Pseudo Random DNS Query Attacks & Resolver Mitigation Approaches

APRICOT 2015

© 2014 ISC

The attacks

- Began in February 2014
- Attack intent is to DDoS DNS authoritative provider, but incidentally degrades ISP resolvers

The parties involved

- Sometimes this is an extortion attack
- Frequently seems to originate and terminate in China

- Target domain may be hosted with many non-targeted domains
- Targets hop from provider to provider

Initiator of DDoS traffic

Target of the DDOS Authoritative provider

© 2014 ISC

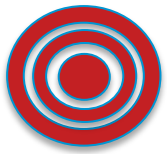
Identifying the attack

high volume of queries for non-existent sub-domains

<randomstring>.www.example.com
<anotherstring>.www.example.com

does not exist

exists



© 2014 ISC

Attack begins

Insecure Home gateways

Home users are unaware

1. Requests for randomstring.www.example.com

nothing about this in the cache

ISP resolvers

2. Attempt to resolve

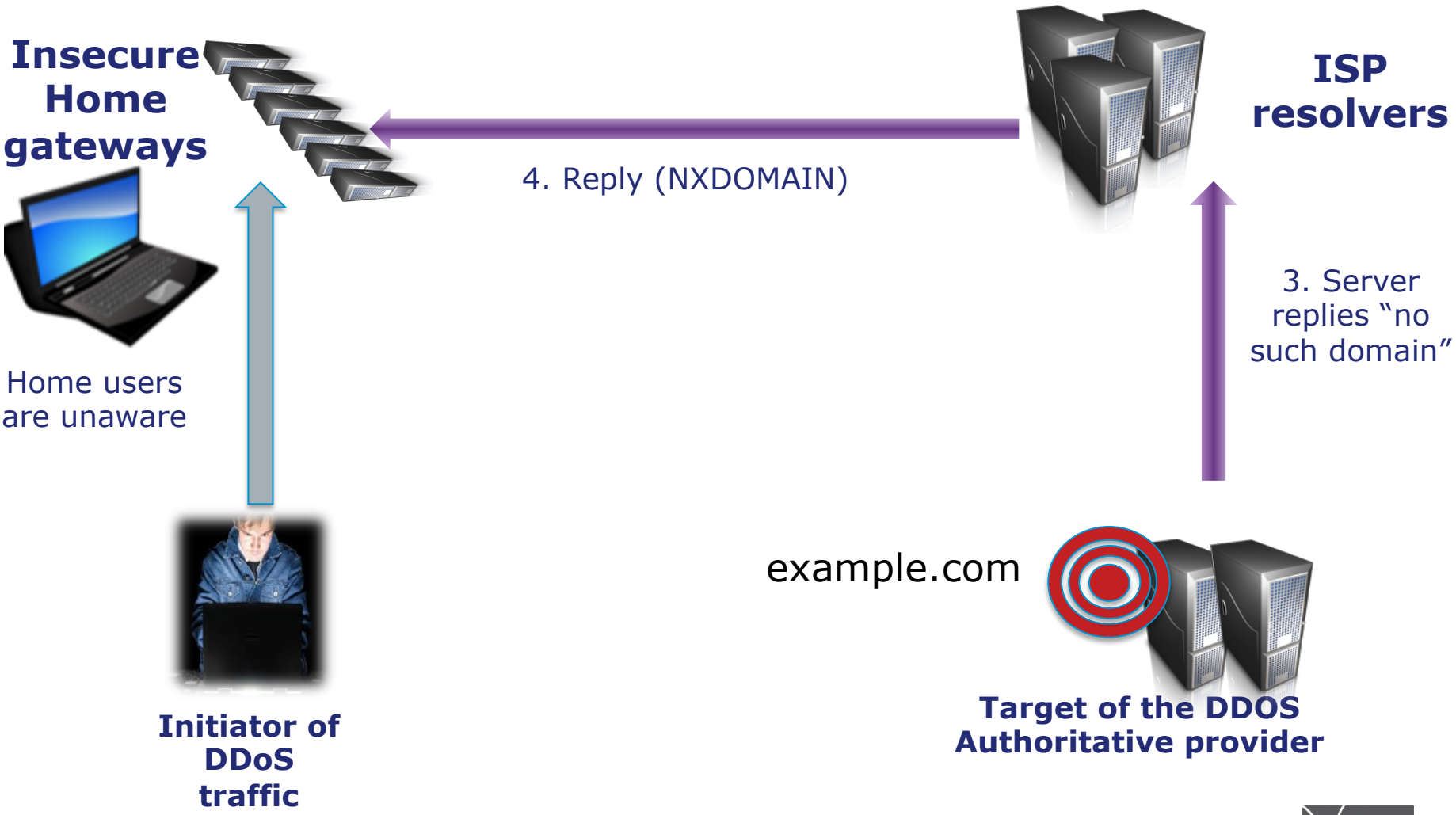
Initiator of DDoS traffic

example.com

Target of the DDOS Authoritative provider

© 2014 ISC

Initially, the target responds



© 2014 ISC

More requests flood in

Insecure Home gateways

1. More requests for randomstrings.www.example.com

ISP resolvers

Home users are unaware

Initiator of DDoS traffic

example.com

Target of the DDOS Authoritative provider

© 2014 ISC

Target is overwhelmed

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

ISP resolvers

2. Attempt to resolve

3. Server is unresponsive

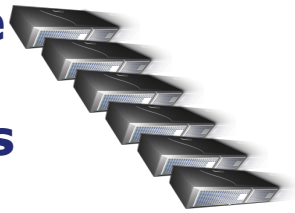
example.com

Target of the DDOS Authoritative provider

© 2014 ISC

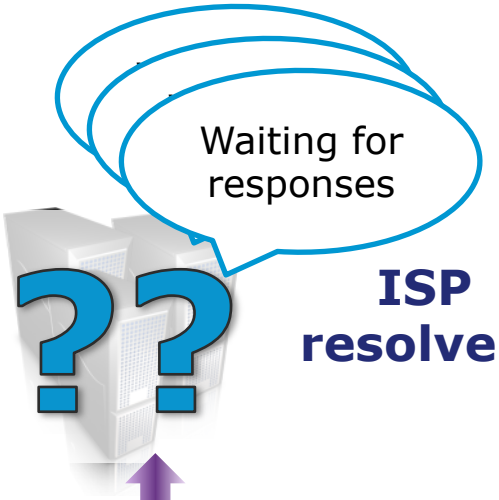
Resolver is degraded

Insecure Home gateways

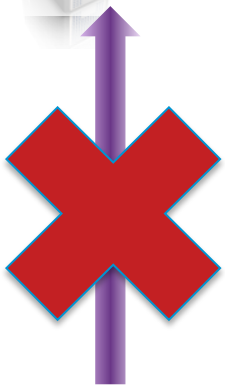


Home users are unaware

Initiator of DDoS traffic



ISP resolvers



3. Server is unresponsive

example.com

Target of the DDOS Authoritative provider

© 2014 ISC

Legitimate queries fail

© 2014 ISC

© 2014 ISC

MITIGATION TECHNIQUES

What can we do?

What has been tried in production?

© 2014 ISC

Option 1: “hair on fire”

© 2014 ISC

LIE
(about authority)

© 2014 ISC

Create a local answer

- Make recursive server temporarily authoritative for the target domain

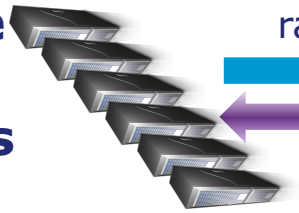
- *Problem of false-positives (might need white-lists if using scripted detection)*
- *Manual configuration change*
- *Need to undo the mitigation afterwards*

© 2014 ISC

Create a local answer

Auth for example.com

Insecure Home gateways



1. Requests for randomstring.www.example.com

2. Reply (NXDOMAIN)

ISP resolvers

Home users are unaware

Initiator of DDoS traffic

example.com

Target of the DDOS Authoritative provider

© 2014 ISC

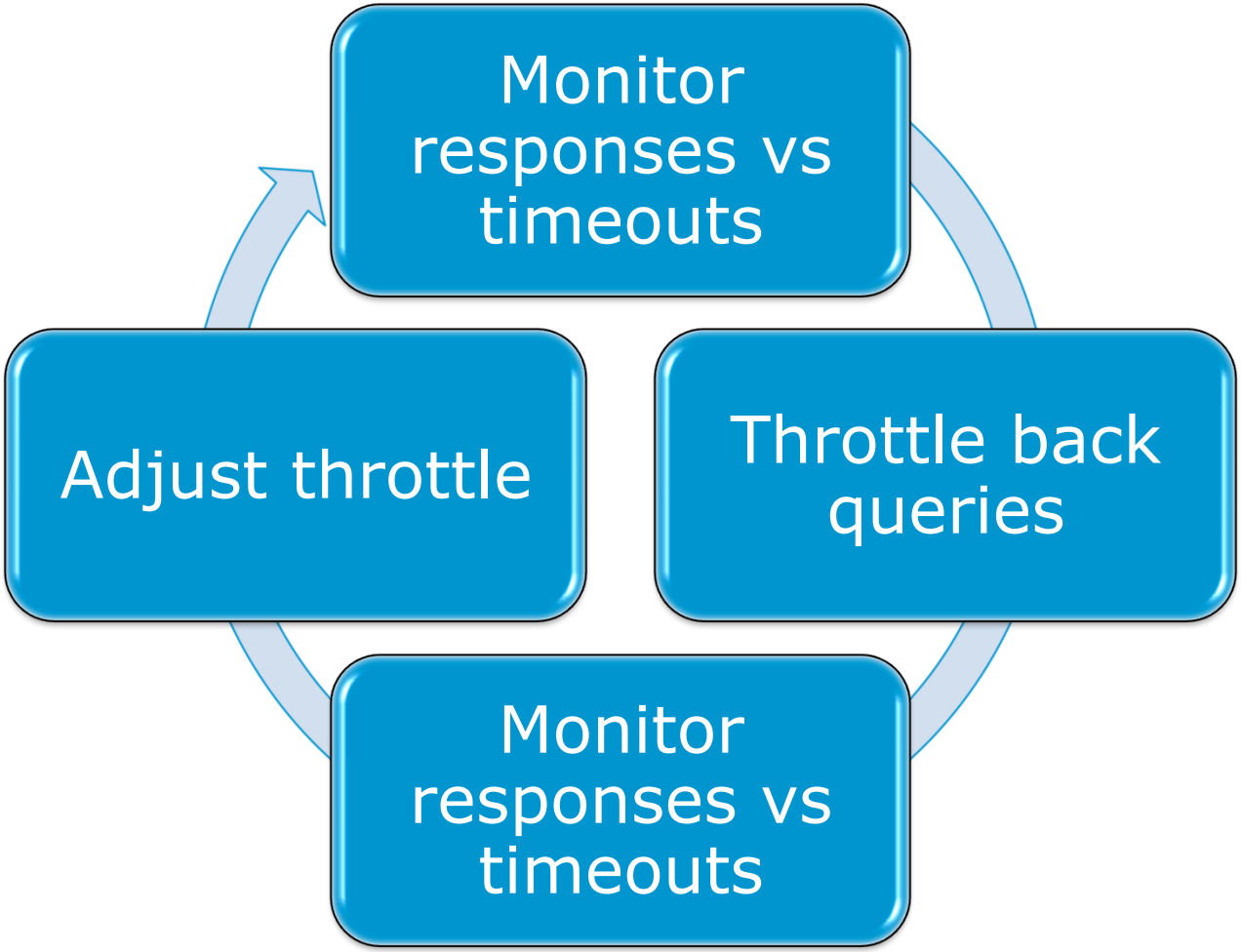
Option 2: Consider Automated filtering

(Near) Real Time Block Lists

- Detect ‘bad’ domain names or just the problematic queries & filter them at ingress to the resolver
- Nominum Vantio
- BIND DNS-RPZ
- There are usually fees associated with feeds

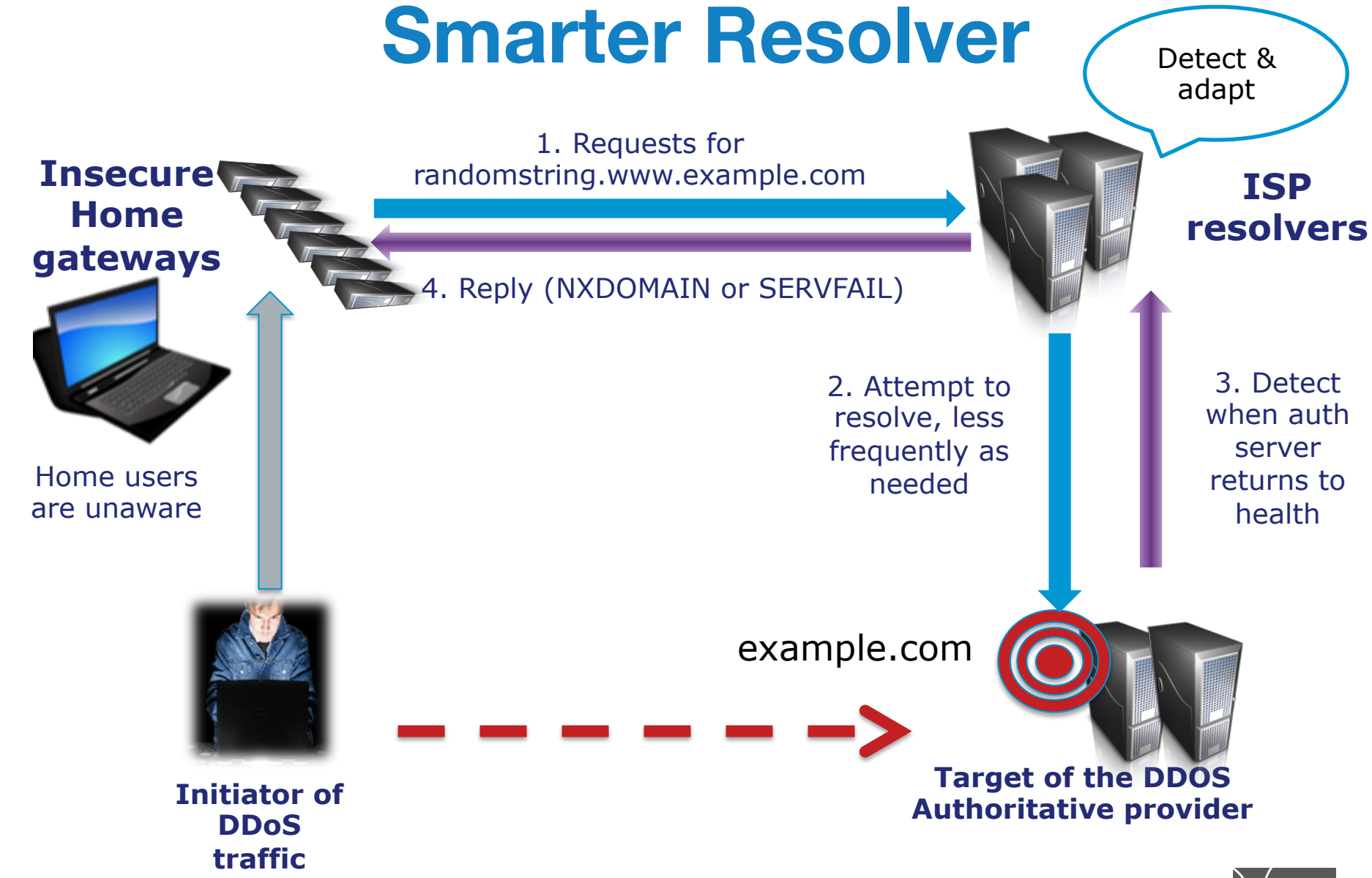
© 2014 ISC

Option 3: Consider making your resolvers smarter



© 2014 ISC

Smarter Resolver



© 2014 ISC

PER ZONE

PER SERVER

© 2014 ISC

fetches-per-server

- Per-server quota dynamically re-sizes itself based on the **ratio of timeouts to successful responses**
- Completely non-responsive server eventually scales down to fetches quota of 2% of configured limit.
- Similar in principle to what NLNetLabs is doing in Unbound

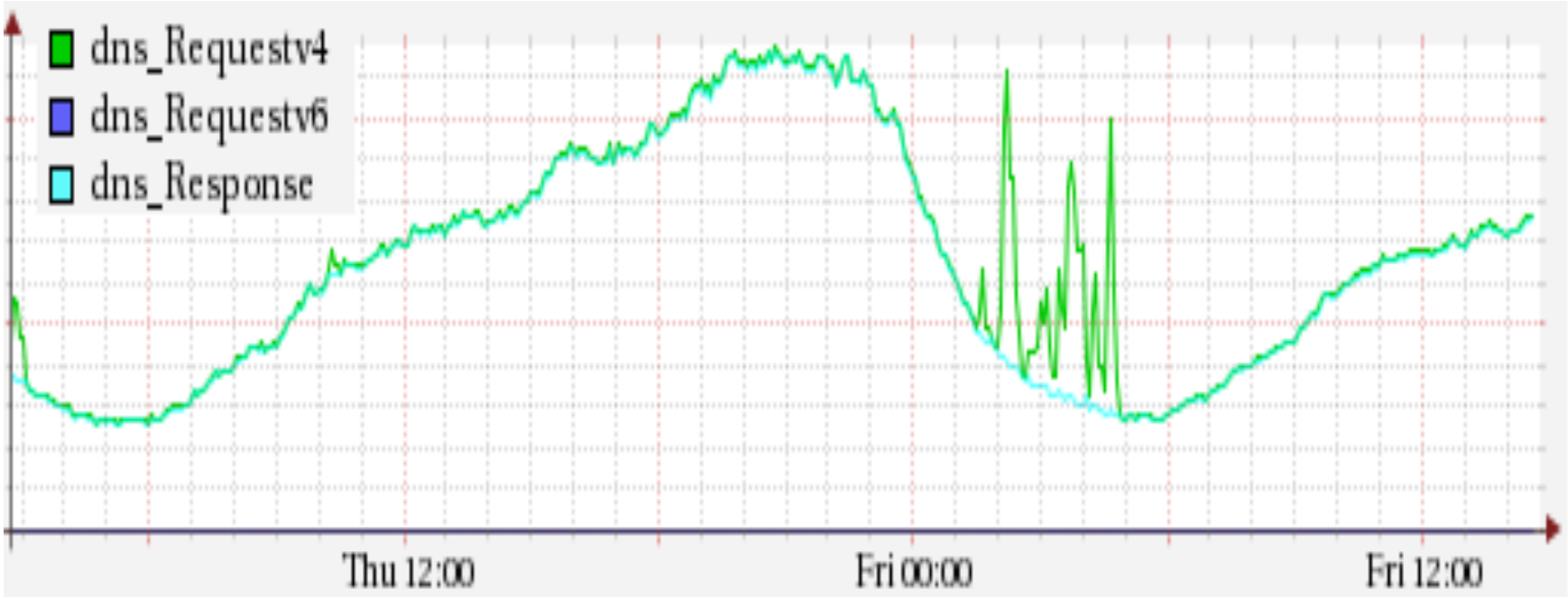
© 2014 ISC

fetches-per-zone

- Works with unique clients
- Default 0 (no limit enforced)
- Tune larger/smaller depending on normal QPS to avoid impact on popular domains
- In practice, this has been the winner so far for those using BIND

© 2014 ISC

Fetches-per-zone at Jazztel



Spanish triple-play ADSL carrier & ISP
Roberto Rodriguez Navio, Jazztel Networking Engineering
used with permission

© 2014 ISC

Still experimental

- Some controversy about adaptive approach vs blacklists
- Whitelists may be needed
- Per-server/zone settings
  - *Configurable override parameters for fetch limits on a per zone or per server basis*
- SERVFAIL cache (for client retries)
- Improved reporting & statistics

© 2014 ISC

Options Summary

1) Configure your resolver to **LIE**
   answer authoritatively yourself
2) Configure a **BLACK LIST** of domains under attack
   possibly subscribe to a feed for this
3) Consider **ADAPTIVE LIMITS**
   per server
   per zone

© 2014 ISC

Ideally, close the open resolvers!!


GOOD LUCK!