



Which TLDs break first?

ccNSO Tech Day, ICANN. October 2026

redsift.com

What we scanned

242

TLDs, every namespace with
100+ Tranco-ranked names

24,200

Seed domains: the top 100 in
each, plus discovered
subdomains

6

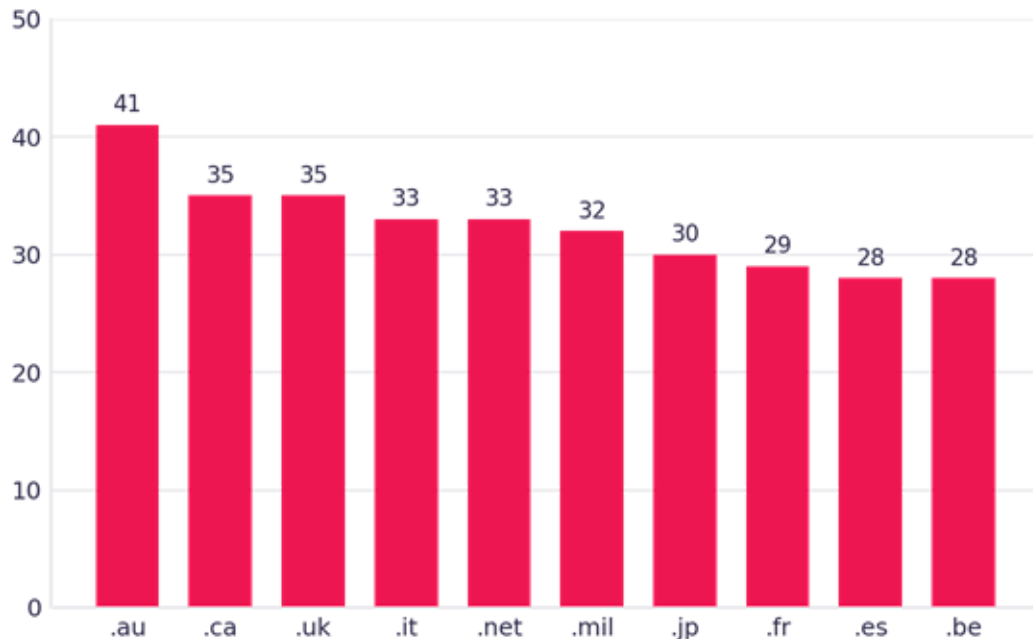
Passive checks per host: NS
health, delegation, dangling,
DNSSEC, email policy

Finding - 1 in 8 carries a dangling record

The headline

- 3,090 of 24,200 seed domains, one in eight, carry at least one dangling record: DNS pointing at something its owner no longer controls.
- 5,632 dangling records in total from the sample, across 222 of the 242 TLDs.
- The typical TLD has 8 of its top 100 affected; a quarter have 20 or more.
- Only 20 TLDs came back completely clean.

Which TLDs break first?



Top of the table

Seeds of 100 with a live dangling record: .au 41, .ca 35, .uk 35, .it 33, .net 33, .mil 32, .jp 30, .fr 29, .es 28, .be 28.

There are more than have DNS issues in the entire zone.

Clean is not who you'd expect

Mature ccTLDs run clean: .ee and .hr at zero, .lt and .lv at one.

Breakage tracks with size and cloud dependency of the estates under a TLD, not the registry's competence.

The fossil record

Records outlive services by years

- 2,274 records still point at Skype for Business and XMPP chat, retired years ago, across 1,863 domains in 188 TLDs. In .edu, 62 of the top 100 still carry one.
- Mostly not exploitable: Microsoft and Google still own those names.
- But they are a perfect lifecycle metric; When a service is switched off, nobody removes the DNS. That same habit produces the dangerous cases.

The ones that matter: 1,161 reclaimable targets

CloudFront
335 records at a deleted distribution

Zendesk
11 records at an unclaimed service

Azure
328 records, reclaimable for most resource types

S3
33 records at a released bucket name

Shopify
10 records at an inactive edge config

Tilda (a worked example)
8 records at removed Tilda sites, e.g. risks.rbc.ru. Site host: reclaim risk

Near misses: broken, not breached

A public-sector typo

dru.agpd.es points at druaepd.edgkey.net, a transposed spelling of Akamai's edgekey.net. Live in DNS, resolving to nothing.

A wound-down CDN

Four Decathlon sites (.be, .cz, .es, .si) point maintenance subdomains at EdgeCast, a CDN that no longer operates.

Why they didn't break

Neither target is registrable by a third party. The records are broken, not breached. That is probably luck, not control.

The fix is upstream

A warning when a new record points at a name that does not resolve would have caught every one at creation.

Beyond dangling: the hygiene floor

37%

Publish DMARC; only 22% enforce it. ccTLDs do better, at 54%, against 23% in new gTLDs.

6.5%

Have validating DNSSEC. MTA-STS is effectively absent at 0.3%.

8%

Of zones return errors: unanswered nameservers, single points of failure, parent and child disagreeing. A registry can see these.

What separates the healthy

Records die with services

When the service goes, the record goes.

Old fossils may linger, but live service records do not.

Delegations match

Parent and child agree on the nameservers. No drift between the registry and the zone.

Secure by default

DNSSEC and email policy are on by default, not something a registrant has to discover.

What registries and registrars can advise customers to do



1. Check every delegation for nameservers that do not resolve, on a schedule.
2. Watch unregistered targets. When a live name points at a target that does not exist, make the DNS change.
3. Push security defaults. DNSSEC on. DMARC with reporting.
4. Move towards automation. Misconfiguration detection, triage, remediation and DNS changes can be automated with confidence.



**Come and
find me.**