DNSSEC-related Outages

A measurement perspective

John Kristoff, Quan Minh Nguyen,
Steve Sheng, Eric Osterweil

Background

DNS w/o DNSSEC → errors and faults are common

~8% of names exhibit inconsistency [1]

Redundancy, timers, and retries mask problems

DNS w/ DNSSEC → less forgiving to problems

Errors and faults can completely disrupt availability

Authenticity demands better operational practices

DNSSEC Deployment Reality

Kaminsky's discovery drove deployment

- Most of the upper namespace is signed [2]
- Many big resolvers validate answers [3]

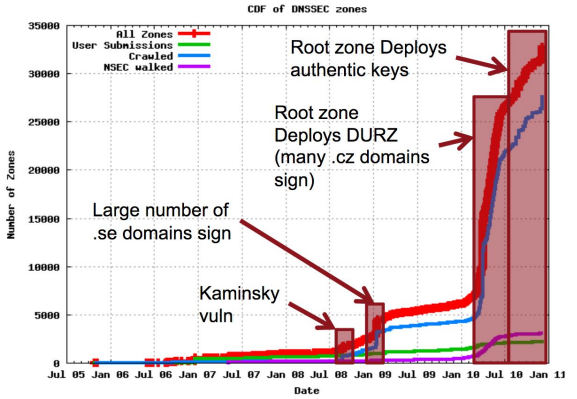


Figure from SecSpider http://secspider.cs.ucla.edu/

Limited end-to-end protection

- ~8-14% zones signed [4], but missing many big names
- Most zones not signed by default

Other Deployments in Perspective

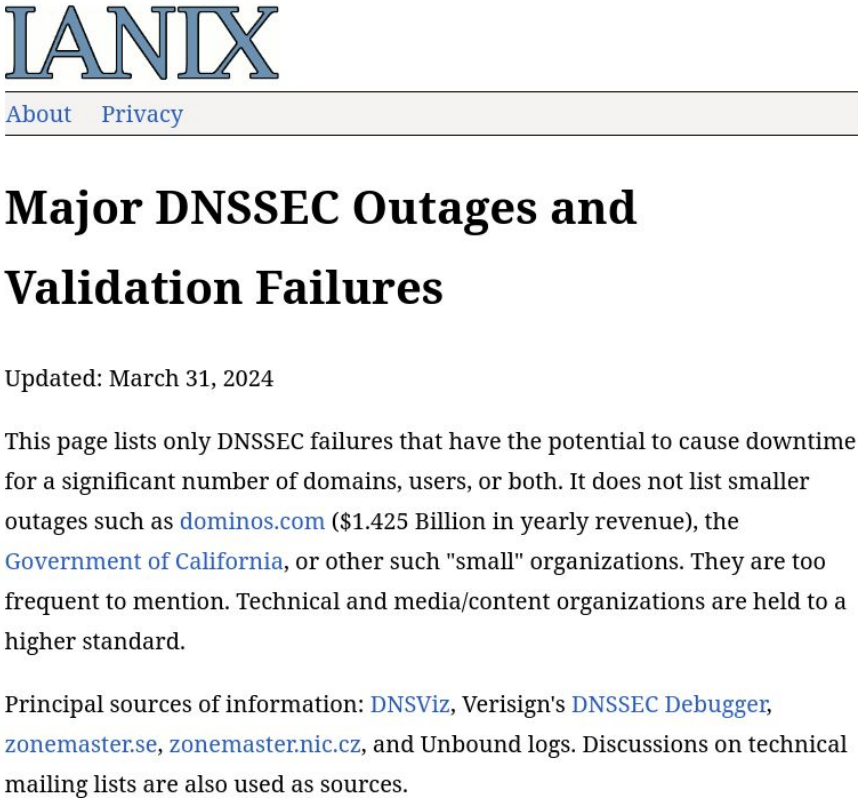
RPKI ROAs cover ~35% of IPv4 total addr space [5]

www x.509 cert usage is high, but validity rate is < 50% [6]

Less comparable, but mixed success:

IPv6, IP multicast, BCP 38, STARTTLS/DMARC/DKIM/SPF

Motivation [7]



IANIX

About Privacy

Major DNSSEC Outages and Validation Failures

Updated: March 31, 2024

This page lists only DNSSEC failures that have the potential to cause downtime for a significant number of domains, users, or both. It does not list smaller outages such as dominos.com ($1.425 Billion in yearly revenue), the Government of California, or other such "small" organizations. They are too frequent to mention. Technical and media/content organizations are held to a higher standard.

Principal sources of information: DNSViz, Verisign's DNSSEC Debugger, zonemaster.se, zonemaster.nic.cz, and Unbound logs. Discussions on technical mailing lists are also used as sources.

This seems like a good time for science

https://SecSpider.net has been active for ~20 years.

Let's use it to analyze outages.

Research Questions

Classification

Is there more than one type of DNSSEC-related outage?

Methodology

How are DNSSEC-related outages detected?

Results

Can we quantify DNSSEC-related outages and impact?

DNSSEC-related Outage Definition

When queries **would not have failed albeit for DNSSEC** enabled on the end-to-end resolution path.

Not just query response failures. e.g., offline signing faults

Not all outages are equal

Is 1/x NS RRs serving stale signatures an outage?

Is a lame delegation a DNSSEC-related outage?

Impact seems to matter. How do we measure it?

Current Scope

Longitudinal study of SecSpider active polling data

DNSKEY RRSIG **expirations**

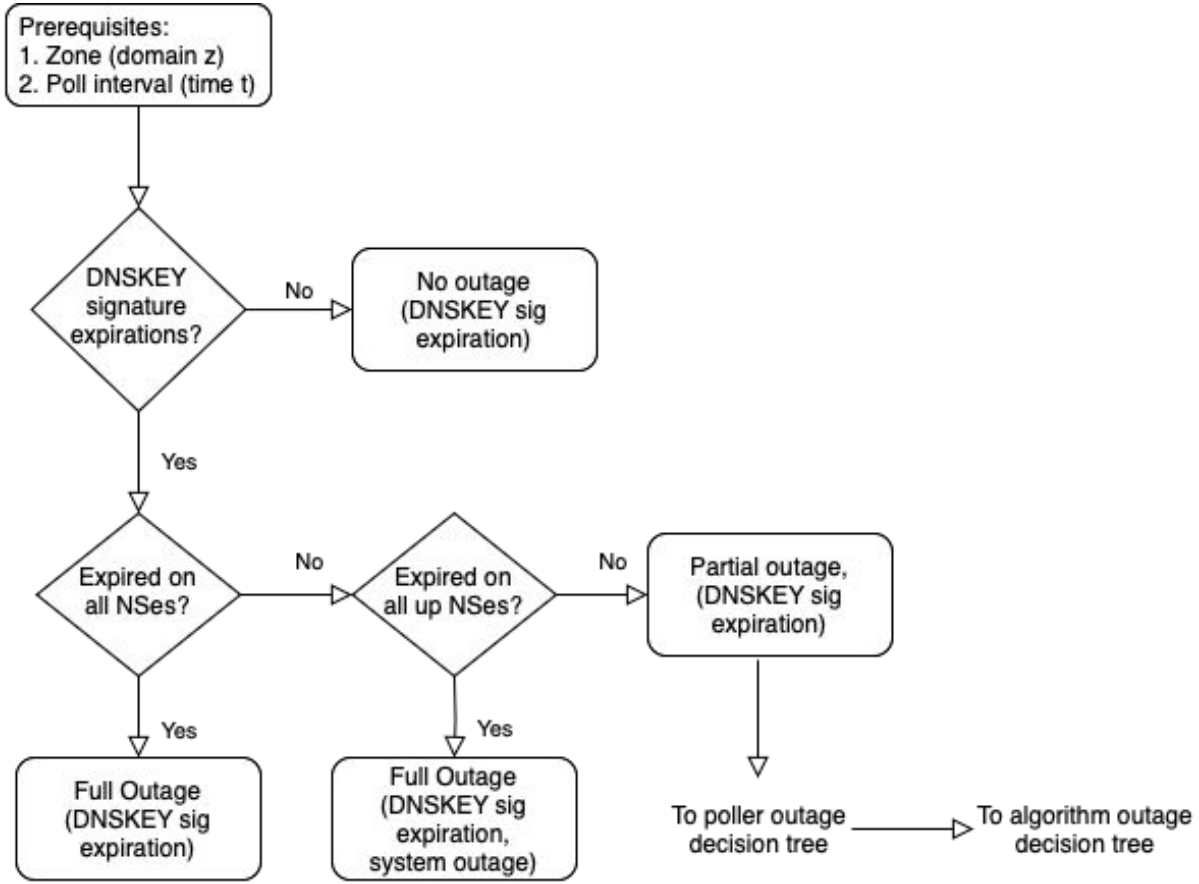
Decision Tree-driven analysis

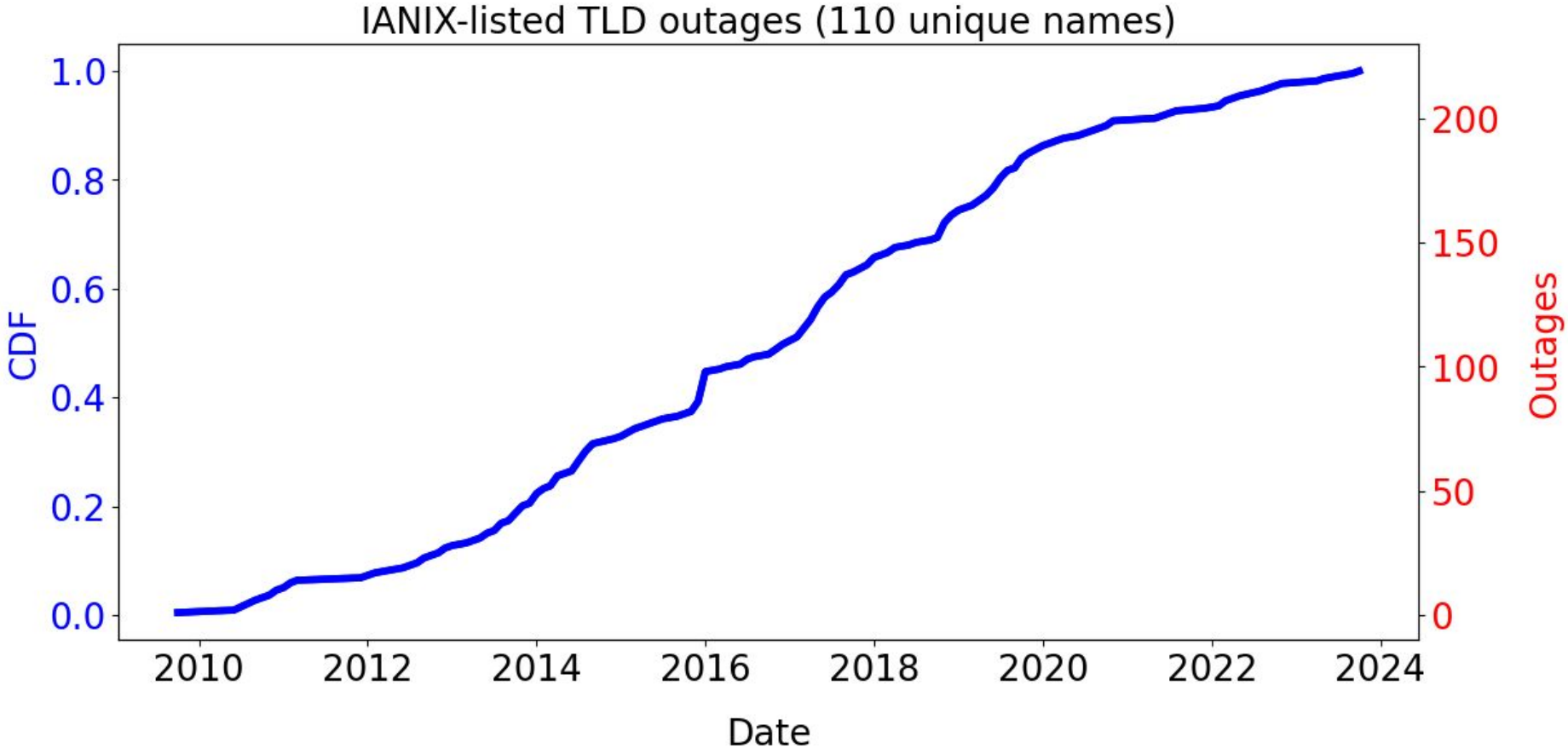
Classify outages by zone, NS RRs, pollers, and algorithms

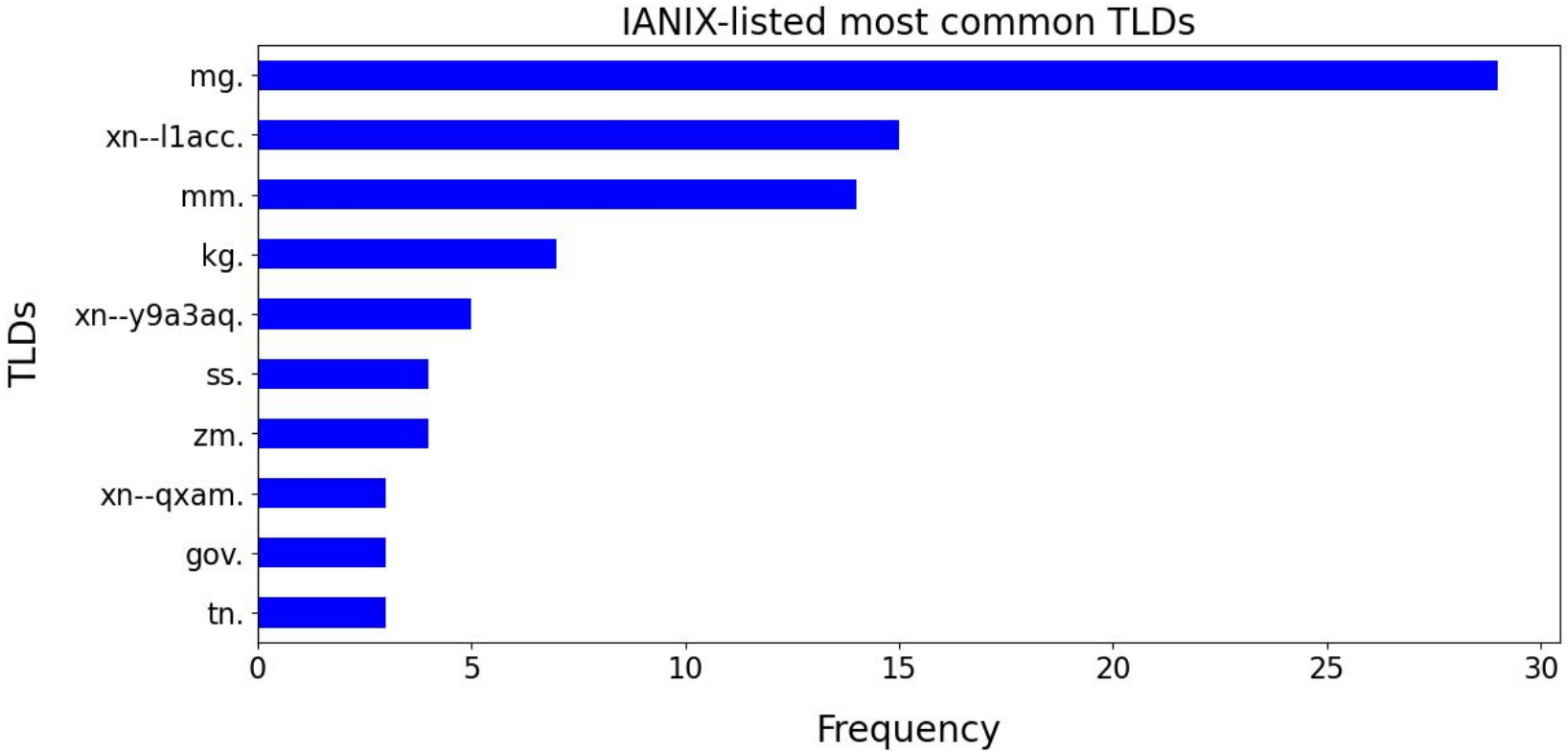
Methodology

DNSSEC Outage Decision Classifier

DNSKEY Expiration




IANIX-listed TLD outages (110 unique names)
CDF
Outages
Date
1.0
0.8
0.6
0.4
0.2
0.0
200
150
100
50
0
2010
2012
2014
2016
2018
2020
2022
2024


IANIX-listed most common TLDs
TLDs
mg.
xn--l1acc.
mm.
kg.
xn--y9a3aq.
ss.
zm.
xn--qxam.
gov.
tn.
0
5
10
15
20
25
30
Frequency

IANIX/SecSpider outage correlation (.mm)*

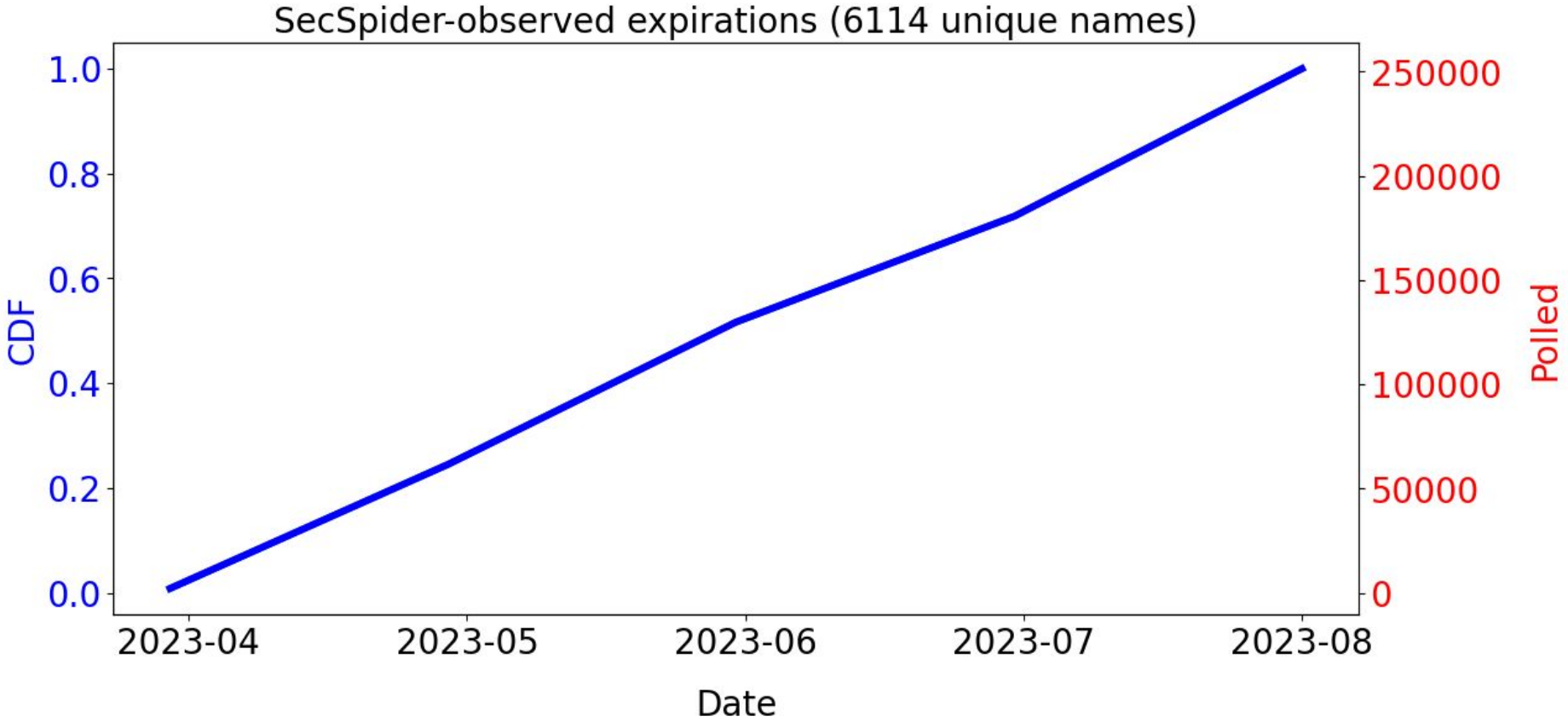
Seen at IANIX	Date	Seen at SecSpider
✅	2013-03-29	✅
✅	2014-07-30	
	2015-09-27	✅
✅	2015-09-29	✅
✅	2015-12-20	✅
	2015-12-24	✅
	2016-01-20 to 2016-02-01	✅
✅	2016-03-02	✅
✅	2018-11-05	✅

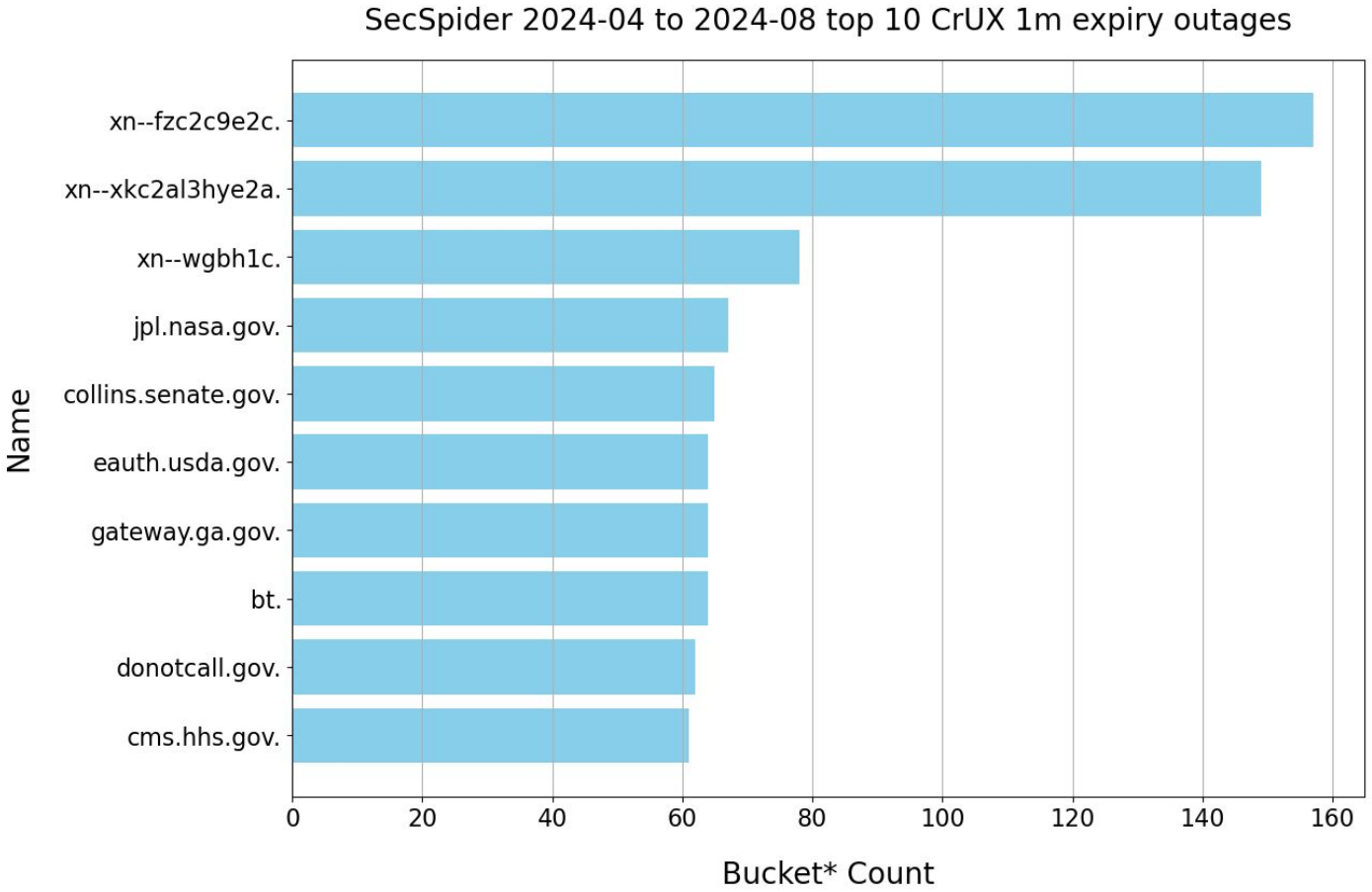
SecSpider Polling Resolution

Zones + NS RRs polled ~daily

We see a lot of what IANIX reports

- And often what it doesn't
- We miss some, but not much


SecSpider-observed expirations (6114 unique names)
CDF
1.0
0.8
0.6
0.4
0.2
0.0
Polled
250000
200000
150000
100000
50000
0
2023-04
2023-05
2023-06
2023-07
2023-08
Date


SecSpider 2024-04 to 2024-08 top 10 CrUX 1m expiry outages
Name
xn--fzc2c9e2c.
xn--xkc2al3hye2a.
xn--wgbh1c.
jpl.nasa.gov.
collins.senate.gov.
eauth.usda.gov.
gateway.ga.gov.
bt.
donotcall.gov.
cms.hhs.gov.
0
20
40
60
80
100
120
140
160
Bucket* Count

Impact Analysis

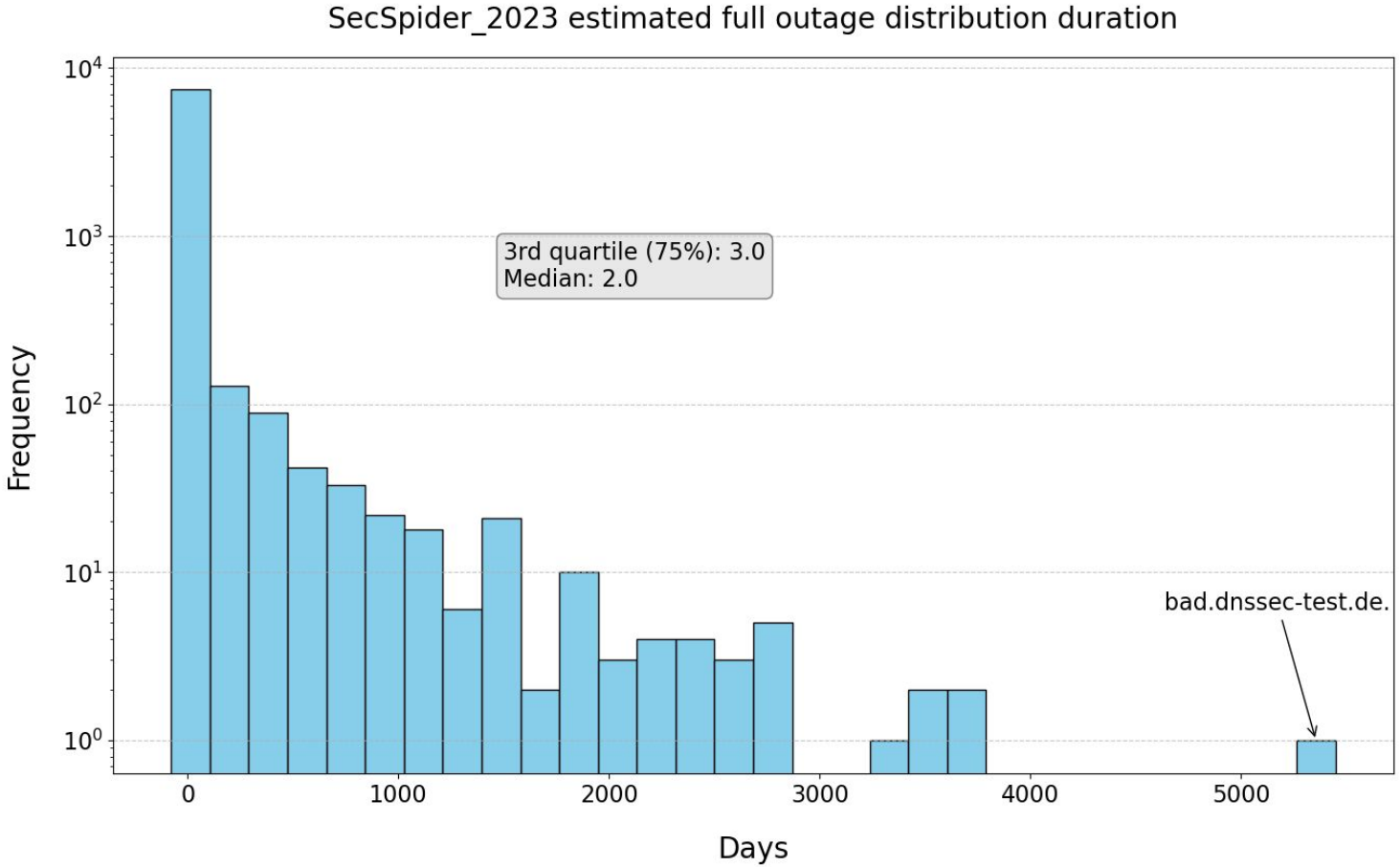
~2024-04 to ~2024-08 SecSpider expiry events:

In Chrome User Experience Report (CrUX) 1m list:

- 17 exact match names
- 63 CrUX parent zone matches
- 4 TLD matches

In Public Suffix List*

- 17 exact match names (mostly IDNs)


SecSpider_2023 estimated full outage distribution duration
Frequency
Days
3rd quartile (75%): 3.0
Median: 2.0
bad.dnssec-test.de.
10^4
10^3
10^2
10^1
10^0
0
1000
2000
3000
4000
5000

Partial outage example - donotcall.gov RRSIG RRset poll

NS_addr	rrset_lastseen	rrsig_inception	rrsig_expiry
205.251.196.159	**2023-07-01 02:37:22**	2023-06-30 15:00:00	**2023-07-01 02:00:00**
205.251.192.16	2023-07-01 02:37:50	2023-06-30 23:00:00	2023-07-01 10:00:00
205.251.199.194	2023-07-01 02:38:15	2023-06-30 23:00:00	2023-07-01 10:00:00
205.251.195.64	2023-07-01 02:39:07	2023-06-30 23:00:00	2023-07-01 10:00:00

Tentative Conclusions

SecSpider observes many outage-related events

Outage classification focuses efforts

Impact measurement to understand system performance

DNSSEC-related outages and impact may be exaggerated

- SecSpider monitors > 5 million names
- < 0.02% names had expiry event in secspider_2023

Future Work

Dependency impacts and MTBF/MTTR trends

Zone performance reports (overall availability vs. outage)

Other types of DNSSEC-related outages

BCPs and fragility-reduction ideas

Maybe we can infer short outages from RRsig time stamps

Academic publication with full results and measurements

Thank you, contact information

Contact: John Kristoff


jtk@dataplane.org


https://dataplane.org/jtk/


https://infosec.exchange/@jtk

References 1/2

[1] Sommese et al., “When parents and children disagree: Diving into DNS delegation inconsistency”, in Passive and Active Measurement (PAM), 2020.

[2] ICANN Identifier Health Indicator Technologies (IHIT), “M7 - DNSSEC Deployment”, https://ithi.research.icann.org/graph-m7.html, retrieved January 2025.

[3] APNIC Labs, “Use of DNSSEC Validation for the World (XA)”, https://stats.labs.apnic.net/dnssec/XA, retrieved January 2025.

[4] NIST, “Estimating IPv6 and DNSSEC Deployments SnapShots”, https://usgv6-deploymon.nist.gov/snap-all.html, retrieved January 2025.

References 2/2

[5] Job Snijders., “RPKI’s 2024 Year in Review”, https://mailarchive.ietf.org/arch/msg/sidrops/wI_PqEMsScRh1-jYl8XYPDI-3qE/, January 16, 2025.

[6] S. Farhan, et al., “Exploring the Evolution of TLS Certificates”, in Passive and Active Measurement (PAM), 2023.

[7] IANIX, “DNSSEC Downtime: List of Outages & Validation Failures”, https://ianix.com/pub/dnssec-outages.html, retrieved January, 2025.

Overflow

Data - measurement record (combined and simplified)

zone

poller

NS address

RR qtype

RRset lastseen timestamp

RRsig inception timestamp

RRsig expiration timestamp

algorithm

Methodology - bucket and sort data hourly

```
# Sort data by lastseen timestamp

bucket_id = 0
bucket_time = event[lastseen].min()

for event in data
    if event[lastseen] >= bucket_time + 1 hour
        bucket_id++
        bucket_time = event[lastseen]
    output(bucket_id, event)
```