DANE/SMTP Usage Report

Viktor Dukhovni
Two Sigma
<ietf-dane@dukhovni.org>

Wes Hardaker
USC/ISI
<hardaker@isi.edu>

Overview

1. Background
2. E-Mail Security without DANE
3. E-Mail Security with DANE
4. DNSSEC and DANE deployment statistics
5. Appendix

DANE SMTP Monitoring

https://stats.dnssec-tools.org

- https://stats.dnssec-tools.org/
  - Created by Viktor Dukhovni and Wes Hardaker
  - A continually updating web-page
- Recent changes:
  - New data sources added
  - More graphs added
    - DNSSEC growth
  - Tables are sortable (click on the column name)

DNSSEC / DANE Survey

(all work by Viktor Dukhovni)

- Monitors domains delegated from public suffixes
- Notifies operators of botched key/cert rotation
- Sourced from ICANN CZDS, Verisign, https://scans.io/, open access for .se, .nu, .fr, .nl, ... (more ccTLD data wanted), FarSight Security
- Covers ~200 million candidate domain names
- Captures DS, DNSKEY, MX, A, AAAA, TLSA records
- Captures certificate chains of MX hosts

Survey Stats

(as of 2019-06-20)

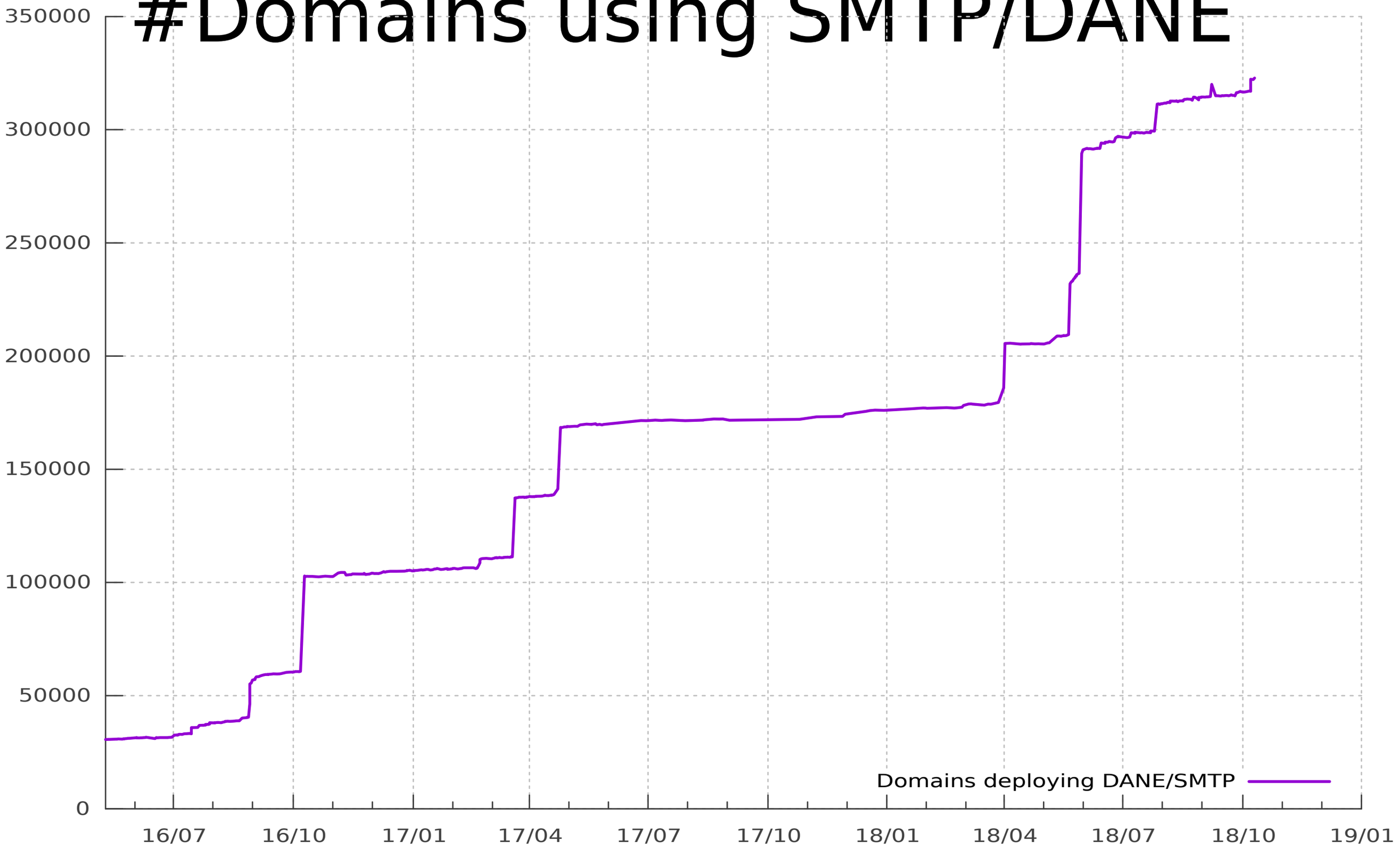
- 9.87 million domains with DNSSEC-validated MX
- **1.18 million** domains with DANE-enabled SMTP
  - (was only 300 thousand in Barcelona!!!)
- Millions of users (gmx.de, web.de, comcast.net)
- DANE-enabled MX servers in 4468 zones

DANE/DNSSEC Deployment Awards

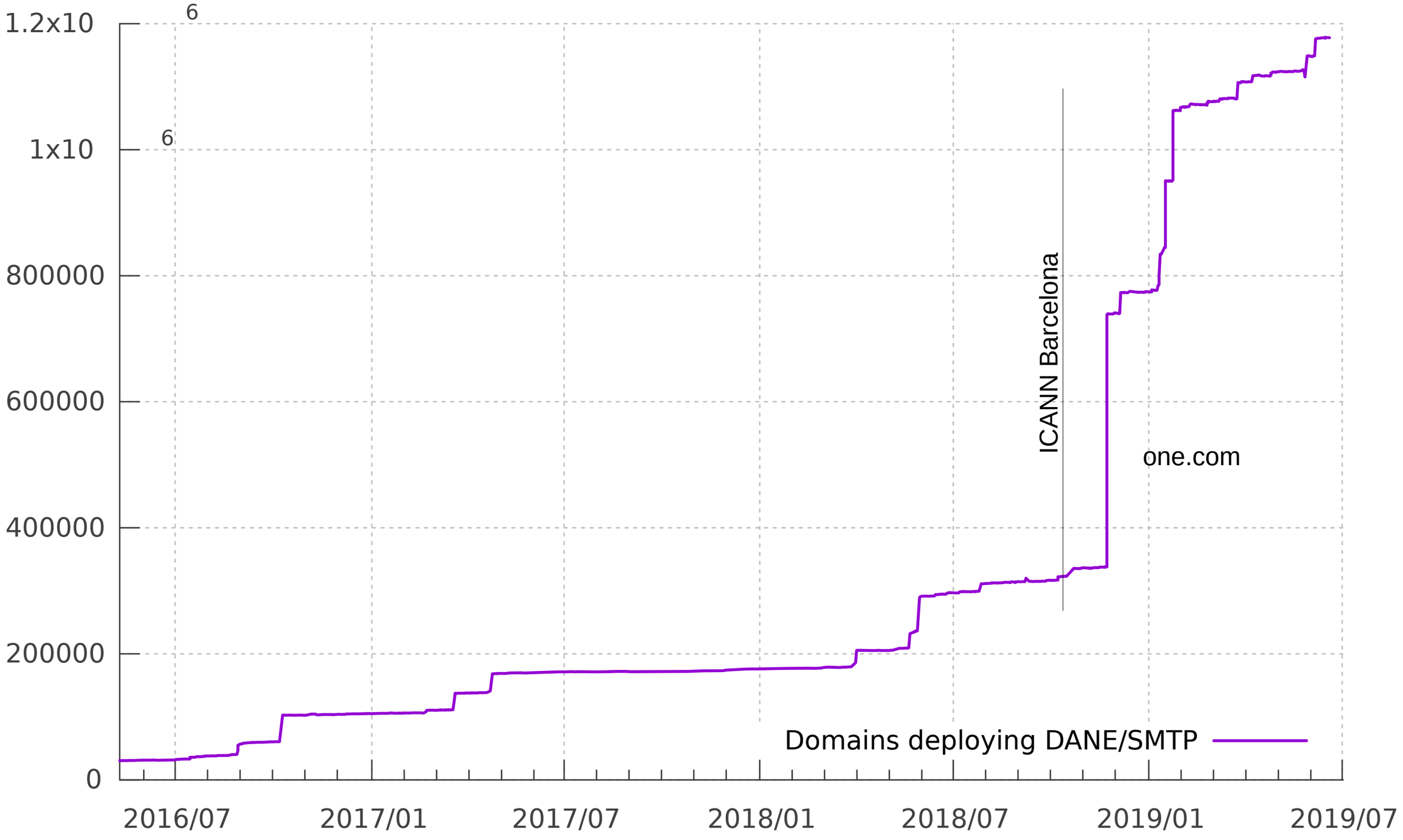
- Best improvement
  - .bank 58.10% → 98.48% DNSSEC problem free!
- Best DANE deployment
  - one.com published 707k DANE/TLSA records
- TLDs with 100% working DNSKEY records
  - .boston
  - .bible
- Large-volume TLD working DNSKEY records
  - .br → 99.6% working
  - Via active monitoring

From LAST TIME

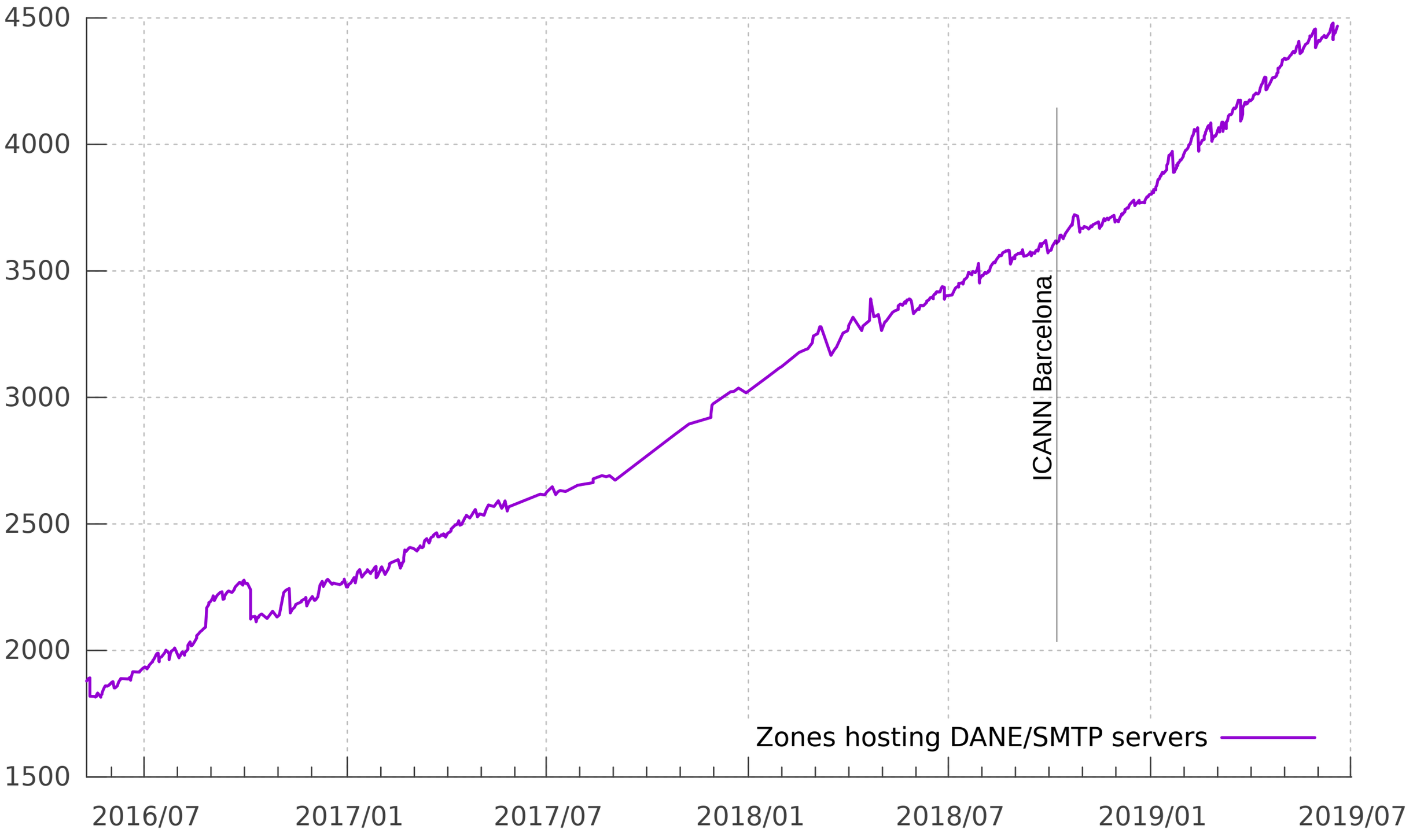
#Domains using SMTP/DANE



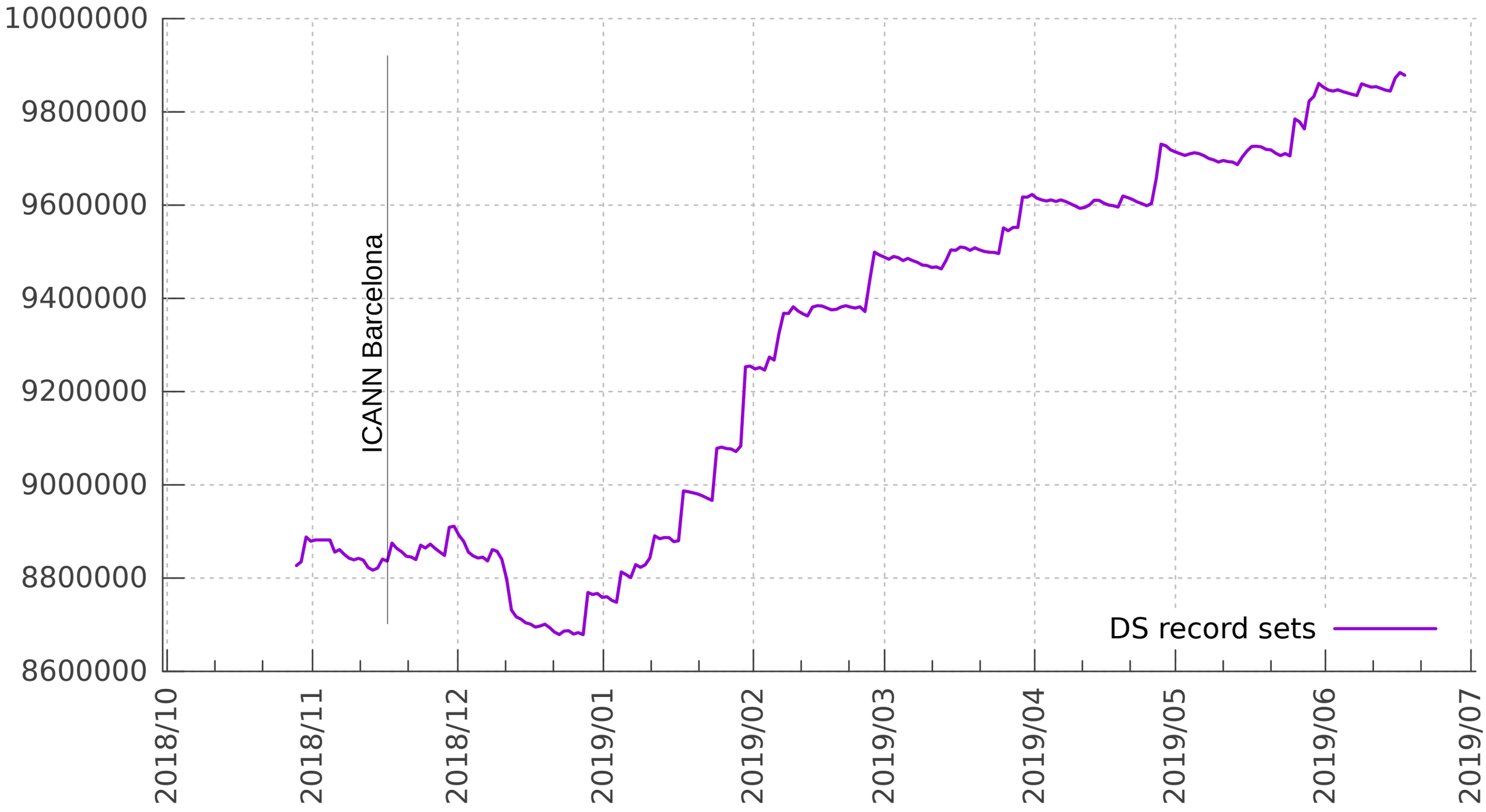
#Domains using SMTP/DANE



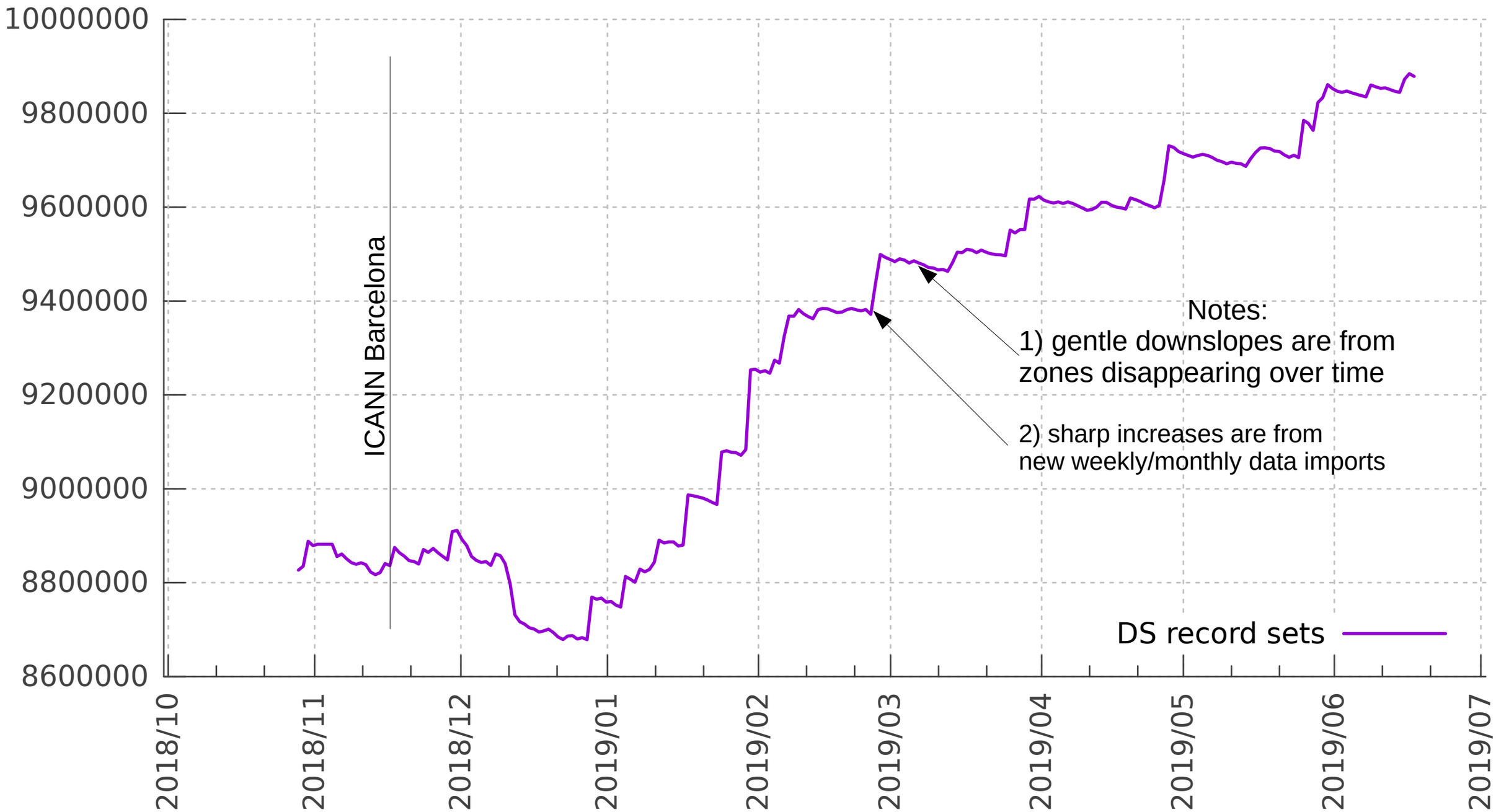
#Zones of DANE MX hosts



#Zones with DS Records



#Zones with DS Records



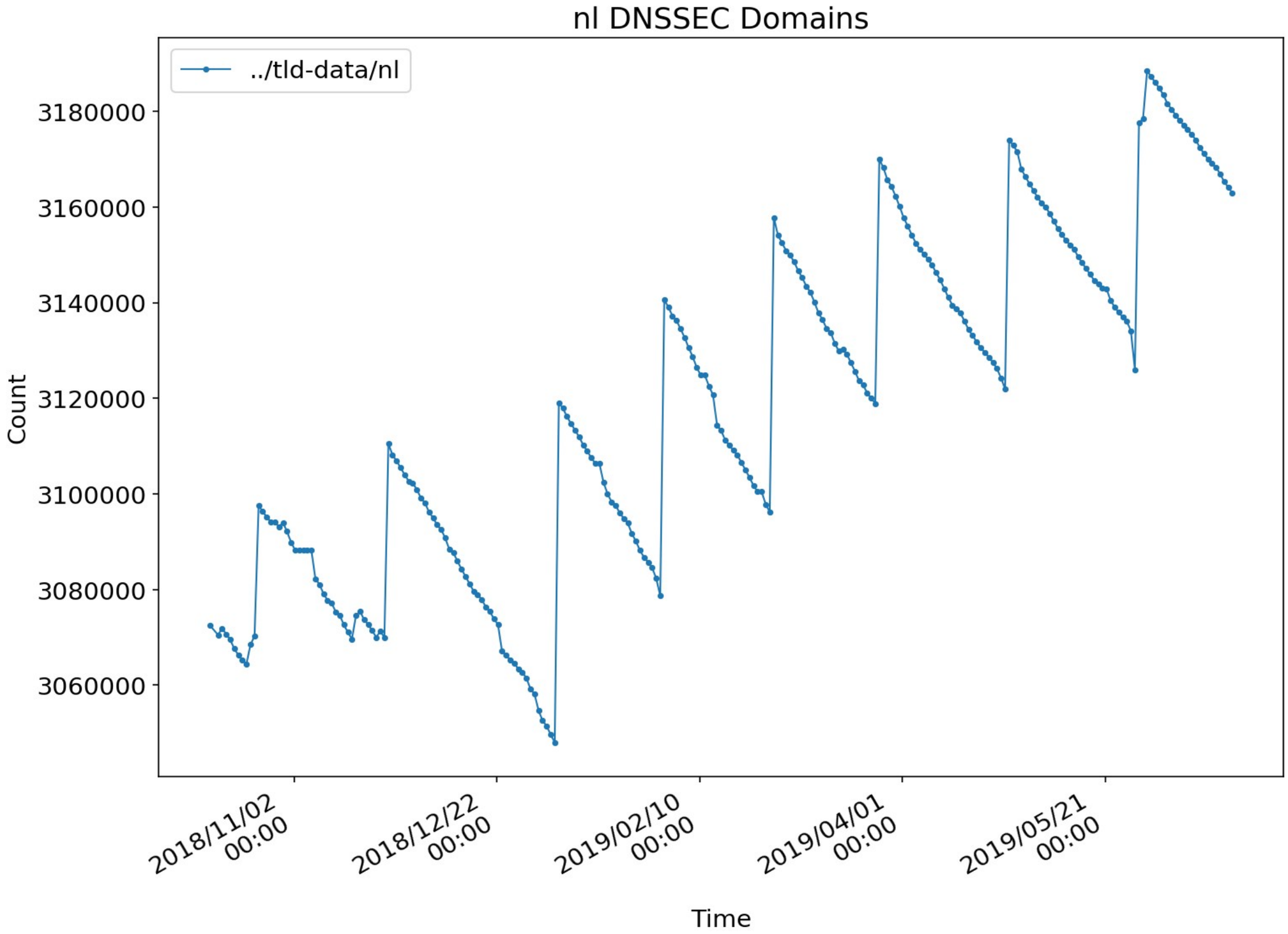
Noteworthy new SMTP/DANE providers

Provider	Deployed SMTP/DANE Records	Initial Date
one.com	706,991	2018-11-23
web4u.cz	27,341	2019-05-30
flexfilter.nl	15,759	2019-03-26
onebit.cz	12,994	2019-01-16
zxcs.nl	12,311	2019-04-09
netzone.ch	6,007	2019-03-26
ips.nl	3,760	2019-03-09

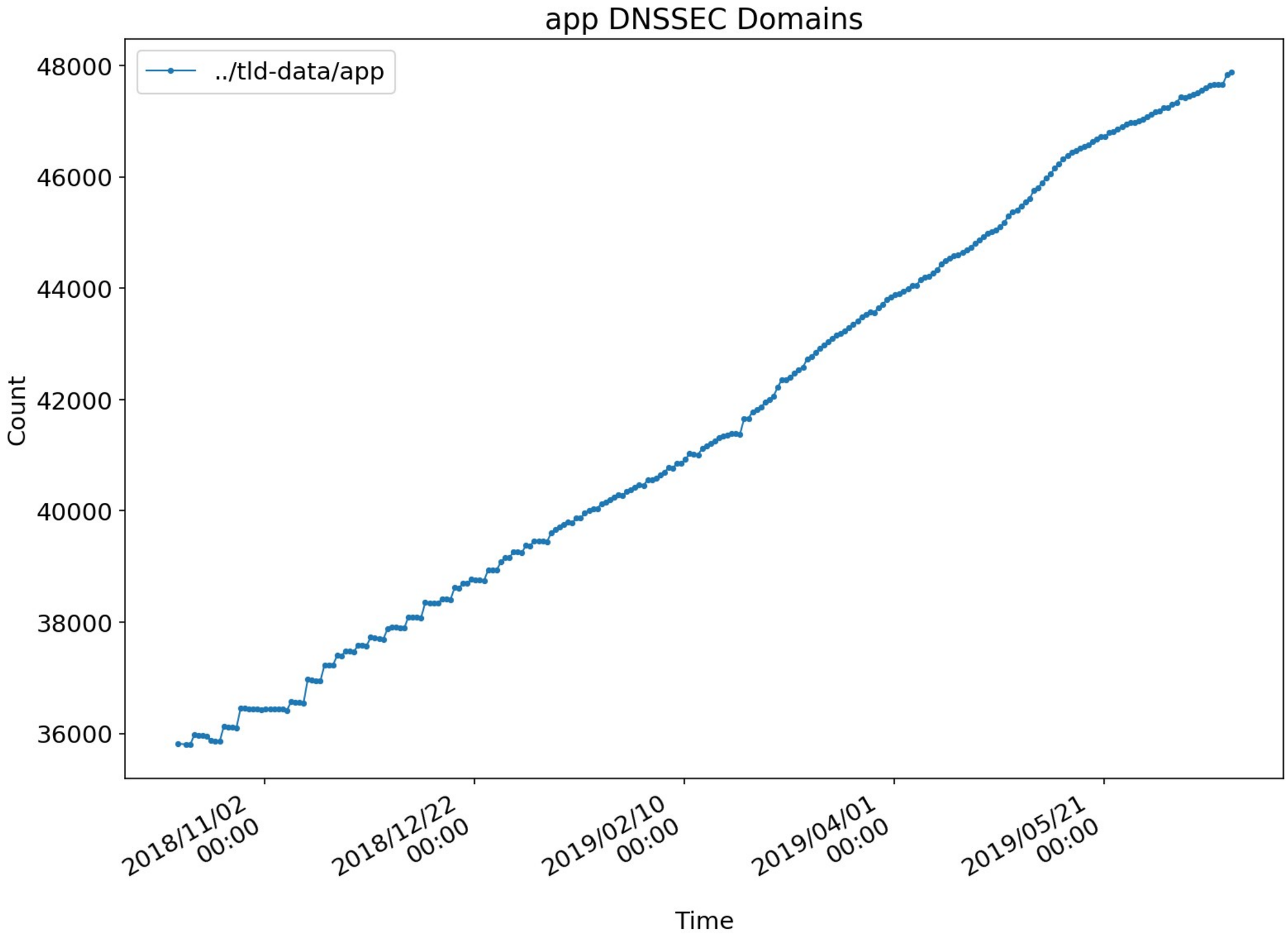
Top DNSSEC TLDs

DNSSEC domains x1000		TLD	
3,144		NL	
1,205		COM	
764		SE	
698		CZ	
560		BR	(potentially low; .br says its higher)
492		EU	
450		PL	
408		FR	
382		NO	
286		BE	
152		NET	
123		HU ↑1	(since Barcellona)
111		ORG ↑1	
109		NU ↕2	
87		CH ↑	
500		other	

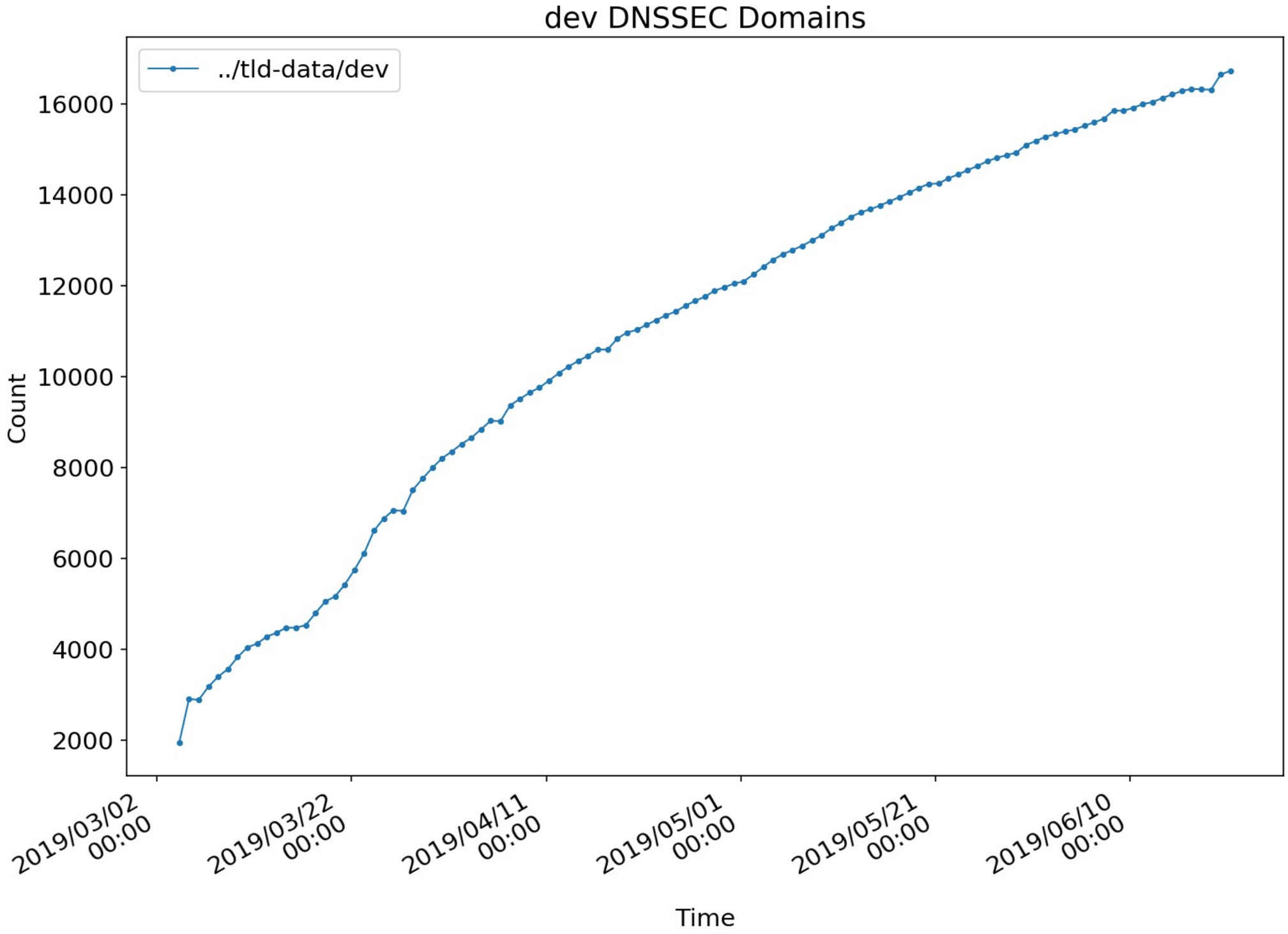
Leader of the Pack: .nl



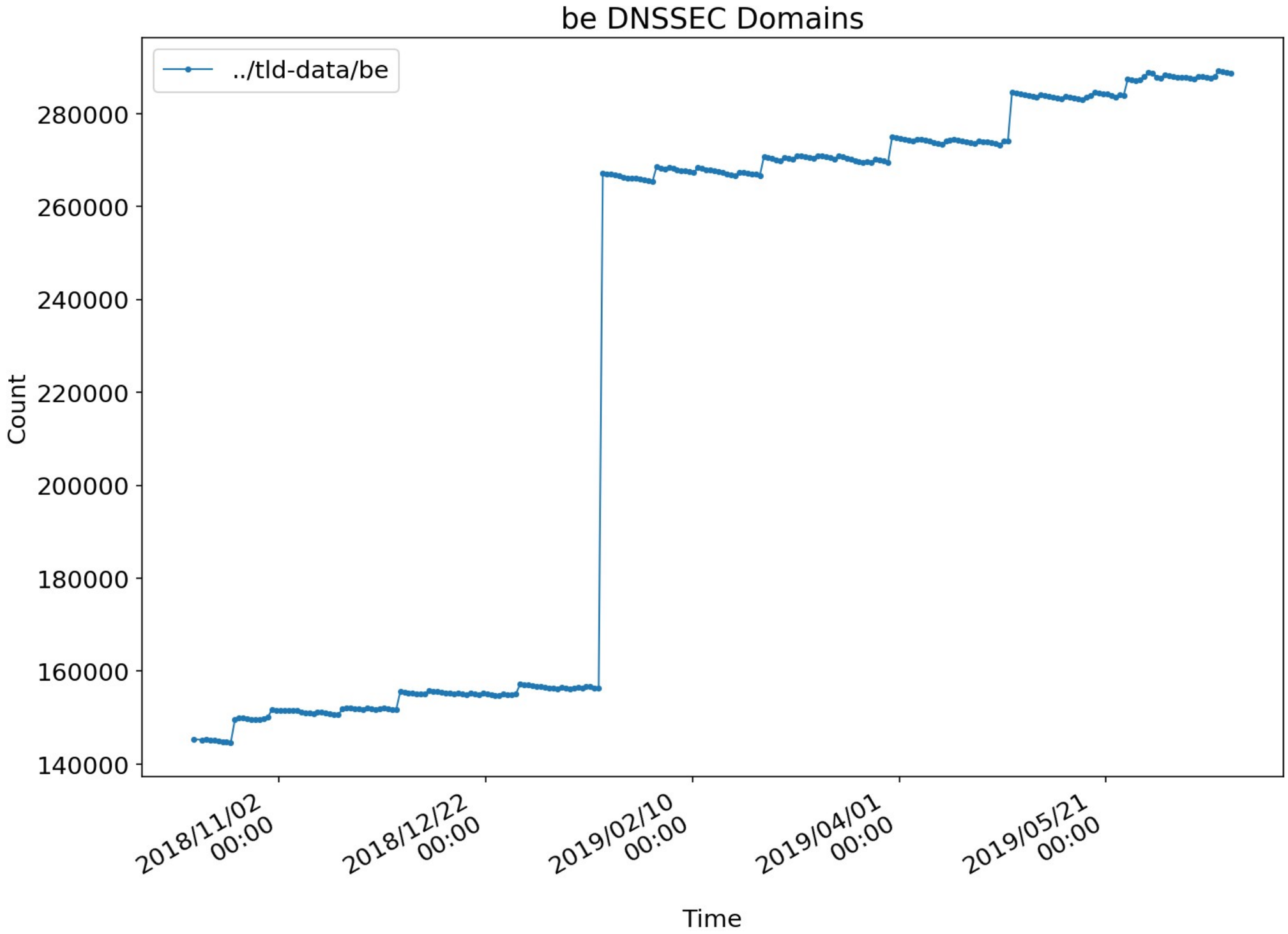
Consistency is Key: .app



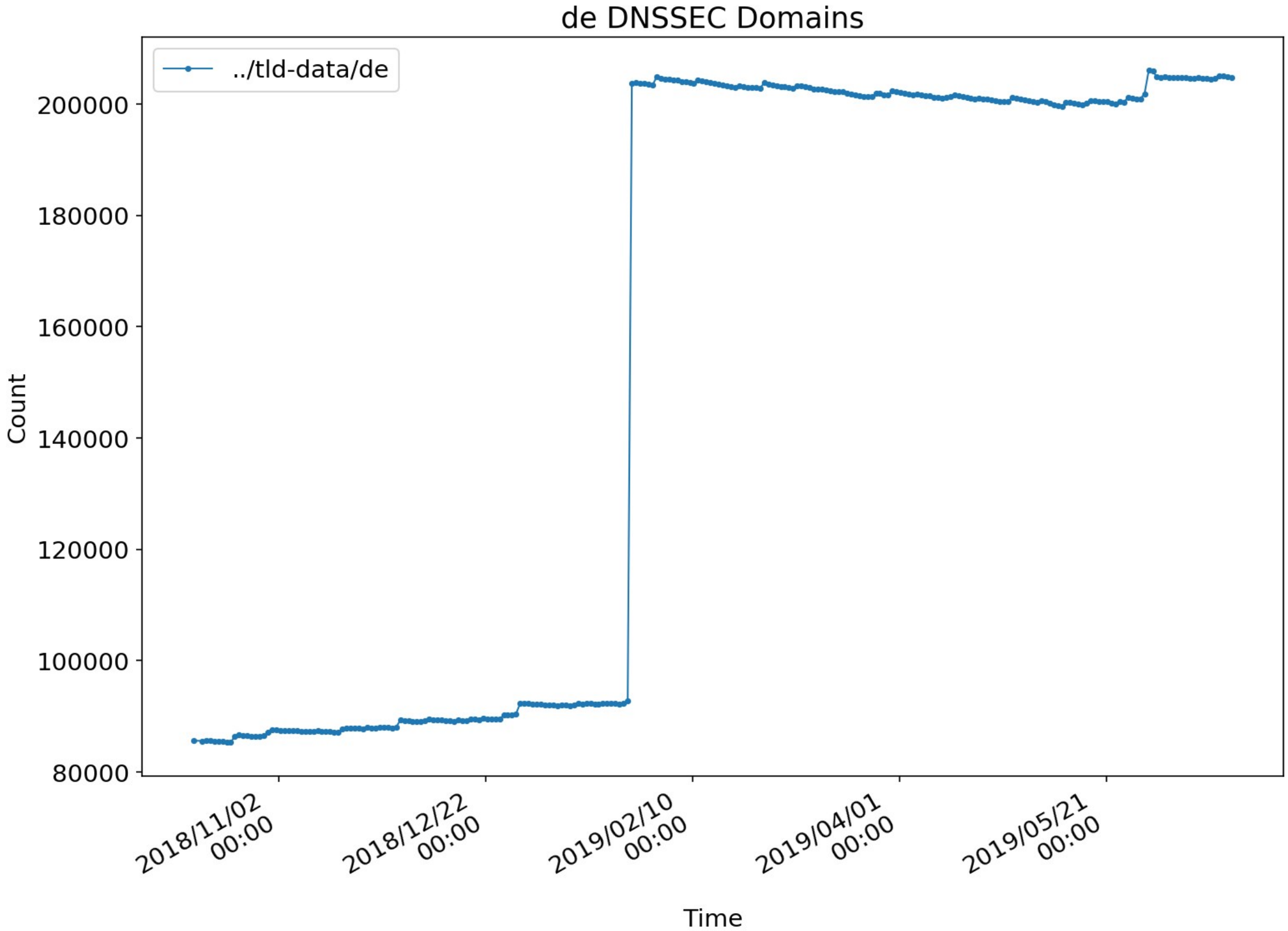
Smooth Operations: .dev



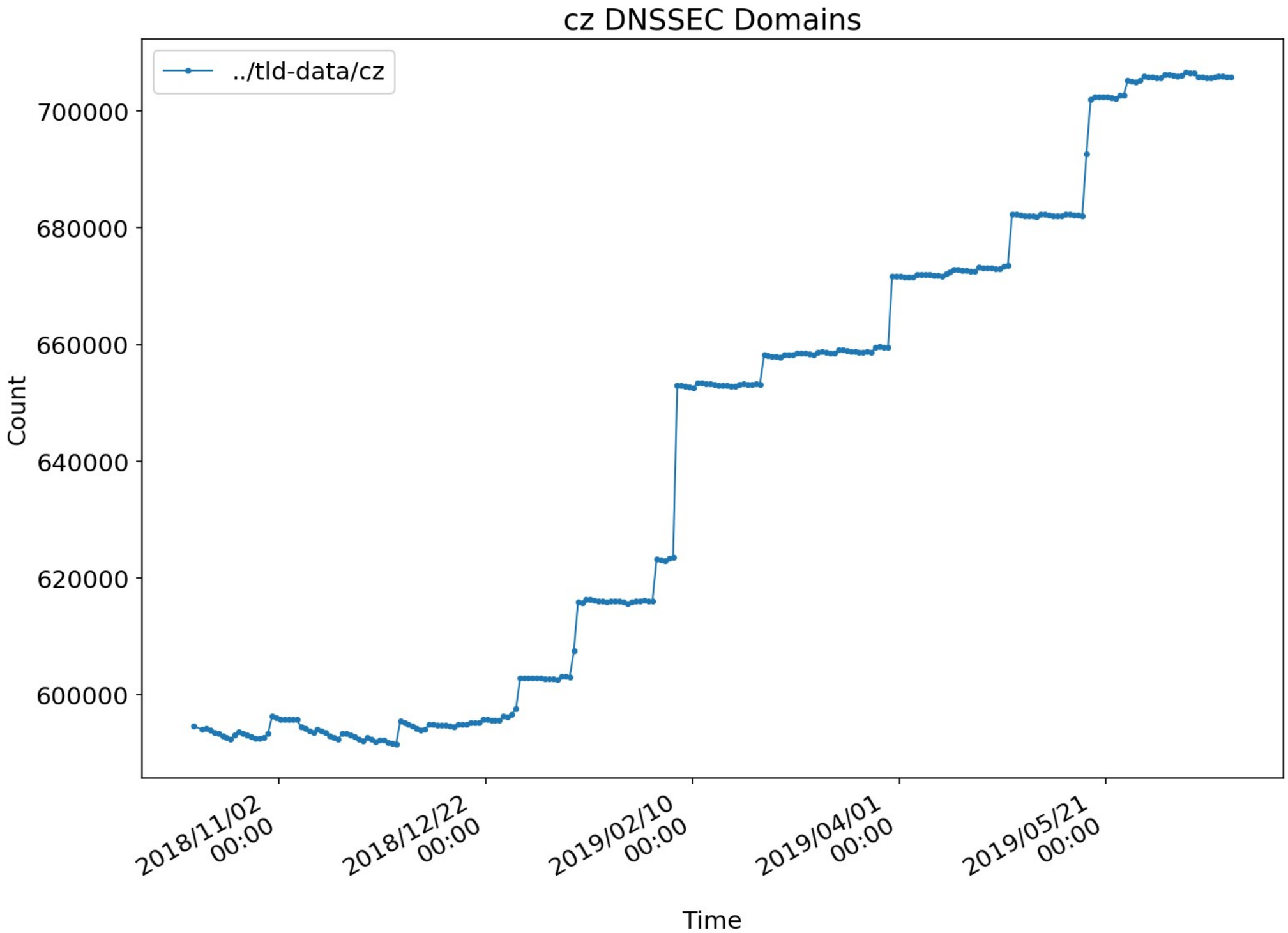
Big Jump: .be


be DNSSEC Domains
../tld-data/be
280000
260000
240000
220000
200000
180000
160000
140000
Count
2018/11/02 00:00
2018/12/22 00:00
2019/02/10 00:00
2019/04/01 00:00
2019/05/21 00:00
Time

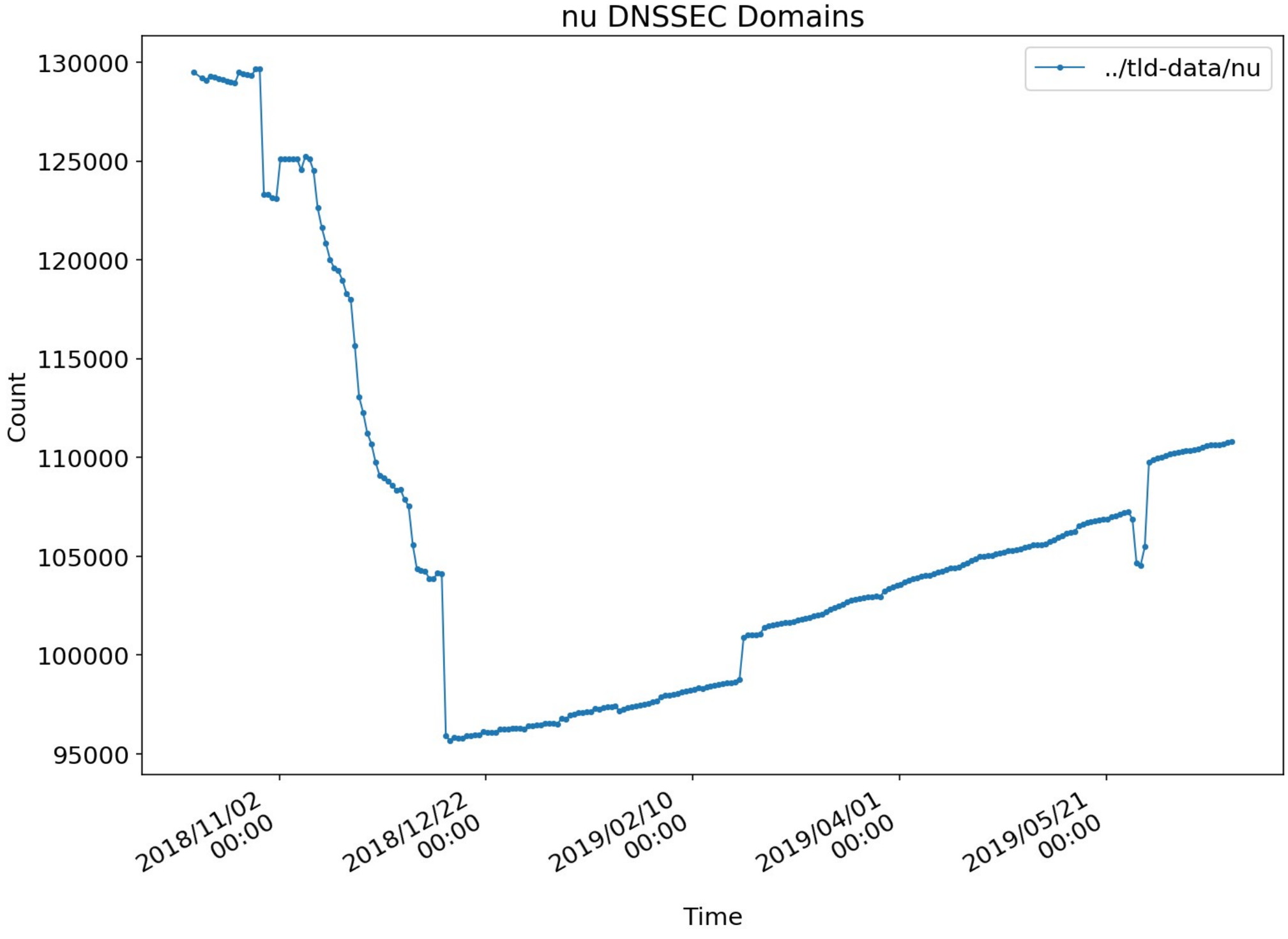
Big Jump: .de


de DNSSEC Domains
../tld-data/de
200000
180000
160000
140000
120000
100000
80000
Count
2018/11/02 00:00
2018/12/22 00:00
2019/02/10 00:00
2019/04/01 00:00
2019/05/21 00:00
Time

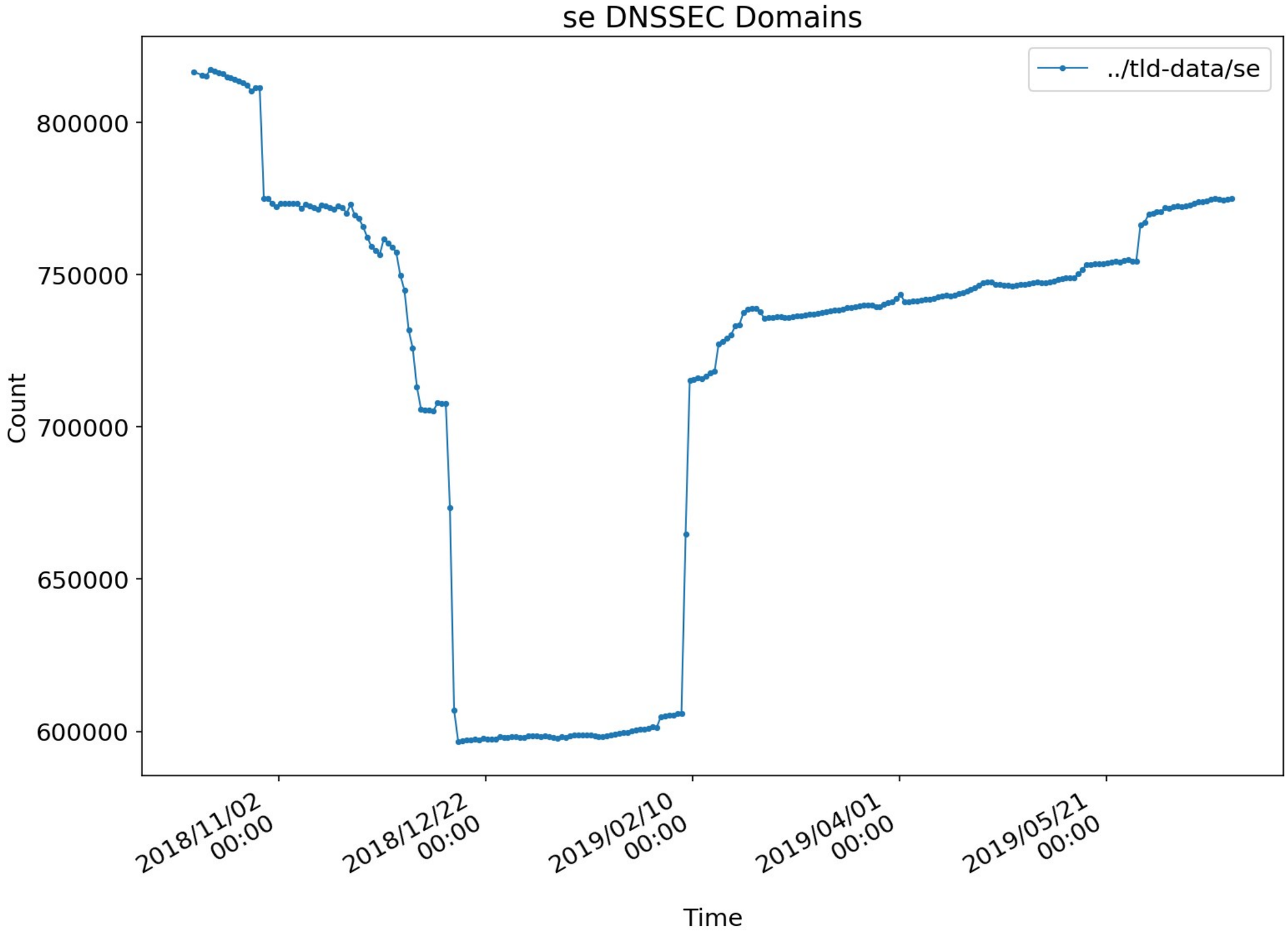
Lots of Small Big Jumps: .cz



Some Loss Of Course Too



Some Disable and Re-enables Of Course



DNSSEC checklist

- Keep name-server software up to date
- Test zones with apex wildcard A or CNAMEs
- Test zones with empty non-terminals
- Always sign **after** changing SOA serial numbers
- Avoid NSEC3 opt-out in most zones
- Avoid high NSEC3 (extra) iteration counts
  - (0 is BCP!)

https://lists.dns-oarc.net/pipermail/dns-operations/2017-December/017127.html
https://lists.dns-oarc.net/pipermail/dns-operations/2018-January/017173.html

DNSSEC Hygiene

- All nameservers need:
  - EDNS(0) support
  - NSEC3 support
- Don't block IP fragments
- Reply NODATA or NXDomain
  - (not NOTIMP, REFUSED, ...)
- Test correct denial-of-existence for each edge case
- Monitor nameservers for correct DNSSEC handling

Rolling Your TLS Keys

- Use multiple TLSA records to publish current and future keys
  - Publish **TLSA records of keys** well in advance of using new certificates
  - Required by DNS caching (publish 2xTTL ahead)

- Two pre-publishing models:
  - EE Key + Next EE Key: (3 1 1 + 3 1 1)
  - EE Key + TA Key: (3 1 1 + 2 1 1)

- Deploy new chain, and publish new TLSA records:

```
_25._tcp.mx.example.com. IN TLSA 3 1 1 curr-pubkey-sha256
_25._tcp.mx.example.com. IN TLSA 3 1 1 next-pubkey-sha256
```

Automate

- Automate:
  - TLSA record updates and zone re-signing
  - Key rollover
  - Acquiring any certs ...
  - … and converting to TLSA records

- Have working contacts in WHOIS, SOA, postmaster

DANE Resources

Dane implementation resources:

- https://github.com/baknu/DANE-for-SMTP/wiki/2.-Implementation-resources

Reasons for 3 1 1, and 3 1 1 + 3 1 1 key rollover info:

- https://github.com/danefail/list/issues/47#issuecomment-456623996
- https://mail.sys4.de/pipermail/dane-users/2018-February/000440.html
- https://tools.ietf.org/html/rfc7671#section-8.1

NYLUG talk slides and video:

- http://files.nylug.org/2018/nylug-20181017-dnssec-dane.pdf
- https://youtu.be/A8SgW9y__io

Internet.nl "toolbox" DANE wiki (Work in progress):

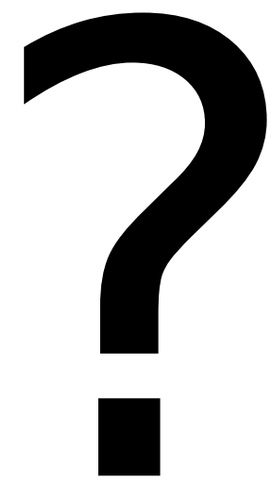
- https://github.com/internetstandards/toolbox-wiki

Help wanted

- More ccTLD lists of signed delegations
- Fix any DNSSEC issues
  - Including ones centered on Denial of Existence!
- Please enable DANE ***outbound***
  - (even if your own domain is unsigned)
- Please enable DNSSEC and DANE on hosting MX servers
  - Especially when hosting thousands signed domains
    - e.g. ovh.net, googlemail.com, ...

Questions?

https://stats.dnssec-tools.org/



Viktor Dukhovni
<ietf-dane@dukhovni.org>

Wes Hardaker
<hardaker@isi.edu>