Pseudo Random DNS Query
Attacks & Resolver
Mitigation Approaches

APRICOT 2015
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
Identifying the attack

high volume of queries for non-existent sub-domains

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

does not exist

exists
Insecure Home gateways

1. Requests for randomstring.www.example.com

Initiator of DDoS traffic

ISP resolvers

2. Attempt to resolve

example.com

Target of the DDoS Authoritative provider

Home users are unaware

nothing about this in the cache
Initially, the target responds

1. Initiator of DDoS traffic
2. Insecure Home gateways
3. Server replies "no such domain"
4. Reply (NXDOMAIN)

Target of the DDoS
Authoritative provider

ISP resolvers

Home users are unaware

example.com

More requests flood in

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

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

ISP resolvers

example.com

Target of the DDoS Authoritative provider
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
Resolver is degraded

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

ISP resolvers

Waiting for responses

example.com

Target of the DDoS
Authoritative provider

3. Server is unresponsive
Legitimate queries fail

Insecure Home gateways

1. Request for www.example.com

ISP resolvers

Waiting for responses

Home users are unaware

Initiator of DDoS traffic

Target of the DDoS Authoritative provider
MITIGATION TECHNIQUES

What can we do?

What has been tried in production?
Option 1: “hair on fire”
LIE
(about authority)
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
Create a local answer

Insecure Home gateways

1. Requests for randomstring.www.example.com

2. Reply (NXDOMAIN)

ISP resolvers

Auth for example.com

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
Option 3: Consider making your resolvers smarter

- Monitor responses vs timeouts
- Adjust throttle
- Throttle back queries
- Monitor responses vs timeouts
Smarter Resolver

1. Requests for randomstring.www.example.com
2. Attempt to resolve, less frequently as needed
3. Detect when auth server returns to health
4. Reply (NXDOMAIN or SERVFAIL)

Insecure Home gateways

Home users are unaware

Initiator of DDoS traffic

Target of the DDoS
Authoritative provider

example.com

Detect & adapt

ISP resolvers
PER ZONE

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.
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
Fetches-per-zone at Jazztel

Spanish triple-play ADSL carrier & ISP
Roberto Rodriguez Navio, Jazztel Networking Engineering
used with permission
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
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
Ideally, close the open resolvers!!

www.shadowserver.org
GOOD LUCK!