Sapphire/Slammer Worm

Impact on Internet performance

Work by Aldridge, Karrenberg, Uijterwaal & Wilhelm.

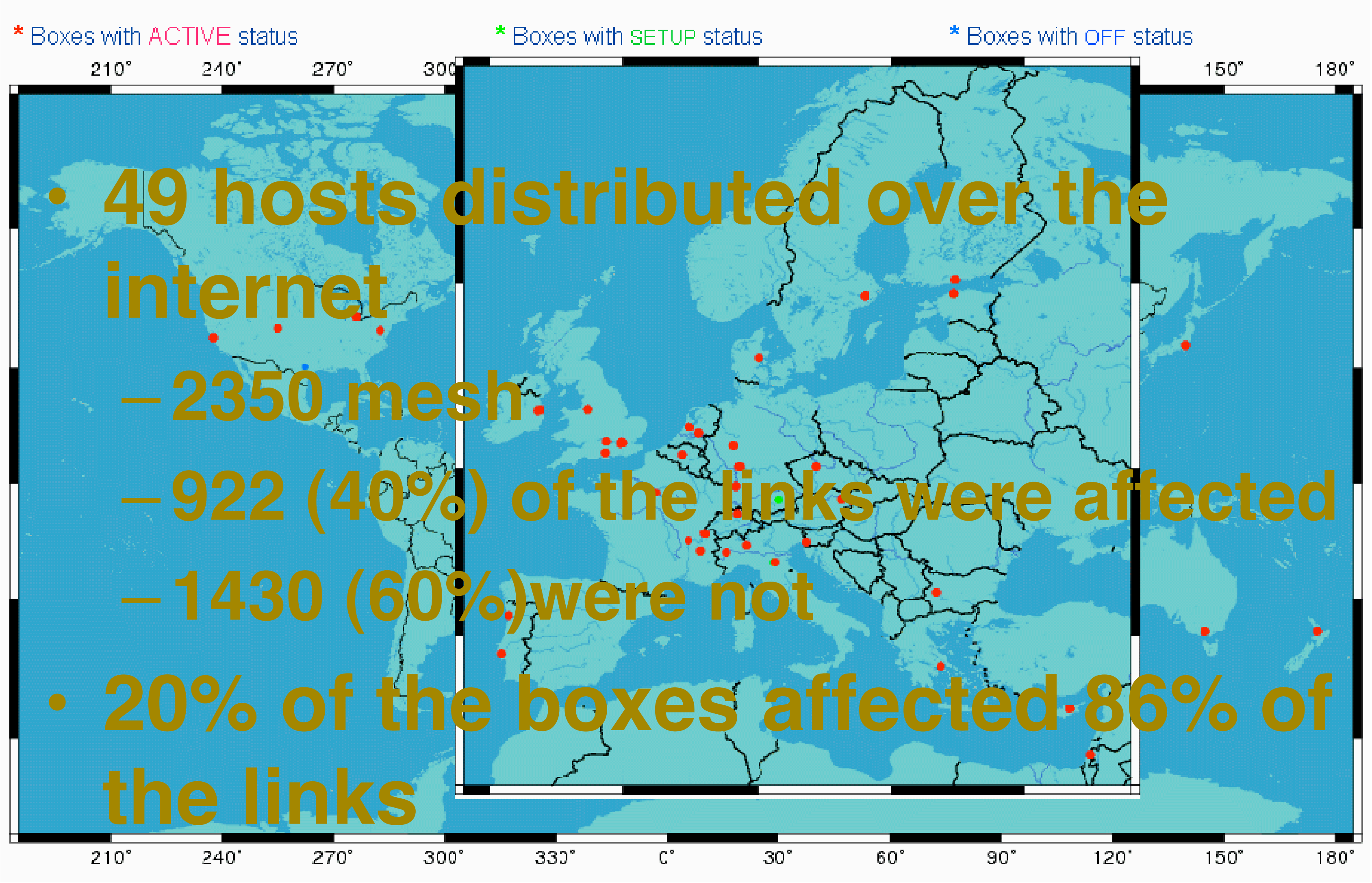
Presented by Olaf Kolkman

http://www.ripe.net/ttm/worm/

Sapphire, Slammer Worm

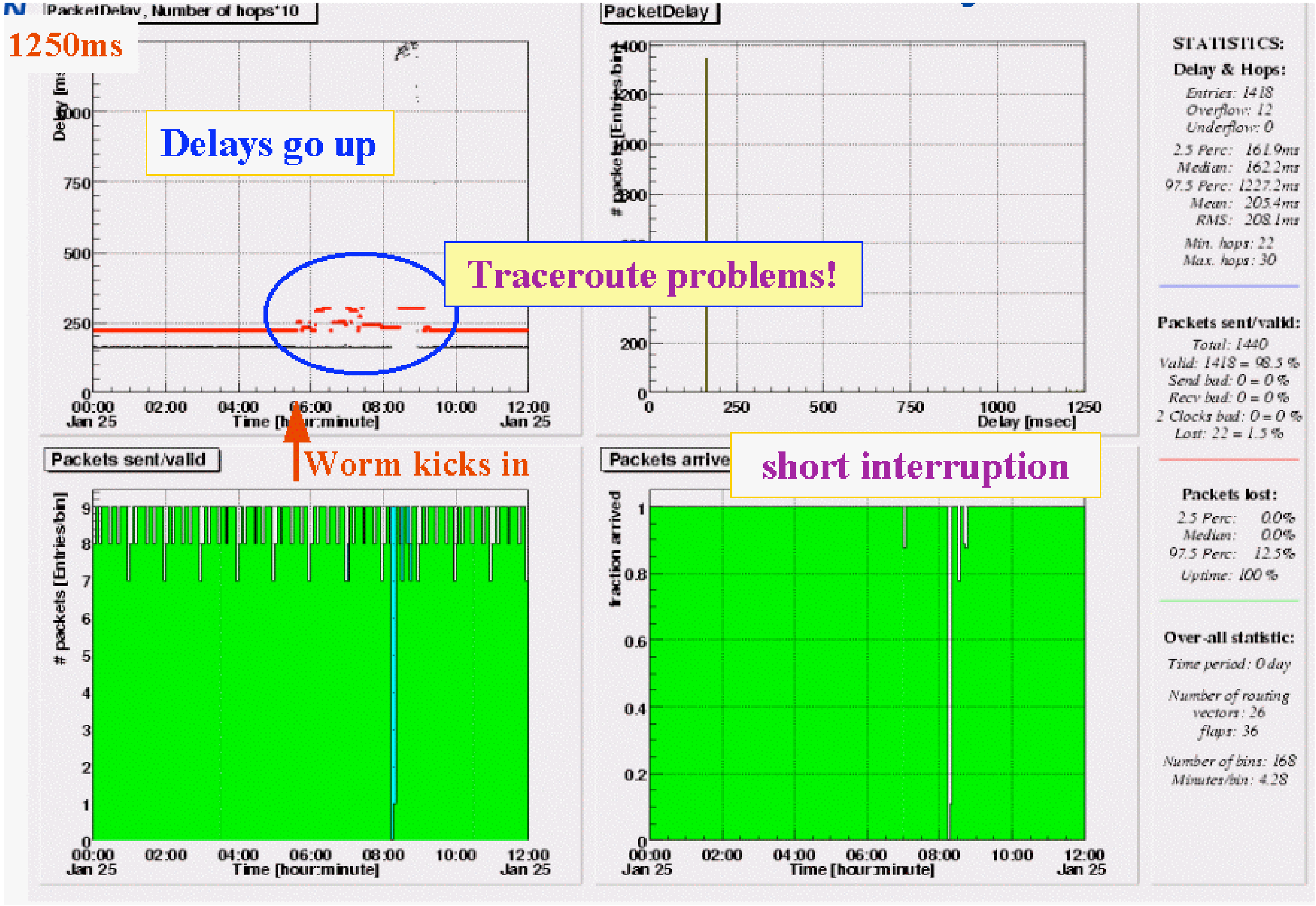
- Sapphire worm aka SQL Slammer
  - Microsoft SQL vulnerability exploit
  - Very aggressive rapid spread
  - Said to have an impact on Internet performance
- Analysis based on TTM, RIS and Route server monitoring.
  - Very rapid onset of observed effects
  - No major impact on the backbone
  - No problems with the root name server system (although 2 servers were affected)

TTM measurements



- 49 hosts distributed over the internet
  - 2350 mesh
  - 922 (40%) of the links were affected
  - 1430 (60%)were not
- 20% of the boxes affected 86% of the links

RIPE NCC to Tokyo test box



1250ms

Delays go up

Traceroute problems!

Worm kicks in

short interruption

STATISTICS:

Delay & Hops:

Entries: 1418
Overflow: 12
Underflow: 0

2.5 Perc: 161.9ms
Median: 162.2ms
97.5 Perc: 1227.2ms
Mean: 205.4ms
RMS: 208.1ms

Min. hops: 22
Max. hops: 30

Packets sent/valid:

Total: 1440
Valid: 1418 = 98.5 %
Send bad: 0 = 0 %
Recv bad: 0 = 0 %
2 Clocks bad: 0 = 0 %
Lost: 22 = 1.5 %

Packets lost:

2.5 Perc: 0.0%
Median: 0.0%
97.5 Perc: 12.5%
Uptime: 100 %

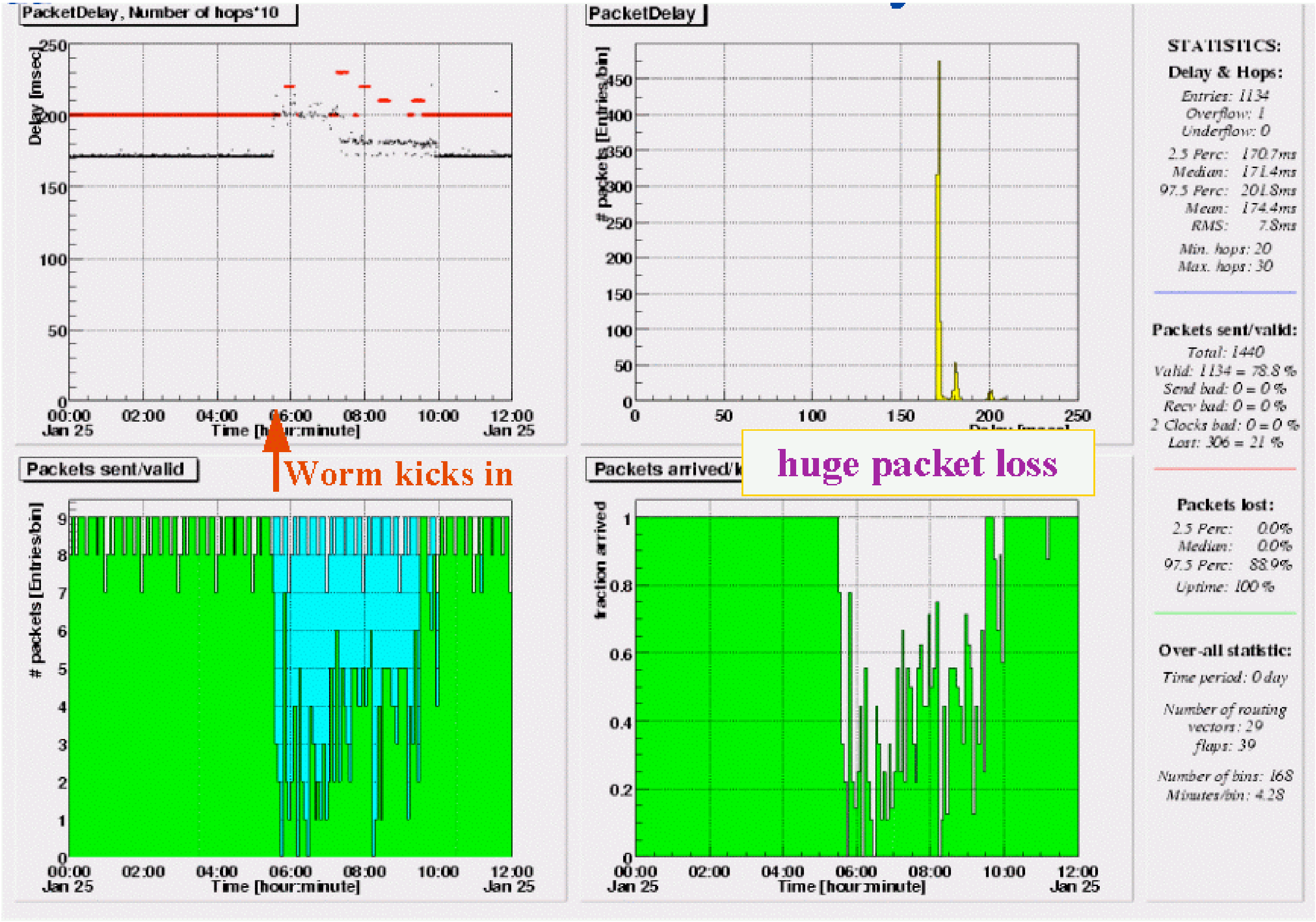
Over-all statistic:

Time period: 0 day

Number of routing vectors: 26
flaps: 36

Number of bins: 168
Minutes/bin: 4.28

Tokyo to RIPE NCC testbox



Worm kicks in

huge packet loss

STATISTICS:

Delay & Hops:

Entries: 1134
Overflow: 1
Underflow: 0

2.5 Perc: 170.7ms
Median: 171.4ms
97.5 Perc: 201.8ms
Mean: 174.4ms
RMS: 7.8ms

Min. hops: 20
Max. hops: 30

Packets sent/valid:

Total: 1440
Valid: 1134 = 78.8 %
Send bad: 0 = 0 %
Recv bad: 0 = 0 %
2 Clocks bad: 0 = 0 %
Lost: 306 = 21 %

Packets lost:

2.5 Perc: 0.0%
Median: 0.0%
97.5 Perc: 88.9%
Uptime: 100 %

Over-all statistic:

Time period: 0 day

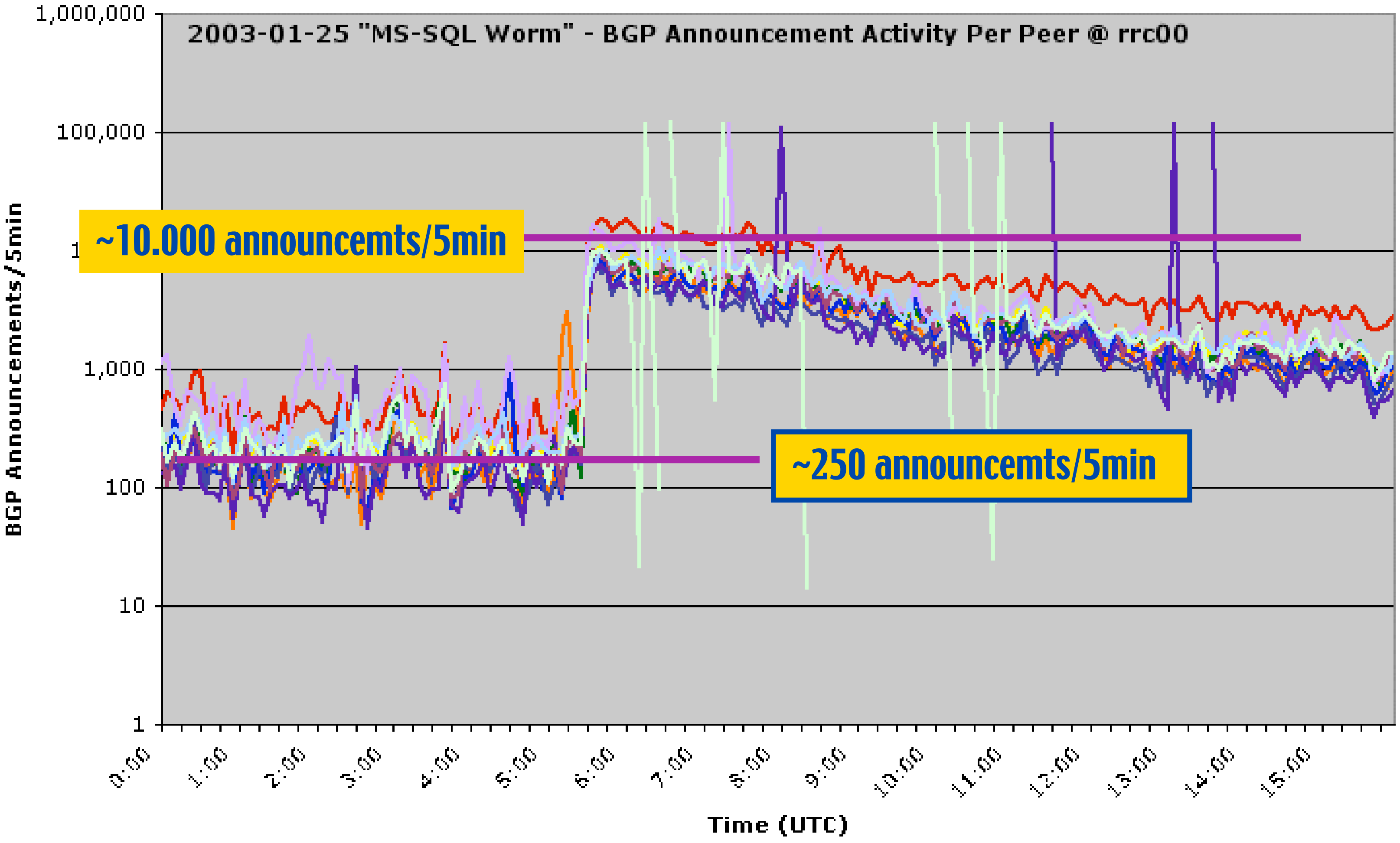
Number of routing vectors: 29
flaps: 39

Number of bins: 168
Minutes/bin: 4.28

Routing information service

- 9 Route collectors, 1 in Japan, 1 in US, others in Europe. All except 1 have a full BGP feed
- All saw about 1-2 orders of magnitude increase in announcements
- It is not clear if specific routes were invisible in the global routing table during the time of increased activity

RRC00 BGP announcements



~10.000 announcemts/5min

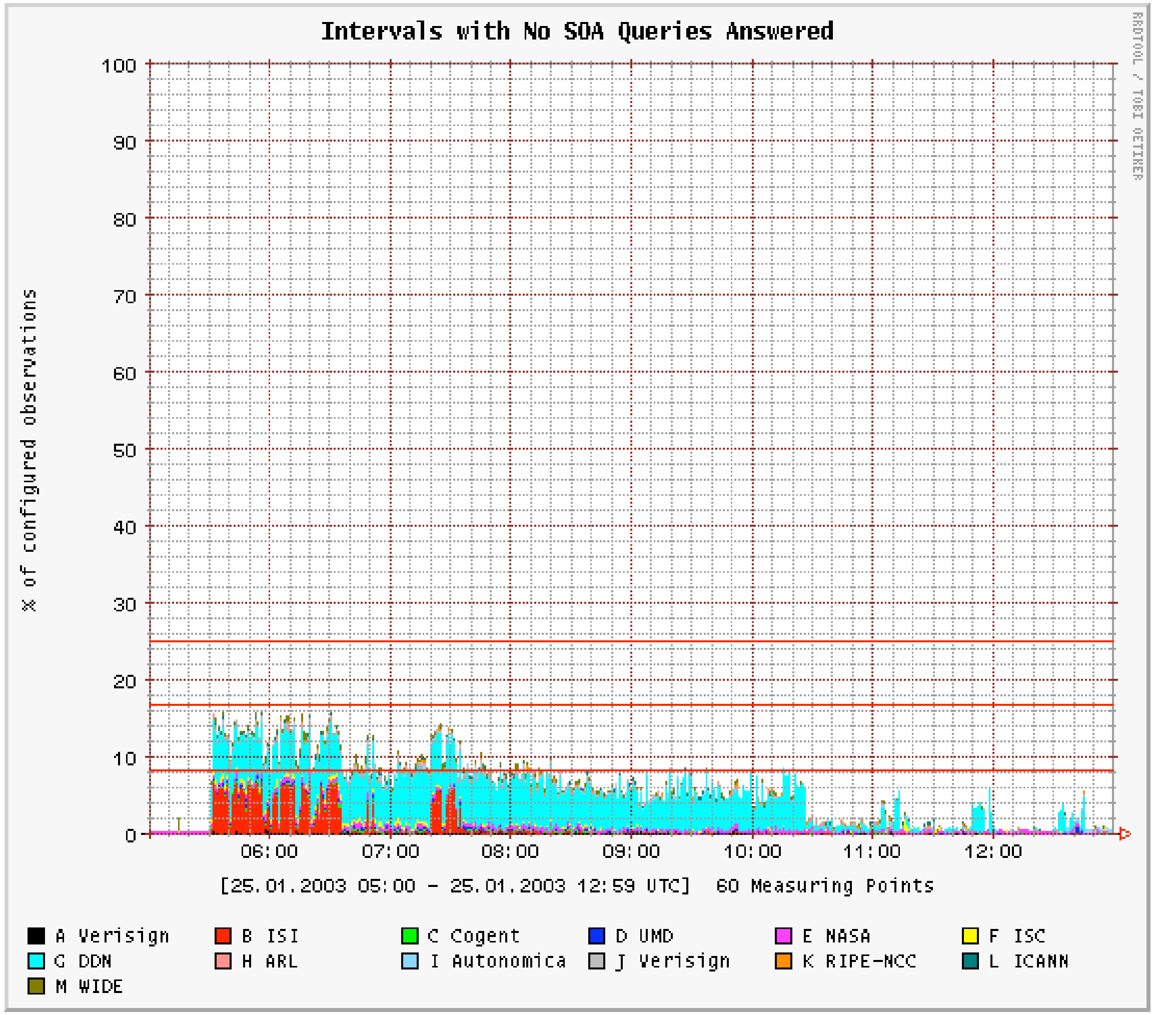
~250 announcemts/5min

Root server monitoring

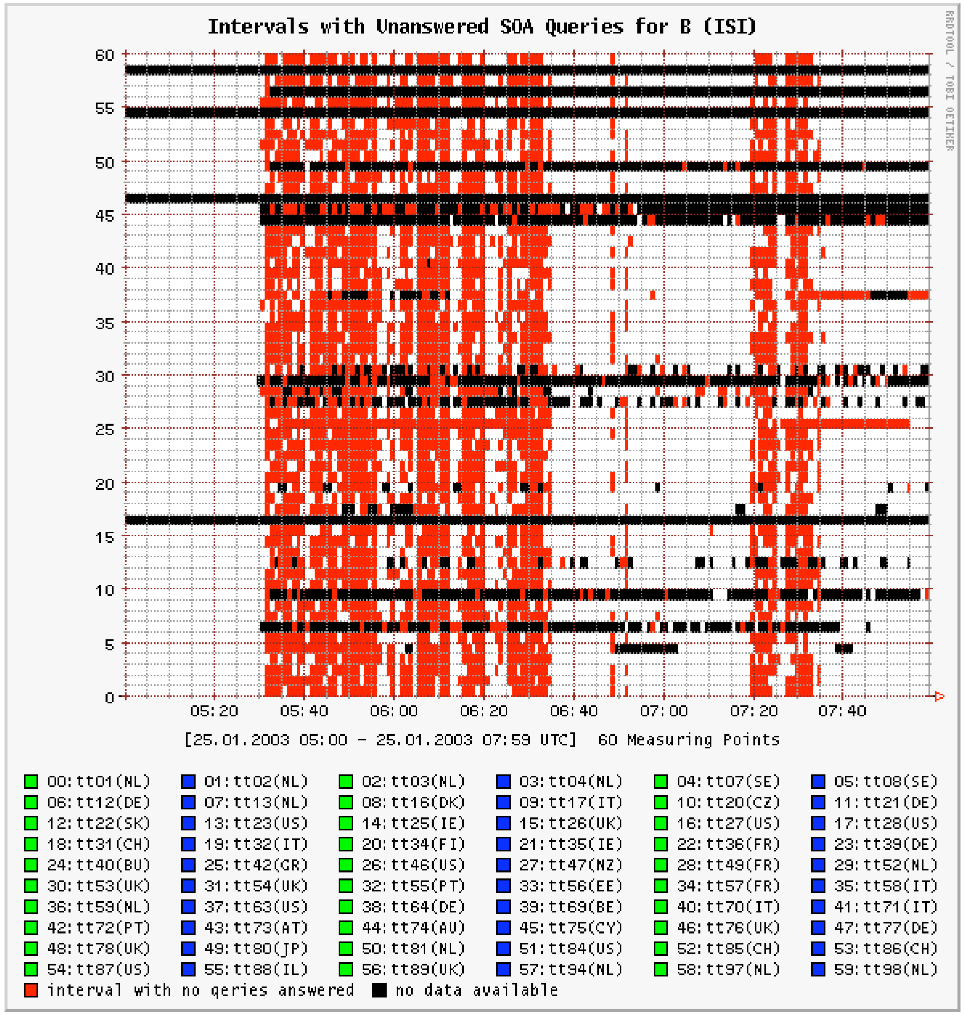
- 60 probe host; worldwide but most in Europe
- 1 measurement per minute.
  - SOA query

- From probe’s perspective 2 root servers were affected.
  - Most probably connectivity problems close to the servers
  - No effect whatsoever towards the other servers.
    - The DNS system did _not_ suffer.

Root server monitoring cumulative



B as seen by 60 probes



Conclusions

- The Internet did not show a global meltdown
- 60% of the test-box relations were not affected
  - Backbone not affected
  - Problems localized at edge networks and their immediate upstreams
- No impact on the root-server service
  - 2 out of 13 servers had problems.
- The data routinely collected can help to distinguish global from localised problems
  - RIPE NCC wants to provide this data real-time

http://www.ripe.net/ttm/worm/