“Upward Referrals Considered Harmful”

Peter Losher
Senior Operations Engineer
Internet Systems Consortium

NANOG 45 Lightning Talk
Santo Domingo, Dominican Republic

Background

- On 01.18.2009, ISPrime became the victim of a DNS-based DDoS attack using spoofed source addresses.
- Some call it an amplification attack because the query ". IN NS" is quite small (47 octets) while an upward referral response is a bit larger (256 octets).
- One interesting aspect of this attack is that the queries are apparently sent to authoritative nameservers only. (rather than open resolvers as seen previously)

Sample

```
% dig +short @10.0.0.1 . NS
K.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.
```

An old debate returns:

What is an authoritative nameserver's appropriate response to a query that cannot be answered?

This is bad because...

1. Upward referrals are generally useless. The resolver that is iterating through the space already knows where to start.
2. A proper iterative resolver should consider the upward referral "out of bailiwick" and ignore the data anyway.
3. The authoritative nameserver's root zone "hints" may become stale over time if not properly maintained, causing delivery of queries to decommissioned root server addresses.
4. Upward referrals can lead to "referral loops" that result in hundreds of useless queries.

Don’t filter these queries!

- it’s a increasing arms race, having to update your firewall rulesets for every permutation. (. NS, .A, etc.)
- There is already a solution.

Solutions

- In BIND:
  - If your nameserver is a master for some zones, it needs the root hints to correctly send NOTIFY messages to the slave nameservers. To prevent upward referral responses, you can add **`additional-from-cache no;`** to the global options:
  - You can also use access controls to accomplish the same thing by denying all queries globally and then allowing queries for each zone.
  - **NOTE:** simply removing the root hints from your configuration does not solve this problem!

Success!

```
% dig @10.0.0.1 . NS

; <<>> DiG 9.4.2-P2 <<>> @10.0.0.1 . NS
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 5314
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;.                                      IN         NS

;; Query time: 6 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)
;; WHEN: Wed Jan 28 05:10:26 2009
;; MSG SIZE  rcvd: 17
```

Solutions (cont.)

- PowerDNS
  - set **`send-root-referral=no`** in your config file.
- Other DNS software suites (NSD, Nominum, etc...)
  - Contact your vendor.

Thanks to:

- Duane Wessels @DNS-OARC

  https://www.dns-oarc.net/oarc/articles/upward-referrals-considered-harmful
- members of the dns-operations and nanog mailing lists