DNS Flag day: kiwi flavour

Sebastián Castro

OARC 30

Bangkok, Thailand

What’s the problem?

- Authoritative DNS servers block responses, don’t answer, or answer with the wrong packet.
  - In general, bad implementations of DNS not following the standards
- Poorly implemented firewalls on the way, poor firewall rules blocking valid traffic or unaware of the standards
- Resolvers have to send a query, wait for a timeout and retry using a different method: TCP or discard EDNS
  - Forces delays and thwarts innovation and deployment of new features

Measuring DNS flag day effects

- “DNS Compliance Testing” tool written by ISC https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing
  - Only check for EDNS compliance at this stage
  - Same test available at https://dnsflagday.net
- “EDNS Compliance scanner for DNS zones” from CZ.NIC:
  - https://gitlab.labs.nic.cz/knot/edns-zone-scanner/tree/master
  - Uniquely test all addresses of a nameserver
  - Preprocess a TLD zone and generate the minimal set of nameserver tests
  - Test multiple times to discard transient errors

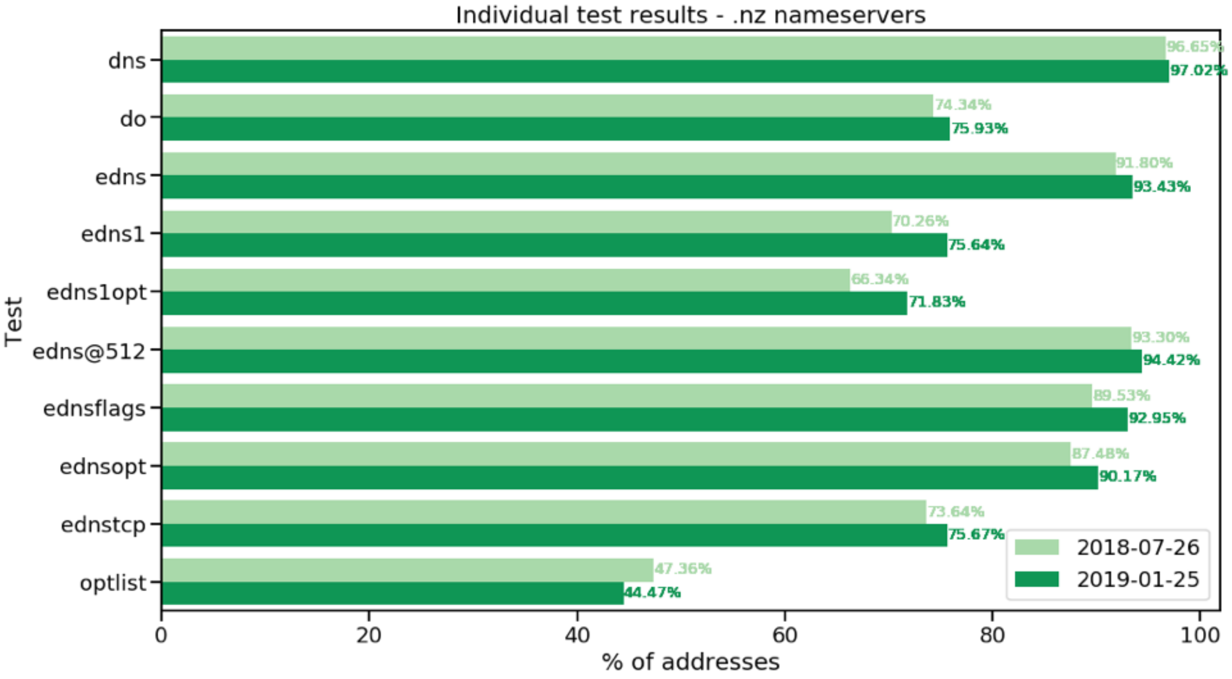
InternetNZ’s involvement

- Early measurement of impact in coordination with CZ and CL
  - First collection in July 2018
- Presentations in different conferences
- Blog post
  - Kindly promoted by APNIC
- Bi-weekly data collection on all .nz domains starting in October
- Communication campaign
  - Registrants, Registrars, DNS Operators, Popular domains

General Statistics

Date	# nameservers	# unique IPv4 addresses	# Unique IPv6 addresses	# Unique addresses
25 Jul 2018	21133	21219	4597	25816
25 Jan 2019	21360	21451	5214	26665

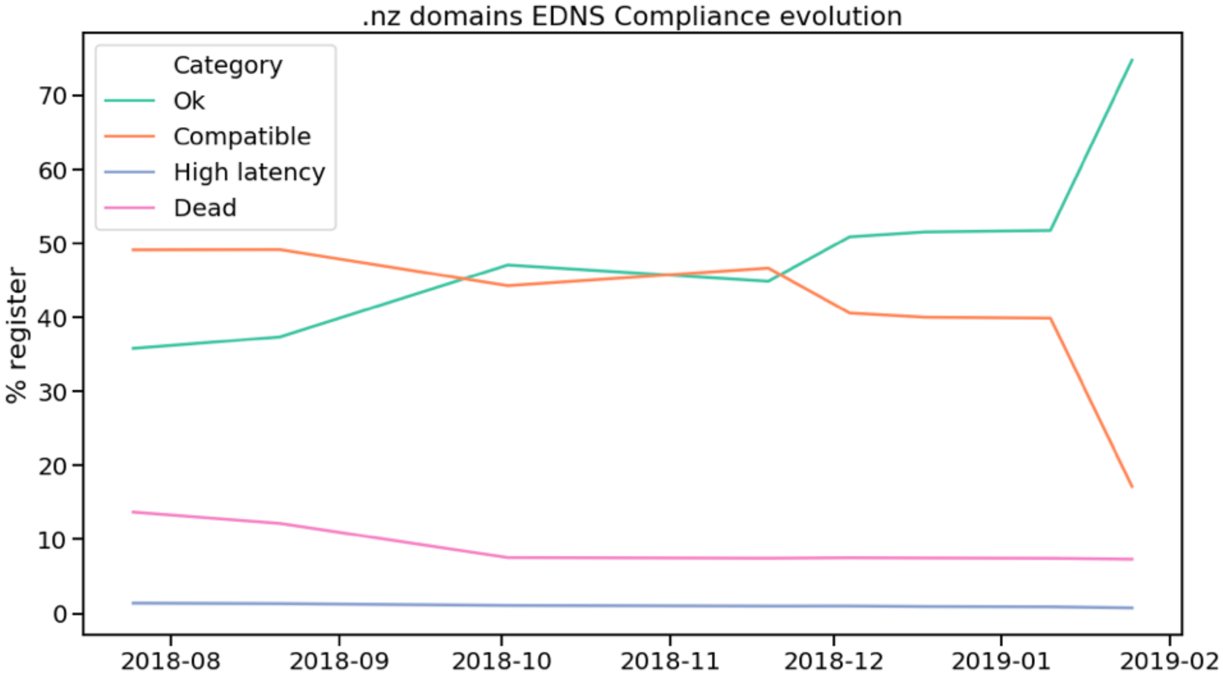
Compliance state by nameserver addresses



Domain Status

- CZ.NIC created a tool that simplifies the understanding of the test.
- Four states:
  - OK: All EDNS tests are ok
  - Compatible: None of the EDNS tests produce a timeout
  - High Latency: Some nameserver addresses generate timeouts
  - Dead: All nameserver addresses generate timeouts
- Two set of rules
  - Permissive: Resolvers as they behave today
  - Strict: Resolvers with workarounds stripped

.nz improvements over time

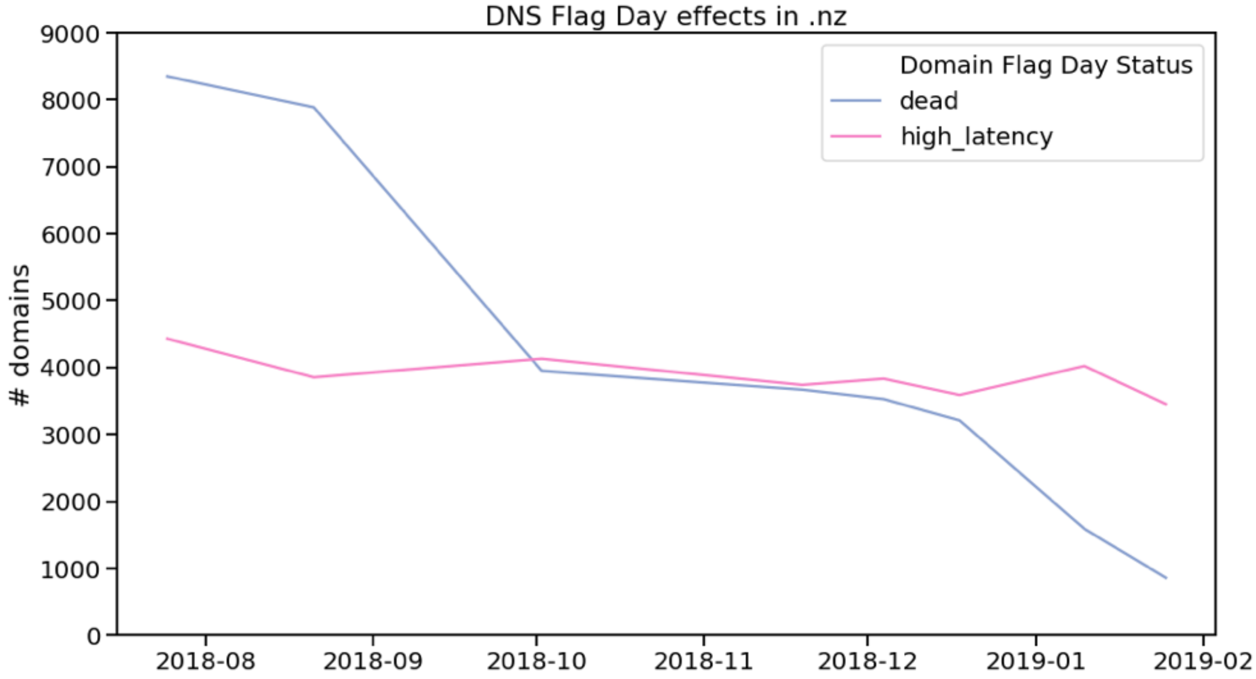


InternetNZ

Caveat

- Not all domains marked as high latency or dead are because EDNS brokenness
- There are a lot with lame nameservers, broken IP addresses, nameservers that can’t resolve.
- The reported domains differ presented a completely different picture!

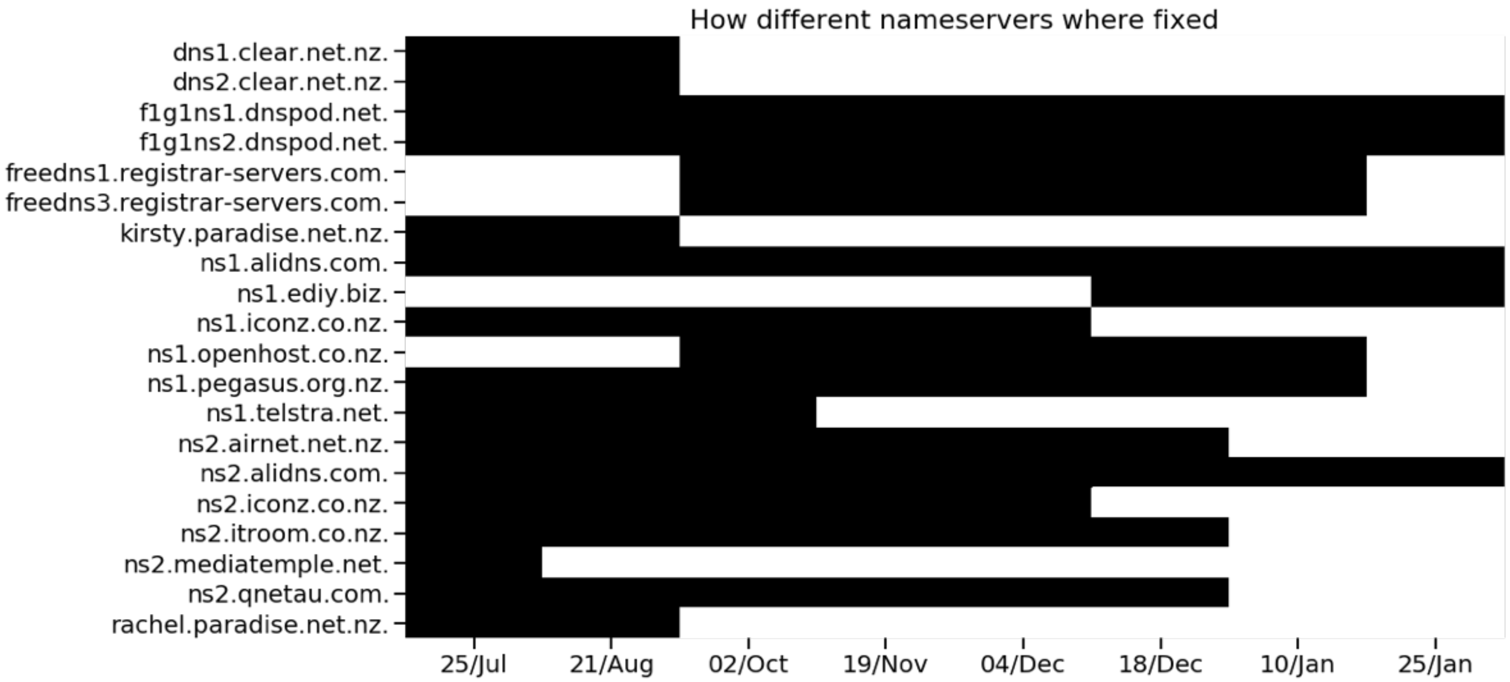
Effectively affected .nz domains



How we got there?

- In the initial list of domains there were
  - A bunch of .govt.nz
  - Banks
  - Consultancy services
  - Newspapers
- We reached to
  - Registrars
  - DNS Operators
  - Registrants
  - NZNOG via Slack

How we got there?



Some stories from the process

- Windows DNS Server support
- Large DNS resolvers rollover plans
- Large authoritative DNS reaching out
- Some operators confused
- Some operators using old software
- Operators using modern software behind DPI firewalls
- “Why I didn’t find out about this sooner?”

Closing remarks

- It was hard to reach the right people in certain cases
- A big shout out to the team at InternetNZ and DNCL
  - Comms team, Channel Manager, Brent and his team

BUSINESS

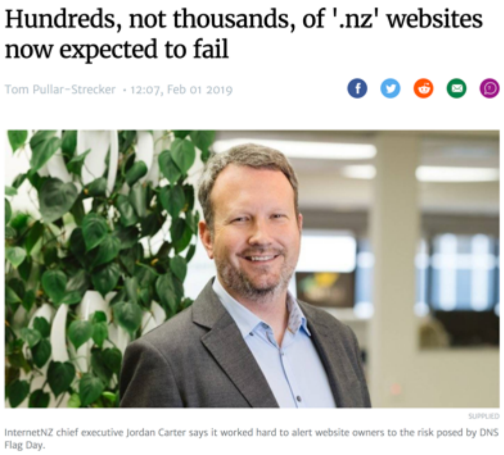
'Flag day' set to throw hundreds of NZ websites offline for hours or days

1 Feb, 2019 11:26am

2 minutes to read

InternetNZ head Jordan Carter says Flag Day could have been a lot worse. As of July, more than 8000 sites were in the gun, including banks and major government departments. Photo / Supplied.

By: Chris Keall
Business writer, NZ Herald
chris.keall@nzherald.co.nz
@ChrisKeall

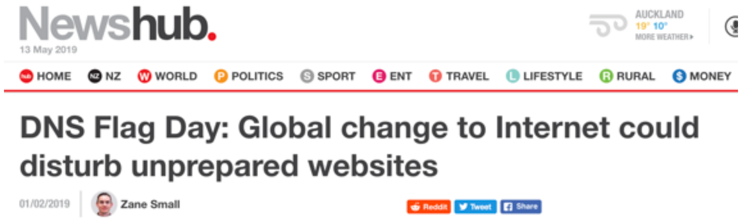


Hundreds, not thousands, of '.nz' websites now expected to fail

Tom Pullar-Strecker • 12:07, Feb 01 2019

SUPPLIED

InternetNZ chief executive Jordan Carter says it worked hard to alert website owners to the risk posed by DNS Flag Day.



DNS Flag Day: Global change to Internet could disturb unprepared websites

01/02/2019 | Zane Small

¡GRACIAS!

sebastian@internetnz.net.nz

InternetNZ