Recent DNS-based DDoS Attacks

Johan Ihrén
Autonomica

(with support from others in SSAC)

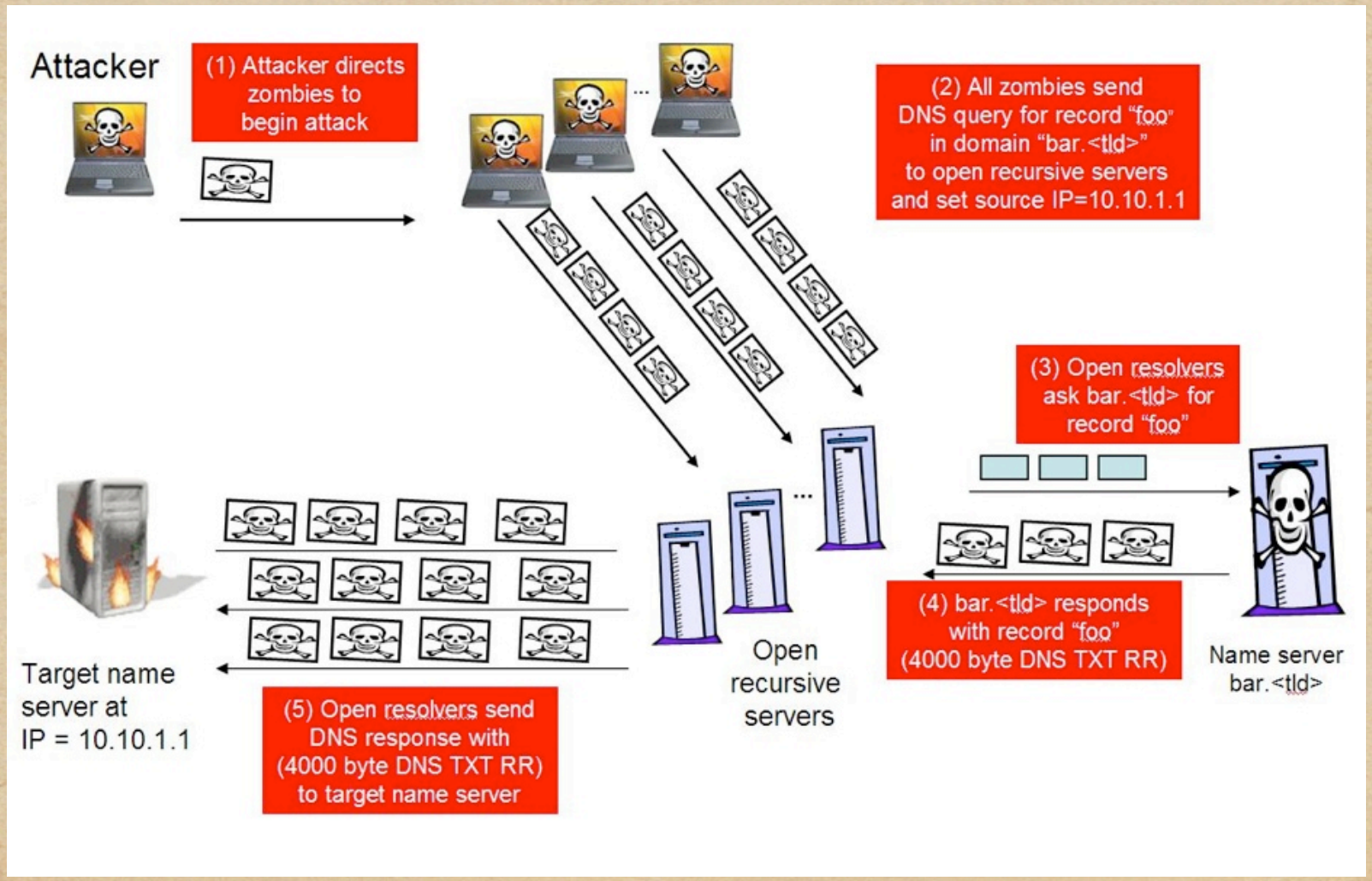
Once Upon A Time...

- The Internet was a friendly place where it was easy to help your friends and neighbors:
  - Open SMTP relay were the norm rather than the exception
  - Open recursive name servers also
  - etc.

Things Change

- The spam problem has long caused SMTP relaying to become a hazardous practice
  - If you're not very careful you will be black-listed and that's painful
- DNS seems to be headed in the same direction

Scenario of an Attack



What is the Problem?

- The problem is that the Internet tradition of open recursive name servers is being abused
  - A "recursive" name server is a server that is prepared to go look up answers to questions it doesn't already know the answer for

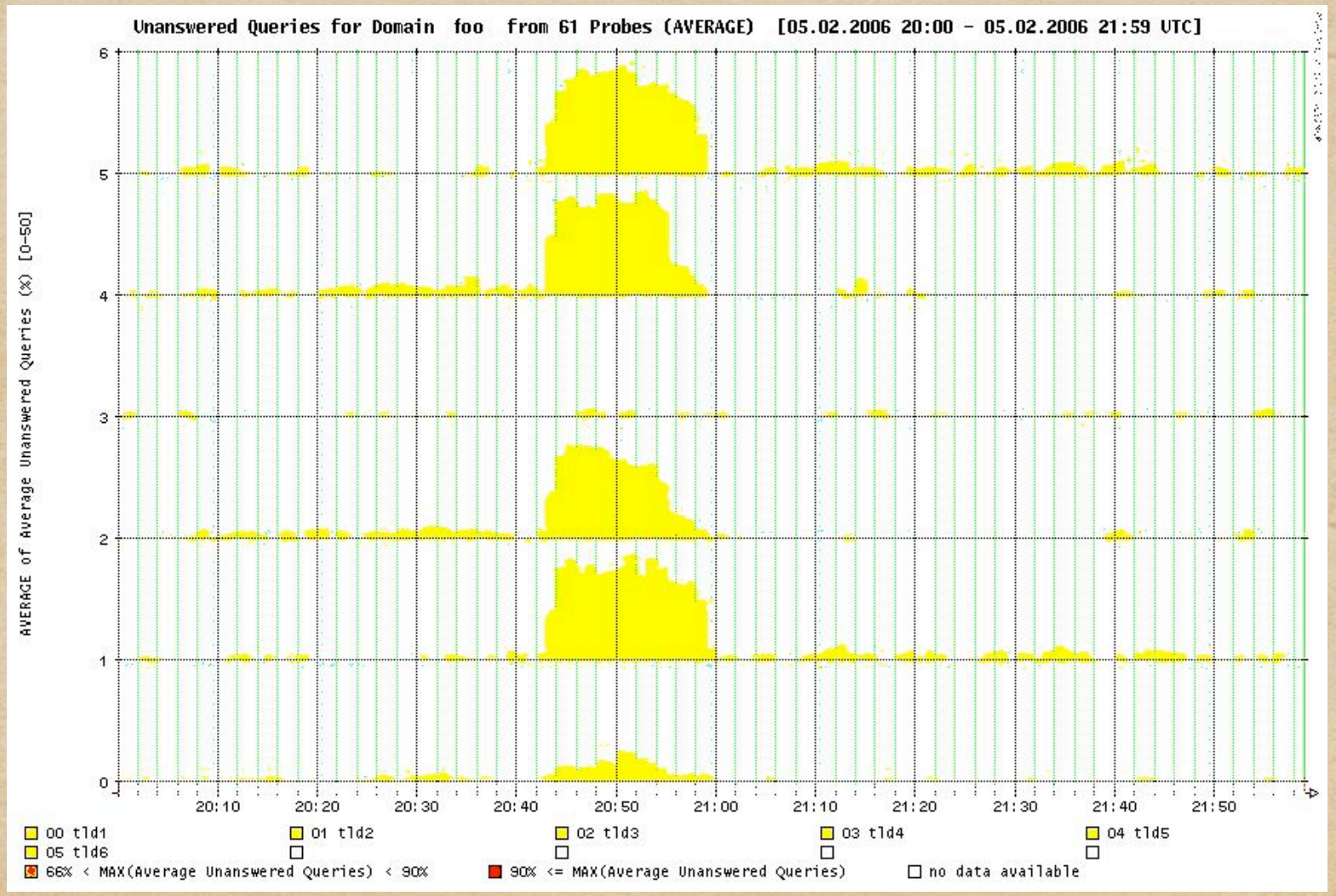
What is the Problem?

- The problem is that the Internet tradition of open recursive name servers is being abused
  - An "open recursive" name server is a server that offers recursive service to anybody, thereby opening up to being used as an amplifier

What is the Problem?

- The problem is very real in the sense that this attack has successfully been used to seriously affect major DNS infrastructure like TLDs
- Not for a prolonged period of time, though, although that is hardly an assurance

This is The Problem

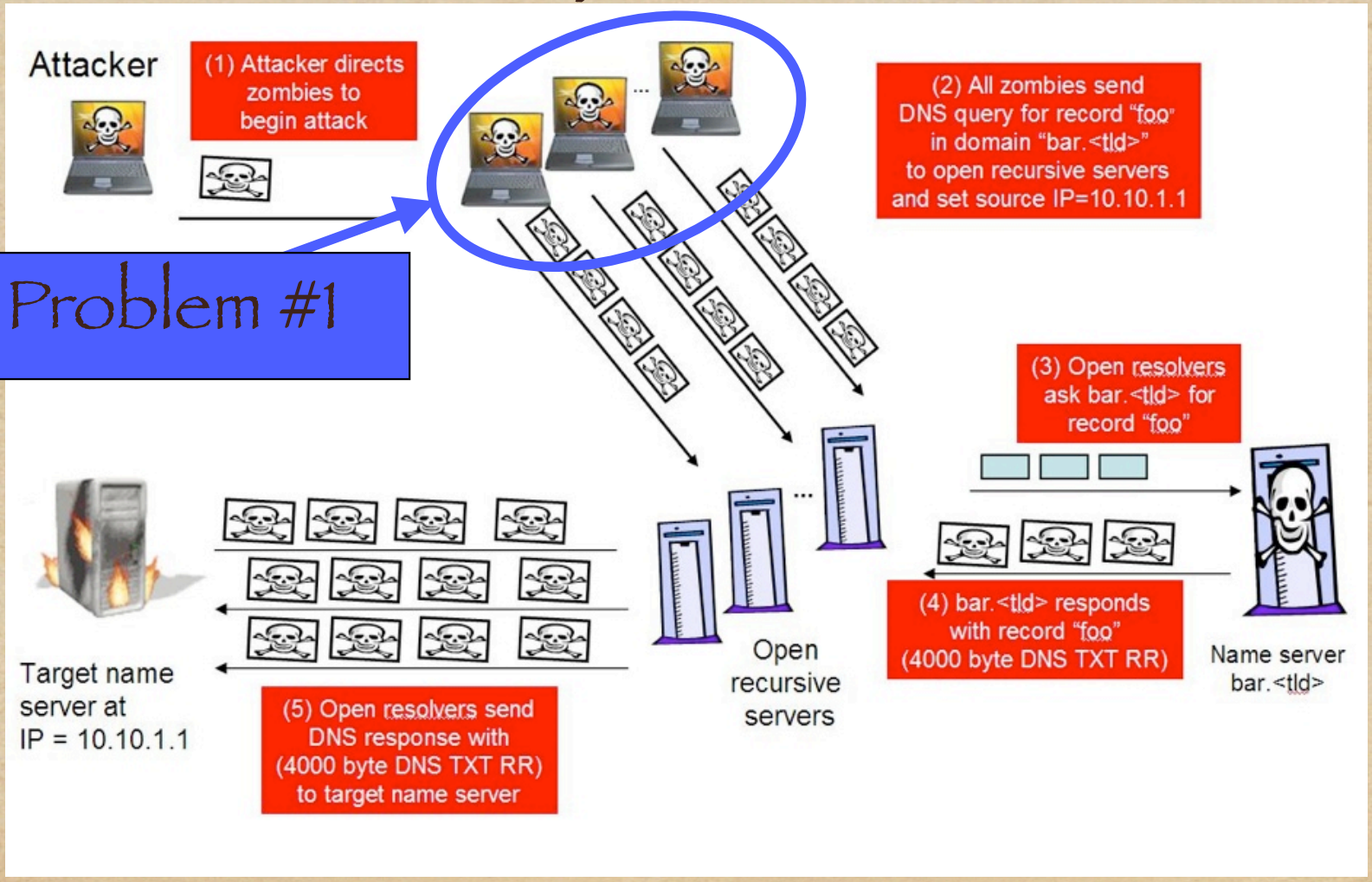


The Problem, cont'd

What is the Cure?

- There are at least two issues at hand:
- First and foremost it is easy to forge the source IP address of a DNS query

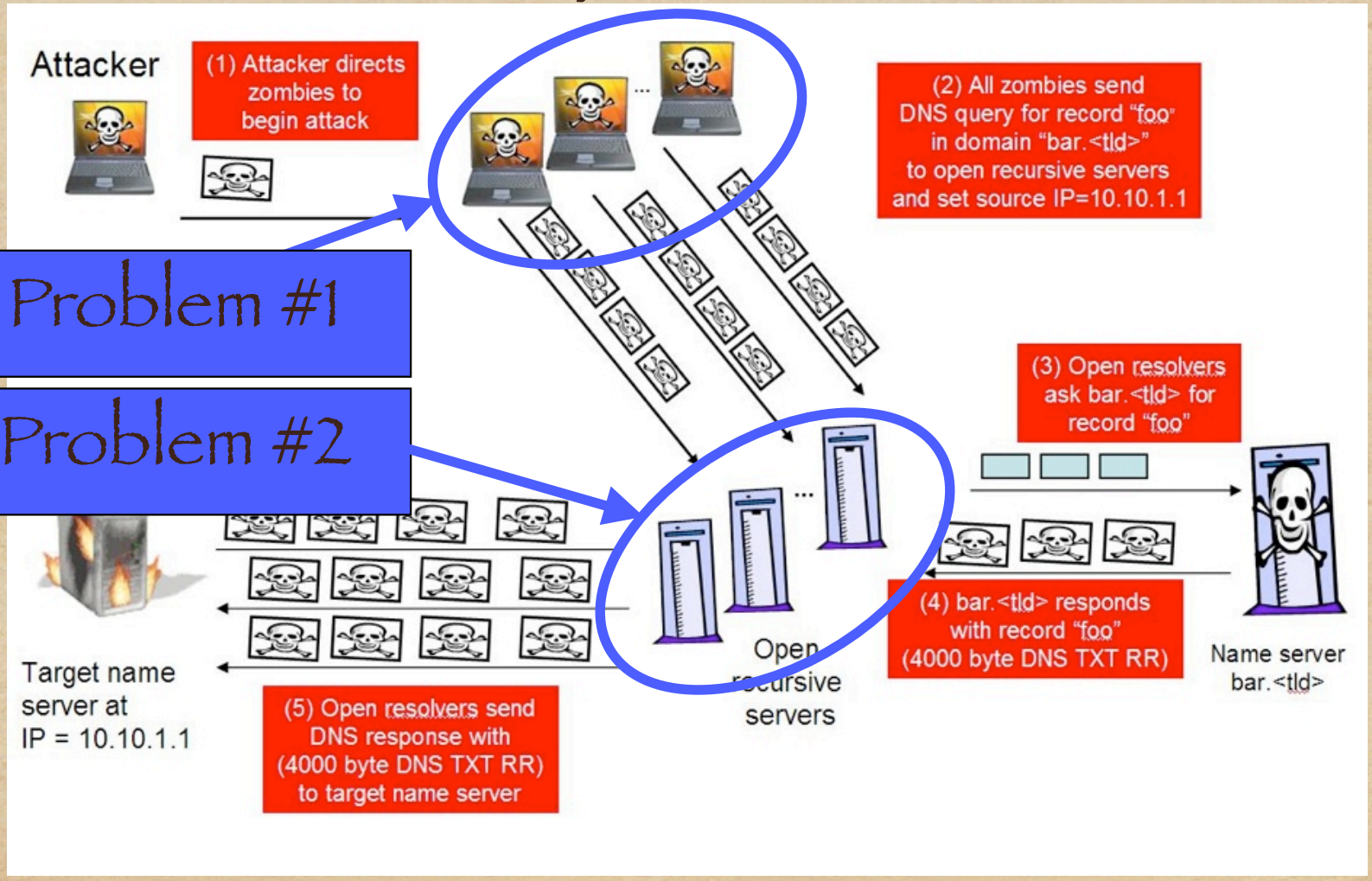
The Cure, cont'd



The Cure, cont'd

- Secondly, it is possible to use an unsuspecting, recursive, name server to cause a DNS-based amplification attack
  - the query is small, but the response is big

The Cure, cont'd



What is the Cure, cont'd

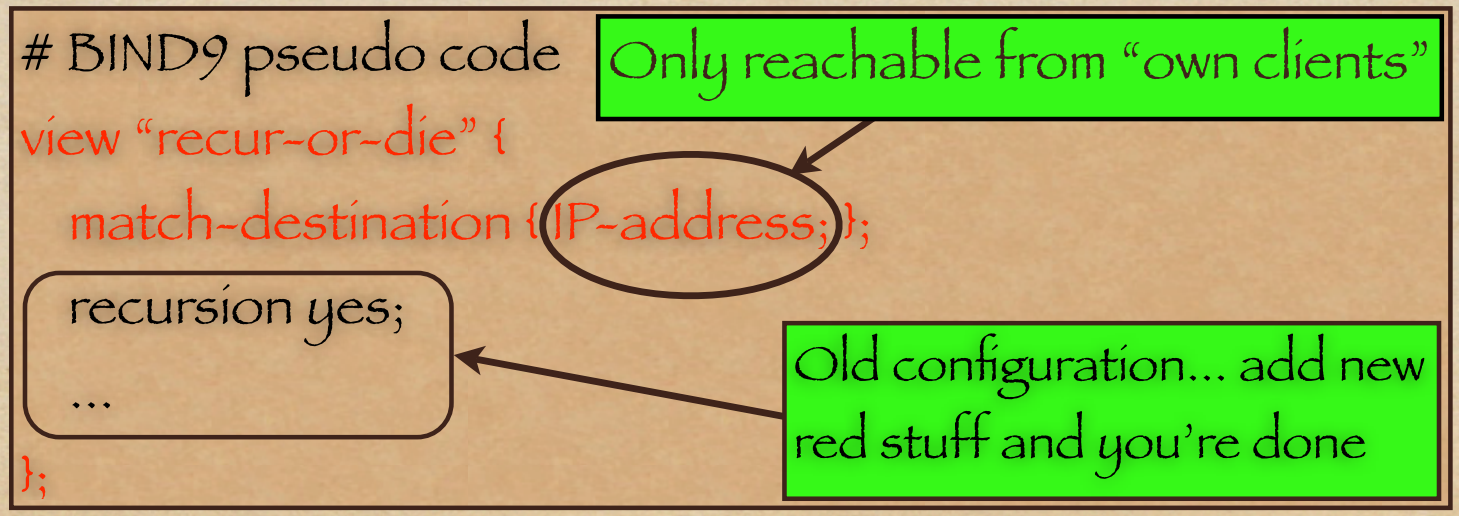
- The cure for the first problem is so-called "ingress filtering"
  - i.e. Internet Service Providers ensure that packets are not accepted into their network unless their source is "reasonable"
- The cure for the second problem is for servers to not allow recursive queries from just anybody

Ingress Filtering

- This is the long term solution which is needed
- Partly because ingress filtering alleviates not only this attack but also many other (non-DNS related) attacks.
- Ingress Filtering is part of "Securing the Edge"

Open Recursive Servers

- These are quite easy to fix... but there are many of them...
- Slightly simplified example config snippet:



Summary

- This is not the end of the world
- There are fixes
- Over time the open recursive name servers are being fixed
- But for real progress we do need the ISPs to do more active ingress filtering