

The recursive DNS rant

@ UKNOF 15

Security

- Dan Kaminsky's "Multiple DNS implementations vulnerable to cache poisoning" – 2008-07



- We've known this for a long time
- DNSSEC is the solution, but until then...

RFC5452 – 2009-01

“Measures for Making DNS More Resilient
against Forged Answers “

- Query Matching rules
- Extending the Q-ID space using ports and addresses
- Spoof detection and countermeasures

Did you implement any of this?

IETF Drafts

draft-vixie-dnsexp-dns0x20-00.pdf – 2008-03

- www.google.com anyone ?

draft-barwood-dnsexp-fr-resolver-mitigations-08 – 2008-10

- Query repetition
- 0x20
- Random source port
- Random nonce prepending
- Maintain bad IDs count
- Use calculated entropy

Public recursive DNS

Google Public DNS – 8.8.8.8, 8.8.4.4

- Shared cache
- Prefetching
- 0x20
- Nonce prepending

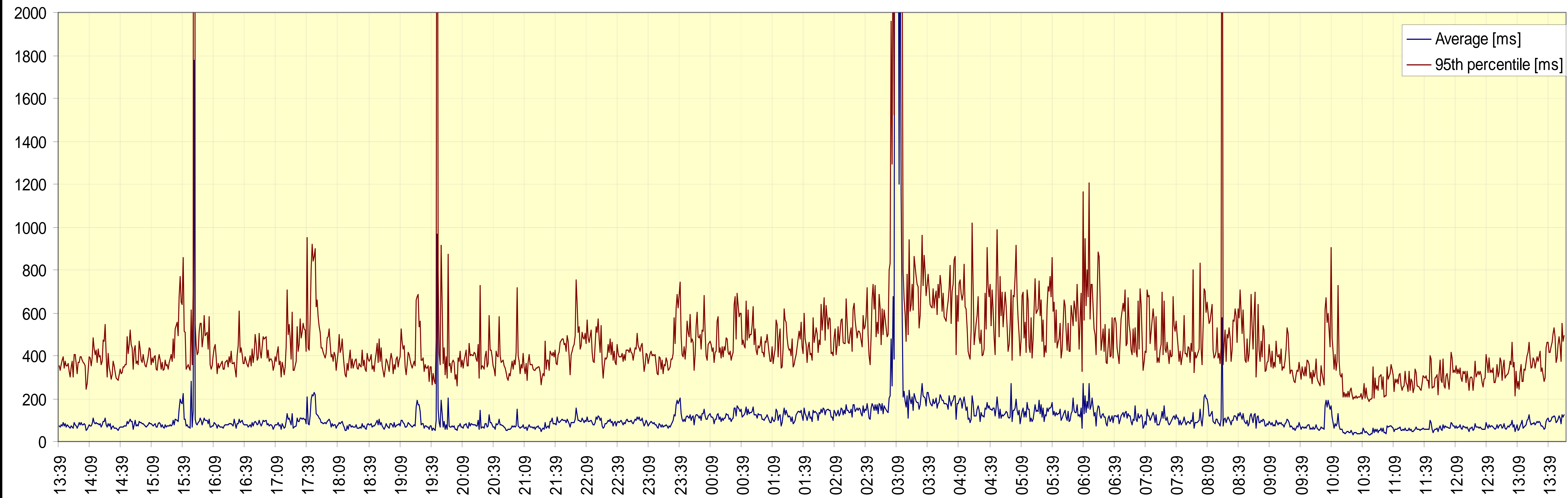
OpenDNS

DynDNS / Internet Guide

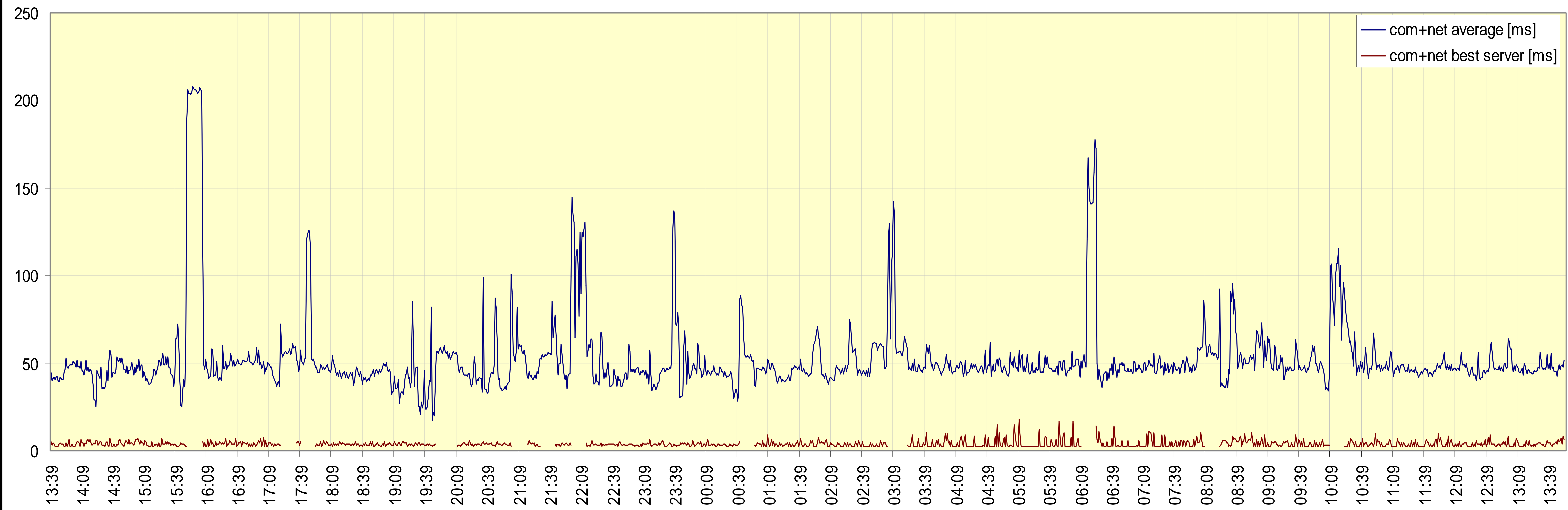
Neustar / DNS Advantage

And many more...

Reponse time for valid responses



COM+NET zones best server response time vs. average response time



How can we improve this?

- Prefetching
- Shared cache

- Better choice of servers to talk to
- Local copies of Root/TLDs

Boyan Krosnov
boyan@krosnov.org
+44 7588 865 702