The KINDNS of strangers

P. Regnauld
NSRC

R. Sommese
University of Twente

UNIVERSITY OF OREGON

UNIVERSITY OF TWENTE.

NSRC
Network Startup Resource Center

KINDNS

?

A Program supported by ICANN to develop and promote a framework that focuses on the most important ***operational*** best practices or concrete instances of ***DNS security best practices***.

https://KinDNS.org

Disclaimer

Phil was tasked by ICANN to identify DNS operational best practices in KINDNS.
But today, we are presenting this independently.

Background

This started out as a discussion on how we could measure uptake of KINDNS…

KINDNS recommendations can be broadly separated into two categories:

- Those that are directly observable / measurable for an external observer
- The rest, including changes in processes that don't necessarily translate to something "visible" on the Internet
  - Platform hardening
  - Improved security practices
  - Implementing 2FA for customer access

Background

We wanted to find out…

- Which recommendations did operators find useful?
- Which ones, less so?
- Which ones weren’t implemented because too costly/complicated?
- For those that were, what was the impact/cost for the organization?
- Which ones had already been implemented beforehand?
- And, finally, what other recommendations did operators feel were missing?

Background

But, we also wanted to understand something else:

- Why was there so little uptake on KINDNS ?
  - Were the respondents aware of KINDNS ?
  - If so, why not join?

We launched the survey mid-august…

Responses

Not a huge amount of response, but we did get some insight:

- Most respondents *are* aware of KINDNS
- Most operate both authoritative and recursive services
- The majority were operating TLDs, SLDs, or public resolvers

Interestingly, more than half of respondents hadn’t attempted to join KINDNS

- As in, register with the initiative – not implementing changes

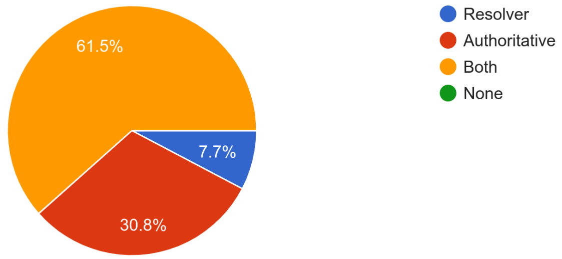
Half of the respondents *did* make changes to their operations as a result

- Either platform hardening / firewall / network configuration, or updating of policies
- Most wanted to either improve their posture, or be an example for the community

Our Responders in Detail

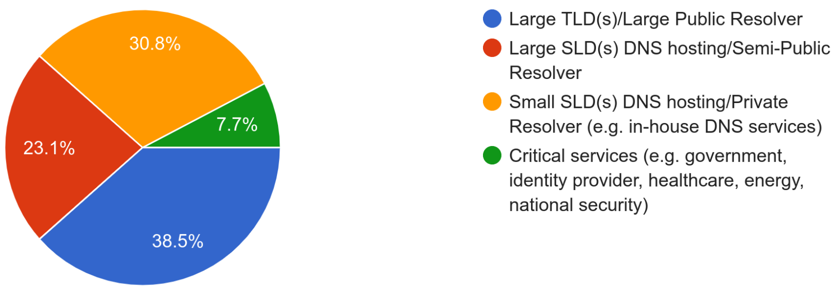
Are you a Resolver Operator or Authoritative Nameserver Operator?

13 responses



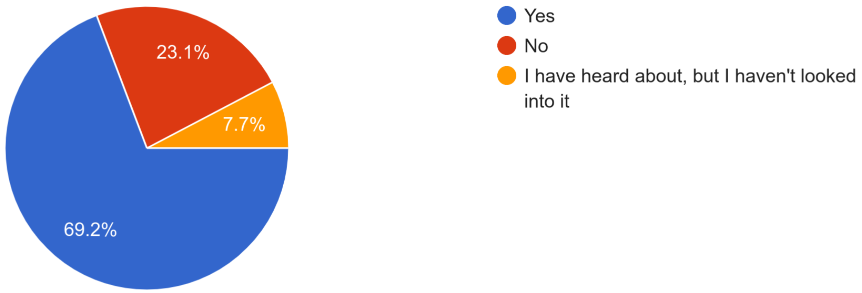
Which kind of infrastructure do you operate?

13 responses



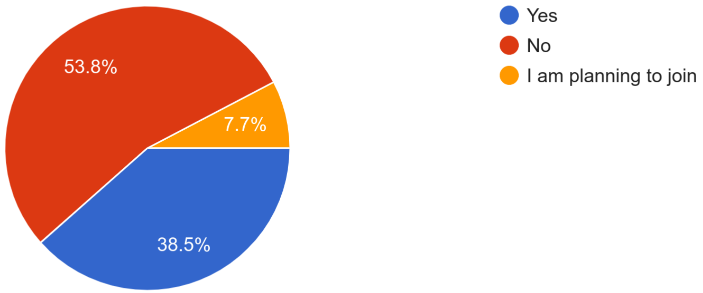
Are you aware of KINDNS?

13 responses



Have you joined (or attempted to) join the KINDNS initiative ?

13 responses



Main showstopper

In the reasons as to why respondents hadn't implemented KINDNS recommendations, we found some interesting comments:

- General lack of willingness to join (2 cases)
- Not knowing about the initiative (2 cases)
- Already implemented in a different way (1 case)
- Not applicable (1 case)
- Not available in their language (1 case)
- Distrust towards the initiative (1 case)

Takeaway: the current initiative suffers from lack of outreach towards the community. Operators aren't aware of the initiative, or they're hesitant to join - either because of too little interest, a too high technical threshold, or lack of buy-in in the initiative itself.

A necessary, but non-marketable effort

Half of the participants joining KINDNS affirmed to have made changes to their infrastructure to become compliant:

- Primarily in terms of reviewing/updating internal administration policies and platform hardening

- However, very few of them perceived KINDNS as a possibly marketable effort
  - (i.e.: one that could contribute to better branding / attracting customers)

Authoritative NS Practices

We asked participants' take on KINDNS authoritative NS best practices in terms of relevance and effort required to implement them.

- Zone Integrity, NS (geographical, network, technical) diversity and Monitoring were rated as most relevant!
- DNSSEC, limiting zone transfers and separation of authoritative and recursive duties considered as mildly relevant.
- Software diversity is controversial for some
- Software diversity also listed as difficult to implement, followed by DNSSEC

Recursive NS Practices

We asked participants' take on the KINDNS recursive NS best practices in terms of relevance and effort required to implement them

- Logging practices highly debated (due to privacy ?)
- DoT/DoH and QNAME minimization are also not considered entirely relevant
  - or outright detrimental to stability due to non-compliant implementations in the case of QNAME miminimization
- Software diversity was again labelled as the most difficult to implement
  - followed by QNAME Minimization and DoH/DoT

Hardening Practices

We asked participant takes on KINDNS hardening best practices in terms of relevance and effort required to implement them

- Implementing proper ACLs, BCP 38/egress filtering and credential considered slightly harder to implement, with no great consensus on their usefulness
- Restricting DNS servers to only run DNS software, and logging practices not perceived as extremely relevant for all parties

Takeaways

- We certainly didn't expect consensus, or that everyone would find all best practices relevant to them.
- Some comments criticized KINDNS for being too prescriptive
- Or for being too vague
- On the more vocal side: criticism of ICANN's approach to the process, BCPs not selected by "real" operators, …

Measurable?

Researcher Hat here

- Some of the current best practices currently defined in KINDNS are nearly impossible to measure.
- This is due or to the lack of a metric for the adoption of that practice or to the lack of third-party verifiability
- How we can assess the usefulness of this practices, if in some cases, even operators cannot assess their adoption?
- Practices to gain widespread should be easy to implement and verify both from operators (a KINDNS compliancy toolchain?) and third-party researchers.

Critical vs Non-Critical: Costs vs Benefit

- In the current KINDNS specification, Critical and Non-Critical services differs very little in terms of BCP.
- There is, however, a huge distinction between them.

For example:

  - Anycast (not a current BCP of KINDNS) is extremely relevant if operating a large registry/registrar or a sensitive deployment (e.g., eGov)
  - Anycast is also an expensive technology to implement, both from the monetary and technical knowledge perspective.
  - Critical deployment should prioritize this investment, while non-critical may focus on other low-hanging fruit practices to increase their resilience.

- How we define the separation between Critical and Non? Different tiers like MANRS and MANRS+?

Marketable KINDNS

- How can operators market their KINDNS effort to their customers?

- Incentives programs of several ccTLDs helped the widespread of DNSSEC adoption (e.g., Sweden and Switzerland).

- Incentives for KINDNS may be, however, hard to implement (or undefinable) given the broadness and the diverse nature of the operators involved in the initiative

- KINDNS as a "sustainability initiative" of the DNS ecosystem

Where to from here?

- While KINDNS initiative started with the best intentions, there was not enough uptake
  - Say, compared to MANRS

- This was due to several reasons outlined before.

- The question remains:

  How we can identify a good set of **measurable** best practices to which operators agree to commit?

Where to from here?

- Do we need to start over, or can we pick up the discussion, and improve the shortcomings ?
- What should ICANN’s role be here ?
- Suggest picking up the discussion on the kindns-discuss list
- Either way, this is too important to just leave alone
  - Threats against the DNS are increasing rapidly
  - We need some sound DNS best practices that we can orient newcomers and experienced operators alike towards.

Questions

?