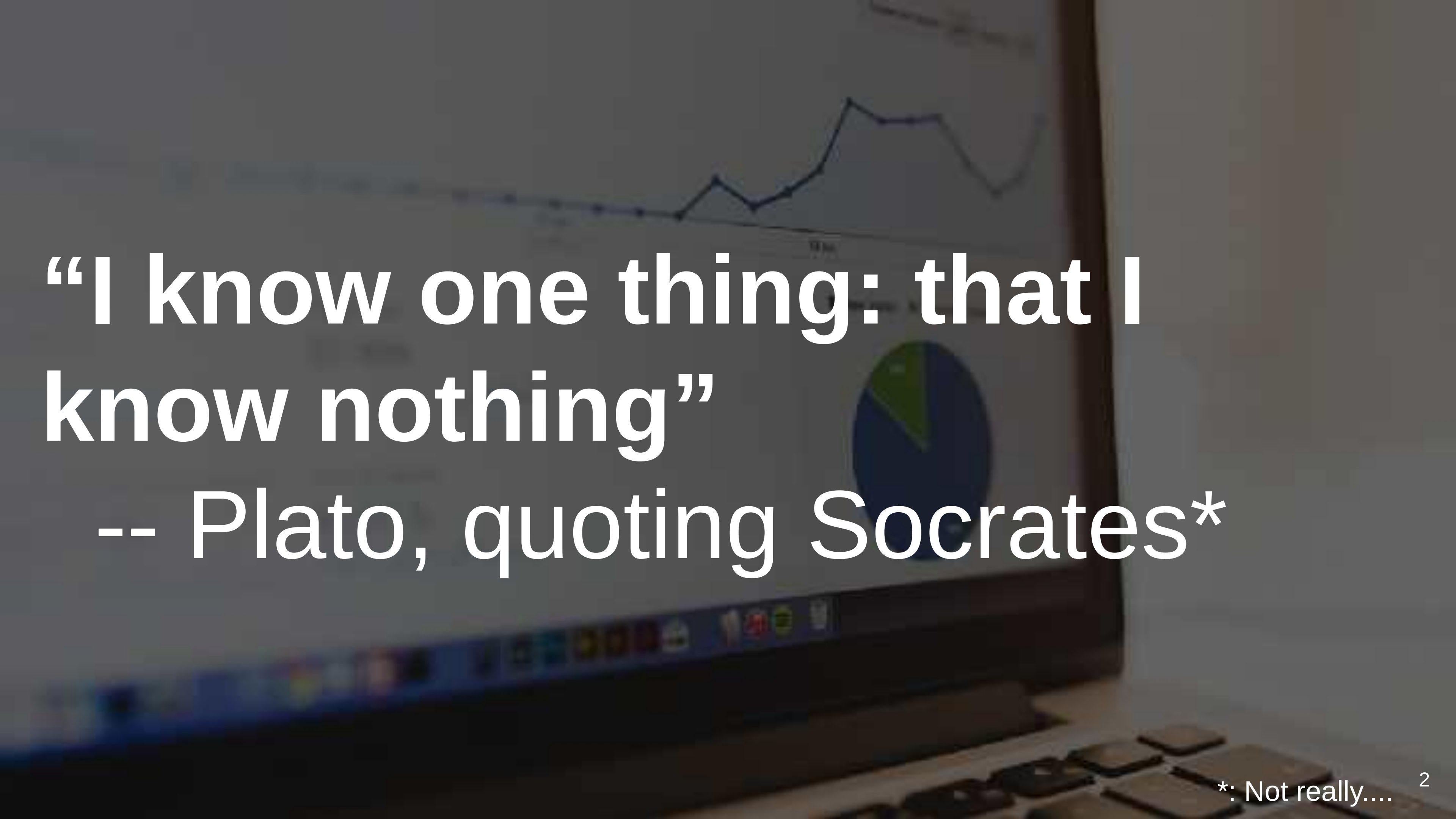
Aggressive use of NSEC/NSEC3

draft-ietf-dnsop-nsec-aggressiveuse

ICANN57 - Hyderabad, .in - 11/2016 V0.02



“I know one thing: that I know nothing”

-- Plato, quoting Socrates*

*: Not really....

Background

DNSSEC provides authentication of both *positive* and *negative* answers

Positive answers get a signature proving that they are valid; negative answers include a signature proving that the name doesn't exist

- NSEC (Next SECure) records list the alphabetical records on each side of the non-existing name, and signs the gaps

50’000ft example / reminder

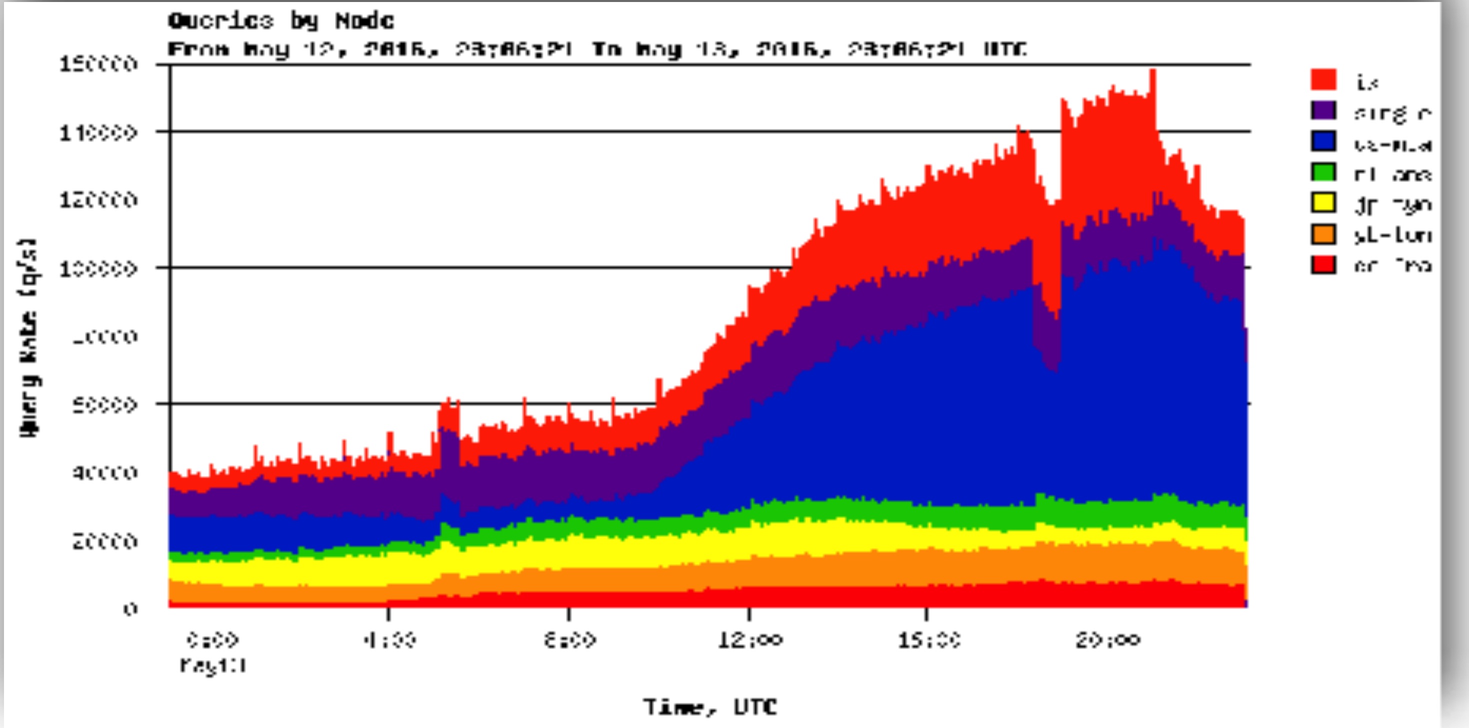
```
wkumari$ dig +dnssec  belkin
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 41230
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; QUESTION SECTION:
;belkin.          IN       A
;; AUTHORITY SECTION:
.        1795     IN       SOA      a.root-servers.net. nstld.verisign-grs.com.
2016070901 1800 900 604800 86400
beer.    21512    IN       NSEC      bentley. NS DS RRSIG NSEC
beer.    21512    IN       RRSIG    NSEC 8 1 86400 20160719170000 20160709160000
46551 . AoT2Oe3eVZ3pC1DousLXDYABGuTTvkyP4rbBXvquGp3T/Lg7Rer3Vx2g oC9p5u6T+lj/
3u879htWNRO62wSdODkvOdtVFA5iJxN9DJ5EtuJdbuL/
xJuPhoin+0Fc6Vtf0X0l7e5TBtxYAyPZqUq6dxm6qE/NW6Ft1nAv3GYX jlg=
;; Query time: 222 msec
```

So?

- This document allows recursive servers to synthesize answers from NSEC (and wildcard) records already in cache
  - Improves privacy
  - Decreases latency / improves performance
  - Saves resources on recursive and auth name-servers
  - Improves DDoS resilience

Couldn’t have made a better example if I’d planned it...

- May 12, 2016 (a Friday afternoon), Colin Petrie / Kaveh Ranjbar from RIPE poked me: “Google is suddenly sending K-root way more junk queries, e.g ‘nq0nnjzba-fn.357.225.340.251’. It burns us, please make it stop…”



Well, that’s not good….

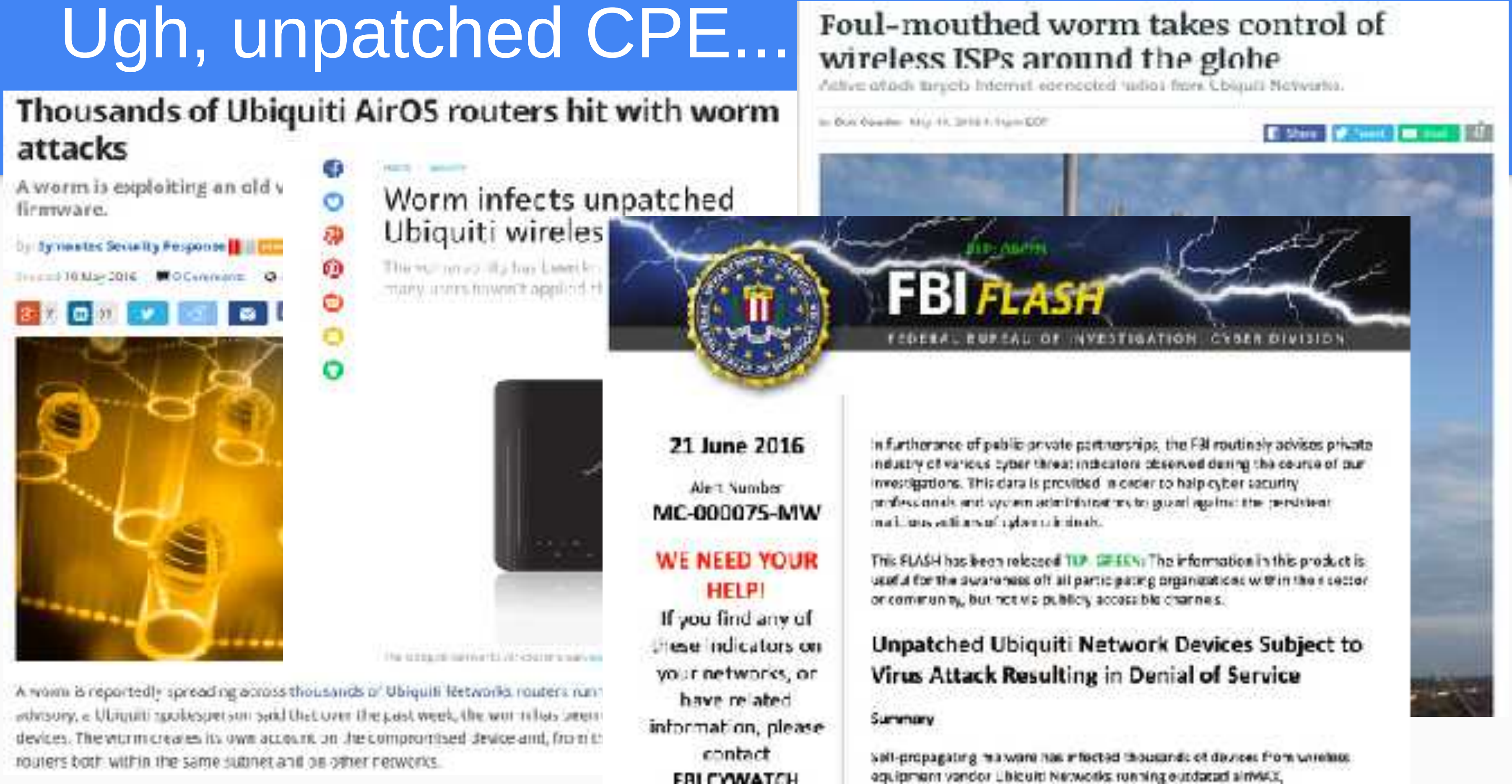
What’s causing this?

- Have we got some bug?
- Did anyone change anything?!
- Are we being used as a DoS reflector?
- Why does the graph look more like organic growth than a DoS attack?

Phew! It’s not just Google Public DNS, just we show up towards the top…

...still, what’s causing this? And why? And can we make it stop?

Ugh, unpatched CPE...



Thousands of Ubiquiti AirOS routers hit with worm attacks

A worm is exploiting an old v
firmware.

by Symantec Security Response

Created 18 May 2016 0 Comments

A worm is reportedly spreading across thousands of Ubiquiti Networks routers run
advisory, a Ubiquiti spokesperson said that over the past week, the worm has been
devices. The worm creates its own account on the compromised device and, from th
routers both within the same subnet and on other networks.

Worm infects unpatched Ubiquiti wireles

The vulnerability has been k
many users haven't applied th

Foul-mouthed worm takes control of wireless ISPs around the globe

Active attack targets Internet-connected radios from Ubiquiti Networks.

by Dan Goodin - May 19, 2016 1:11pm EDT

TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 June 2016

Alert Number
MC-000075-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact
FBI CYWATCH

In furtherance of public private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

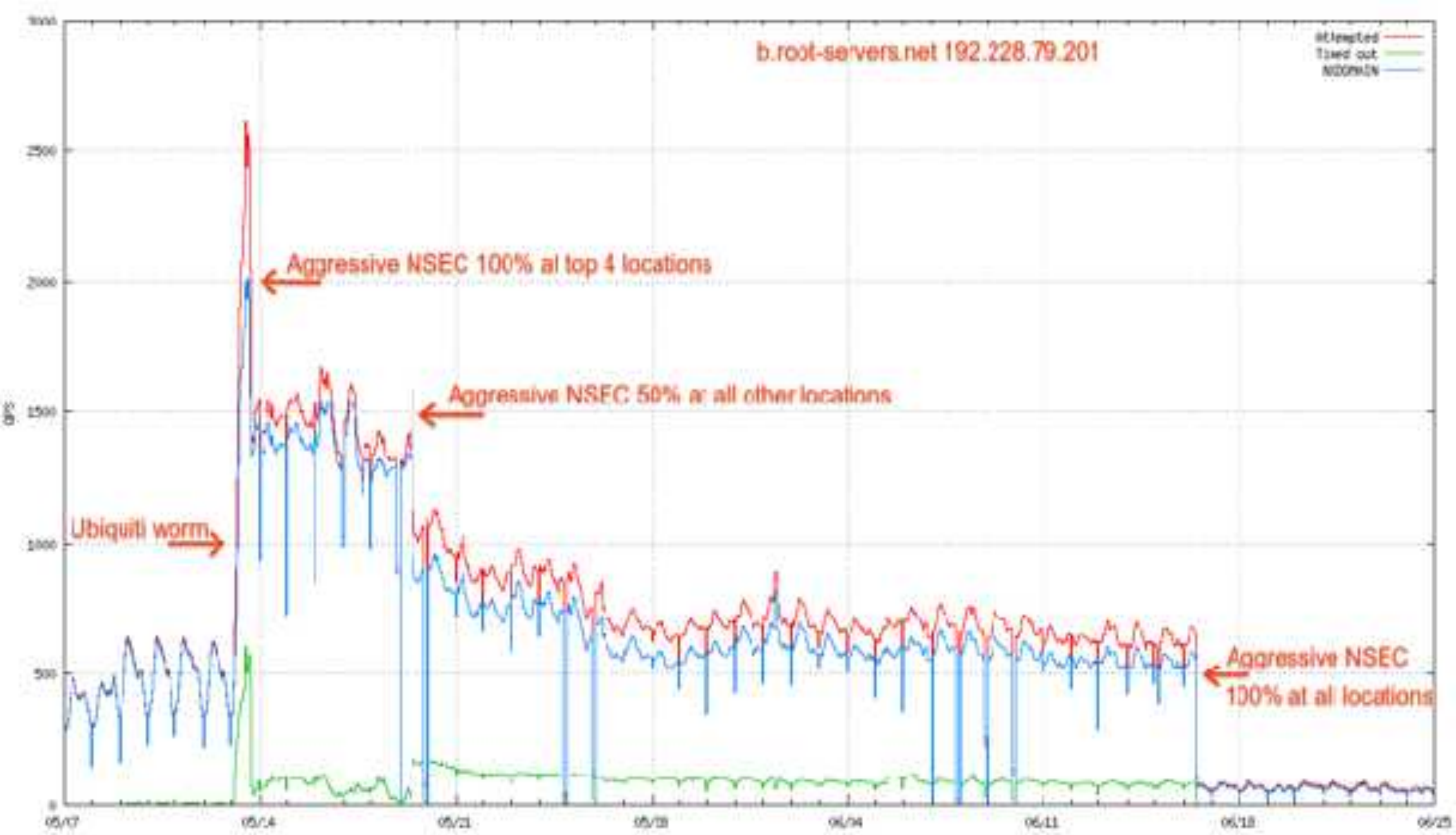
This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but not via publicly accessible channels.

Unpatched Ubiquiti Network Devices Subject to Virus Attack Resulting in Denial of Service

Summary

Self-propagating malware has infected thousands of devices from wireless equipment vendor Ubiquiti Networks running outdated airMAX,

… turning on Aggressive NSEC



What does the document *say*?!

NSEC/NSEC3 records which cover the question can be used to synthesize answers

Wildcards which covers the question can be used to synthesize answers

This relaxes the restrictions in RFC4035:

```
In theory, a resolver could use wildcards or NSEC RRs to generate
positive and negative responses (respectively) until the TTL or
signatures on the records in question expire.  However, it seems
prudent for resolvers to avoid blocking new authoritative data or
synthesizing new data on their own.  Resolvers that follow this
recommendation will have a more consistent view of the namespace.
```

Aggressive NSEC Draft

Status:

Re-added Wildcards

Expanded implementation

Google & Unbound implement

Completed WGLC

Questions?

Notes

This technique may occlude newly added information

- If you ask for foo.example.com, and it doesn’t exist, it doesn’t exist for the NSEC TTL

NSEC3 is trickier than NSEC

- So implementations may choose to only support this for NSEC
  - NSEC3 involves hashing the answers, sorting those, then signing the space between hashes. Aggressive-NSEC3 works like Aggressive-NSEC, you just check if the (hashed) question falls within the space between hashes. Clear as mud?

Wildcard support

- Very similar to NSEC - you get back NSEC and a (signed) wildcard. Use the wildcard instead of NXDOMAIN

Provide knobs for enabling / disabling on a per-domain basis