Hunt for the DNS Anomalies

CZ.NIC Labs
Ondřej Surý
ondrej.sury@nic.cz
4. 5. 2011

cz nic
cz domain registry

Detecting hidden anomalies in DNS

- Work based on:
  - Extracting Hidden Anomalies using Sketch and Non-Gaussian Multi-resolution Statistical Detection Procedures by Guillaume Dewaele, Kensuke Fukuda, Pierre Borgnat, Patrice Abry and Kenjiro Cho
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.130.6104&rep=rep1&type=pdf
- Modified for work with DNS traffic
  - The original paper works with IP networks

Steps used in the method

- Random projections and Time aggregation
  - Assign a packet to a sketch using a hash
  - Time aggregate at various levels
- Statistical Modelling
  - Using Gamma distribution
- Statistical Reference and Statistical Distance
  - Reference parameters are compared to Sketches.
  - Sketches with distance above threshold are anomalous
- Repeat with different hash and intersect

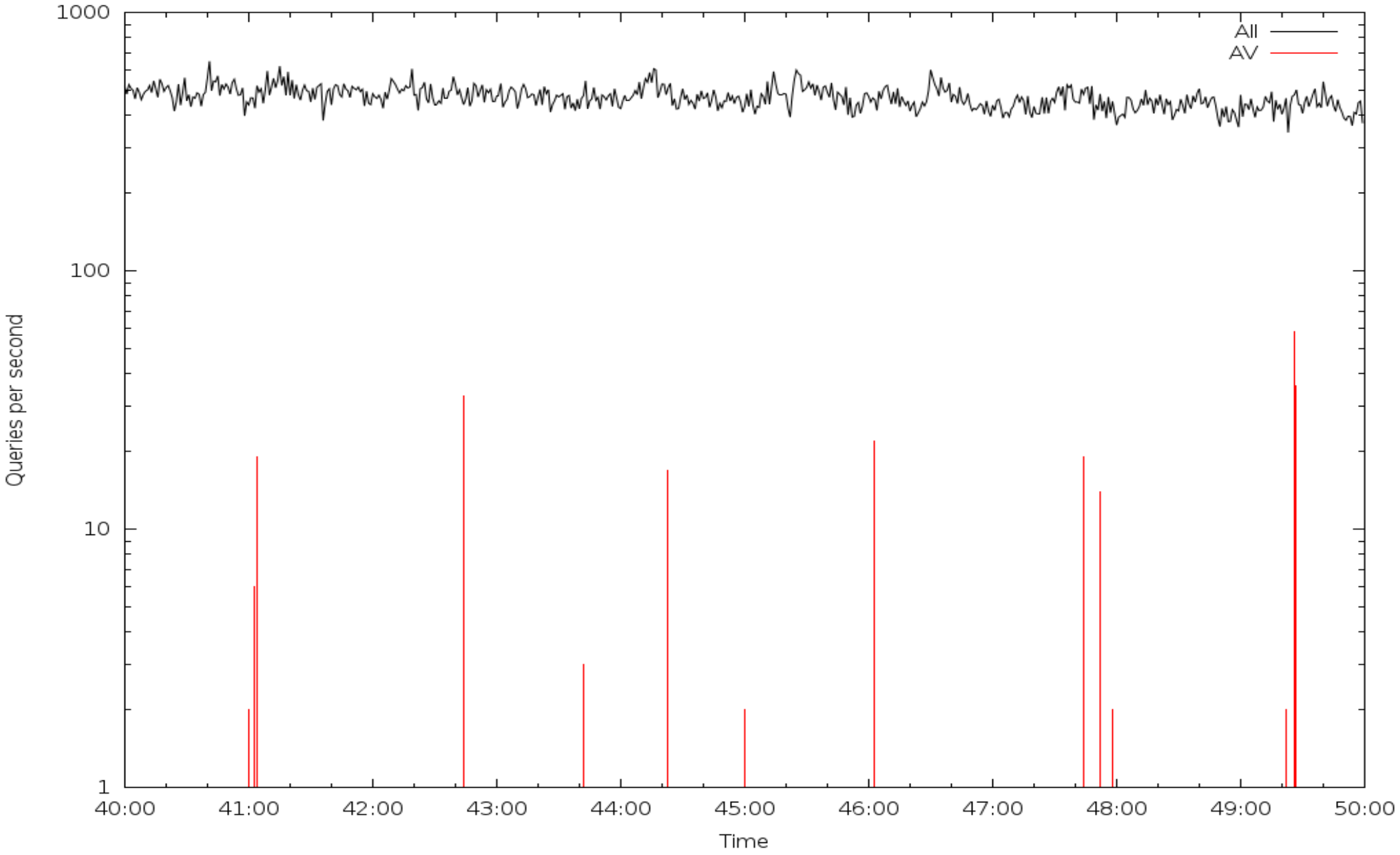
Implementation

- Compile time policies
  - SrcIPPolicy
    - Only the source IP is used as connection identifier
    - Destination IP/port, and protocol show no variability :)
  - QueryNamePolicy
    - QNAME is used as connection identifier
- More policies can be implemented

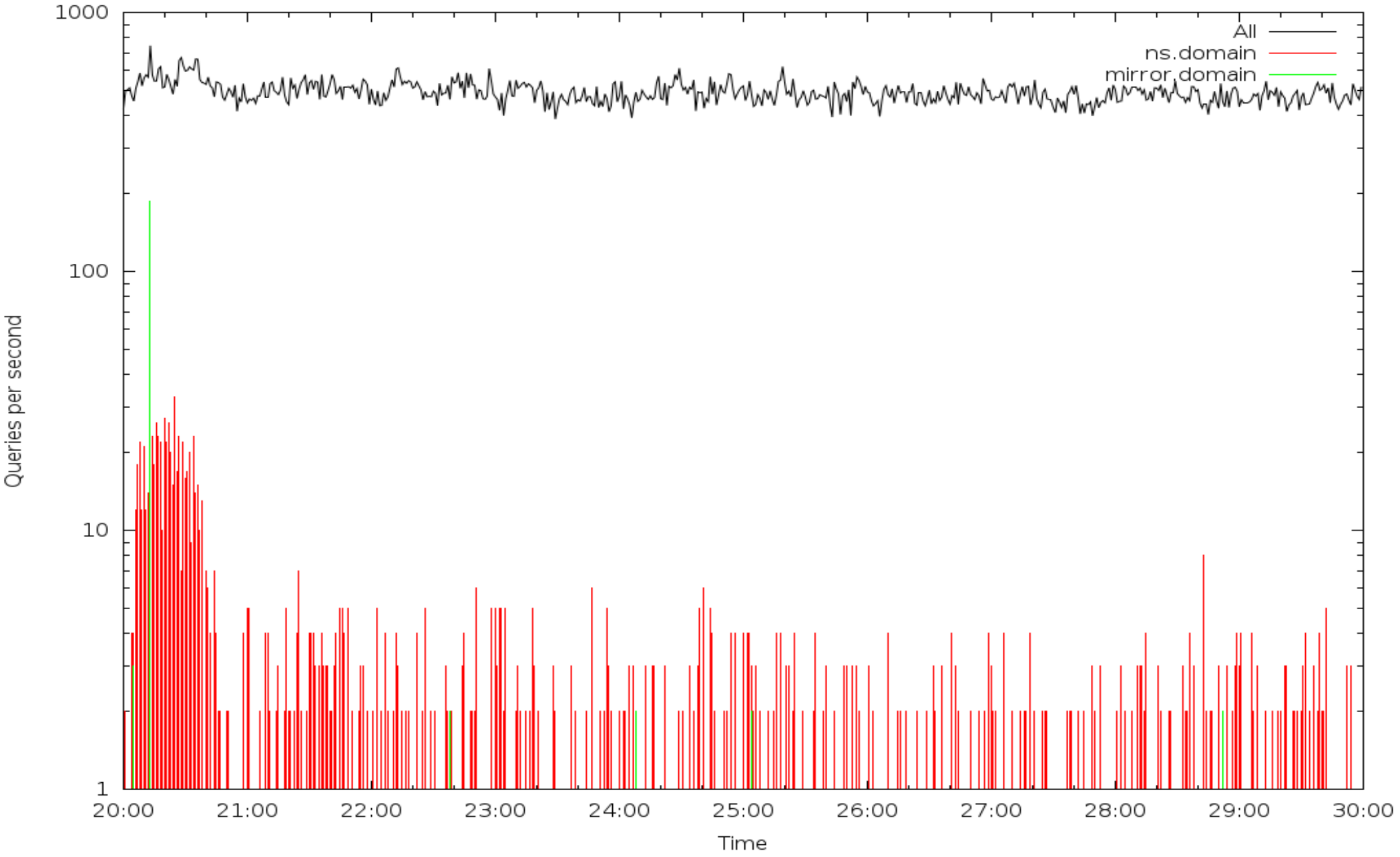
Testing and results

- Data set
  - 12h of captured data from one authoritative DNS
  - Filtered to contain only DNS queries
  - 10 minute time windows (no overlapping)
- Results
  - Single spike, repeated spike, other
  - QueryNamePolicy
    - AV homepage, FTP mirror, other/unknown
  - SrcIPPolicy
    - FTP mirror, Picture Spider Bot, other/unknown

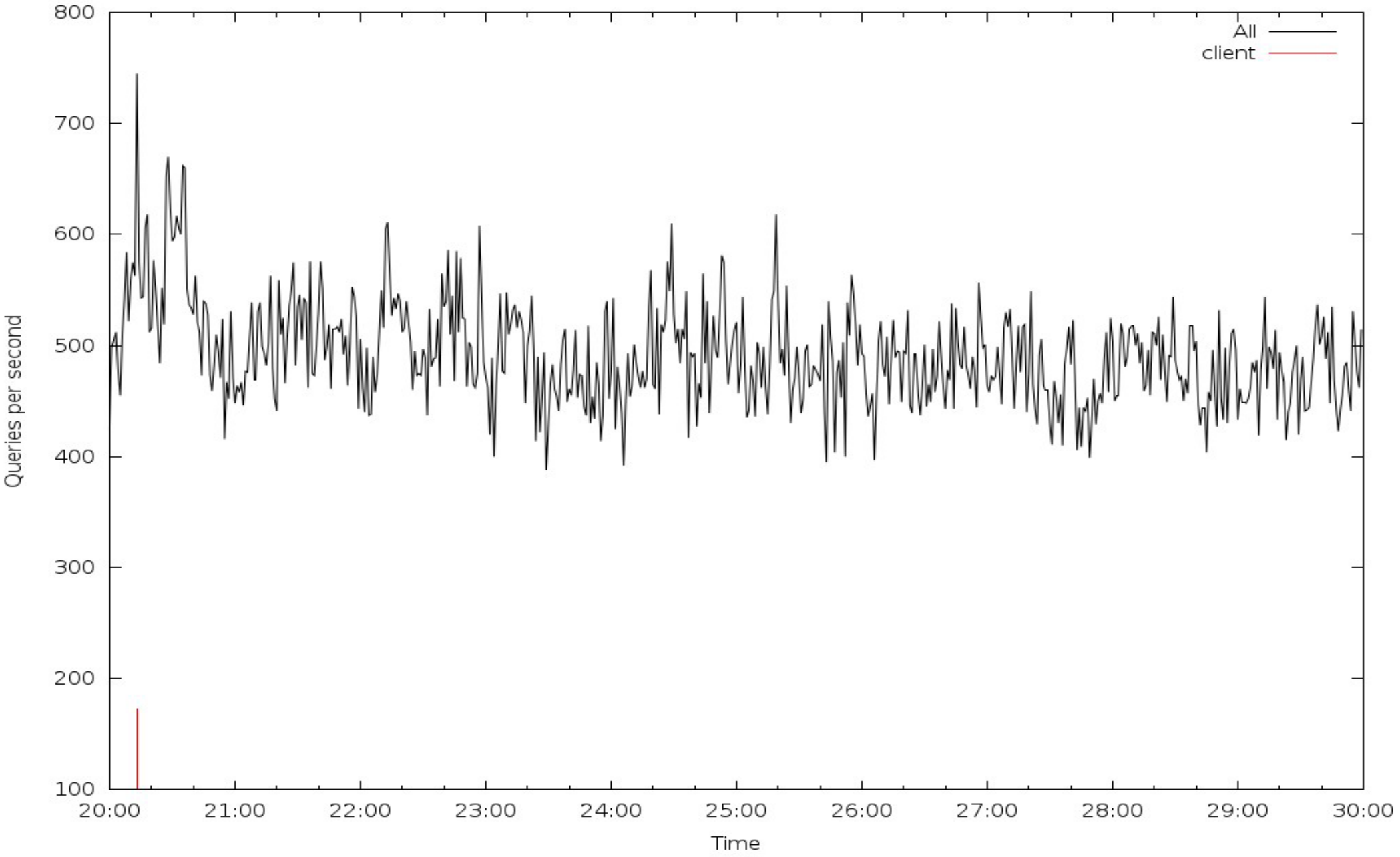
AV homepage (QNAME, logscale)



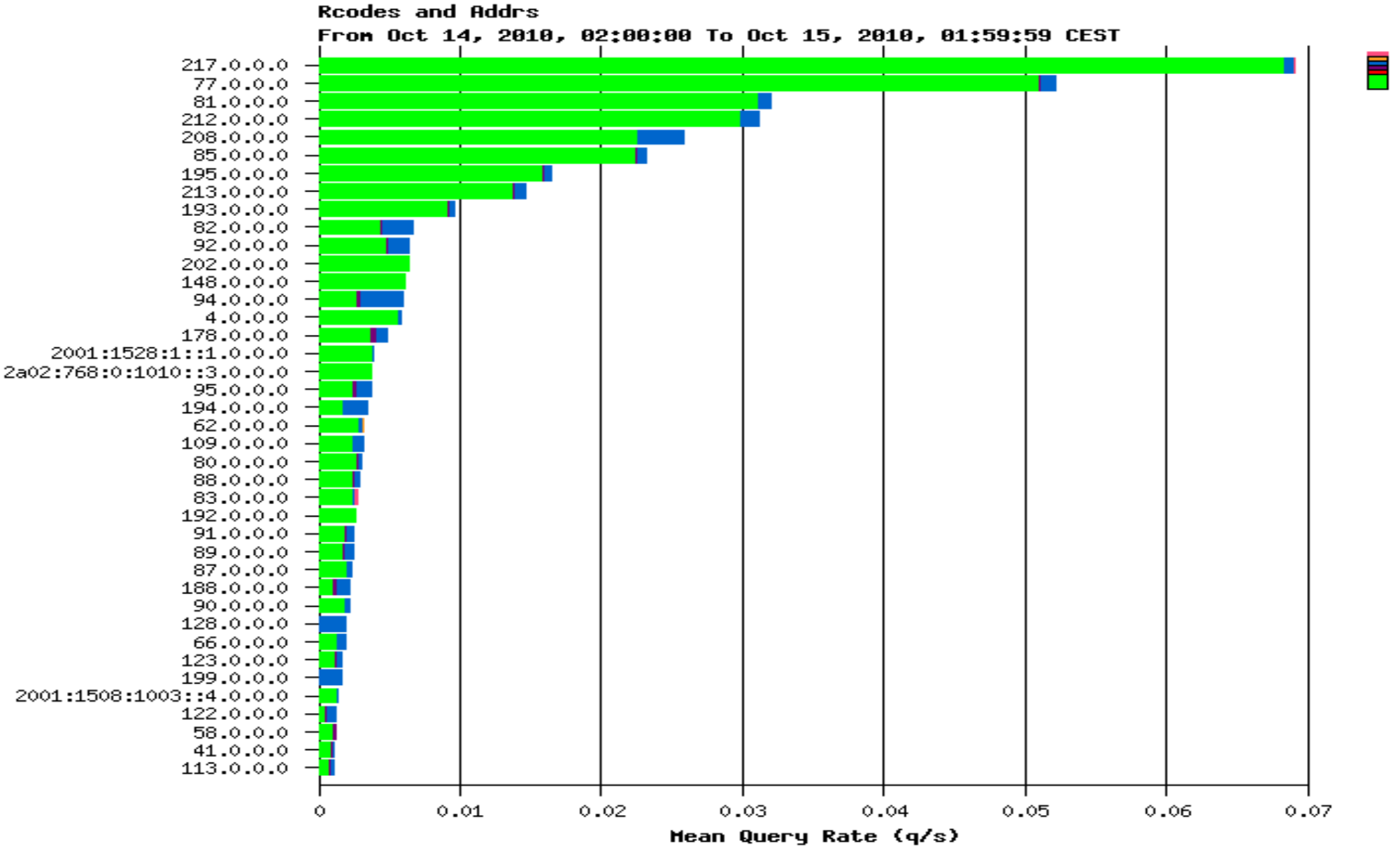
FTP mirror (QNAME, logscale)



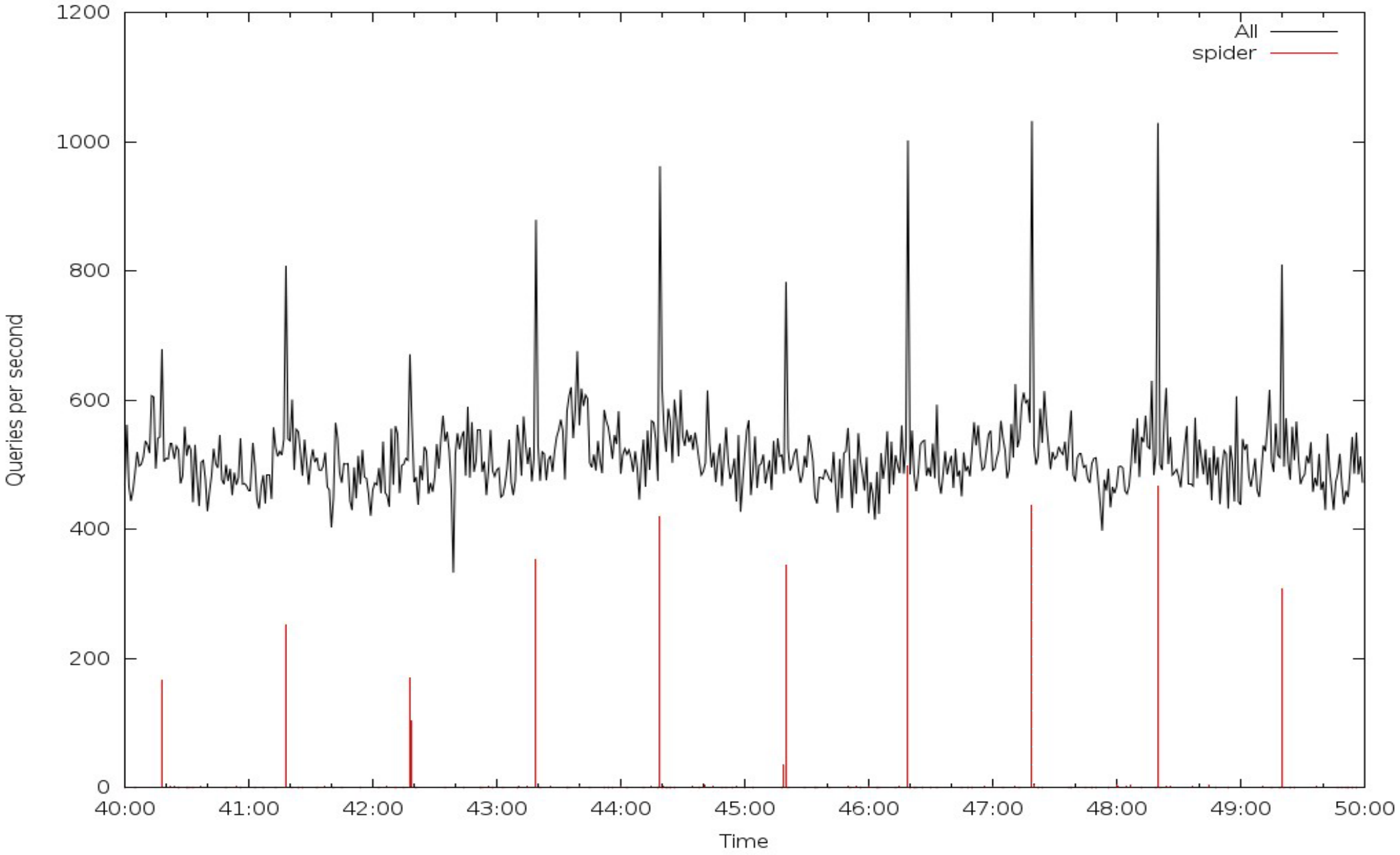
FTP mirror (SrcIP)



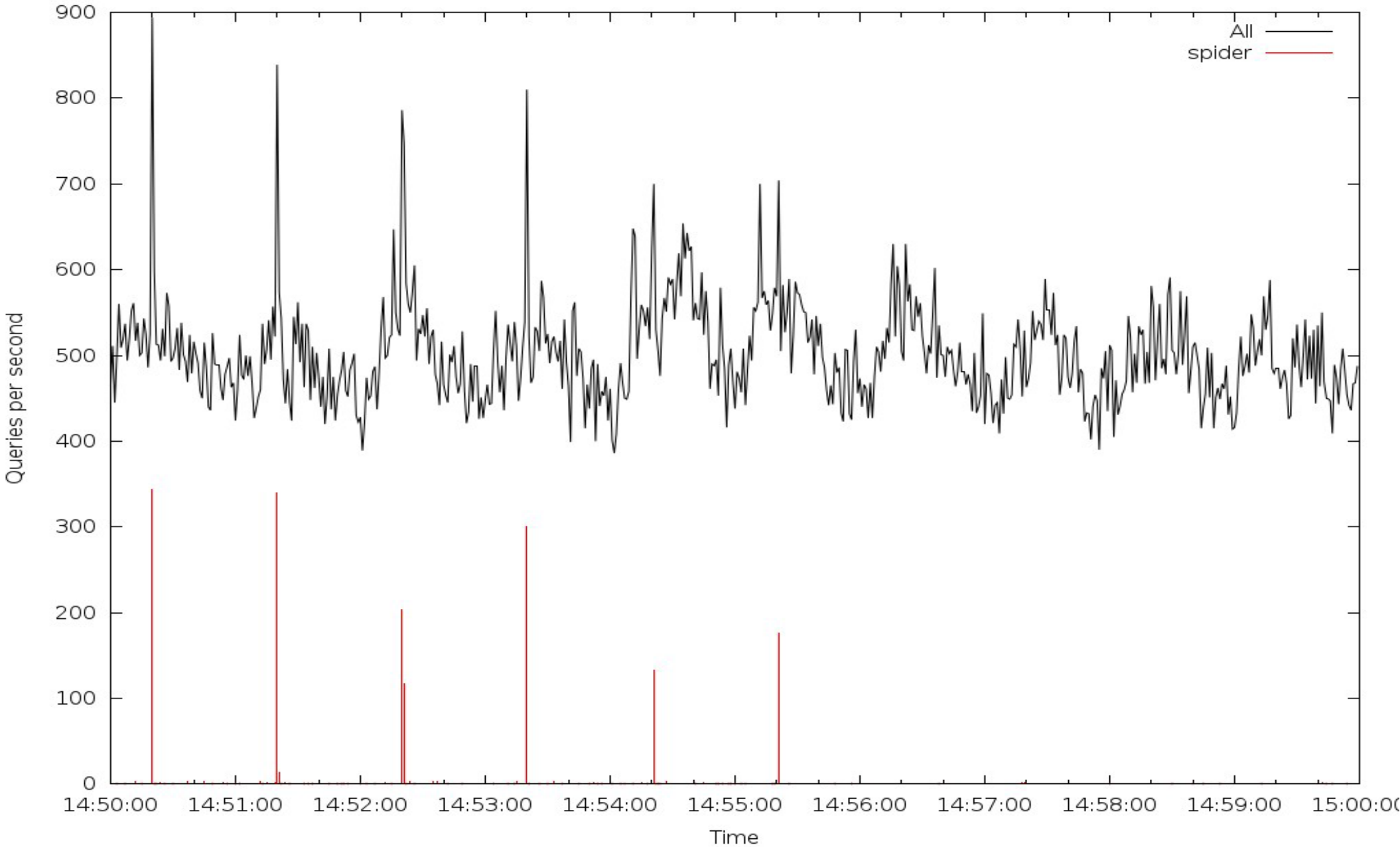
Spider bot (DSC)



Spider bot (SrcIP, start)



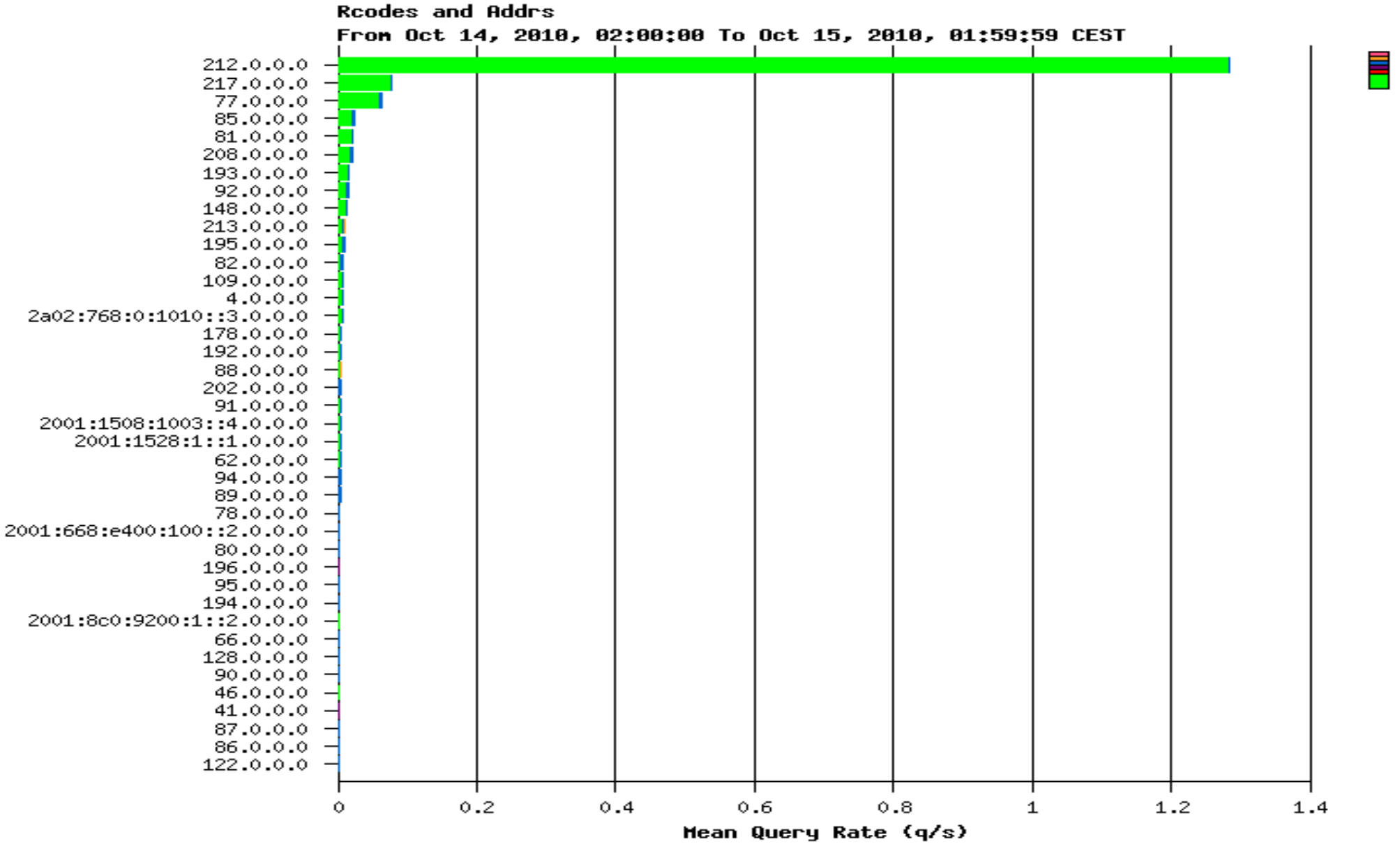
Spider bot (SrcIP, end)



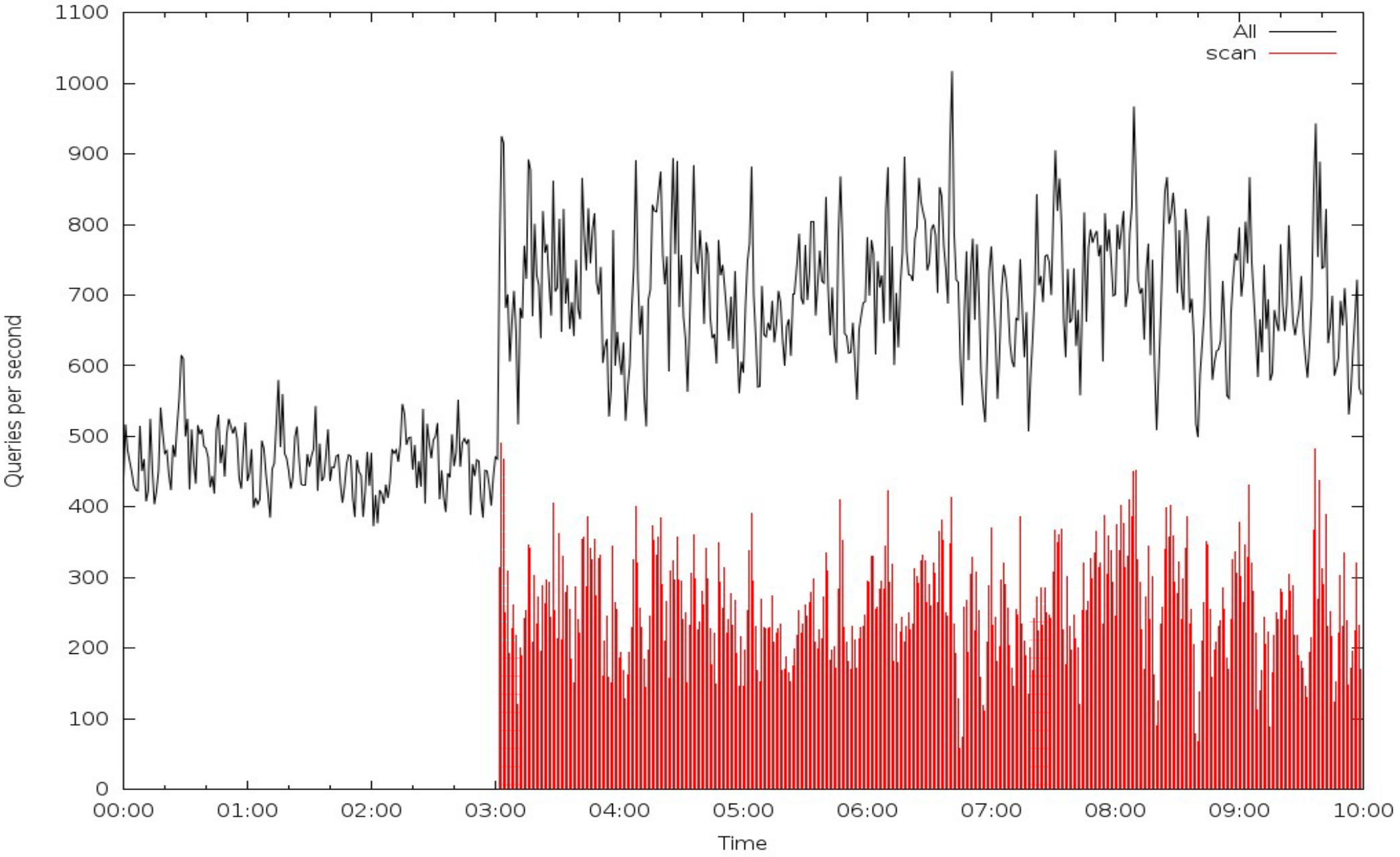
Spider bot

- Seen in DSC as well
  - Most active IP
- Regular pattern seen in SrcIPPolicy
  - Queries came in alphabetical order

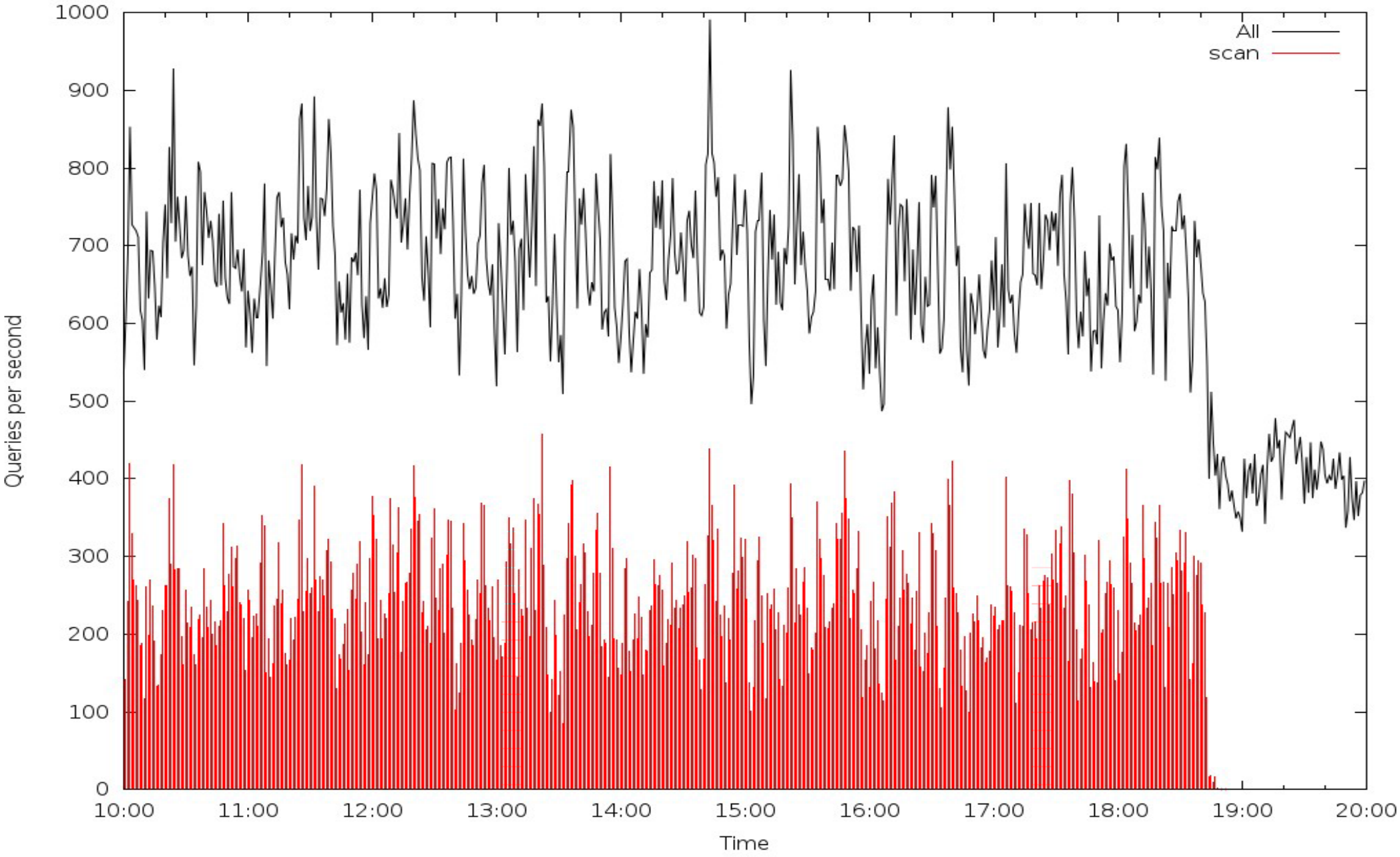
Name server scan (DSC)



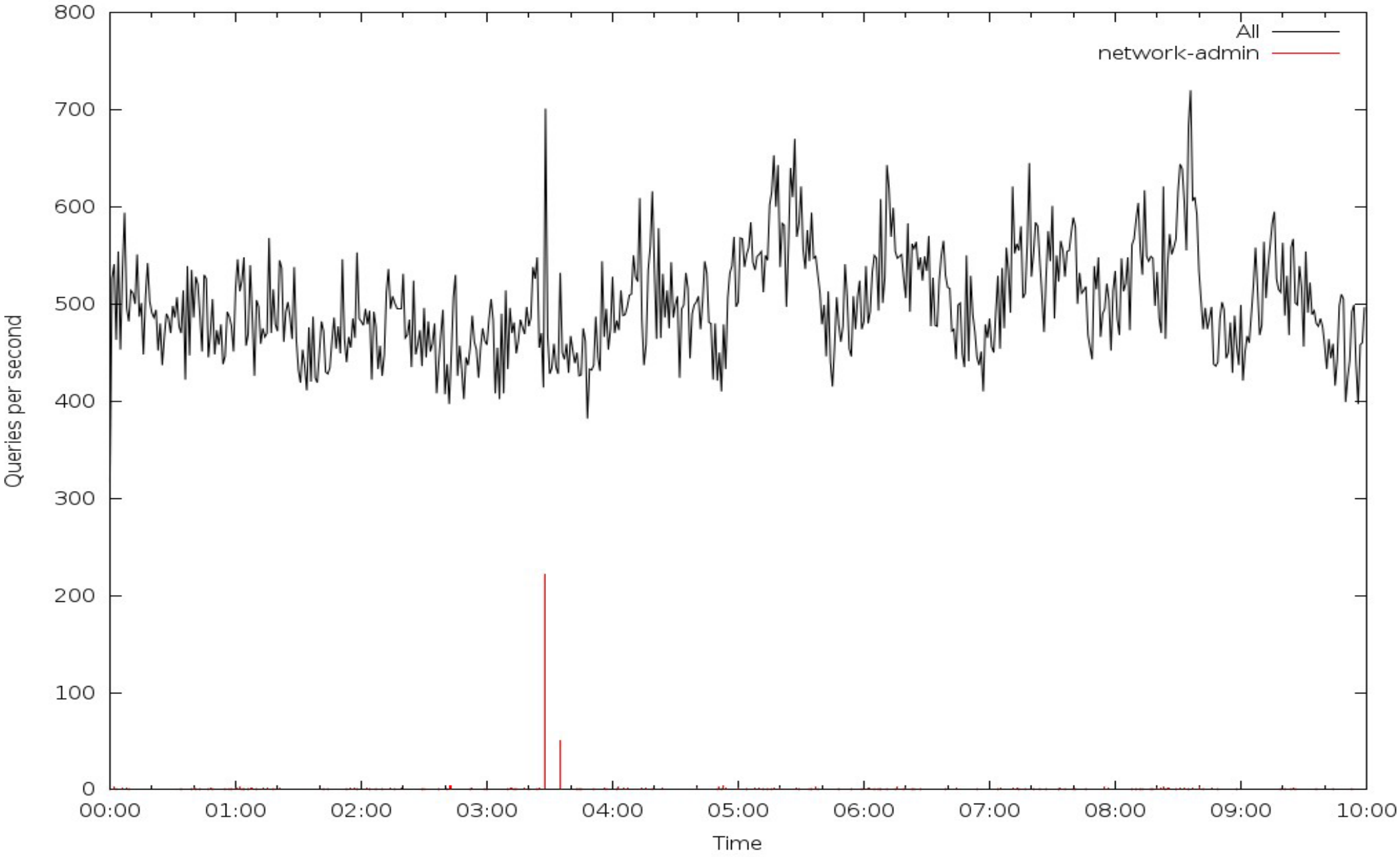
Name server scan (SrcIP, start)



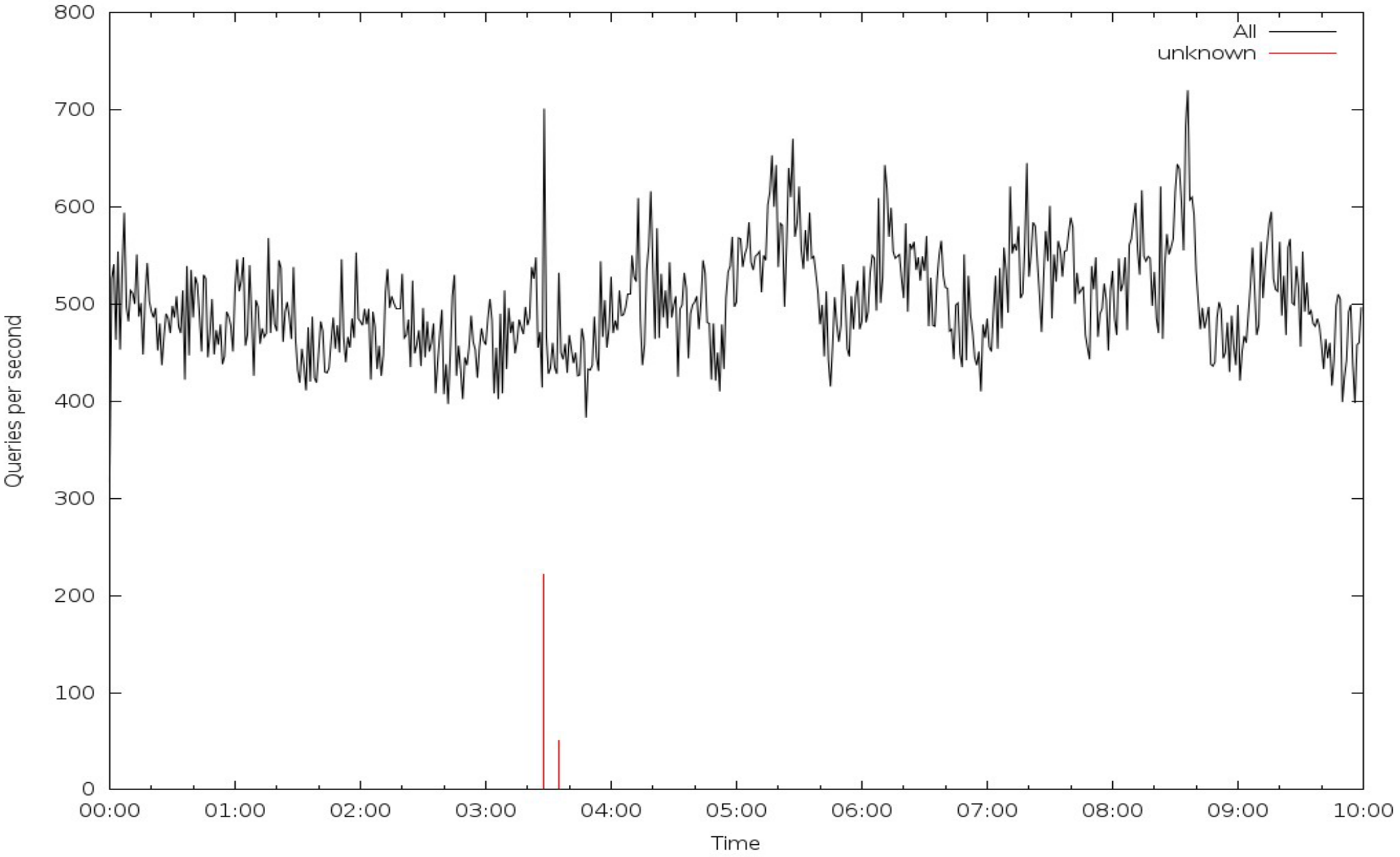
Name server scan (SrcIP, end)



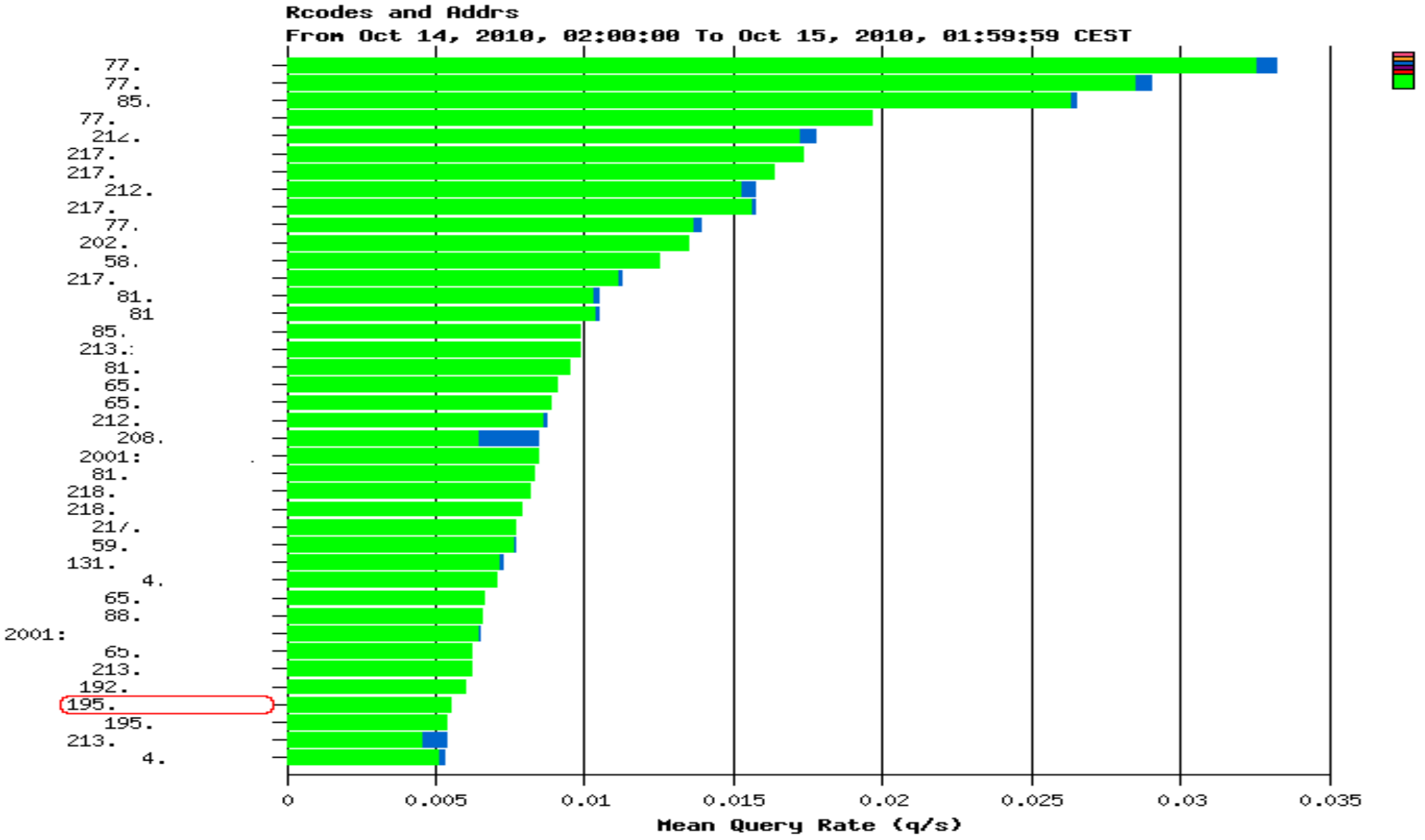
Other/unknown (QNAME)



Other/unknown (SrcIP)



Other/unknown (DSC)



Other/unknown

- Single source (somewhere in Ukraine)
  - Redirects to some network administration tool
- All queries for single A record
- Not seen by DSC

Future work

- Implement more policies
  - Intersect results between policies
- Implement different methods
- Test with more data
  - DITL
  - Data from recursive resolver
- Use the results
  - CSIRT (malware detection, …)
  - Monitoring failures of DNS caches

Questions?