Resolver Patch Statistics

OARC Amsterdam 2009 Workshop

Otmar Lendl <lendl@cert.at>

Reminder: July 8th, 2008: VU#800113

- Dire Warning
  - Insufficient entropy in ID
  - Multiple outstanding requests
  - Fixed source port
- Recommendation
  - Update Software
  - Implement Source Port Randomization
  - Restrict Recursion
  - Filter spoofed IP traffic

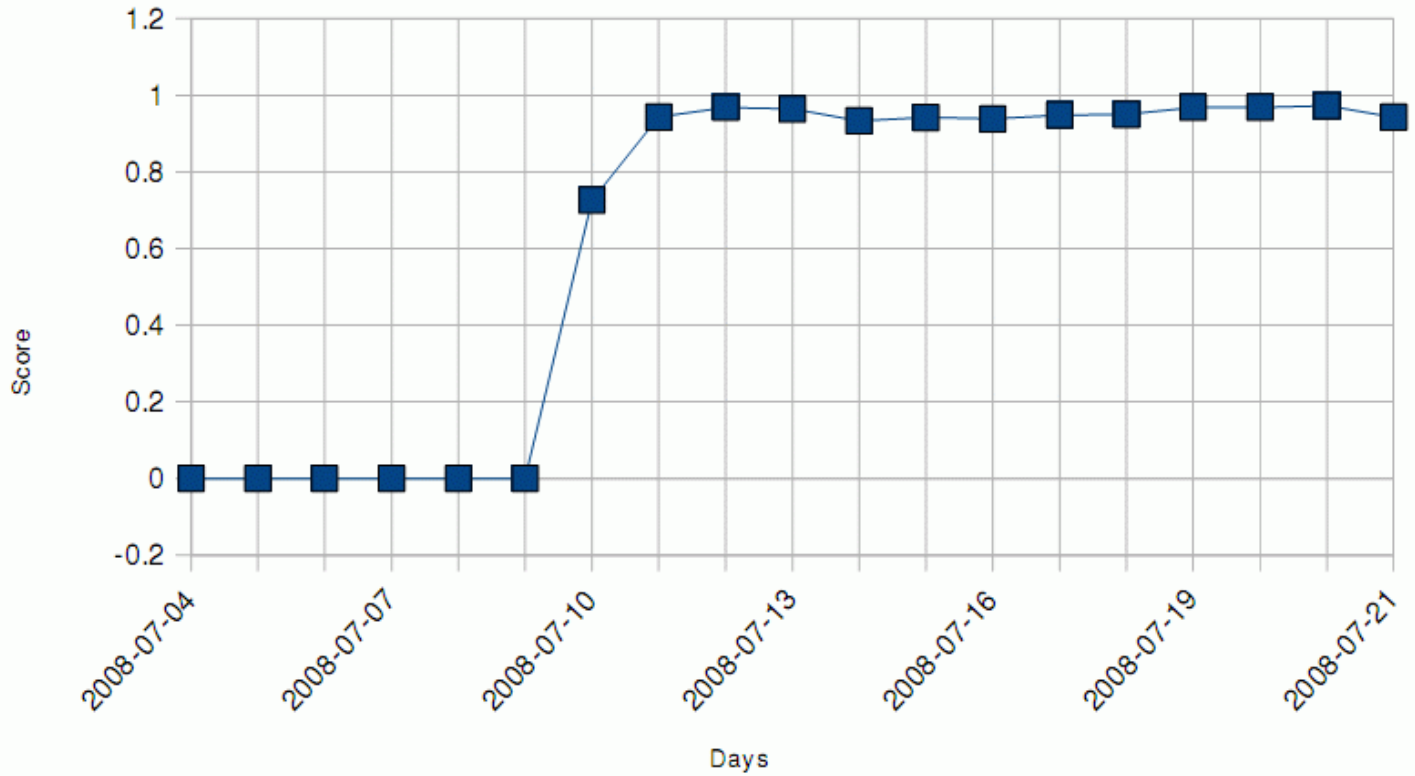
How did CERT.at react?

- Warnings on all channels
- Wait a second …
  - the patch changes the query pattern
  - important resolvers ask for a lot of domains
  - resolvers in Austria query for domains under .at
  - CERT.at is run by nic.at: we have query-logs of the .at nameservers

We can monitor the patching progress!

Scoring Resolvers

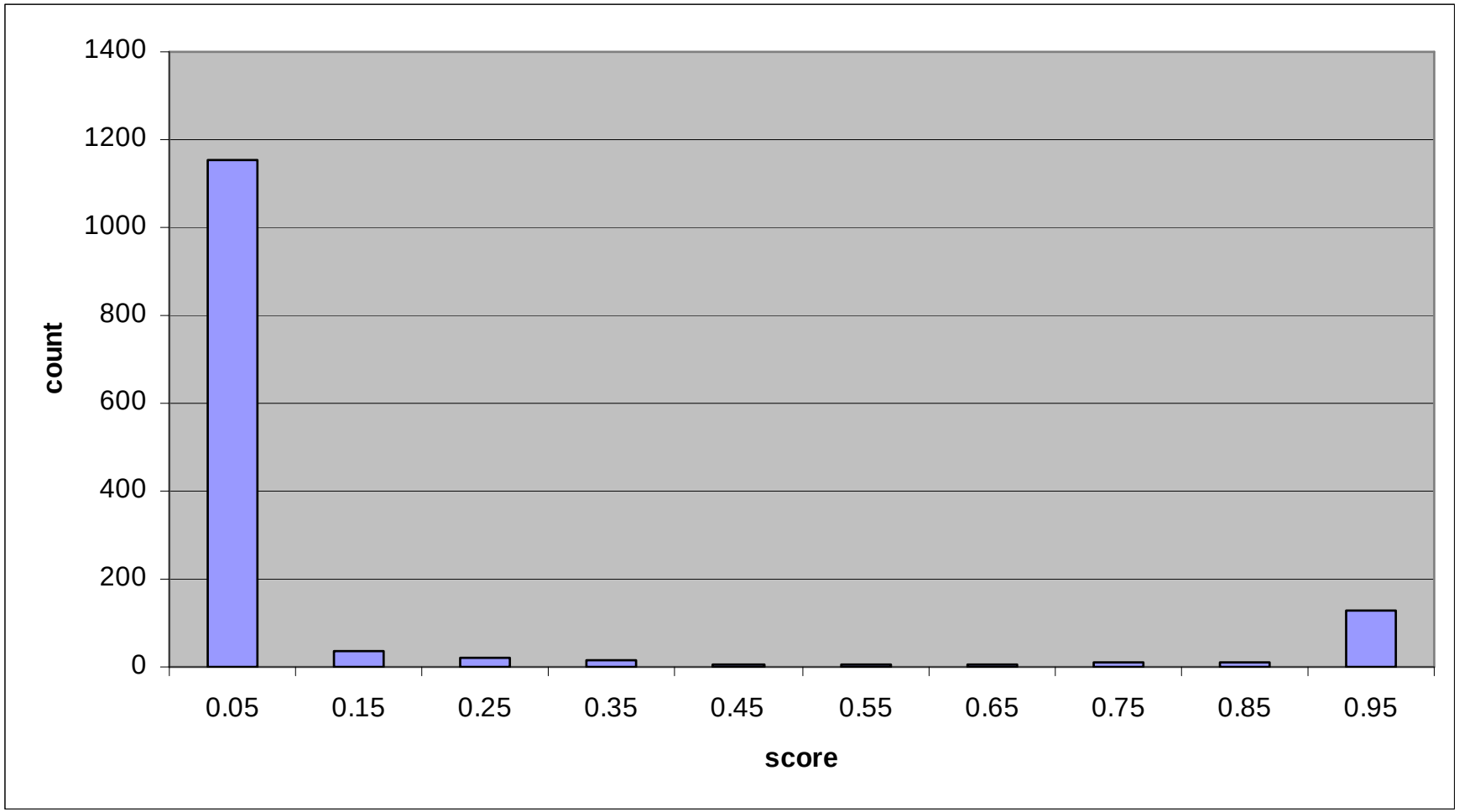
$$score = \frac{portchanges}{queries} * \frac{ports}{min(queries, 65536)}$$



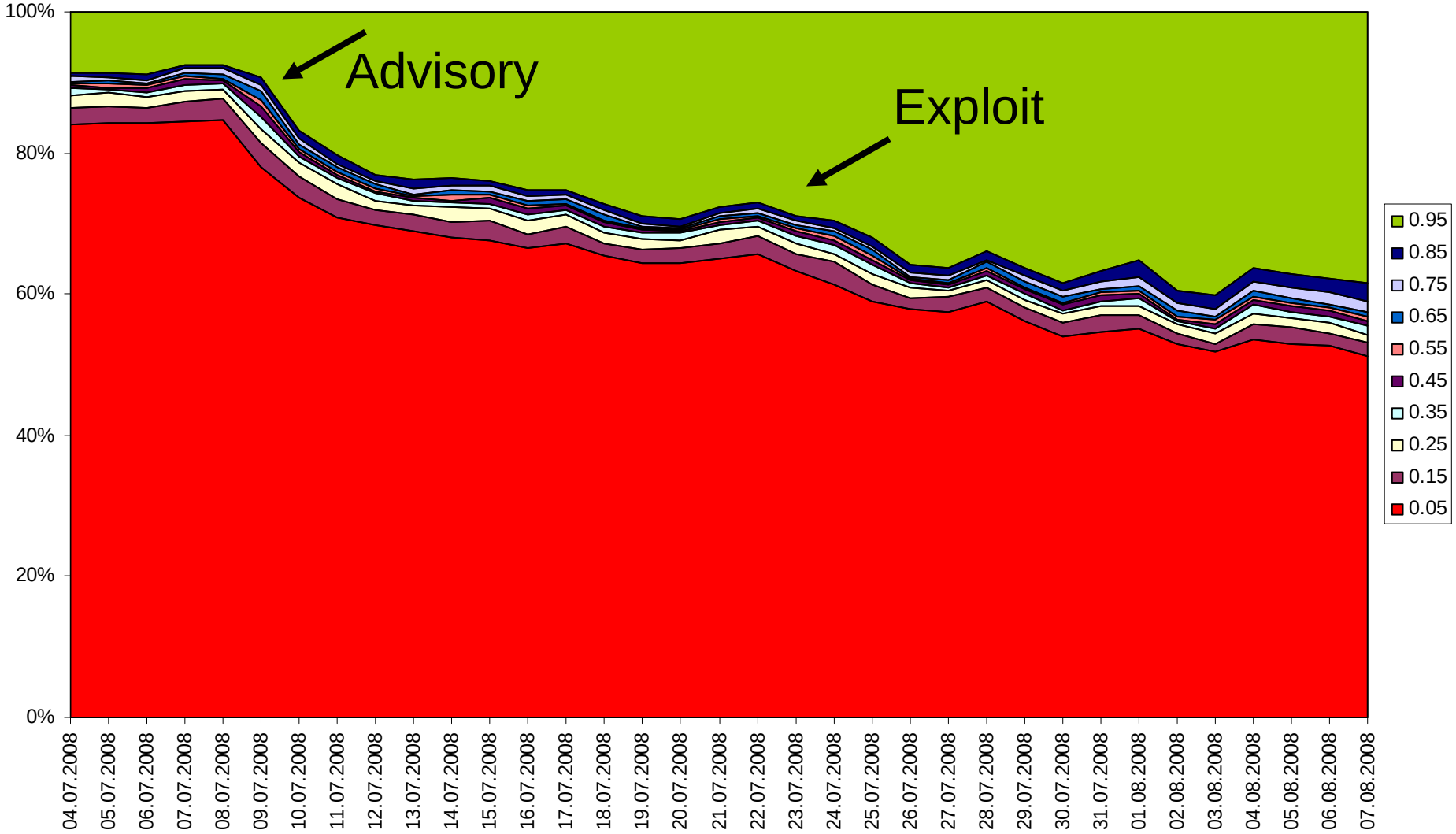
Data set

- Query log of one server in Austria
- ~ 10M queries / day (from Austrian IP space)
- from ~ 13.000 IP addresses
- ~2000 of which sent more than 100 queries
- Known domain catchers / registrars excluded
- Data starts with July 4th, i.e. before the announcements
- Still ongoing (with twice the data/day)

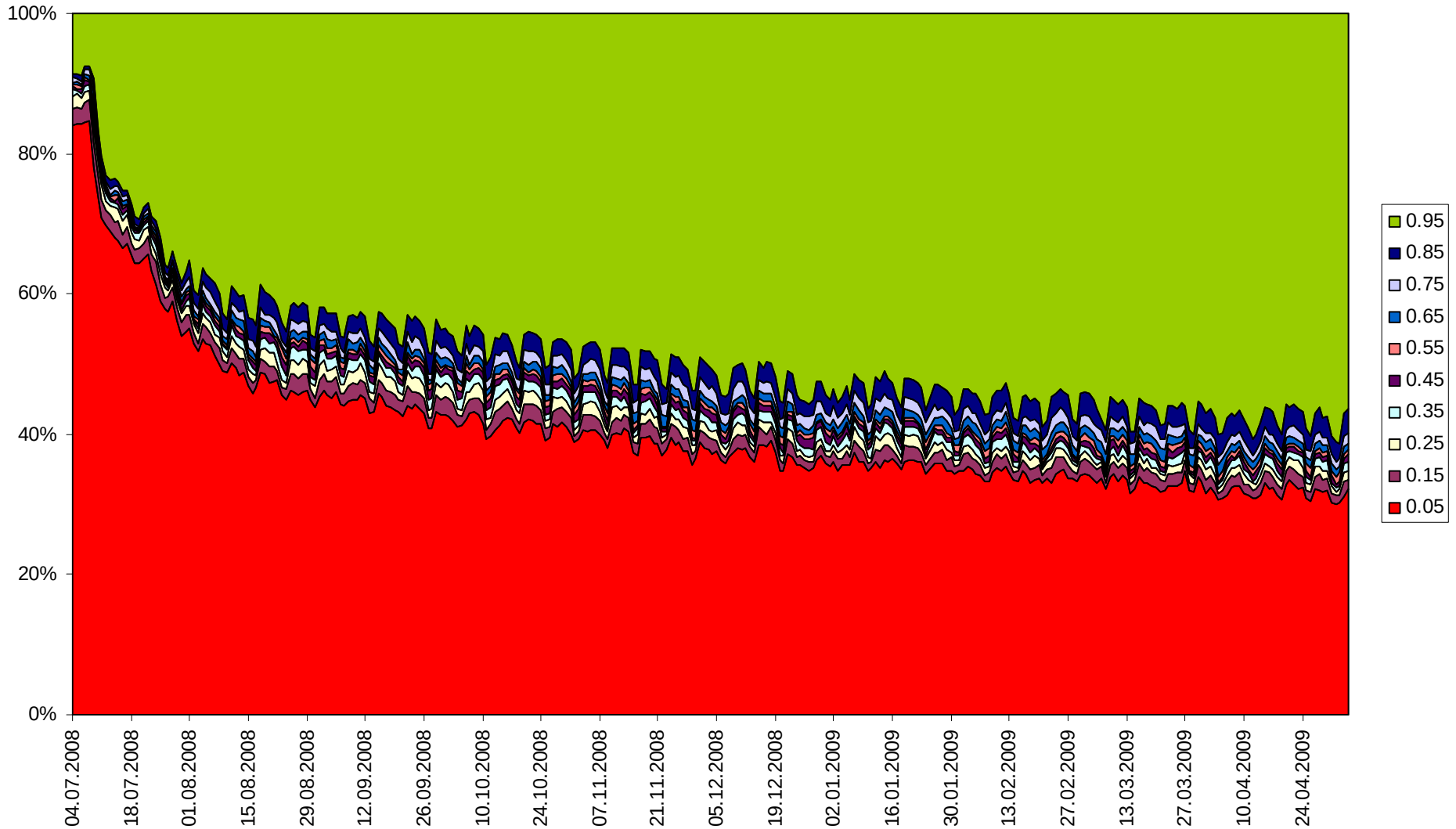
Before ..


1400
1200
1000
800
600
400
200
0
count
0.05
0.15
0.25
0.35
0.45
0.55
0.65
0.75
0.85
0.95
score

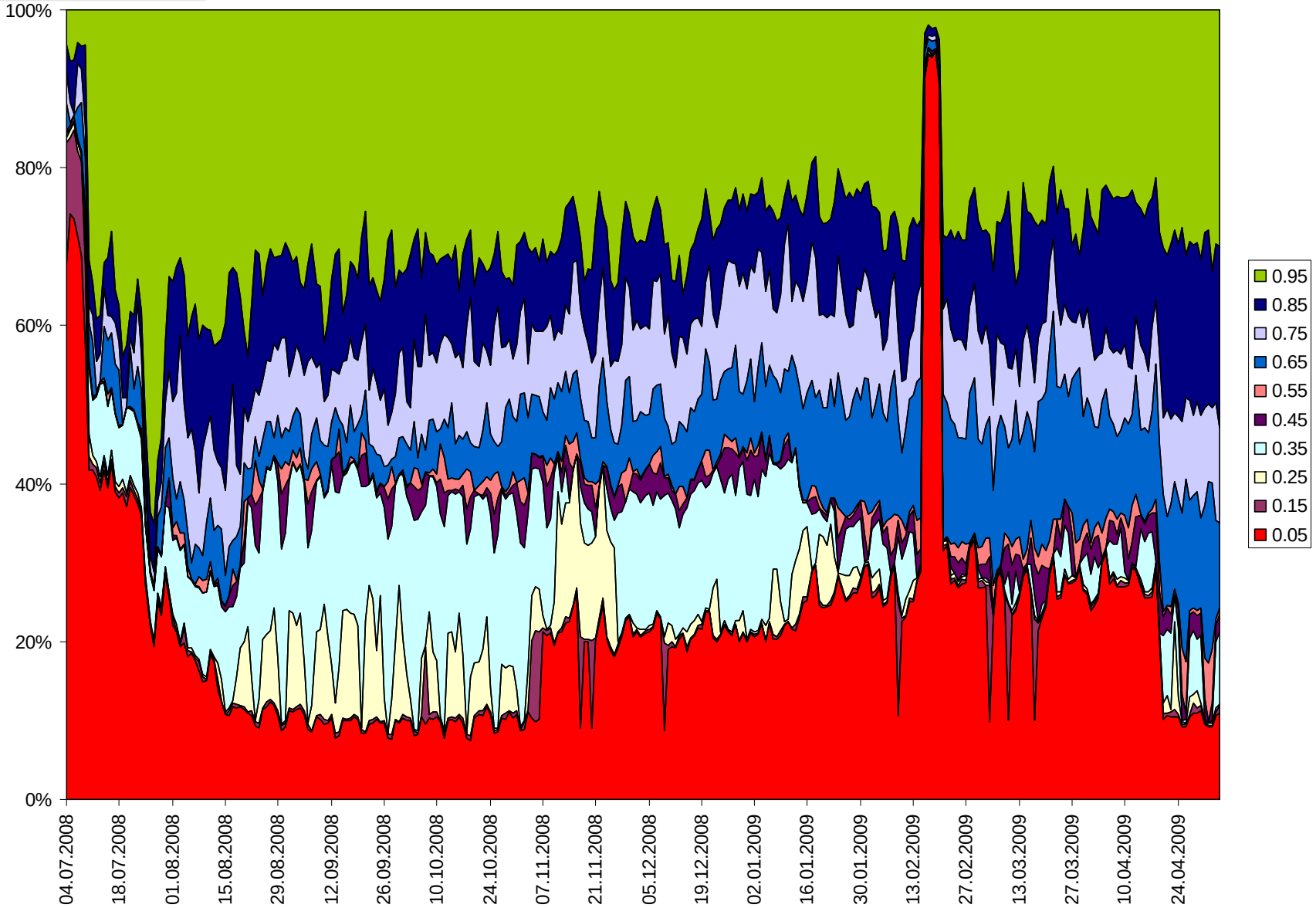
Patching by Server (short term)



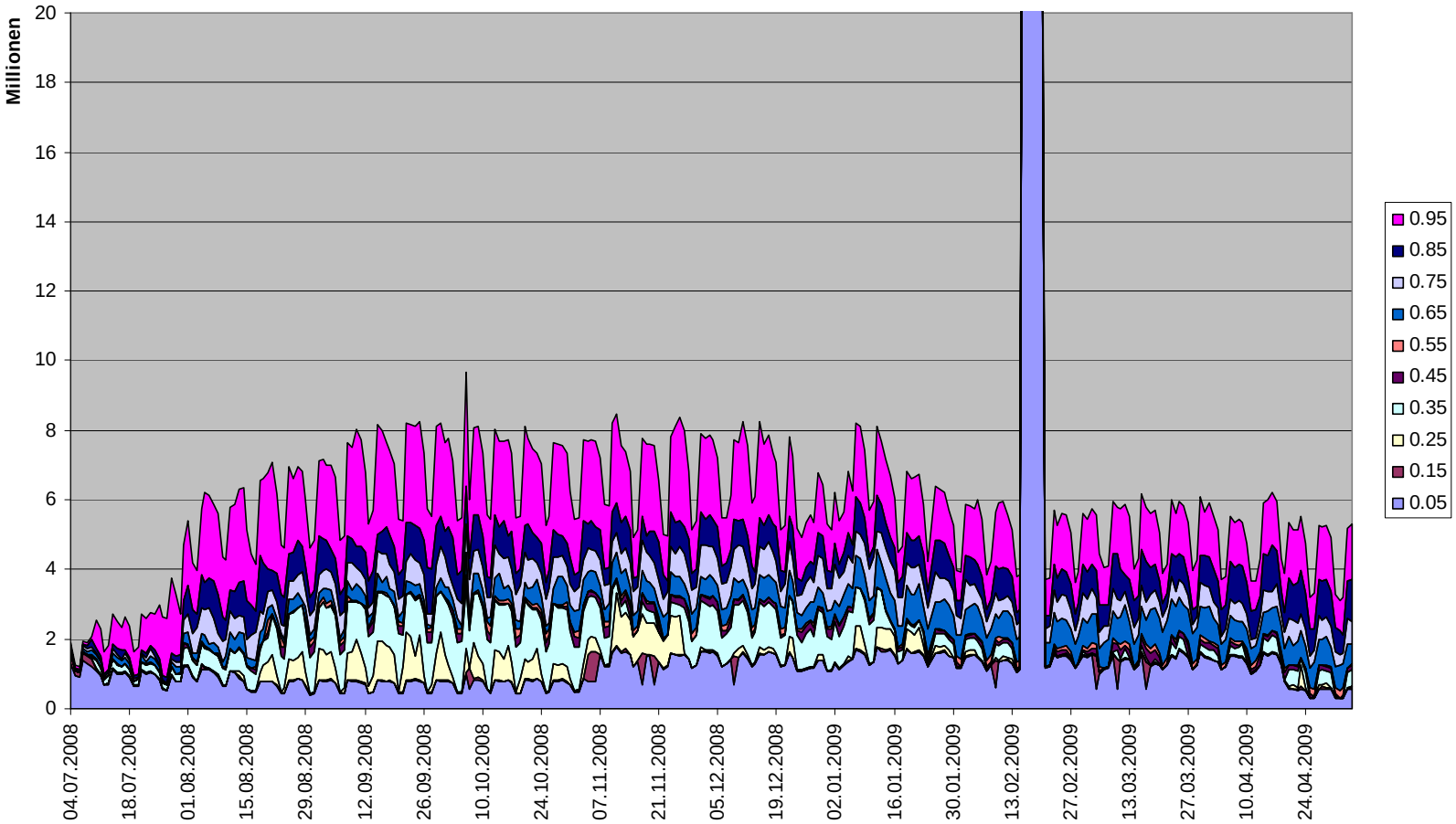
Patching by Server (long term)



By request, not by server:



Absolute numbers



Looks like a number of ISPs reworked their DNS setup over the summer.

Conclusions (1)

- By resolver vs. by request is a huge difference.
- Getting the big ISPs to patch was important (and rather easy).
- Getting all the NAT – Gateways, SME – servers (mail.<domain>.at), … patched is hard.

Conclusions (2)

- There is a huge installed base out there that is not well maintained.
- Many Nameservers seem to run in “installed once, never touched again”-mode
  - What does this mean for e.g. edns0-ping?
  - Do we have any chance of running DNSSEC in such an environment?