Mirror - Mirror

The dangers of DNS reflection attacks

MEN&MICE

About me

DNS

Windows

DHCP

DNSSEC

Men & Mice, Iceland

IPv6

Unix

DNS

www.strotmann.de

↓

`2001:470:1f08:f1d::2`

Trust-System

Service locator

Reputation-System

Problem, in DNS?

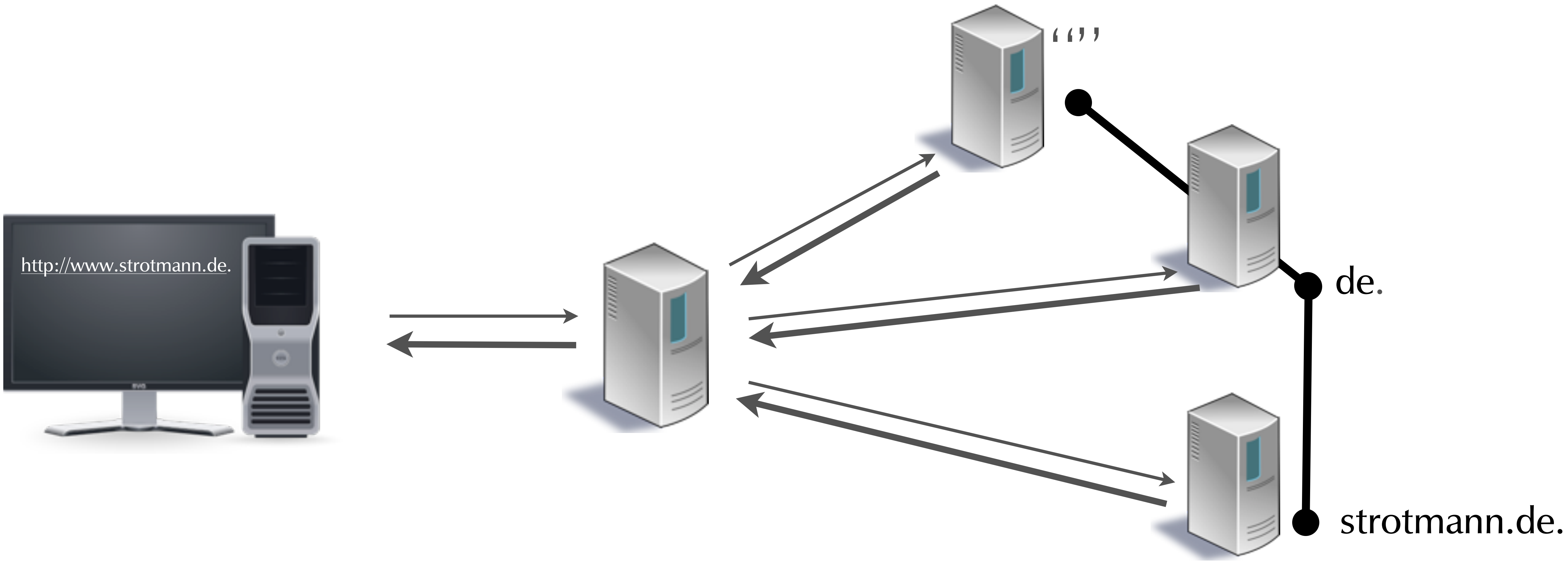
DNS has a problem

A small problem growing

not new (since 1983)

but getting popular with troublemakers

DNS operation



Observation: DNS answers are larger than queries

© Men & Mice http://menandmice,com

DNS response sizes

Query:
45 Byte

```
17:23:19.306630 IP 192.168.1.27.49252 > 192.168.1.2.domain: 7395+ [1au] AAAA? www.strotmann.de. (45)
17:23:19.308328 IP 192.168.1.2.domain > 192.168.1.27.49252: 7395 1/2/1 AAAA 2001:470:1f08:f1d::2 (159)
```

Answer is 3.5 times bigger

Answer:
159 Byte

DNS response sizes

```
; <<>> DiG 9.9.2-vjs287.12 <<>> www.strotmann.de aaaa +qr @192.168.1.2
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60154
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.strotmann.de.         IN    AAAA
```

Query:
45 Byte

```
; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60154
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.strotmann.de.         IN    AAAA

;; ANSWER SECTION:
www.strotmann.de.     71645 IN    AAAA  2001:470:1f08:f1d::2

;; AUTHORITY SECTION:
strotmann.de.         56293 IN    NS    ns.norplex-communications.com.
strotmann.de.         56293 IN    NS    ns.norplex-communications.net.

;; Query time: 2 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Thu Jan 17 17:35:24 2013
;; MSG SIZE  rcvd: 159
```

Answer:
159 Byte

DNS response sizes

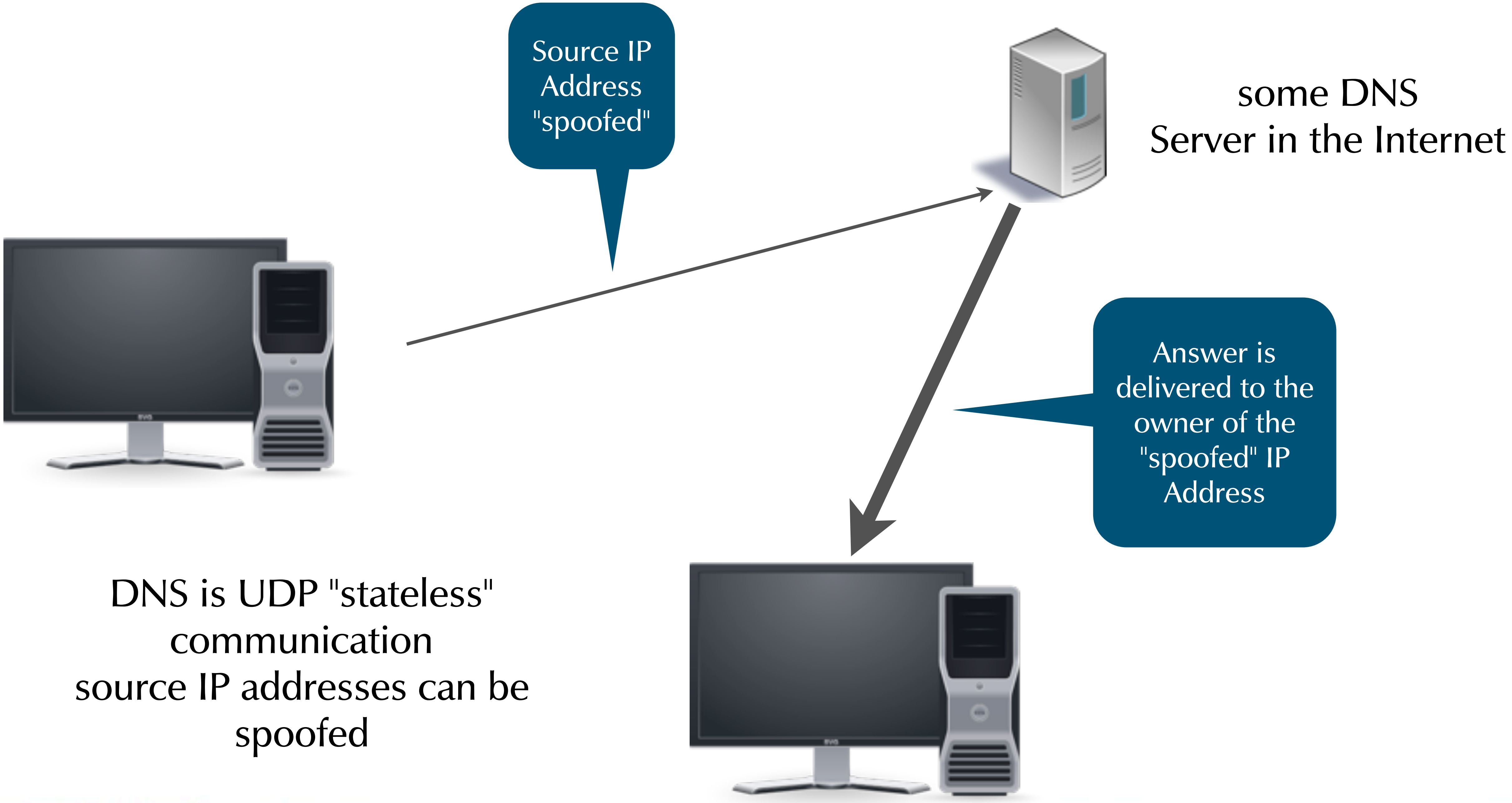
```
17:28:15.035136 IP 192.168.1.27.65533 > 192.168.1.2.domain: 42995+ [1au] ANY? isc.org. (36)
17:28:15.036408 IP 192.168.1.2.domain > 192.168.1.27.65533: 42995$ 27/0/6 SOA,
     RRSIG,
     NS sfba.sns-pb.isc.org.,
     NS ord.sns-pb.isc.org.,
     NS ns.isc.afilias-nst.info.,
     NS ams.sns-pb.isc.org.,
     RRSIG,
     A 149.20.64.42,
     RRSIG,
     MX mx.ams1.isc.org. 10,
     MX mx.pao1.isc.org. 10,
     RRSIG,
     TXT "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16 ip6:2001:04F8::0/32
          ip6:2001:500:60::65/128 ~all",
     TXT "$Id: isc.org,v 1.1760 2013-01-17 01:51:59 jdaniels Exp $",
     RRSIG,
     AAAA 2001:4f8:0:2::d,
     RRSIG,
     NAPTR[|domain] (3169)
```

Query:
36 Byte

Answer:
3169 Byte

88 times bigger!

Where is the problem?



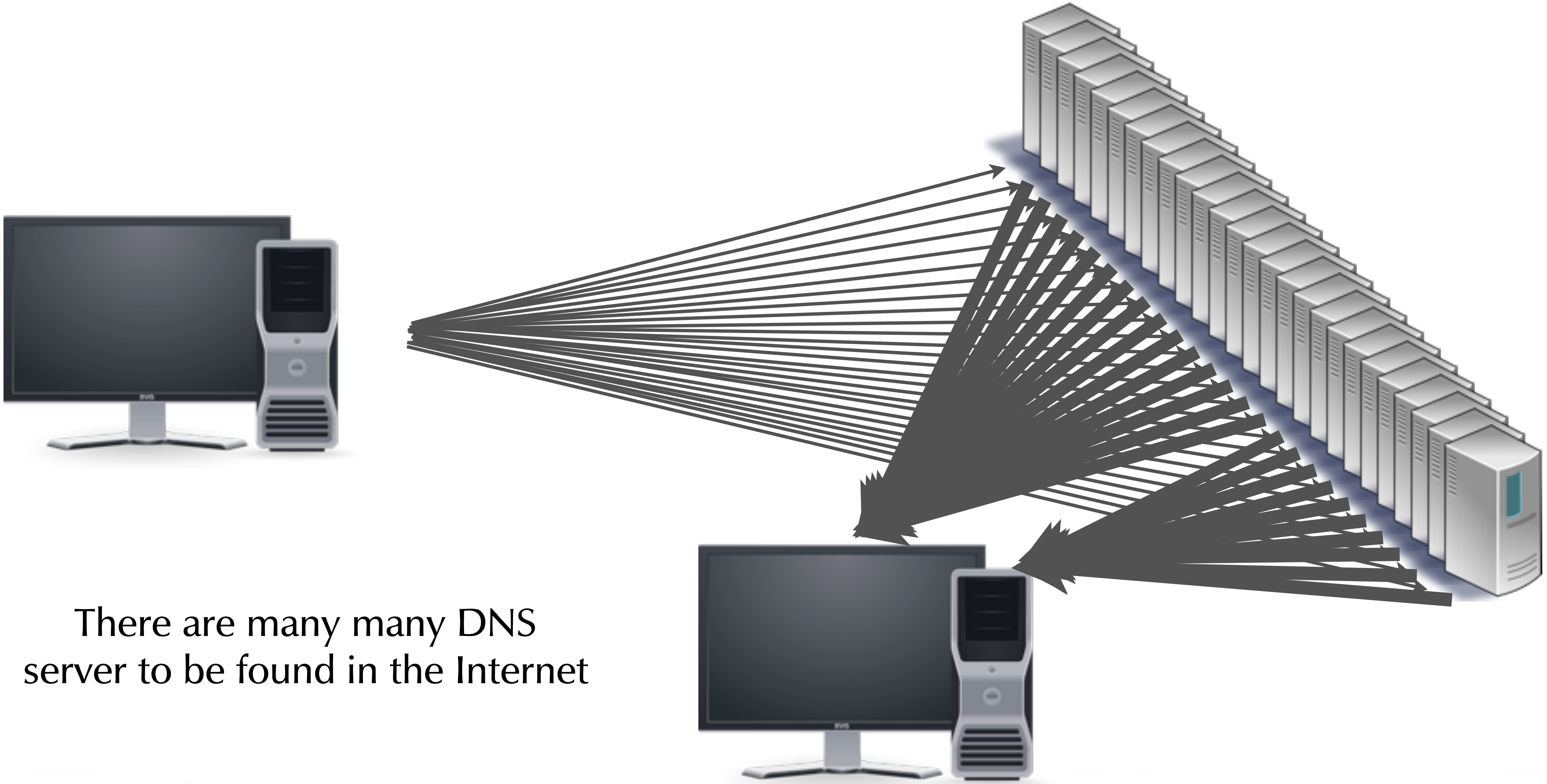
Source IP Address "spoofed"

some DNS
Server in the Internet

Answer is delivered to the owner of the "spoofed" IP Address

DNS is UDP "stateless" communication
source IP addresses can be spoofed

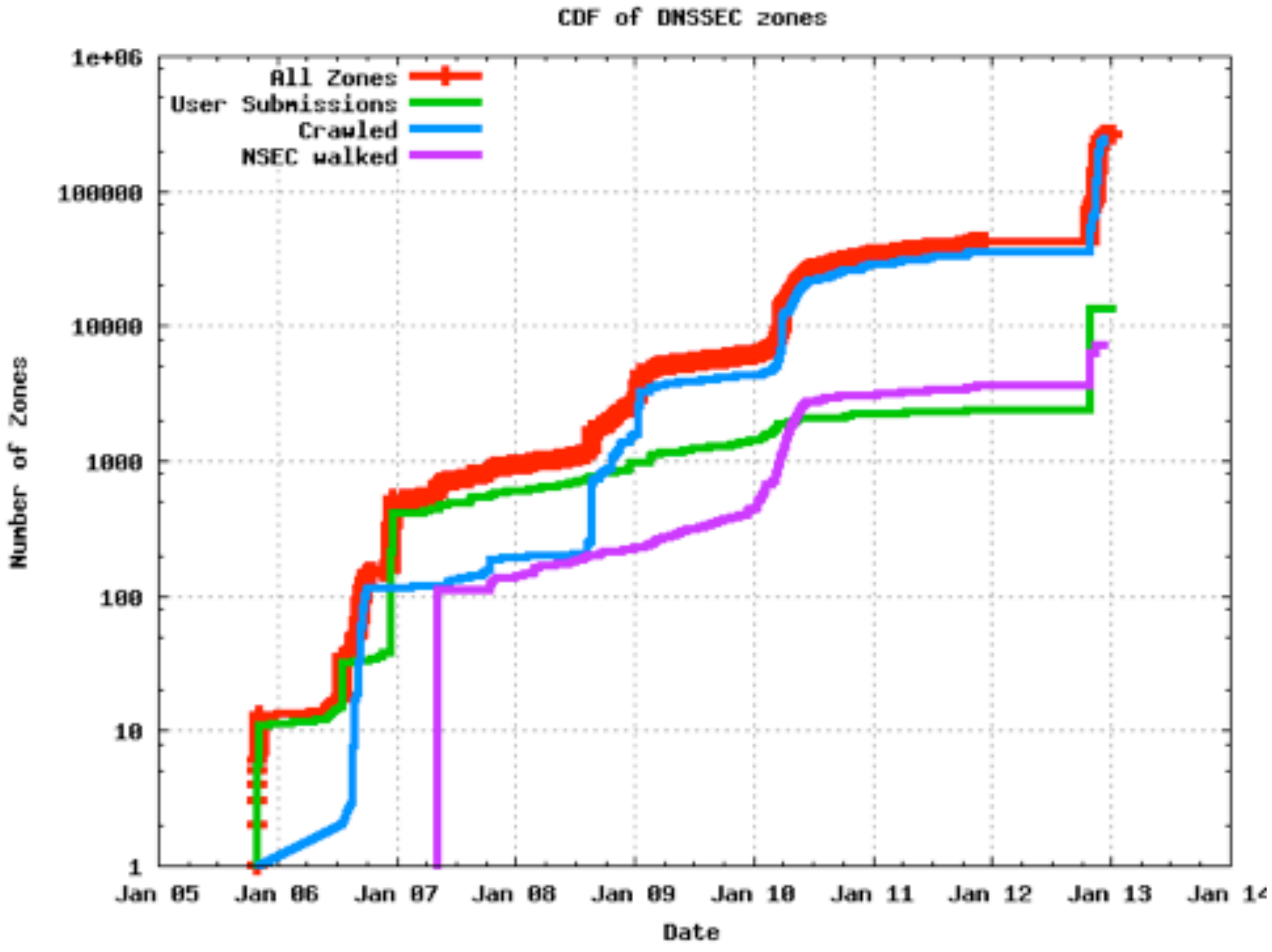
Where is the problem?



There are many many DNS
server to be found in the Internet

© Men & Mice http://menandmice,com

Is it a DNSSEC problem?



DNSSEC deployment brought this issue into the light

but the problem existed before DNSSEC, and it was exploited before

DNSSEC is not the problem! but it doesn’t help either

Dramatis personae

There are 3 parties:

1) the sender (attacker)

2) the mirror DNS server (the weapon)

3) the recipient (victim)

if you operate a DNS server, you might provide the weapon for this attack

What can we do?

- 🔵 easy slope
- 🔴 advanced track
- ⚫ expert level

DNS monitoring ● advanced track

Do you know who is using your DNS?

What questions are asked?

What answers are given?

DNS Monitoring can reveal interesting facts about networks

© Men & Mice http://menandmice,com

DNS monitoring ● advanced track

open source and commercial tools are available

DNS wittness

DNS Statistics Collector (dsc)

DNSTOP

PacketQ

Firewall?

● expert level

First instinct!

lets block the
source
address!

But wait!

It ain’t that
easy!

© Men & Mice http://menandmice,com

Firewall?

● expert level

Manual blocking is too much work

Automatic blocking could harm the victim!

Remember: the source IP we see is the victims address!

You don’t want to block IP’s like 8.8.8.8

Firewall?

● expert level

Fighting the reflection attack on the firewall level is not impossible

but don’t forget your helmet and avalanche gear!

interview the daredevils that have taken this track before you

links provided in the notes

Open resolvers

● easy slope

BIND 9.4 and older and all Windows DNS are open resolvers by default

open resolver = a DNS server that does DNS recursive lookups for ALL IP addresses

An easy target for attackers to launch a reflection attack

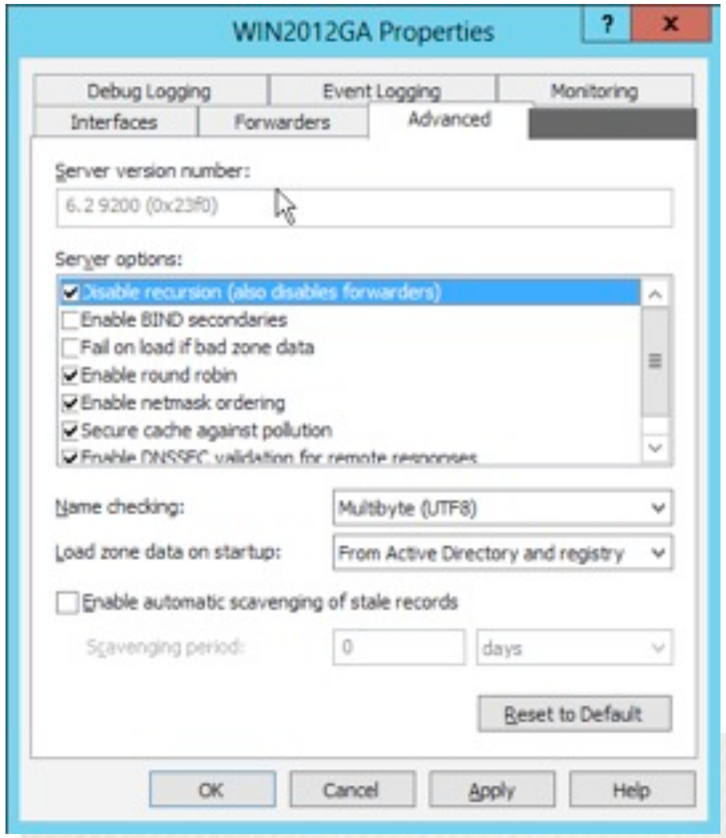
© Men & Mice http://menandmice,com

Open resolvers

● easy slope

For BIND 9, use "`allow-recursion`" to limit recursion to your client networks

```
options {
   allow-recursion { localnets; };
};
```



Server version number: 6.2 9200 (0x23f0)

Server options:

- ☑ Disable recursion (also disables forwarders)
- ☐ Enable BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution
- ☑ Enable DNSSEC validation for remote responses

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

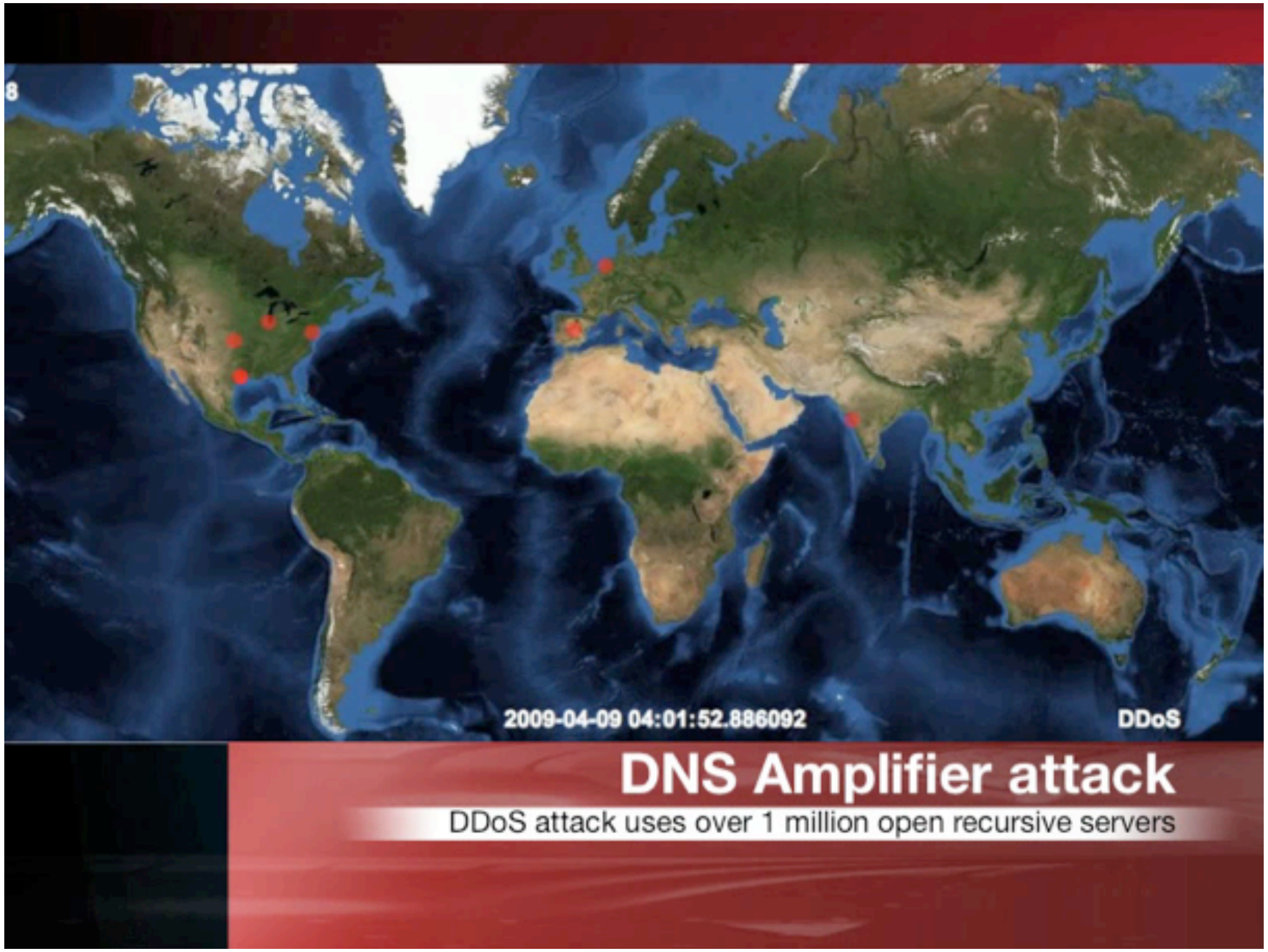
For authoritative Windows DNS, disable recursion

Don't operate a caching server open in the Internet

© Men & Mice http://menandmice,com

Open resolvers

● easy slope



2009-04-09 04:01:52.886092

DDoS

DNS Amplifier attack

DDoS attack uses over 1 million open recursive servers

http://www.team-cymru.org/Services/Resolvers/

Open resolvers

● easy slope

RFC 5358 (BCP 140)

Preventing Use of Recursive Nameservers in Reflector Attacks

Minimal responses ● easy slope

```
% dig @ns2.xb.nl. mx ncsc.nl

; <<>> DiG 9.9.2-vjs287.12 <<>> @ns2.xb.nl. mx ncsc.nl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60070
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 2, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ncsc.nl.                       IN      MX

;; ANSWER SECTION:
ncsc.nl.        60      IN      MX      20 min3.govcert.nl.
ncsc.nl.        60      IN      MX      20 min4.govcert.nl.
ncsc.nl.        60      IN      MX      30 min5.govcert.nl.
ncsc.nl.        60      IN      MX      40 smtp.espritxb.nl.
ncsc.nl.        60      IN      MX      10 min1.govcert.nl.
ncsc.nl.        60      IN      MX      10 min2.govcert.nl.

;; AUTHORITY SECTION:
ncsc.nl.        60      IN      NS      ns1.xb.nl.
ncsc.nl.        60      IN      NS      ns2.xb.nl.

;; ADDITIONAL SECTION:
min1.govcert.nl. 60     IN      A       193.172.9.50
min2.govcert.nl. 60     IN      A       193.172.9.51
min3.govcert.nl. 60     IN      A       31.161.17.13
min4.govcert.nl. 60     IN      A       31.161.17.14
min5.govcert.nl. 60     IN      A       217.169.231.54
smtp.espritxb.nl.       60      IN      A       80.248.34.142
smtp.espritxb.nl.       60      IN      A       80.248.34.141
ns1.xb.nl.              300     IN      A       80.248.34.15
ns2.xb.nl.              300     IN      A       212.67.179.100

;; Query time: 39 msec
;; SERVER: 212.67.179.100#53(212.67.179.100)
;; WHEN: Fri Jan 18 13:02:08 2013
;; MSG SIZE  rcvd: 362
```

DNS server are very helpful my nature

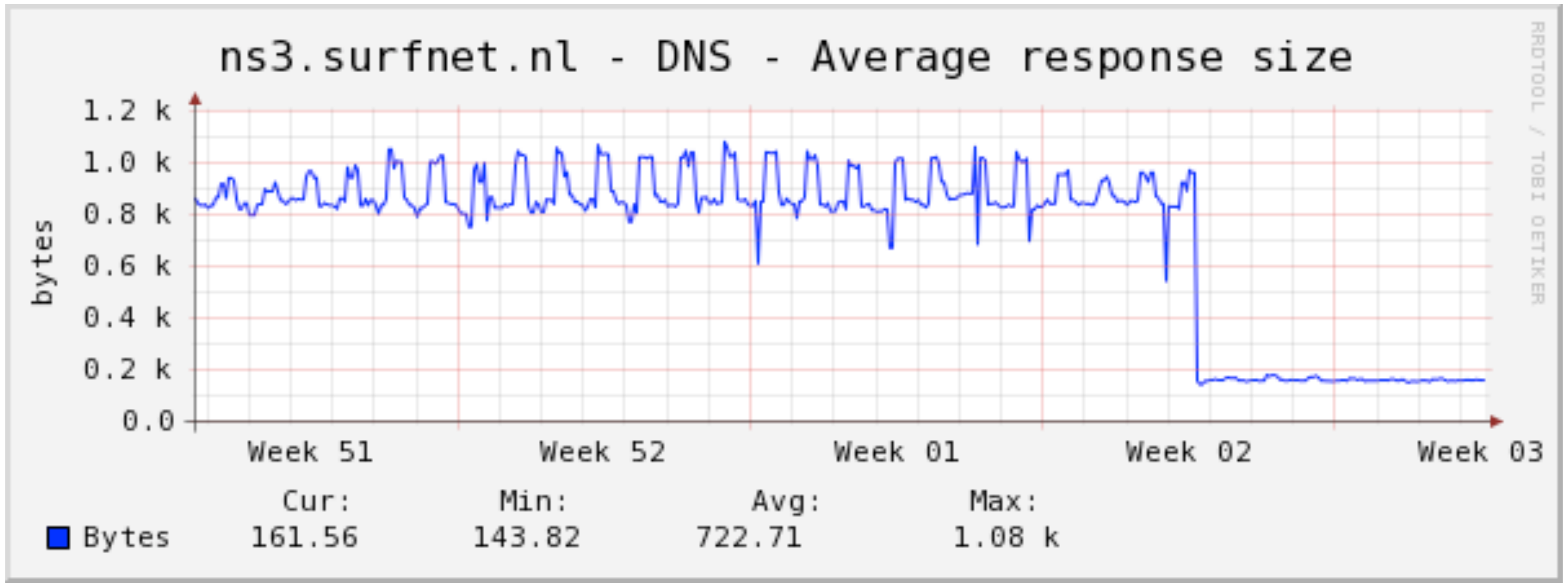
they deliver data not explicitly asked for

they try to be nice and help other DNS servers out there

© Men & Mice http://menandmice,com

Minimal responses ● easy slope

using the "`minimal-responses`" you can configure a BIND 9 to be less helpful (to strangers)



this reduces the "ammo" available to attackers

© Men & Mice http://menandmice,com

Response Rate Limiting

● advanced track

three rules of good DNS

1

Clients never send queries to authoritative DNS Server

2

authoritative DNS Server answer to caching servers

3

caching DNS server cache responses

© Men & Mice http://menandmice,com

Response Rate Limiting

● advanced track

all good DNS answers are cacheable

1
good positive
(NOERROR+DATA) answers

2
domain does not exist
(NXDOMAIN) answers

3
record-type does not exist
(NOERROR+NODATA) answer

Response Rate Limiting

● advanced track

as all DNS queries should go through a caching server ...

... identical querys should not be seen from the same source inside the TTL (Time to Live) ...

... if we see recurring queries, it is likely an attack ...

... or crappy software :(

Response Rate Limiting

● advanced track

response rate limiting counts the number of identical responses send to a given network

will throttle outgoing responses if too much identical responses are send

allows legit clients in the victims network to still resolve DNS data

Response Rate Limiting

● advanced track

in case an attack is detected, (almost) empty answers are send with "TC" flag set

"TC" flag = answer truncated, retry over TCP

real caching DNS server will repeat the query over TCP (slow, but harder to spoof)

Response Rate Limiting

● advanced track

Response Rate Limiting is available in some Unix DNS servers

BIND 9 patch by Vernon Schryver and Paul Vixie
(will be in the official BIND 9 soon)

NSD 3 and NSD 4 from NLnetLabs

DNS dampening

● advanced track

Lutz Donnerhacke ist working on a different idea called "DNS dampening"

BIND 9 patch is available

BCP 38

● expert level

Network Ingress Filtering:
"Defeating Denial of Service Attacks which employ IP Source Address Spoofing"

RFC 2827 - May 2000

would be the real fix:
stop IP spoofing

BCP 38

● expert level

network operators find many many reasons **not** to implement BCP 38

time, knowledge, money, "not my department", ...

BCP 38

● expert level

if you operate a network:
implement it

if you are a customer:
ask your ISP to
implement it

Summary

Checklist

make sure not to run an open DNS resolver ✓

consider "minimal-responses" ✓

implement Response Rate Limiting ✓

turn on ingress filtering ✓

know your DNS traffic ✓

Questions!

Thank you

Slides and links on `http://dnsworkshop.org`

`carsten@menandmice.com`

MEN&MICE