DNSSEC & PowerDNS
Large Scale DNSSEC Deployments

"lessons learned"
http://tinyurl.com/icann-powerdns

ICANN44, Prague

Bert Hubert
bert.hubert@netherlabs.nl
E.164: +31-622-440-095

POWERDNS

Agenda

- PowerDNS & Netherlabs
- Evolution of thoughts on DNSSEC
- DNSSEC “the great divider”
- DNSSEC profile of PowerDNS
- Lessons learned from Swedish & Other deployments

POWERDNS

PowerDNS & Netherlabs

- PowerDNS is the name of the products: Authoritative & Recursor
- Around since late 1990s. Started out as proprietary software, saw the light 10+ years ago, now 100% Open Source
- Powers ±30% of all domains in Europe, 90+% of DNSSEC in Scandinavia.
- Major SLA-supported users include lots of telecommunications companies named after their country.
- Developed by Netherlabs & Community, 100% SLA-backed supported by Netherlabs

POWERDNS

PowerDNS Authoritative distinguishing features

- Serves data from plain zone files, MySQL, PostgreSQL, Microsoft SQL Server, LDAP, Oracle, SQLite, etc etc, Lua scripts, all other scripts
  - Including geographical load balancing & failover
- Can serve data from:
  - native djbdns/tinydns zonefiles
  - native MyDNS data
- Excitingly, adds DNSSEC to djndns & MyDNS!

POWERDNS

DNSSEC & PowerDNS

- Spent a decade on IETF mailing lists explaining DNSSEC was over-engineered, too complex and tricky to implement
  - In 2010 we gave up & implemented DNSSEC "if it has to be done, let's do it in a way that can be deployed"
  - Now powers 200k+ DNSSEC domains!
- By now however we are **SURE** DNSSEC is over-engineered, too complex and tricky to implement ;-)

POWERDNS

Enabling DNSSEC on a domain in PowerDNS

- Step 1:
  - $ **pdnssec secure-zone icann.org**
- Step 2
  - there is no step 2
- Step 3:
  - get DS from '**pdnssec show-zone icann.org**' and inform registrar

POWERDNS

PowerDNS DNSSEC

- NSEC, NSEC3, NSEC3-'narrow', all relevant algorithms
- Online signing
  - "No need to change anything"
    - Even works in BIND zonefile mode!
- Offline signing
- Inline signing
- 100% database controlled for easy provisioning & replication

POWERDNS

DNSSEC: (not) making the grade

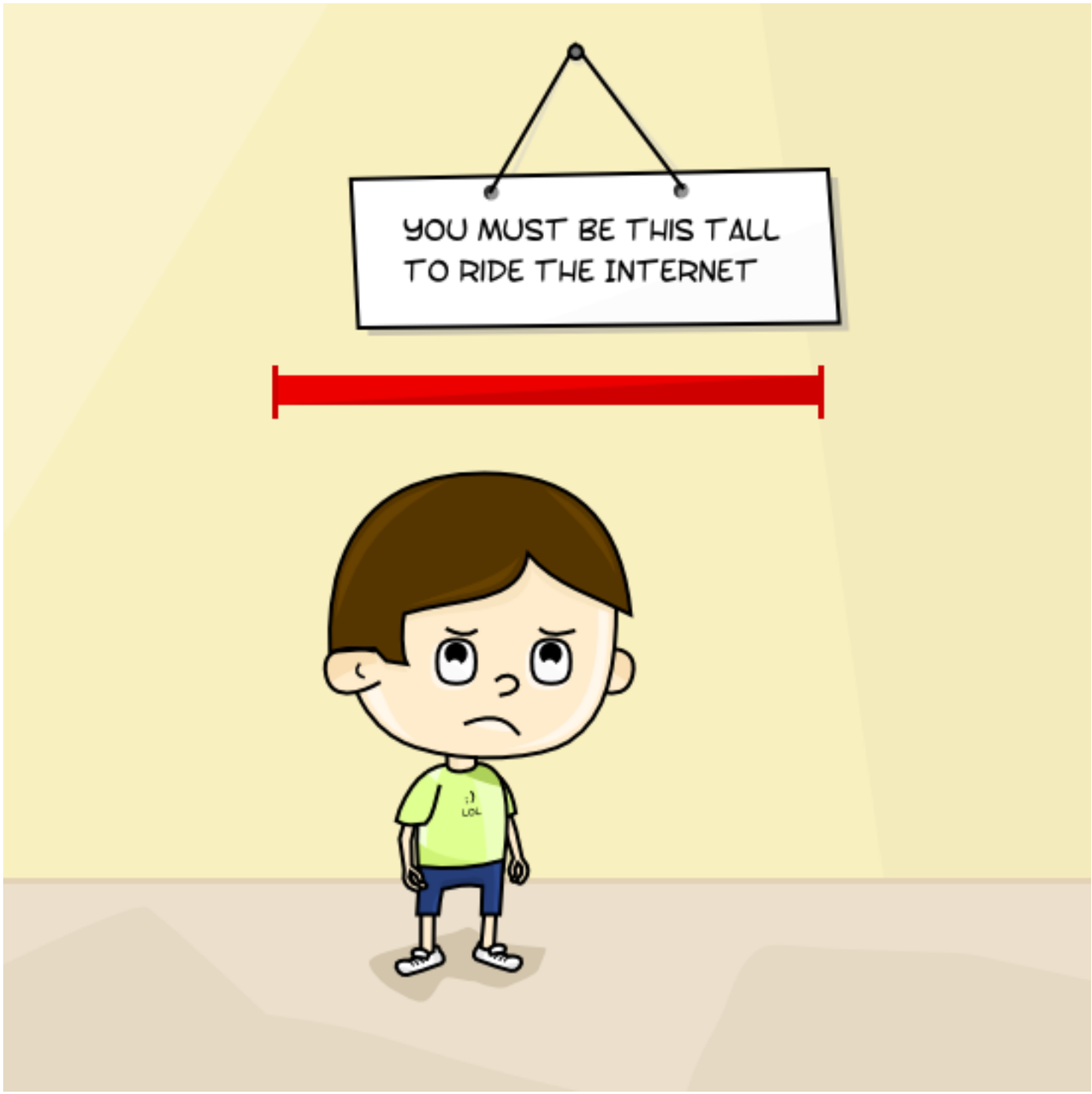
~~MaraDNS~~

~~TinyDNS/ DJBDNS~~

~~Cisco CNR~~

NSD

Unbound



~~Posadis~~

~~MyDNS~~

~~SimpleDNS~~

Knot

Yadifa

http://huwshimi.com/comic/

POWERDNS

DNSSEC: (not) making the grade

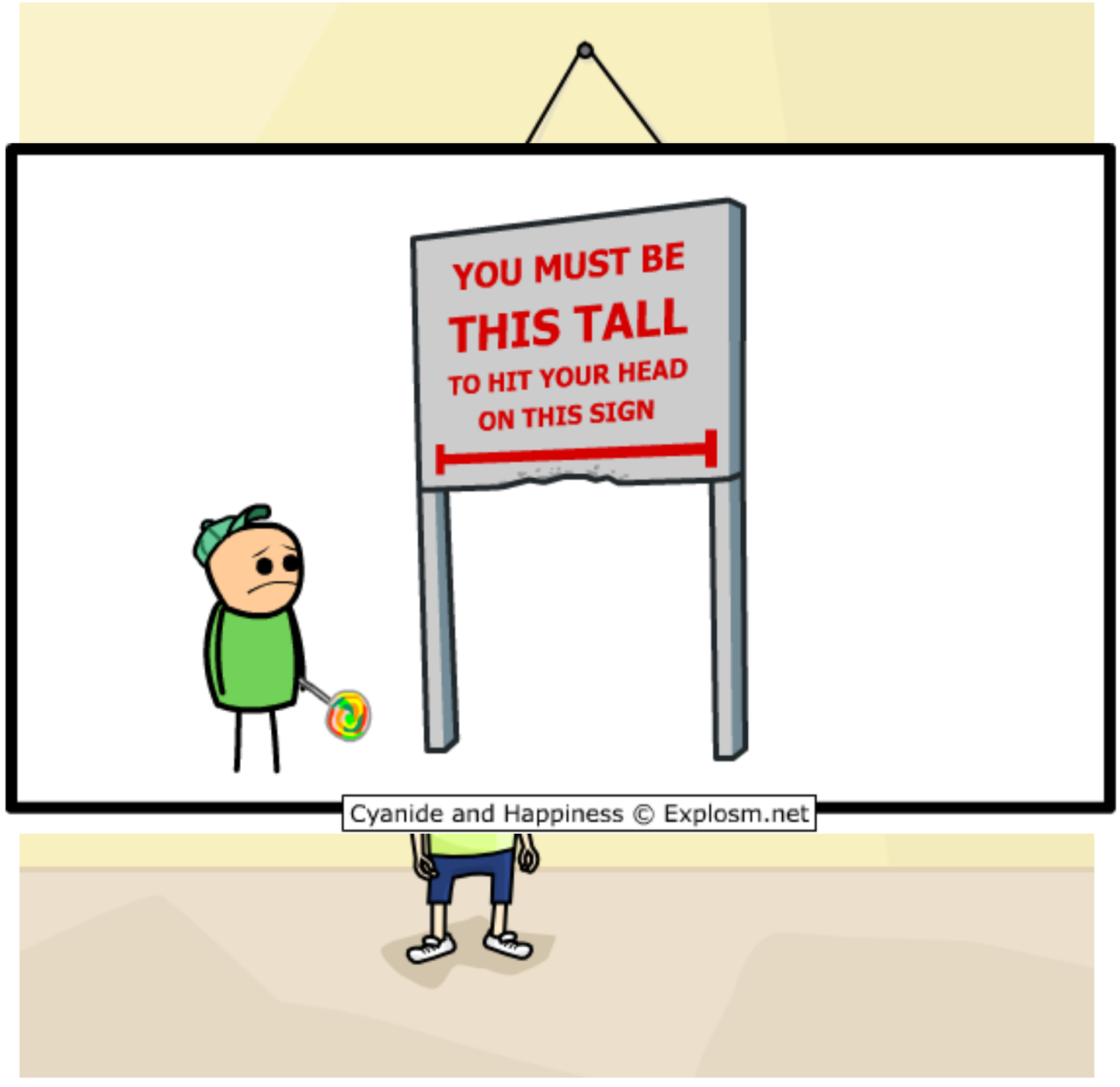
~~MaraDNS~~

~~TinyDNS/ DJBDNS~~

~~Cisco CNR~~

NSD

Unbound



~~Posadis~~

~~MyDNS~~

~~SimpleDNS~~

Knot

Yadifa

http://huwshimi.com/comic/

POWERDNS

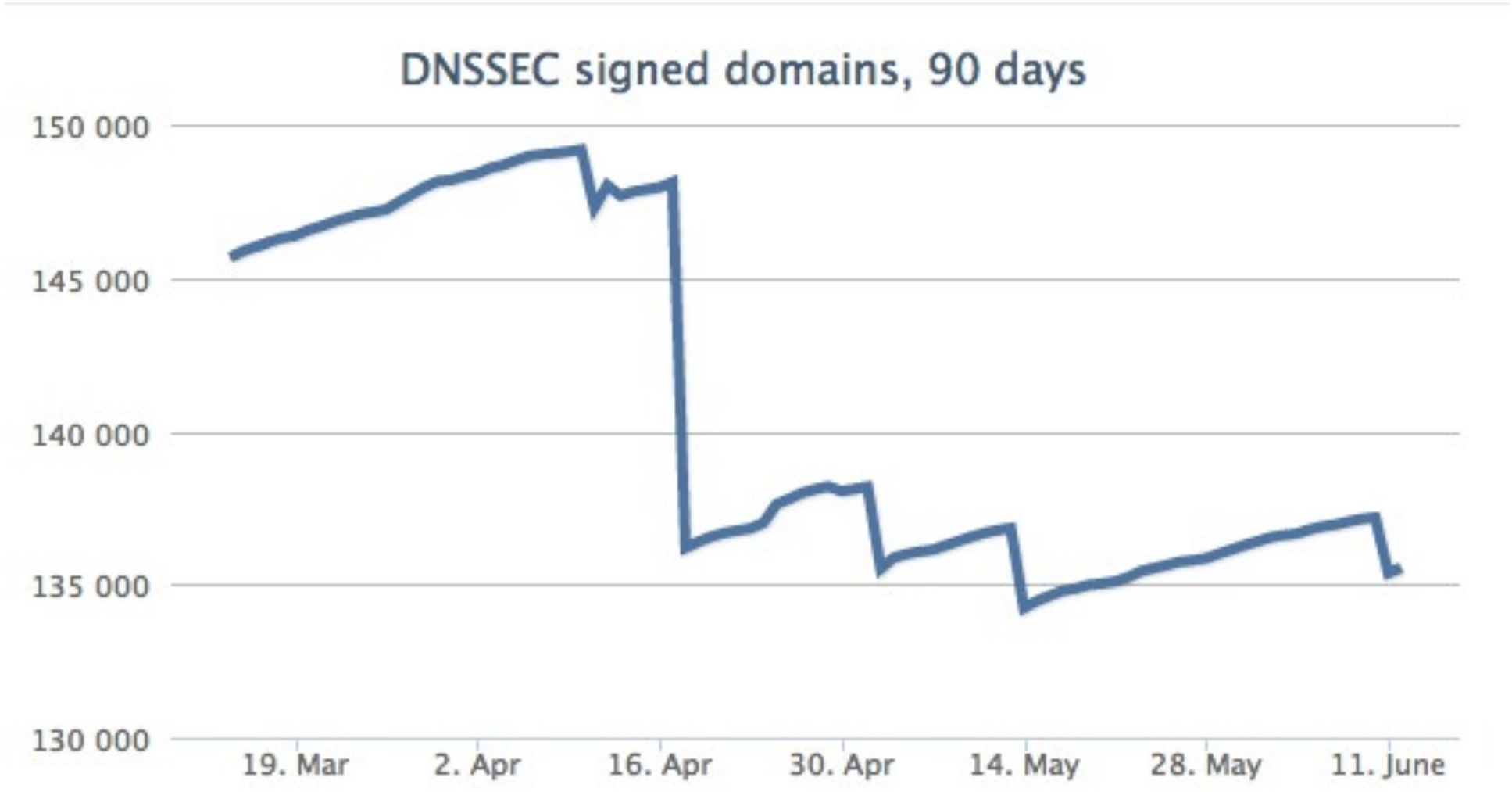
Things we discovered

- There is always one more bug in your DNSSEC logic or code
  - Our regression tests found issues in both the NSD and BIND implementations too
    - ISC & NLNetLabs helped find bugs in PowerDNS too, thanks!
- The benchmark case: two overlapping zones on a single server, parent zone has wildcard CNAMEs to child zone and delegates securely to the child zone
  - **GOOD LUCK**

Things we discovered

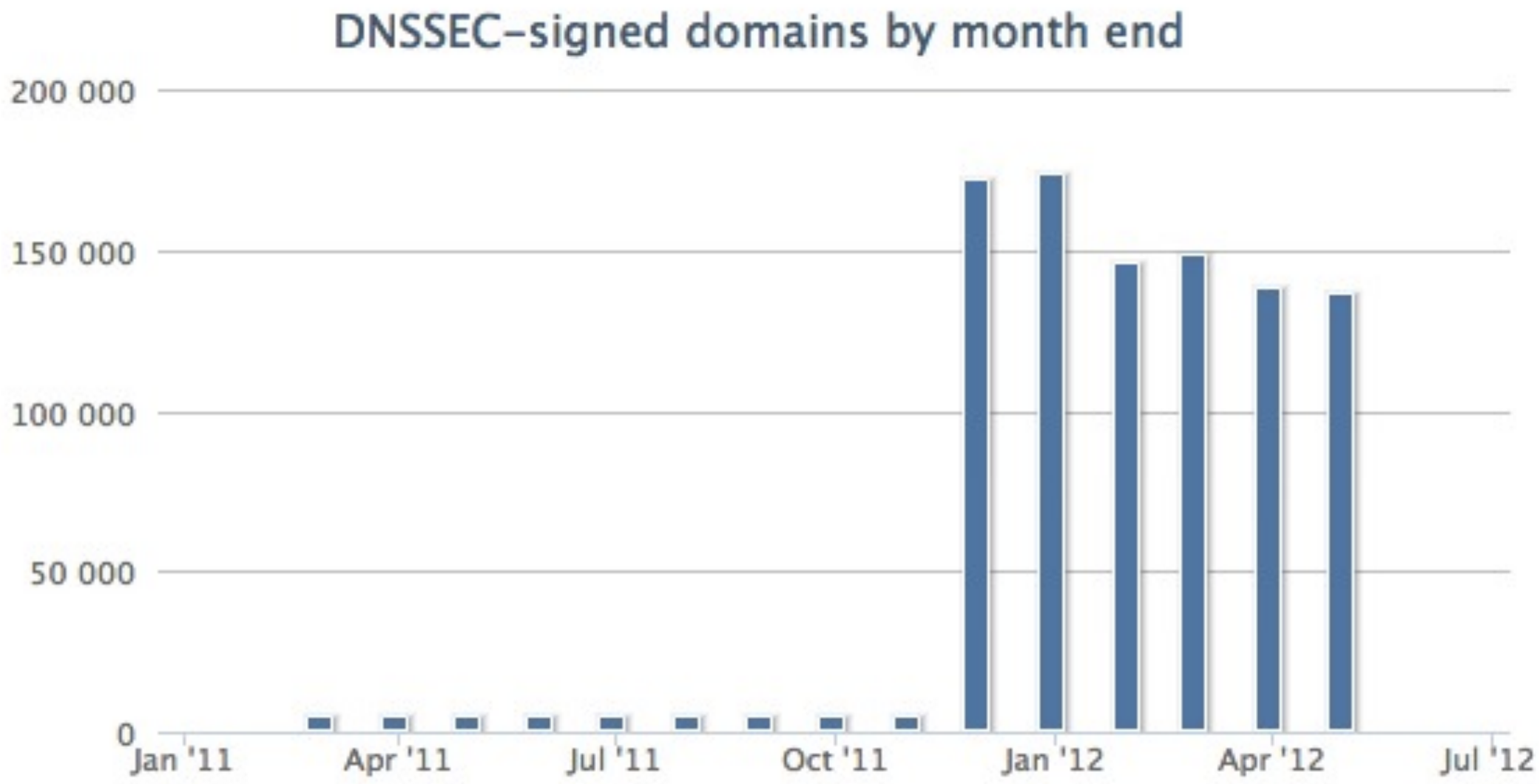
- It appears that there is a large market for online signing DNSSEC that is open source and easy to use (and comes with SLA-backed support)
  - >60% of .NL launching DNSSEC registrars are on PowerDNS, for example
- Online signing has not proven to be a problem

“Bugs in action”



https://www.iis.se/en/domaner/statistik/tillvaxt?chart=per-type

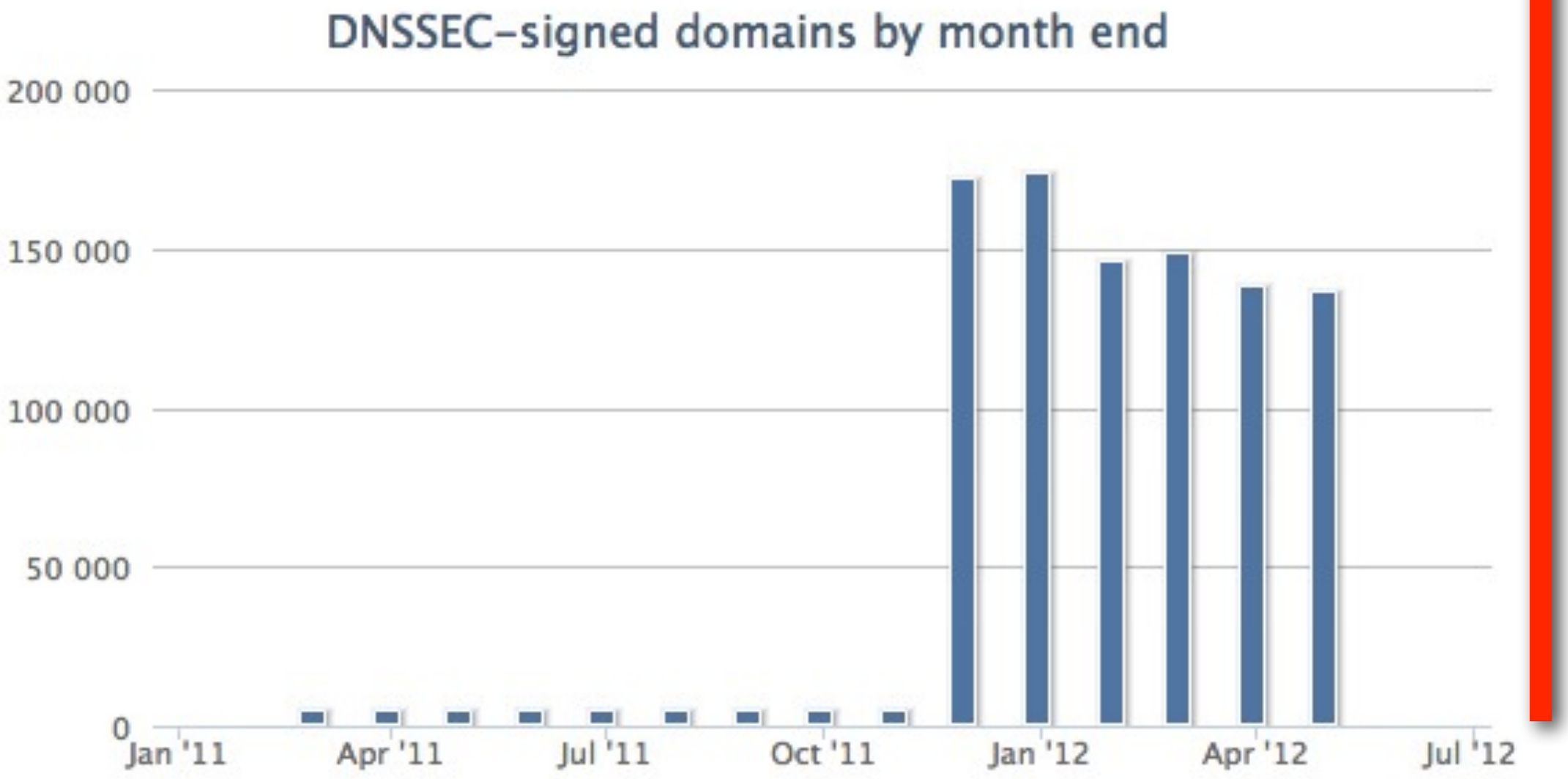
“Bugs in action”



https://www.iis.se/en/domaner/statistik/tillvaxt?chart=per-type

POWERDNS

“Bugs in action”



https://www.iis.se/en/domaner/statistik/tillvaxt?chart=per-type

POWERDNS

Surprising developments

- In the course of 3.0 and 3.1 development it became clear there is large interest in using PowerDNS as an inline signer
  - We had not figured that as a usecase, but added support for fiddling with SOA serial numbers &c.
  - Idea is then to offload the actual serving to a cloud provider
- In this sense, PowerDNS 'competes' with OpenDNSSEC (except without HSM support)

Surprising developments

- It was fully expected that the first big deployments would run into DNSSEC bugs or quality of implementation issues
  - And it happened
- We however have had very few reports of the other issue we'd been fearing: firewalls & networking equipment blocking/interfering with DNSSEC
  - Unexpected lack of problems!

Recommendations when doing large scale DNSSEC deployment

- If you've been in business for a while, your zones will have accumulated 'crust': manual additions, removals, changes etc, silent errors, **forgotten slaves**, 'floating glue', serving "auth" from glue, **strange load balancers**, wildcard NS records..
- DNSSEC will expose many of these issues, and may not react kindly
- Run (the equivalent) of 'pdnssec test-zones' before migrating
- Be **hypervigilant** about 'my domain no longer works' post-migration - this WILL happen.

Summarizing

- PowerDNS is an enthusiastic supporter of DNSSEC these days
- Very large scale migrations have already happened, in the most validating country in the world
  - There were hiccups, resolved in 3.1
  - Thanks to the active PowerDNS community!
- Any large scale DNSSEC migration will have issues, be hypervigilant, but generally things work!

POWERDNS

DNSSEC & PowerDNS
Large Scale DNSSEC Deployments

"lessons learned"
http://tinyurl.com/icann-powerdns

ICANN44, Prague

Bert Hubert
bert.hubert@netherlabs.nl
E.164: +31-622-440-095

POWERDNS