DNSSEC / DANE SURVEY UPDATE

Wes Hardaker <hardaker@isi.edu>
Viktor Dukhovni <ietf-dane@dukhovni.org>

Background

- We’ve presented previously about this work
  - 2018/03 Puerto Rico
  - 2018/10 Barcelona
  - 2019/06 Panama
- Updates since then
  - Scanning site move
  - Web site statistics improvements
  - New data exploration site

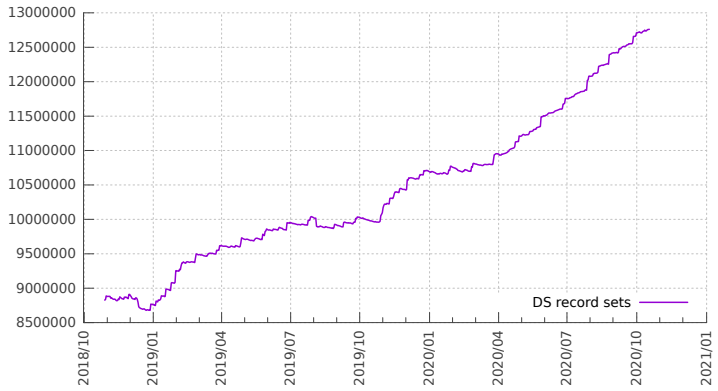
Infrastructure Improvements: Scanning Site Moved

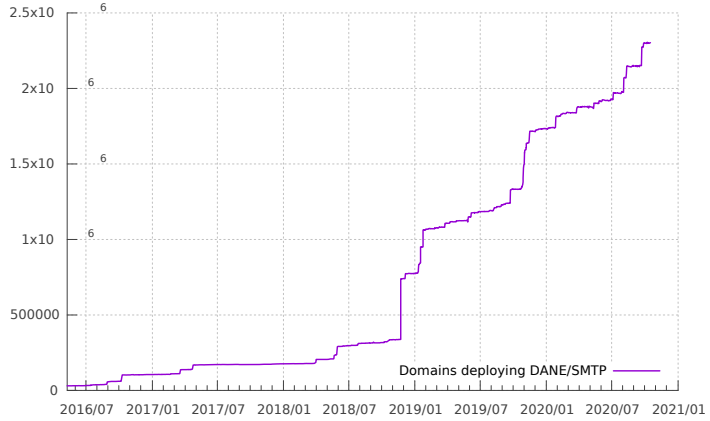
- Viktor has been running it from his apartment until now!
  - ISI's **Analysis of Network Traffic** (ANT) lab[1] has donated hardware to the cause
- Thanks also to the cooperation of many external parties:
  - Resolvers: Google, Cloudflare, Verisign and Quad9
  - Data sources: AFNIC, Afilias, DK Hostmaster, Farsight Security, ICANN, IIS, ISNIC, Neustar, Project Sonar, Rapid7 Labs, Public Interest Registry, SIDN, Switch, Verisign

[1] https://ant.isi.edu/

Infrastructure Improvements: Scanning Site Moved

- Daily scanning:
  1) Create a list of **all DNSSEC signed zones** registered under a *Public Suffix List (PSL)* point
  2) **Collect DNS records** for each zone: DNSSEC keys, DS, MX records, and TLSA records for each MX
  3) **Open a SMTP connection** to each MX host to test TLS capabilities and collect certificates
  4) A lot of number crunching to summarize the results
  5) Results updated daily at https://stats.dnssec-tools.org/

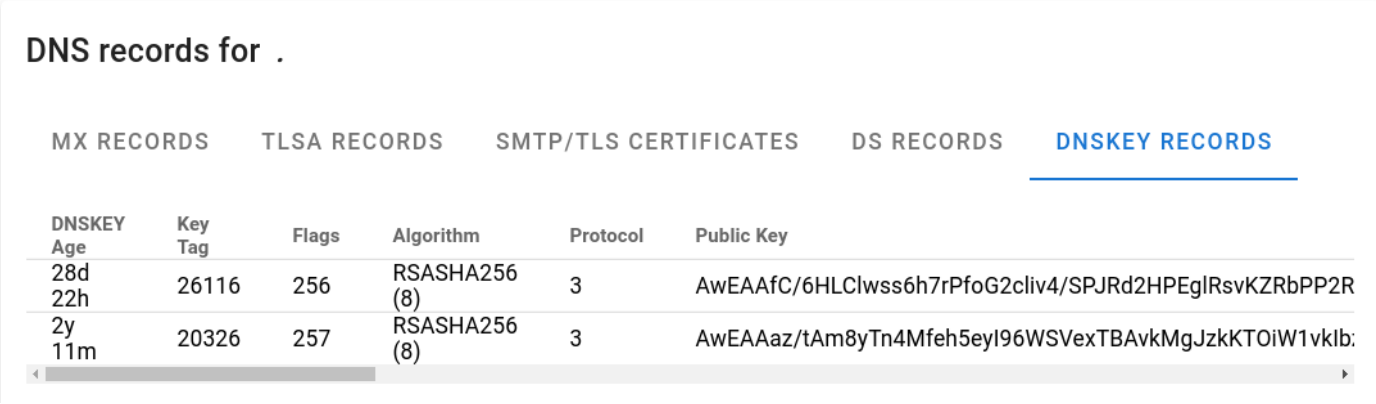




[1] https://ant.isi.edu/

Recent Website Improvements

- Main page: A few new graphs added with better web-UI support
- New data-explorer website:
  - Easy exploration of DNSSEC/DANE issues for zone owners
  - REST API created to fetch data per site
- Compliments existing sites:
  - **dane.sys4.de**
  - **dnsviz.net**



New Explore Page Errors and Warnings

- MX lookups or MX address lookups are failing
- MX hosts that are invalid or without IP addresses
- SMTP connection failures
- DNSKEY lookups are failing
- Deprecated DNSSEC/RSA algorithms
- DANE TLSA records fail to validate SMTP certificates
- TLSA record lookups are failing, or the records are unusable
- MX hosts have no TLSA records or are in unsigned zones

Demo Time

A closing word of warning: Let's Encrypt TLSA records

- Many people use TLSA type "2 1 1" to point to the Let's Encrypt CA
  - _25._tcp.each.mx.host. IN TLSA 2 1 1 60b87575447dcba2a36b7d11ac09fb24a9db406fee12d2cc90180517616e8a18
  - _25._tcp.each.mx.host. IN TLSA 2 1 1 b111dd8a1c2091a89bd4fd60c57f0716cce50feeff8137cdbee0326e02cf362b
- You need to add their new CA TLSA records ASAP
  - _25._tcp.each.mx.host. IN TLSA 2 1 1 276fe8a8c4ec7611565bf9fce6dcace9be320c1b5bea27596b2204071ed04f10
  - _25._tcp.each.mx.host. IN TLSA 2 1 1 bd936e72b212ef6f773102c6b77d38f94297322efc25396bc3279422e0c89270
  - _25._tcp.each.mx.host. IN TLSA 2 1 1 8d02536c887482bc34ff54e41d2ba659bf85b341a0a20afadb5813dcfbcf286d
  - _25._tcp.each.mx.host. IN TLSA 2 1 1 e5545e211347241891c554a03934cde9b749664a59d26d615fe58f77990f2d03
- Or the mail won't go through!
- Leave all 6 in place until the first two **expire in 2021-09-30**
- Further information: http://dnssec-stats.ant.isi.edu/~viktor/x3hosts.html

Come out and play

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

- Sign your zone!
- Secure your mail!

- Contact us: ant-dnssec-operators@isi.edu