draft-ietf-dnsop-nsec-aggressiveuse
and
draft-wkumari-dnsop-cheese-shop
“I know one thing: that I know nothing”
-- Plato, quoting Socrates*

*: Not really....
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 .
AoT2o3e3eVZ3pC1DousLXDYABGuTTvkyP4rbBXvquGp3T/Lg7Rer3Vx2g
oC9p5u6T+lj/3u879htWNRO62wSdODkvOdtVFA5iJxN9DJ5EtuJdbuU/
xJuPhoin+0Fc6Vtf0X017e5TBtxYAyPZqUq6dxm6qE/NW6Ft1nAv3GYX jlg=
;; Query time: 222 msec
Could’ve made a better example if I’d planned it...

- May 12, 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?

- 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 firmware.

Worm infects unpatched Ubiquiti wireless

The vulnerability has been known for many years, and many users haven't applied the update.

21 June 2016
Alert Number
MC-000075-MW
WE NEED YOUR HELP!
If you find any of these indicators on your network, or have related information, please contact FBL CYWATCH.

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 4:14pm EDT

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 the 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 / Cheeseshop
Aggressive NSEC Draft

Rewritten to be more readable

Integrated comments / no longer applicable

Better examples

Seeing as this is moving along, no need for Cheese-shop
Updates

- Document adopted by DNSOP WG
- Adoption comments
- Changed main purpose to performance
  - Thanks to Jinmei.
- Use NSEC3/Wildcard keywords
  - Thanks to Matthijs
- Improved wordings (from good comments)
- Simplified pseudo code for NSEC3
- Added Warren as co-author
- Reworded much of the problem statement
- Reworked examples to better explain the problem / solution
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

● Provide knobs for enabling / disabling on a per-domain basis
A few minor edits:

Jinmei provided some comments, mainly suggesting removing references to subdomain attacks.

Typos and grammar nits, fixing references

https://github.com/wkumari/draft-ietf-dnsop-nsec-aggressiveuse