K-root traffic spike

Wolfgang Nagele
Global Information Infrastructure Manager

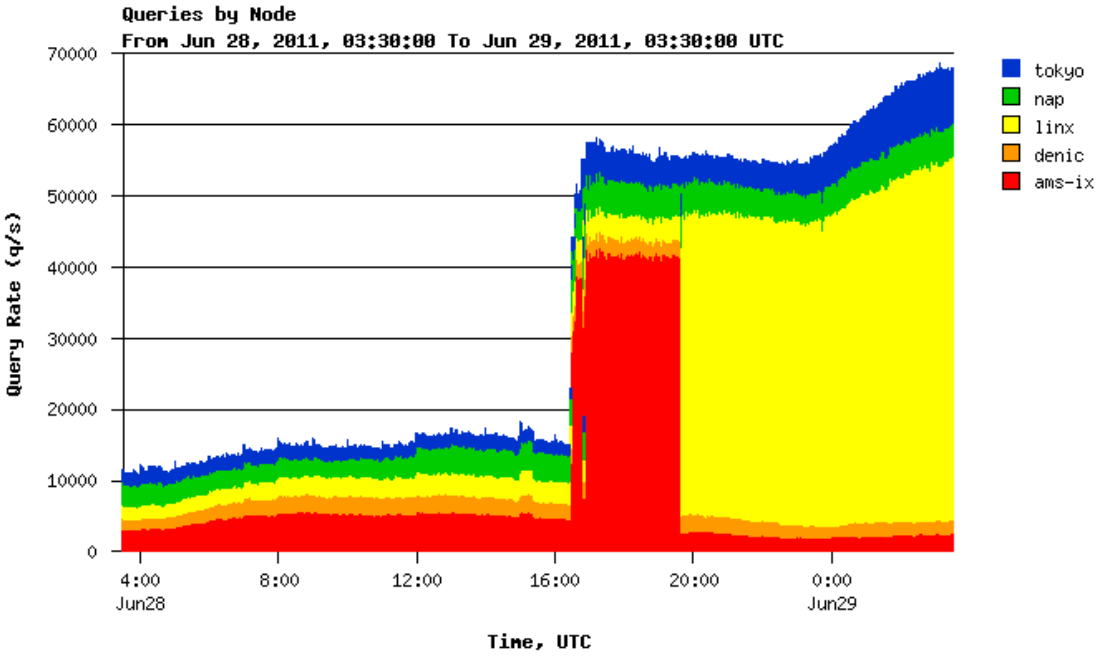
RIPE NCC

Remember …

- We did not make the front-page of the New York Times that day
  - Not even the business section ;-)
  - No user noticeable impact of this event
- Drops were visible in DNSMON
  - Counter action to use spare capacity

Just another day at the office – until …

- Jump from 15.000 qps (regular baseload)
- To 55.000 qps
- ~250% query rate increase



Timeline - 28 June 2011

- 16:54 UTC
  - Confirm 55k qps hitting Amsterdam site
- 23:02 UTC
  - Report from Stefan Schmidt about drops in root server queries (on dns-operations@lists.dns-oarc.net)
- 23:12 UTC
  - Shift traffic to London site with more spare capacity

Timeline - 29 June 2011

- 9:31 UTC
  - Escalate details to CNNIC and CN-CERT
- 10:12 UTC
  - Initial conclusions showing that bulk of traffic is sourced from a few AS in China
  - Possible victim of a misguided attack against rival site
- 13:15 UTC
  - Publish initial data on RIPE Labs
- 15:58 UTC
  - Similar TTLs suggest spoofed attack

Timeline - 30 June 2011

- 8:56 UTC
  - Verified TTLs against ICMP results disproving spoofing theory
  - Elevate pressure on Chinese ISPs to investigate
- 13:39 UTC
  - Traffic starts to fall and normalizes over the following days

Initial glance

- Random queries for a Chinese gaming site
  - Traffic remains high throughout the day
  - Received at single location
    - Suggested single (or few) originators
    - We forced it from Amsterdam to London because of higher spare capacity at this location and fear of quick increase
  - Communicate initial findings on RIPE Labs

Observation

- Few Chinese autonomous systems carrying the bulk of the traffic
  - Hard to establish contact
  - Took 5 days for reactions
  - Used all the leverage and contacts we had in the region
    - CNNIC, CN-CERT, APNIC
  - Close coordination among other Root Server operators about the ongoing efforts

Conclusions

- Communication with source ISPs
  - Europe and North America have traditionally good communication among engineering staff
  - Not so in APAC – long winded and hard to establish contacts
- Good communication and coordination among Root Server operators was essential

Conclusions

- Most likely fallout of DDoS against Chinese gaming site and probably unintended
- Huge Autonomous Systems
  - Initially looked like a spoofing attack
  - Need for more anycast deployments to localize impact

Aftermath

- Upgrade of global nodes to full GigE capacity
  - Amsterdam, London, Frankfurt, Miami and Tokyo
- Additional query server at global nodes
  - 3 servers allowing for ~250k qps per global instance

Remember …

- You still got to Facebook that day

Questions?

wnagele@ripe.net

Get the inside scoop …

http://goo.gl/fD2LJ

RIPE NCC