DANE/DNSSEC survey

Viktor Dukhovni &

Wes Hardaker

https://stats.dnssec-tools.org

DNS-OARC31 | November 01 2019

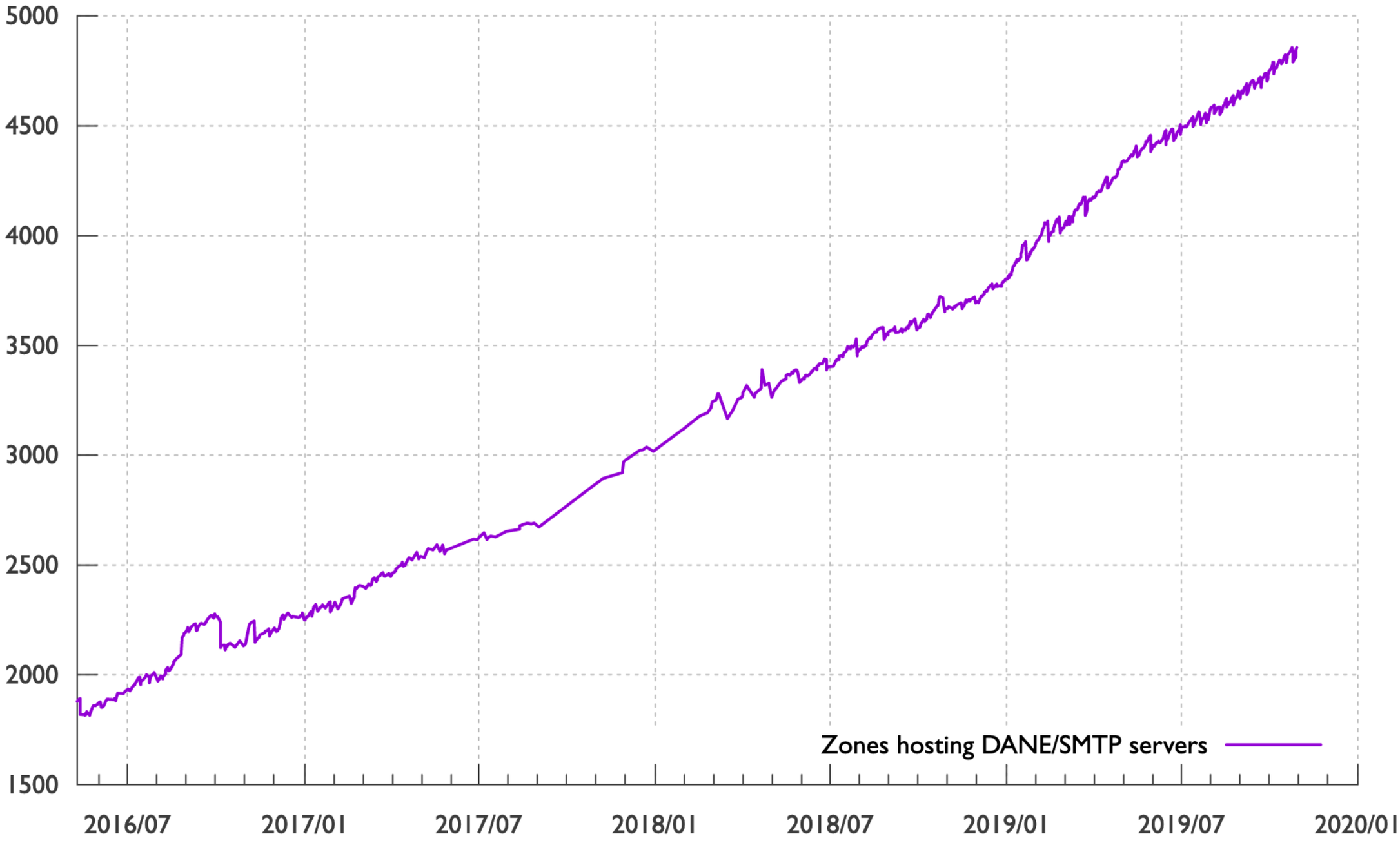
Survey goals

- Monitor SMTP TLSA records
  - Nag "inbound" domain owners to fix problems (~6k notices over 5 years).
  - Removes disincentives to "outbound" deployment
- Statistics are a useful byproduct
  - Make a marketing case for further deployment

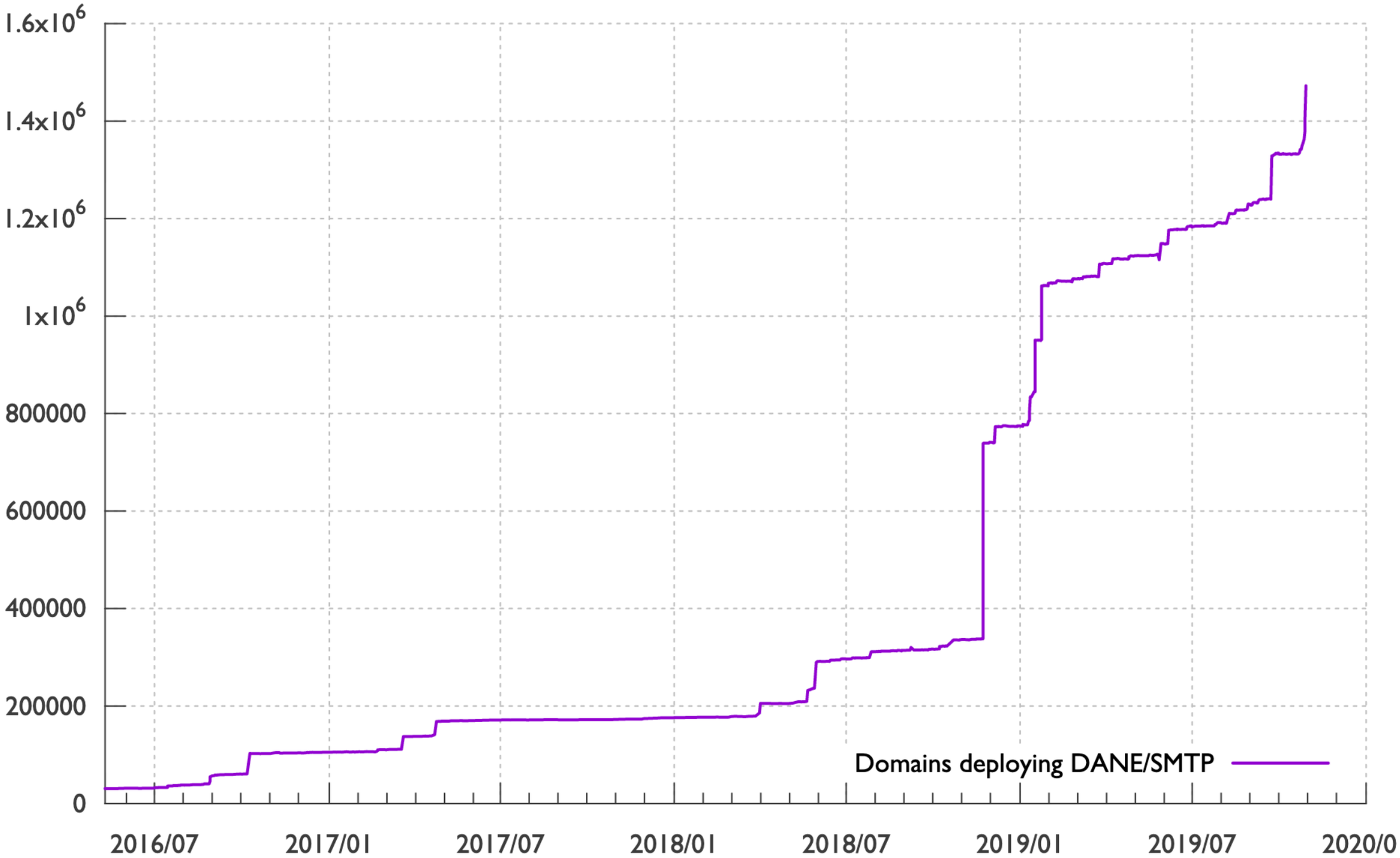
Survey Tech

- 25W 4-core Xeon (Skylake) server (64 GB RAM, 2TB SSD)
- Postgres DB:
  - history of DS, DNSKEY, MX, A, AAAA, TLSA RRs & certificate chains
- Unbound resolver and local root zone copy, some TLDs forwarded to Google, Cloudflare, Verisign and Quad9
- 4k LoC Haskell: SMTP, DNS, TLS, DANE, DB, concurrent

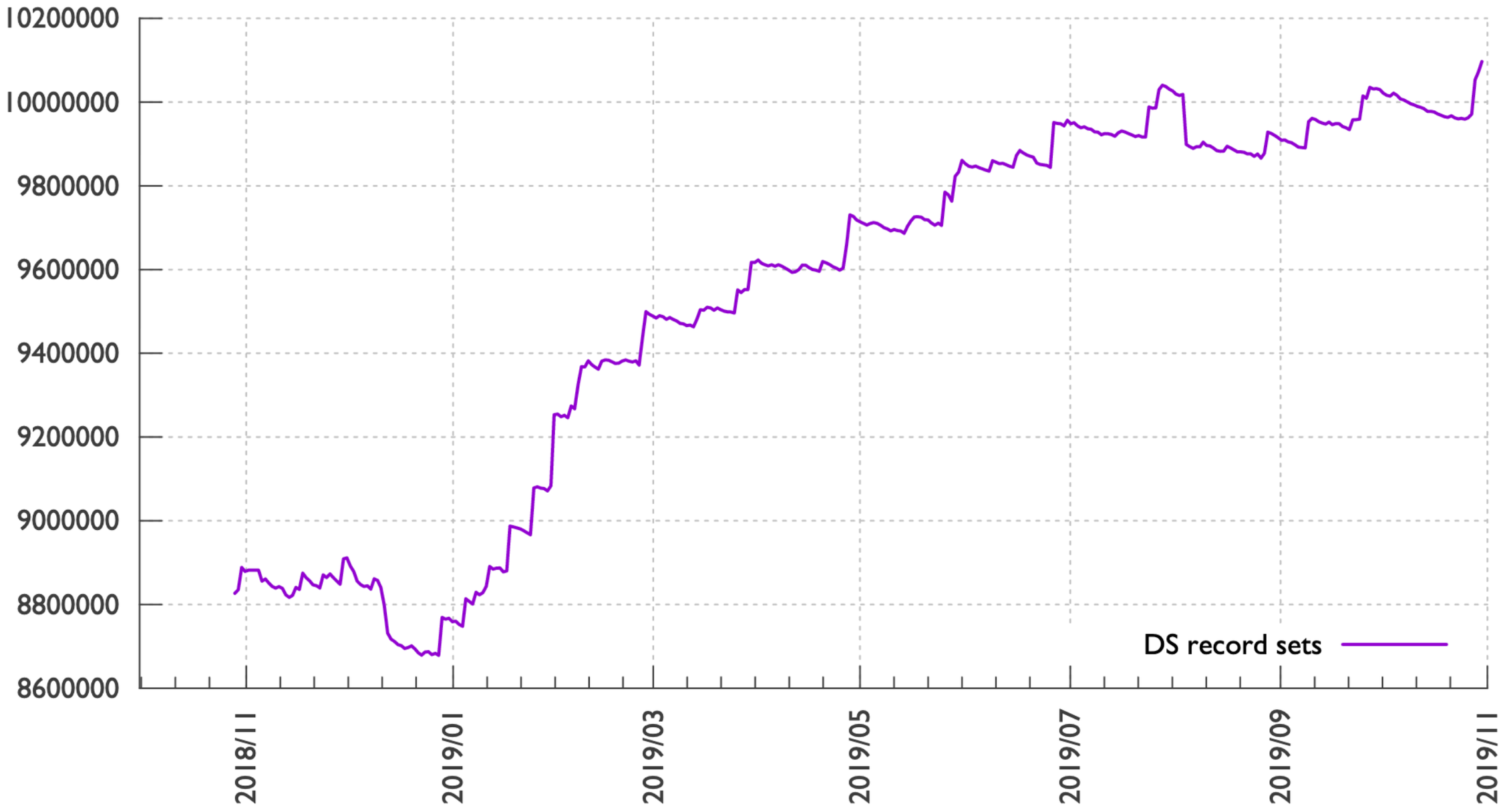
#Zones of DANE MX hosts



DANE protected domains



Signed Delegations



DANE numbers

- 10.1 million domains with DNSSEC-validated MX
- 1.49 million domains with DANE SMTP
- ~7400 DANE MX hosts in ~4850 zones
- 10s of millions of users (gmx.de, web.de, comcast.net)
- ~1000 domains with TLSA record lookup problems
- ~450 domains with wrong TLSA records or no STARTTLS

DNSSEC numbers

- ~250 million domain sample
- ~10 million signed, ~11 million estimated
- ~3.2 million ECDSA P-256 (often just a single key that is both KSK and ZSK), rest RSA
- KSK typically 2048-bit, ZSK typically 1024-bit

Help wanted

- ccTLD signed domain lists. I have zone data for gTLDs,
  - but ccTLD data generally incomplete
    - exceptions: CA, CH, DK, FR, IS, LI, NL, NU, SE
- Please forward notices to customers with TLSA breakage
  - WHOIS often useless