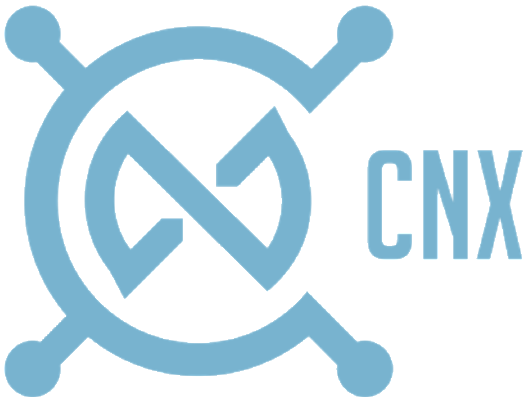
THE MOST IMPORTANT SERVICE and its future

The road to resolverless DNS



Mike Gaertner @ CNX

Thank you to:
Geoff Huston, Chief Scientist, APNIC

KHNOG
Cambodia Network Operators Group

KHNOG 4 CONFERENCE
Sharing for Better Community

DNS today

- Infrastructure
- Problems
- Solutions
- The Future

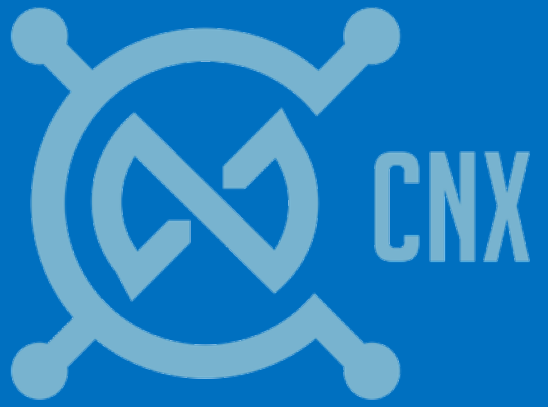
CNX

KHNOG
Cambodia Network Operators Group

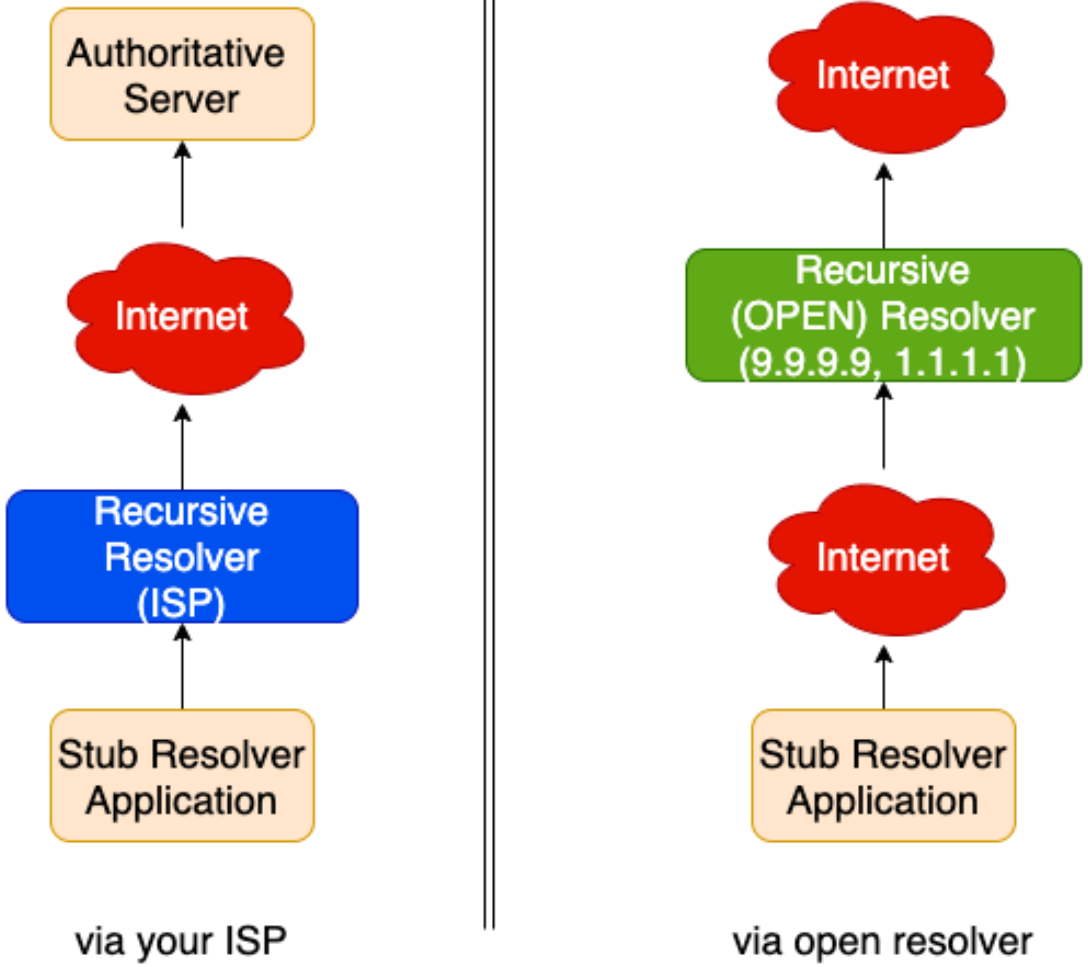
KHNOG 4 CONFERENCE
Sharing for Better Community

DNS ???

- DNS works (kind of)
- Nobody (really) cares about it
- Nobody invests in it (!!!)
- Nobody is interested … except
  - by the people who want to know you, or
  - want to control what you can access, or
  - people sell the domains and ICANN
- BUT YOU USE IT every day

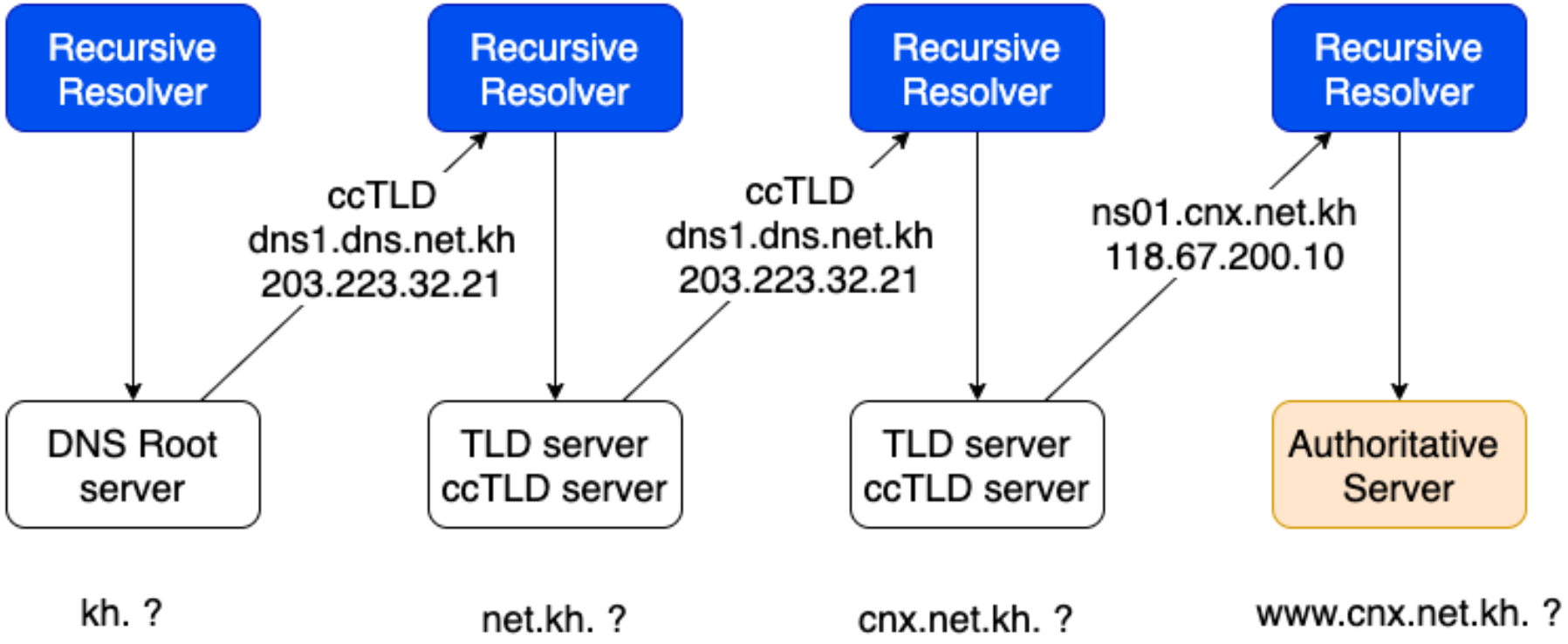


DNS infrastructure



Authoritative Server where are you?

Find the authoritative server



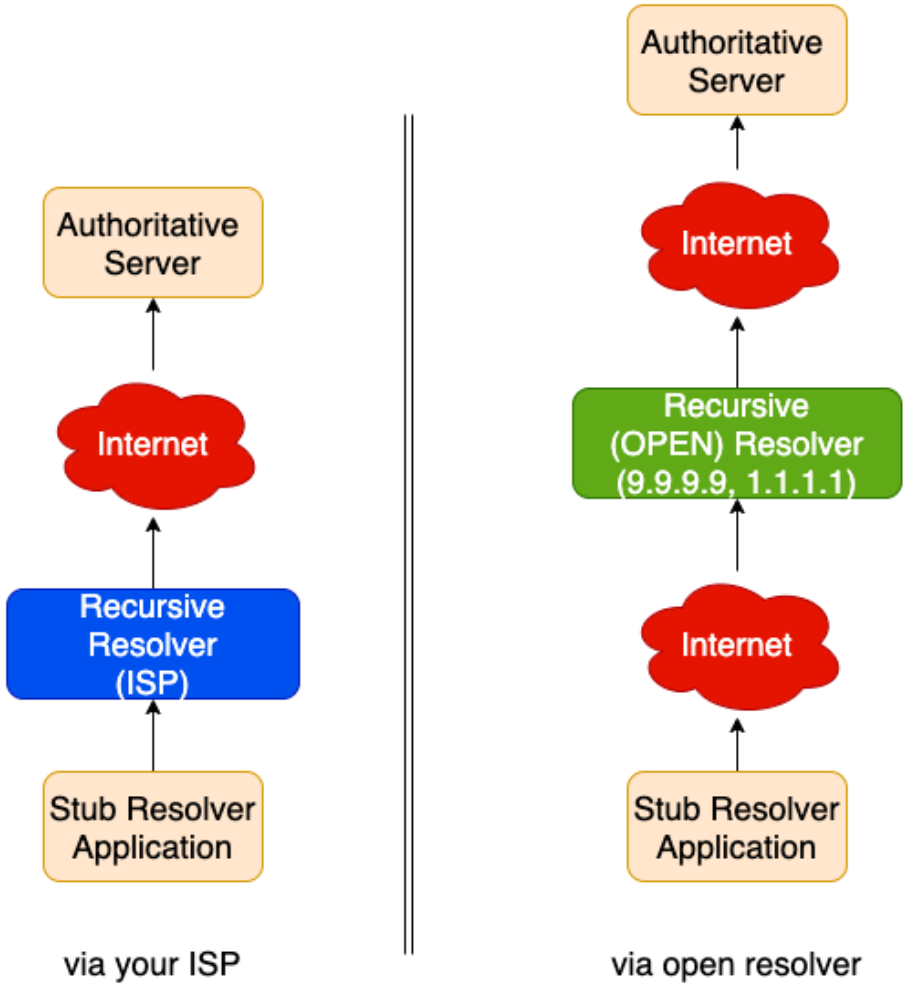
CNX

KHNOG
Cambodia Network Operators Group
KHNOG 4 CONFERENCE
Sharing for Better Community

Root servers, the missing link

- **Q: How does the resolver know the root server ?**
- A: they have a list, there are 13 root servers with know IP address, named a,b,c … m.root-server.org
- **Q: Where are they?**
- A: everywhere around the world using any-cast IP
- **Q: Are they in Cambodia**
- A: yes
  - CNX hosts D,E and I root
  - Mekong Net hosts F-Root
  - Neocom hosts K-Root

DNS infrastructure is open!



DNS queries are send using **unencrypted UDP by default**

Those unencrypted packets transit across the public internet

Any transit network can:

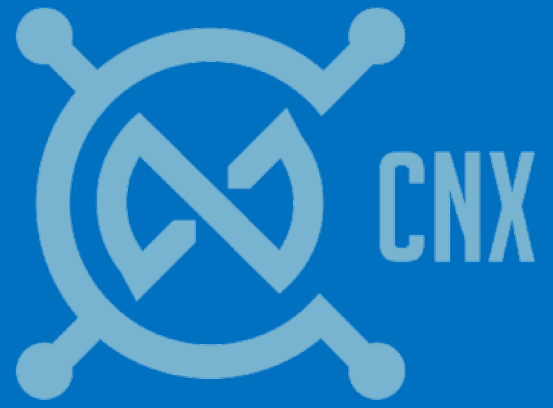
- Monitor
- Intercept
- Substitute

CNX

KHNOG
Cambodia Network Operators Group
KHNOG 4 CONFERENCE
Sharing for Better Community

The problem with DNS

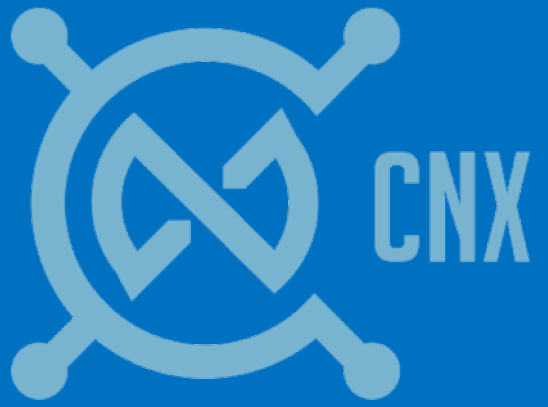
- **Speed** – DNS can be very slow and cached result can make the resolution unpredictable
- **Filtering** – the DNS is a convenient control point for content management
- **MetaData** collection – the DNS is a real time window on user behaviour
- **Search** - NXDOMAIN rewriting into active search



Without DNS
Users are lost

More …

- There is no authentication method for DNS Servers,
- the stub resolver (your computer or phone) has no way to verify that it is talking to the real resolver or an imposter
- 9.9.9.9 in your local network maybe is a resolver operated by your ISP and not by google
- The stub resolver and the recursive resolver have no way to validate a standard DNS response, mostly it is asking you to blindly trust the answer



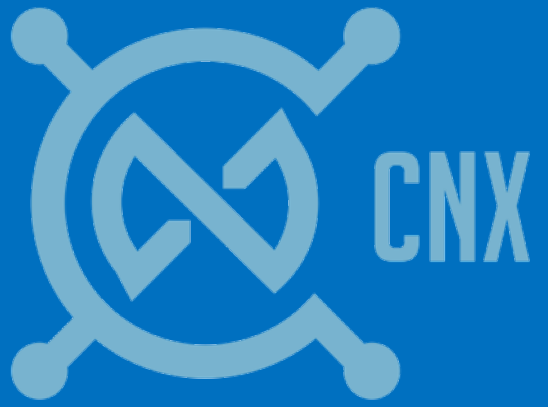
In summary

- Standard DNS is broken
- It is a huge privacy leak
- any network the packets cross, can fake the response

There is no guarantee that the server your are trying to reach, is the real server

Your domain can be moved anywhere

(if I can fake the DNS,
I most likely can get a new SSL cert as well)

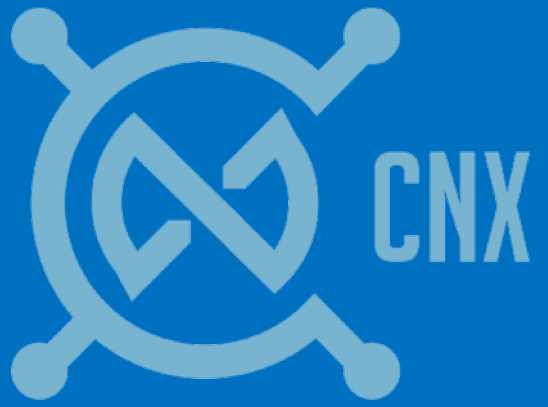


Reminder:
Most cypher attacks
Are state sponsored

KHNOG
Cambodia Network Operators Group
KHNOG 4 CONFERENCE
Sharing for Better Community

None of that is new …

- DNS was born in 1983 (its most likely older then you!)
- DNS attacks are happening with increasing frequency today
- DNS cache poisoning is know attack vector since 2005
- DNS attacks can be carried out in your local network with ARP spoofing and a simple python script



The Security Picture

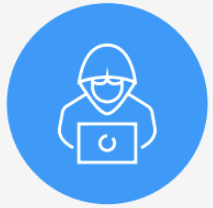
88%
experienced one or more attack

$942k
average cost of attack

7
attacks on average per organization in the past 12 months

70%
suffered application downtime (cloud or in-house)

51%
were victim to a phishing attack



24%
had data stolen as a result of an attack

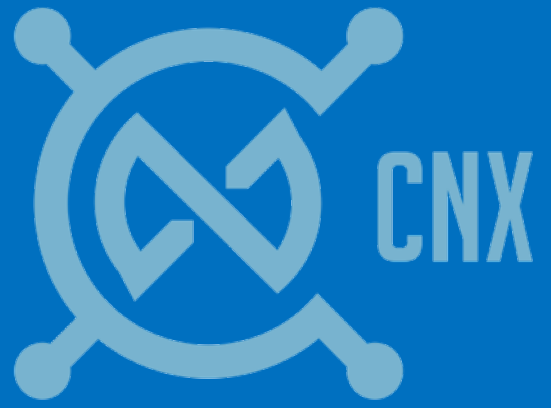
Awareness of DNS security is very strong:
73%
say it is critical

IDC 2022
Global DNS Threat Report

KHNOG
Cambodia Network Operators Group
KHNOG 4 CONFERENCE
Sharing for Better Community

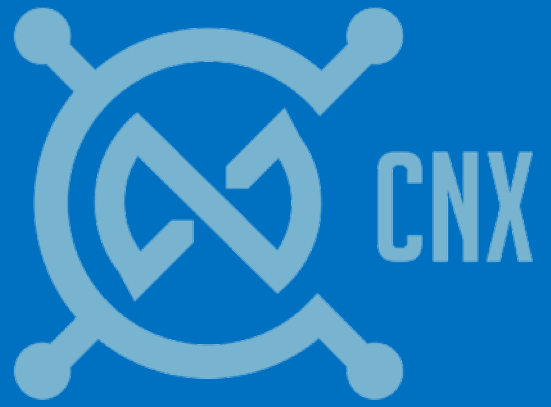
What's the roadmap

1. Securing the DNS response using DNSSEC
2. Securing DNS queries in transport with
   - DNS over TLS
   - DNS over QUIC
   - DNS over HTTPS (DoH) <- the new developing default



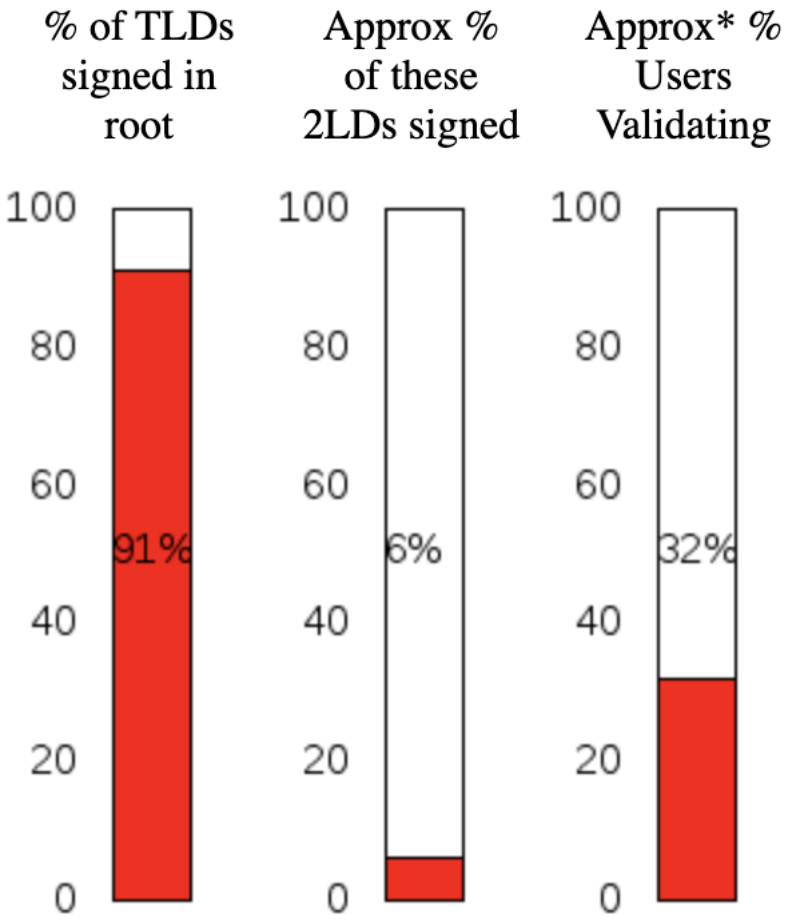
DNS SEC

- DNSSEC provides
  - origin authority,
  - data integrity, and
  - authenticated denial of existence
- Validation of DNS responses occurs through the use of digital signatures that are included with DNS responses
- These digital signatures are contained in new, DNSSEC-related resource records that are generated and added to the zone during zone signing

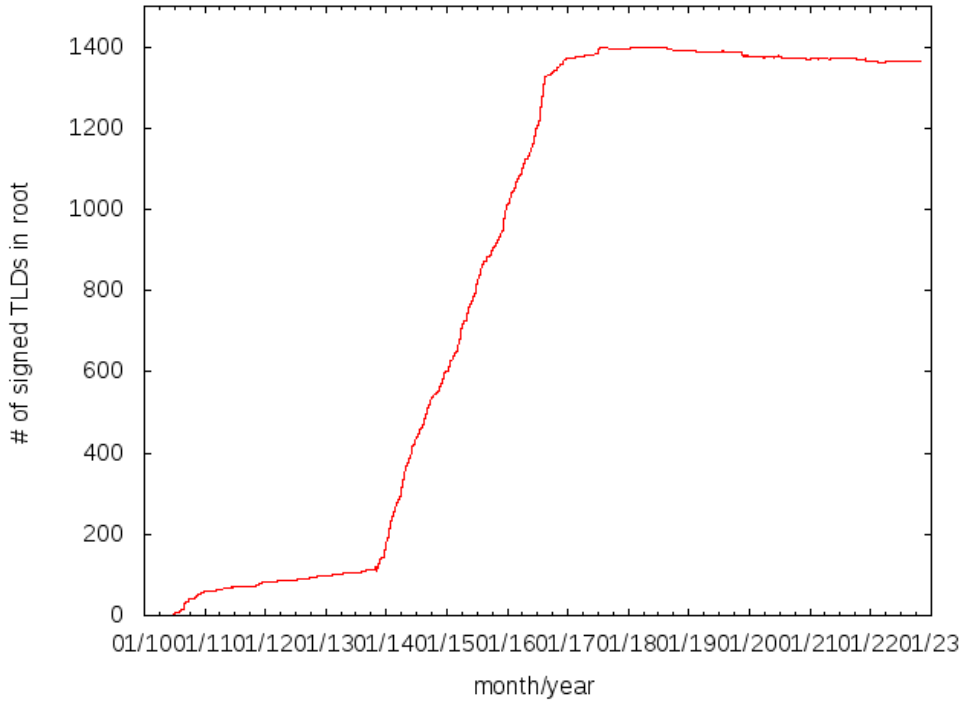


Fully supported in
- Bind9
- powerDNS
- MS DNS

The problem is -> with us…



TLD's signed

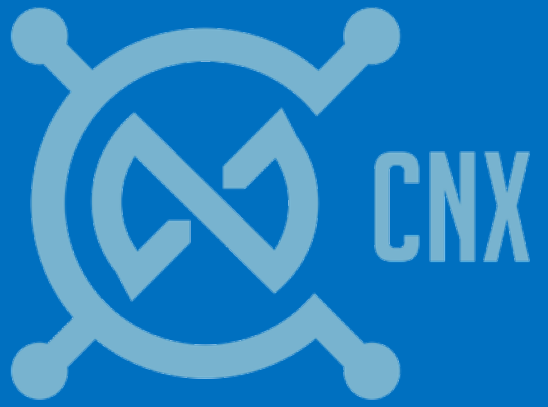


KH. ?☹

DNS SEC

- Protecting the DNS since 2005, **not**
- Majority implemented by all registrars 2010-17
- .com was signed March 31, 2011 (over 10 years)
- .com has 159mm domains and some 2mm NS servers, only 5.8mm use DNSSEC

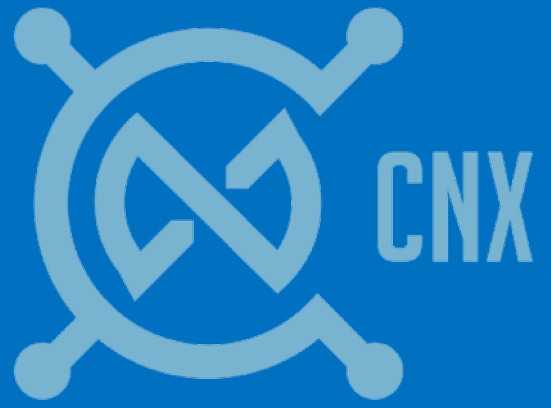
But sure 73% of engineers think it is critical!



TLD Zone File Statistics
November 2022 Reports

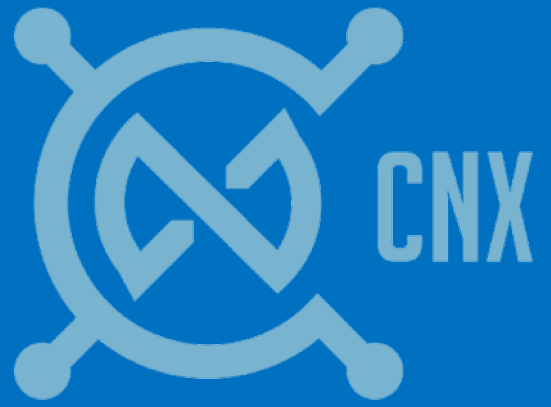
DNS in transport, DoT/DoQ/DoH

- Stub resolver can authenticate the recursive resolver using TLS
- Session is encrypted, no more payload tampering or data leakage into the internet
- No UDP fragmentation and TCP failover issues



DoH the leading contender

- DoH sits alongside all other HTTPS traffic on TCP port 443 (HTTP/2) and UDP port 443 (HTTP/3) and is harder for network level isolation of DNS traffic
- generic HTTP caching controls can be used to enable or disable the use of HTTP caching
- applications need not use the local stub DNS resolver and can direct DoH queries to a recursive resolver of its own choice
- **DoH is an emerging browser default these days for encrypted DNS**



18% of queries to Cloudflare's Open Resolver are using **DoH** already

What is to come?

- Because HTTP/2 and HTTP/3 includes “Server Push”

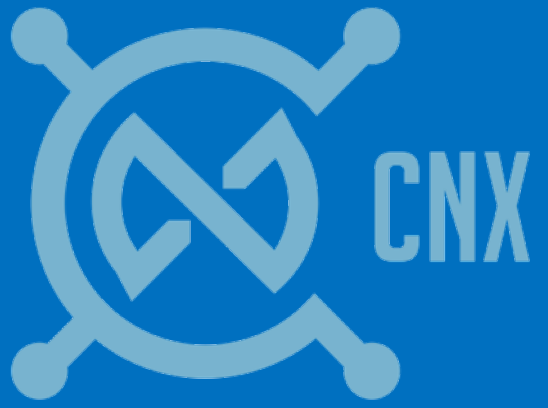
RFC 7540: **Hypertext Transfer Protocol Version 2 (HTTP/2)**

8.2. Server Push

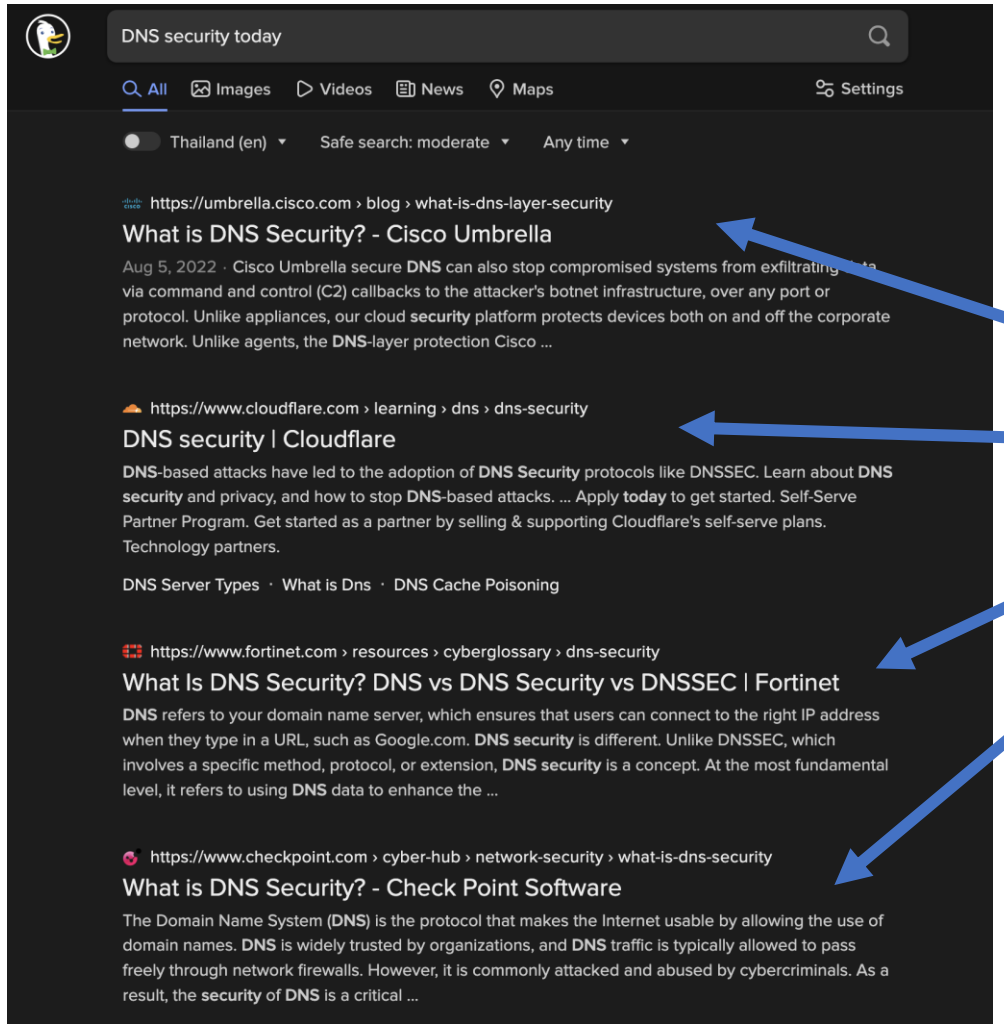
HTTP/2 allows a server to pre-emptively send (or "push") responses (along with corresponding "promised" requests) to a client in association with a previous client-initiated request. This can be useful when the server knows the client will need to have those responses available in order to fully process the response to the original request.

Which means …

- When a server sends a response to an HTTP request it can also push unrequested DNS responses
- This allows the user application to use these DNS resolution outcomes immediately and bypass DNS resolution delays (much faster !!!)
- The user is not making these resolution queries, and is not generating meta data within the DNS (increased privacy)



Example



Potential server
Push objects

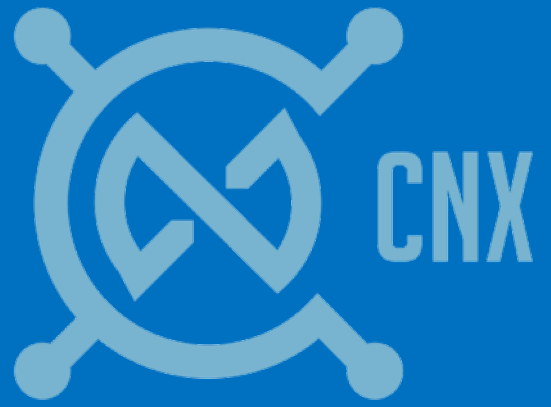
CNX

KHNOG
Cambodia Network Operators Group

KHNOG 4 CONFERENCE
Sharing for Better Community

But …

- How do you know that the server is pushing the “truth” when it provides these DNS answers?



DNS SEC to the rescue

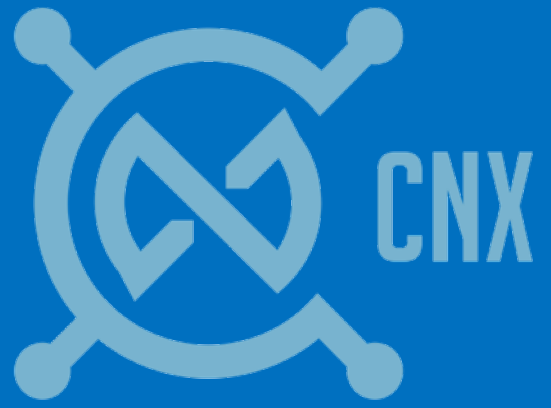
- The server could also push the collection of DNSSEC validation responses to the client
- The server could also repackage these responses into a RFC 7901 EDNS0 Chain Response, attached to the original response
- That way the response and the reason why the response is authentic can be packaged into a single pushed DNS object

DNSSEC validation is providing the assurance that the data is usable

And **without** DNS SEC?

- You have no idea how the server obtained the DNS data in the first place
- You don’t know how current the data is
- You really don’t know if the server is trying to deceive you
- And you have no idea who you are implicitly trusting if you use the data

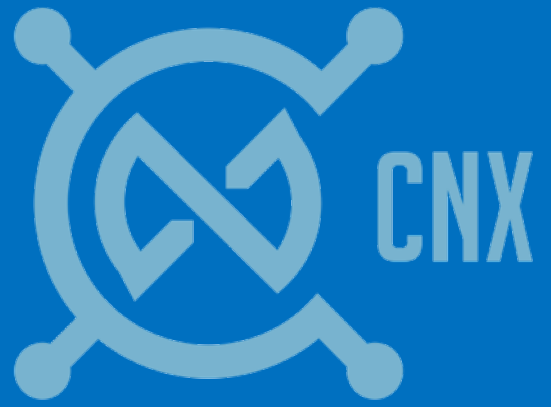
It’s probably best to discard it!



Why is it happening?

We have spent a huge amount of effort over the last decade trying to make the Internet faster:

- We've been deploying CDNs to replicate content and services and bring them closer to users
- We've been deploying non-blocking transport protocols (such as QUIC) to exploit parallelism
- We've been tuning TCP and network behaviour to create more efficient and faster network transactions
- We've been packing more information in the DNS to make service startup faster (SVC and HTTPS records)

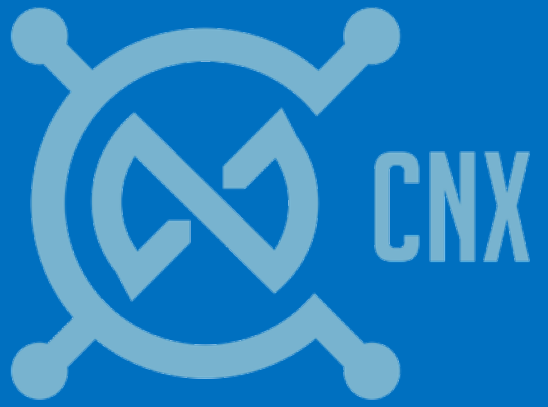


last (?) barrier to faster browsing

- DNS is a massive time penalty
- DNS is a significant privacy leak
- DNS is a consistent source of failure

DoH won’t fix all at once …

- But it can hand a significant amount of control over application and service quality back to these HTTPS-based applications and services
- It can allow the end client to directly validate DNS information **without blind trusting** in a recursive resolver
- **And it’s a whole lot faster!**
- And is hides the client from the DNS resolution infrastructure



Good By,
thank you for 40 years of service

buLDwInbErTH