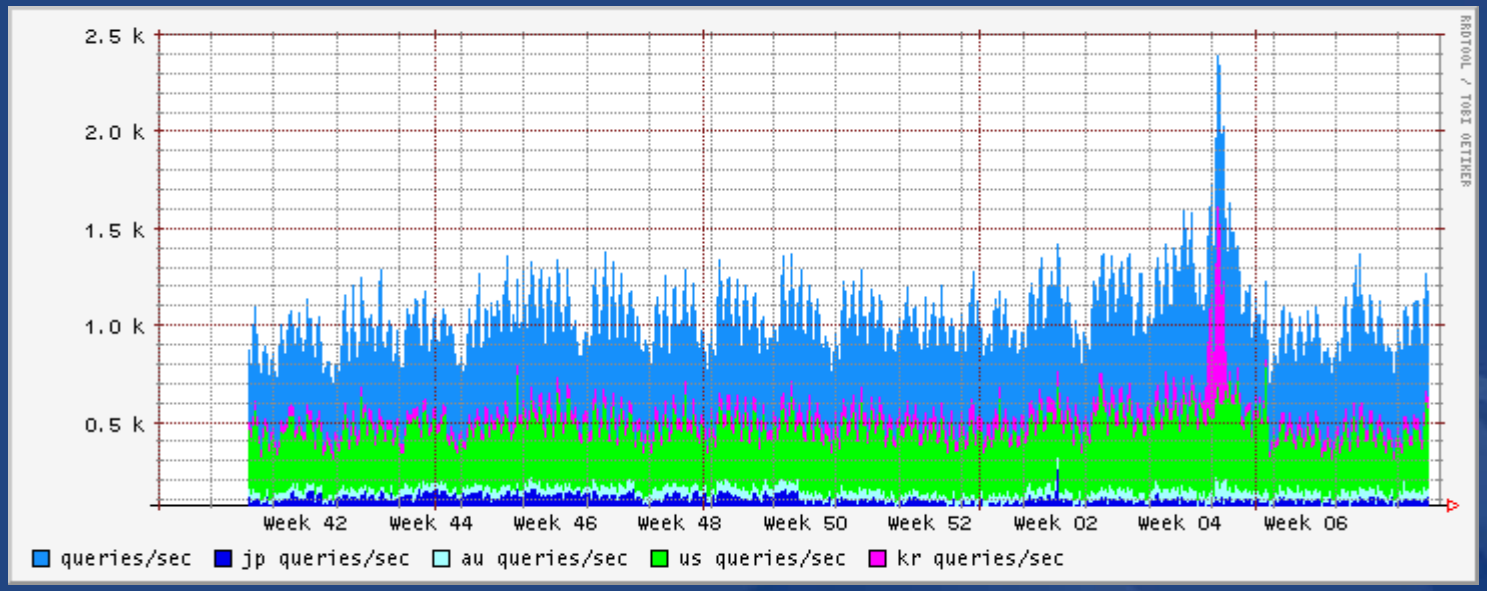
Reverse DNS traffic during the 'slammer' worm incident

DNS OPS SIG

APNIC 15 Taipei, Taiwan

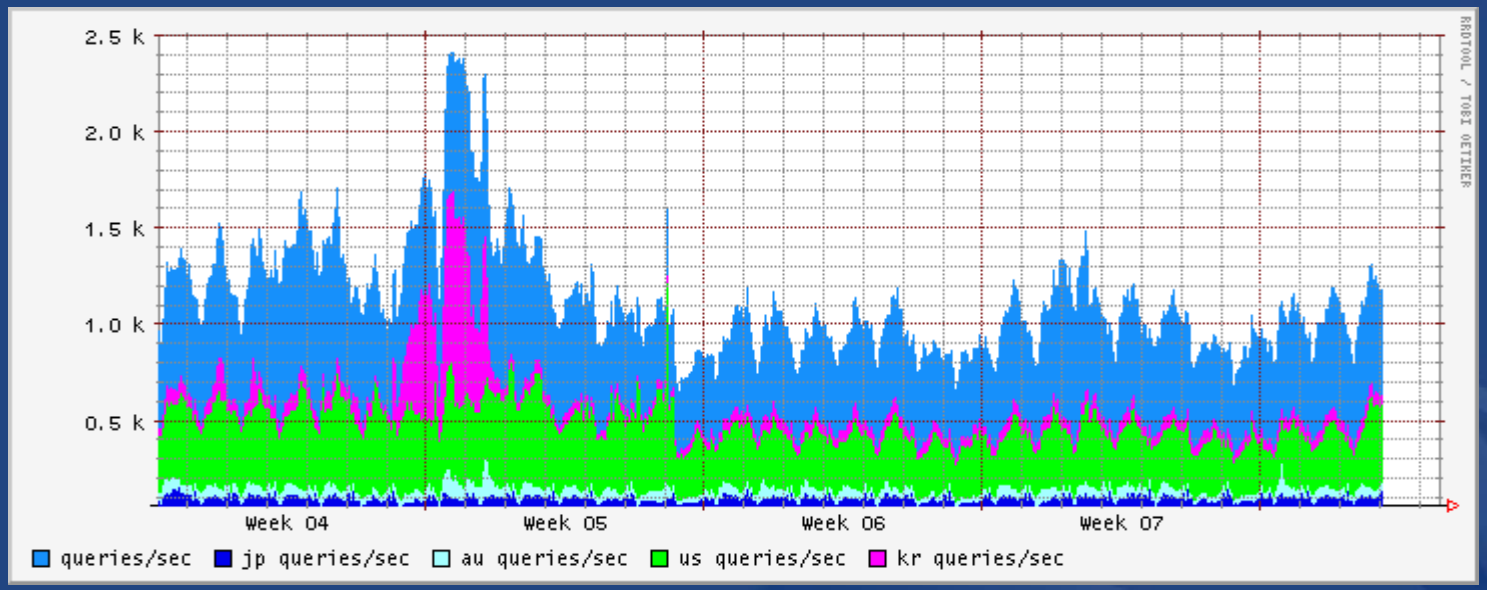
26 February 2003

Longterm trends



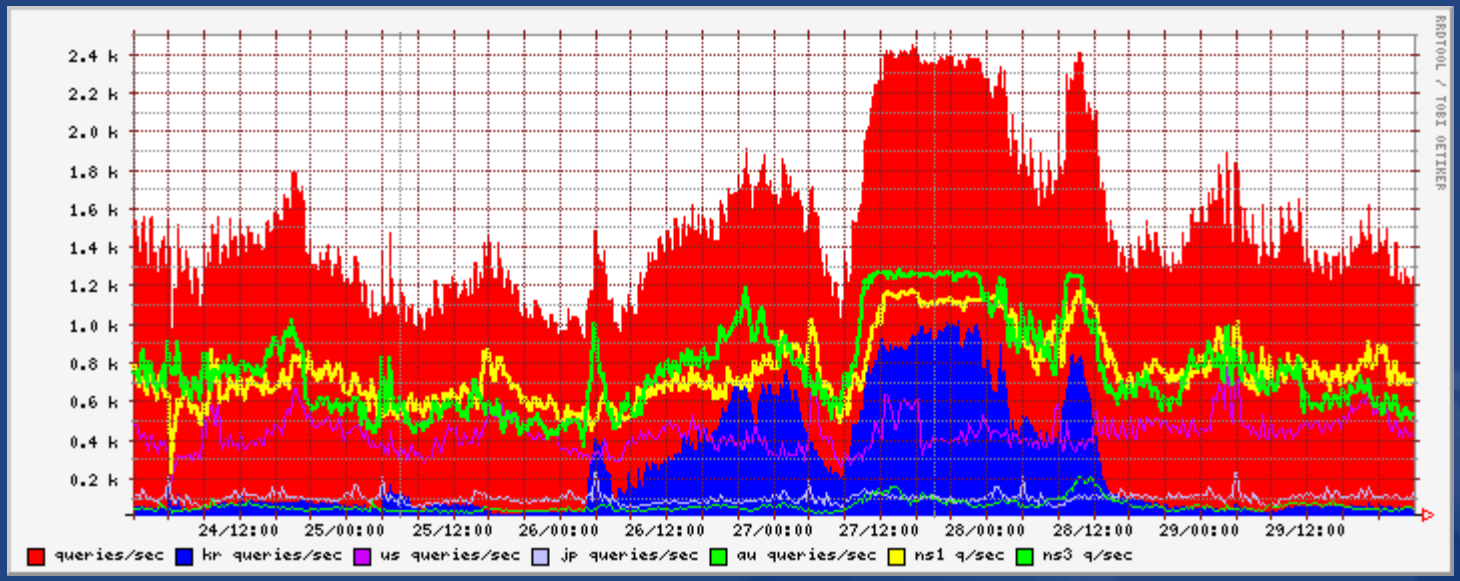
- Stable longterm DNS behaviour
  - Strong daily cycle pattern
  - No major variances day-to-day
- 'Slammer' incident stands out
  - Double load on APNIC DNS servers

Slammer attack on .KR



- Normal .KR load less than 100 query/sec
- During Slammer, peaked at 2,400 query/sec
  - Exceeded US mainstream load
- Two spikes
  - Probably side-effects of in-country firefighting

Zooming in to the day-view



- Cisco assisting with remediation during attack
  - Sub-events probably filtering and server disconnects
- 'flatline' not due to bandwidth limits at APNIC
  - Japan DNS server at NSPIXP2

Where did dns load come from?

- Normal load is from intermediate caching resolvers re-freshing cache for /8
- May be failover load as in-country DNS systems failed under load
- May be 'lame DNS' query load as end ISPs take systems offline
- Further study, logfile analysis needed

Impact on services

- No impact on APNIC reverse DNS
  - Scaled to cope with significantly greater DNS load than longterm trend, observed peaks
- Impact in-country probably greater
  - APNIC only sees 'passing through' refresh load plus LAME DNS impact