Open Recursive Nameservers

P. van Abswoude
P. Tavenier

System and Network Engineering

University of Amsterdam

February 7, 2007

Introduction

What we are going to tell...

- What is the problem?
- What is a Caching Open Recursive Nameserver?
- Practical Research
  - Reconnaissance work
  - DNS query (maximum UDP packet size)
  - DNS answer (TXT records)
  - UDP and DNSSEC
  - An actual DNS DDoS attack
- Defending strategies
- Do we have to be concerned of large DNS DDoS attacks using CORNS?

Once Upon A Time...

- The Internet was a happy place where it was easy to help your friends and neighbors:
  - Telnet was THE remote administration tool/protocol
  - Open SMTP relays were the norm rather than the exception
  - Nameservers were Open Recursive...
  - etc.
- In short: the Internet was build to be used by everybody – NOT abused!

But unfortunately, things change...

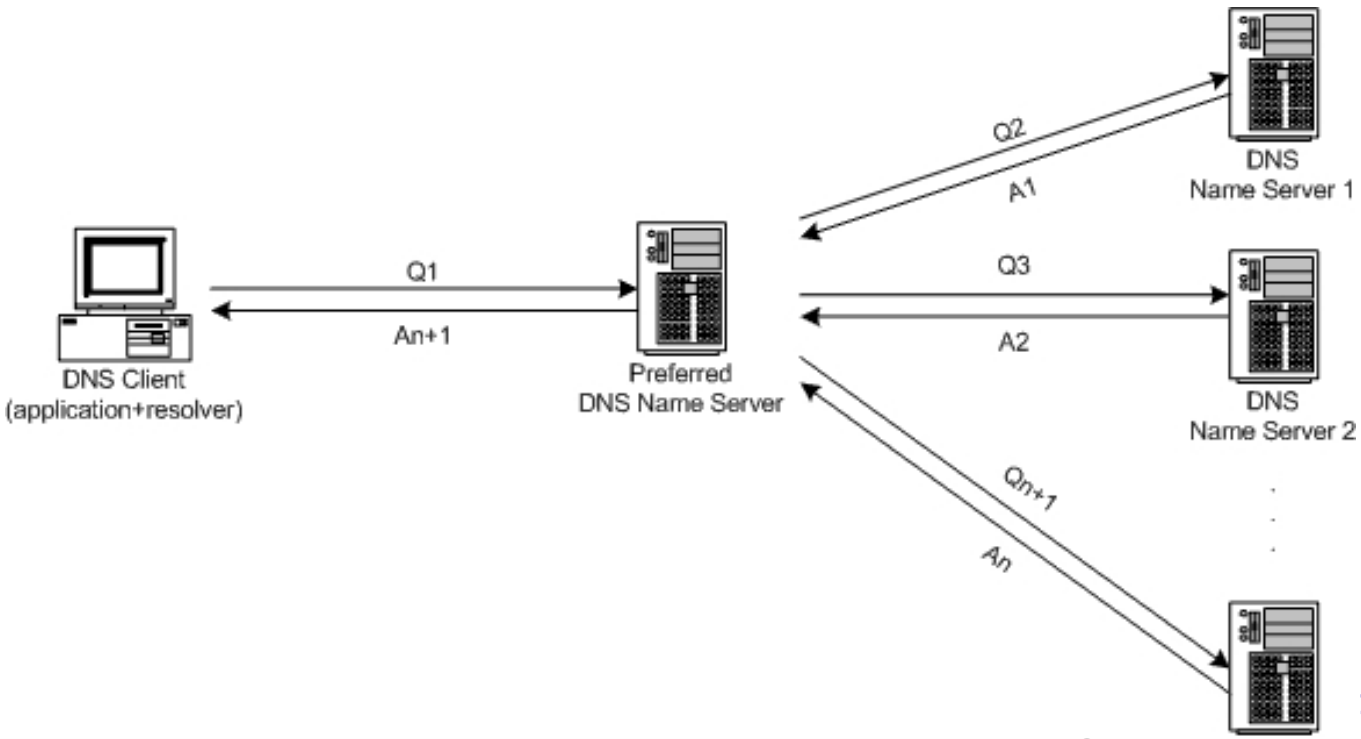
- In 2006 several high-impact Distributed Denial of Service (DDoS) attacks.
- Primary attackers: Caching Open Recursive Nameservers further revered to as CORNs.

But unfortunately, things change...

- In 2006 several high-impact Distributed Denial of Service (DDoS) attacks.
- Primary attackers: Caching Open Recursive Nameservers further revered to as CORNs.

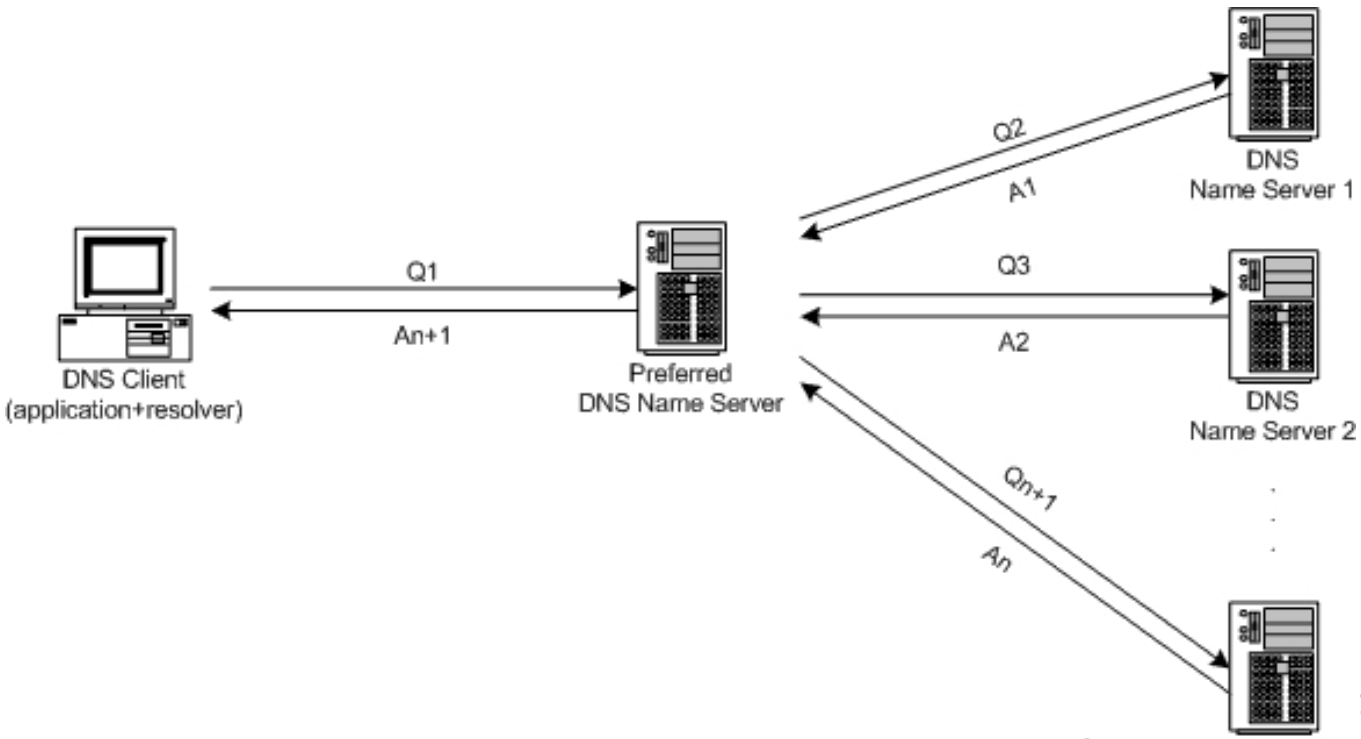
What is a CORN?

- What is a DNS server?
  - Converts FQDN to IP-addresses and vice versa
- What is a Open Recursive Nameserver (further: ORN)
  - A recursive NS for the whole wide world
- What is Caching Open Recursive Nameserver



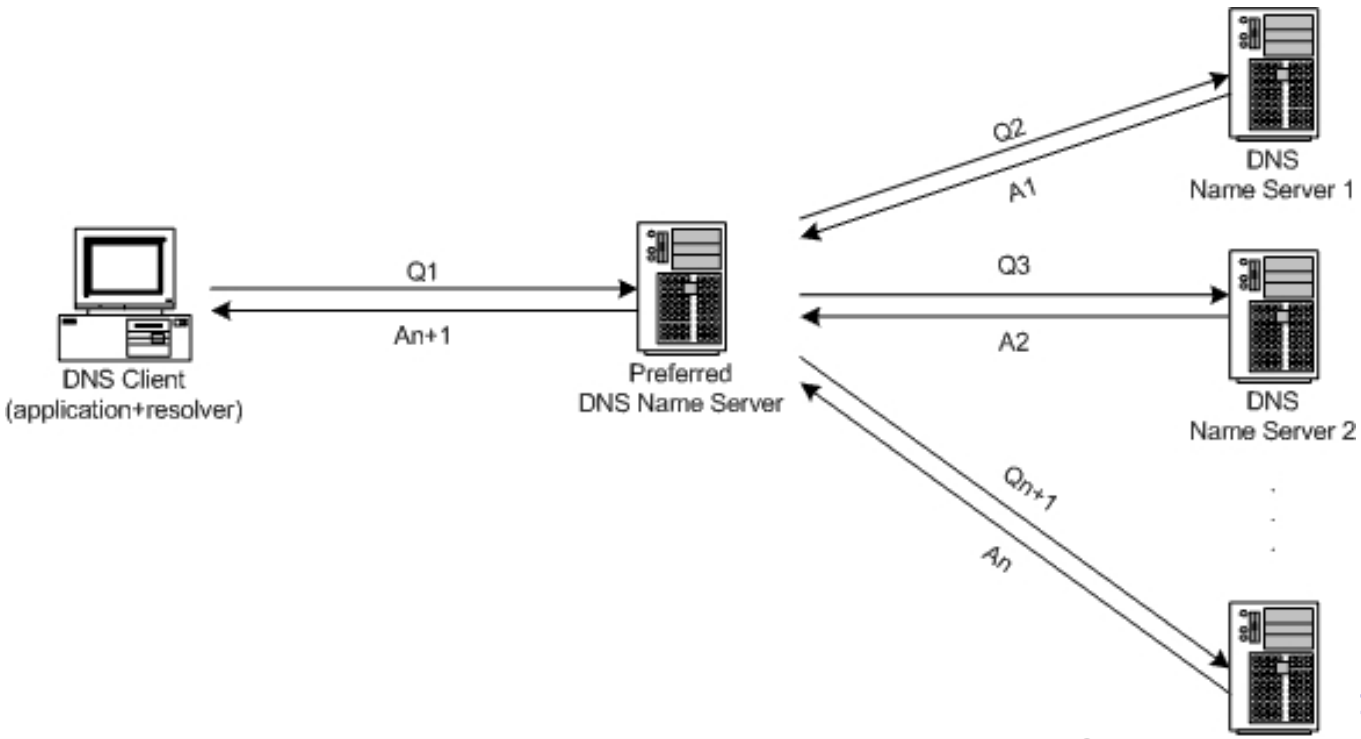
What is a CORN?

- What is a DNS server?
  - Converts FQDN to IP-addresses and vice versa
- What is a Open Recursive Nameserver (further: ORN)
  - A recursive NS for the whole wide world
- What is Caching Open Recursive Nameserver



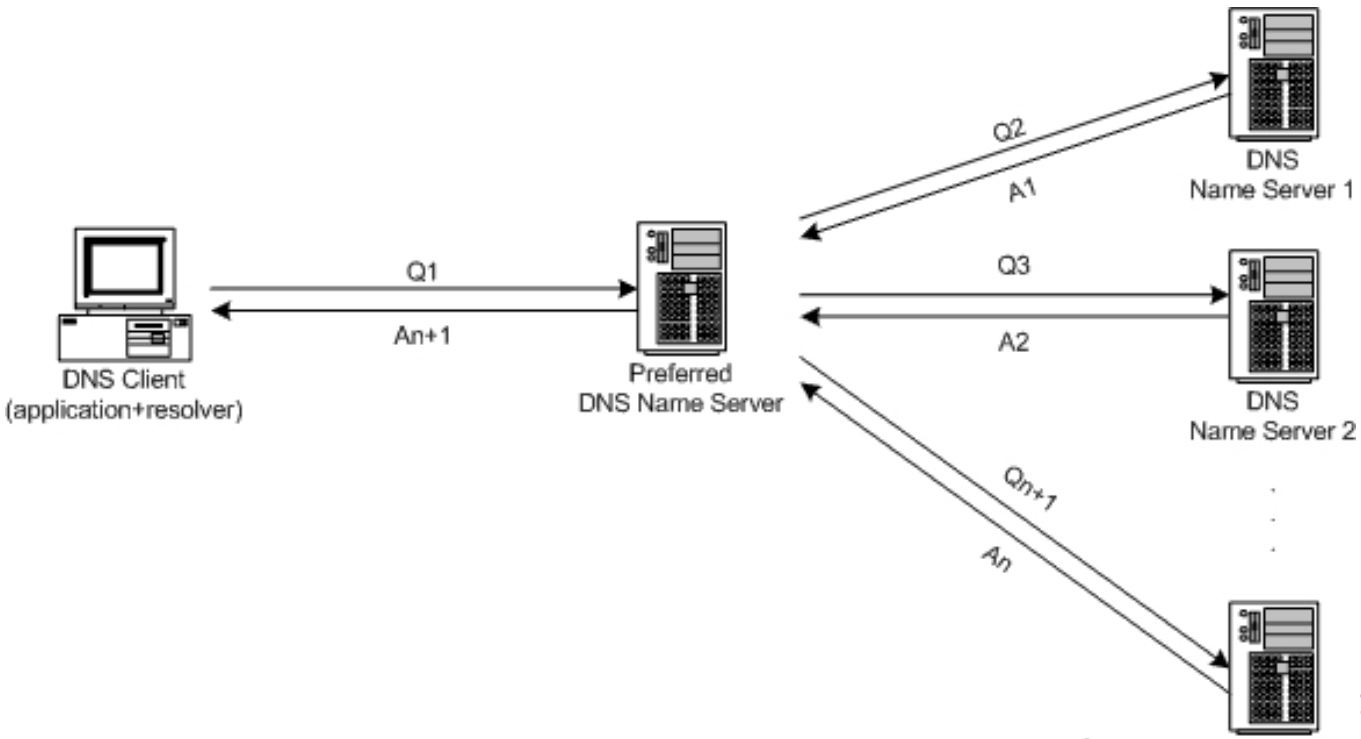
What is a CORN?

- What is a DNS server?
  - Converts FQDN to IP-addresses and vice versa
- What is a Open Recursive Nameserver (further: ORN)
  - A recursive NS for the whole wide world
- What is Caching Open Recursive Nameserver



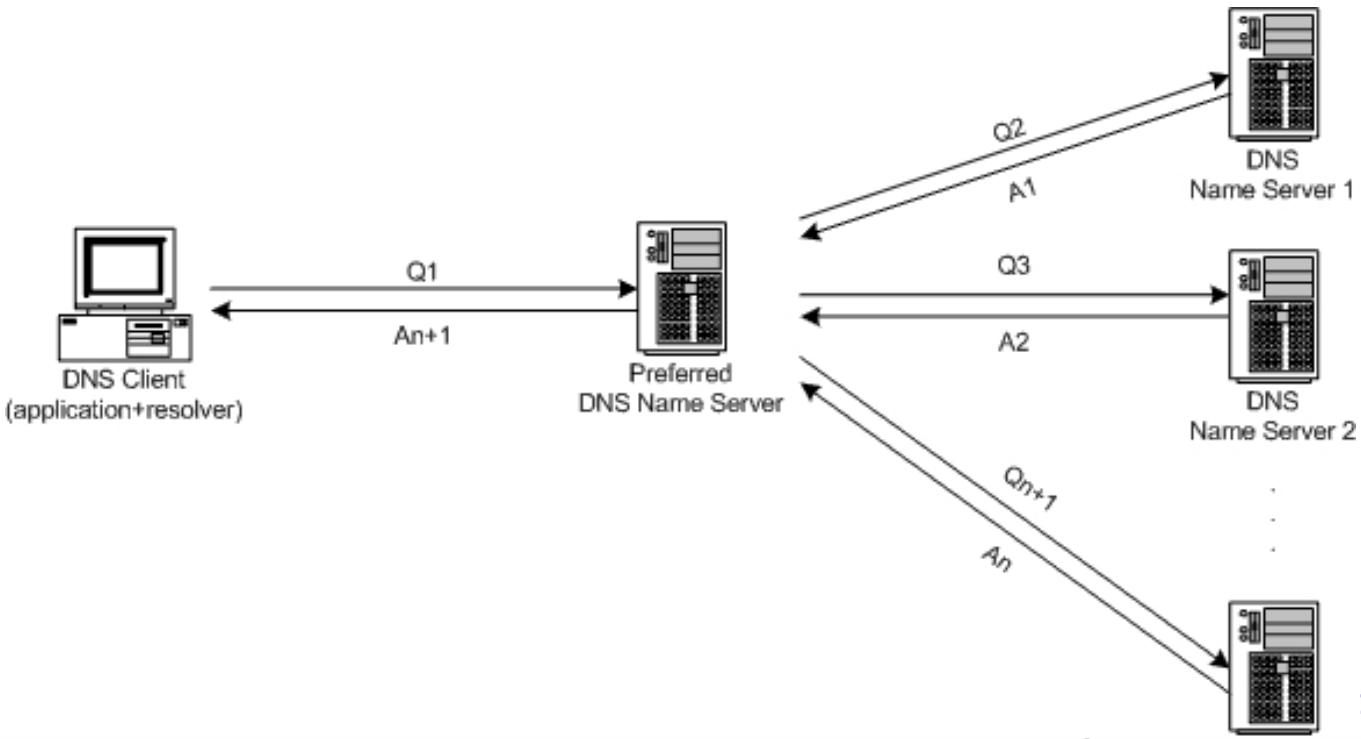
What is a CORN?

- What is a DNS server?
  - Converts FQDN to IP-addresses and vice versa
- What is a Open Recursive Nameserver (further: ORN)
  - A recursive NS for the whole wide world
- What is Caching Open Recursive Nameserver



What is a CORN?

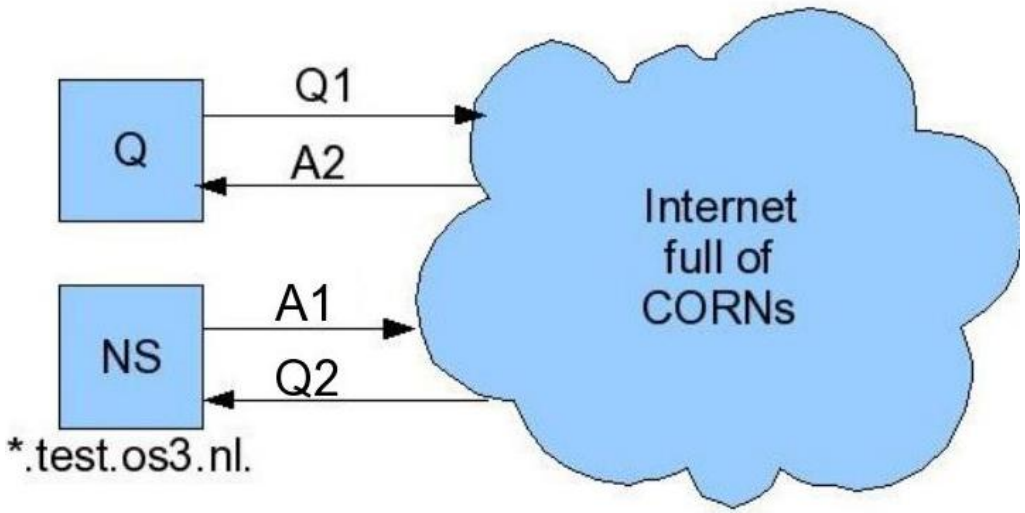
- What is a DNS server?
  - Converts FQDN to IP-addresses and vice versa
- What is a Open Recursive Nameserver (further: ORN)
  - A recursive NS for the whole wide world
- What is Caching Open Recursive Nameserver



Practical Research

Reconnaissance work...

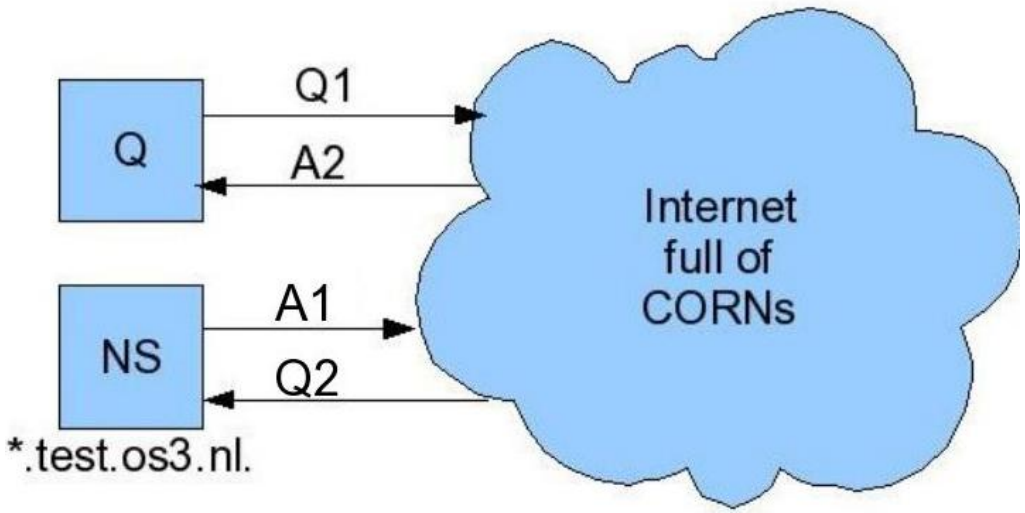
- How to create a list of Nameservers?
- How to determine if they are Open Recursive?
- How to determine if they cache?
- How to determine if the NS is a forwarder?



Practical Research

Reconnaissance work...

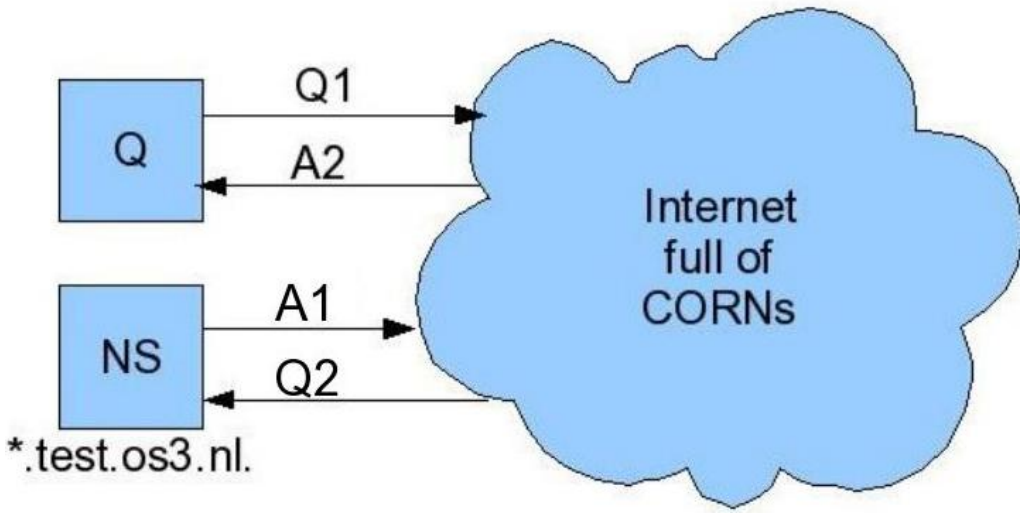
- How to create a list of Nameservers?
- How to determine if they are Open Recursive?
- How to determine if they cache?
- How to determine if the NS is a forwarder?



Practical Research

Reconnaissance work...

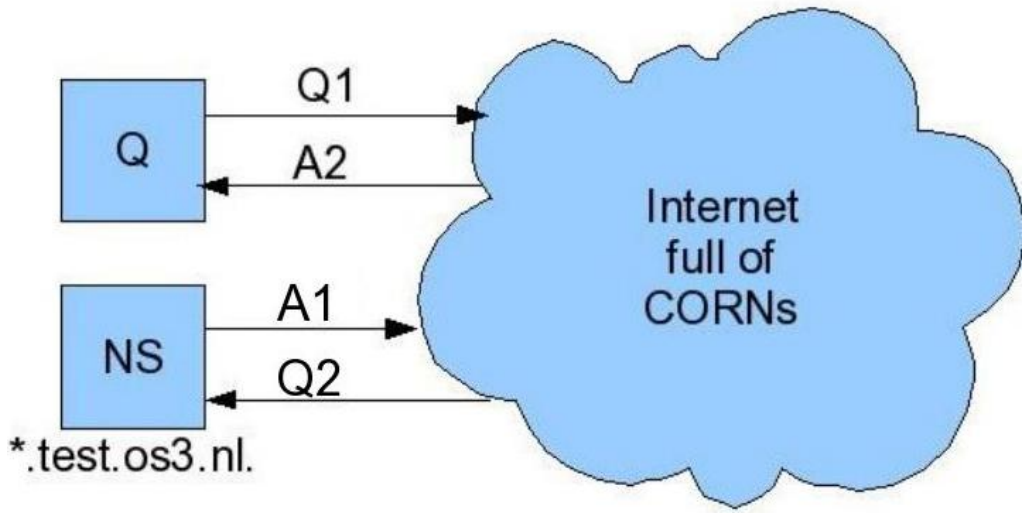
- How to create a list of Nameservers?
- How to determine if they are Open Recursive?
- How to determine if they cache?
- How to determine if the NS is a forwarder?



Practical Research

Reconnaissance work...

- How to create a list of Nameservers?
- How to determine if they are Open Recursive?
- How to determine if they cache?
- How to determine if the NS is a forwarder?



Practical Research

Zonefile	NS	NS (without timed-out)	CORNs
.int (inside .int domain)	59	51	21 (36%)
.int (outside .int domain)	203	195	65 (32%)
.edu (inside .edu domain)	4264	3333	2142 (50%)
.edu (outside .edu domain)	5124	4552	2173 (42%)
totals	9650	8131	4401 (46%)

Table: Total numbers zonefiles statistics

DNS Measurement estimates 9.000.000 nameservers running on the Internet.
With our test results we could estimate ~3.690.000 nameservers are CORNs!

Practical Research

The query (maximum DNS UDP packet sizes)...

- Maximum DNS UDP packet size: 512 bytes
- Normal DNS query size: ~50 bytes

Practical Research

The query (maximum DNS UDP packet sizes)...

- Maximum DNS UDP packet size: 512 bytes
- Normal DNS query size: ~50 bytes

Practical Research

The answer (TXT records)...

- Already explained: Maximum DNS UDP packet size: 512 bytes
- Normal DNS query size: ~50 bytes
- Normal DNS answer size: ~200 bytes
- Question: How to get the answer to 512 bytes
- Answer: TXT records (maybe other RRs?)

Practical Research

The answer (TXT records)...

- Already explained: Maximum DNS UDP packet size: 512 bytes
- Normal DNS query size: ~50 bytes
- Normal DNS answer size: ~200 bytes
- Question: How to get the answer to 512 bytes
- Answer: TXT records (maybe other RRs?)

Practical Research

The answer (TXT records)...

- Already explained: Maximum DNS UDP packet size: 512 bytes
- Normal DNS query size: ~50 bytes
- Normal DNS answer size: ~200 bytes
- Question: How to get the answer to 512 bytes
- Answer: TXT records (maybe other RRs?)

Practical Research

The answer (TXT records)...

- Already explained: Maximum DNS UDP packet size: 512 bytes
- Normal DNS query size: ~50 bytes
- Normal DNS answer size: ~200 bytes
- Question: How to get the answer to 512 bytes
- Answer: TXT records (maybe other RRs?)

Practical Research

UDP and DNSSEC...

Already explained:

- Question: How to get the answer to 512 bytes
- Answer: TXT records
- With DNSSEC extension enabled: bump up to 2048 bytes!!!

Practical Research

UDP and DNSSEC...

Already explained:

- Question: How to get the answer to 512 bytes
- Answer: TXT records
- With DNSSEC extension enabled: bump up to 2048 bytes!!!

Practical Research

patrick@patrick-desktop: /media/sdb5/rp1/code

File Edit View Terminal Tabs Help

```
; <<>> DiG 9.3.2 <<>> 0.test.pvabswoude.practicum.os3.nl @pvabswoude.practicum.os3.nl TXT +dnssec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50891
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;0.test.pvabswoude.practicum.os3.nl. IN TXT

;; ANSWER SECTION:
0.test.pvabswoude.practicum.os3.nl. 3600 IN TXT "This is a test by SNE students of the University of Amsterdam, more information is available at www.os3.nl/~
ptavenier" "hgdtezEmCUSWyGW05CfLylAawJT0idgOtccKU8ThuS8VkhWeV5s1OUe8uJHXvpyTFSyw2RUK7bx6ciKayunAOq9hhUMBTJX4lyQpep7Pj6q6T8E6QDtmjMXR1x34uGaw4KwZxWOsgBS6PRAX3
HrzCQ7b2gLi5RY4IjWZvzldZXoKWKdupF9wHnZIpS8eLw20shFkYMh" "lPn0XhuooVNxpvKxLGxXpZAOxmwXUGpaqY4wD8w769mmHlSmGmlKRo1aDuSOPbqfOJTcPVks5hQFhpRsonoTKzUdOP6PKAZMHubU
ZHLlYRF9FqJDeRz7aCEGNe5utS9cOZIH4Unfh3iBUh23eOjMOHuFdxRpce1PQ42TNnUxueC9ied2OB5V8uhLAT9Ulelljc8GXxAK" "heF5TeWYKYlewgOMasKj60vcpma11bvlydkpHe8uXiyIpza6nTgflJ
ow5osd9pwNnywZL7MRwdsue3LvKdH4M2FvKwL2UDRoBIH8lJUYGfgZLDYTDJHHIwaUB8RNOkpZwBlIiUAXU1CAtfkVKnwLB8Z15PxQIHHK2w554IZFqPDgzHW706b1tn0A74cS3IDuoOvTkYms" "TFWcgJ9B
OG4bFHsTnX3XwdYHUXNNPWTVeOM0GfXnATJJh49dqrC2BxCSXI21B26JiduUTIFOBF0ATSv0wPA07IMFAT6pBieK8nwRqaxvNY8kHs0uS1qAbJfiEBIqt8uAM5LS85ObIwZvFObwmF1jb9SIl6EYEcGXwBivB
tn20VSZviOPizauh2AmB0qlEFfpOCnOVvJu" "xS2kvafgg4DPc2IgG4zPTL1sTWsBrqp2eLLPLgddYqKXfbuGAYCjvXaLbyMGA3L19HYYN0EeBTDhCeiTBD5onoCQ2CsPvUkRKU1xktPg76tyUISDTSM9ZWS
Rx1jQ3nwxAWsXg88qYy2FIWjuhyX3te9cAaVBiG44NpDlmwl7UmqsQTRgaPDRwBOvDJSFf27ueVxaPn5F" "y4pZ5sWqoz1ewZvfdddQERHrUKLmRODlVRqZjcpWS1Ys0YIVGv8vt5W6f5oVZ69a03KC6kj1c
vhIiO4ahTeq4SZStVYx2GYbtcK38YL4WP5QXKwfh6Ww8z7mfYN0xwoBo3vc2FVgFNMEn9IcZqHNeEtKtnRaUGq2miPmNoloRRQq58ewhSraanU2qIGDwvQu7RStVFPF" "xvjWea2LdDobjFFS49OxrzRjgE8
IwVQtPOK9oQDCwBmuC7YAzxHsz1IzppV6yPEkofkDzph3lElpQZVZkoGs1x7atvjYuGZMNCVaXlLGLlhLB54QcRI40qGXVgYtqA3FIGDuRKfvy51RhyDzoJuXPevdxUVuEWlSctTjKsBZUoDdgmYXJrO5J62c
ITRLEYpFSPYOugMf" "UENAQGkHVmhD2b9wCS1K6WilzjtVTn9W1P5DI8VElOoO4f84Y4EzKjKrlMN6kXZLjkWN8x3xhHVsG78Su0AXlFuG0wIk0m6skHpkMe55LlH3Zb422qu4xvuxvwRuz1RZDNdypnlHDE
I5q9rVHmE0sNagyvcW5byoHA8AsiYYVRESo4XwqcE4XZrQv86FbLZWsXO8qUME" "lTwWpwXUybys6TISZDWnBPlPLp2i2hP9C6poA2FvBp5OWFwPMByntIU1nAQfZcdmGk1B7J04fO0lbl3kG4uZdmOlQaia
p4Leu30E7uHahsaWi7i8dD7Ro33GFr4OJ6Dx2mvV4xEgdGXMMnH4ufcel0w4mvuFkhXQiGo0Vpoe5Q8iq234avdPvsr9LJypDeMiqSCD7Xb2" "A6FQnCnoUtEcPStefm9pUGLmpyhN"

;; AUTHORITY SECTION:
pvabswoude.practicum.os3.nl. 3600 IN    NS      ns1.pvabswoude.practicum.os3.nl.

;; Query time: 45 msec
;; SERVER: 145.92.25.11#53(145.92.25.11)
;; WHEN: Sun Jan 28 15:31:40 2007
;; MSG SIZE  rcvd: 2048

patrick@patrick-desktop:/media/sdb5/rp1/code$
```

Figure: DNSSEC and UDP

Practical Research

```
;; AUTHORITY SECTION:
pvabswoude.practicum.os3.nl. 3600 IN    NS      ns1.pvabswoude.practicum.os3.nl.

;; Query time: 45 msec
;; SERVER: 145.92.25.11#53(145.92.25.11)
;; WHEN: Sun Jan 28 15:31:40 2007
;; MSG SIZE  rcvd: 2048
```

Figure: Authority section zoomed in

Practical Research

An actual DNS DDoS attack...

- We conducted 3 tests.
- Following statistics gathered from our own CORN.

incoming: 148KB/s – outgoing: 5430 KB/s
incoming: 151KB/s – outgoing: 5670 KB/s
incoming: 149KB/s – outgoing: 5441 KB/s

- Each byte that comes in (the query) the victim will get a answer that is **36-38 times greater!**
- You need about 2.7 - 2.8% bandwidth of the victim you attack.

Practical Research

An actual DNS DDoS attack...

- We conducted 3 tests.
- Following statistics gathered from our own CORN.

incoming: 148KB/s – outgoing: 5430 KB/s
incoming: 151KB/s – outgoing: 5670 KB/s
incoming: 149KB/s – outgoing: 5441 KB/s

- Each byte that comes in (the query) the victim will get a answer that is **36-38 times greater!**
- You need about 2.7 - 2.8% bandwidth of the victim you attack.

Practical Research

An actual DNS DDoS attack...

- We conducted 3 tests.
- Following statistics gathered from our own CORN.

incoming: 148KB/s – outgoing: 5430 KB/s
incoming: 151KB/s – outgoing: 5670 KB/s
incoming: 149KB/s – outgoing: 5441 KB/s

- Each byte that comes in (the query) the victim will get a answer that is **36-38 times greater!**
- You need about 2.7 - 2.8% bandwidth of the victim you attack.

Defending strategies

- Nameserver config solutions
  - Disable Open Recursion
  - Use Access Control Lists
  - Create Views
  - Get your logging straight
- –NOT– nameserver config solutions (firewall, routers etc.)

Further Research

- How many servers have DNSSEC enabled?
- Are there any CORNs behind forwarders?
- Is there a way to conduct this kind of attack with other RRs?
- Could you use ORNs and still stay undetected?

Question to the audience...

Do we have to be concerned of large DNS DDoS attacks?

Our opinion: YES!

and definitely with the upcoming of DNSSEC

Question to the audience...

Do we have to be concerned of large DNS DDoS attacks?

Our opinion: YES!

and definitely with the upcoming of DNSSEC

Question to the audience...

Do we have to be concerned of large DNS DDoS attacks?

Our opinion: YES!

and definitely with the upcoming of DNSSEC

Questions?