Analysis of Amplifications Attacks

(Protocols as Weapons)

Jaap Akkerhuis

http://www.nlnetlabs.nl/

NLnet Labs

who m i

- Old Timer, no grey beard
- NLnet Labs guy
- Ripe DNS-WG co-chair
- IETF participant
- SSAC member

Overview

- Requirements for Abuse
- Amplification
- Reflection
- Spoofing
- Mitigation of Attacks
- Some conclusions

Successful Abuse

- Widely used services
- No authentication required (UDP based service preferred)
- Poorly or not maintained service
- Difficult to block clients of the service

Amplification

- Anyone can ask a small questions
- Answers (far) bigger then questions

NLnet Labs

Reflection & Spoofing

- Make answer go somewhere else:

"Reflection"

- Lie about origin of the question
  - Replace with victims address/port

"Source address spoofing"

NLnet Labs

Popular Protocols

- Chargen
- Qotd
- NTP
- SNMP (v2)
- DNS, preferred low hanging fruit of the day
- Games related protocols

Character Generator

- Meant for debugging RFC 864
- single byte to port 19
- (TCP) Stream of bytes
  - Stream stops when connection is closed or broken
- (UDP) Gives 0 … 512 bytes back (UDP)

Quote of the Day

- Yet Another Debugging tool (RFC 865)
- Port 17
- (TCP) Answer with short message, drop connection
- (UDP) Send short message as answer
- What *is* a short message?
- Amplification 576x for UDP

NTP

- Server in nearly every CPE, router etc
- Monitoring command: `monlist`
- Last 600 servers used will be listed
- Amplification up to 4000x or so

SNMP

- Version 2c "preferred"
- Standard community string `public`
- GetBulk request
- Query ca. 40 bytes
- Amplification up to 1700x

DNS Abuse
Two Flavours

- Open resolvers
- Authoritative servers

Mitigation, Open Resolver Abuse

- Answer only to who you know
  - Close Open Resolvers
    - 21 Million of them
    - Don't forget the nasty NAT boxes (CPEs)
    - Saves bandwidth, reputation, headaches
- RFC 5358

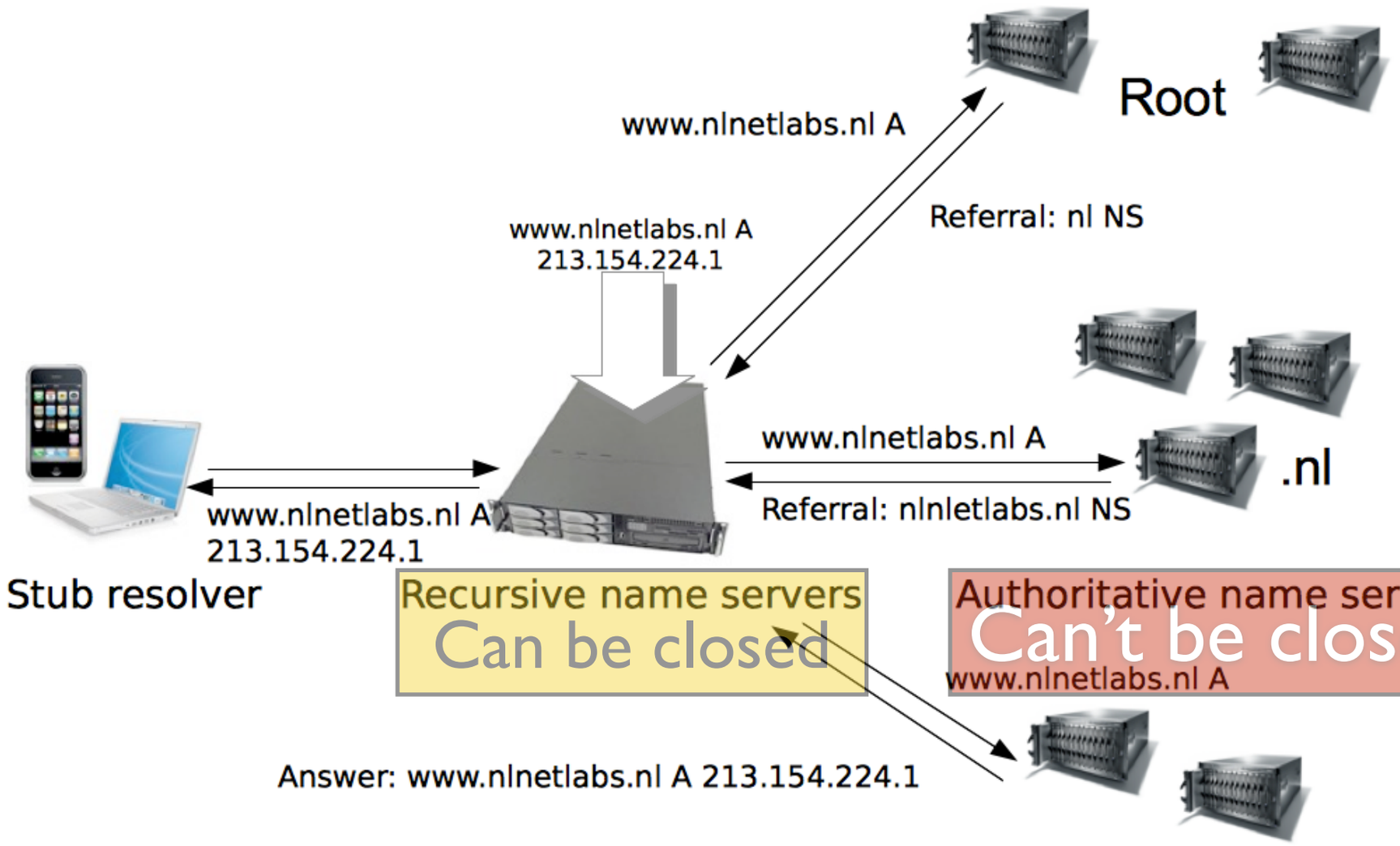
Abusing the Authoritative

Service to many recursive name servers

Wide Audience, RFC 5358 not applicable

NLnet Labs

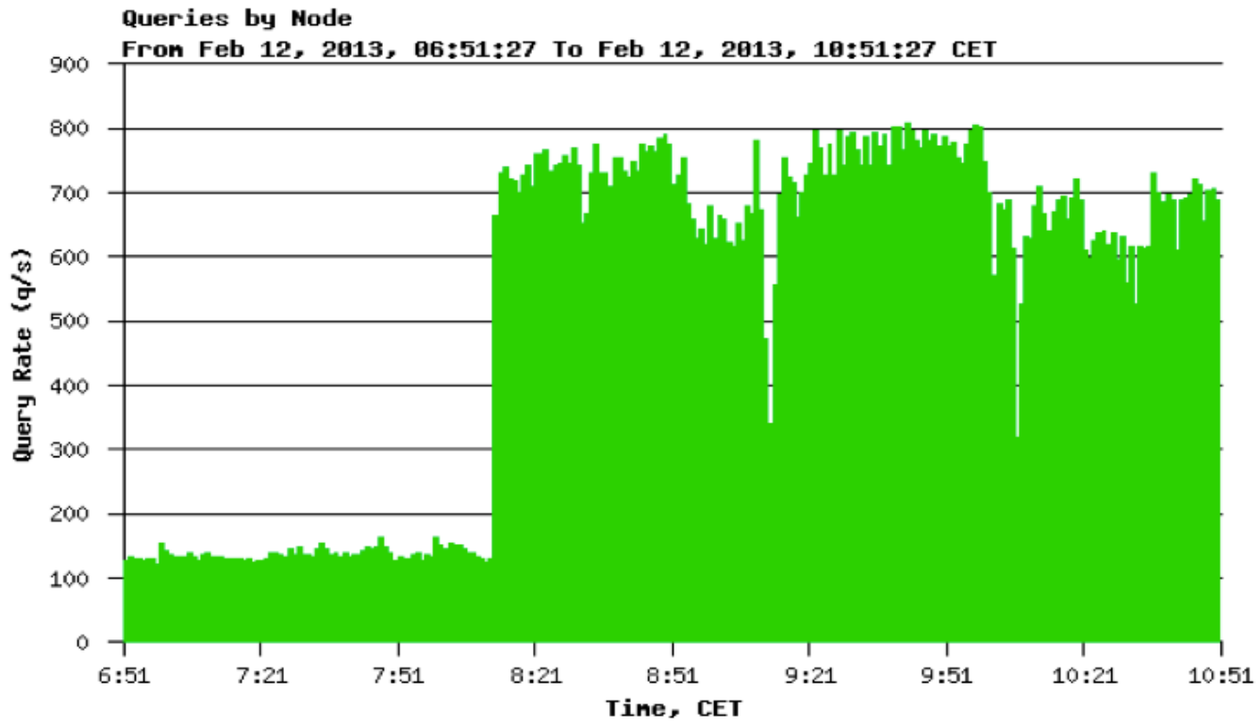
DNS Overview



DNS Amplification rates

- ANY Queries
  - Up to 80 times
- NXDomain + DNSSEC
  - NXDOMAIN, NSEC: 18x
  - NXDomain, NSEC3: 25x

Impact of Attack



Mitigation Principle

- Don't help the attacker
  - Keep answering some queries to well behaving clients
- No Service degrading
  - (victims or other clients)

Mitigation Proposals

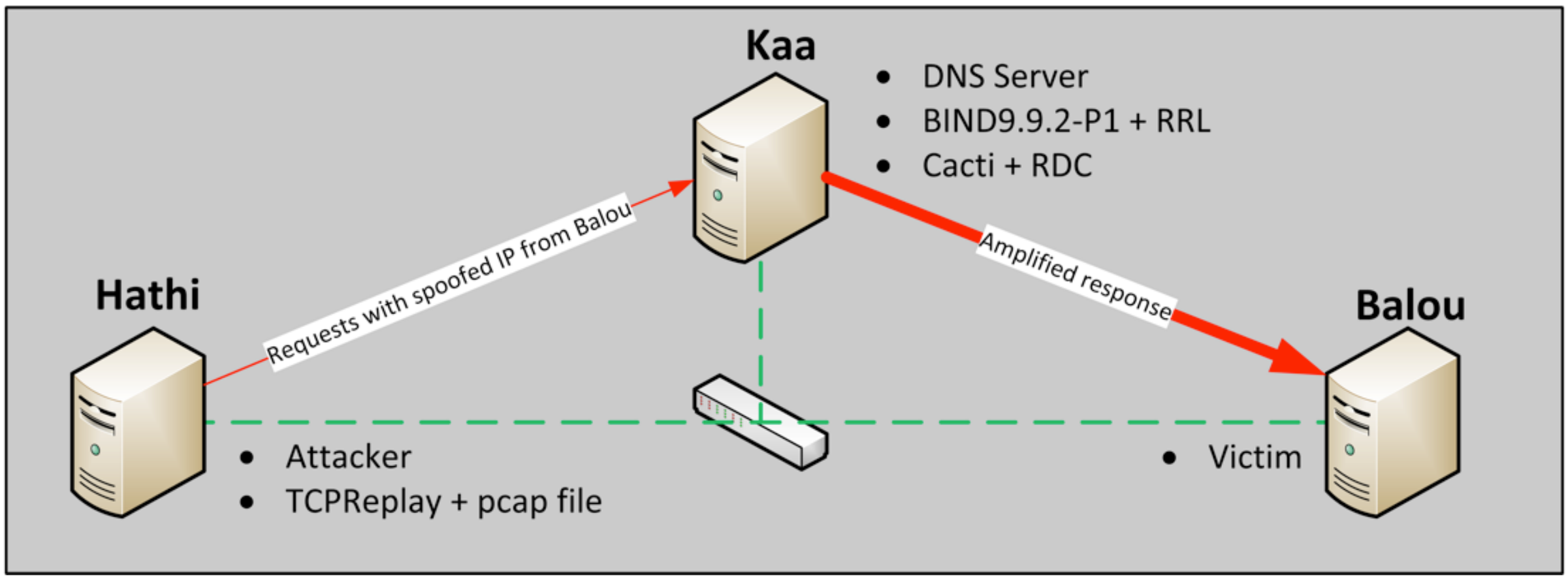
- Query limiting (external to server)
  - DNS Firewalls
    - Suppress ANY Queries
- DNS Dampening
- Response Rate Limiting (RRL)

RRL

- Drop answers that exceed certain limits
- False positive mitigation
- TCP fallback
  - Allows victim to contact server over TCP
- Performs reasonably well

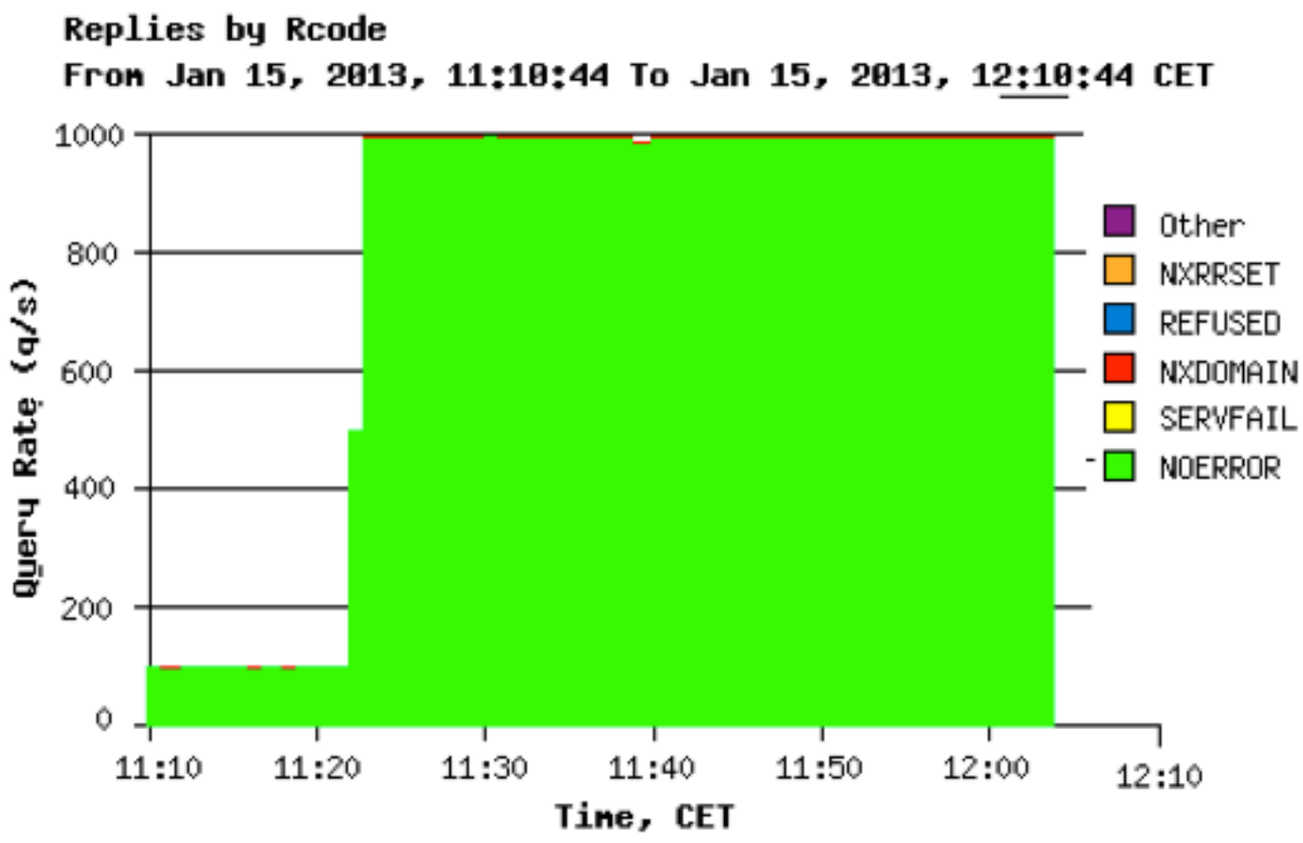
RRL Measurements

- Set up



RRL Measurements

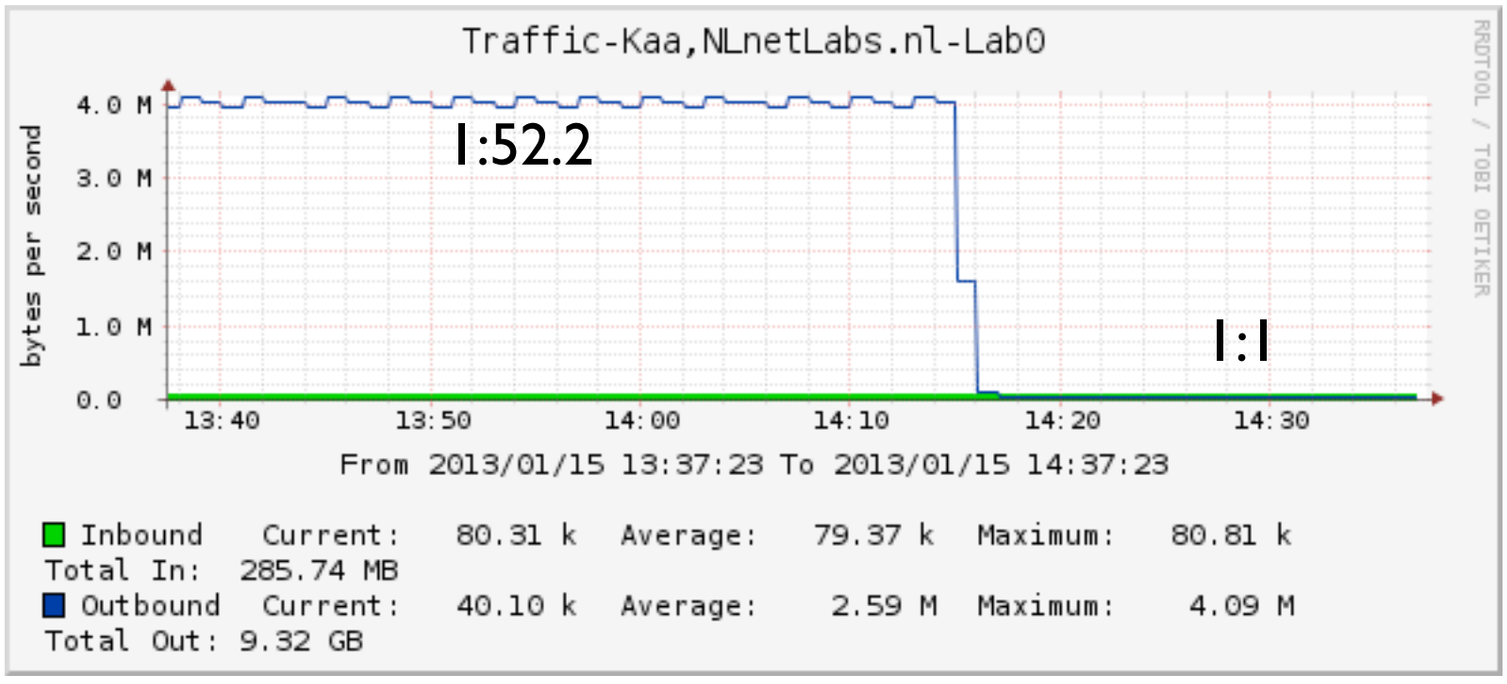
- ANY attack at 11:20



NLnet Labs

RRL Measurements

- ANY attack at 11:20, RLL enabled at 14:15

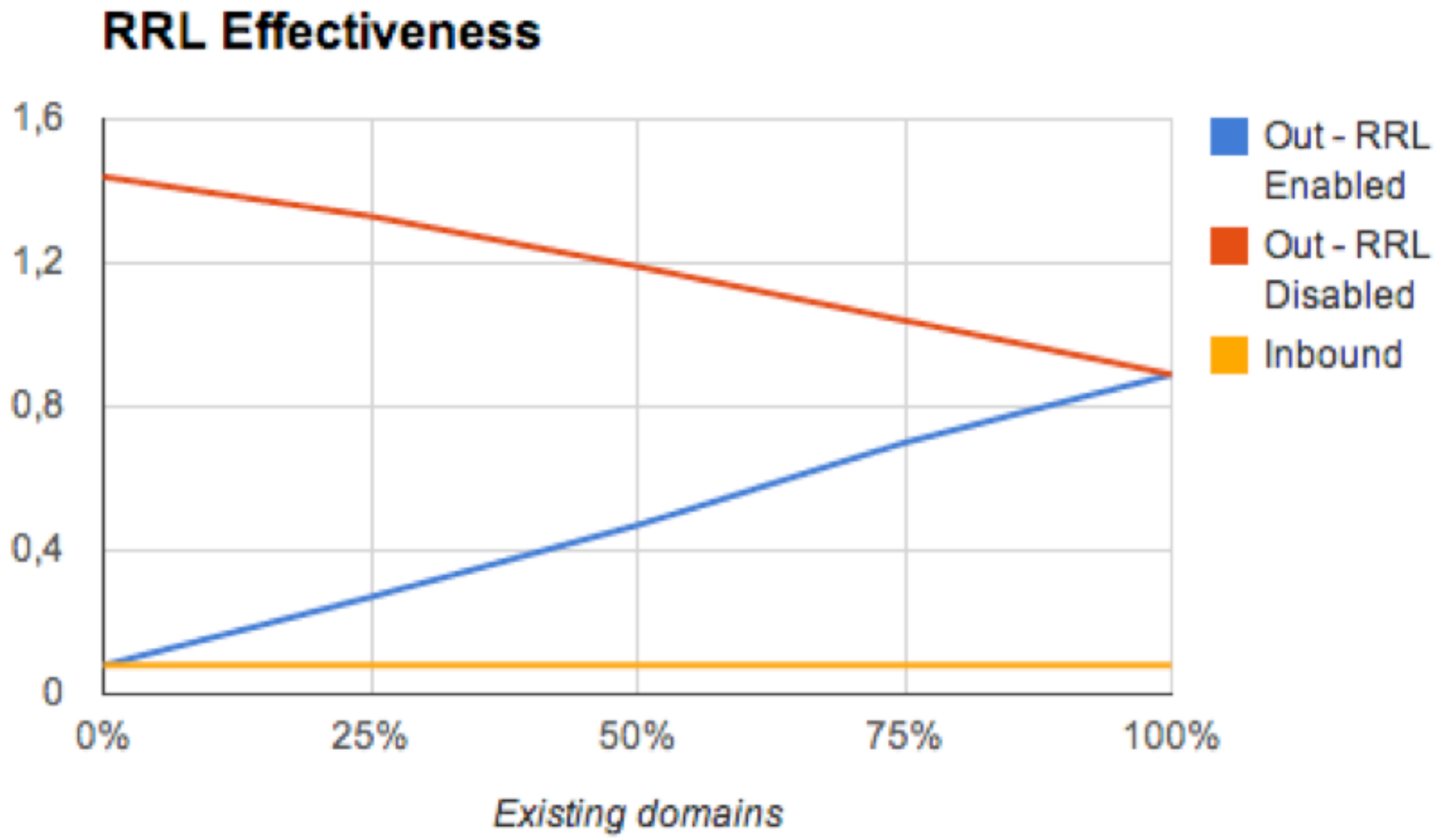


RRL Measurements

SLIP	In	Out	Amp. Ratio	False positives*	TCP responses
1	80 KB/s	81 KB/s	≈1:1	0%	100 %
2	79 KB/s	39 KB/s	≈1:0.5	50%	87.5 %
3	79 KB/s	26 KB/s	≈1:0.3	66.6%	66 %
5	80 KB/s	16 KB/s	≈1:0.2	80%	49 %
10	80 KB/s	8 KB/s	≈1:0.1	90%	27 %

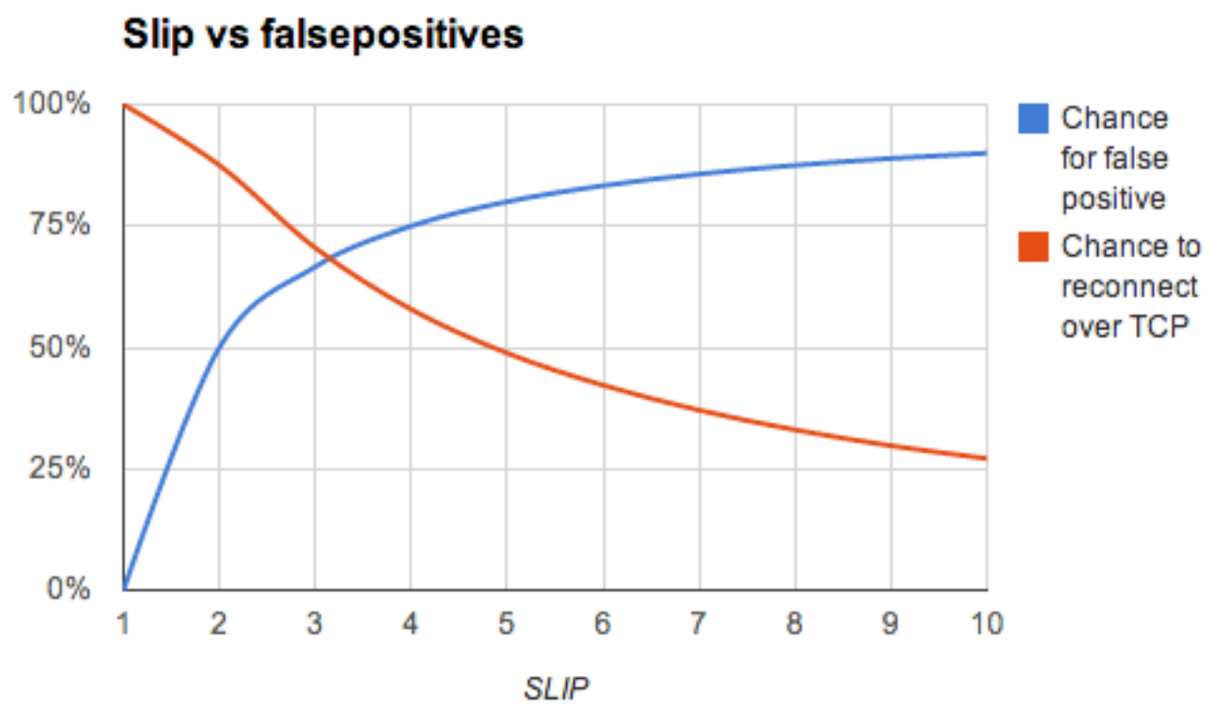
* Possible fps, assuming 3 tries

RRL Measurements



RRL Measurements

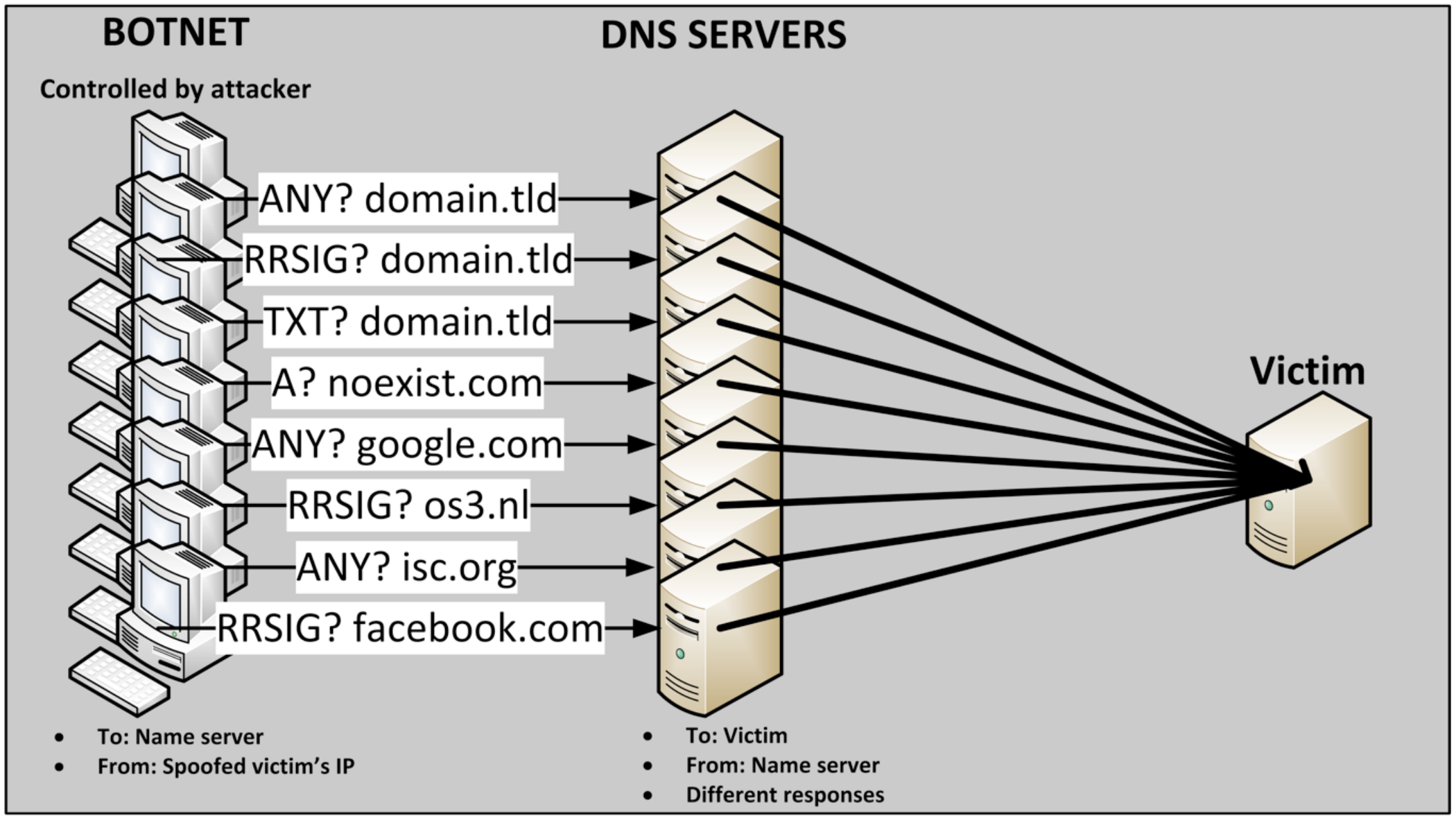
- Slip
  - Trade off between # of false positives and # of TCP sessions
- Default 2



Whac-A-Mole

NLnet Labs

Getting sophisticated



RRL Failures?

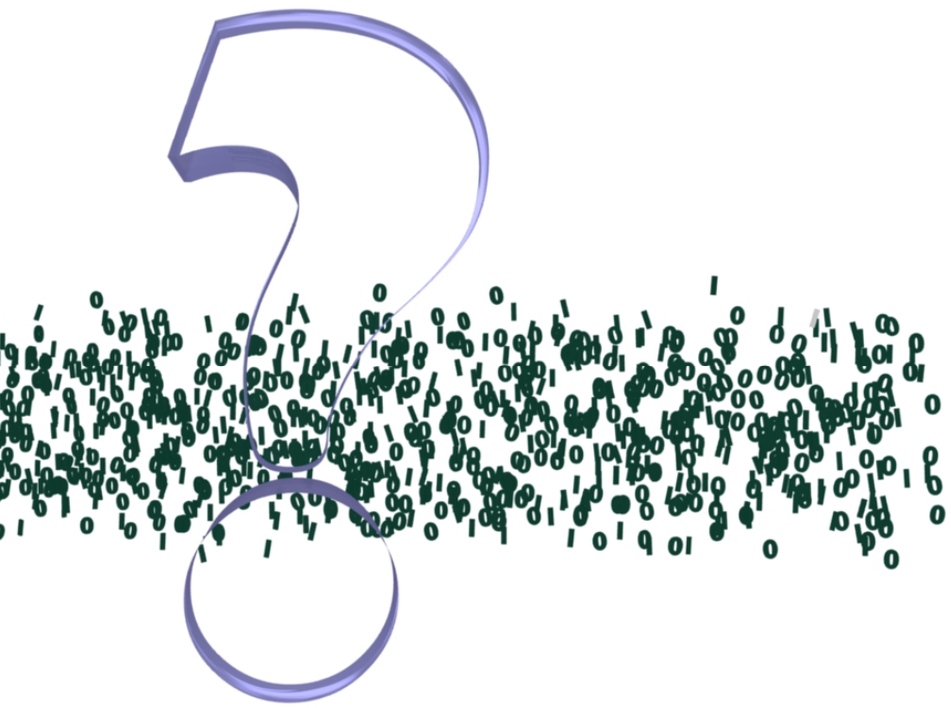
- Garrier Grade NAT
  - Muliple clients behind 1 IP
- DNS stays the low hanging fruit of the day

Prevent Spoofing

- Implement source validation
  - Don't let fake packages leave your network
- SAC 004, 008, BCP 38, 84 and more
  - For the good of the internet
  - For the good your reputation

Further reading

- DNS Firewall rules: http://www.bortzmeyer.org/files/generate-netfilter-u32-dns-rule.py
- Dampening: http://lutz.donnerhacke.de/eng/Blog/DNS-Dampening
- Rate limiting
  - Proposal by Paul Vixie and Vernon Schryver: http://www.redbarn.org/dns/ratelimits
  - NSD Rate limiting: https://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/
  - Knot Rate limiting: https://www.knot-dns.cz
- DNS Rate Limiting, A Hard Lesson: http://conference.apnic.net/__data/assets/pdf_file/0011/58880/130226.apops-dns-rate-limit_1361839670.pdf
- RLL Measurements: http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf
- Website: http://www.bcp38.info/
- SNMP DOS Attacks: http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf
- SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure (18 February 2014): https://www.icann.org/en/groups/ssac/documents/sac-065-en.pdf



Questions

(If you like our work, please consider sponsoring us)

NLnet Labs

NLnet Labs