# Counting DNSSEC for fun

Ondřej Caletka

cesnet

June 14, 2019

Lightning talk is either good or short.

cesnet

# DNSSEC

- cryptographic authentication of DNS data
- well deployed somewhere (55 % of .CZ domain)
- less deployed elsewhere (.SK, deployed in May 2019)

cesnet

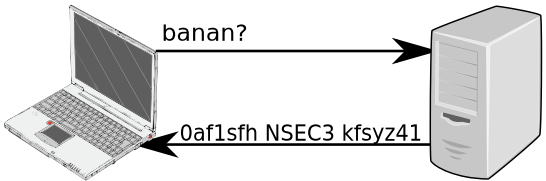
# Who deployed DNSSEC in .SK?

- almost 400k domains
- not even `sk-nic.sk` is signed
- full zone scan is very slow
- luckily there's NSEC3 Opt-out
  - only DNSSEC-secured domains have NSEC3 records

cesnet

# NSEC3

- repeated SHA-1 hashing of domain names
- *only three people in the world actually understand it*




```
hash(@)      = 0af1sfh
hash(ananas) = z781sfa
hash(citron) = kfsyz41
hash(banan)  = 27acj54
```

```
0af1sfh IN NSEC3 kfsyz41
kfsyz41 IN NSEC3 z781sfa
z781sfa IN NSEC3 0af1sfh
```

cesnet

# We need to break SHA-1

cesnet

# We need to break SHA-1

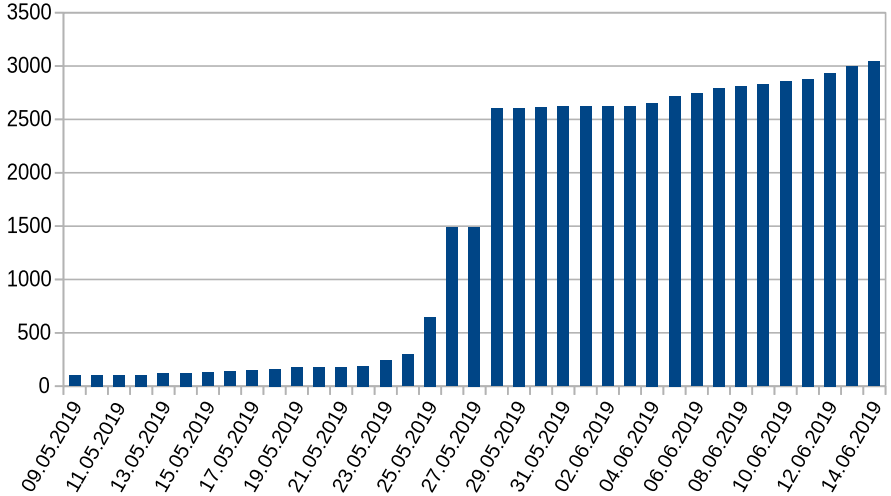
Actually, we don't.
SK.NIC publishes list of all domains.

cesnet

# Walk NSEC3 chain of .SK

1. download list of domains
2. create a rainbow table for all domain names
3. follow the chain of NSEC3 records
4. abuse Travis CI to do it for you every day
5. publish CSV results at GitHub pages
6. PROFIT!

cesnet


3500
3000
2500
2000
1500
1000
500
0
09.05.2019
11.05.2019
13.05.2019
15.05.2019
17.05.2019
19.05.2019
21.05.2019
23.05.2019
25.05.2019
27.05.2019
29.05.2019
31.05.2019
02.06.2019
04.06.2019
06.06.2019
08.06.2019
10.06.2019
12.06.2019
14.06.2019

cesnet

https://github.com/oskar456/walk_dotsk_ds

Thank you!

**Ondřej Caletka**
**Ondrej.Caletka@cesnet.cz**
https://**Ondřej.Caletka.cz**


Slides are already online.