Estimating impact of 2019 (E)DNS flag day

https://dnsflagday.net

Petr Špaček • petr.spacek@nic.cz • 2018-10-14

Prepare for impact

What happens if …

- DNS resolvers do not disable EDNS version 0 after query timeout?
  - ➔ DNS servers which do not respond *at all* to EDNS queries will be treated as *dead*
- *What impact should we expect on day-to-day operation?*

What does it *really* mean?

Checking: 'facebook.com' as at 2018-10-13T15:06:26Z

facebook.com. @69.171.239.12 (a.ns.facebook.com.): dns=ok edns=ok **edns1=noerror,badversion** edns@512=ok ednsopt=ok **edns1opt=noerror,badversion** do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet
facebook.com. @2a03:2880:fffe:c:face:b00c:0:35 (a.ns.facebook.com.): dns=ok edns=ok **edns1=noerror,badversion** edns@512=ok ednsopt=ok **edns1opt=noerror,badversion** do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet

facebook.com. @69.171.255.12 (b.ns.facebook.com.): dns=ok edns=ok **edns1=noerror,badversion** edns@512=ok ednsopt=ok **edns1opt=noerror,badversion** do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet
facebook.com. @2a03:2880:ffff:c:face:b00c:0:35 (b.ns.facebook.com.): dns=ok edns=ok **edns1=noerror,badversion** edns@512=ok ednsopt=ok **edns1opt=noerror,badversion** do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet

Impact on *domains*

- Consistent timeouts after EDNS0 query
  - → NS IP address will "die"

- One domain
  - multiple NS names
    - multiple IP addresses
      - are these authoritative?

Possible domain results

- **ok**
  all IPs work + tests passed, thank you!
- **compatible** (with 2019 flag day)
  all IPs work + EDNS 0 query always gets ***a*** reply
- **high_latency** (two definitions!)
  retries required: NS not auth, EDNS timeout, etc.
- **dead** (two definitions!)
  permissive 2018 vs. strict 2019

Evaluation methodology (part 1)

- https://gitlab.labs.nic.cz/knot/edns-zone-scanner/blob/master/README.rst

1) Create mapping domain
   → *n* NS names (zone)
   → *n* IP addresses (glue + resolver)
   all NS IPs unresolvable → dead *domain*
2) Not authoritative NS IP → dead *IP*
3) Test authoritative IPs using genreport
4) Repeat genreport 5 times, majority wins

Evaluation methodology (part 2)

5) Combine NS IP results from genreport
   - all IP ok → domain ok (incl. EDNS 1+)
   - no timeouts → compatible (excl. EDNS 1+)
6) Evaluate IPs in "permissive" mode (<= 2018)
   - plain DNS works but others timeout → high_latency
7) Evaluate IPs in "strict" mode (>= 2019)
   - timeout in EDNS 0 tests → dead
8) Combine IP mode-dependent results

Limitations

- Anycast → results might depend on location
- Lower levels of DNS tree are not visible
- EDNS support on a given IP address does not depend on domain name used for test
  - as long as the IP address is authoritative
  - (optimization)
- **Not all domains are equal**

Results: Root zone

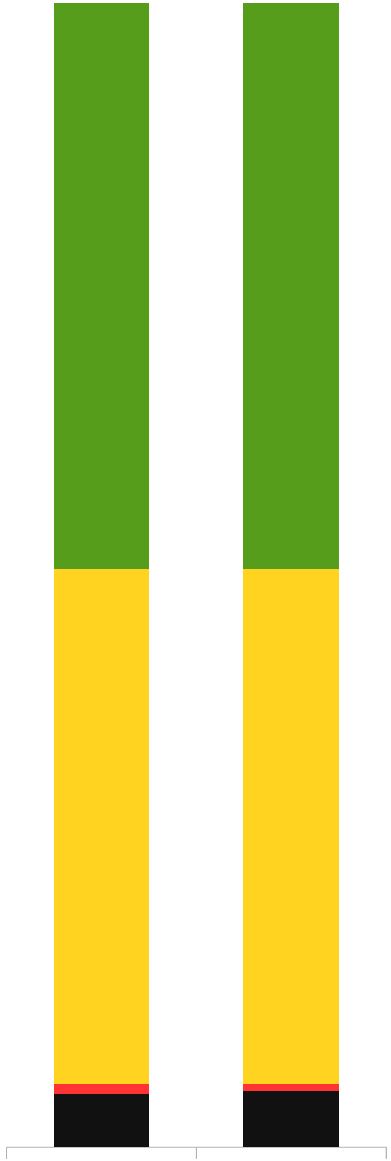
Mode	Permissive (<= 2018)	Strict (2019+)
Ok	1494	
Compatible	17	
High latency	25	24
Dead	0	1
Breakage		+1 (kp.)

Results: CZ TLD

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	73.22 %	
Compatible	9.71 %	
High latency	5.40 %	5.24 %
Dead	11.67 %	11.83 %
Breakage		+0.16 %

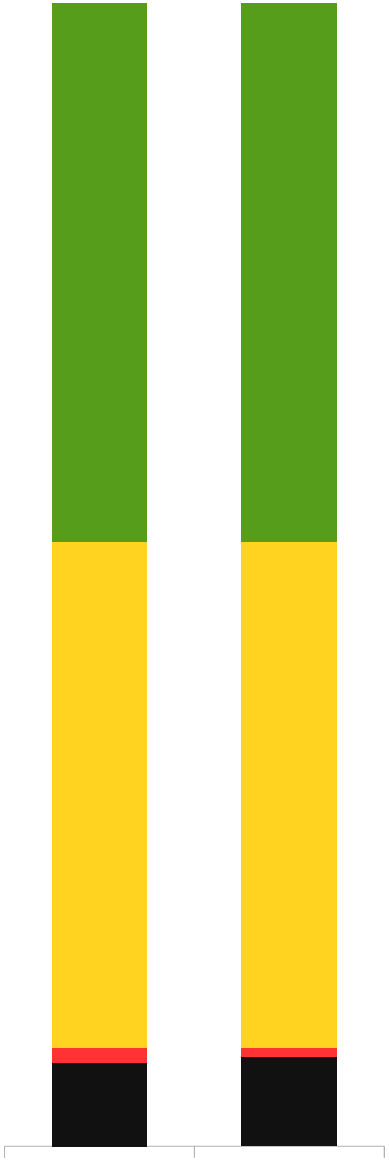
Results: SE TLD

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	49.43 %	
Compatible	45.03 %	
High latency	0.86 %	0.60 %
Dead	4.68 %	4.95 %
Breakage		+0.27 %



Results: NZ TLD

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	47.08 %	
Compatible	44.29 %	
High latency	1.35 %	0.80 %
Dead	7.28 %	7.83 %
Breakage		+0.55 %

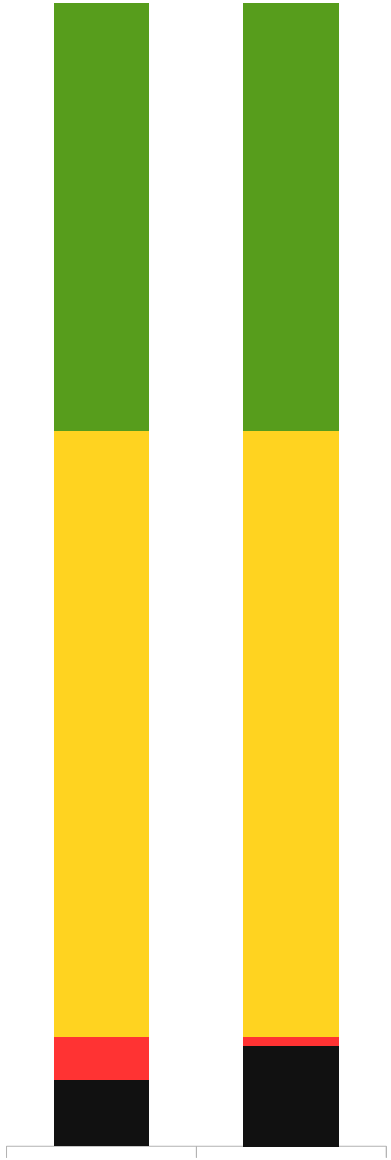


Results: CL TLD

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	69.94 %	
Compatible	13.92 %	
High latency	3.48 %	2.74 %
Dead	12.66 %	13.59 %
Breakage		+0.93 %

Results: NU TLD

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	37.41 %	
Compatible	53.06 %	
High latency	3.69 %	0.71 %
Dead	5.84 %	8.84 %
Breakage		+3.00 %

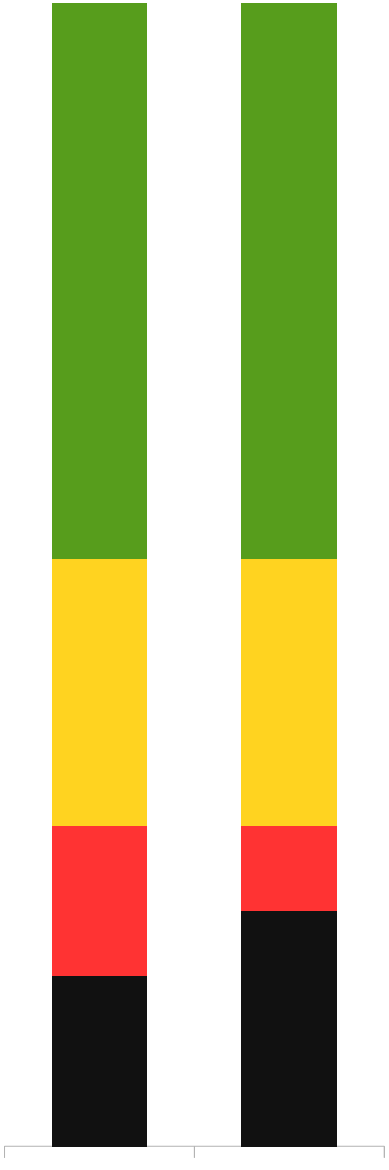


Results: NET TLD

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	57.03 %	
Compatible	23.11 %	
High latency	6.00 %	2.07 %
Dead	13.86 %	17.79 %
Breakage		+3.94 %

Results: grand total (23 M domains)

Mode	Permissive (<= 2018)	Strict (2019+)
Ok	48.61 %	
Compatible	23.37 %	
High latency	13.15 %	7.48 %
Dead	14.87 %	20.55 %
Breakage		+5.68 %



Top ten: total # delegations

TLD	breakage	size
net	3.94 %	13 865 540
loan	21.25 %	2 225 994
xyz	12.14 %	1 862 673
se	0.27 %	1 657 718
cz	0.16 %	1 296 393
nz	0.55 %	711 101
cl	0.93 %	431 187
work	3.15 %	423 126
nu	3.00 %	387 911
ooo	1.30 %	295 462

Top ten: % breakage per TLD

TLD	breakage	size
mma	99.82 %	1 668
redstone	66.67 %	9
dhl	60.00 %	10
loan	21.25 %	2 225 994
kim	17.88 %	18 595
xyz	12.14 %	1 862 673
pink	11.05 %	6 751
lotto	9.09 %	66
xn--6frz82g	7.05 %	2 949
yokohama	6.10 %	5 359

Top ten: EDNS-broken providers

provider domain	breakage	# broken
hichina.com.	35.78 %	469 611
dnspod.com.	25.66 %	336 797
myhostadmin.net.	5.04 %	66 208
xincache.com.	4.82 %	63 246
dnspod.net.	3.27 %	42 881
dnsdun.net.	2.85 %	37 435
gmoserver.jp.	2.71 %	35 595
registrar-servers.com.	1.64 %	21 533
alidns.com.	1.63 %	21 369
metaregistrar.nl.	1.20 %	15 762

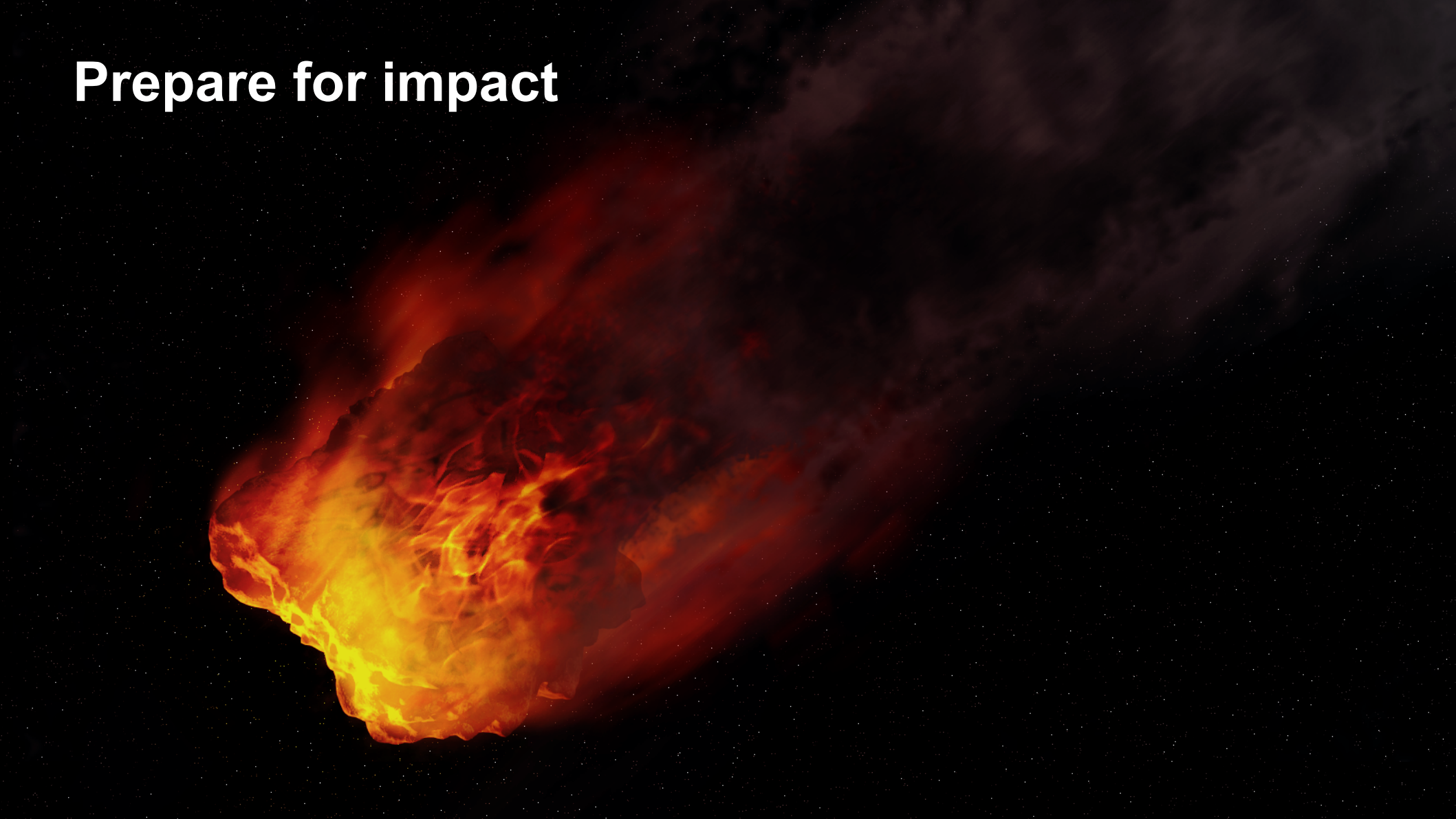
$\sum$

66 %

$\sum$

85 %

Prepare for impact



'cos he will not save you!

Contacts needed! Top ten EDNS-broken providers

provider domain	breakage	# broken
hichina.com.	35.78 %	469 611
dnspod.com.	25.66 %	336 797
myhostadmin.net.	5.04 %	66 208
xincache.com.	4.82 %	63 246
dnspod.net.	3.27 %	42 881
dnsdun.net.	2.85 %	37 435
gmoserver.jp.	2.71 %	35 595
registrar-servers.com.	1.64 %	21 533
alidns.com.	1.63 %	21 369
metaregistrar.nl.	1.20 %	15 762

∑

66 %

∑

85 %