to attempt to re-direct people trying to access a real website to a fake, phishing or criminal site. To learn more about DNSSEC see:
http://www.dnssec.comcast.net
https://www.dnssec-deployment.org
http://www.dnssec-tools.org

1 - Executive Summary
On January 18, 2012, the NASA.GOV domain had a DNS Security Extensions (DNSSEC) signing error that blocked access to all NASA.GOV sites when using DNS recursive resolvers performing DNSSEC validation. As one of the largest ISPs in the world utilizing DNSSEC validation, users of Comcast noticed a problem when attempting to connect to the website. This caused some people to incorrectly interpret this as Comcast purposely blocking access to NASA.GOV and recommending users switch from Comcast security-aware DNS resolvers to resolvers not performing DNSSEC validation. Ironically, the NASA Watch website suggested it was curious why Comcast chose to block NASA.GOV websites during the SOPA and PIPA protest day. The DNS resolution issue with NASA.GOV was *not* a form of blocking or censoring of the domain. Instead, the administrators of the NASA.GOV domain had enabled DNSSEC signing for their domain, and the security signatures in their domain were no longer valid. The Comcast DNS resolvers correctly identified the DNSSEC signature errors and responded with a failure to Comcast customers. This is the expected result when a domain can no longer be validated, and this protects users from a potential security threat.

2 - Does Comcast Monitor for DNSSEC Validation Failures?

Yes. Comcast subscribes to many industry email lists, where current DNS issues are discussed (i.e. bind-users@lists.isc.org, dns-operations@lists.dns-oarc.net, etc.) and these users on those lists often report DNSSEC operational issues. DNSSEC validation failures are also one of the Key Performance Indicators (KPIs) that we track. Above certain thresholds, alarms are triggered that alert our engineers to a potential problem that requires investigation. Depending upon the issue, Comcast may proactively contact the domain owner to help them identify and correct the problem, as we have done over the past few years. In some cases, Comcast may implement a "Negative Trust Anchor" (Section 7) to temporarily bypass DNSSEC validation for the affected domain in order to give that domain time to resolve a misconfiguration while also restoring access for Comcast customers.

3 - What Does Comcast Recommend in Cases of DNSSEC Validation Failures?

1. Check what the Comcast DNS recursive resolvers are showing by visiting http://dns.comcast.net and using the cache check tool.
2. Verify the Comcast DNS recursive resolvers are not showing errors for that domain by using the "dig" tool, which is natively available in Linux and Mac OSX. (i.e.: dig +dnssec @75.75.75.75 domain.com)
3. Verify that DNSSEC validation is the problem by using a diagnostic tool.
    a. Test with DNSViz, created and maintained by Sandia National Laboratories, at http://dnsviz.net.
    b. Test with the DNSSEC Debugger, created and maintained by VeriSign Labs, at http://dnssec-debugger.verisignlabs.com.
4. If DNSSEC is broken, locate and contact the appropriate email of the affected domain by using dig (i.e.: dig @75.75.75.75 domain.com SOA) and/or report this in a public forum such as a web forum or on Twitter.
5. After attempting to contact the domain owner, alert Comcast.
    a. Via Twitter @ComcastCares
    b. Via our customer support forum at http://forums.comcast.com
6. Comcast will conduct an investigation of the issue and, in some cases, implement a "Negative Trust Anchor" (Section 7) to temporarily bypass DNSSEC validation for the affected domain. This would restore access for Comcast customers and provide enough time for the domain owner to resolve a misconfiguration.

4 - How Did the NASA.GOV Domain Fail?

The NASA.GOV domain administrators performed a Key Signing Key (KSK) rollover by (1) generating a new key and (2) signing the NASA.GOV domain with the new key. However, they did not use a double-signing procedure for the KSK and a pre-publish procedure for the ZSK. Double-signing refers to signing a zone with two KSKs and than updating the parent zone with the new DS record so that both keys are valid at the same time.

This meant that the domain NASA.GOV was signed with the new KSK, but it was not double-signed with the old KSK. So, the new key was used for signing the zone but the old key was not. As a result, the domain could not be trusted and returned an error when trying to reach the domain.

Thus, the domain was in a situation where the DNSSEC chain of trust was broken because the Delegation Signer (DS) record pointed to the old KSK , which was no longer used for signing the zone. (A DS record provides a link in the chain of trust for DNSSEC from the parent zone to the child zone – in this case between .GOV and NASA.GOV.) While an investigation found this to be due to a failure in updating the key, a similar breakage could have occurred if an attacker gained access to the domain's authoritative servers and modified those records or had the domain pointed to their own rogue authoritative servers.

5 - How Did Comcast Respond?

Comcast noticed the issue, checked resolution of the domain in our servers, and then checked DNSSEC validation via DNSViz. Once we saw it was an apparent DNSSEC misconfiguration, we contacted the domain administrator to confirm this. Once we were able to confirm this, we added a "Negative Trust Anchor" (Section 7) for the domain on a temporary basis.

6 - How did the NASA.GOV Domain Fix the Issue?

The domain fixed the problem by reverting back to the old key that was trusted upstream in the .GOV TLD. The NASA.GOV domain administrators also corrected their internal procedure to prevent this issue from occurring again in the future.

7 - What is a Negative Trust Anchor?

When a domain has been confirmed to be failing DNSSEC validation due to a DNSSEC-related misconfiguration, Comcast may in some cases use a Negative

Trust Anchor for a domain. This instructs Comcast DNS recursive resolvers to temporarily NOT perform DNSSEC validation for the domain in question. This immediately restores access to the domain for Comcast customers while the domain's administrator corrects the misconfiguration(s). This tool is unlikely to be used over the long-term, and continued and frequent use of the tool is not scalable. However, it is useful in the short-term as organizations that are new to signing their domains are still maturing their DNSSEC operational practices.

8 - How Does This Compare to Other DNS Misconfigurations?

Utilizing Negative Trust Anchors for DNSSEC misconfigurations increases operational overhead and is not scalable over the long-term. Negative Trust Anchors have proven useful during the early stages of DNSSEC adoption, but as DNSSEC becomes another standard for DNS configuration, domain owners will ultimately be responsible for managing and ensuring their DNS records are configured correctly. Comcast cannot correct misconfigured A, CNAME, MX, etc. records of domains that we are not authoritative for (not the domain owner). Comcast may continue to implement Negative Trust Anchors on a case-by-case basis to address the misconfigurations, but this is only a short-term solution.

9 - How Did Users Interpret the Failure?

The DNSSEC-related misconfiguration of the NASA.GOV domain unfortunately occurred on the same day that some Internet websites such as Wikipedia and Reddit blacked out their sites in protest over the proposed SOPA and PIPA bills in in the U.S. Congress. Comcast has recently made clear, following the completion of our deployment of DNSSEC, the challenges and incompatibilities of DNS modification (at http://blog.comcast.com/2012/01/comcast-completes-dnssec-deployment.html and http://blog.comcast.com/2012/01/comcast-domain-helper-shuts-down.html).

Despite this, a website that discusses NASA-related news and information, called NASA Watch (http://www.nasawatch.com) accused Comcast of blocking access to the NASA.GOV domain, seemingly on purpose.

Users on Twitter also reported this and interpreted this as Comcast blocking access to NASA.GOV, generally by re-tweeting a tweet by @NASAWatch. Users

also reported and discussed this on the Comcast customer support forums (http://forums.comcast.com).

Finally, Alan Boyle, science editor for MSNBC.com, suggested on Twitter that affected users change their DNS from Comcast's secure DNS to Google Public DNS. (See https://twitter.com/b0yle, and http://www.msnbc.msn.com/id/10912485/ns/technology_and_science/t/alan-boyle/ - .Txd7_mNSTQU) He later tweeted that the issue was resolved and that users should switch back to the Comcast DNS servers.

See Section 12 for details.

10 - Why is Switching to an Alternative (Non-Validating) Resolver a Bad Idea?

If a domain fails DNSSEC validation and is inaccessible, this could very well be due to a security-related issue. In order to be as safe and secure as possible, we strongly recommend against changing to DNS servers that do not perform DNSSEC validation as a workaround. Even if a website in a domain seems to look "normal" and valid, including any applicable SSL certificates, according to the DNSSEC protocol, that domain is not secure. Domains that fail DNSSEC for legitimate reasons may be in control of hackers or there could be other significant security issues with the domain.

11 - What Did Diagnostic Tools Reveal During the Failure?

Comcast used the DNSViz tool, at http://dnsviz.net, to diagnose the failure. This tool was developed and is maintained by Sandia National Laboratories.

(SECTION CONTINUES ON NEXT PAGE)

Analysis of DNSSEC Validation Failure
Comcast – DNS Engineering

Figure 1: This is a diagnostic image of NASA.GOV when the issue occurred on 18 January 2012, with the problems highlighted in red:

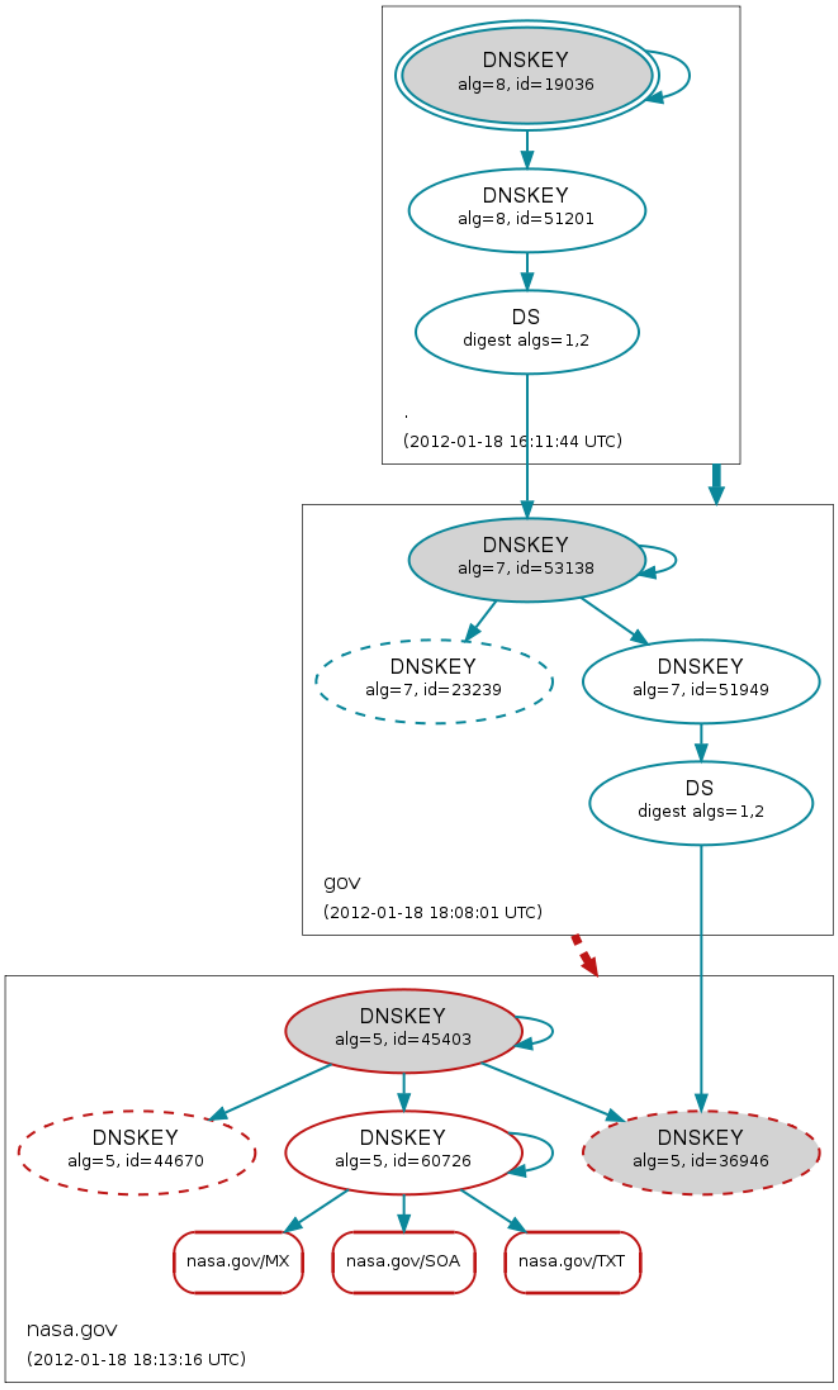


Figure 2: This is a diagnostic image of NASA.GOV on 19 January 2012, with the issue solved (no errors shown):

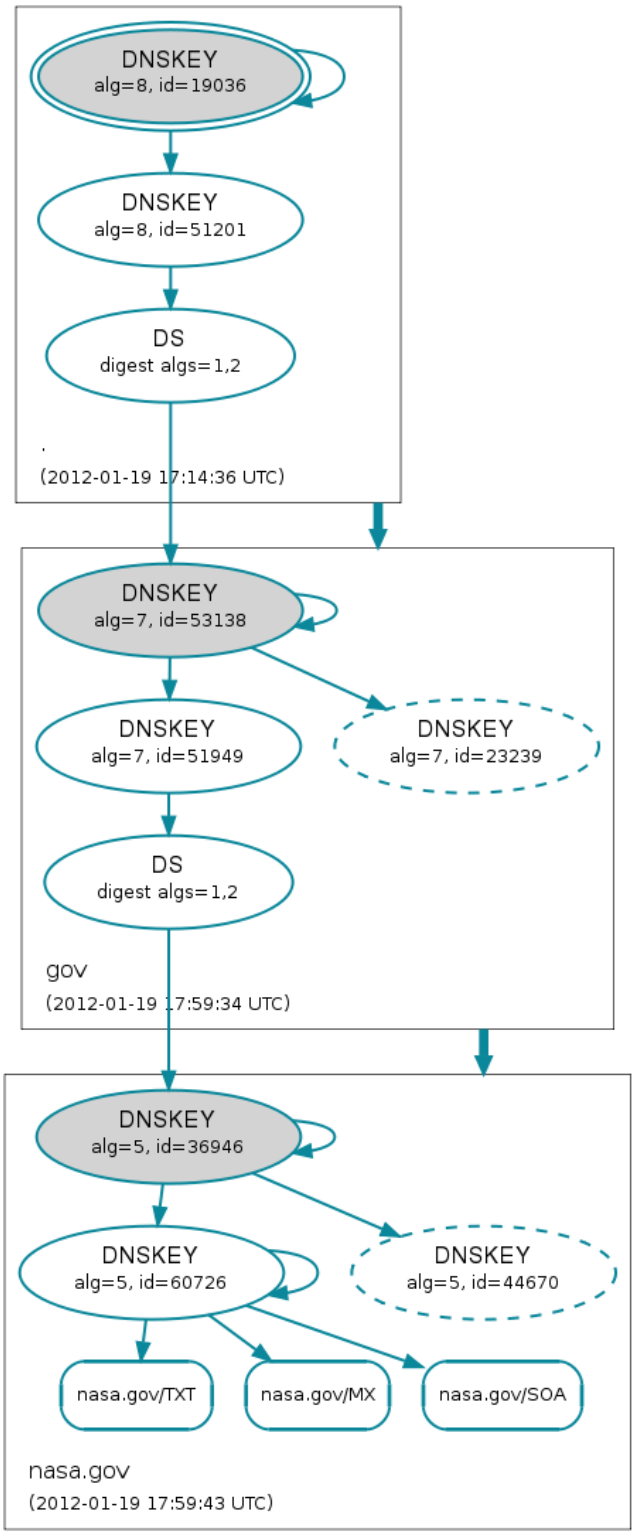
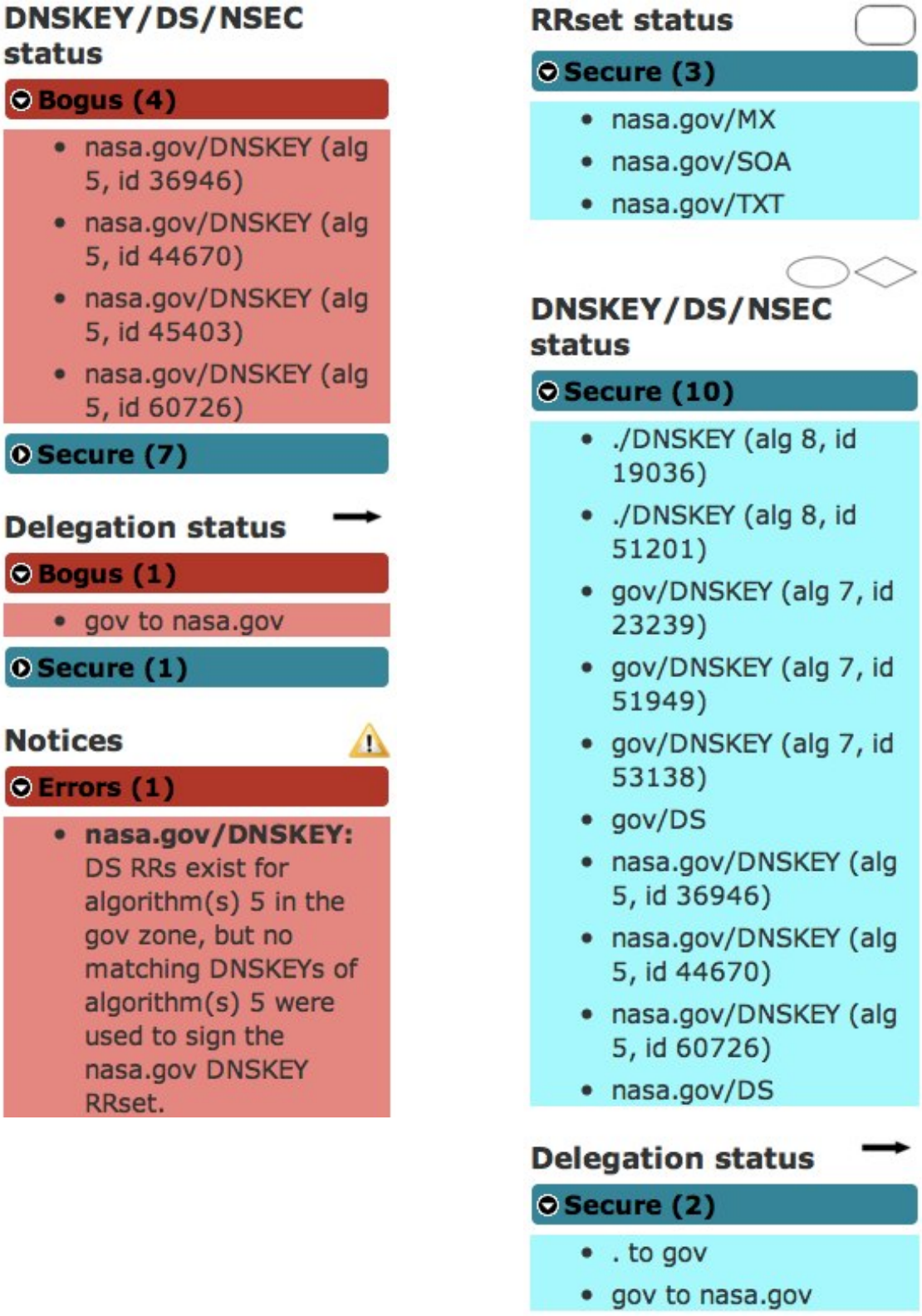


Figure 3: The following images are detailed comparative diagnostics of the NASA.GOV domain during the failure (left) and after it was resolved (right).



12 – Selected Mentions on the Internet

Figure 4: NASA Watch, http://nasawatch.com/archives/2012/01/comcast-blocks.html

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.

Keith's update: I have confirmed this via IT professionals at NASA and in several places across the U.S. that Comcast DNS is broken - but only for NASA.gov, it would seem.

Keith's update: Alan Boyle from MSNBC tweeted some good advice - change your DNS setting to Google's Public DNS. Info here.

Keith's update: Everything works again. Apparently NASA provided an update key for DNS and the new key did not match the Comcast key. So Comcast simply cut off DNS access for all of its customers to everything at NASA.gov. The old key has been sent by NASA and everything works again - so far.

Categories: IT/Web

Tags: Comcast, NASA.gov

ARTICLE TOOLS Print Tweet 36

Figure 5: Twitter amplification of the NASA Watch report

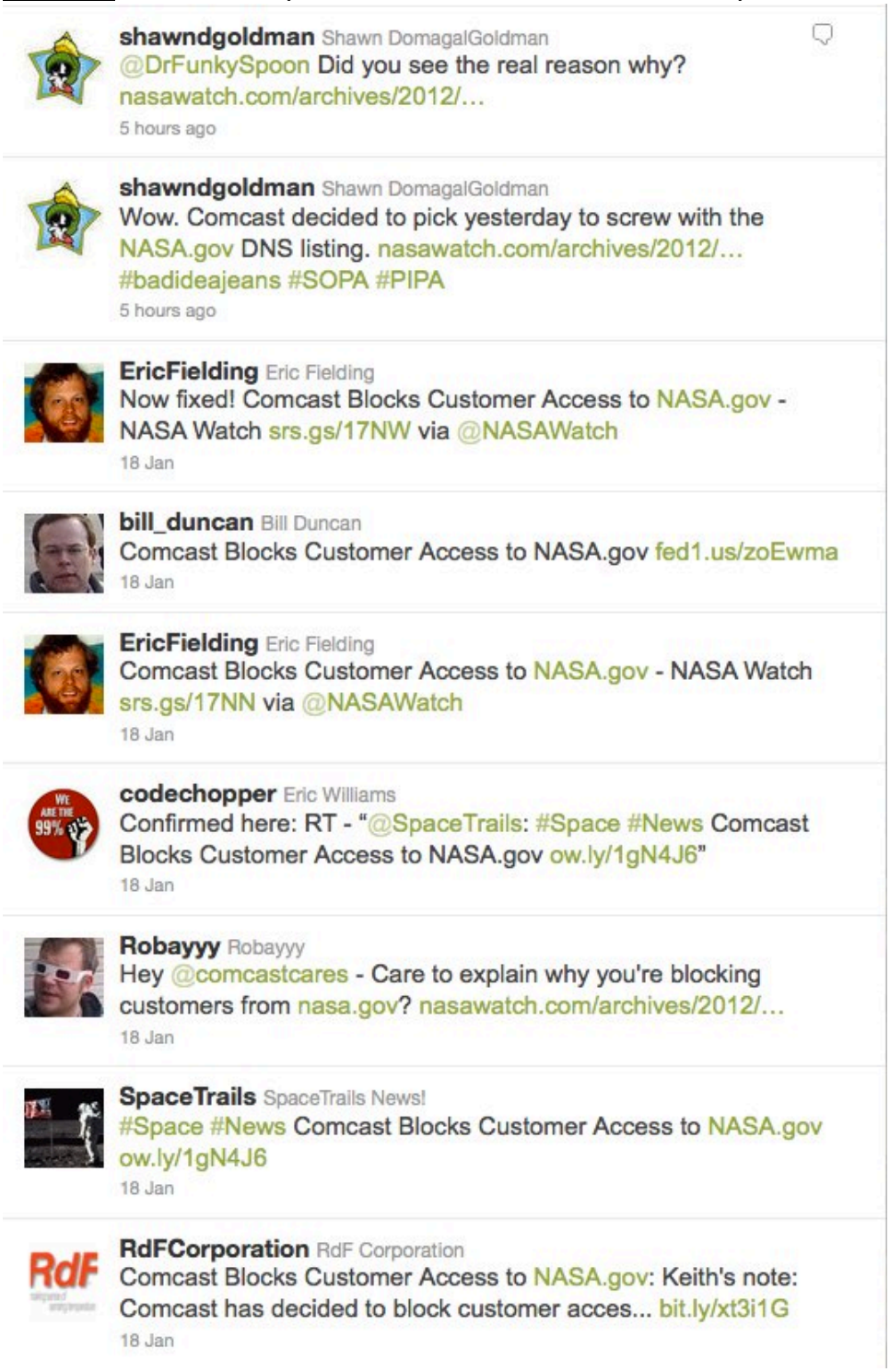
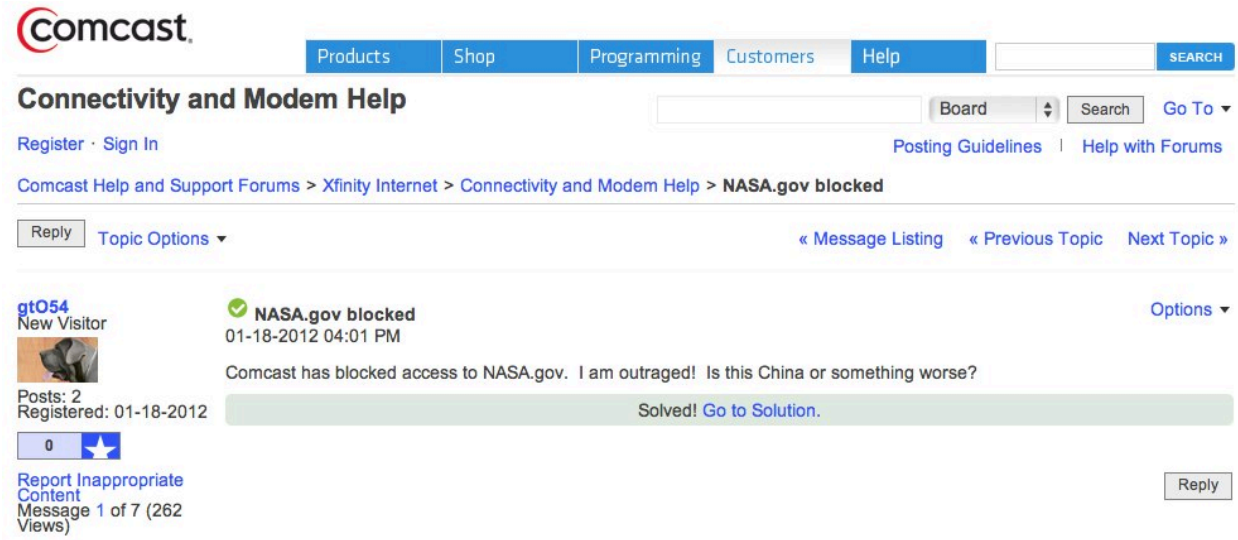


Figure 6: MSNBC science editor's tweets

Figure 7: Report on Comcast's Customer Forum at http://forums.comcast.com/t5/Connectivity-and-Modem-Help/NASA-gov-blocked/td-p/1169657



Authors and Key Contributors
John Barnitz, Comcast
Ralph Bischof, Jr., NASA
Tom Creighton, Comcast
Chris Ganster, Comcast
Chris Griffiths, Comcast
Jason Livingood, Comcast

Acknowledgements
The Contributors wish to thank Russ Mundy, from Sparta, Inc., for his review and feedback on a draft of this document. We also wish to thank Ralph Bischof, Jr., from NASA for his insight into the incident and his contributions to the document, which will surely help other DNSSEC implementers in the future.