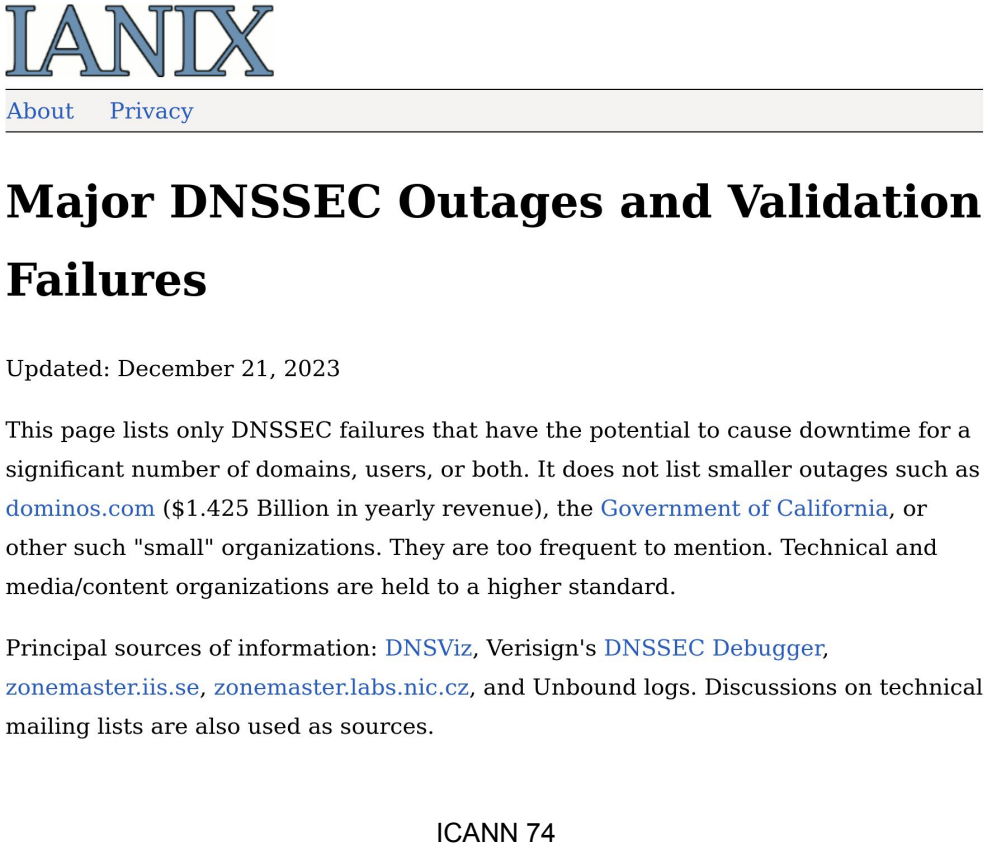
DNSSEC “event” measurement

John Kristoff, Steve Sheng, Eric Osterweil

Motivation



IANIX

About Privacy

Major DNSSEC Outages and Validation Failures

Updated: December 21, 2023

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.iis.se, zonemaster.labs.nic.cz, and Unbound logs. Discussions on technical mailing lists are also used as sources.

Research Questions

Classification

What is a DNSSEC-related outage?

Methodology

How are DNSSEC-related outages detected?

Results

Can we quantify DNSSEC-related outages and impact?

DNSSEC-related Outage Definition (in progress)

A DNSSEC-related outage exists when queries or system components **would not have failed albeit for DNSSEC** being enabled on the end-to-end DNS resolution and processing path.

Furthermore, DNSSEC-related outages are not just authentication failures, but can occur whenever any system or software component such as zone loading or offline signing results in resolution discrepancies.

Not all outages are equal

Is a single NS serving stale signatures an “outage”?

Probably just a partial outage

Is a lame delegation a DNSSEC-related outage?

Maybe, but might not have anything to do with DNSSEC

“Impact” seems to matter. How do we measure it?

Don’t parts of name space have varying tolerance?

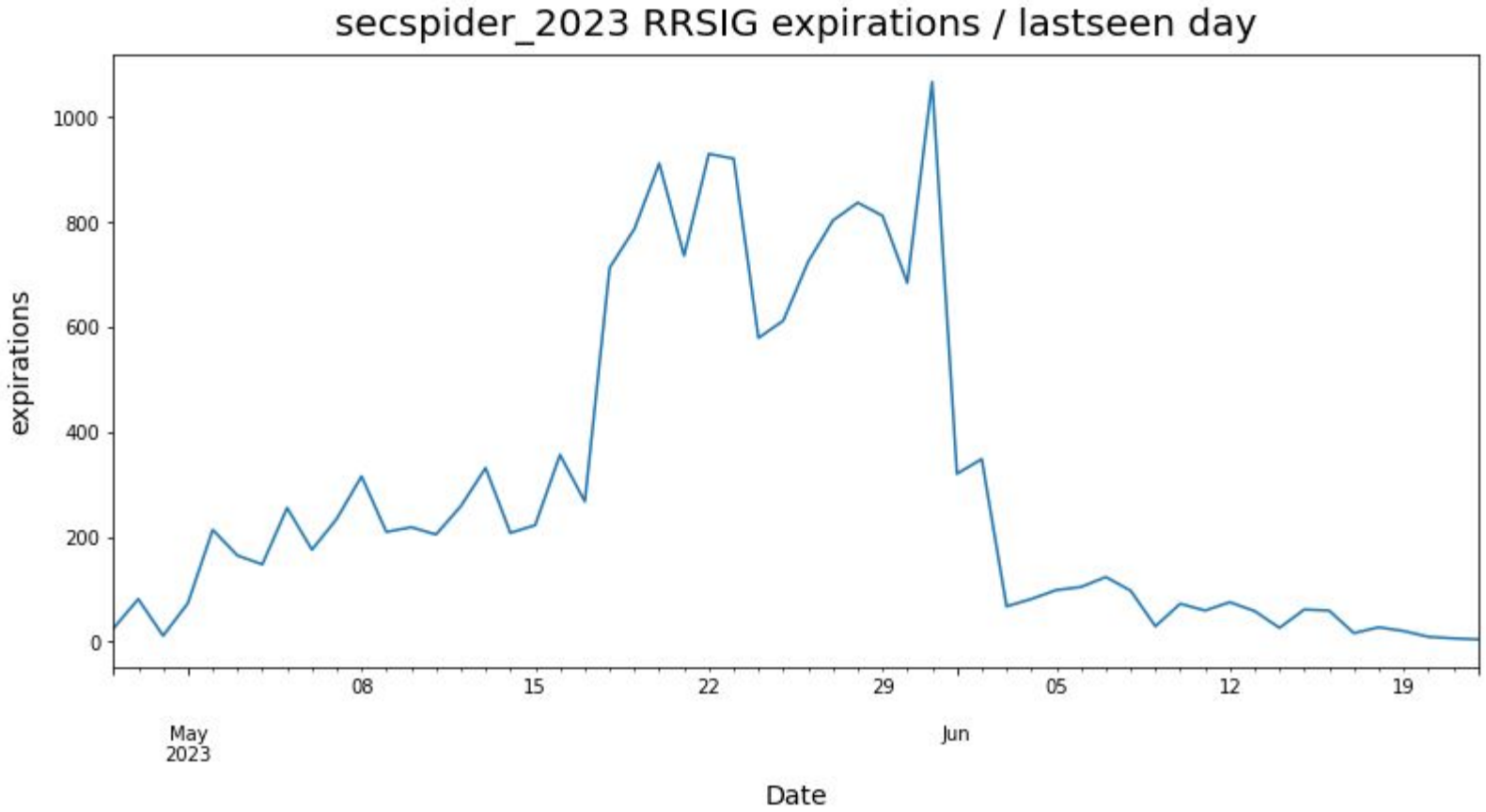
Do recovery mechanisms (e.g., retries) limit impact?

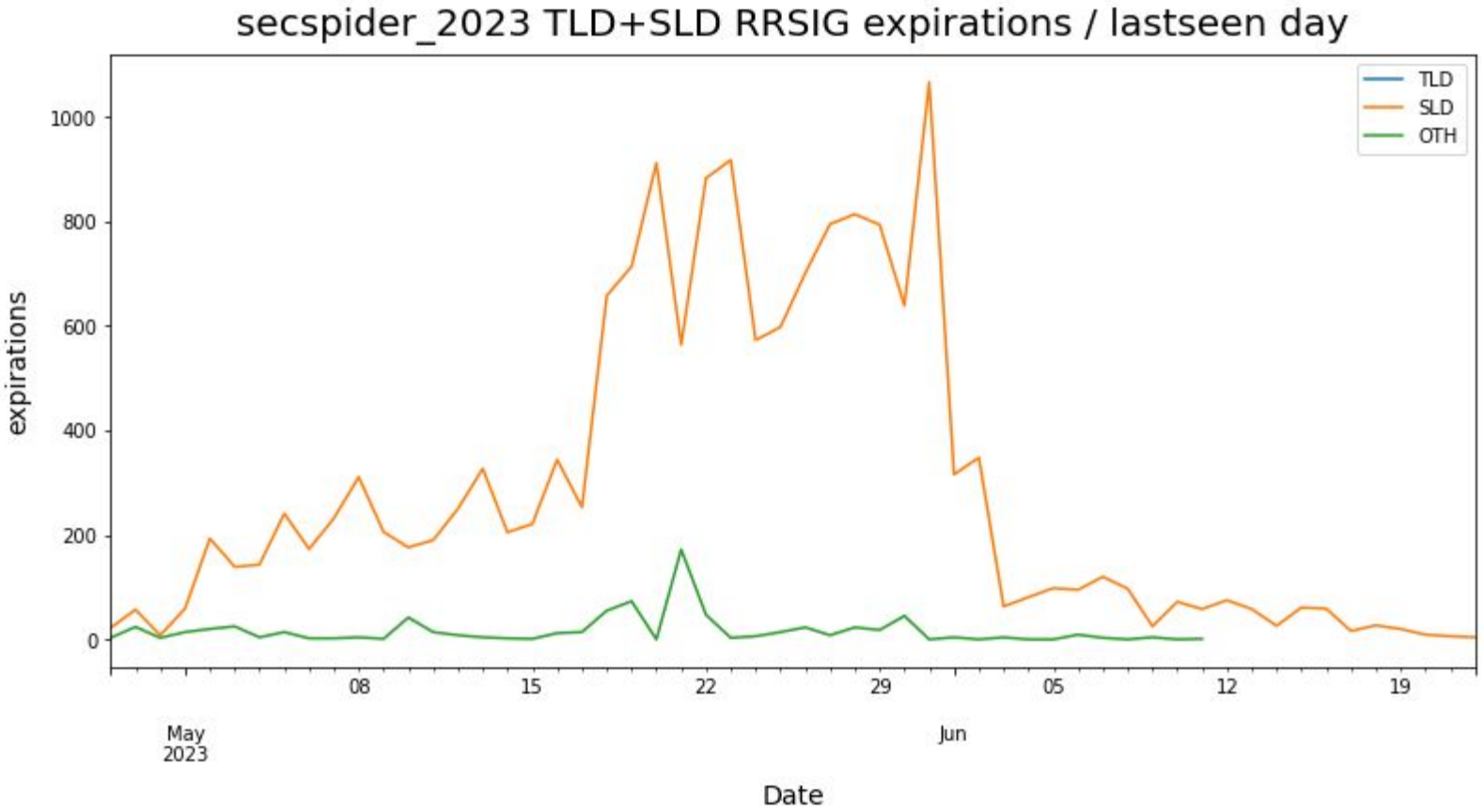
Methodology: start simple = RRSIG expirations*

SELECT [fields] FROM table[s] WHERE expiry < last_seen

output(name, type,
last_seen, first_seen, expiry,
RRSIG keytag,
poller,
NS RR responder,
)

* SecSpider for historical data measurement


secspider_2023 RRSIG expirations / lastseen day
expirations
1000
800
600
400
200
0
08
15
22
29
05
12
19
May
2023
Jun
Date


secspider_2023 TLD+SLD RRSIG expirations / lastseen day
TLD
SLD
OTH
expirations
1000
800
600
400
200
0
08
15
22
29
05
12
19
May
2023
Jun
Date

Top TLDs and second-level domains (SLDs)

TLD	count		SLD	count
com	7068		com.br	394
nl	1711		com.pl	87
se	1628		hemgtechnology.com	38
net	698		inf.br	22
org	556		elvis-frisor.no	19

Top NS RRs

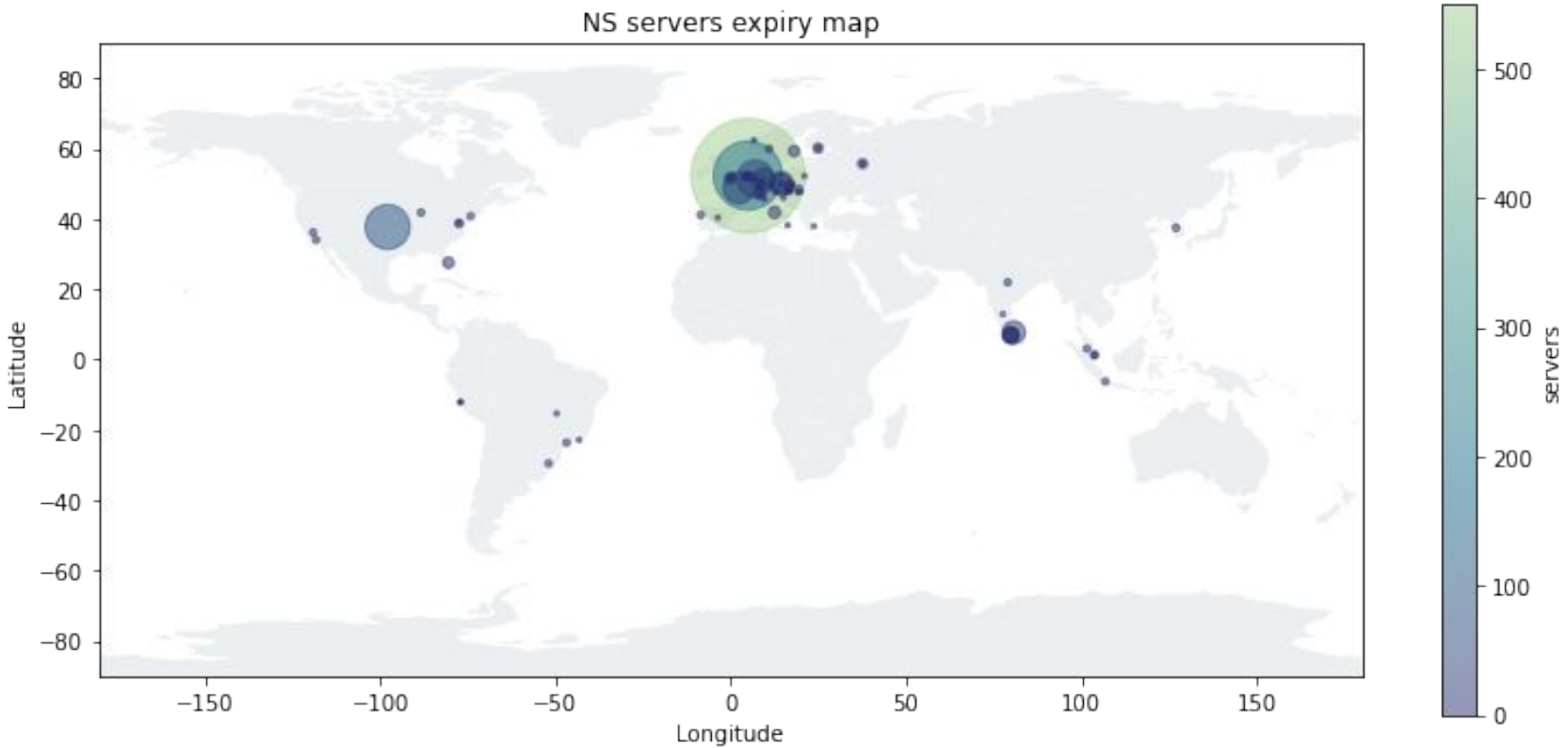
address	count	ptr
64.227.79.141	6976	ns3.savvii.com
62.221.192.231	1383	ns1.savvii.nl
62.221.197.30	1053	ns2.savvii.eu
185.104.28.19	247	ns1.zxcs.nl
78.47.104.13	240	ns.vas-hosting.com

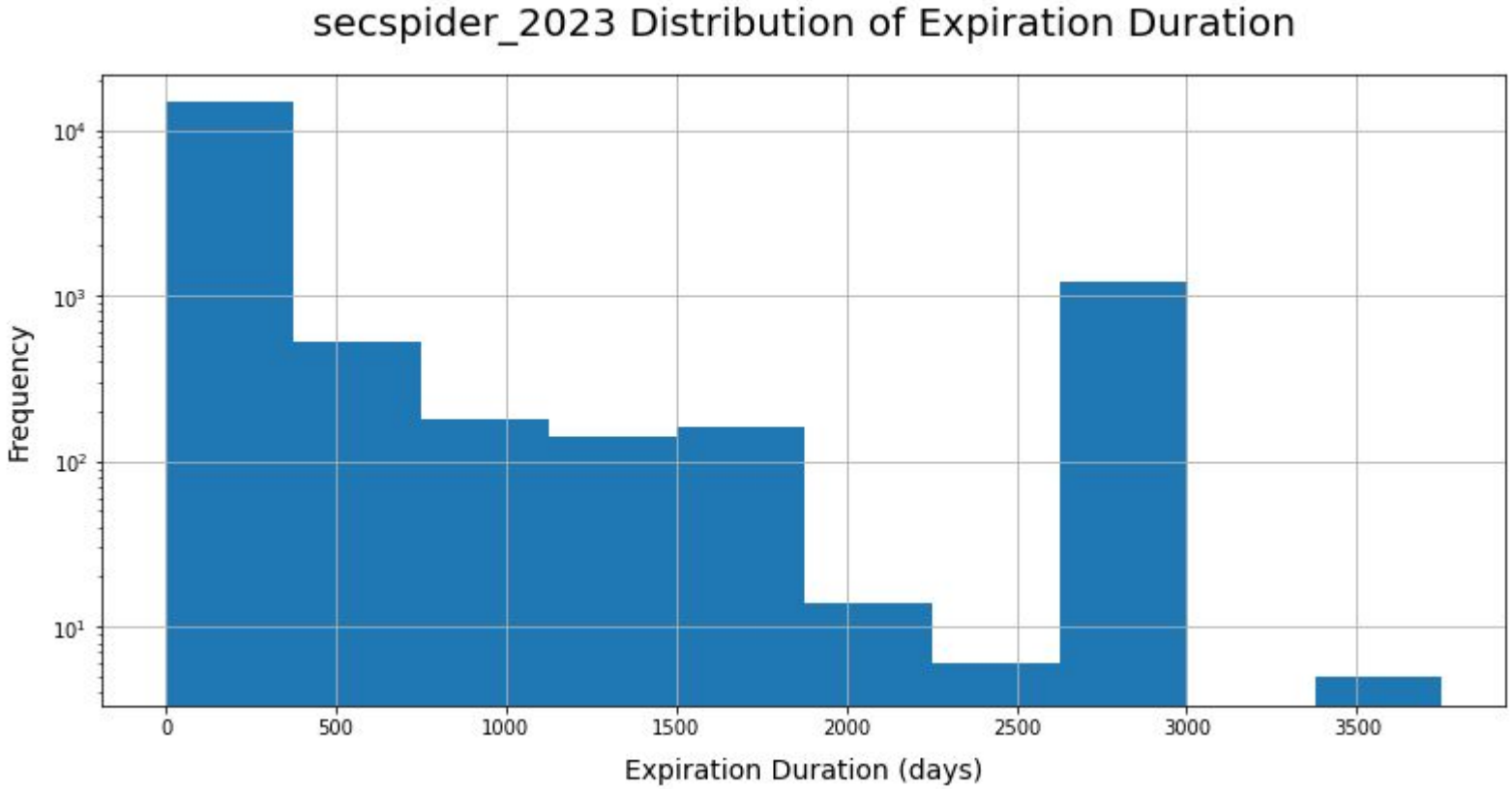
Top ASes (unique NS RRs)

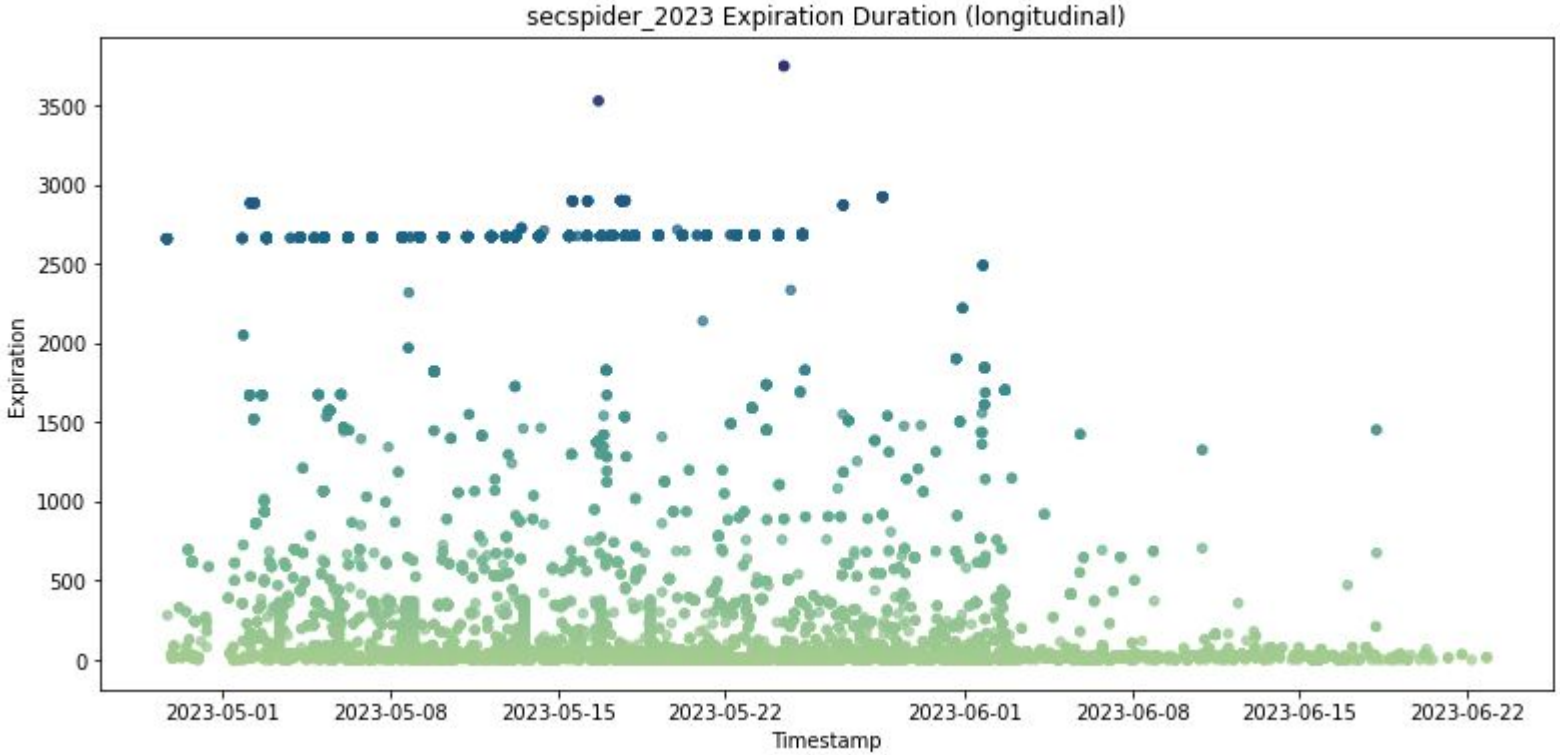
ASN	count	ASname
16509	423	AMAZON-02
16276	53	OVH OVH SAS
24940	31	HETZNER-AS Hetzner Online GmbH
31898	28	ORACLE-BMC-31898
14061	23	DIGITALOCEAN-ASN

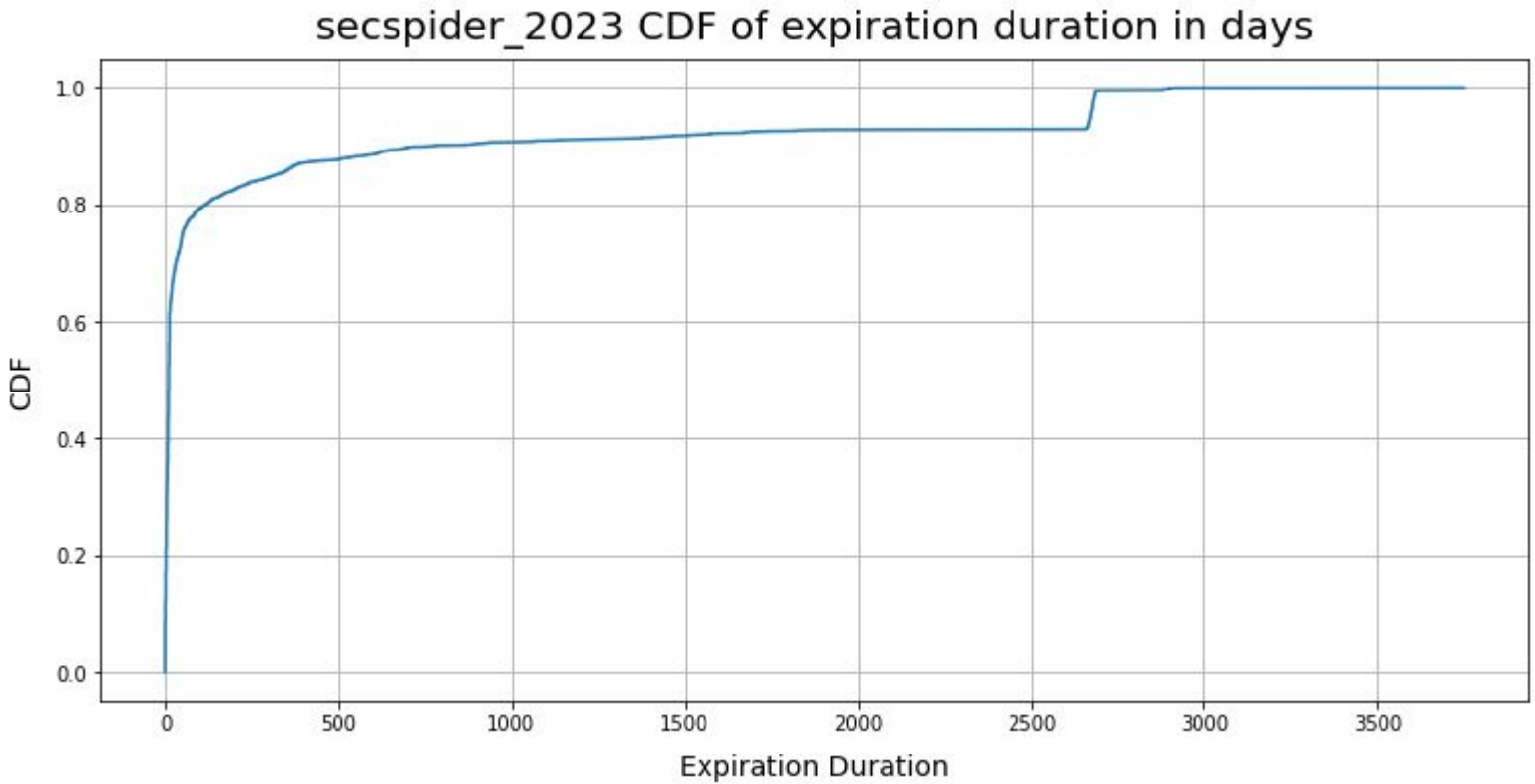
Top Countries (unique NS RRs)

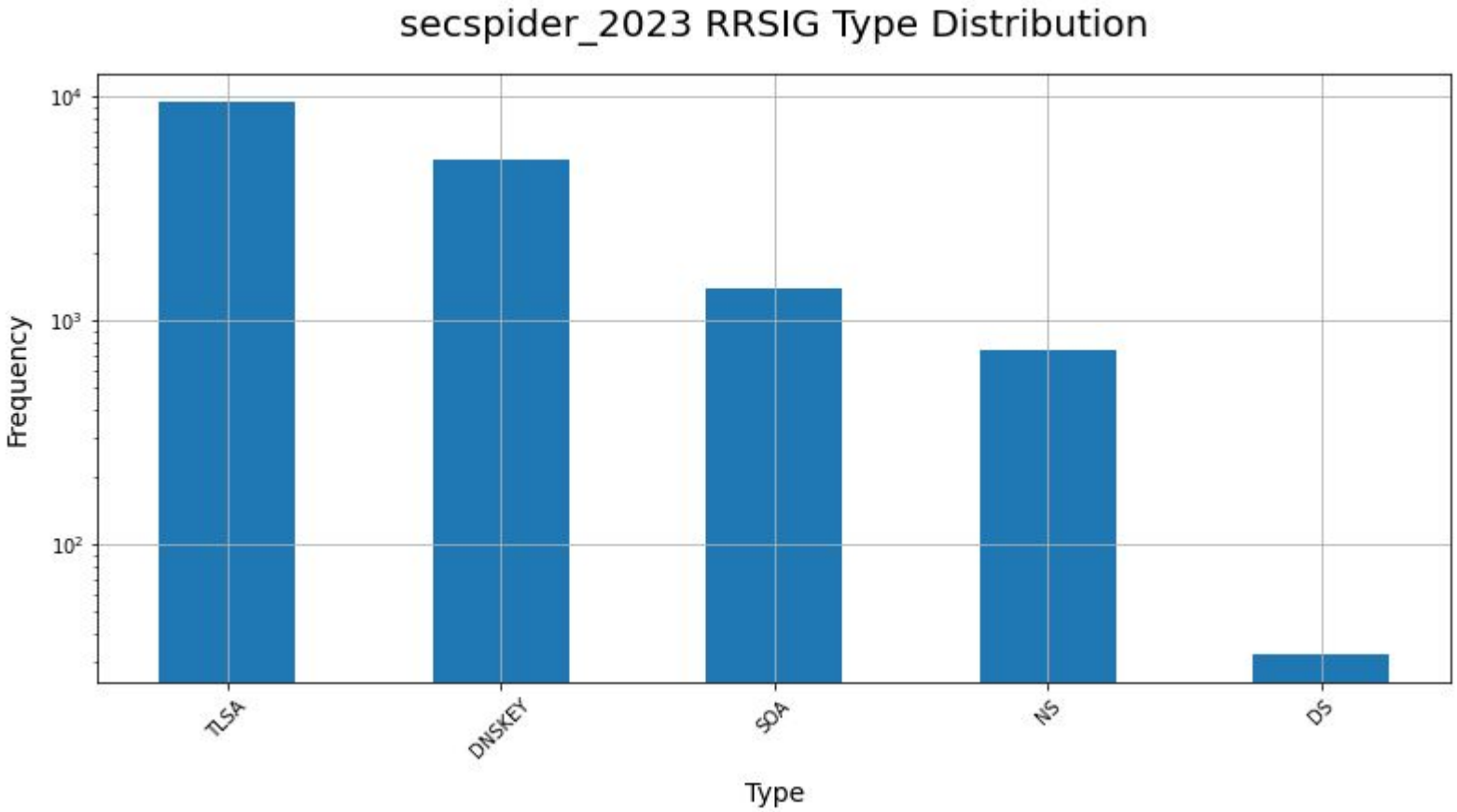
country	count
NL	763
US	101
DE	85
LK	52
CZ	48


NS servers expiry map
Latitude
Longitude
servers
80
60
40
20
0
−20
−40
−60
−80
−150
−100
−50
0
50
100
150
500
400
300
200
100
0


secspider_2023 Distribution of Expiration Duration
Frequency
10^4
10^3
10^2
10^1
0
500
1000
1500
2000
2500
3000
3500
Expiration Duration (days)


secspider_2023 Expiration Duration (longitudinal)
Expiration
3500
3000
2500
2000
1500
1000
500
0
2023-05-01
2023-05-08
2023-05-15
2023-05-22
2023-06-01
2023-06-08
2023-06-15
2023-06-22
Timestamp


secspider_2023 CDF of expiration duration in days
CDF
1.0
0.8
0.6
0.4
0.2
0.0
0
500
1000
1500
2000
2500
3000
3500
Expiration Duration


secspider_2023 RRSIG Type Distribution
Frequency
10^4
10^3
10^2
TLSA
DNSKEY
SOA
NS
DS
Type

More questions than answers. For now.

What is normal?

What events do we find that have gone unnoticed?

Do pollers exhibit unique local views?

We have literally just begun

Very, very rough look at some 2023 data

Aiming to produce proper results in ~2 months

Thank you, contact information

Contact: John Kristoff

jtk@dataplane.org

jkrist3@uic.edu

john.kristoff@icann.org

https://dataplane.org/jtk/

@infosec.exchange@jtk