

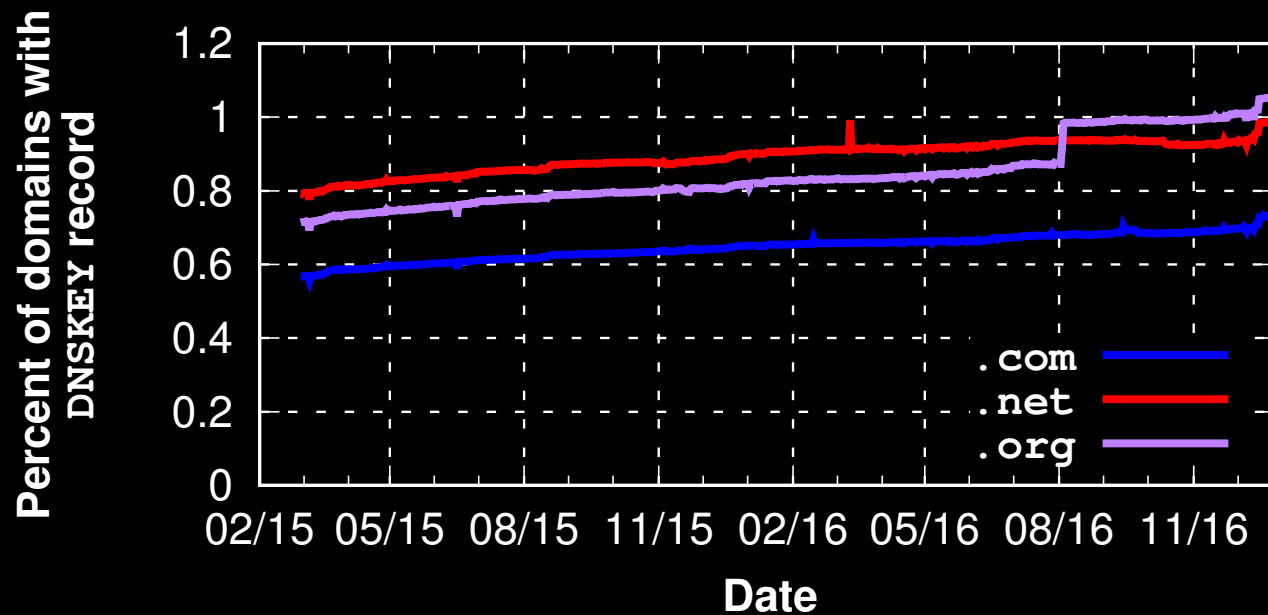
Understanding DNSSEC challenges from the administrator's point of view

Ishtiaq Ashiq, Tijay Chung*, Casey Deccio
Virginia Tech, Brigham Young University

DNSSEC is important.

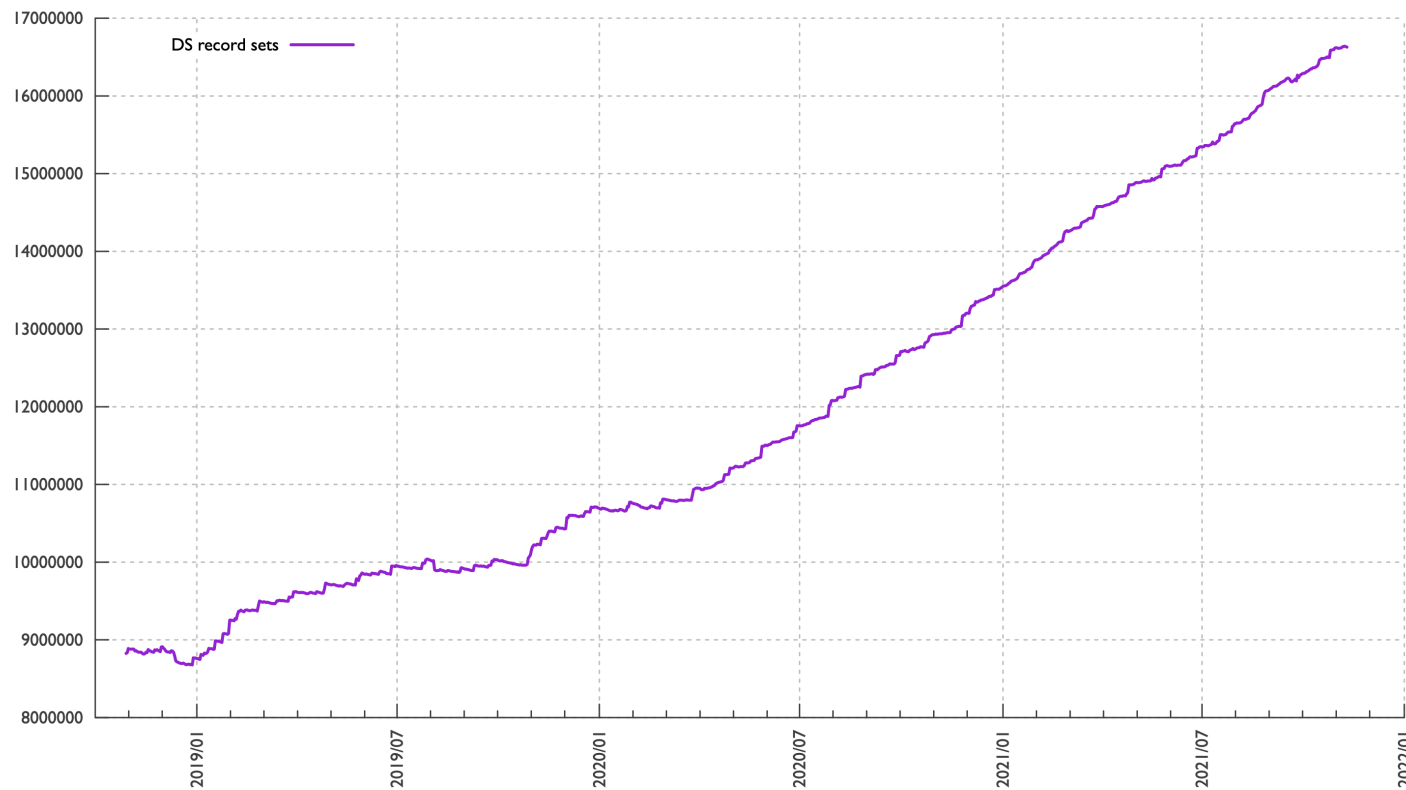
- DNSSEC (Domain Name System Security Extensions) provides integrity and authenticity of DNS messages
- More new Internet security protocols rely on DNS and DNSSEC
 - Emails: MTA Strict Transport Security (MTA-STS), DNS-based Authentication of Named Entities (DANE), Brand Indicator Message Identification (BIMI), and so on.
 - HTTPS: HTTPS records (HTTPSSVC, ESNL, and so on)

DNSSEC Deployment

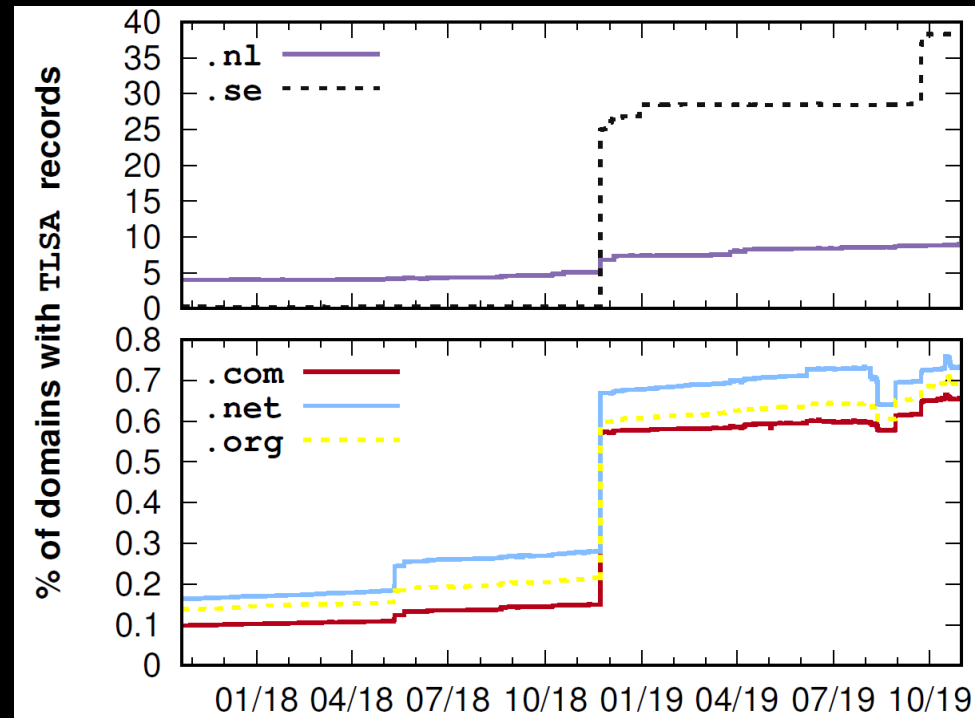


DNSSEC Deployment

The following graph shows the growth of observed DS record sets over time (i.e. the number of signed zones):

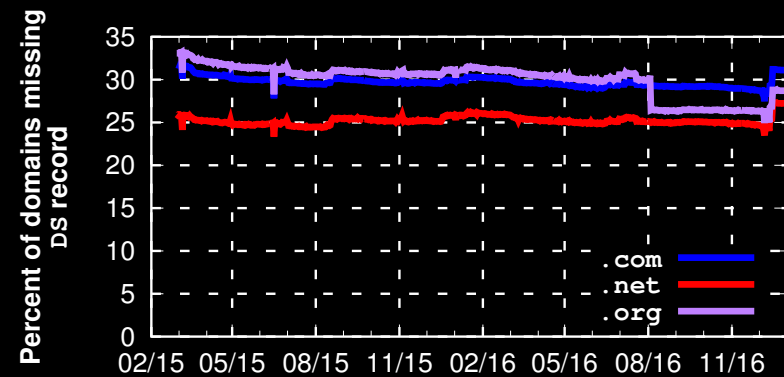
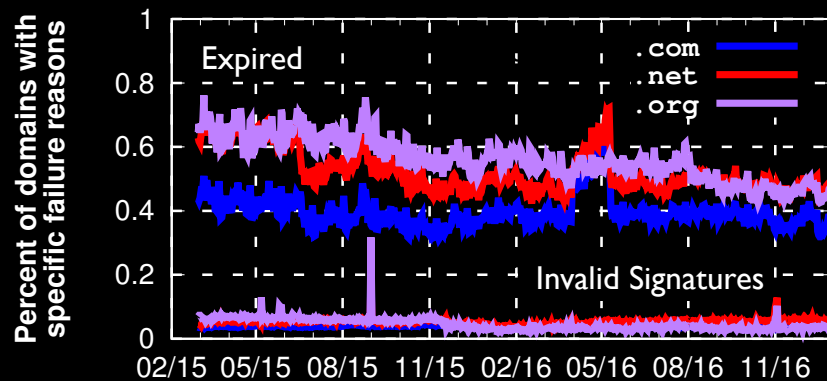


DANE Deployment



A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
[USENIX Security'20]

Server-side DNSSEC management



[dns-operations] slack.com bogus

Peter van Dijk peter.van.dijk@powerdns.com

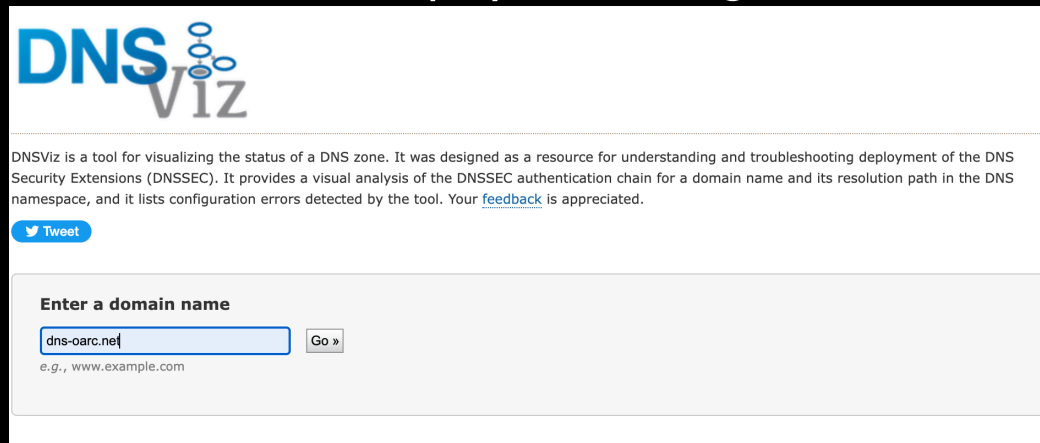
Thu Sep 30 18:00:33 UTC 2021

nsf.gov DNSSEC Outage: 2019-11-22 to 2019-11-23

Date: November 23, 2019

DNSViz

- <https://dnsviz.net/>
- A tool for visualizing the status of a DNS zone, built and maintained by Casey Deccio (Brigham Young University)
- DNSViz helps DNS administrators deploy and manage DNSSEC



The screenshot shows the DNSViz website interface. At the top is the logo "DNS Viz" with a stylized DNS hierarchy icon. Below the logo is a paragraph of text: "DNSViz is a tool for visualizing the status of a DNS zone. It was designed as a resource for understanding and troubleshooting deployment of the DNS Security Extensions (DNSSEC). It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool. Your [feedback](#) is appreciated." Below this text is a blue "Tweet" button. Further down is a section titled "Enter a domain name" containing a text input field with "dns-oarc.net" and a "Go »" button. Below the input field is a small example text: "e.g., www.example.com".

RRset status

Secure (6)

- dns-oarc.net/A
- dns-oarc.net/AAAA
- dns-oarc.net/MX
- dns-oarc.net/NS
- dns-oarc.net/SOA
- dns-oarc.net/TXT

DNSKEY/DS/NSEC status

Secure (8)

- ./DNSKEY (alg 8, id 14748)
- ./DNSKEY (alg 8, id 20326)
- dns-oarc.net/DNSKEY (alg 8, id 3701)
- dns-oarc.net/DNSKEY (alg 8, id 56266)
- dns-oarc.net/DS (alg 8, id 3701)
- net/DNSKEY (alg 8, id 35886)
- net/DNSKEY (alg 8, id 40649)
- net/DS (alg 8, id 35886)

Delegation status

Secure (2)

- . to net
- net to dns-oarc.net

Notices

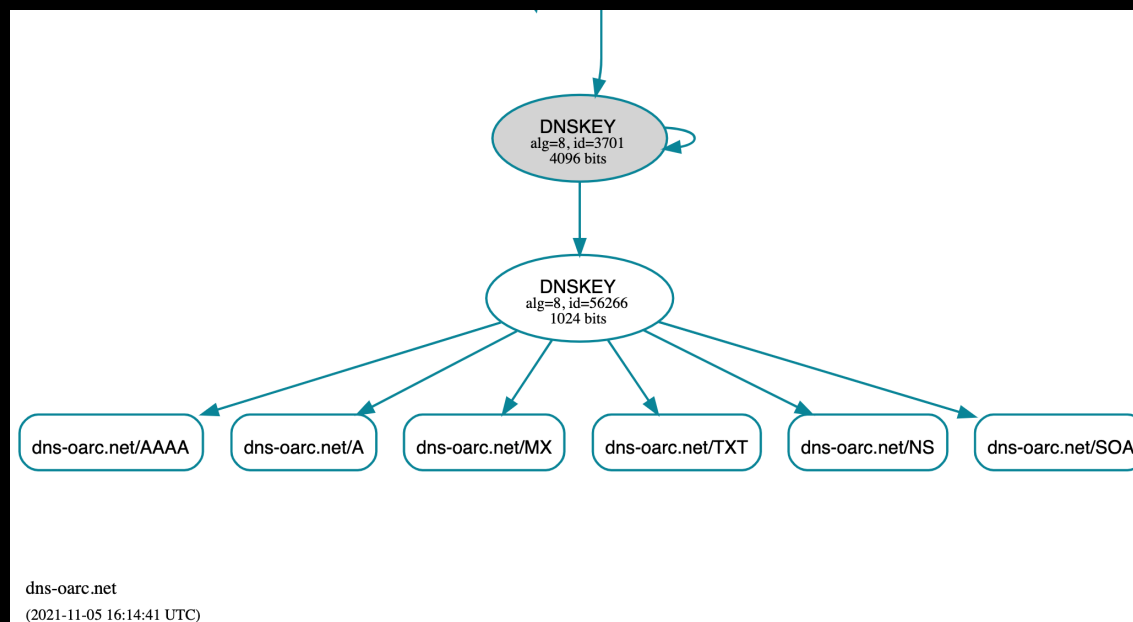
Warnings (2)

- net to dns-oarc.net: Authoritative AAAA records exist for udns1.ultradns.net, but there are no corresponding AAAA glue records.
- net to dns-oarc.net: Authoritative AAAA records exist for udns2.ultradns.net, but there are no corresponding AAAA glue records.

DNSKEY legend

[Full legend](#)

- SEP bit set
- Revoke bit set
- Trust anchor



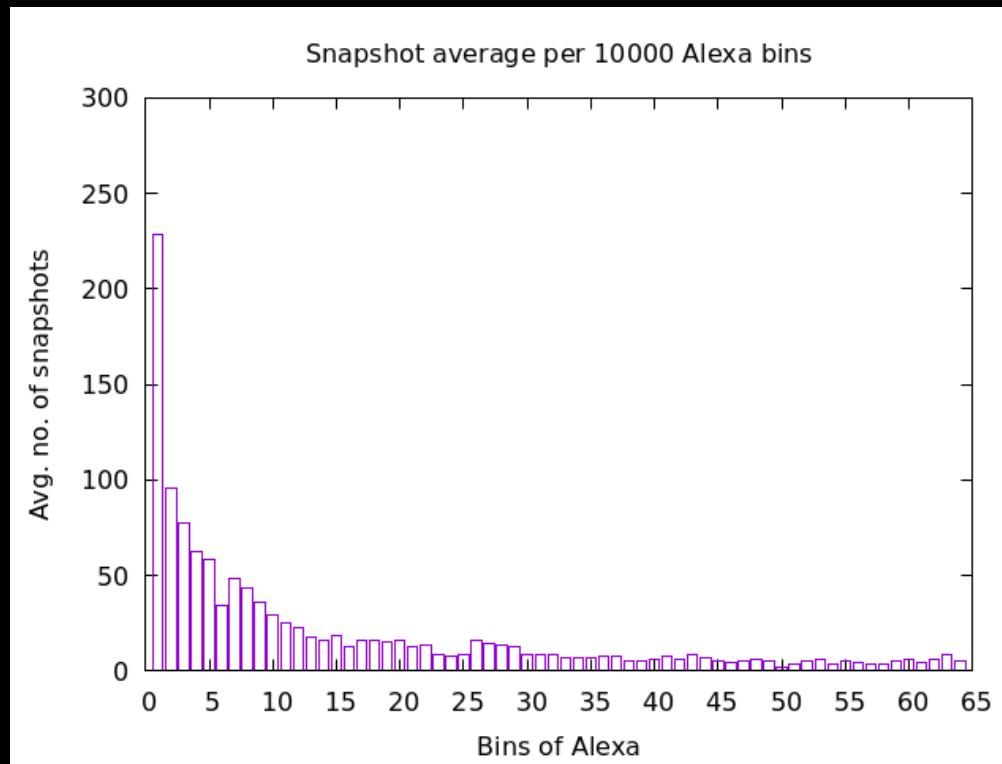
How's the DNSViz dataset looks like

	DNSViz Datasets
Scans Period	August 2014 ~ January 2021
# of domains	866,544
# of signed domains	251,098 (28.9%)
# of average analyses per domain	226

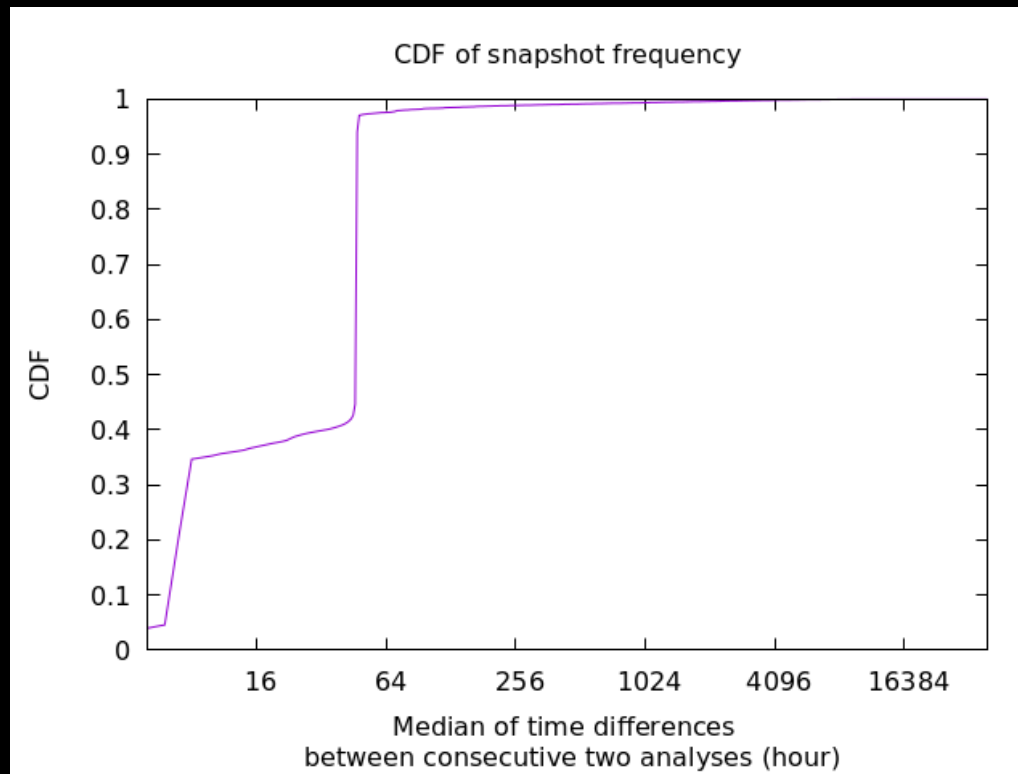
Research Goals

- Can we use DNSViz to understand the most challenging things for **DNS administrators** to deploy/manage DNSSEC?
- We are only interested in “DNSViz analyses” requested by **actual administrators**, but how?

Challenges (I) – Domain Name Popularity



Challenges (2) – DNSViz self-scan



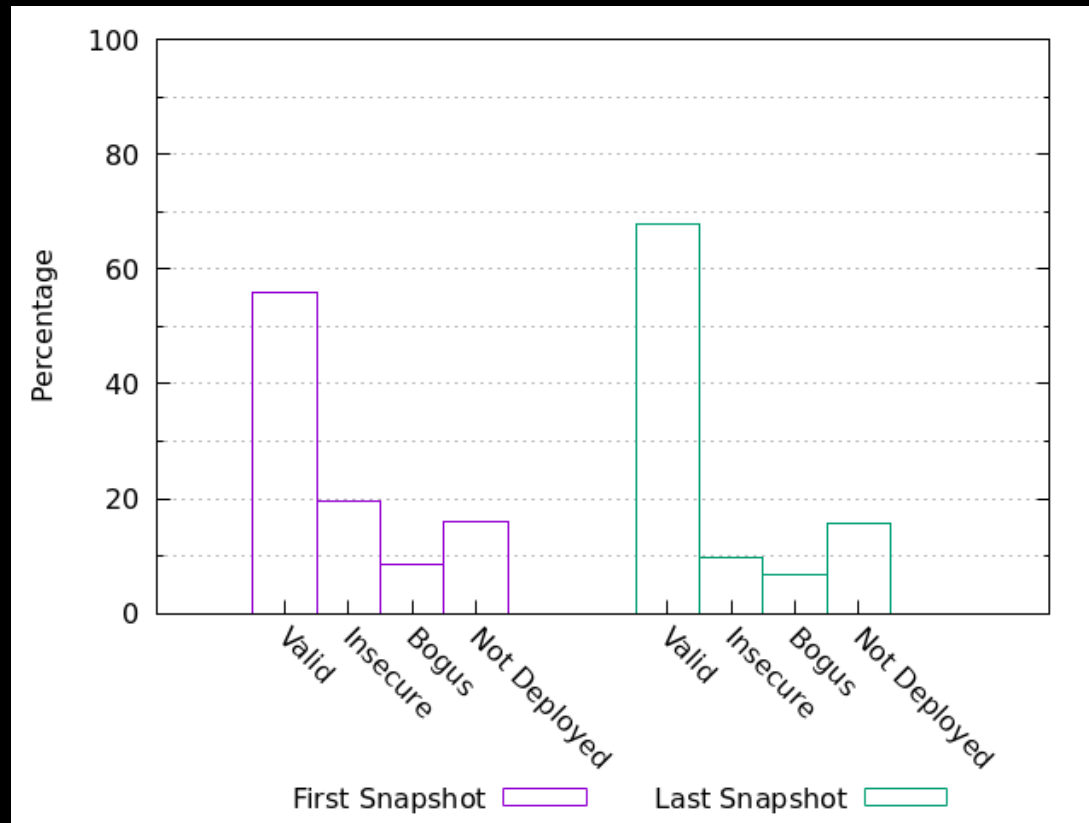
Obtaining Domains we are interested in

- Filter out the domains which have only snapshots taken every 48 hours, which are highly likely to be DNSViz scan
- Filter out popular domains (Alexa IM)

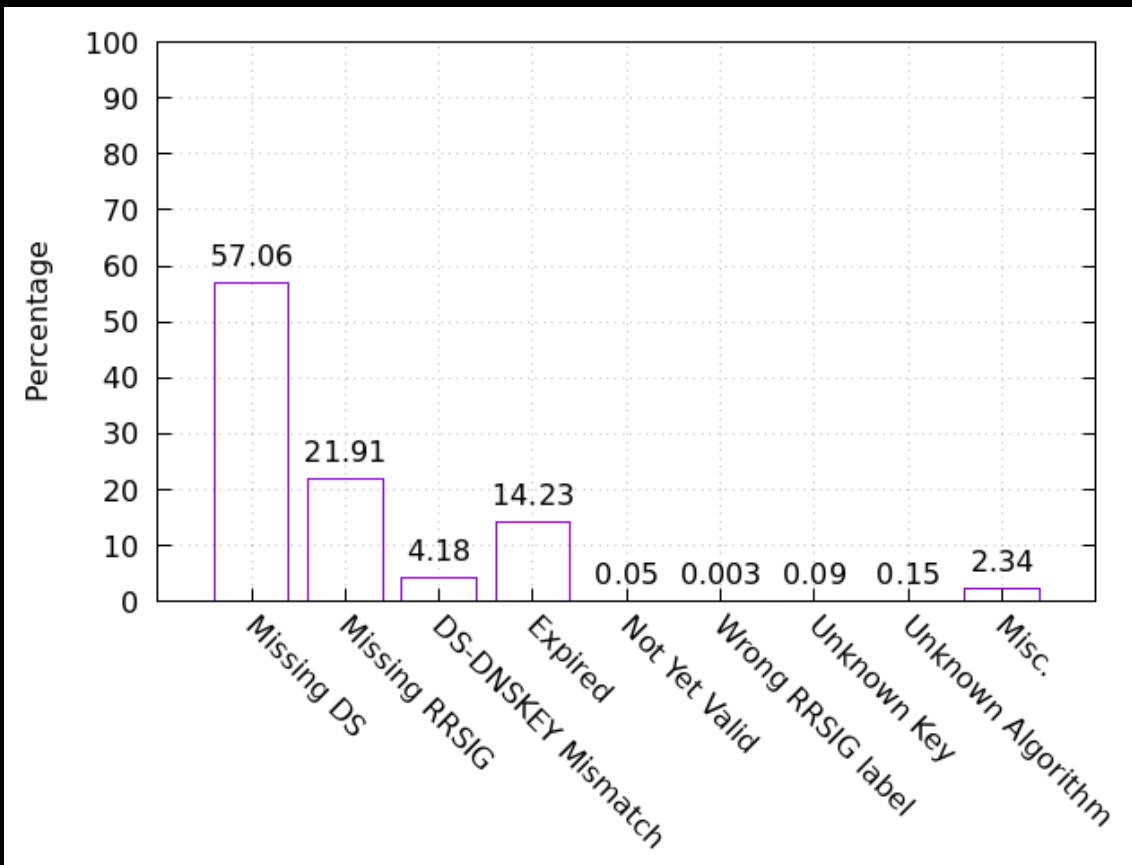
Domains (we are interested)

	DNSViz Datasets
# of domains	94,888
# of signed domains	80,376 (85%)
# of average analyses per domain	1,335
% of signed, but ever-bogus domains	26.94%
% of signed, but ever-unsigned domains	10.69%

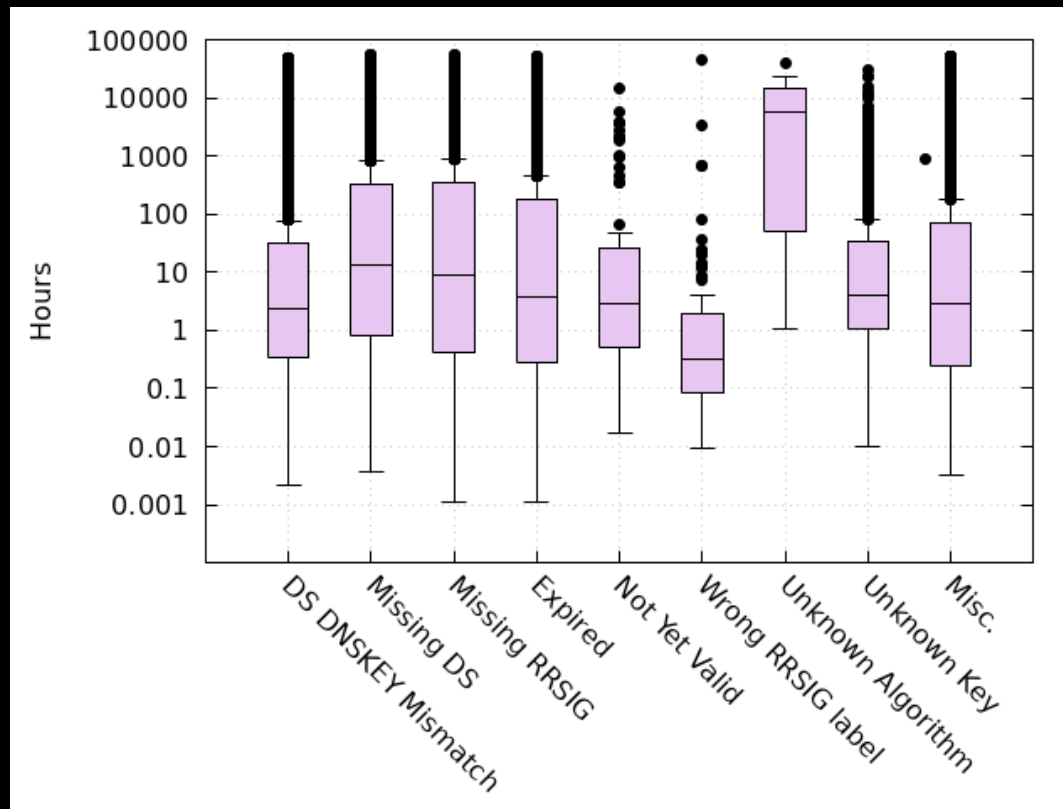
Is DNSViz helpful?



Most common errors



Time taken to fix?



Future steps

- Relationship between each error
 - One error may cause another
- Managing entity
 - Registrar, self-managing, third-party DNS operators?
- Suggestions/comments would be highly appreciated!

Questions