DNSSEC for security and performance

Petr Špaček • petr.spacek@nic.cz • 2018-02-04

KNOT RESOLVER

cz.nic | CZ DOMAIN REGISTRY

Outline

- DNS performance
- Random subdomain attack
- DNSSEC aggressive cache
- How it helps

DNS performance under stress

- Heavy over-provisioning
- Normal traffic → not interesting
  - caches
- DDoS → consumes everything
  - various types
  - "resilient", not "guaranteed"
  - costs defender vs. attacker

Security & performance

- "Security" usually slows things down
- Higher resource consumption
  => easier to DDoS

- Not always!

Random subdomain attack

- Queries
  `blah09k23jk234.www.example.com.`
  `eek8aomajkejqh.www.example.com.`
  `poop992983923c.www.example.com.`
  `wtf3-090n32nii.www.example.com.`
  → DNS API → resolver → auth server
- Easy to execute
- Minimal control of zombie (Javascript, ad, ...)

DNSSEC aggressive cache

- RFC 8198
  Aggressive Use of DNSSEC-Validated Cache
- DNSSEC-signed domain with NSEC
- Query names
  `example. ; example2. ; exampleeeeee.`
- Answer – proof of nonexistence
  `status: NXDOMAIN`
  `everbank. 3600 IN NSEC exchange. ...`

DNSSEC vs. random subdomain attack

- **DNSSEC-signed** domains are protected
- No configuration or heuristics needed!
- **Sign** to get protection against
  - DNS spoofing
  - cache poisoning
  - random subdomain attack

- **Validate**
  - use modern resolvers