

Digital Fraud: Preventing DNS Security Threats

Regulatory Forum 2025 – Ulaanbaatar, Mongolia.

25 September 2025



Champika Wijayatunga
Technical Engagement Director (APAC)

DNS contains a wealth of data about your systems

- Your organization's domain names – **xyz.mn**
- Your organization's individual host names – **host.xyz.mn**
- IP addresses
- Mail server data (MX records) – **mail.xyz.mn**
- Database locations – **db0.xyz.mn**
- etc

Protecting DNS is extremely important

Maliciously Registered Domains

Domains registered by miscreants for

- Counterfeit goods
- Data exfiltration
- Exploit attacks
- Illegal pharma
- Infrastructure (ecrime name resolution)
- Malware C&C
- Malware distribution, ransomware
- Phishing, Business Email Compromise
- Scams (419, reshipping, stranded traveler etc.)
- and more

Some measurements ...

Statistical Overview for 23 Sep 2025

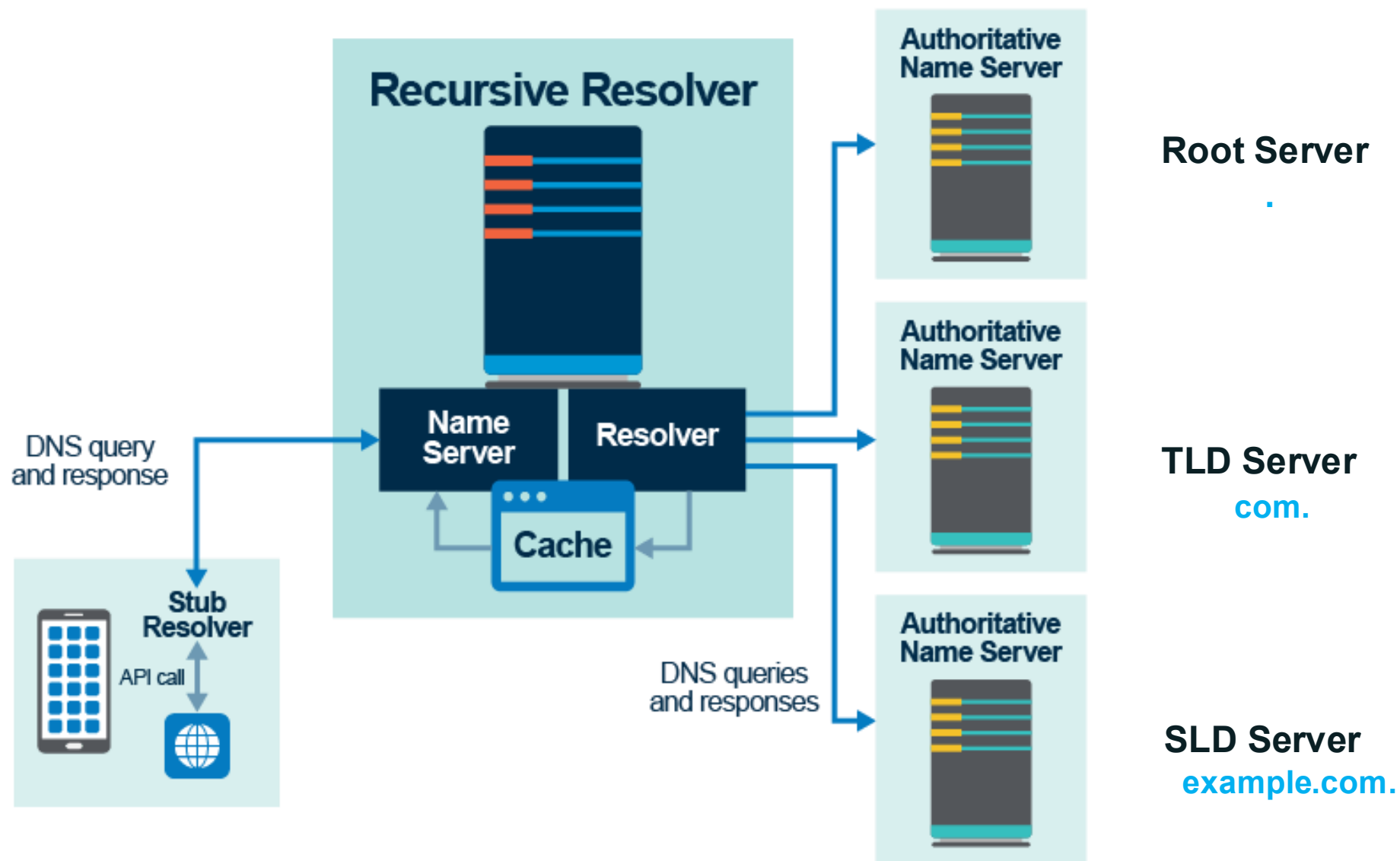
230.1M	1,113	688.7K	442	2,936	1,895
Total number of domains	Total number of gTLDs	Total number of domains with abuse reports	Number of gTLDs with one or more reported domains	Total number of registrars seen	Number of registrars with one or more reported domains

Current Reported Abuse

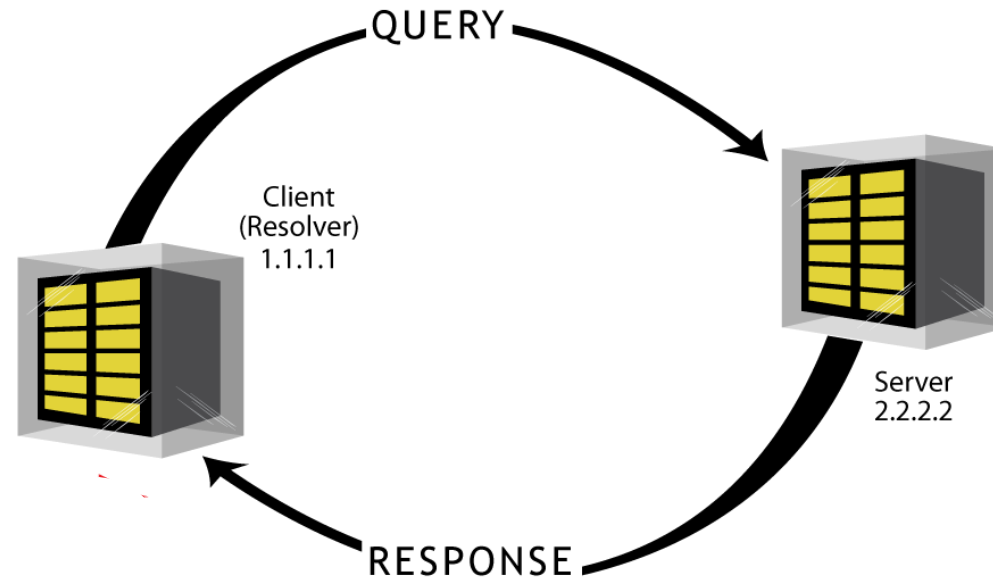
Summary of the Latest Reported Abuse Updated Daily

Reported Abuse Type	Unique Domain Counts	Percentage of gTLD Domain Count
Phishing	683443	0.297%
Malware	4892	0.002%
Botnet C&C	3160	0.001%

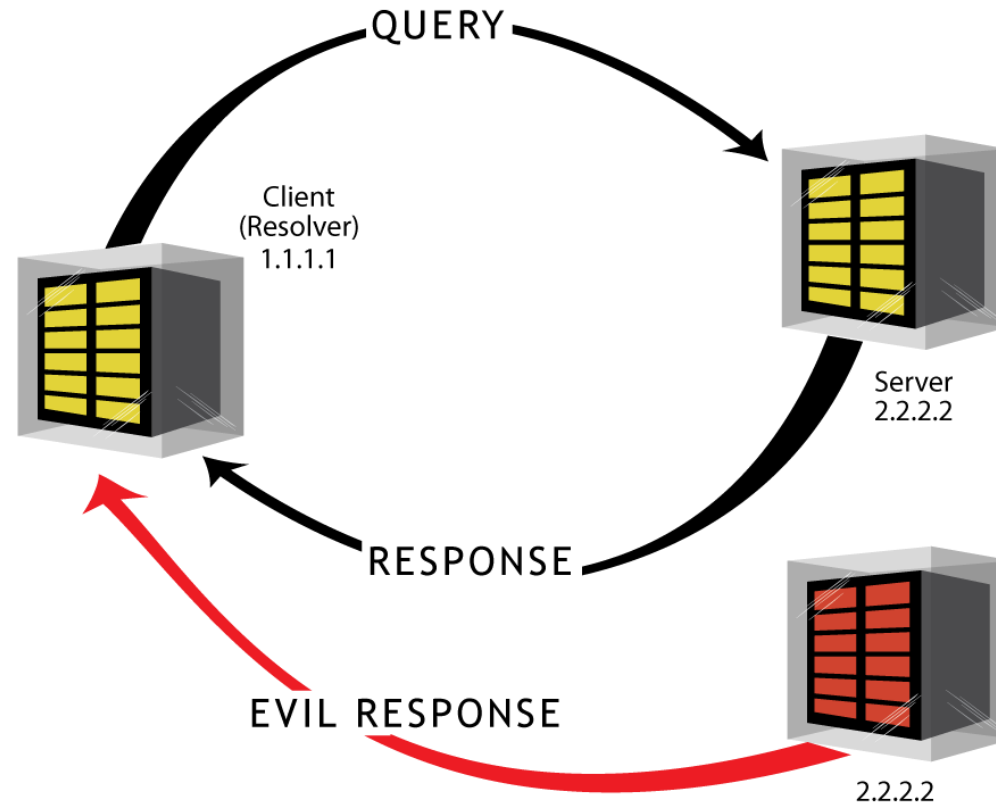
DNS Components at a Glance



DNS and Lack of Security

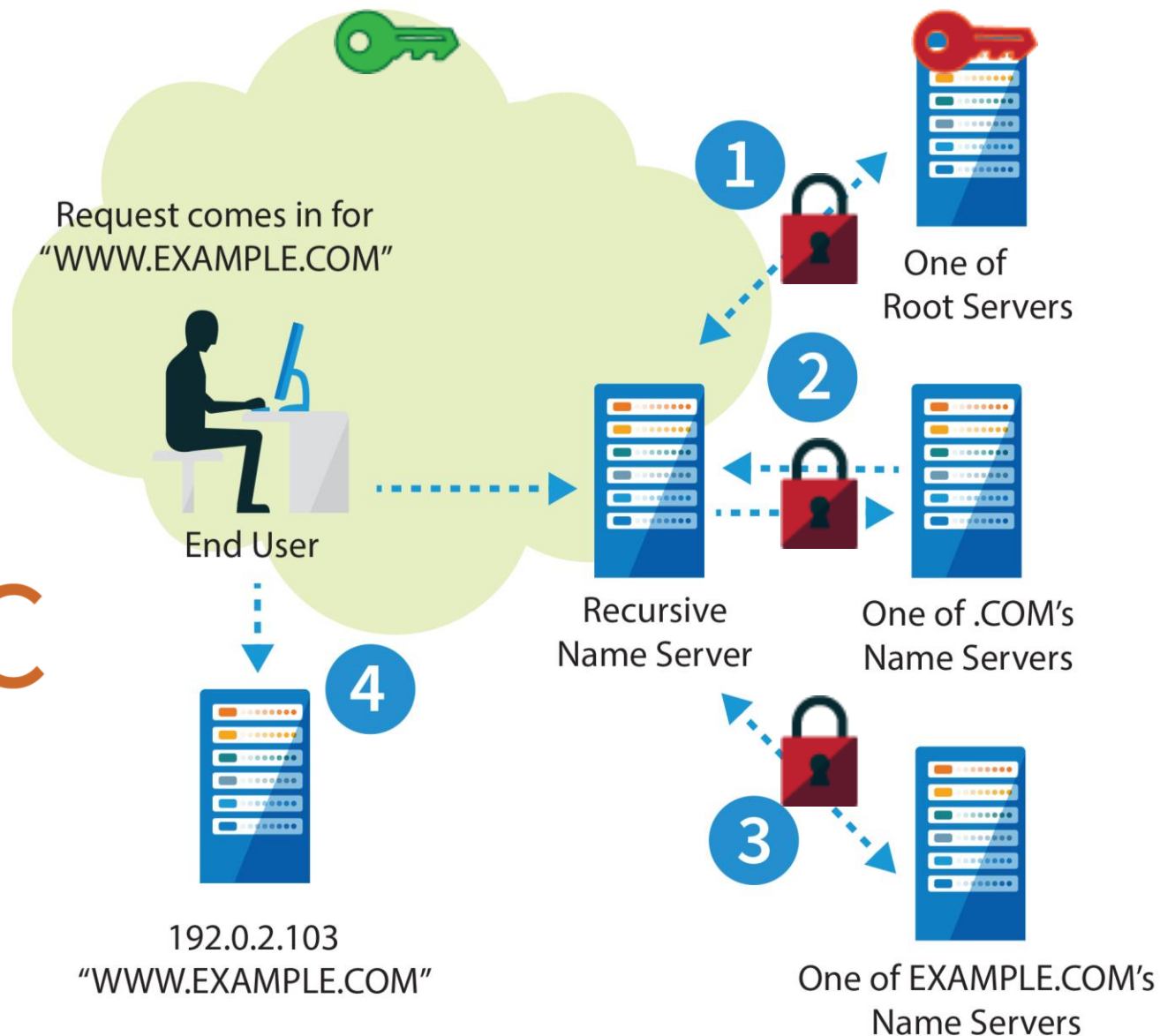


DNS and Lack of Security



DNS Security Extensions

DNSSEC



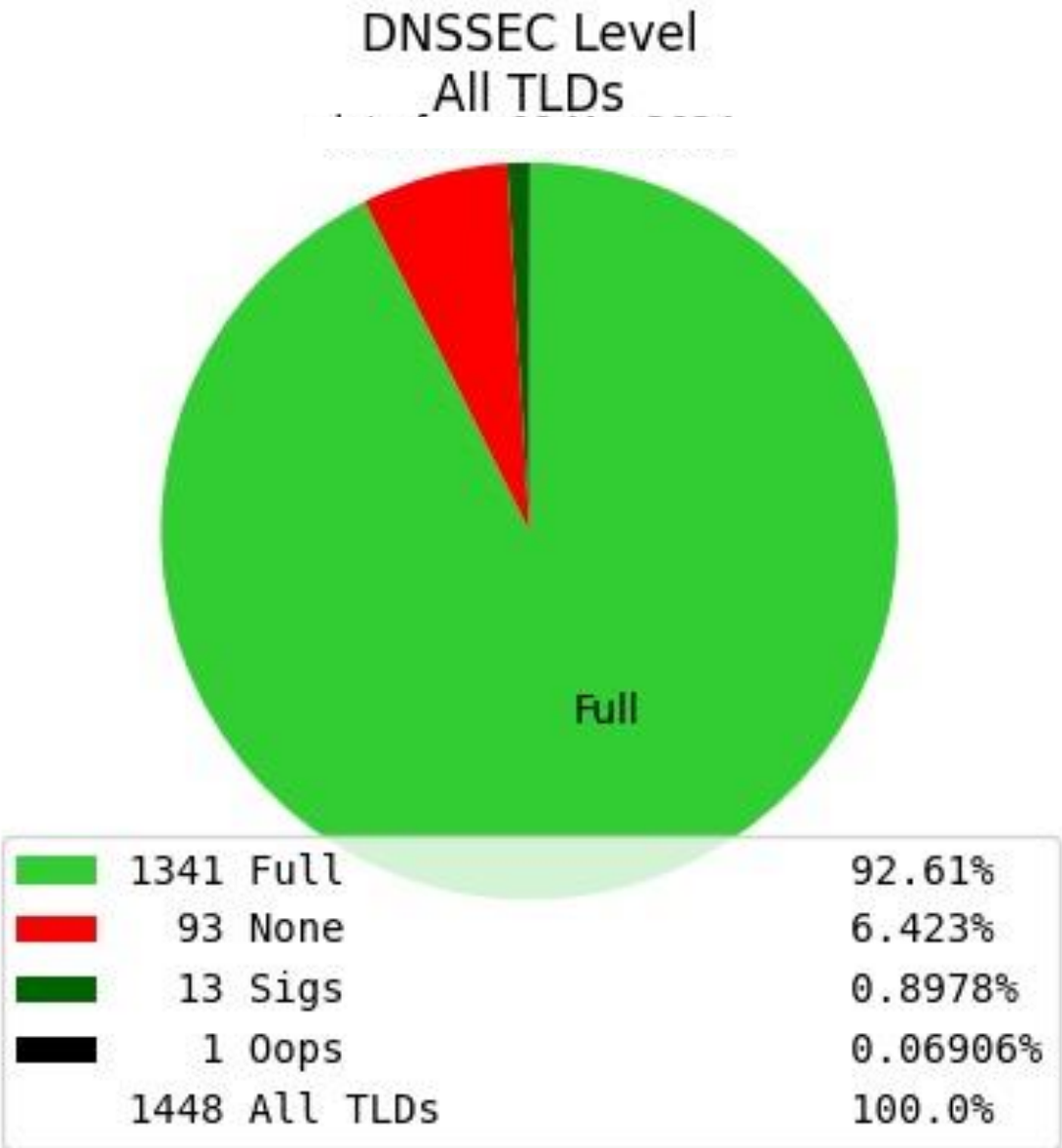
How does DNSSEC work?



Two actions are required :

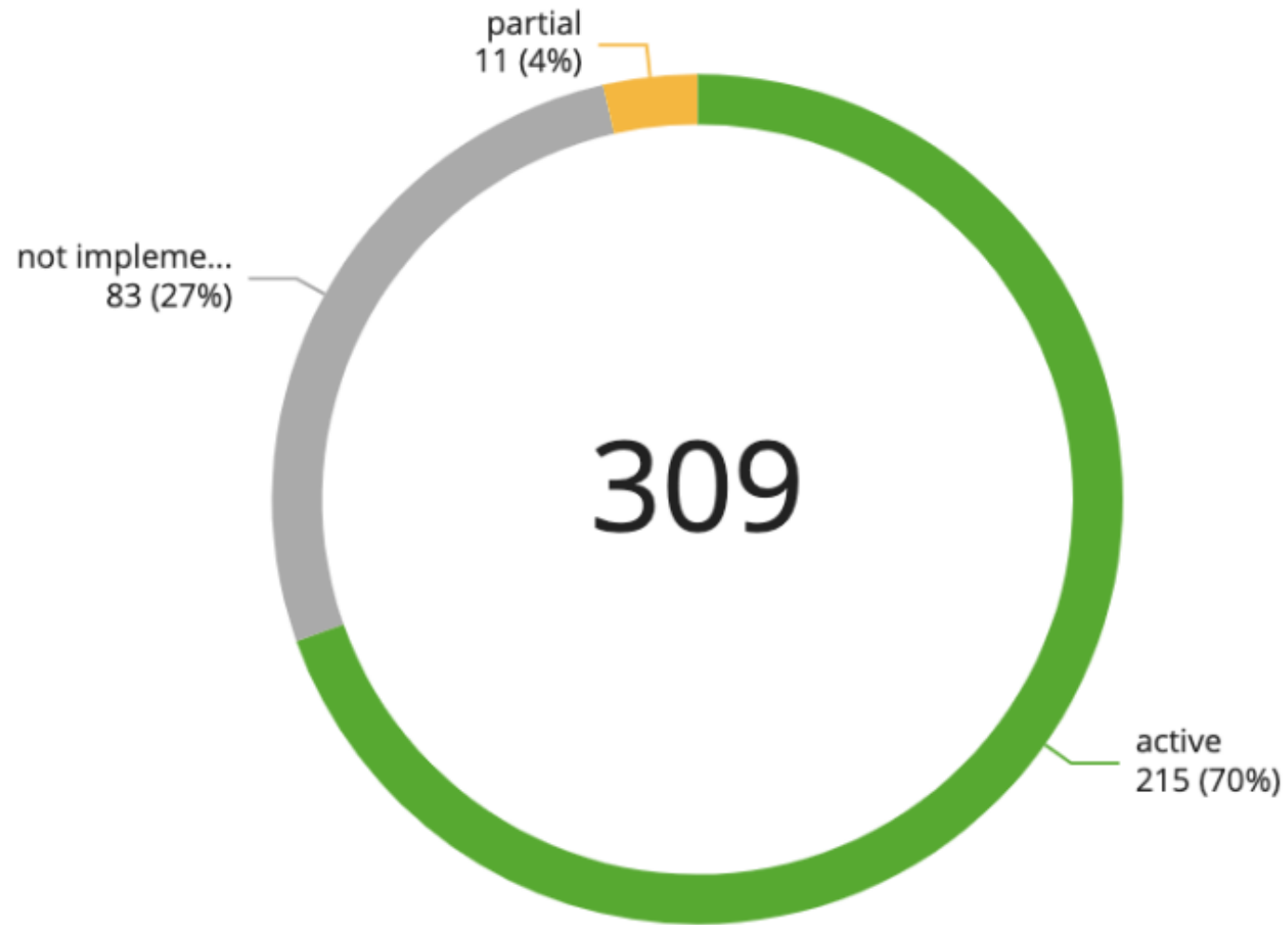
- Registrants (domain name holder) should cryptographically **sign their domain**
- DNS operators, ISPs, mobile operators, hosting providers etc. should **activate DNSSEC validation** in their recursive resolvers

DNSSEC Deployment - All TLDs



Source: ICANN

DNSSEC Deployment – ccTLDs



Source: ICANN

DNSSEC Deployment – Mongolia

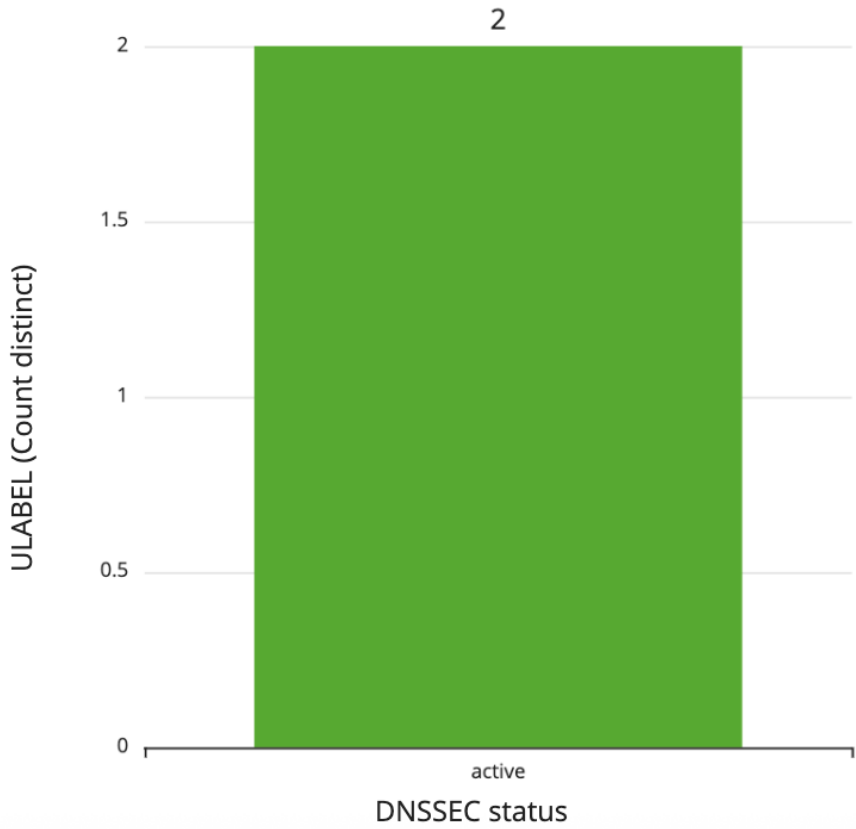
ccTLDs DNSSEC status - dot representation

- Green:** DNSSEC operational (DNSKEY in TLD zone + DS in root zone)
- Yellow:** Partial signed (DNSKEY in TLD zone without DS in root zone)
- Grey:** No DNSSEC (No DNSKEY in TLD zone)



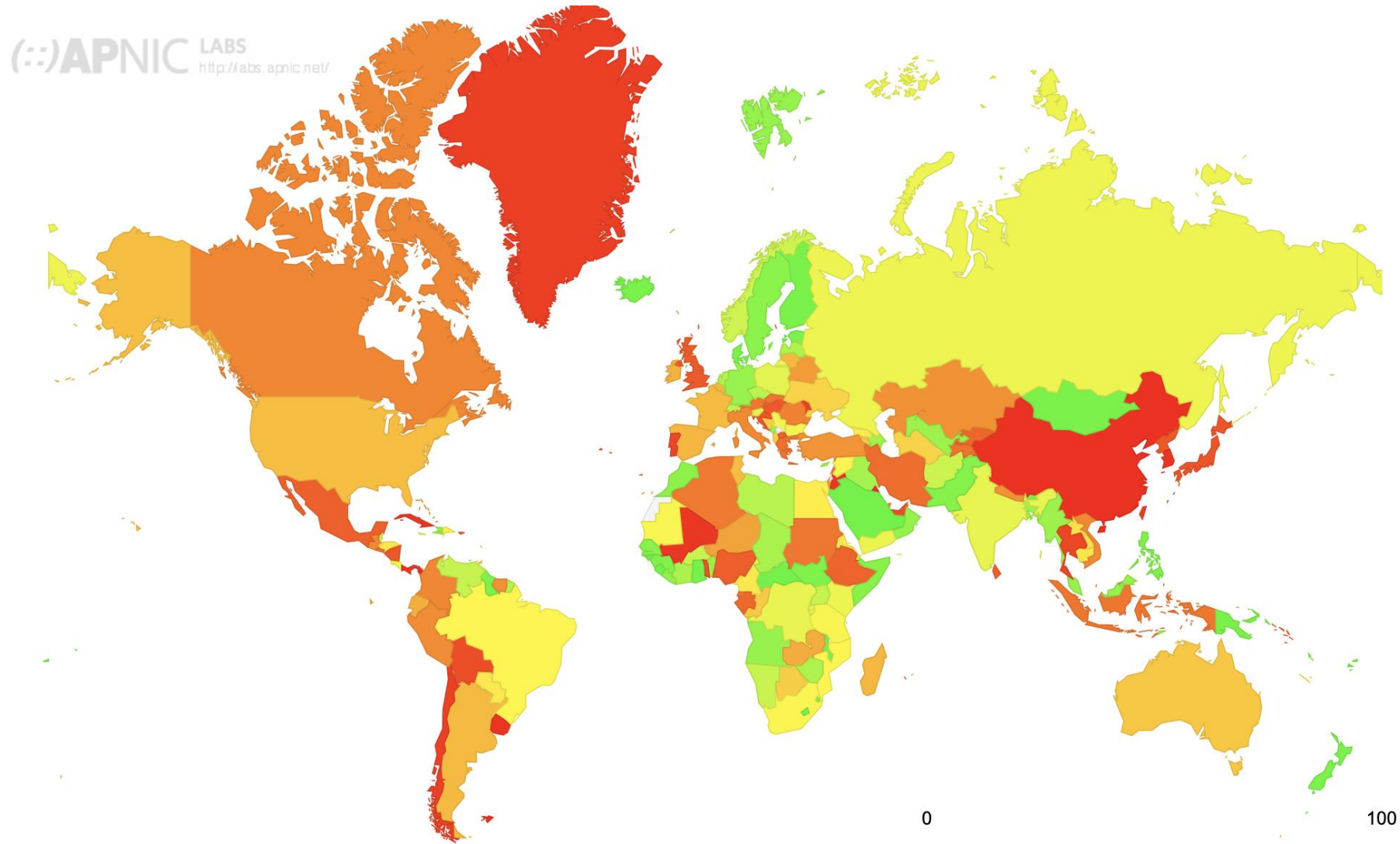
DNSSEC status distribution for selected ccTLDs

- Green:** DNSSEC operational (DNSKEY in TLD zone + DS in root zone)
- Yellow:** Partial signed (DNSKEY in TLD zone without DS in root zone)
- Grey:** No DNSSEC (No DNSKEY in TLD zone)



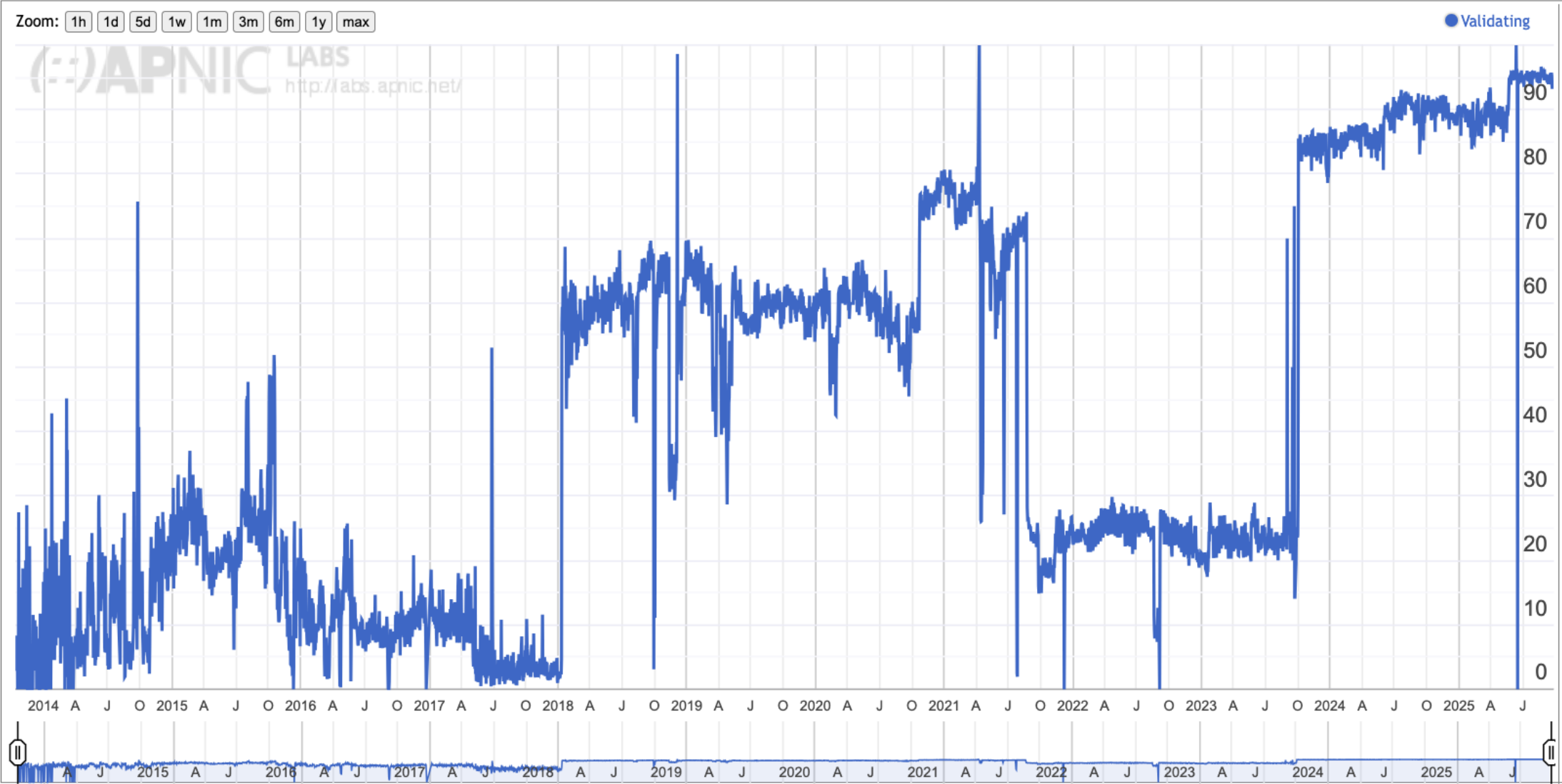
Source: ICANN

DNSSEC Validation – Mongolia



Source: APNIC Labs

DNSSEC Validation – Mongolia



Source: APNIC Labs

What you can do

- **Governments, Policy makers**
 - Encourage DNSSEC compliance
- **Registries/Registrars/DNS Operators**
 - Offer DNSSEC services to registrants
- **For Companies, Financial Institutions etc.**
 - Sign your corporate domain names
 - Enable DNSSEC validation on corporate DNS resolvers
- **Internet Service Providers (ISPs), Mobile Operators**
 - Enable DNSSEC validation on ISP resolvers
- **For Users**
 - Request ISP to turn on validation on their DNS resolvers
- **For All**
 - Awareness about DNSSEC, training and education

Engage with ICANN – Thank You and Questions



One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann