DNS Flag Day and beyond – how will it affect you?

UKNOF42: Cathy Almond, ISC

What’s it all about?

- Some sites still operate software that doesn’t comply with published DNS standards
- DNS software vendors and DNS service providers have ‘helpfully’ been deploying workarounds (checks and retries for a long time)
- The complexity of the workarounds slow down DNS performance and make it harder to implement new features
- These workarounds will be dropped, on or after 1st February 2019

Are you bothered?

- You perhaps should be…
- If your company’s DNS zones are not being served by compliant servers then your online presence will slowly degrade or disappear as ISPs and other organisations update their resolvers
- When you next update your internal DNS resolvers, some sites and email servers may become unreachable – what is your response going to be?

Who is supporting this?

facebook
NLNETLABS
cisco
Google
cz.nic
Quad9
ISC Internet Systems Consortium
CLOUDFLARE
POWERDNS AN OX COMPANY
CleanBrowsing

Source: https://dnsflagday.net/#supporters

See also: https://github.com/dns-violations/dnsflagday

DNS FLAG DAY

BIND

- BIND 9.14 (stable) to be released early 2019 – removes resolver workarounds for servers that misbehave when queried with EDNS
- BIND as an authoritative server is already compliant with current DNS standards

PowerDNS

- PowerDNS recursor 4.2 (to be released soon) will be the first one to no longer accommodate non-compliance
- On the authoritative side, PowerDNS 4.1 is fully compliant; 4.0 has some corner cases that ednscomp notices but that are not a problem in practice - disabling caching removes those edge cases

Knot

- Knot Resolver – newer than the others – already written without most of the workarounds for misbehaving servers. 3.3.0 (soon to be released) has some minor changes
- In general anyone already running the latest version (3.2.0) should not notice any significant differences upgrading to 3.3.0

Unbound

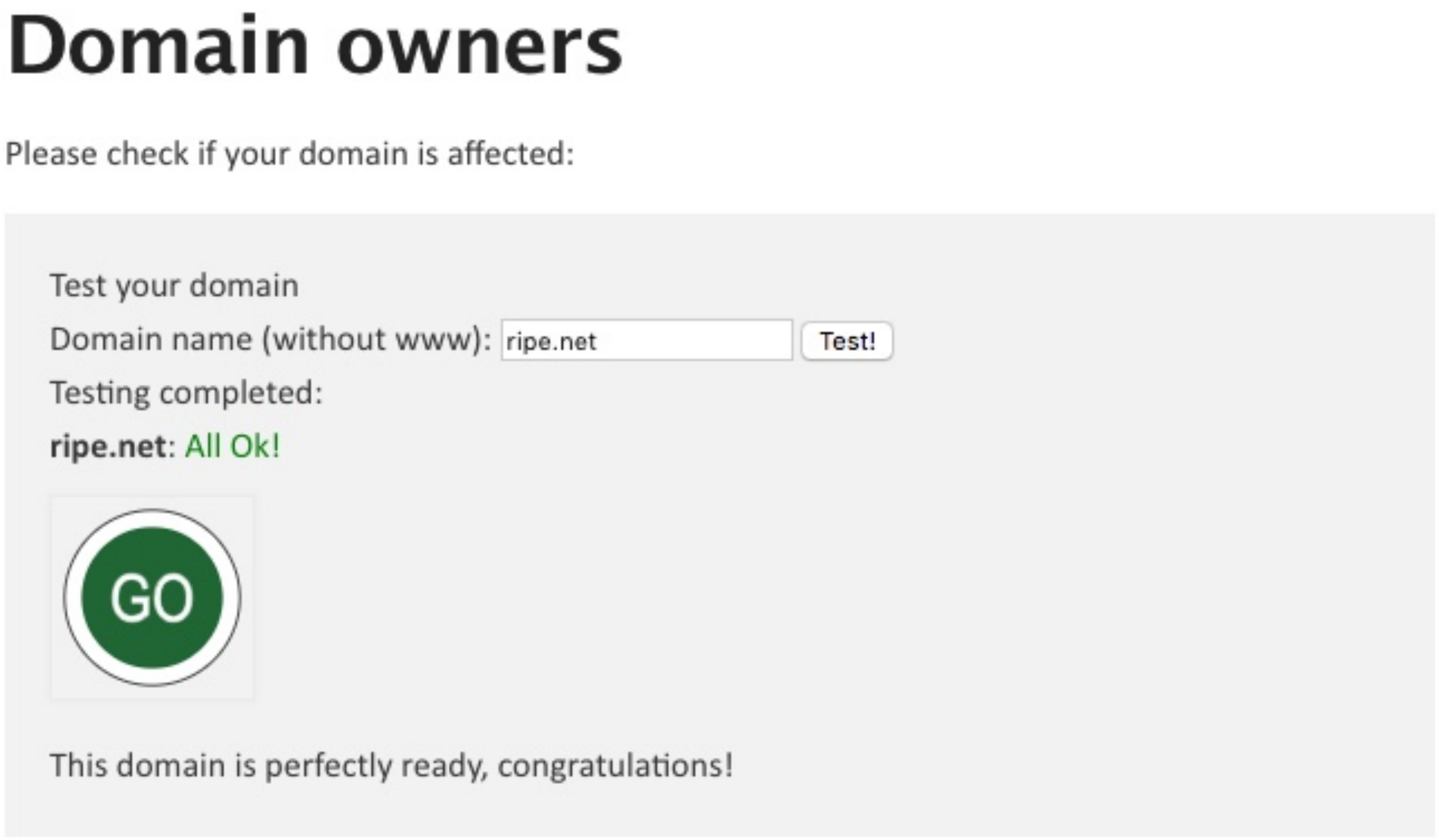
- Unbound versions released after 1st February 2019 (1.8.4, 1.9.0 and newer) will no longer retry without EDNS when no response is received
- Unbound will still accept answers without EDNS, and will still send a query without EDNS when it receives a FORMERR or NOTIMPL answer. (This change will only affect queries that result in a time-out because of EDNS in the query)

Others

- Supporters who provide public resolvers (recursive servers) will, over a short period of time, drop workarounds and thus stop resolving broken domains
- Appliance vendors whose DNS engine is based on source code from the Open Source providers listed earlier, will also over time drop workarounds and stop resolving broken domains

Test your domains

https://dnsflagday.net/



Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): ripe.net

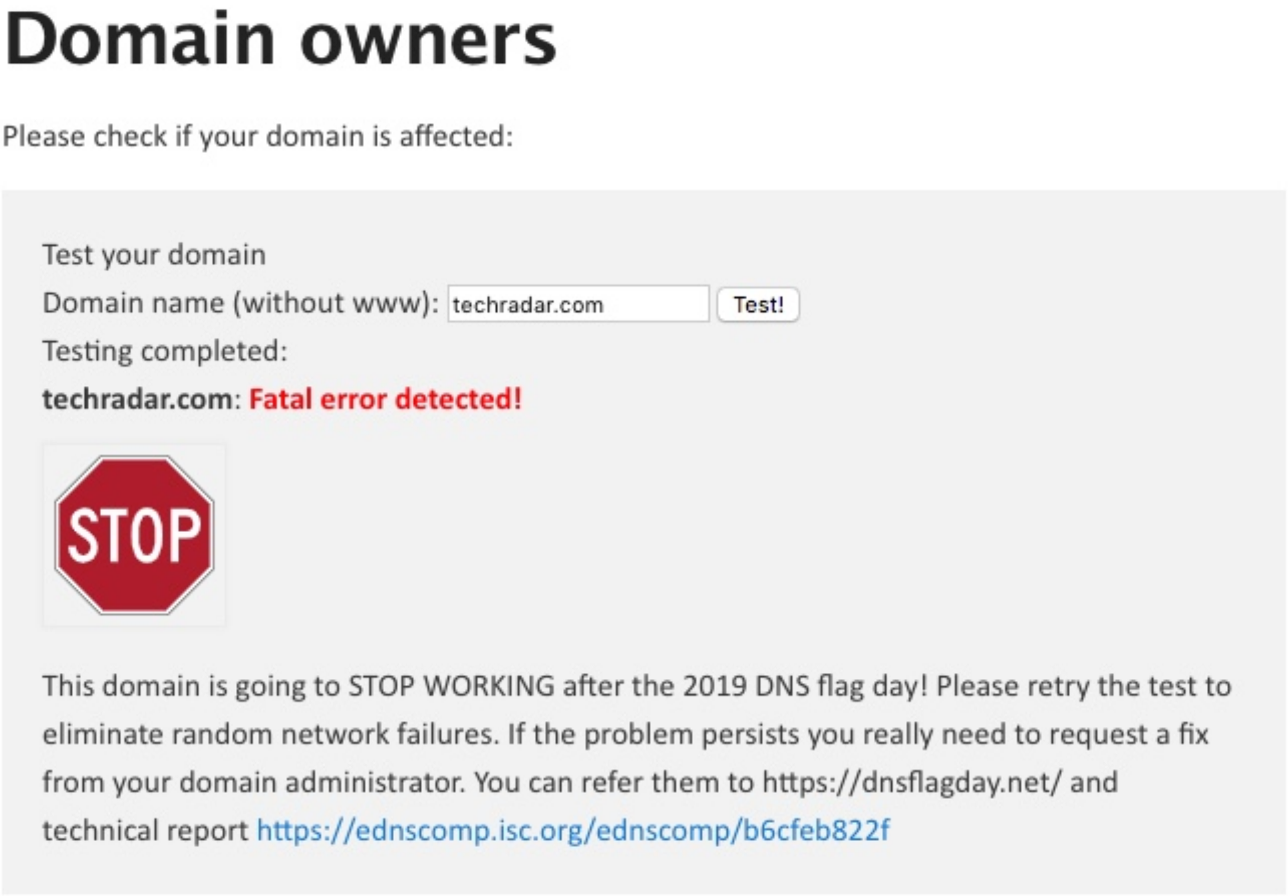
Testing completed:

ripe.net: All Ok!

This domain is perfectly ready, congratulations!

Test your domains

https://dnsflagday.net/



Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): techradar.com Test!

Testing completed:

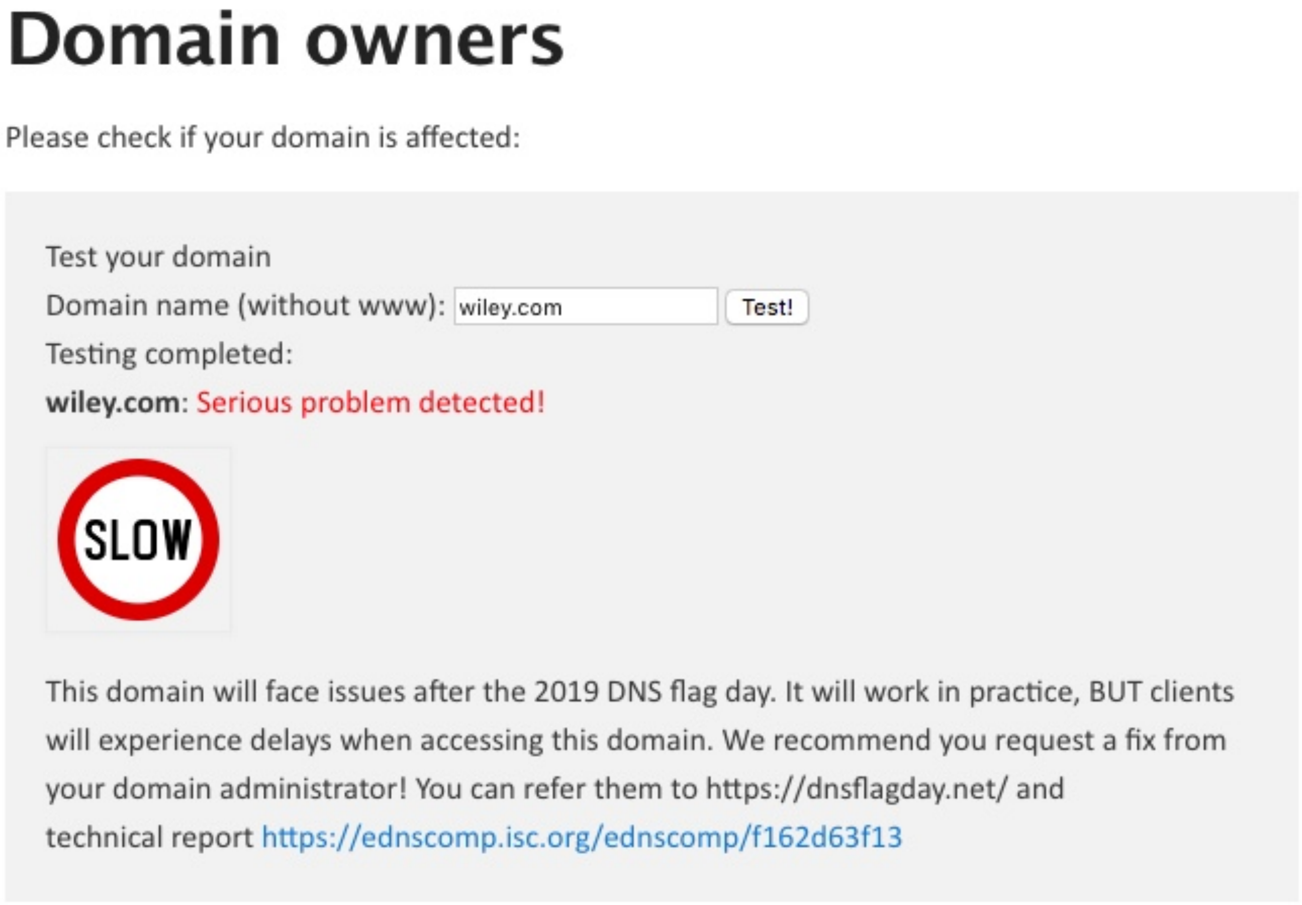
techradar.com: **Fatal error detected!**

This domain is going to STOP WORKING after the 2019 DNS flag day! Please retry the test to eliminate random network failures. If the problem persists you really need to request a fix from your domain administrator. You can refer them to https://dnsflagday.net/ and technical report https://ednscomp.isc.org/ednscomp/b6cfeb822f

(Hosted on non-compliant nameservers at future.net.uk)

Test your domains

https://dnsflagday.net/



Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): wiley.com Test!

Testing completed:

wiley.com: Serious problem detected!

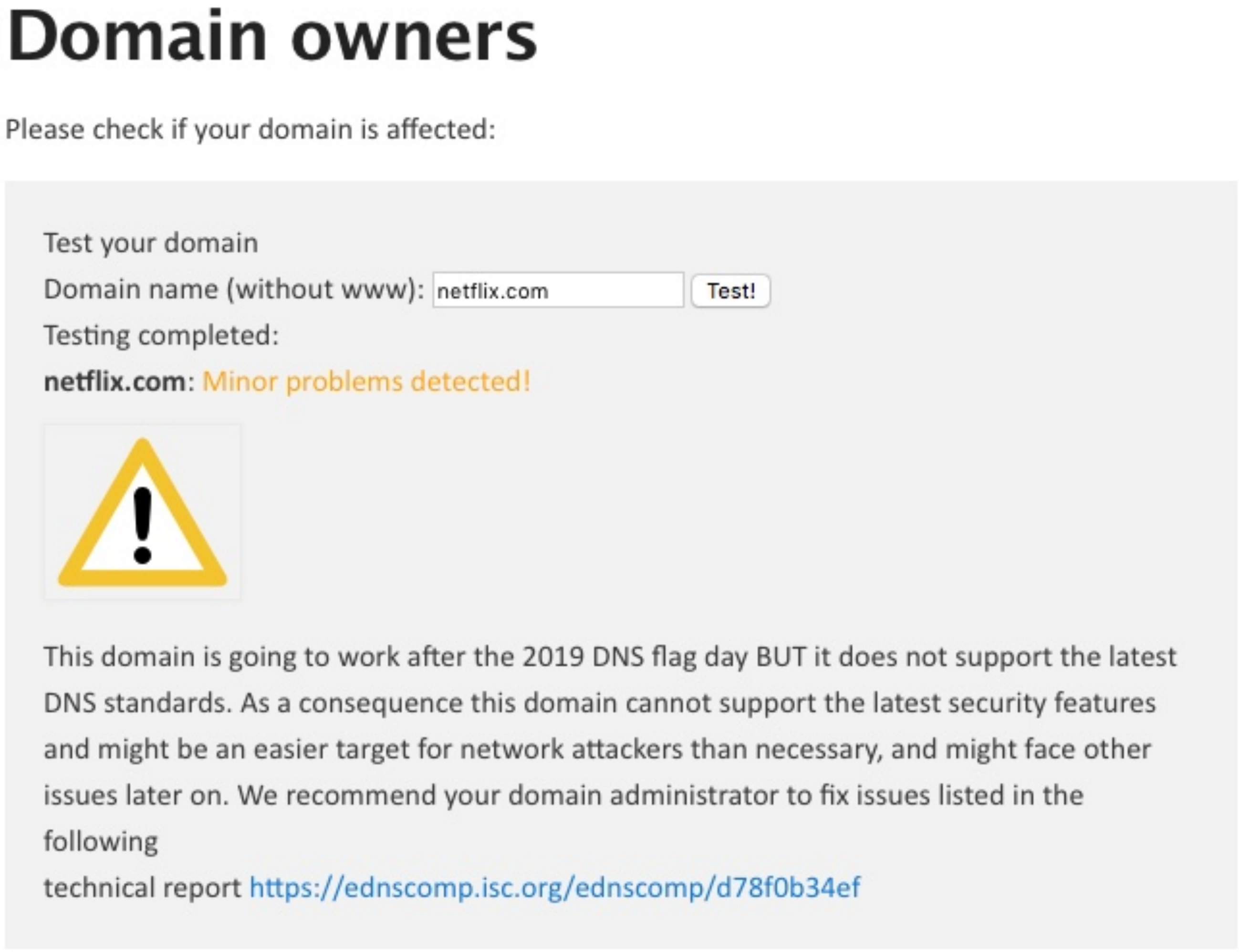
This domain will face issues after the 2019 DNS flag day. It will work in practice, BUT clients will experience delays when accessing this domain. We recommend you request a fix from your domain administrator! You can refer them to https://dnsflagday.net/ and technical report https://ednscomp.isc.org/ednscomp/f162d63f13

(Hosted on non-compliant nameservers at wiley.co.uk)

DNS FLAG DAY

Test your domains

https://dnsflagday.net/



Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): netflix.com

Testing completed:

netflix.com: Minor problems detected!

This domain is going to work after the 2019 DNS flag day BUT it does not support the latest DNS standards. As a consequence this domain cannot support the latest security features and might be an easier target for network attackers than necessary, and might face other issues later on. We recommend your domain administrator to fix issues listed in the following

technical report https://ednscomp.isc.org/ednscomp/d78f0b34ef

DNS FLAG DAY

And then.. ?

- Review https://ednscomp.isc.org/ednscomp/your-domain-report
- Perhaps you just need to upgrade your DNS server software (what are you running?)
- Check that any load-balancers or DNS proxies are compliant (and/or correctly configured)
- Do you have firewalls or routers that are trying to inspect DNS packets but which don’t understand modern DNS protocol?
- Does your infrastructure block DNS over TCP?

Help?

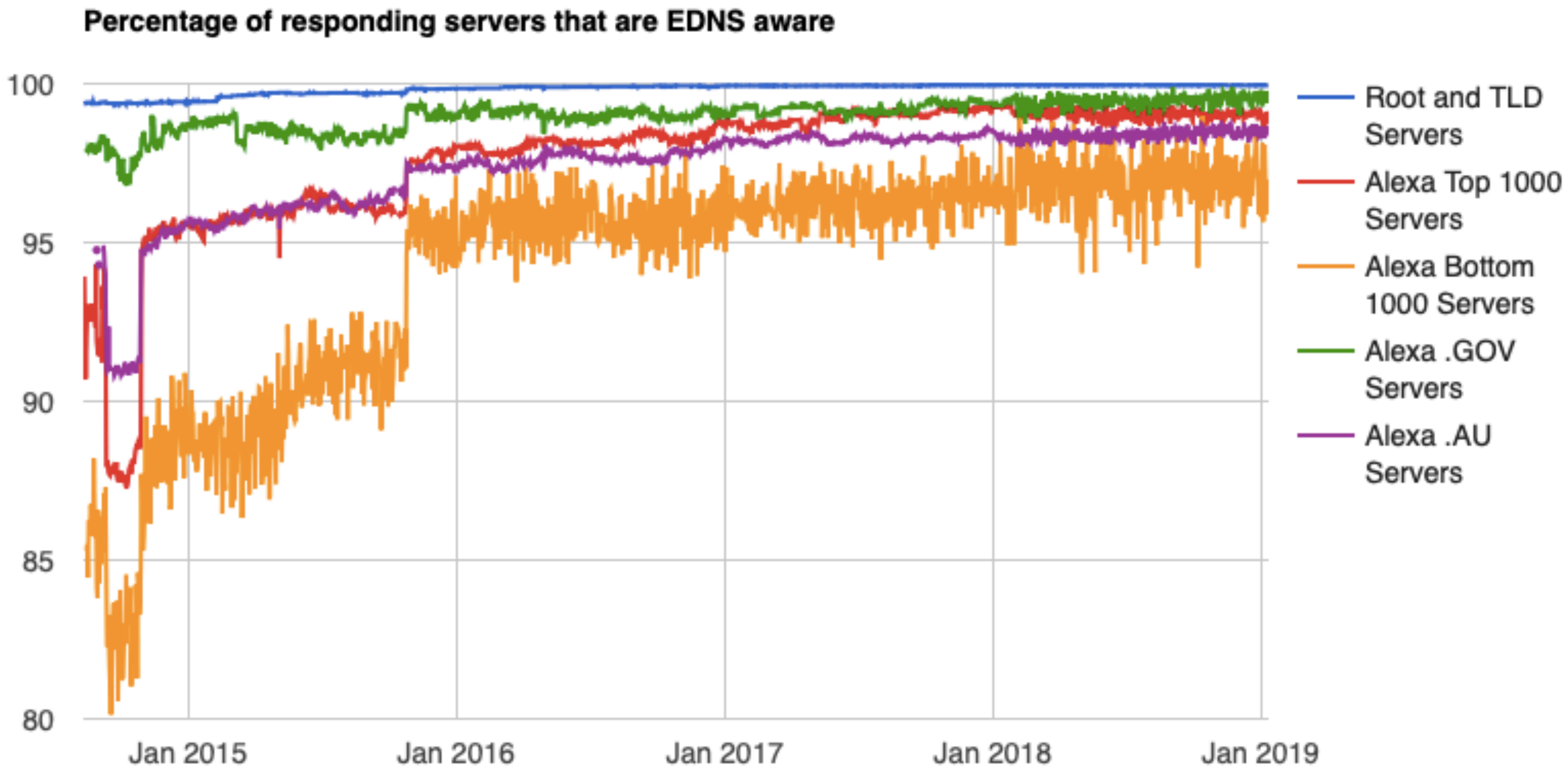
- Not everyone is a DNS expert
- Ask your software providers for support (or ask for advice on their user community mailing lists)
- Consider migrating to a hosted DNS solution (but check their DNS protocol compliance when choosing)
- Consider migrating to an appliance-based solution

What about the resolvers?

- As you upgrade (or your service provider updates), some domains that your users/clients want to reach are going to disappear or become ‘slow’
- Use the testing tool (as if they were your own zone) to see if reachability problems are due to DNS
- Don’t forget that webpages typically have large numbers of embedded URLs – web pages may be partially slow or incomplete (you might have to delve a little..)

Other people's domains…

- .. are theirs to fix
- .. often have more than just one problem – try them in the dnsviz tool too: http://dnsviz.net/
- It would be helpful and responsible to try to let them know that they have a problem (but email might not work)
- No longer accommodating broken DNS implementations is the point of having a DNS Flag Day – the workarounds are gone



Source: https://ednscomp.isc.org/compliance/summary.html

In conclusion:

- Check your own domains today
- Fix (or ask your domain hosting company to fix) any issues identified
- If you see ‘funny problems’ reaching other services or websites, check their domains for DNS compliance failures
- Remember this talk – you might not encounter problems right away

Any Questions?

Useful Sites and Tools

- https://dnsflagday.net/
- https://twitter.com/dnsflagday
- https://ednscomp.isc.org/
- http://dnsviz.net/
- https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing
- https://gitlab.labs.nic.cz/knot/edns-zone-scanner/

What else is being said?

https://en.blog.nic.cz/2018/03/14/together-for-better-stability-speed-and-further-extensibility-of-the-dns-ecosystem/

https://www.isc.org/blogs/end-to-bandaids/

What else is being said?

https://www.nlnetlabs.nl/news/2018/Jun/07/putting-an-end-to-workarounds-for-broken-software/

https://blog.powerdns.com/2018/03/22/removing-edns-workarounds/

https://blog.nzrs.net.nz/dns-flag-day/

Presentations:

DNS-OARC 28: Abstract; slides; video

LOADAYS 2018: Abstract; slides; video

RIPE 76: Slides; video

DNS-OARC 29: Abstract; slides; video