ISC Webinar:
Random Subdomain Resolver DDoS Mitigation

Cathy Almond, Sr. Technical Support Engineer

Welcome

- Presentation: 45 minutes
- All attendees are on mute
- Q&A at the end of this webinar
  - 10 minutes
  - Use WebEx chat window to submit questions
  - In the interest of time, please email unanswered questions to info@isc.org
- A recording of this event will be posted on the ISC web site

Presenter

Cathy Almond

ISC Senior Technical Support Engineer, Support Team Lead

Agenda

1. **Pseudo-random subdomain attack**
2. Recognizing the attack
3. Recommended mitigation
4. Results from live environments
5. Questions & Answers

The attack

- First seen in 2009 in China

https://indico.dns-oarc.net/event/12/contribution/3/material/slides/0.pdf

- Major reports to ISC from early 2014
- Attack is directed at DDOSing DNS authoritative provider
- Incidentally degrades ISP resolvers in the path

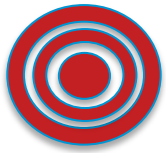
Unusual Queries

high volume of queries for non-existant sub-domains

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

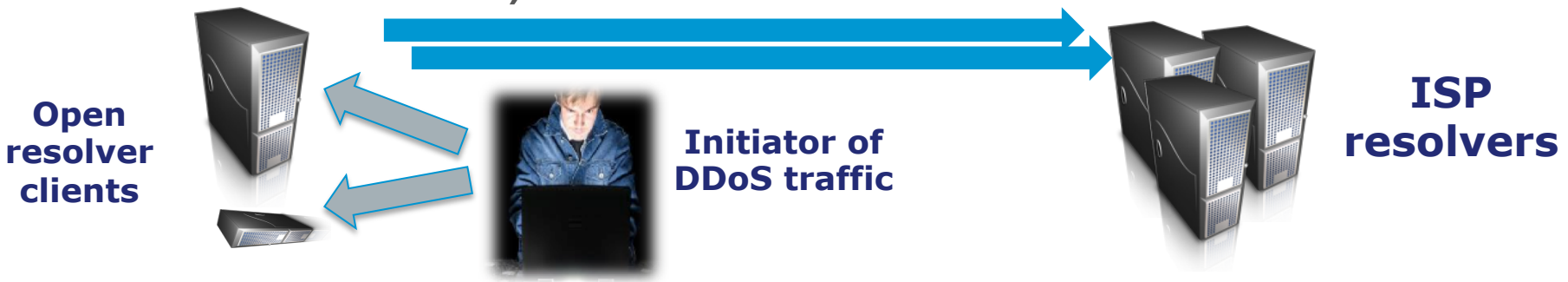
does not exist

exists



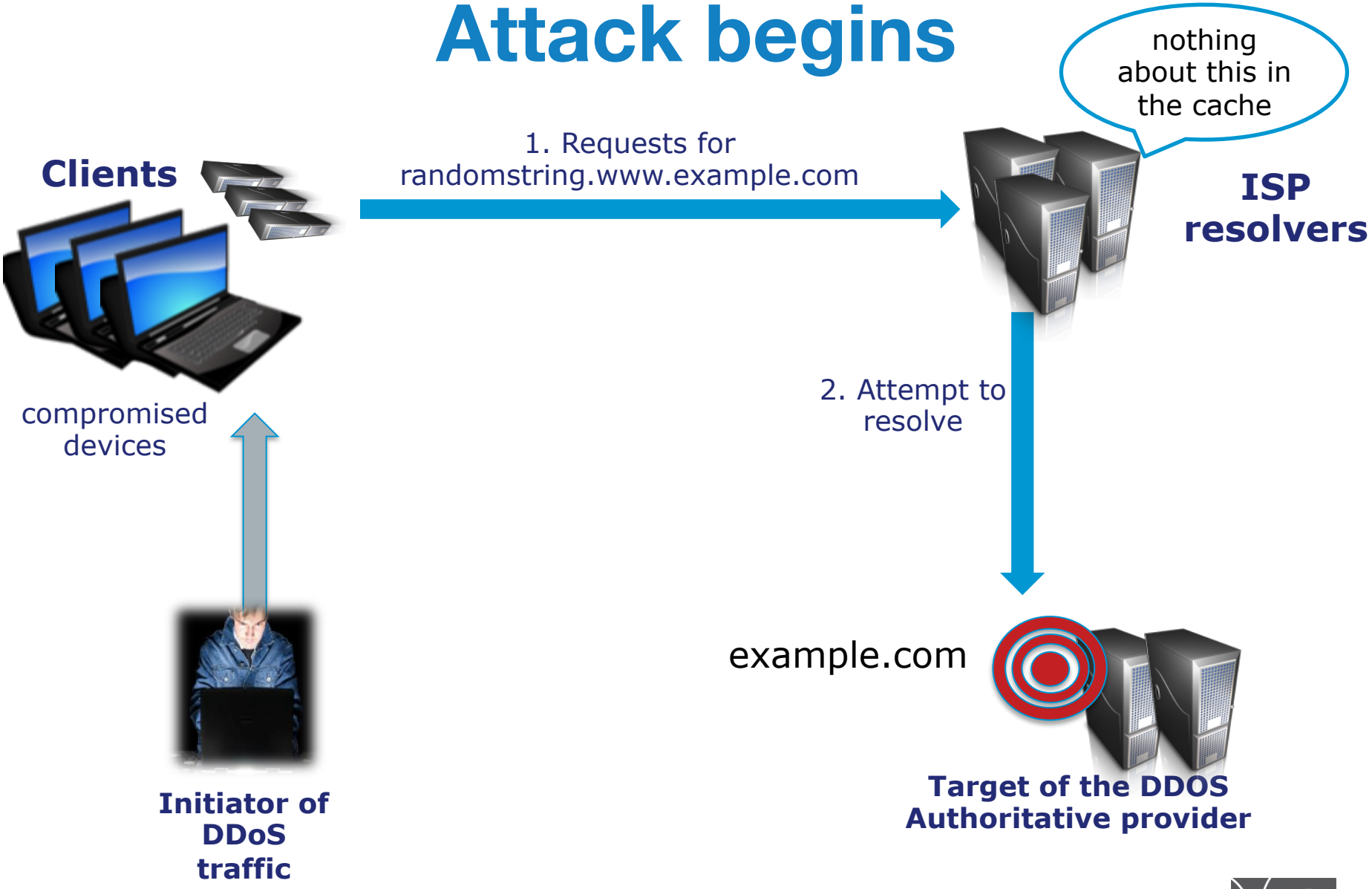
The source

- Open resolvers
  - your servers
  - your clients (CPE devices/proxies and forwarders)

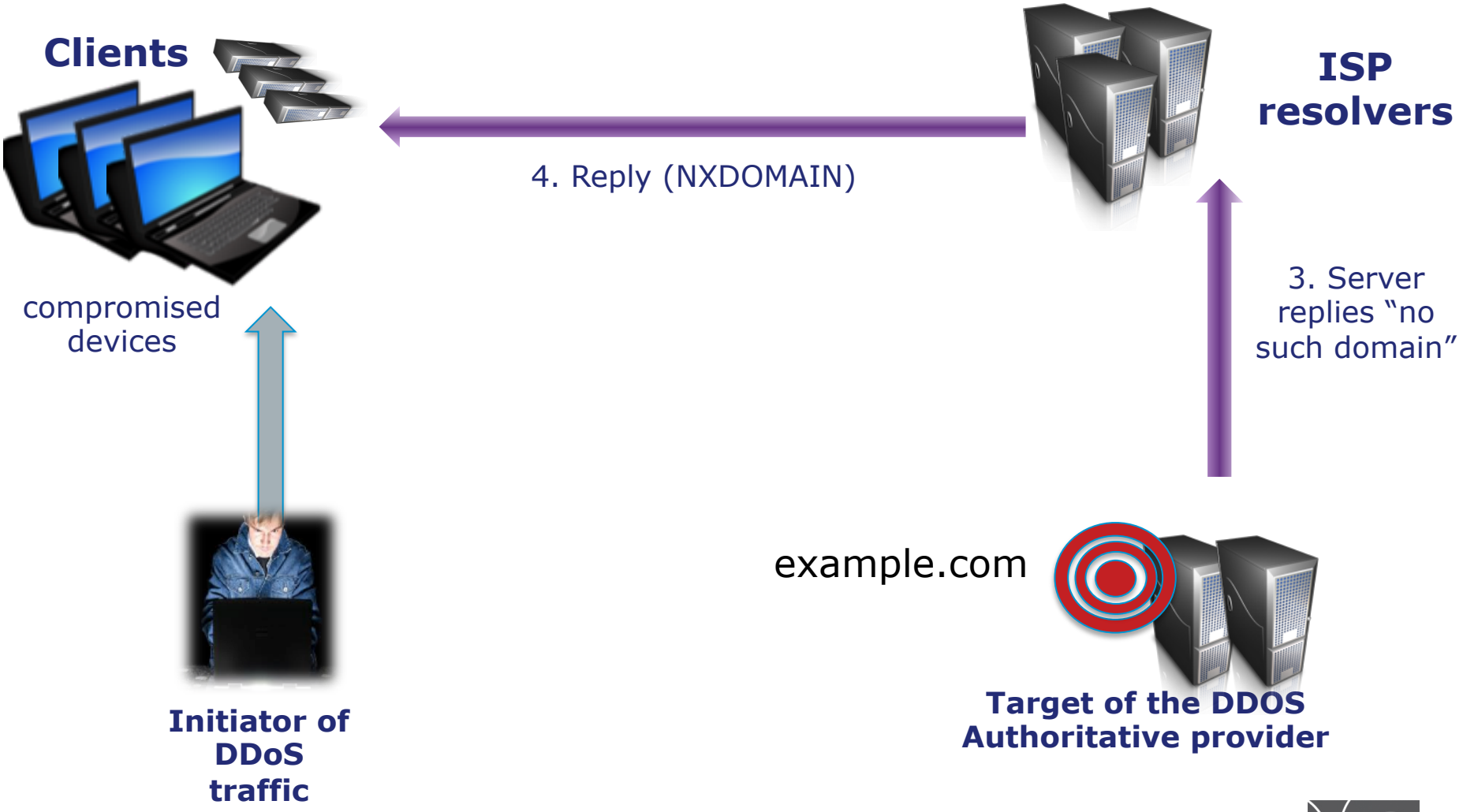


- Compromised clients (botnets)
- Compromised devices

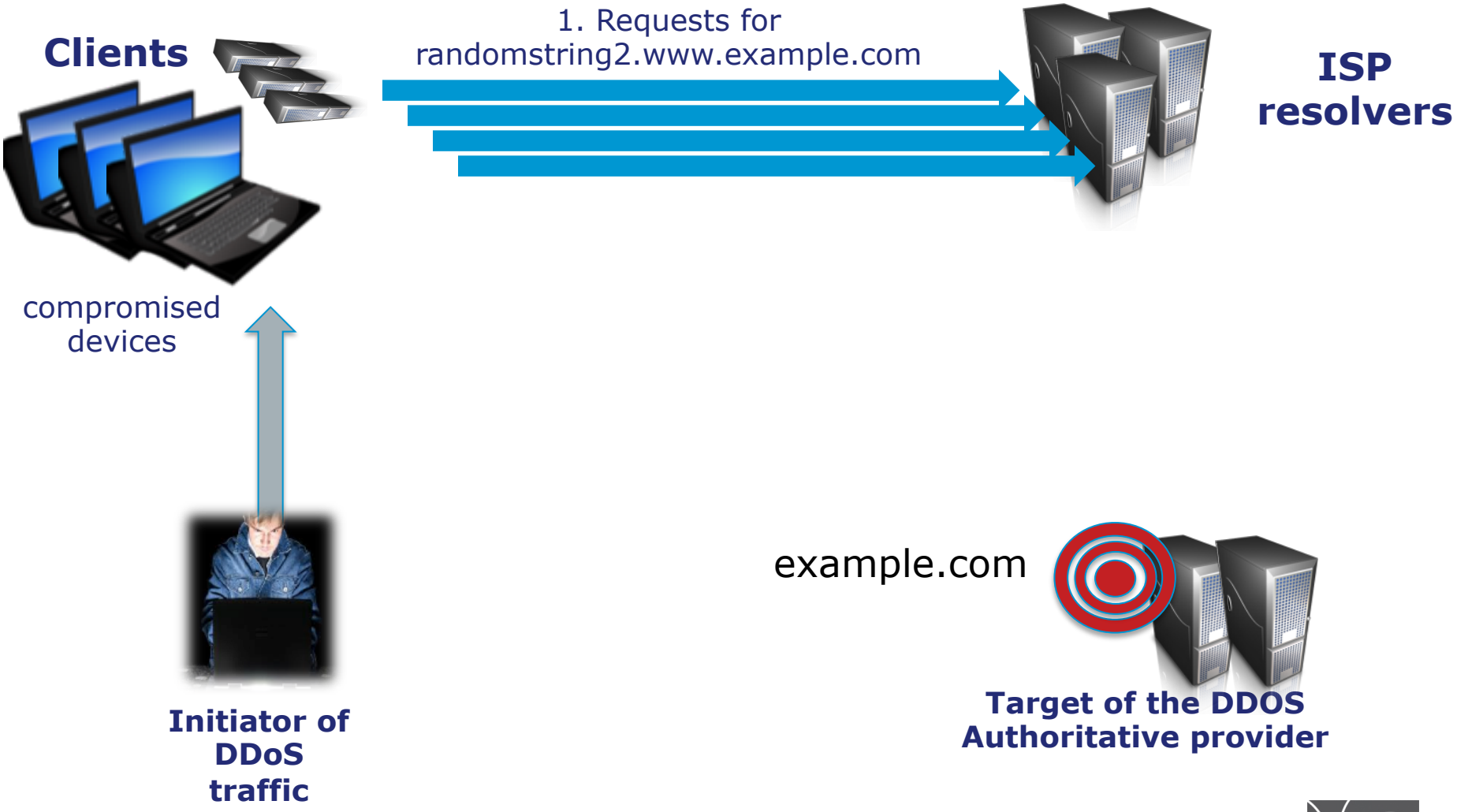
Attack begins



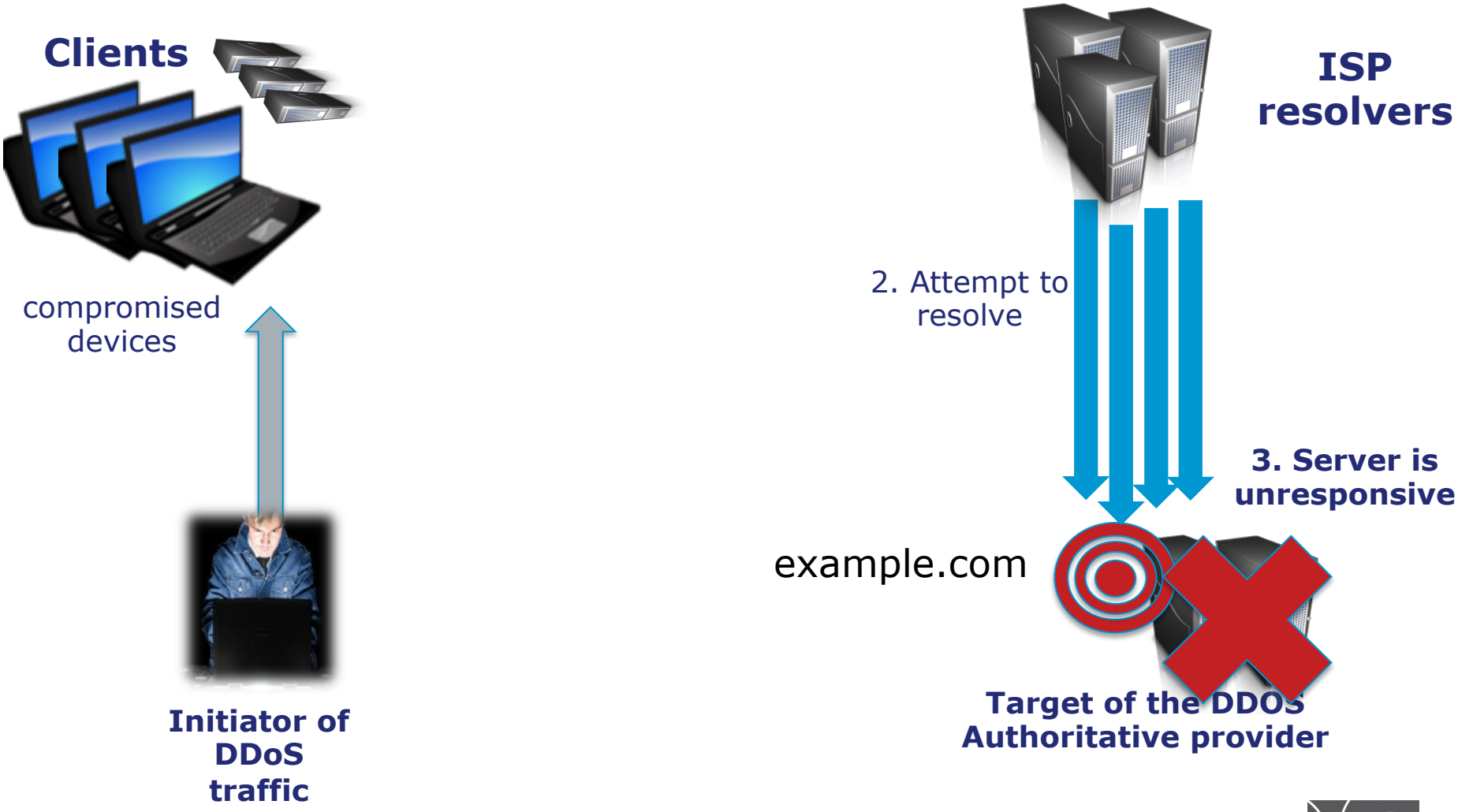
Initially, the target responds



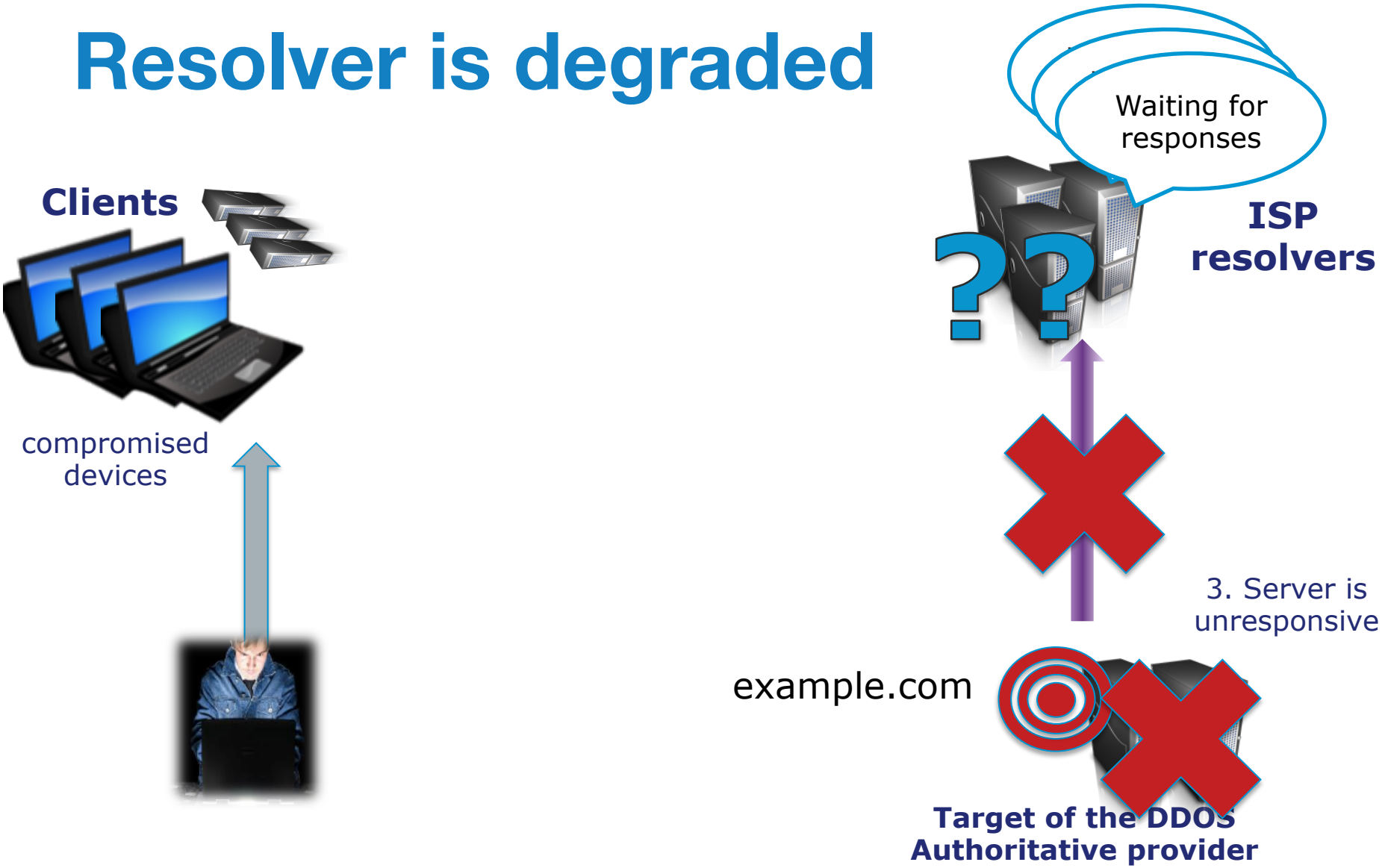
More requests flood in



Target is overwhelmed



Resolver is degraded



Legitimate queries fail

All Clients

Request for www.othersite.com

Reply SERVFAIL

ISP resolvers

Target of the DDOS Authoritative provider

Other domains affected

All Clients

Requests for other names from the same authoritative providers

ISP resolvers

Servers for example.com are overwhelmed by attack traffic and unable to respond to queries for names in other domains that they are authoritative for

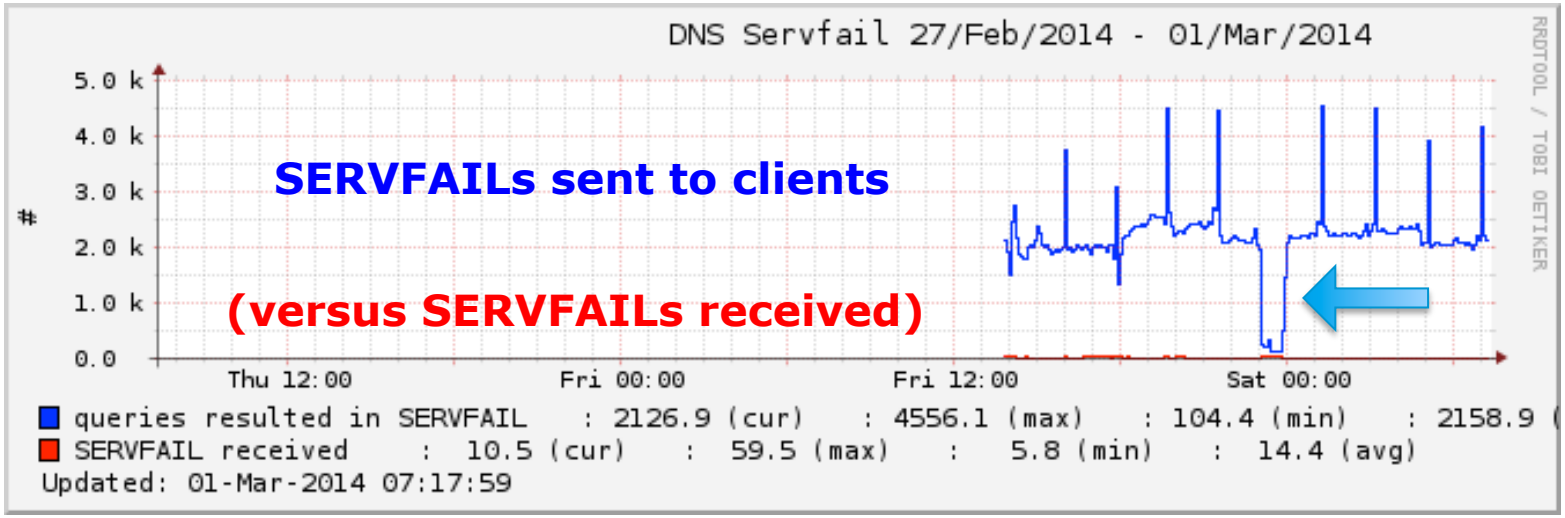
Target of the DDOS Authoritative provider

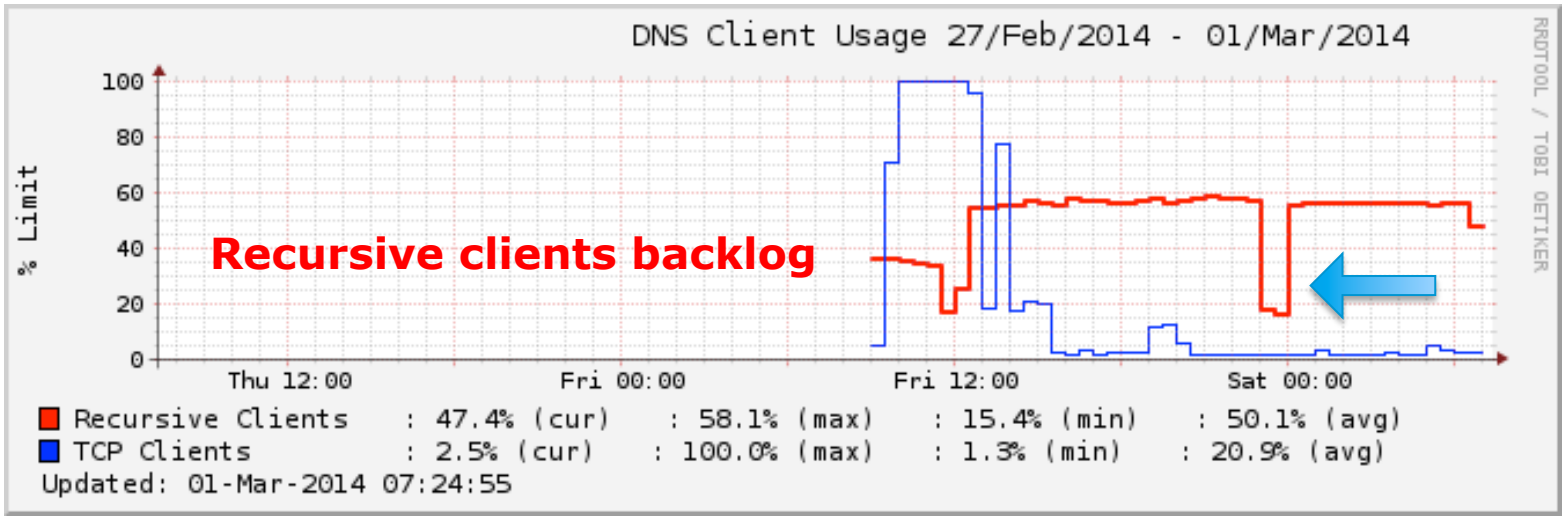
2. RECOGNIZING THE ATTACK

Symptoms

- ✓ Increased inbound client queries
- ✓ Increased outbound NXDOMAIN and SERVFAIL responses
- ✓ Resolution delays to clients
- ✓ Dropped responses
- ✓ Increased memory consumption
- ✓ Firewall connection table overflows

Evidence





Accurate diagnosis

1. Do you have a significant (and unusual for you) backlog of recursive client contexts?

   rndc status

   recursive clients: 0/1900/2000

   rndc recursing

2. What are those queries for?
3. Why are they in the backlog?
4. Where are they coming from?

ISC

Accurate diagnosis

- Backlog of recursive client queries
  - which queries are in the backlog?
  - is there a pattern?
  - originating from few or many clients?
- Open outbound sockets
  - to which servers; is there a pattern?
- *Query logging / query-errors logging*
- *Network packet traces*

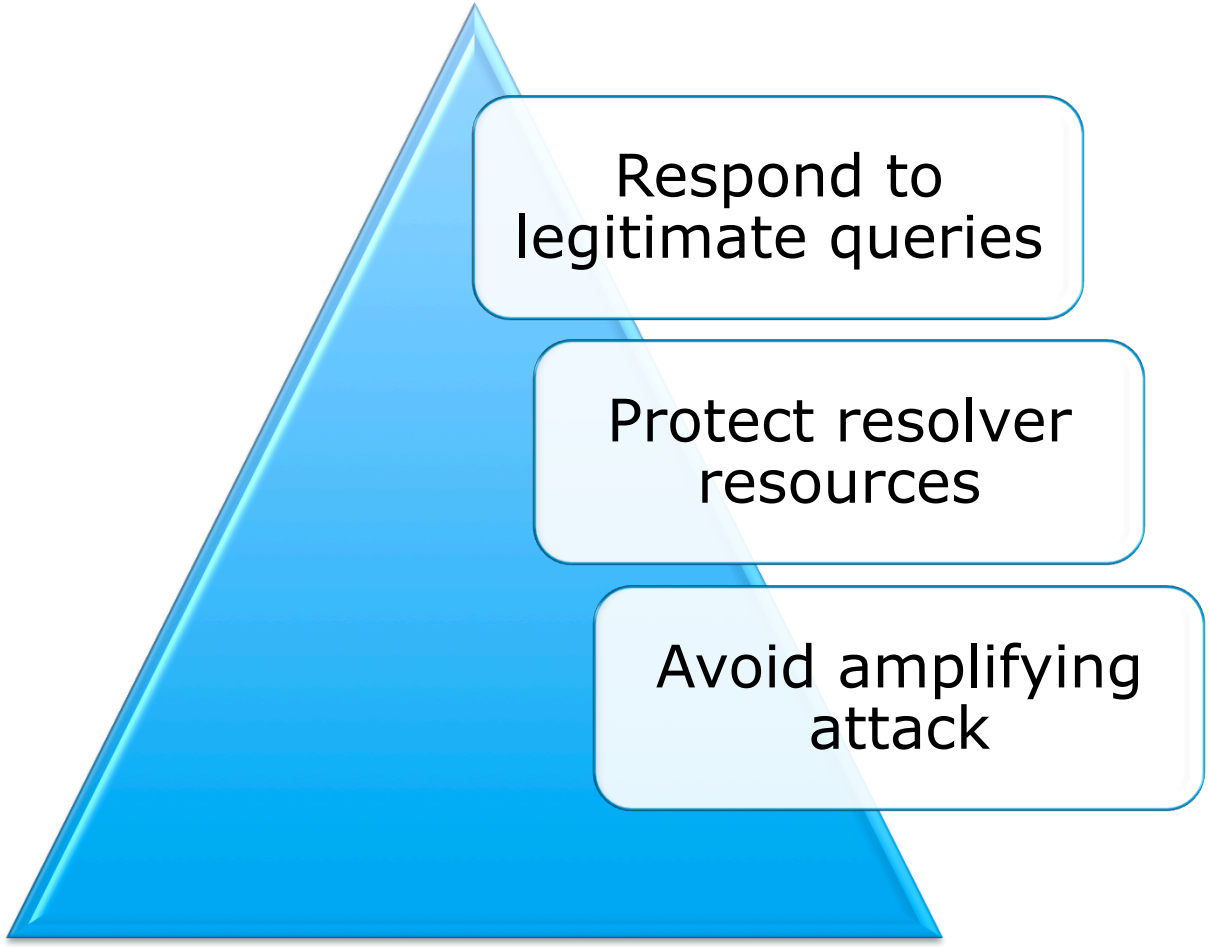
POLL

Have you been impacted by a pseudo-random domain attack?

Yes **No** **?? Not Sure**

3. MITIGATION

Mitigation Goals



Don’t…

- Panic!!
- Assume that increasing server resources (e.g. recursive client contexts, sockets, network buffers etc..) is going to help *
- Block your clients (although, it depends…)

* For very large/busy resolvers, take a look at BIND 9.10 and new configuration option --with-tuning=large

Step 1: Lie if necessary

- Make recursive server temporarily authoritative for the target domain
  - Local zone
  - DNS-RPZ (*qname-wait-recurse no;)

- *Manual configuration change*
- *Need to undo the mitigation afterwards*

Step 2: Filtering

(Near) Real Time Block Lists

- Detect ‘bad’ domain names or just the problematic queries & filter them
- Local auto-detection scripts that dynamically add local authoritative zones (potential false-positives)
- BIND DNS-RPZ *
- Costs associated with feeds

* Requires ‘qname-wait-recurse no;’

Step 3: Rate-limiting

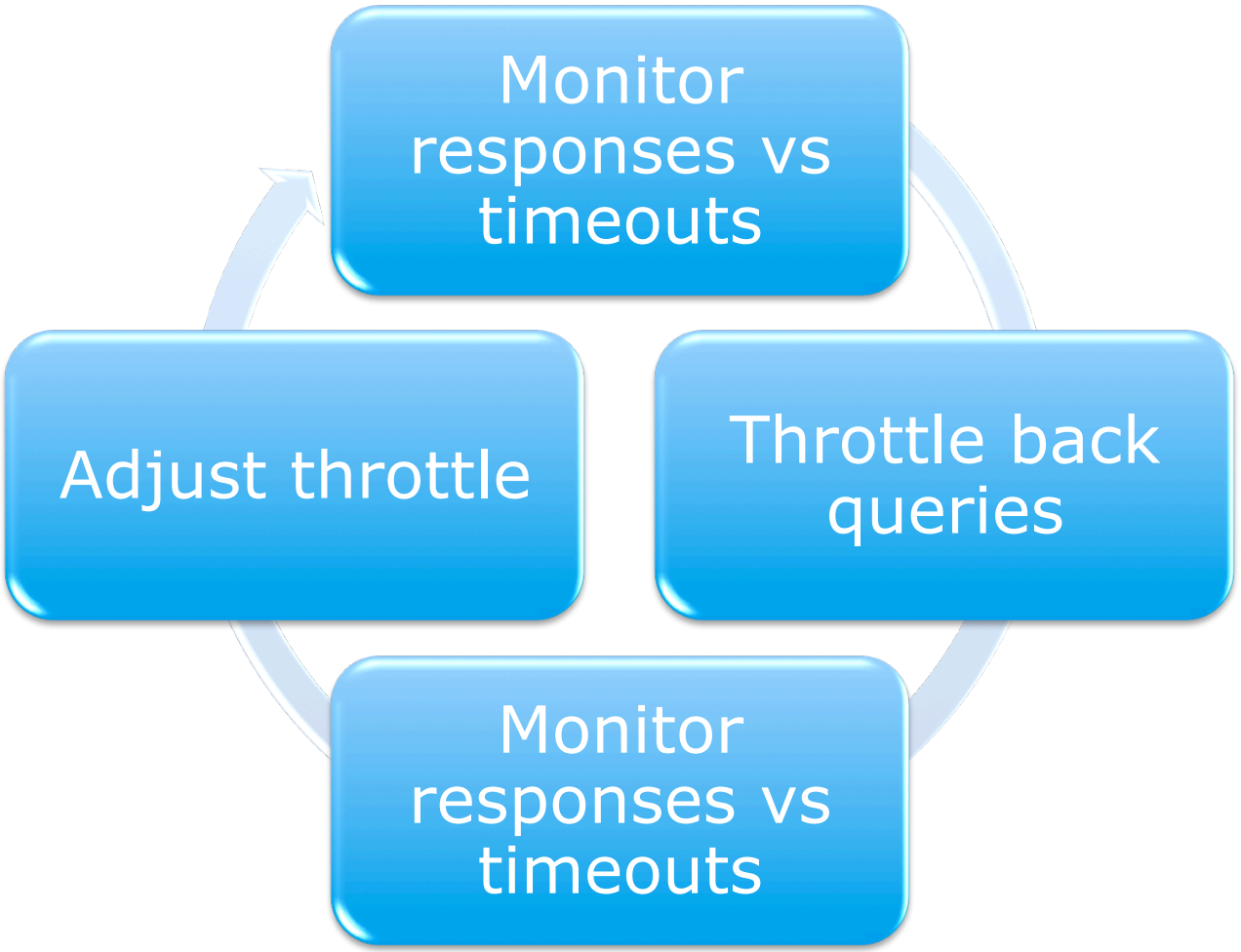
- Experimental BIND code
  - available now on request from support@isc.org
  - https://kb.isc.org/article/AA-01178
- Publicly available (soon) in Open Source with BIND 9.10.3
  - look for a call for beta testers in late July

New BIND tuning knobs

PER ZONE

PER SERVER

NEW: fetches-per-server



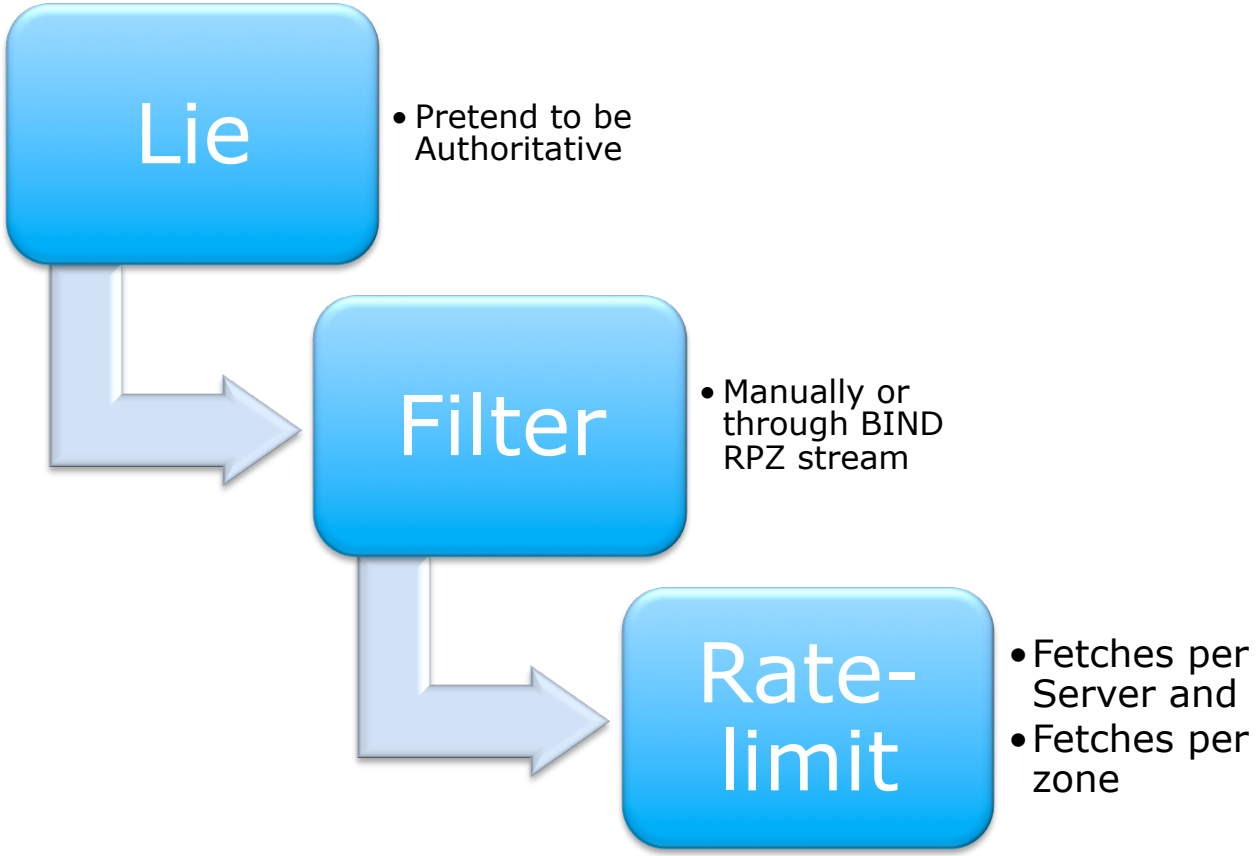
fetches-per-server

- 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 (loosely) in principle to what NLnet Labs is doing in Unbound

NEW: fetches-per-zone

- Works with unique clients (as does fetches-per-server)
- Does NOT auto-adjust
- Tune larger/smaller depending on normal QPS
- Use as a ‘backstop’ for fetches-per-server

Mitigation Summary

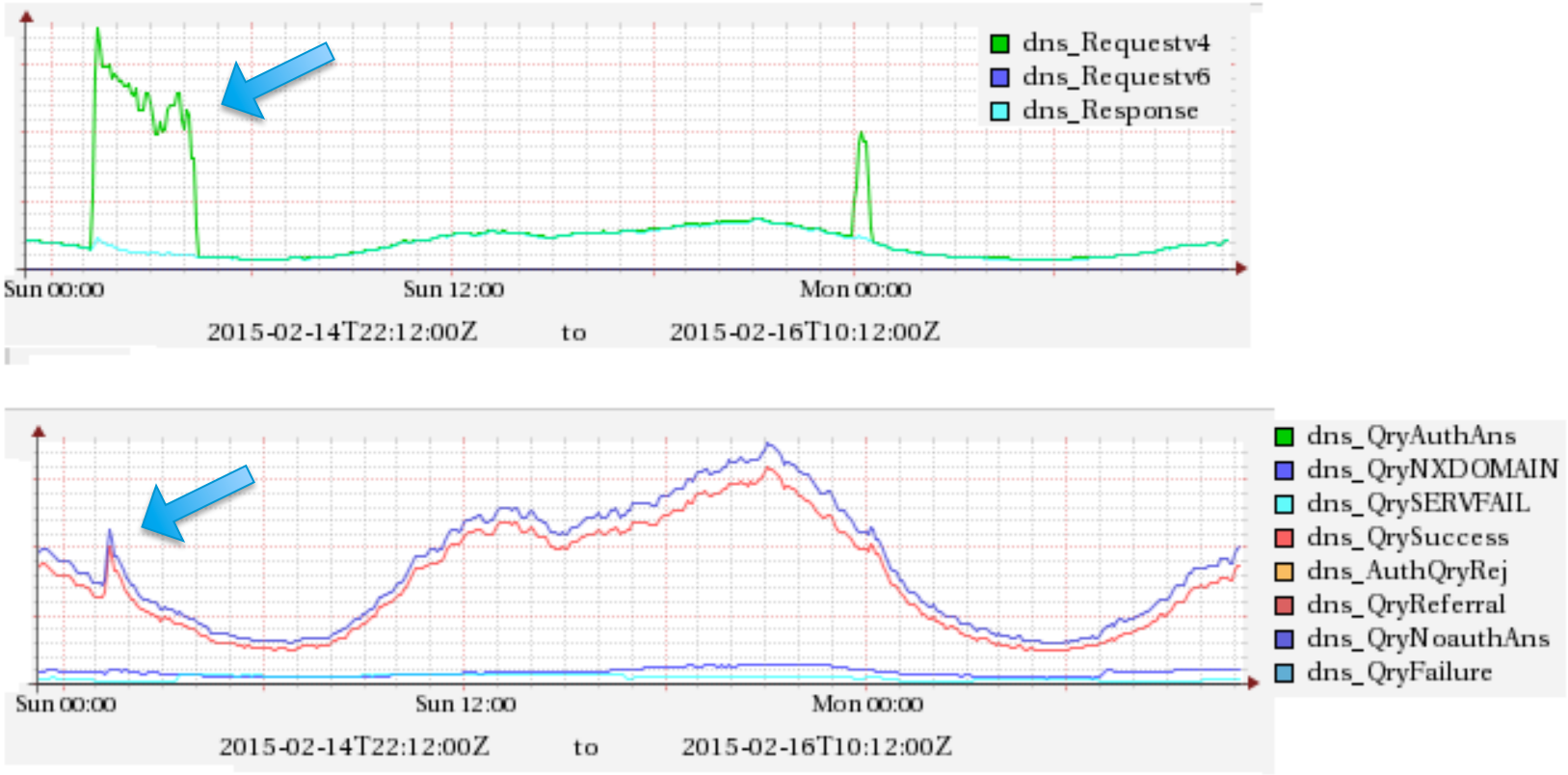


4. RESULTS FROM LIVE PRODUCTION SYSTEMS

fetches-per-zone

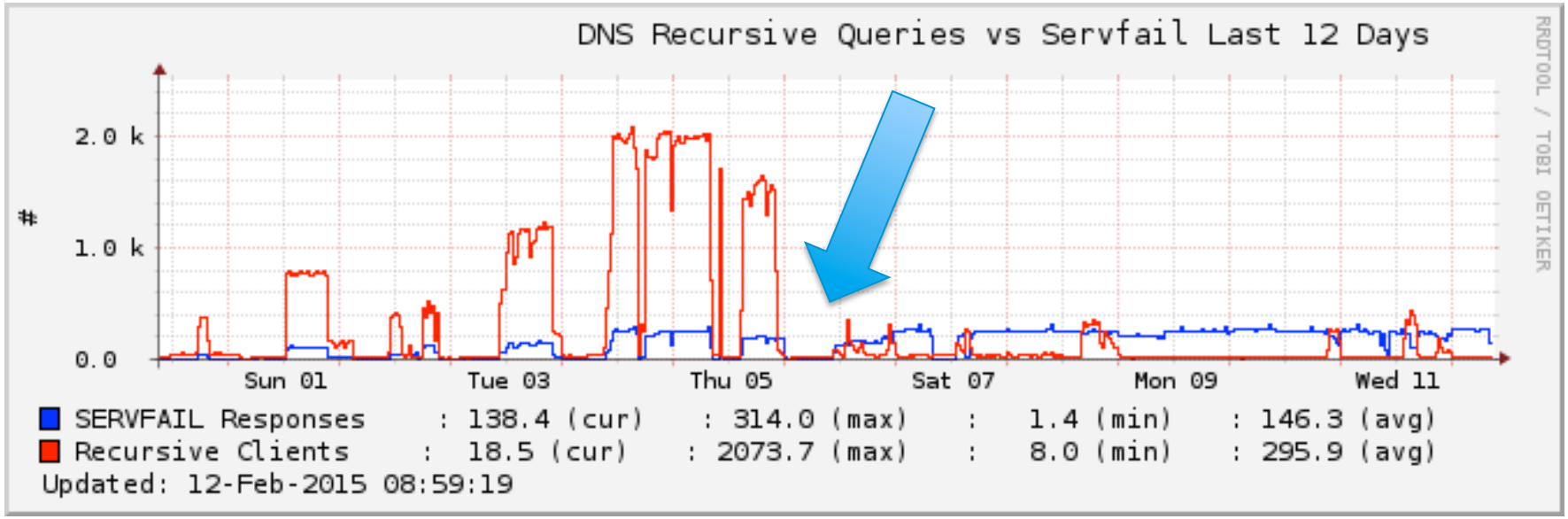
Spanish triple-play ADSL carrier & ISP
Roberto Rodriguez Navio, Jazztel Networking Engineering
used with permission

More on fetches per zone

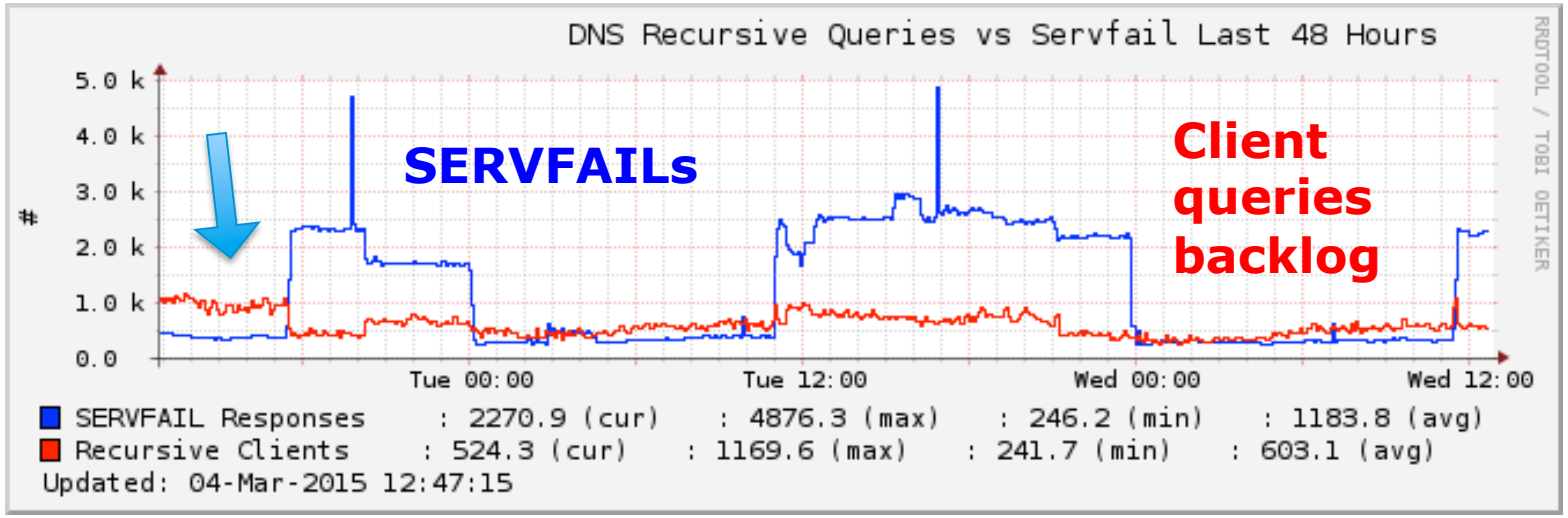


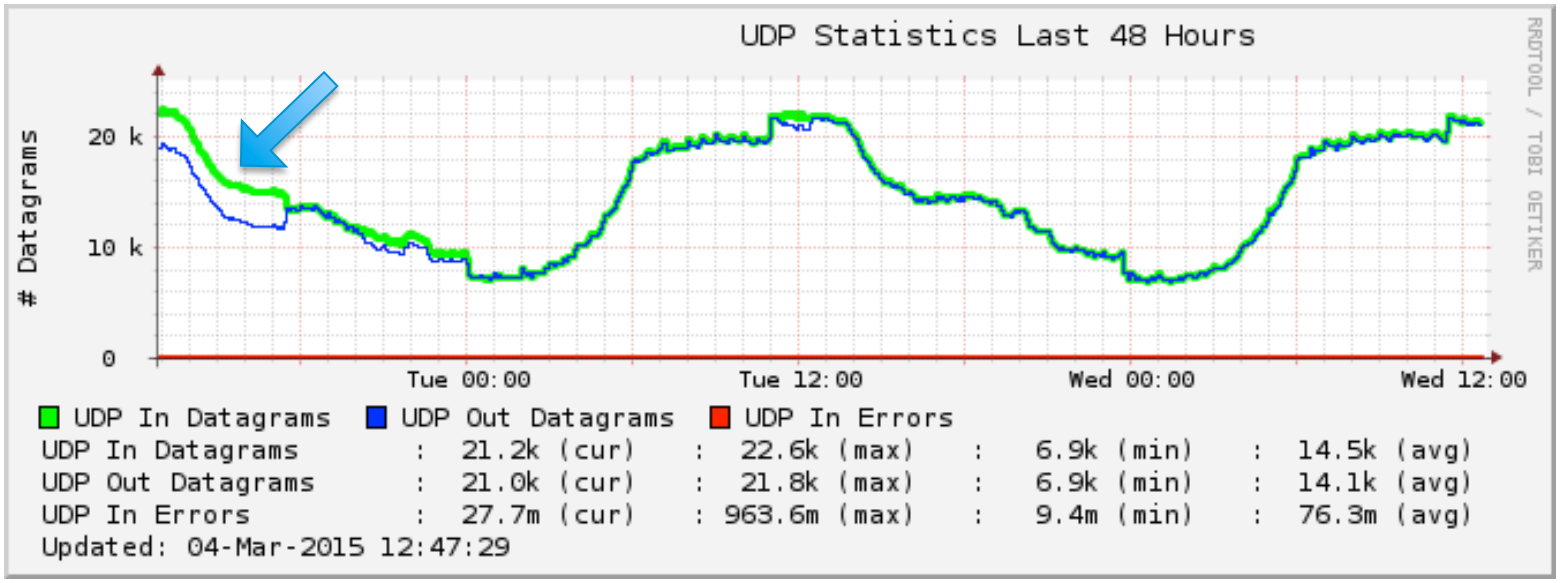
Spanish triple-play ADSL carrier & ISP
Roberto Rodriguez Navio, Jazztel Networking Engineering
used with permission

fetches-per-server



per-zone v. per-server





Comparison

Fetches Per Server

- Rate-limits per server
- Impacts queries for all zones served by the same machine
- Dynamically re-sizes based on the ratio of timeouts to successful responses

Fetches Per Zone

- Rate-limits per zone
- Manually tuned
- Set to larger value on higher-performance machines

What will the user see?

- Situation normal – no change to their usual experience (for most)
- (Some) SERVFAIL responses to names in zones that are also served by under-attack authoritative servers (collateral damage)
- NXDOMAIN responses for names in legitimate zones for which we ‘lie’

Client gets ..

No Response

- Legitimate queries will retry
- Could be a problem for forwarding servers when the forwarder ‘doesn’t respond

SERVFAIL

- Legitimate queries will retry
- Doesn’t protect resolver as much, but is the ‘correct’ response when the authoritative server is overwhelmed

NXDOMAIN

- Stops client from retrying
- Same response the authority would send for the DDoS queries
- (May be) wrong response to genuine clients

Protect your Resolvers

- High volume of queries for non-existent domains
- Rapid increase in backlog of client queries on the resolver
- Install filter with dynamic feed or
- **New BIND recursive client rate-limiting**

QUESTIONS

info@isc.org, bind-suggest@isc.org, cathya@isc.org

https://kb.isc.org/article/AA-01178

BIND Roadmap