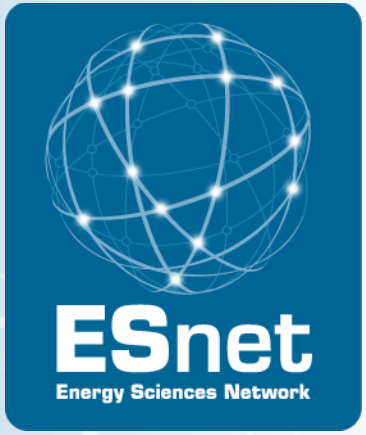


DNS Reflection(?) attacks seen in Berkeley

Michael Sinatra, Network Engineer

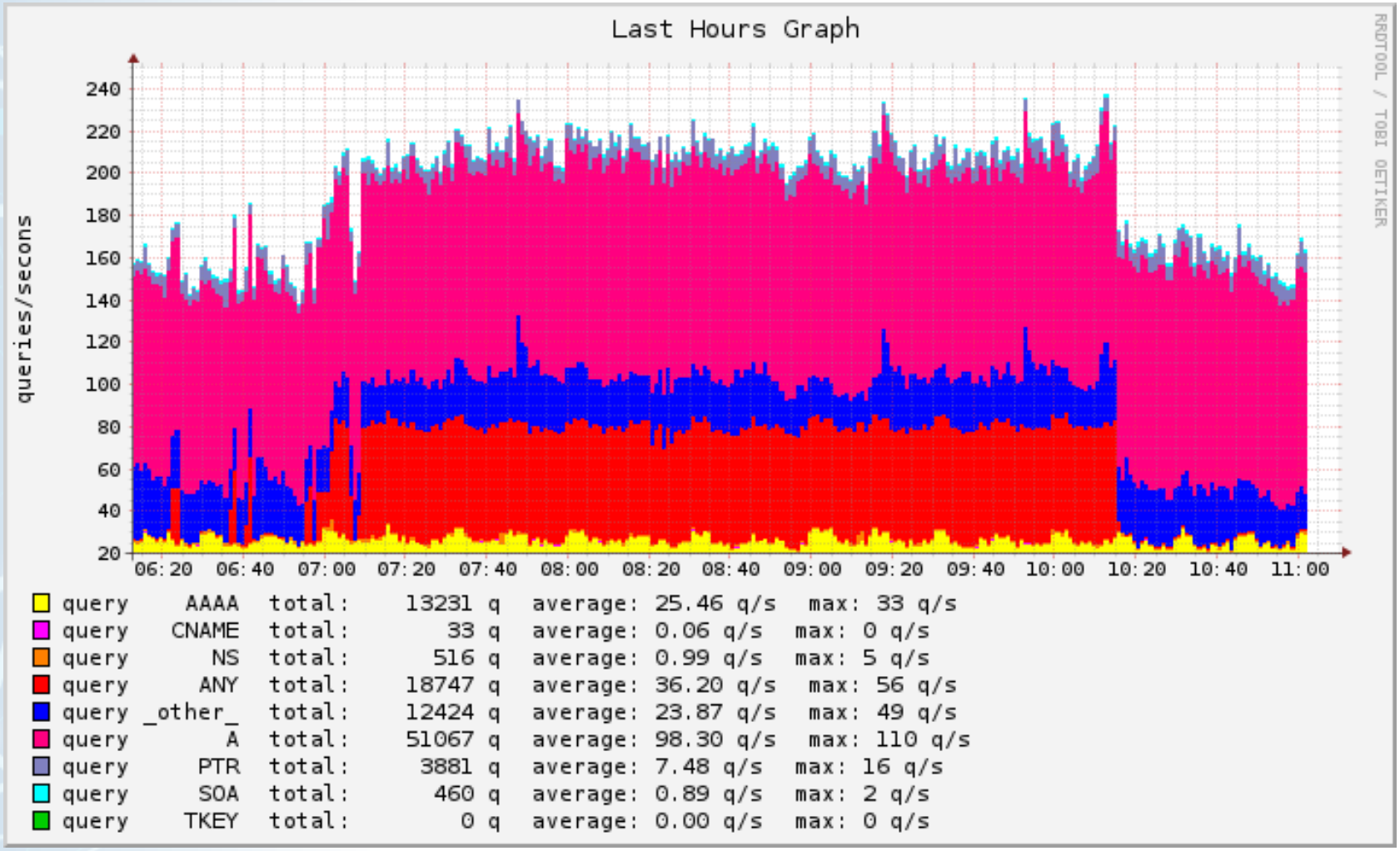
ESnet Network Engineering Group

NANOG 56 DNS Security (not DNSSEC) Track

Dallas, TX, USA

October 2012

One day, I was just minding someone else's business…



DNS ANY queries

- Were hitting both UCB and ESnet servers.
- qtype = ANY
- RD set
- But, all domains for which each set of servers was already authoritative.
- Several different source IP addresses, alternating, changing over time.
- But they don’t seem to be spoofed!
- Many cable/broadband-looking hosts.

DNS ANY queries

- Cycle through a set of 5-10 domains periodically.
- Many, but not all, are DNSSEC-signed.
- Occasionally, we have seen things like source 80/udp → 53/udp ANY es.net, which really does look like a reflection attack.
- But this ongoing “event” doesn’t seem to be an attack per se.

This doesn't make sense

- Source addresses don't seem to be spoofed.
- ANY + RD for zones which we are authoritative? Doesn't seem legit.
- But it is really low-and-slow. 20-100 qps per nameserver.
- A research project?
- Intelligence-gathering?

Some clues?

- Footprint seems to be spreading.
- Noticed the UCB+ESnet issue back in June.
- More recently there have been more reports, including on public mailing lists.
- Hacked hosts? A misconfigured or poorly thought-out botnet?

Mitigation?

- DNS RRL patch
- Actually is triggering rate-limiting.
- Mainly to be ready if this is a prelude to something bigger.
- Not a big enough “attack” to apply the “DNS Dampening” patch or anything else that could cause collateral damage.

- RRL: http://www.redbarn.org/dns/ratelimits
- DNS Dampening: http://altlasten.lutz.donnerhacke.de/mitarb/lutz/bind-9.9.2-dampening.patch
  - But see Lutz’s message to dns-operations@

Answers!