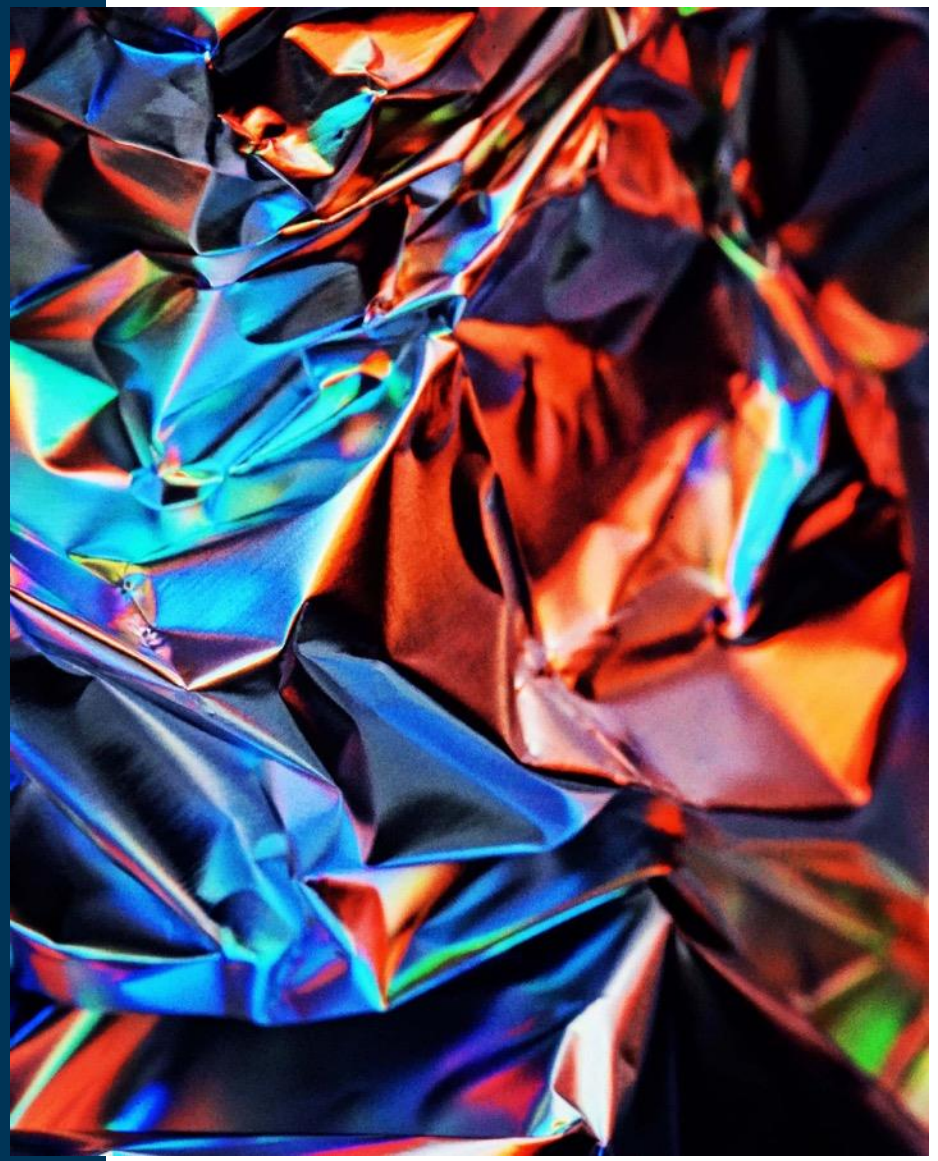
DNS Data and Analysis

Quoc Pham – Senior Product Manager, GoDaddy Registry

GoDaddy Registry



TLD DNS

GoDaddy Registry is a Backend Registry Operator (BERO)

- Clients include ccTLDs (.us) and gTLDs (.biz)
- Support over 200 "TLDs" combined

Provide DNS at the Top Level

- 30+ globally diverse nodes
- Multiple anycast networks

As DNS Operators our Key Principle is to Provide a DNS Service that:

- Aims for Availability (DDOS protection), Performance (fast response/resolution time) and Stability (30+ nodes)
- Adheres to industry best practices (DNSSEC, req of gTLDs however it should be the case for all TLDs regardless of type)
- Exceeds contracted SLAs and internal expectations

GoDaddy Registry

TLD DNS Versus Recursive

- We don’t operate a recursive, for our TLDs we are purely the authoritative server
- Recursive servers get all the interesting data, in general we provide NS records
- However, we also do get some interesting data as well
  - NXDomains, leads to
  - Clues to potential misconfigured networks (e.g. smtp.domain.example, intranet.domain.example, home.domain.example, router-name.domain.example)
  - New botnets not yet launched? (e.g. fd70q43fhjd.domain.example)
  - Zone walking

Name Collision and Controlled Interruption

All gTLD launches required a "name collision" assessment

- SSAC (Stability Advisory Committee) analysed all DNS queries found in the root for TLDs that previously did not exist
- Reason may be due to misconfigured networks (go out to the internet first before looking locally)
- Used to determine client networks that may be impacted

Name Collision and Controlled Interruption

Prior to launch all gTLDs go through a Controlled Interruption (CI) for 18 months

- Zone file published with a wildcard record (NOT STANDARD!!!)
- For 90 days a gTLD MUST NOT have any delegated domains and all DNS responses
- Response to queries that hit the zone must alert the client that they DNS setup needs to be reviewed

```
<TLD>. 3600 IN MX 10 your-dns-needs-immediate-attention.<TLD>.
* 3600 IN MX 10 your-dns-needs-immediate-attention.<TLD>.
<TLD>. 3600 IN SRV 10 10 0 your-dns-needs-immediate-attention.<TLD>.
* 3600 IN SRV 10 10 0 your-dns-needs-immediate-attention.<TLD>.
<TLD>.    3600    IN    TXT    "Your    DNS    configuration    needs    immediate    attention    see
https://icann.org/namecollision"
*    3600    IN    TXT    "Your    DNS    configuration    needs    immediate    attention    see
https://icann.org/namecollision"
<TLD>. 3600 IN A 127.0.53.53
* 3600 IN A 127.0.53.53
```

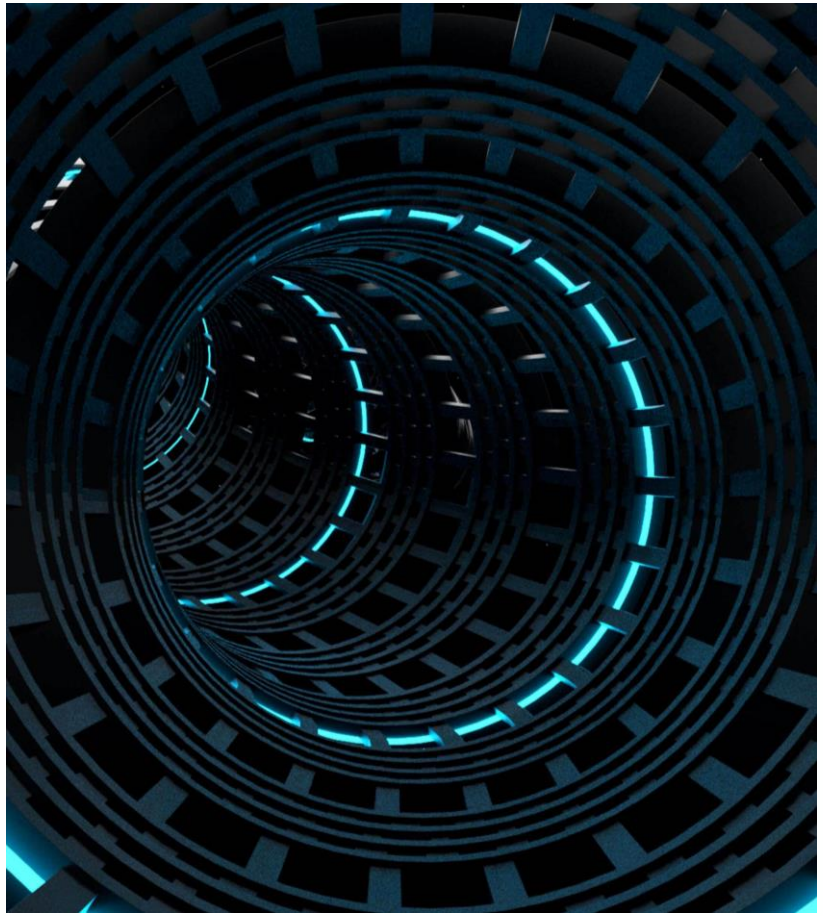
- After the initial 90 days until the remainder of the CI period, Registries have to provide an emergency contact which can be called upon if client experienced a catastrophic failure (e.g. a hospital network, national emergency network, etc)
- No known catastrophic events, over 1200 gTLDs added in the root since 2014 (xn--ngbc5azd or (شبكةwas the first gTLD… operated by GoDaddy Registry

Reference material
https://www.icann.org/resources/pages/ctld-mitigation-2014-10-02-en

GoDaddy Registry

Data Analytics

DNS data is massive…that would be an understatement



GoDaddy Registry

Data Analytics

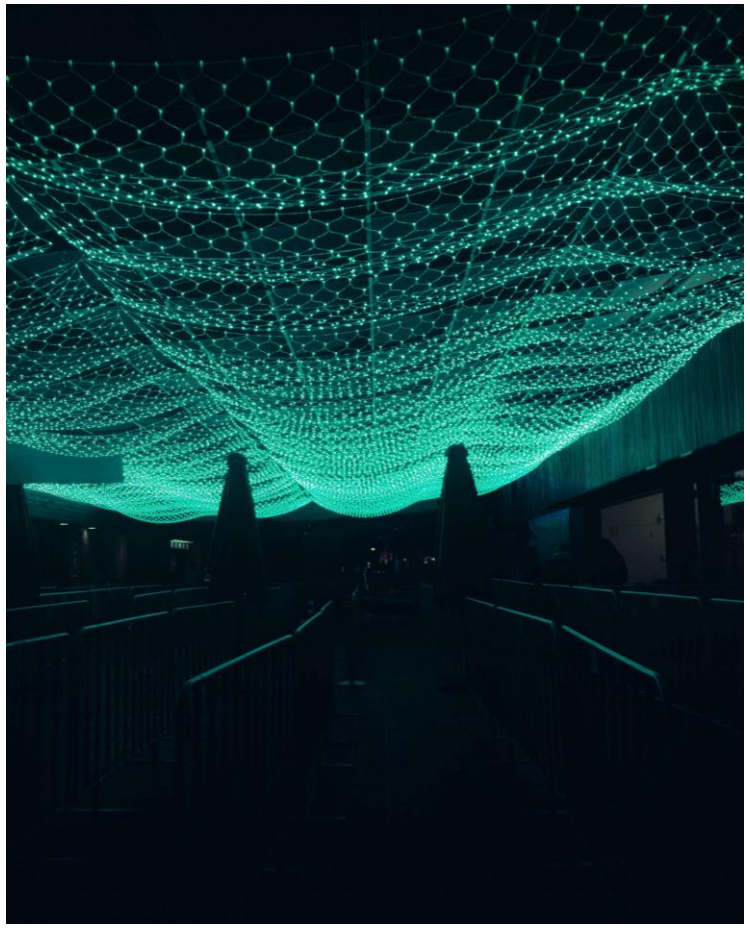
DNS is more than just A and MX records

- IoT devices
- Creative use of TXT records
- DNSSEC … making DNS response size larger! (increase in capacity and throughput requirements!!!)
- Everybody is online now

Data Analytics

What a you looking for?

- Spike in queries for a particular domain (hacked-site.gov.ccTLD)
- "random" queries at sub-domain level (at GDR anything below the zones that we manage)
- "DNS and domain history" … searching for bad actors - same IP for many domains where the IP is a known phishing host



Data Analytics

DNS data is BIG DATA...

GoDaddy Registry

Data Analytics

DNS data is not enough, DNS data provides the roadmap, combine it with other data to tell the whole story

- Depends on what level you are at
- Historical patterns
- Domain registration data
- Application code

GoDaddy Registry

Future/Now Enhancements

DNS over HTTPS – DoH

Harder for traditional methods in "traffic management“ in a corporate network … e.g you can just block DNS lookups and responses to and from hacker.domain.example anymore.

Need more rigid application group policy perhaps?

https://tools.ietf.org/html/rfc8484

DNS over TLS

Network admin can still monitor and block DNS queries

https://tools.ietf.org/html/rfc8310

User privacy and security is important

GoDaddy Registry

Thank You

GoDaddy Registry