# VU#800113 & DNS UDP Src Port Randomization

## - Observations made at a TLD server -

Dublin, IEPG, 27 July 2008

**Peter Koch <koch@denic.de>**

# You‘ve heard that already …

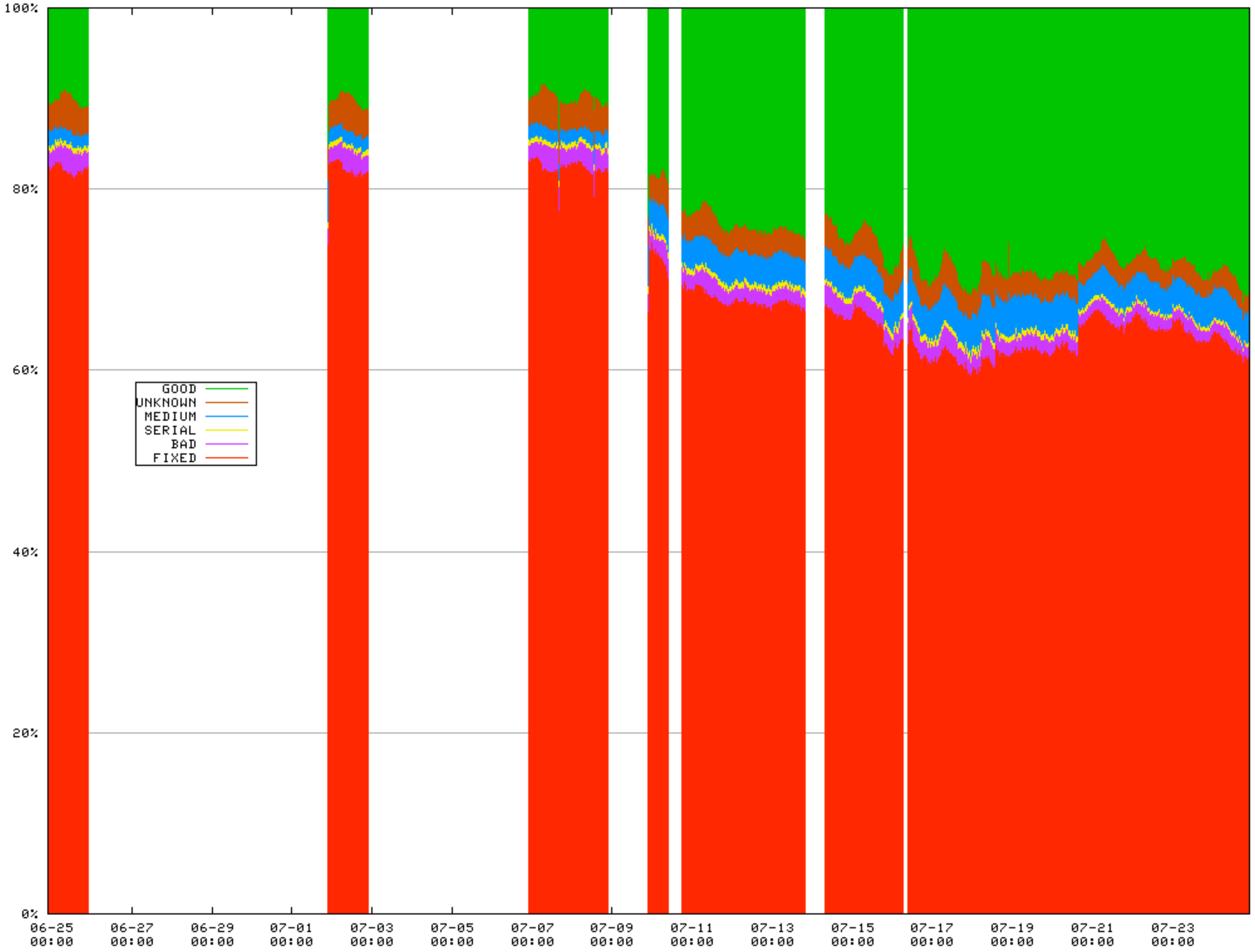
- VU#800113 is DNS Cache Poisoning reloaded
- Announced 8 July 2008
  - Together with various vendors‘ patches
- Interim countermeasure
  - DNS UDP Source Port Randomization
    - Originally proposed by Dan Bernstein
    - `draft-ietf-dnsext-forgery-resilience-XX.txt`
- Exploit code available (earlier than hoped)

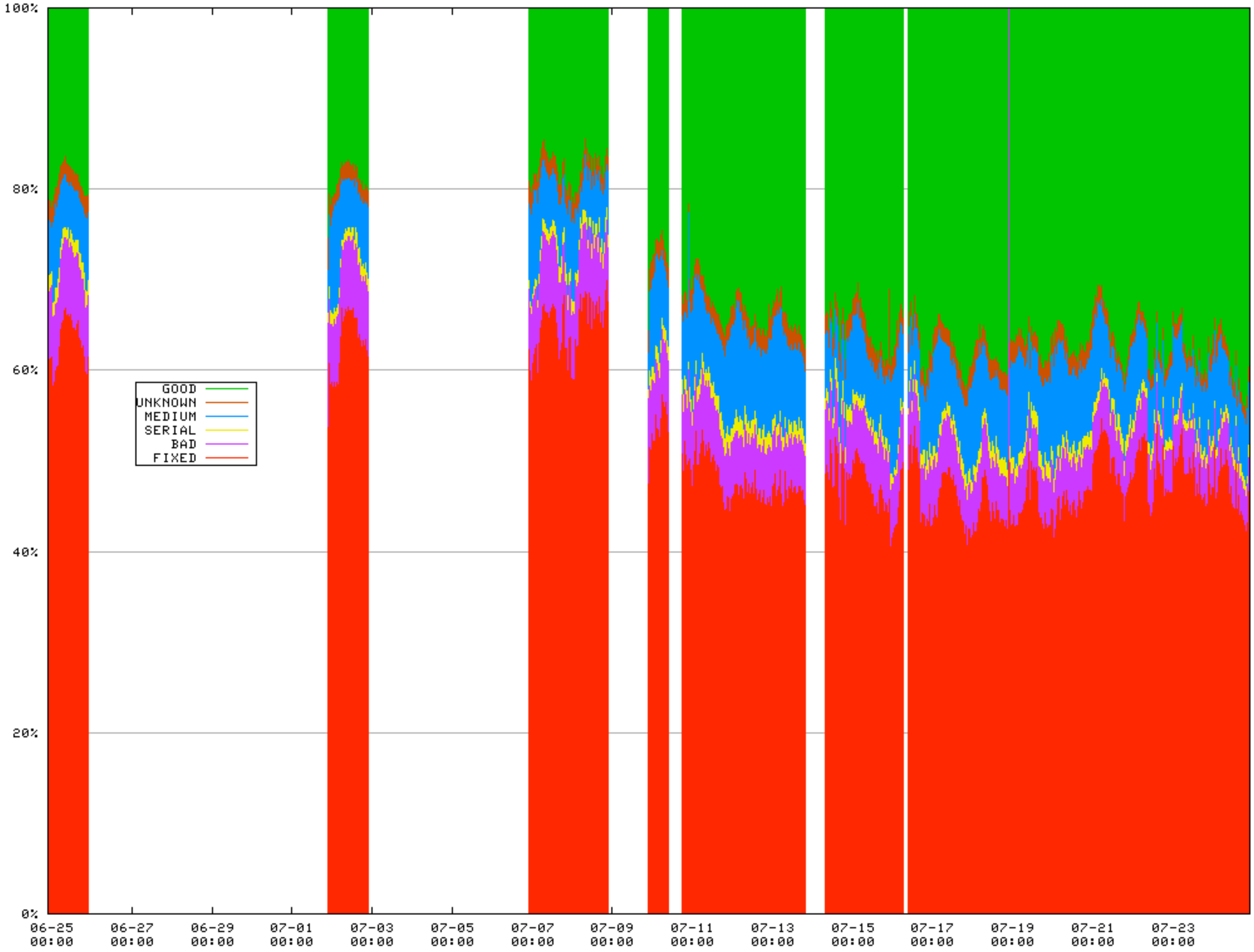
# (How) do people react?

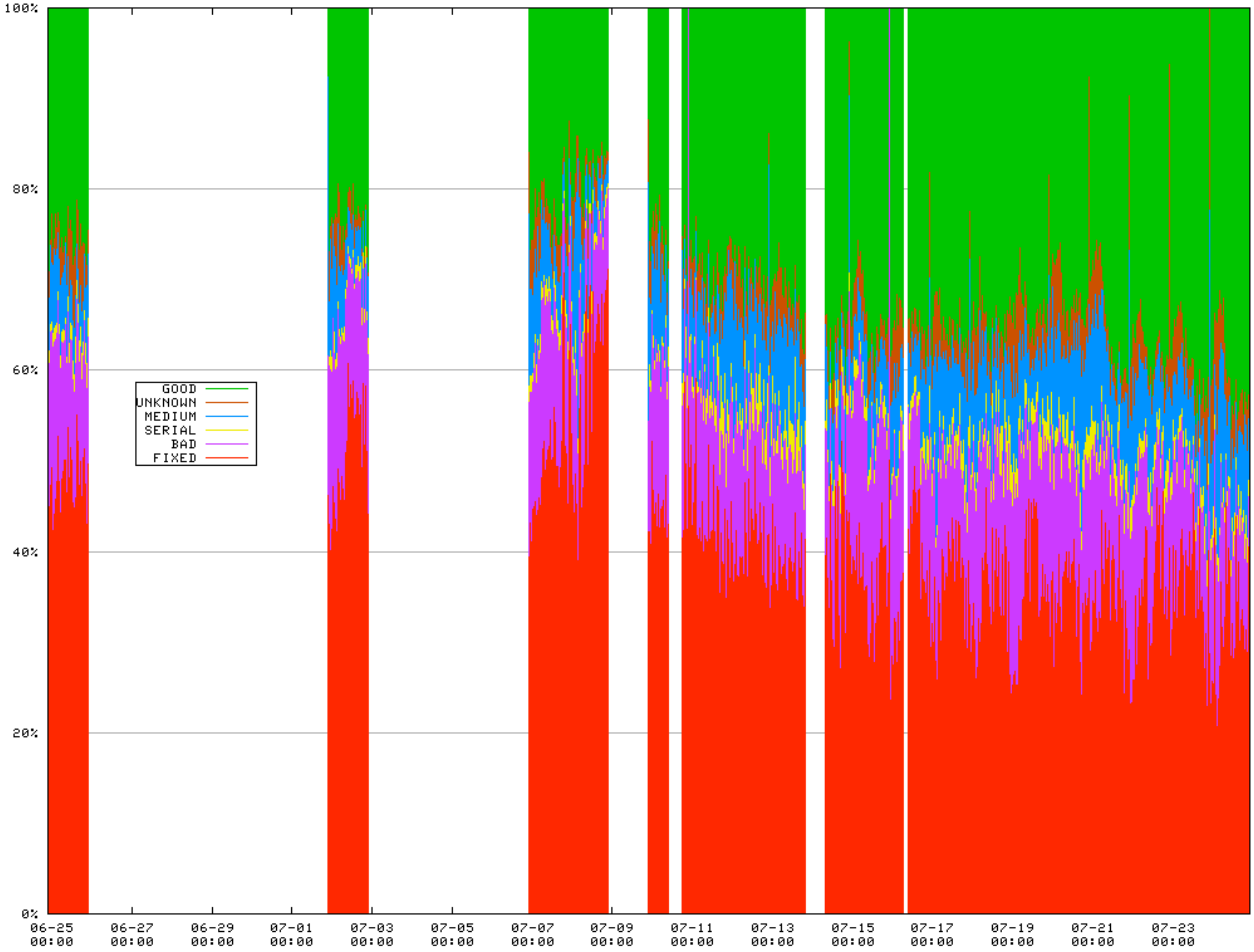
- Various advisories by CSIRTs, Vendors, DNS Community
- Online Test Tools made available by Dan Kaminski, OARC, and others
    - <https://www.dns-oarc.net/oarc/services/dnsentropy>
- Deployment observations by various parties
    - Dan, ISC-SIE, OARC
    - CERT.AT/NIC.AT
    - …

# Measurements at an auth DE TLD server

- Gathered traffic snapshots
  - Had to cope with „drop catching“ traffic
  - … and background noise
- Categorized Query Streams
  - FIXED, BAD, SERIAL, MEDIUM, UNKNOWN, GOOD
  - #ports/min(65536, #queries)
  - 1-(#ports-1)/delta
- Three graphs: all, > 0.1 q/s, > 1 q/s


100%
80%
60%
40%
20%
0%
GOOD
UNKNOWN
MEDIUM
SERIAL
BAD
FIXED
06-25 00:00
06-27 00:00
06-29 00:00
07-01 00:00
07-03 00:00
07-05 00:00
07-07 00:00
07-09 00:00
07-11 00:00
07-13 00:00
07-15 00:00
07-17 00:00
07-19 00:00
07-21 00:00
07-23 00:00


100%
80%
60%
40%
20%
0%
GOOD
UNKNOWN
MEDIUM
SERIAL
BAD
FIXED
06-25 00:00
06-27 00:00
06-29 00:00
07-01 00:00
07-03 00:00
07-05 00:00
07-07 00:00
07-09 00:00
07-11 00:00
07-13 00:00
07-15 00:00
07-17 00:00
07-19 00:00
07-21 00:00
07-23 00:00


100%
80%
60%
40%
20%
0%
GOOD
UNKNOWN
MEDIUM
SERIAL
BAD
FIXED
06-25 00:00
06-27 00:00
06-29 00:00
07-01 00:00
07-03 00:00
07-05 00:00
07-07 00:00
07-09 00:00
07-11 00:00
07-13 00:00
07-15 00:00
07-17 00:00
07-19 00:00
07-21 00:00
07-23 00:00

# Credits

- Duane Wessels, OARC, for using stddev as a quality measure
- Otmar Lendl and Aaron Kaplan, cert.at, for their work and discussing the port diversity quality function

# Fragen?

?

Thanks!

Peter Koch, DENIC eG

<koch@denic.de>
<http://www.denic.de>