NEGATIVE TRUST ANCHORS

March 2018

Joseph Crowe

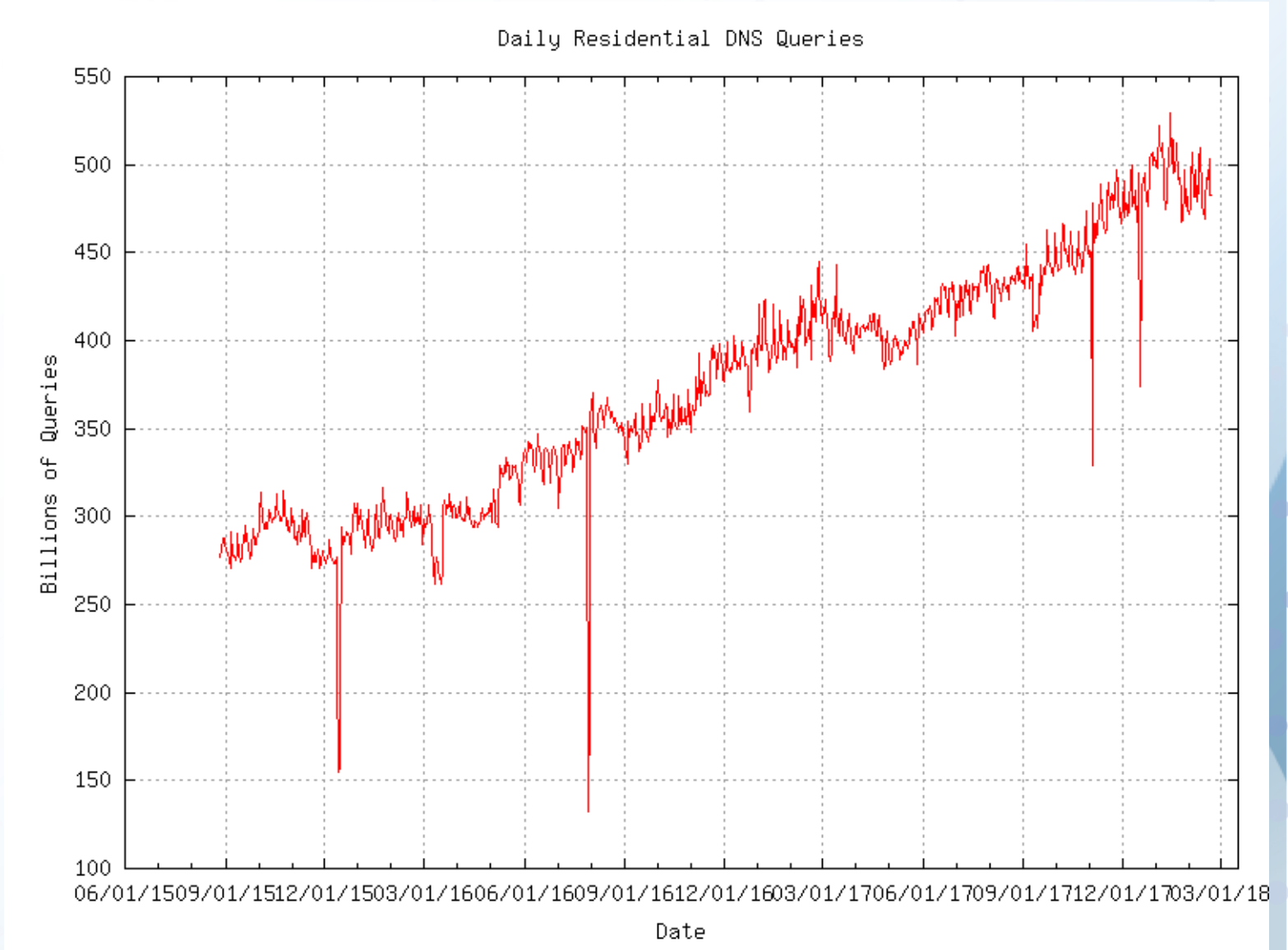
Technology Product Xperience – Comcast

COMCAST

DNS AT COMCAST

THAT'S A LOT OF QUERIES!

- Over 500B queries per day across our footprint
- DNSSEC Validation since 2012
- DNSSEC **Does scale.**



COMCAST

WHAT DOES THAT MEAN FOR COMCAST?

WHEN DNSSEC VALIDATION FAILS, WE GET THE BLAME

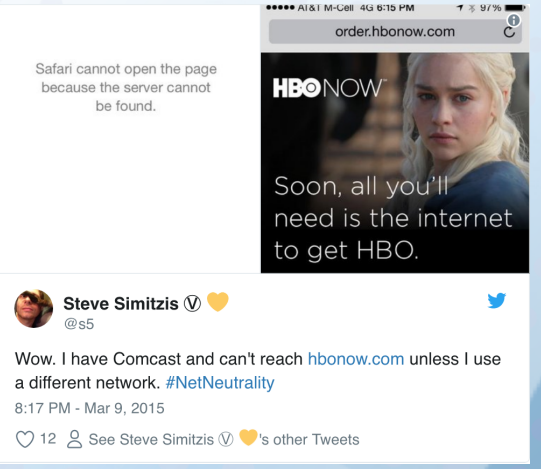
- Customers will believe we are “blocking” websites
- When big companies break DNSSEC, Comcast customers will reach out, **QUICKLY**
- Suggested “Fixes”
  - Switch to a non-validating resolver
  - Guess what?! Google’s public resolvers will fail to resolve as well
  - Temporarily ”Fix” with a Negative Trust Anchor (RFC 7646) and allow for the zone to be repaired
    - Re-sign the zone and update DS record
    - Allow for TTL to expire (Improper key roll-over)
    - Remove DS record at registrar

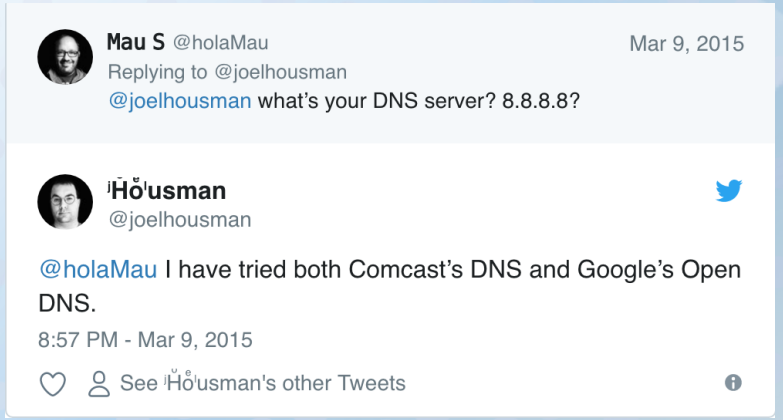

Deploy360 10 March 2015

HBO NOW DNSSEC Misconfiguration Makes Site Unavailable From Comcast Networks (Fixed Now)

By Dan York
Senior Manager, Content and Web Strategy

Wow! Talking about insanely bad timing... yesterday at Apple’s big event, HBO announced “HBO NOW”, a new streaming service available





COMCAST

WHY USE A NEGATIVE TRUST ANCHOR?

BEING TOO BIG TOO FAIL

If a major domain fails DNSSEC validation:

- There may be a major security issue
- There may be an operational error
- There may be a process error
- There may be a technical error

DNSSEC FAILURE EXPERIENCE

- Most DNSSEC failures are a result of an error
- Very rarely have noticed security related issues
- Customer complaints can be very vocal, especially with social media and phone calls

WHAT DO WE DO?

There are a few options:

- Just let the domain to continue to fail
- Turn off DNSSEC validation
- Use a Negative Trust Anchor and turn off validation for that one domain

COMCAST

IMPLEMENTING A NEGATIVE TRUST ANCHOR

PROCESSES ARE A GOOD THING

- Initiate conversation
- Come up with when and why
- Figure how to implement within your resolvers
- Stay consistent with processes and revisit as new things may shape a new process

STANDARD PROCESS

- Understand the risks of keeping a domain fail DNSSEC
- Reach out to the domain owners and let them know that DNSSEC is failing
- Usually allow them time to fix the issue
- Update the community via our @ComcastDNS twitter handle that we are aware of an issue

AUTOMATE ALL THE THINGS!

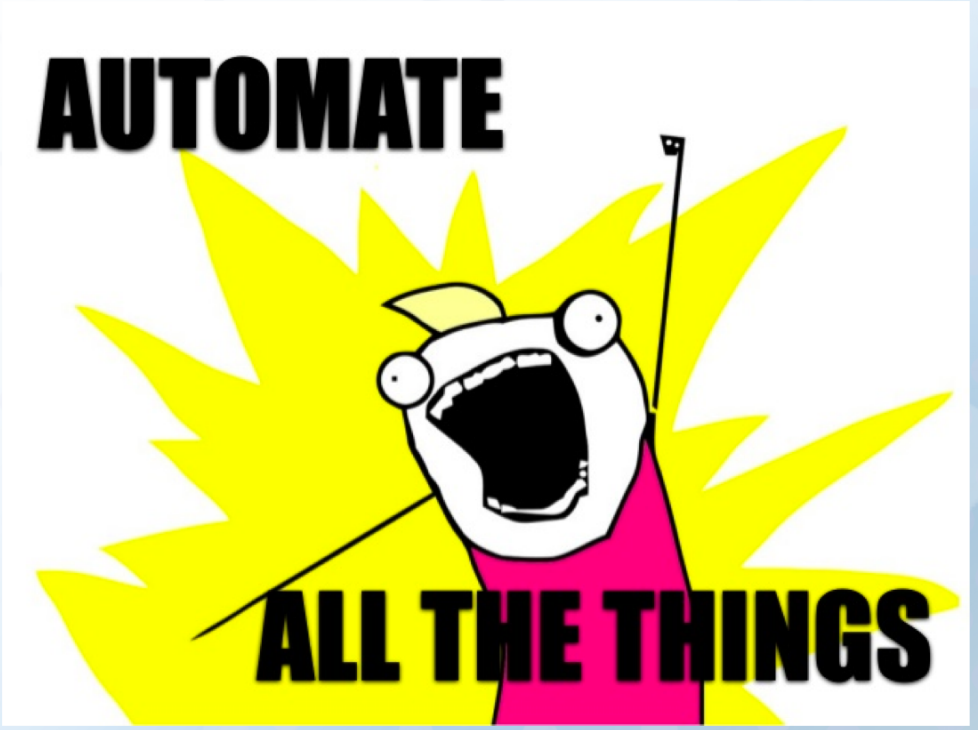
- Automation is a major key to success
- If a Negative Trust Anchor is approved to be put in, updating one location is better than multiple
- After domain is fixed use the same automation to remove the Negative Trust Anchor
- Do NOT rush to implement a Negative Trust Anchor

COMCAST

AUTOMATION HELPS AT SCALE

WHY AUTOMATE

- Trying to implement a Negative Trust Anchor for more than 25 resolvers can be time consuming
- May be running multiple vendors with different commands
- If there is an error, there is an error in one spot and it’s broken the same across the board



COMCAST

AUTOMATION HELPS AT SCALE

BASIC AUTOMATION @COMCASTDNS

- Utilize SaltStack for our automation tools
- Pillar data allows us to use one spot to our create and apply our Negative Trust Anchors
- Allows that pillar data to be consumed by more than one vendor
- One command needs to be run from a Salt Master and can reach our entire foot print

BASIC STRUCTURE

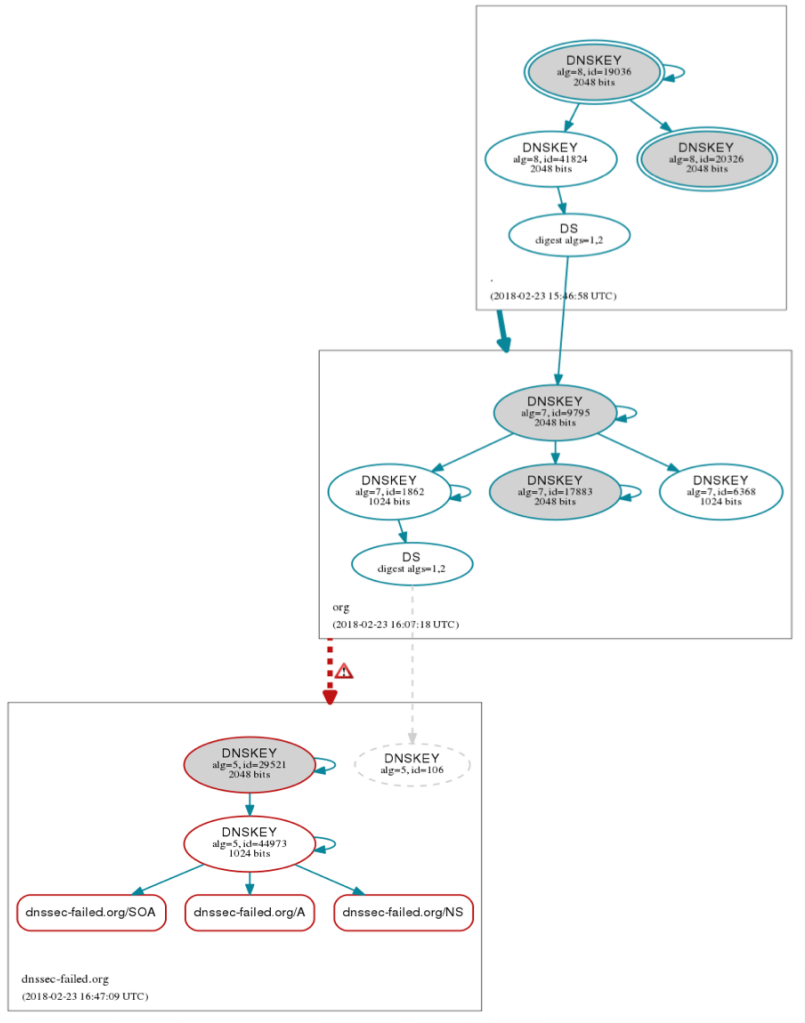
- We include something similar in our pillar data below in YAML format

```
cust_nta:
  - site1.com
  - site2.net
  - site3.com
  - dnssec-failed.org
```

- We then apply the NTA state to all of our resolvers via a salt command on our Salt Masters
- The above pillar data is then used to populate files and scripts, which in turn run the NTA commands needed for all of our resolvers across our footprint

COMCAST

TROUBLESHOOTING DNSSSEC



- Can you dig it?
  - DNSSEC Failure will result in a SERVFAIL
  - Appending a +cd to dig will disable DNSSEC checking and confirm a DNSSEC issue
  - Test with another DNSSEC validating resolver
- dnsviz.net is your friend
  - Third-party tool that allows you to show the customer that it's not just your resolver.
  - Provides information on what is broken and where
- In case of key rollover issue
  - Automate checking the domains you own
  - Cache flush may fix DNSSEC failure – just for your resolvers

COMCAST

SOME LIGHT READING MATERIAL

HTTPS://WWW.INTERNETSOCIETY.ORG/BLOG/2015/03/HBO-NOW-DNSSEC-MISCONFIGURATION-MAKES-SITE-UNAVAILABLE-FROM-COMCAST-NETWORKS-FIXED-NOW/

HTTPS://TOOLS.IETF.ORG/HTML/RFC4035

HTTPS://TOOLS.IETF.ORG/HTML/RFC7646

HTTP://DNSVIZ.NET

HTTP://WWW.SALTSTACK.COM

COMCAST


COMCAST