Evaluating a DNS Servers value in a DDoS attack

Introducing DNS Hammer

Abstract

- DNS Servers are popular for DDoS attacks
- We make our DNS servers useless for a botmaster

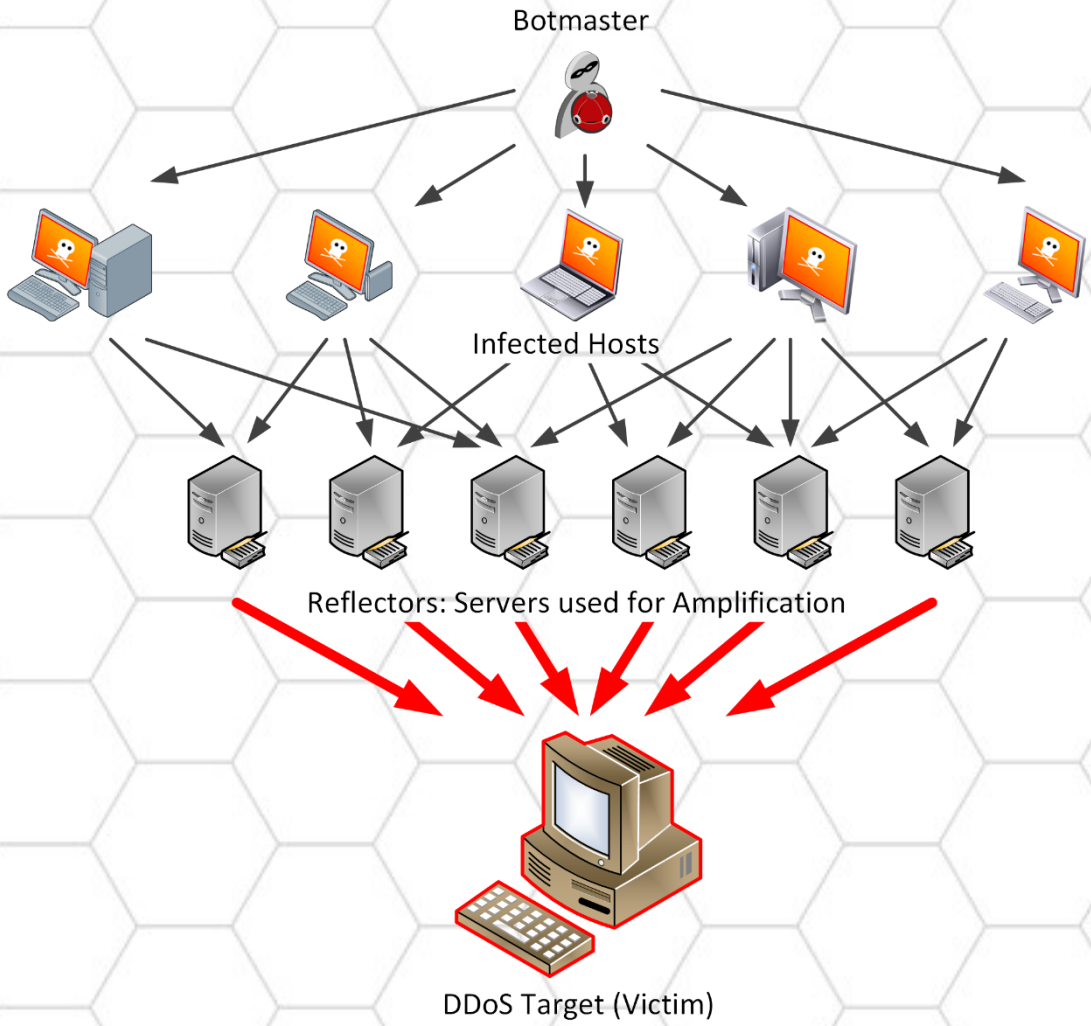
About Me

- Eddi Blenkers
- Security Blue Team: ICT Security Specialist for Kanton Aargau
- Pcap Addict: Sharkfest Speaker, occasional blogs at packet-foo.com

- Twitter: @PcapReader

Short Recap: DNS Reflection Attacks

- A Botmaster controls a number of infected computers.
- Infected hosts send DNS requests with a spoofed IP source address.
- The victim whose source address is spoofed receives a ton of responses.

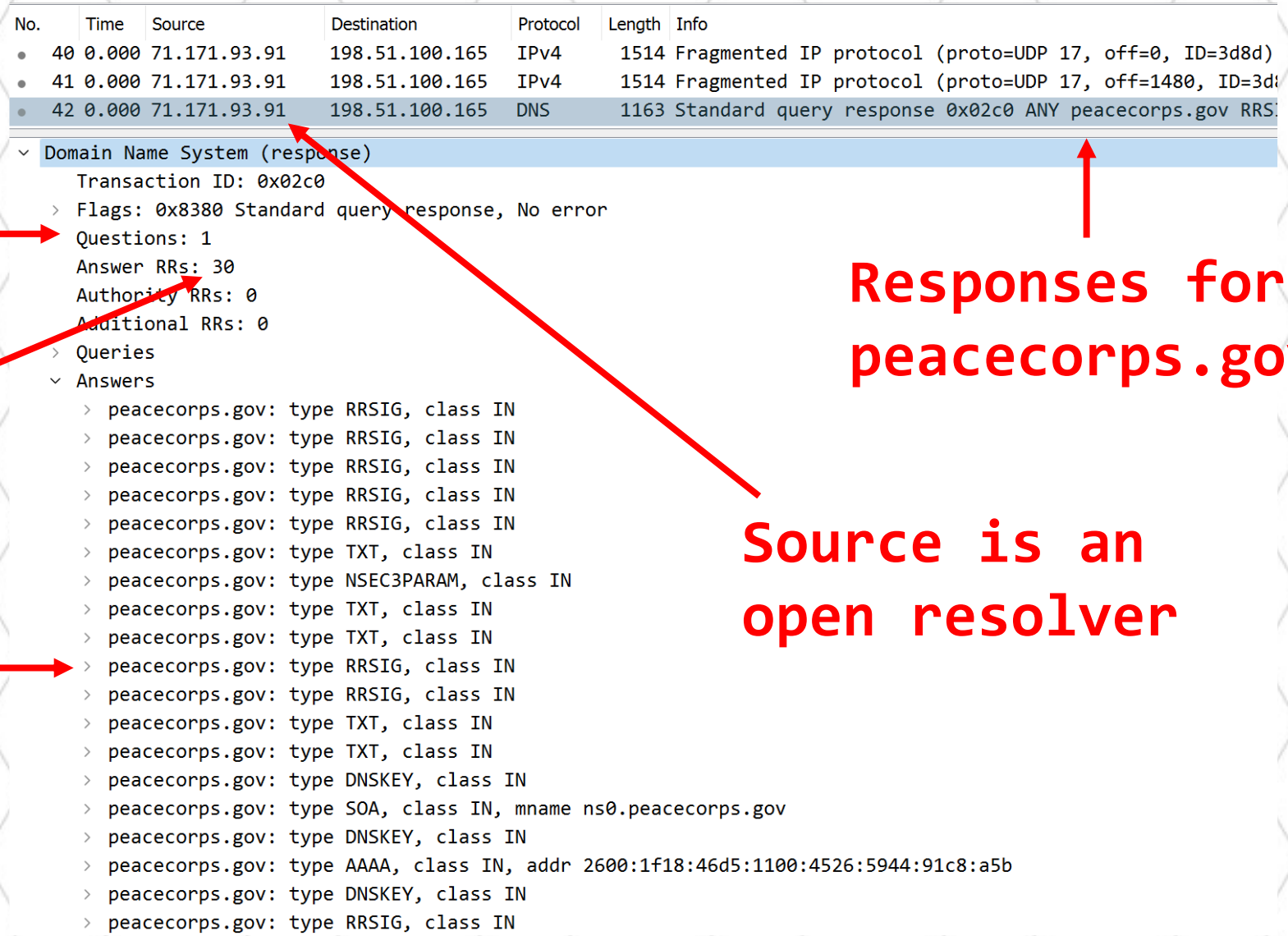


DDoS from a Packet Level

Asked for ANY
MX works, too

30 DNS Answers in 3 IP Fragments

DNS Payload: 4’081 Byte

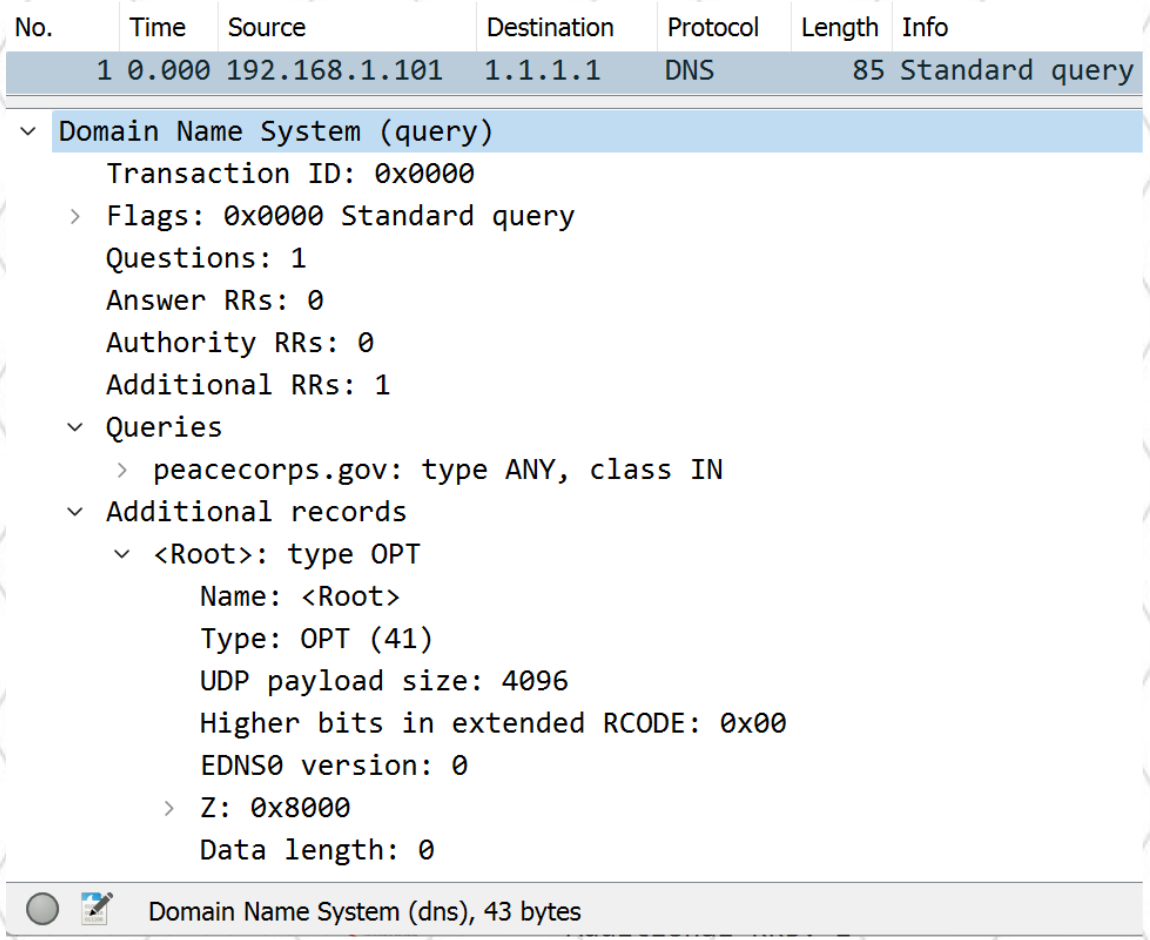


Responses for peacecorps.gov

Source is an open resolver

The DNS Request

- The request is a 71-byte IP packet
- The response was a total of 4’157 byte in 3 IP packets (ignoring Ethernet)
- The attackers’ traffic is amplified 58 times!



Why is the attack so effective?

- Domain peacorps.gov supports DNSSEC
  - DNSSEC is not a misconfiguration!
- The open resolver sends 4k DNS messages.
- The open resolver responds to queries for ANY.
- The open resolver is not configured for rate limiting.
- The open resolver is … well, open. But is it intentionally open?

Common DNS Reflectors

- Open resolvers:
  - Respond to anyone for all domains by design.
  - Usually have rate limiting enabled.
- Authoritative name servers:
  - Respond to anyone for “their” domain by design.
  - Some lack rate limiting.
- Company-internal name servers:
  - Should only respond to internal hosts for all domains.
  - Should.
  - Usually no rate limiting.

Make Name Servers useless for Botmasters

- DNS reflections would be impossible if all operators
  - Implement Rate Limiting
  - Limit DNS traffic with a QoS policer
  - Implement egress filters
  - Block requests for ANY records
    or at least redirect clients to TCP
  - Limit UDP message size to $USEFUL_SIZE
- Alas, not a all systems are run by professionals.

Open Resolvers

- Send responses to all clients for all domains
- Implement good rate limiting, if they are designed as open resolvers
  - Examples: 1.1.1.1, 8.8.8.8, 9.9.9.9
- A few DNS servers run without rate limit
  - Respond to everyone
  - Dish out ANY records in vast quantities
  - Support DNS extensions for 4 kB message size

Authoritative Name Servers

- Respond to all clients, if they are authoritative for the desired domain
- Interesting for a botmaster if
  - Servers respond to queries for ANY
  - Domains have large MX or TXT records
  - Domains are signed (DNSSEC)
  - Servers send large records
  - No rate limiting is enforced

Company Internal Name Servers

- A firewall blocks queries from external hosts
  - Nothing can happen, right?
  - Our server only receives valid queries for production traffic, doesn't it?
  - All security measures are a waste of time, money, usability. Basta.
- Great for infected clients:
  - Server does not check the clients IP address.

- Hint: Even if you don't implement rate limiting, at least block traffic with a source IP address that's not on your local network.

How valuable is my DNS server for an attacker?

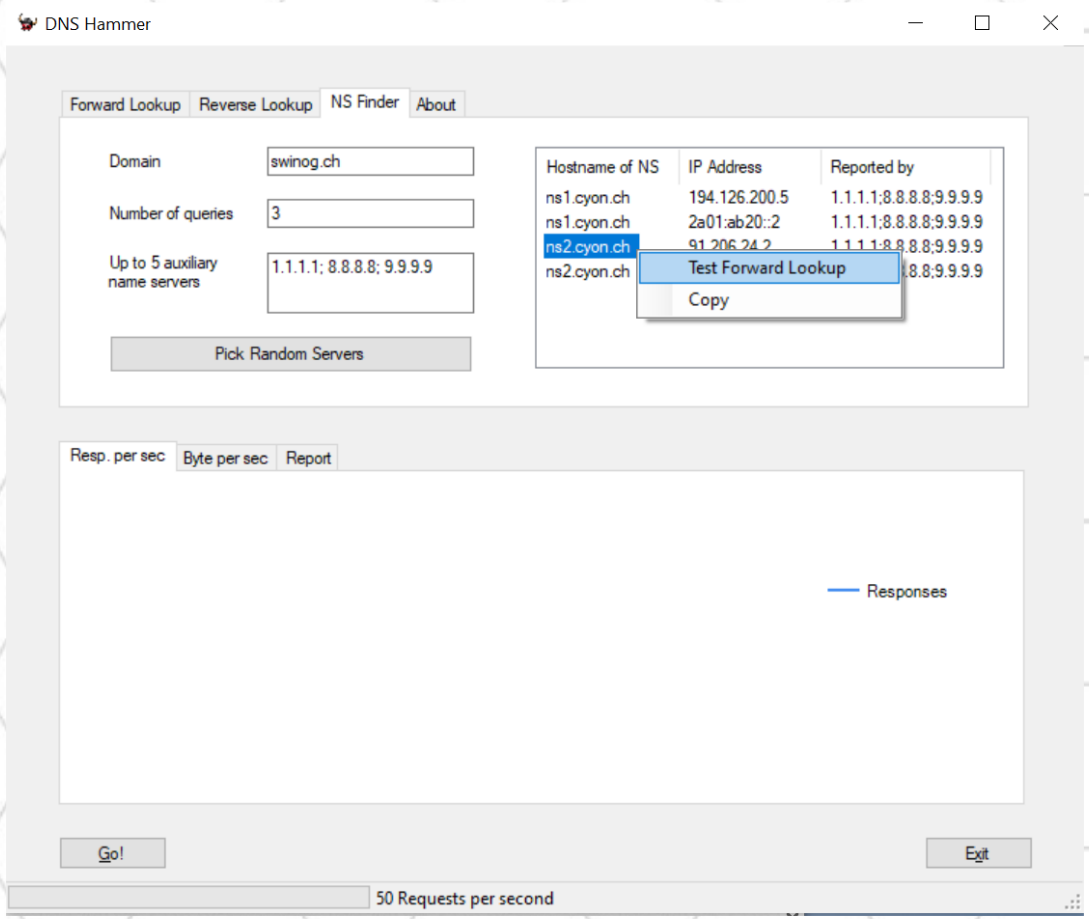
- Option A: ~~Get infected, become part of a botnet, see what will happen~~
- Option B: Use DNS Hammer to test your configuration

Introducing DNS Hammer

- Find out, if a DNS server would be a “good” reflector for a botmaster.
- Find out, how the configuration affects DNS clients.
- Explore DNS configurations of other organizations to get ideas for your own servers.

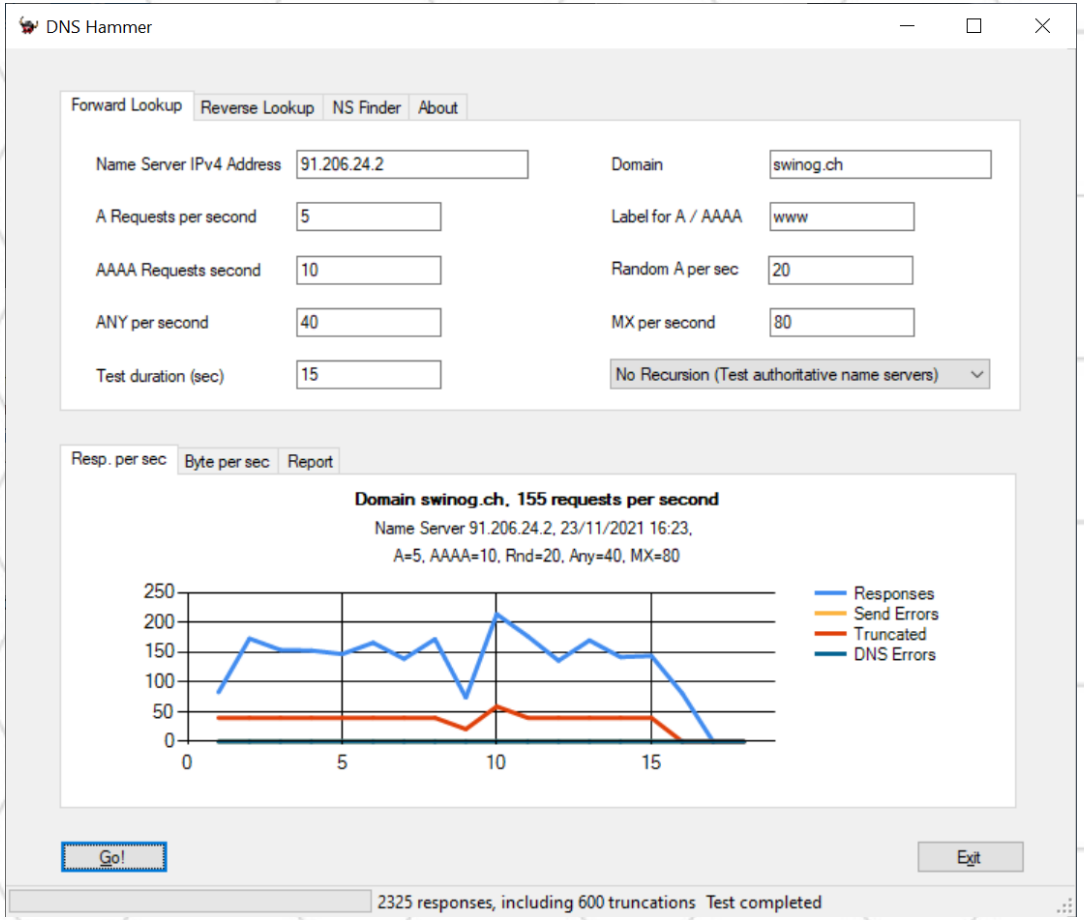
Locate Authoritative Name Servers

- Use the NS Finder tool to identify authoritative servers
- Select an IPv4 address
- Right-click and “Test Forward Lookup”
- IPv6 support will follow



Test Name Server

- Define number of DNS records
  - A, AAAA, MX, ANY
- Note the orange line
  - swinog.ch sets the truncated flag for queries to ANY
  - ANY is requested 40 times per second



DNS Truncated Flag

- Informs the client that there is more data available through TCP.
- Users won’t notice the switch to TCP.
- TCP stops spoofing attacks .

- Remember: DNS uses UDP **and TCP** port 53!

Report for swinog.ch

```
Test Report for Domain swinog.ch
Name server: 91.206.24.2, recursion disabled
…
Requests send: 2325
Responses received: 2325
Truncated responses received: 600
The following DNS errors were encountered:
Error code 3 (Non-existent Domain): 300 (likely caused by
random queries)
Bytes send: 153,4 kB
Bytes received: 241,4 kB
Amplification factor: 1,6
```

Demo DNS Hammer

- RIPE has authoritative name servers with ARIN, APNIC, AfriNIC, LACNIC
- Each server has its own configuration.
- Let’s explore ripe.net

Configuring DNS Rate Limiting

- Beyond the scope of this talk
- Well documented for BIND, UNBOUND and Microsoft
  - https://kb.isc.org/docs/aa-01000
  - https://www.nlnetlabs.nl/documentation/unbound/unbound.conf/
  - https://docs.microsoft.com/en-us/powershell/module/dnsserver/set-dnsserverresponseratelimiting?view=windowsserver2019-ps

More on DNS Hammer

- https://www.dnshammer.com
- https://blog.packet-foo.com/2021/01/introducing-dns-hammer-part-1-ddos-analysis-from-dns-reflection-to-rate-limiting/

Questions?