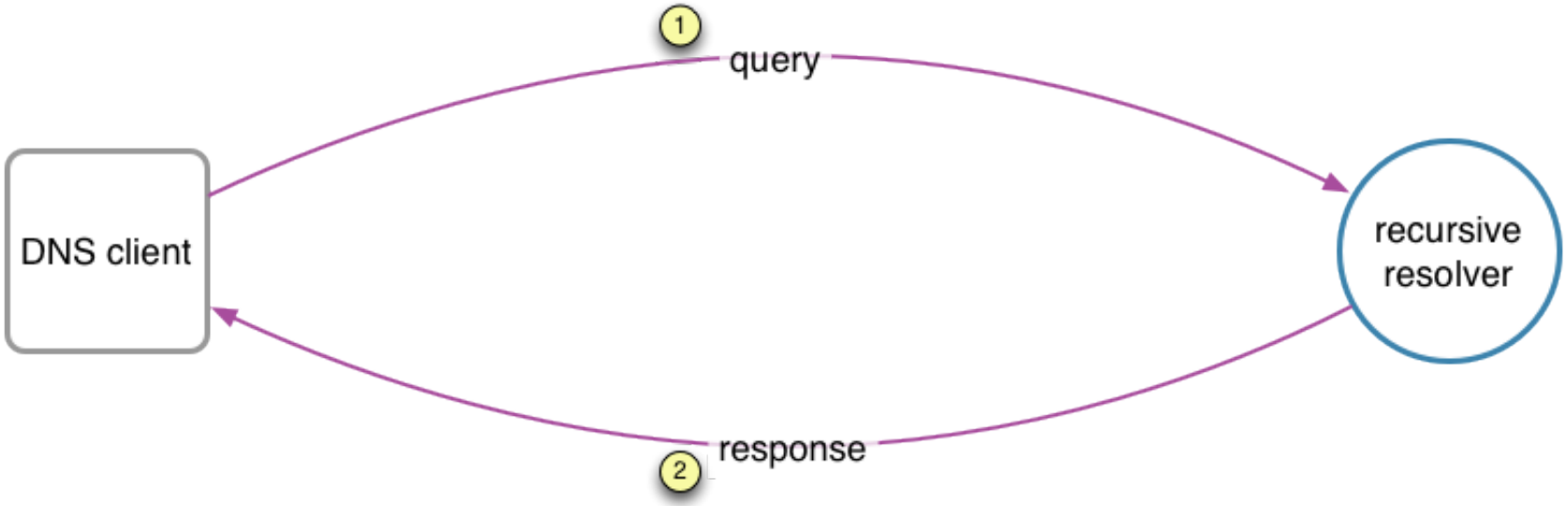
Open recursive resolvers

Jay Daley

2013

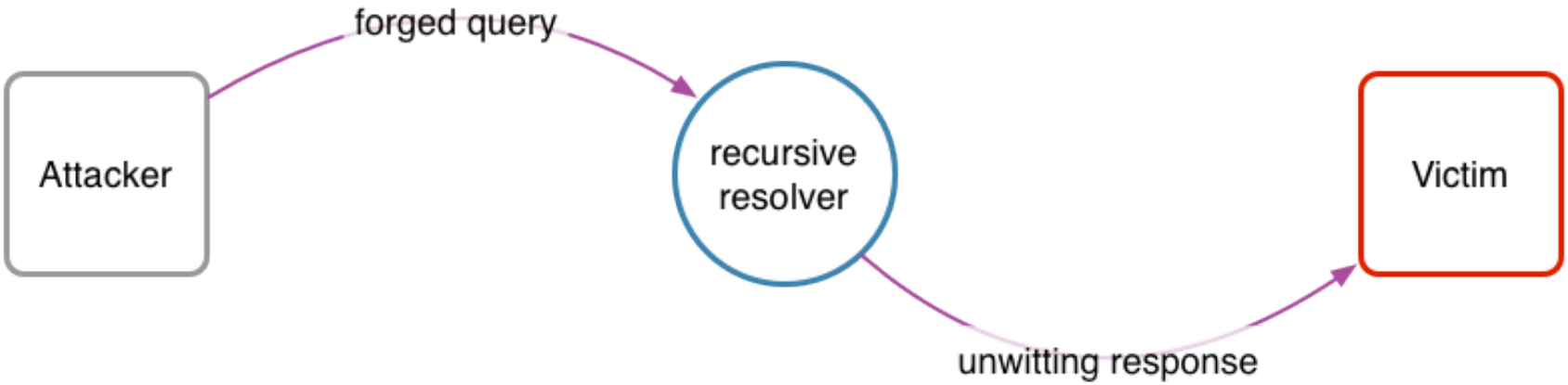
p: (+64) (4) 931 6977
e: registry@nzrs.net.nz
f: (+64) (4) 931 6979
w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited

Standard DNS query



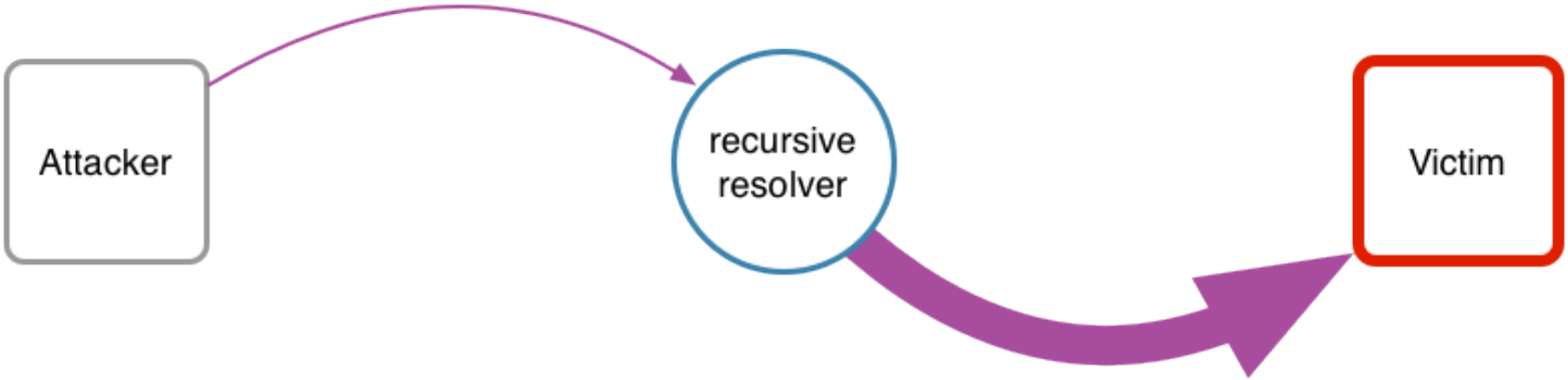
- DNS uses UDP
  - Trusts source address
  - Single packet query – single packet response

Forged query



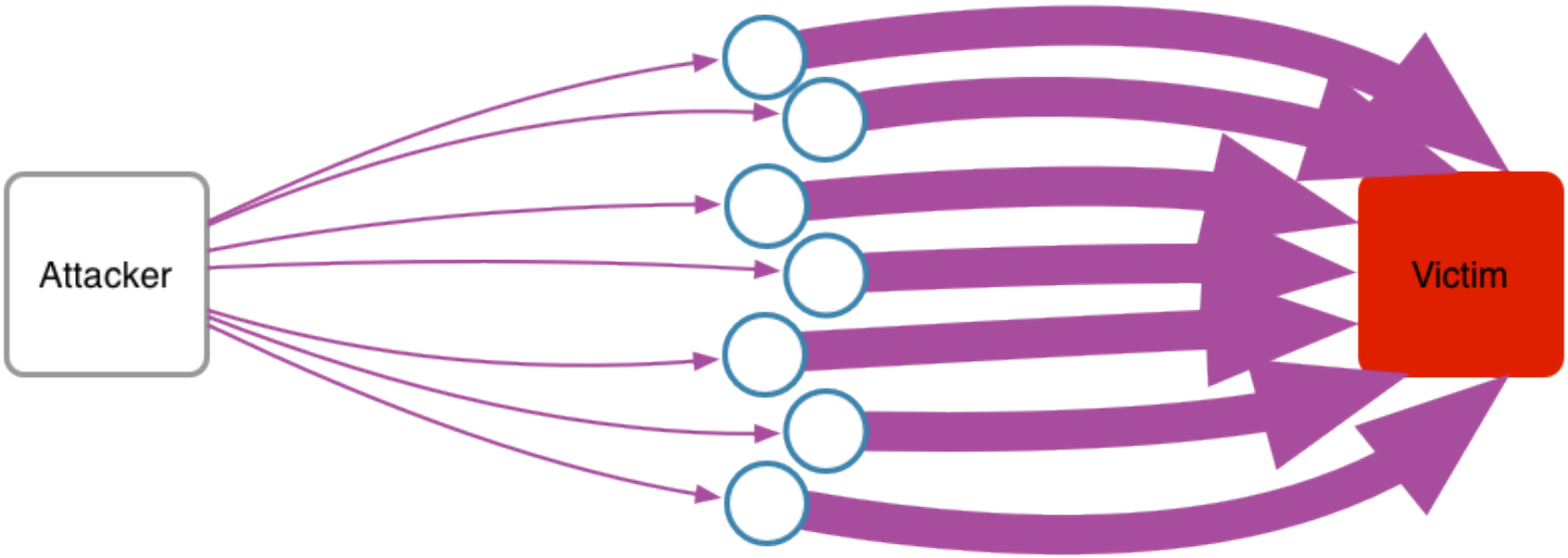
- Queries can have fake source address
- Resolver responds to that fake address

Traffic amplification



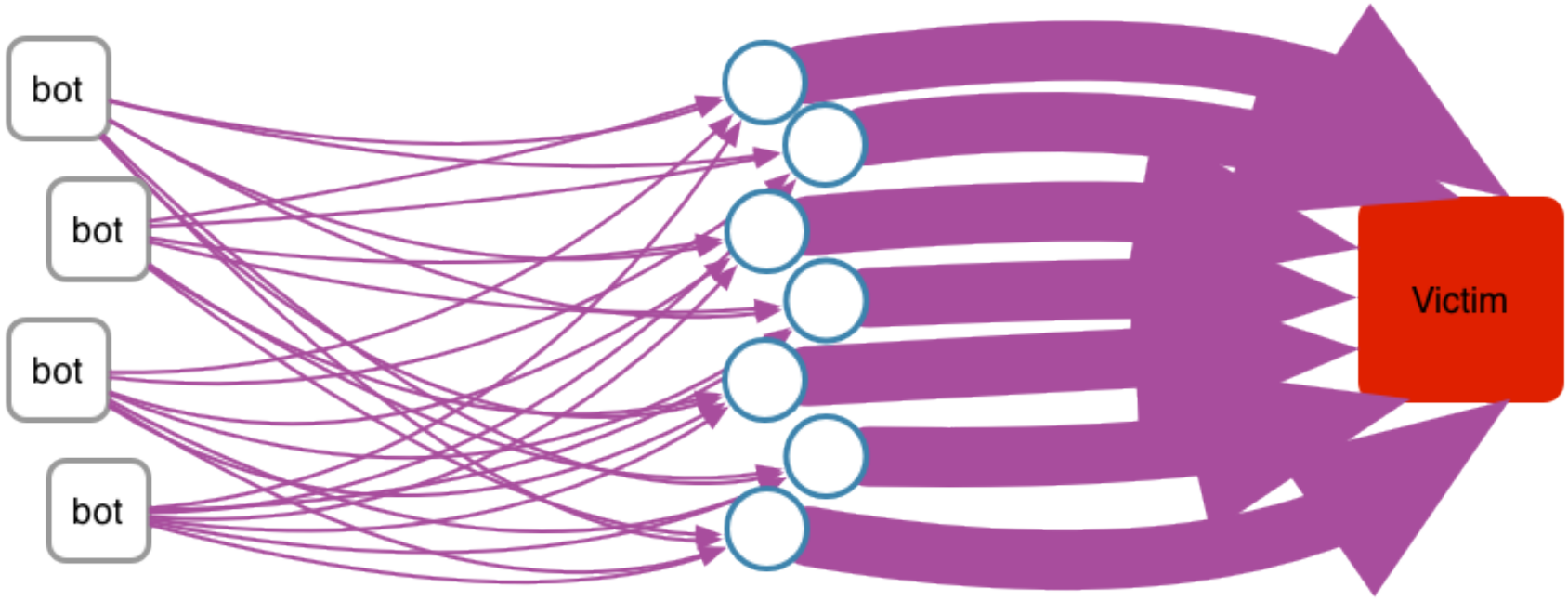
- Traffic can be amplified by factor of 80
  - Query is normally 52 to 64 bytes
  - Response can be over 4000 bytes

Distributed attack



- Use multiple resolvers
  - Over 25 million to use
  - Limits detection by individual resolvers

Distributed botnet attack



- If the attacker controls a botnet
  - Could by 100,000 strong or more

Mitigation

- Limit networks served (no longer open)
  - Best mitigation available
- Rate limit responses
  - Queries per second to same IP address
  - Average amplification to same IP address

- BUT
  - Very few mitigated
  - Easy to stay below threshold on any one server

History and future

- 2005 – First advisories
- 2006 – Scanning for open resolvers began
- 2006 – OpenDNS launched
- 2008 – RFC 5358 published
  - “Preventing Use of Recursive Nameservers in Reflector Attacks”
- 2009 – Google Public DNS launched
- Strategic value in open DNS resolvers.
  - Collect data
  - Filter via DNS
- Not going away soon

Any questions?

jay@nzrs.net.nz

p: (+64) (4) 931 6977
f: (+64) (4) 931 6979
e: registry@nzrs.net.nz
w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited