FRNOG 25 Meeting:
BIND9 – Recursive Client Rate limiting

Cathy Almond, Sr. Technical Support Engineer
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. Any questions?
The attack - unusual queries

high volume of queries for non-existant sub-domains

<randomstring>.www.example.com <a
does not exist

exists
The source

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

- Compromised clients (botnets)
- Compromised devices
Attack begins

Initiator of DDoS traffic → Clients

1. Requests for randomstring.www.example.com

examples.com

nothing about this in the cache

ISP resolvers

Target of the DDoS Authoritative provider

compromised devices
Initially, the target responds

Clients

compromised devices

Initiator of DDoS traffic

example.com

Target of the DDoS Authoritative provider

ISP resolvers

3. Server replies “no such domain”

4. Reply (NXDOMAIN)

© 2015 ISC
More requests flood in

1. Requests for randomstring2.www.example.com

Clients

compromised devices

Initiator of DDoS traffic

ISP resolvers

example.com

Target of the DDoS Authoritative provider
Target is overwhelmed

Initiator of DDoS traffic

Clients

compromised devices

2. Attempt to resolve

example.com

ISP resolvers

3. Server is unresponsive

Target of the DDoS Authoritative provider
Resolver is degraded

Clients

compromised devices

ISP resolvers

Waiting for responses

example.com

3. Server is unresponsive

Target of the DDOS Authoritative provider
Legitimate queries fail

All Clients

Request for www.othersite.com

ISP resolvers

Waiting for example.com responses

Reply SERVFAIL

No more resources available to handle new queries!

Target of the DDOS
Authoritative provider
2. RECOGNIZING THE ATTACK
Symptoms

☑ Many SERVFAIL responses
☑ Increased inbound client queries
☑ Resolution delays to clients
☑ Dropped responses
☑ Increased memory consumption
☑ Increased NXDOMAIN responses
☑ Firewall connection table overflows
Evidence

SERVFAILs sent to clients
(versus SERVFAILs received)

Recursive clients backlog
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?
3. MITIGATION
Mitigation Goals

- Respond to legitimate queries
- Protect resolver resources
- Avoid amplifying attack
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

PER ZONE

PER SERVER
NEW: fetches-per-server

- Monitor responses vs timeouts
- Adjust throttle
- Throttle back queries
- Monitor responses vs timeouts
**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

- **Lie**
  - Pretend to be Authoritative

- **Filter**
  - Manually or through BIND RPZ stream

- **Rate-limit**
  - Fetches per Server and
  - Fetches per zone
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

DNS Recursive Queries vs Servfail Last 48 Hours

SERVFAILs

Client queries backlog

UDP Statistics Last 48 Hours

© 2015 ISC
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

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

SERVFAIL

* fetches-per-server
- 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

* Default behavior (configurable, except for NXDOMAIN)
Further Resources

- Recursive Client Rate Limiting
  - available now in BIND 9.8.8 and 9.10.3
  - [https://kb.isc.org/article/AA-01304](https://kb.isc.org/article/AA-01304)

- Feature Webinar Recording available (8 July 2015)
  - [https://www.isc.org/mission/webinars/](https://www.isc.org/mission/webinars/)

- FAQs:
  - [https://kb.isc.org/article/AA-01316](https://kb.isc.org/article/AA-01316)
QUESTIONS

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

https://kb.isc.org/article/AA-01304