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.
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...
What is a CORN?

- What is a DNS server?
  - Converts FQDN to IP-addresses and vice versa
- What is an 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
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?

[Diagram showing a query (Q) going to a Nameserver (NS) with responses A1 and A2, and queries Q1 and Q2 being handled by an internet full of CORNs.]

Open Recursive Nameservers
**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

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

Table: Total numbers zonefiles statistics

DNS Measurement estimates 9.000.000 nameservers running on the Internet.
With our test results we could estimate $\sim$3.690.000 nameservers are CORNs!
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
The answer (TXT records)...

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

Figure: DNSSEC and UDP
Practical Research

Figure: Authority section zoomed in
Practical Research

An actual DNS DDoS attack...

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

<table>
<thead>
<tr>
<th>incoming</th>
<th>outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>148KB/s</td>
<td>5430 KB/s</td>
</tr>
<tr>
<td>151KB/s</td>
<td>5670 KB/s</td>
</tr>
<tr>
<td>149KB/s</td>
<td>5441 KB/s</td>
</tr>
</tbody>
</table>

- Each byte that comes in (the query) the victim will get an answer that is **36-38 times greater**!
- You need about 2.7 - 2.8% bandwidth of the victim you attack.
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 an 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?
Do we have to be concerned of large DNS DDoS attacks?

Our opinion: YES!
and definitely with the upcoming of DNSSEC
Do we have to be concerned of large DNS DDoS attacks?

Our opinion: **YES!**

and definitely with the upcoming of DNSSEC
Do we have to be concerned of large DNS DDoS attacks?

Our opinion: **YES!**

and definitely with the upcoming of DNSSEC
Questions?