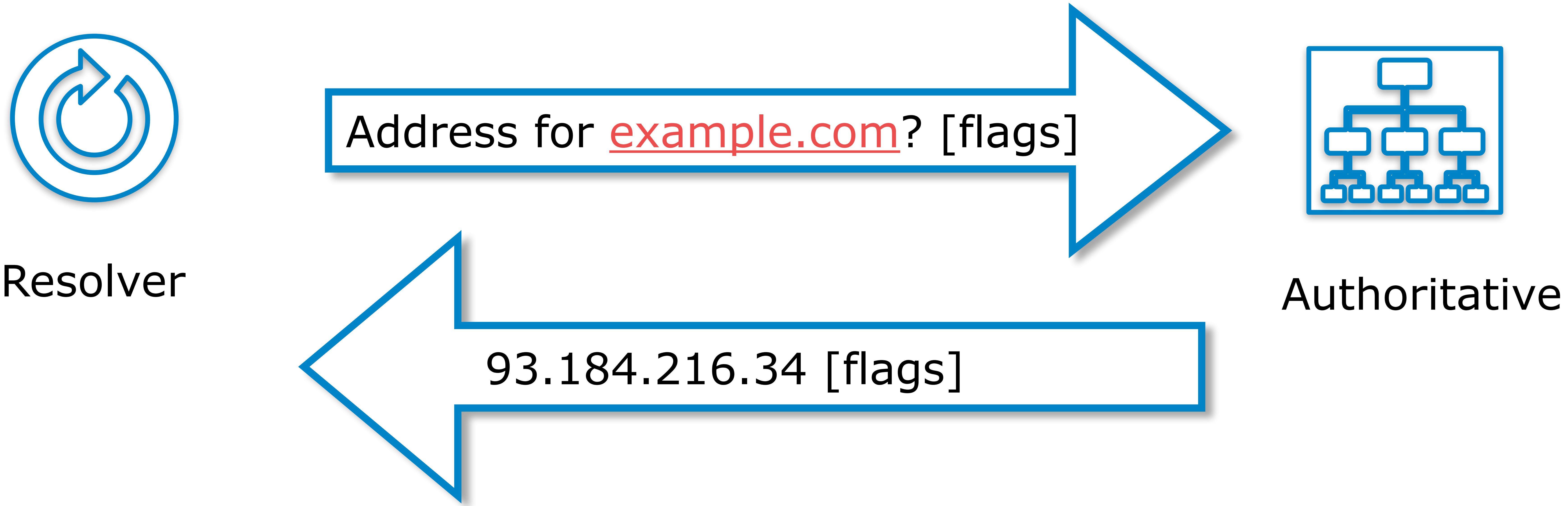
DNS Flag Day and beyond - how will it affect you?

NANOG75: Eddy Winstead, ISC

dnsflagday.net

Most transactions on the Internet start with a dialog like this:



Resolver

Address for example.com? [flags]

Authoritative

93.184.216.34 [flags]

DNS FLAG DAY

Response codes

Resolver

NOERROR	No Error
FORMERR	Format Error
SERVFAIL	Server Failure
NXDOMAIN	Non-existant Domain
NOTIMP	Not Implemented
REFUSED	Refused
....	
BADVERS	Bad OPT version
BADSIG	TSIG signature failure
BADKEY	Key not recognized
...	

Authoritative

DNS FLAG DAY

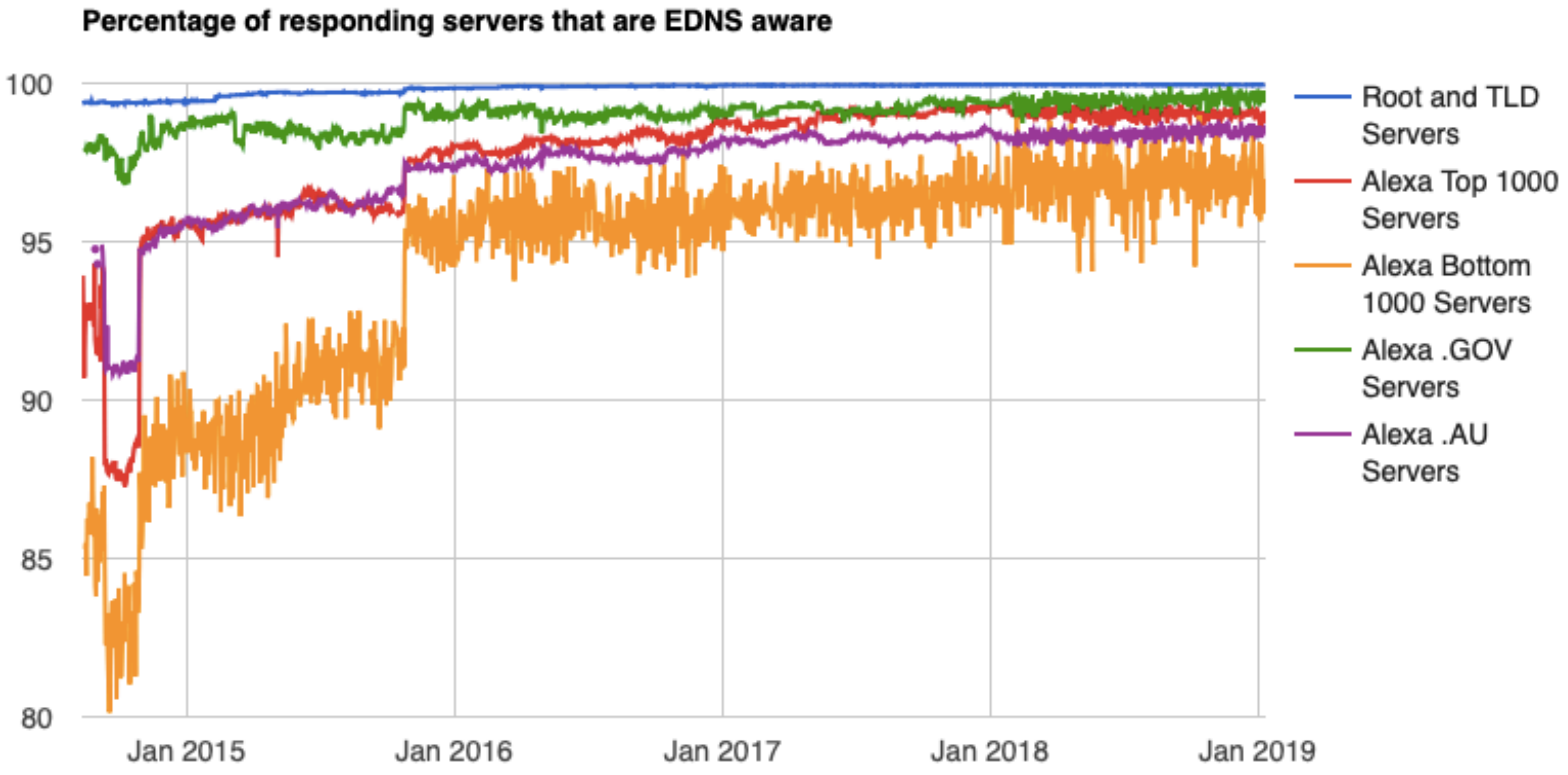
Extension Mechanisms for DNS

- Designed so that you can deploy any of the extension mechanisms in the client or server independent of requiring it to be supported at the other end. To do this EDNS(0) specified how to handle versions, flags and options that are unknown.

- * EDNS version -> response code BADVERS by server / ignored by client.
- * EDNS flag -> ignored by other end.
- * EDNS option -> ignored by other end.

EDNS is used for…

- UDP DNS messages over 512 bytes
- DNSSEC
- DNS Cookies
- Client-subnet identifier
- TBD



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

Specific issues observed

- Firewalls blocked EDNS(1)
- Firewalls blocked the EDNS NSID option.
- Firewalls blocked reserved EDNS flags.
- Firewalls block fragmented responses.
- Load balancers drop fragmented responses.
- Load balancers mishandle ICMP PTB messages.
- Older Microsoft DNS software didn’t implement EDNS.

Interpreting Timeouts

- Network congestion
- DNS server failure
- Firewall or Load Balancer blocking EDNS traffic
- DNS server just doesn’t support EDNS

‘Workarounds’ for EDNS incompatibility problems

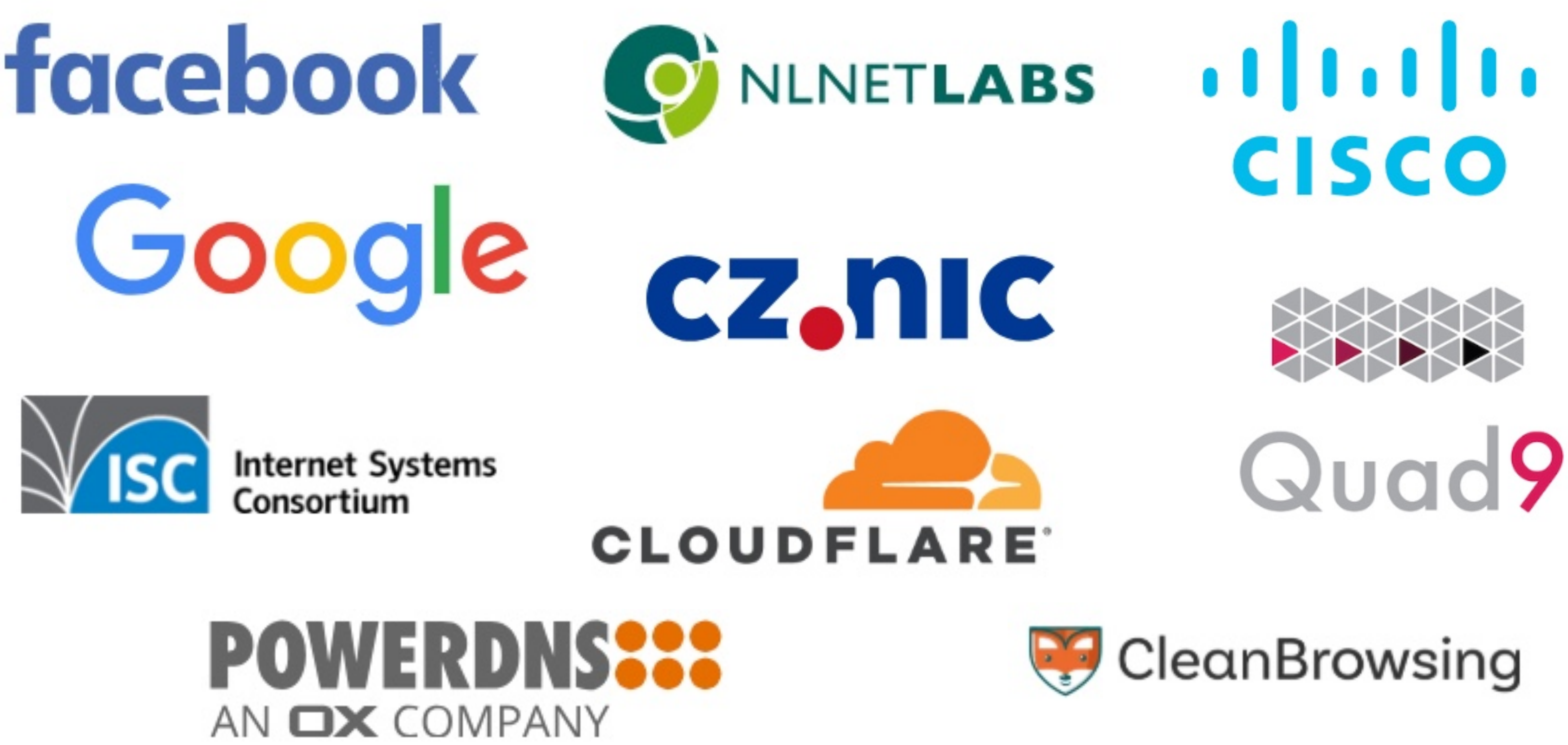
- retry without EDNS
- retry with TCP
- ….disabling EDNS is the main workaround

Why remove the workarounds?

- the workarounds **slow down** the DNS
- they make it harder to implement new features
- layers of exception handling complicate the DNS code and make it more fragile

- most of the DNS has been upgraded, and the remaining breakage seemed to be mostly parked domains

Removing workarounds on or after 1 Feb 2019



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

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

DNS FLAG DAY

Open Source

	Flag Day version	Notes
BIND 9	9.13.6 9.14.0	
PowerDNS	4.2	4.1 auth is fully compliant. 4.0 is compliant if you disable caching
Knot	Knot had no workarounds	Run Knot 3.3.0 for best compliance
Unbound	1.84, 1.90	

Product updates

BlueCat: https://www.bluecatnetworks.com/blog/dns-flag-day-is-coming-and-bluecat-is-ready/

Citrix: https://support.citrix.com/article/CTX241493

DNSimple: https://simpledns.com/news/78/simple-dns-plus-v-8-0-build-108-released-dns-flag-day-update

EfficientIP: http://www.efficientip.com/dns-flag-day-notes/

F5: https://support.f5.com/csp/article/K07808381?sf206085287=1 and https://worldtechit.com/dns-flag-day-for-f5-dns/

InfoBlox: https://community.infoblox.com/t5/Community-Blog/DNS-Flag-Day/ba-p/15843?es_p=8449211

Juniper: https://kb.juniper.net/InfoCenter/index?page=content&id=TSB17513

Microsoft Azure: https://azure.microsoft.com/en-us/updates/azure-dns-flag-day/

Microsoft Windows: https://support.microsoft.com/en-sg/help/4489468/windows-server-domain-name-system-dns-flag-day-compliance

Palo Alto Networks firewall: https://live.paloaltonetworks.com/t5/Community-Blog/DNS-Flag-Day-Are-You-Ready/ba-p/248284

Pulse: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43996

SimpleDNS: https://simpledns.com/news/78/simple-dns-plus-v-8-0-build-108-released-dns-flag-day-update

Service Operators

Dyn: https://dyn.com/blog/what-you-need-to-know-about-dns-flag-day/

Exabytes: https://support.exabytes.com/en/support/discussions/topics/14000013075

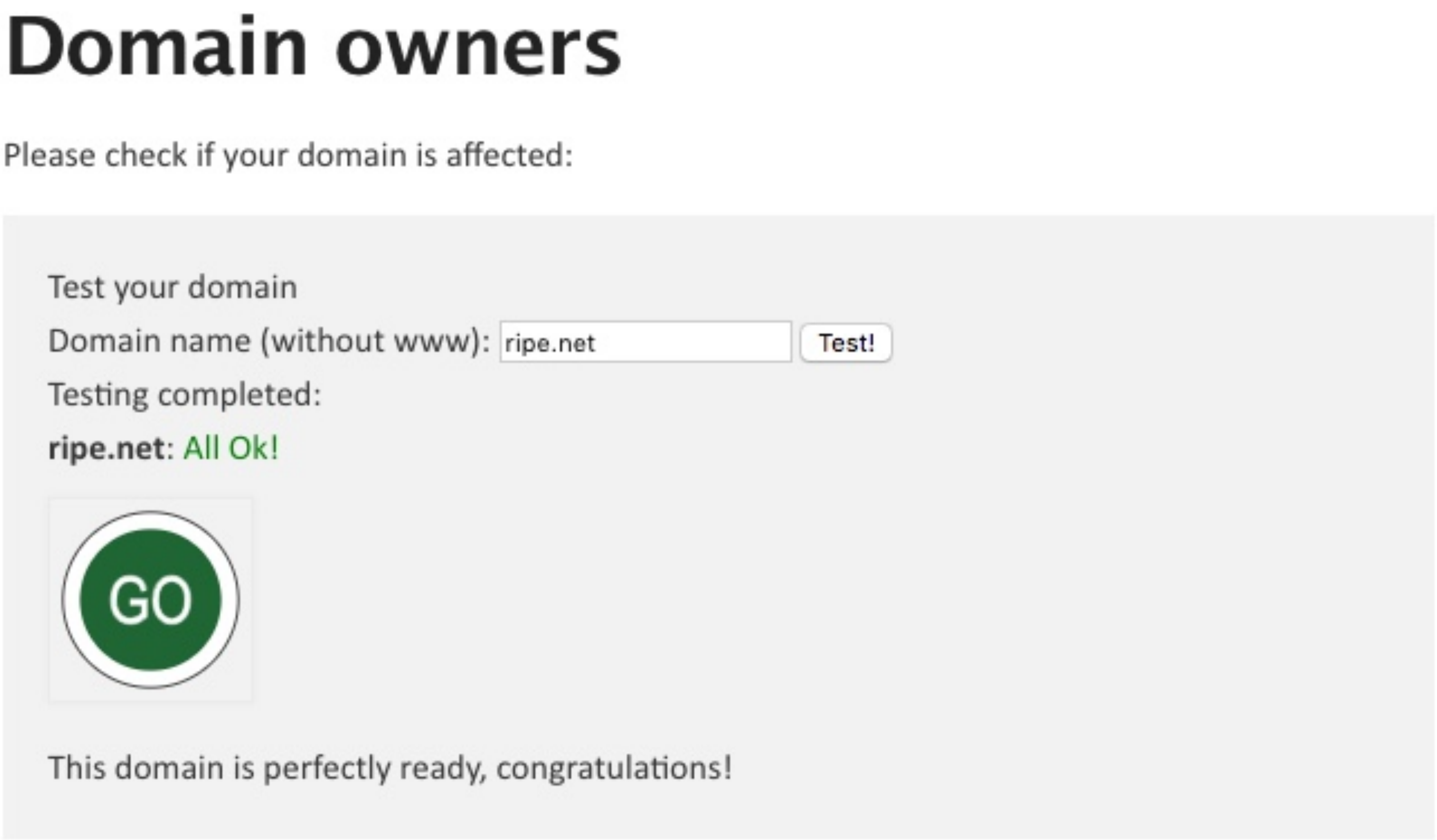
Google: https://groups.google.com/forum/#!msg/public-dns-announce/-qaRKDV9InA/CsX-2fJpBAAJ

Quad9: https://quad9.net/dns-flag-day-2019/

Valimail: https://www.valimail.com/blog/what-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): ripe.net

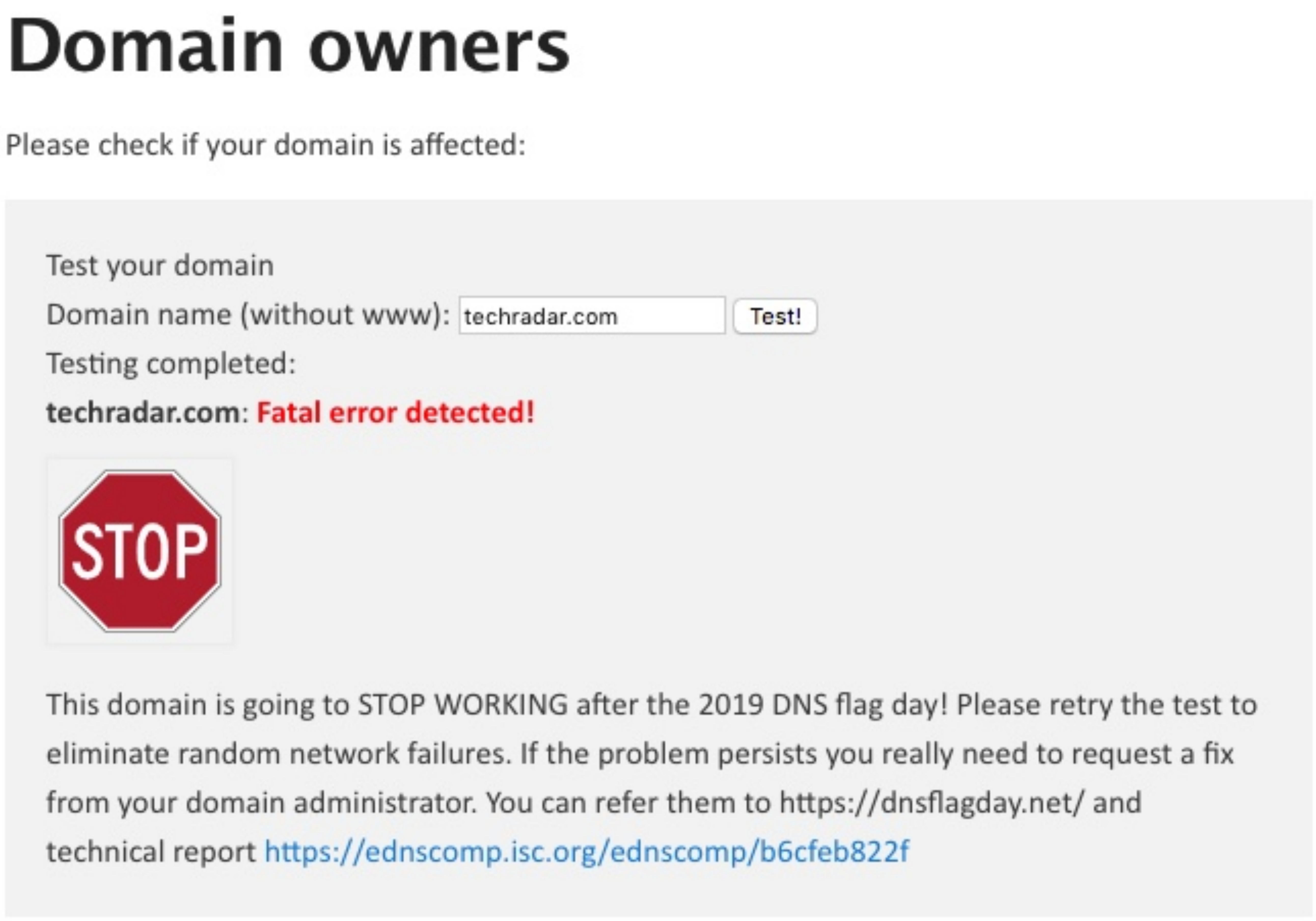
Testing completed:

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:

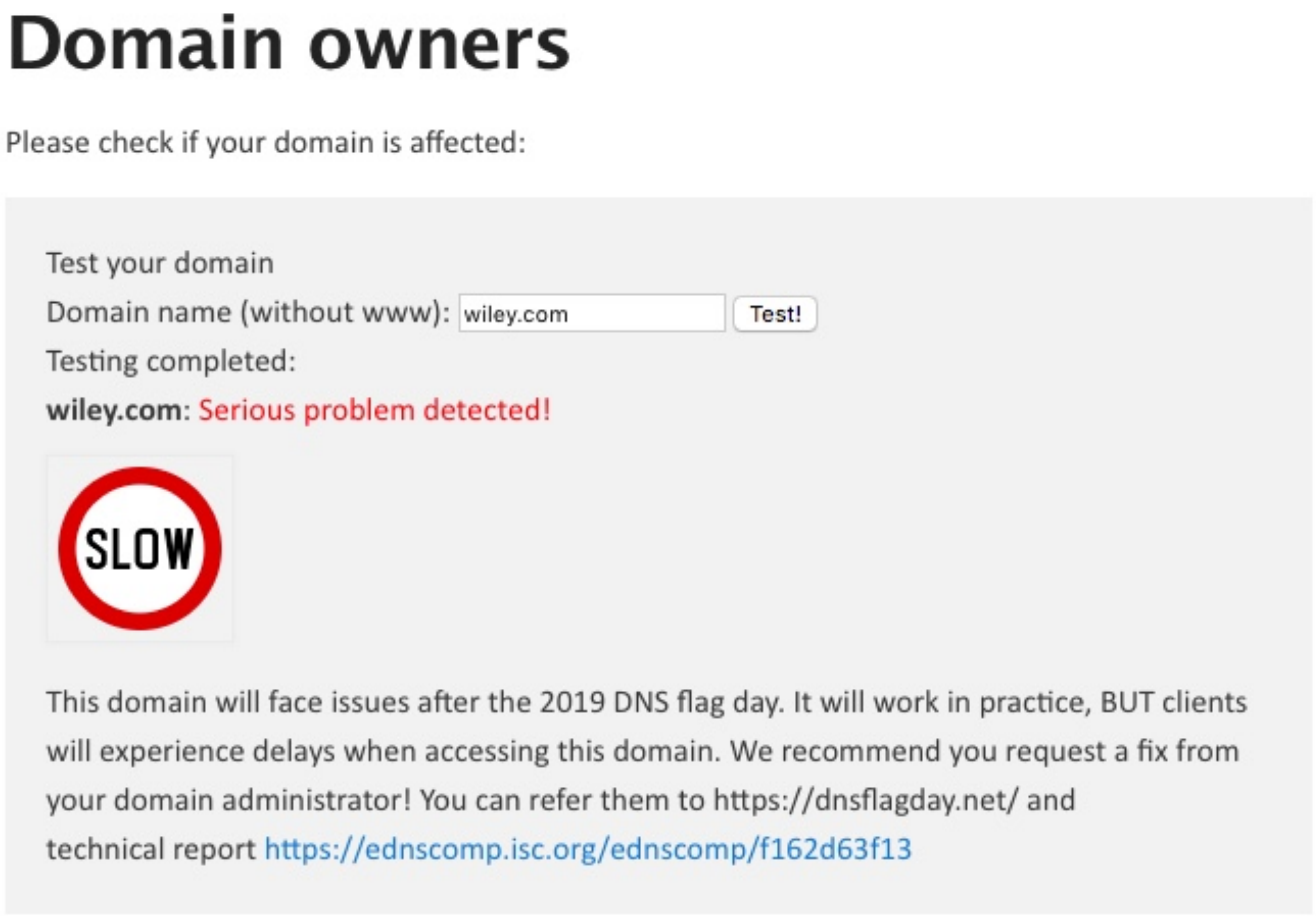
techradar.com: **Fatal error detected!**

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:

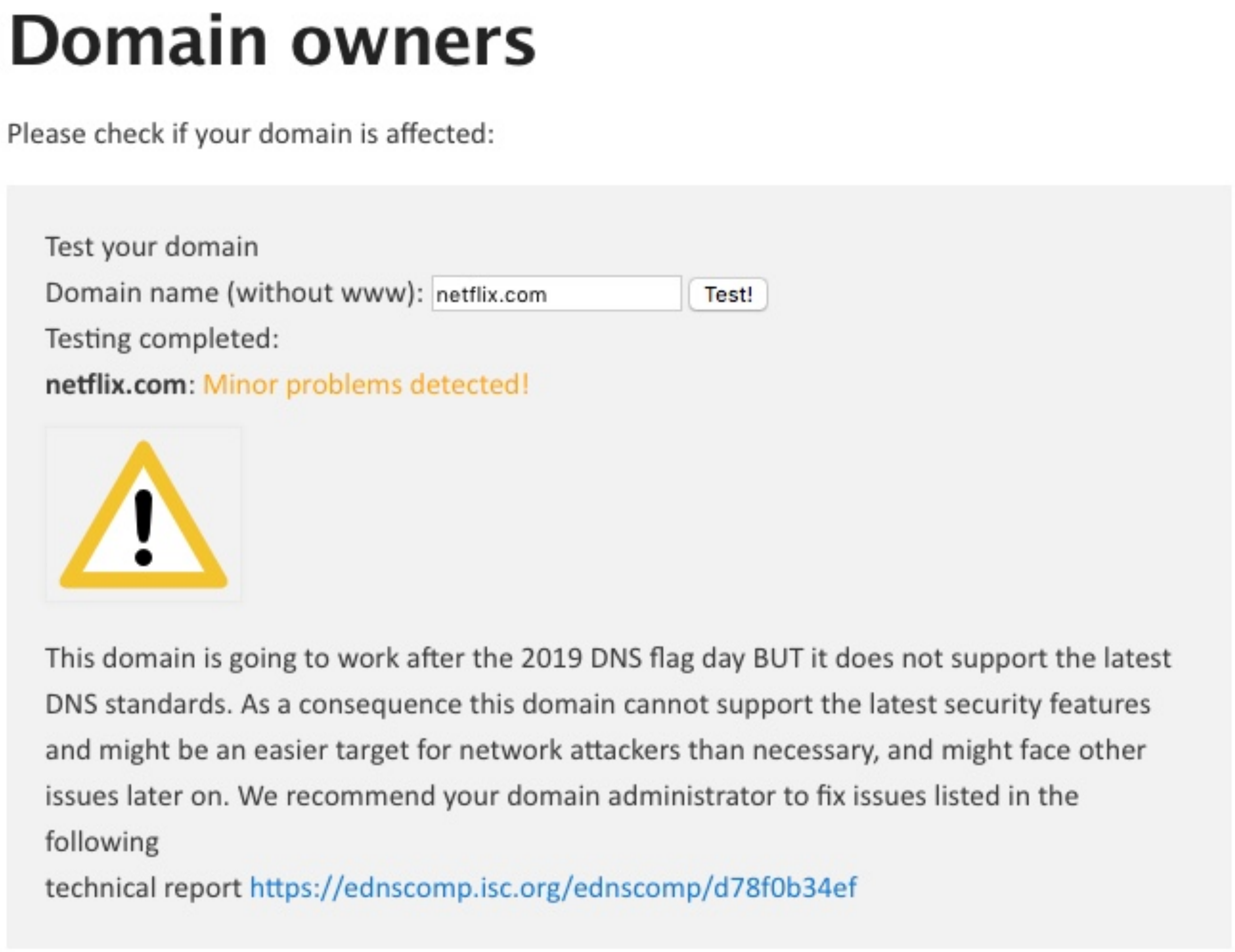
wiley.com: Serious problem detected!

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)

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

Testing Summary

- Review https://ednscomp.isc.org/ednscomp/your-domain-report
- If you get an error other than timeout, upgrade your DNS software to the latest your vendor has.
- If you are getting timeouts check the firewall settings.

Long-term Benefits

- resolvers will stop disabling EDNS unnecessarily
- DNS will be more resilient
- resolvers will become more efficient, less persistent

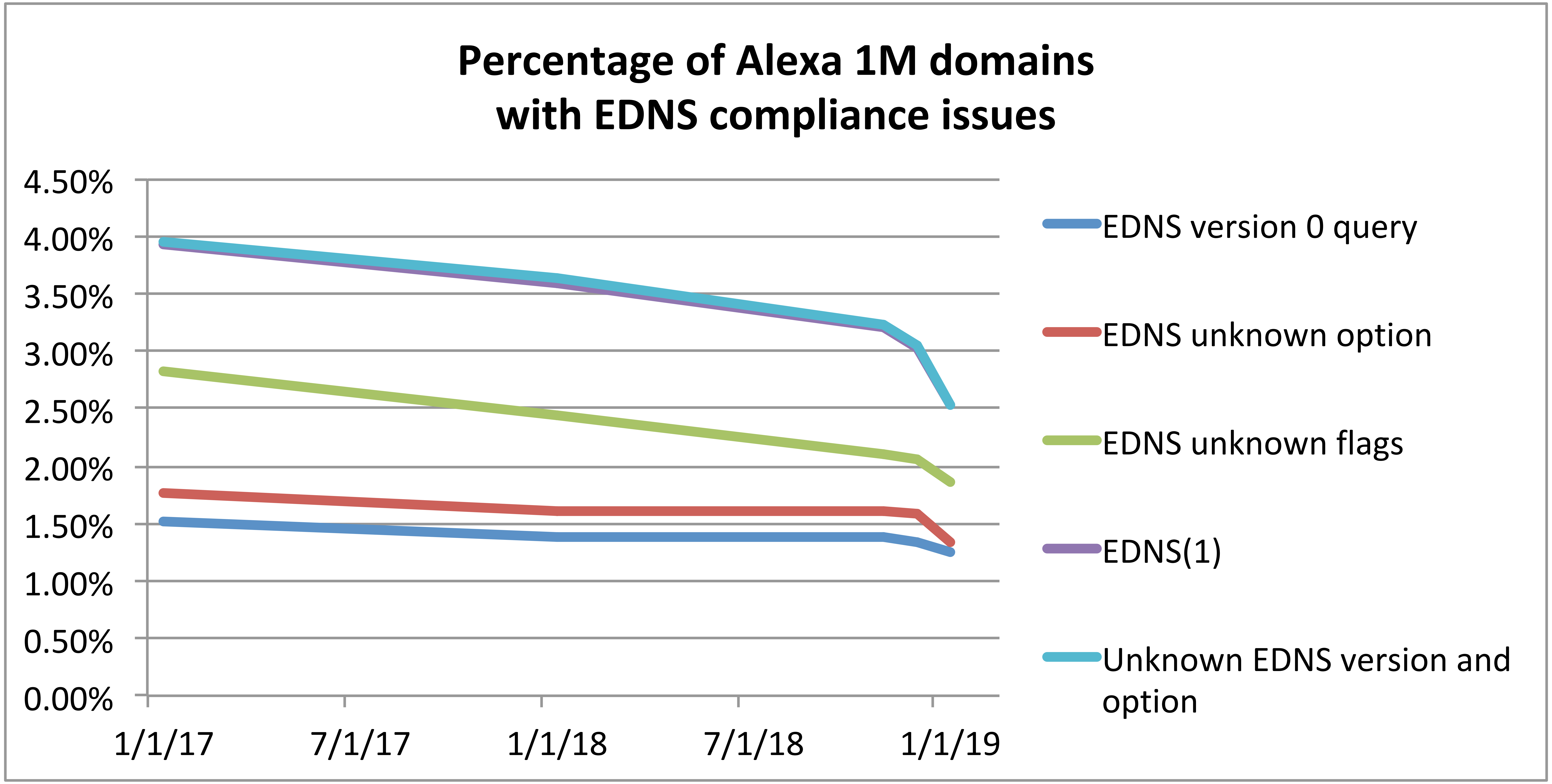
- newer features like DNSSEC, DNS cookies, EDNS client subnet, etc., will work better

(DNS) Fun with Flags (Day)

Lessons learned

- not on a Friday
- not before Super Bowl
- beware echo-chamber

Flag Day accelerated progress



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?

DNS FLAG DAY