# Strange Things Found in an Open Resolver Survey

Duane Wessels
The Measurement Factory/CAIDA

WIDE+CAIDA Workshop #9
January 19, 2008

# Open Resolvers

- Defined: A nameserver or other DNS application that forwards queries from "anywhere" to an authority server.
- Used in some large-scale DDoS spoofing attacks.
- Increase susceptibility to cache poisoning and software bugs.
- Useful for geeks who travel a lot.

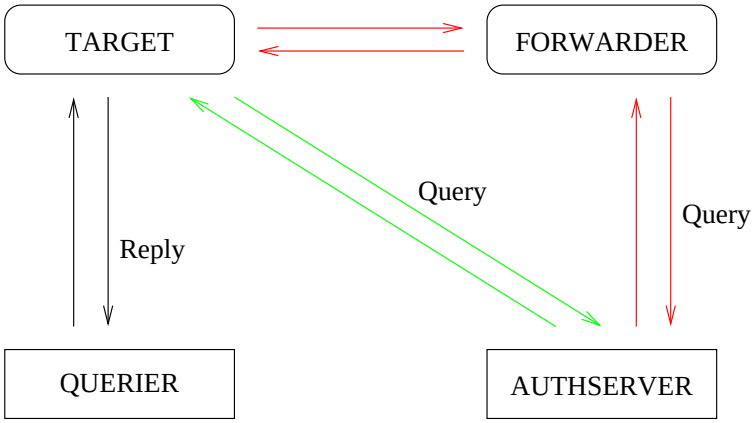
# How Many?

- Measurement Factory tracks about 450,000 open resolvers from known nameservers.
  - authority servers
  - caching resolvers
- John Kristoff counted about 16,000,000 by probing every IANA-allocated IPv4 address in April–June 2007.

# TMF October 2007 Survey

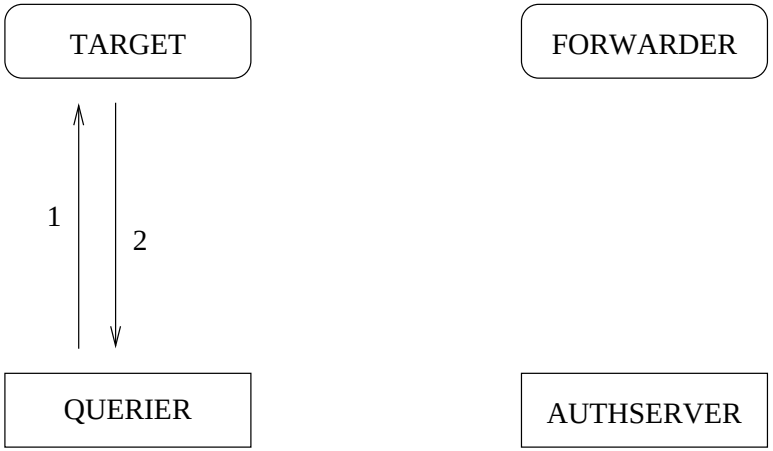
- Similar to Kristoff survey, except that we only probed 5% of address space found in a routeviews snapshot.
- Send queries like '$target.$timestamp.openresolvers.org' to 87,737,391 targets.
  - Query name contains target address
  - Query name contains timestamp, to add uniqueness and allow gross trip-time measurements.

# The Model




- QUERIER sends a QUERY to TARGET
- Look for that QUERY to reach AUTHSERVER
- QUERY may or may not go through a FORWARDER
- AUTHSERVER always answers with a REPLY
- Expect REPLY to reach QUERIER

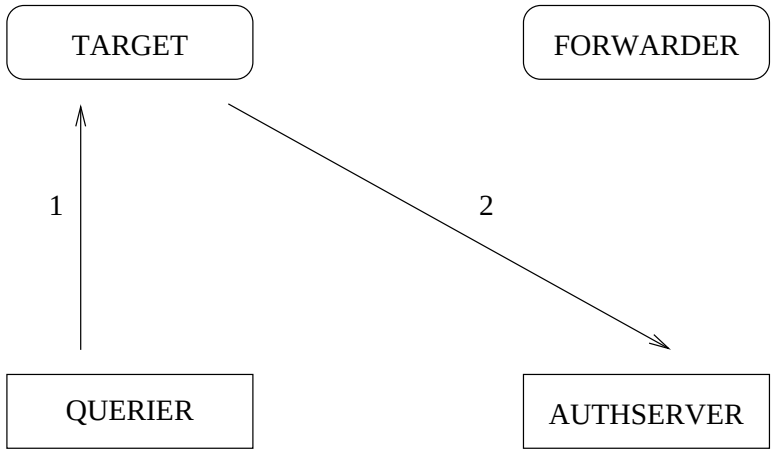
# Closed Resolvers




- We say that the Target is a "closed resolver" if we receive a Reply but the Authserver does not receive a Query.
- Of all resolvers that we find, **7.2%** are Closed.
- This means that **92.8%** of resolvers that we find will forward a Query.

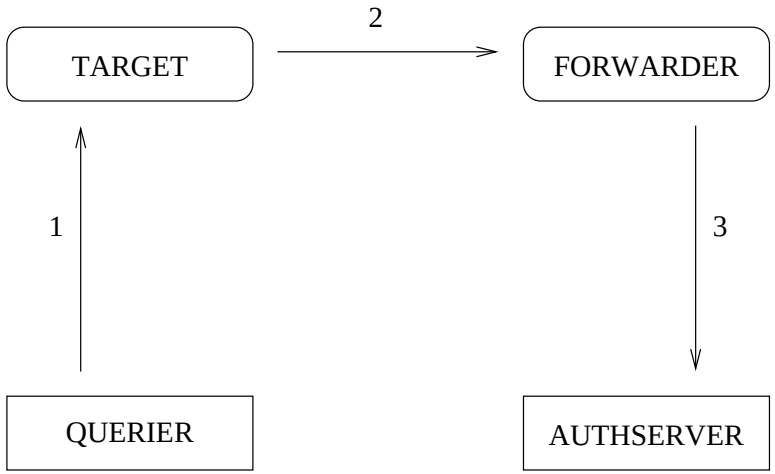
# Where do Open Target's Queries come from?

# Open Target, Query from Target




- Among open Targets, only **3.7%** of Queries are received directly from the Target.

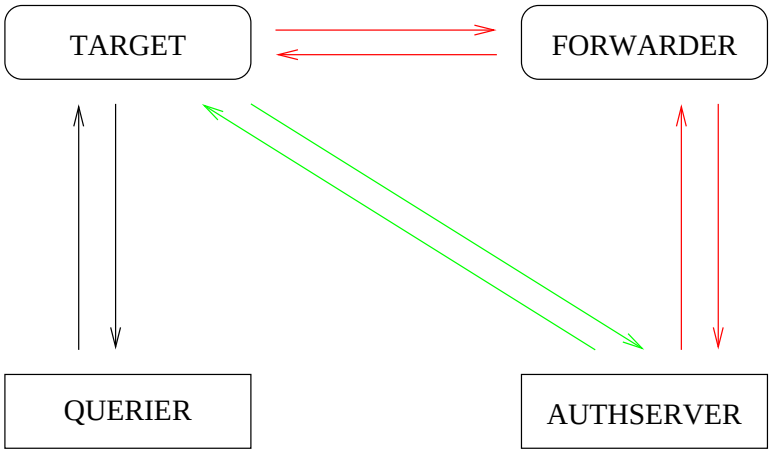
# Open Target, Query from Forwarder




- Among open Targets, **96.3%** of Queries are received from a Forwarder.
- Possibly more than one Forwarder in the path, can't tell.
- Leads us to believe that most open Targets simply forward queries to their ISP-configured nameserver.
- @@ plot "distance" between target and forwarder

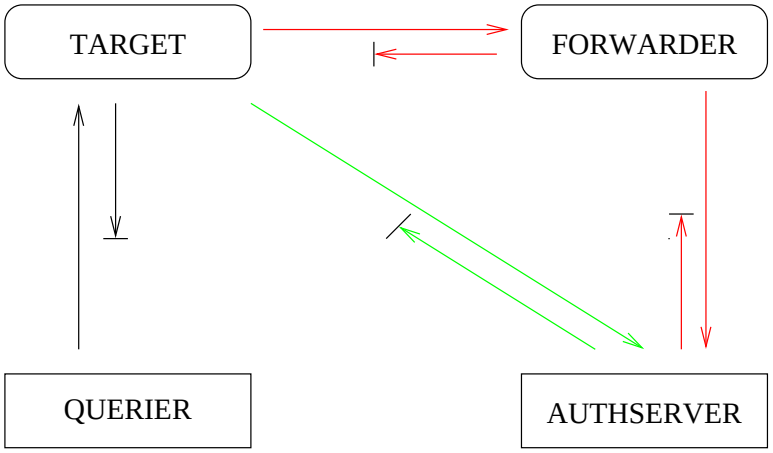
# Where do Open Target's Replies come from?

# Open Target, Reply from Target



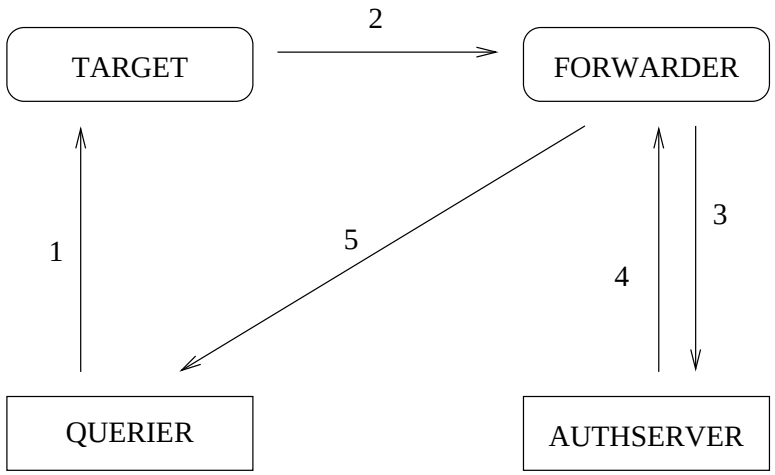

- For **79.9%** of open Targets we a Reply back from the Target.
- Obviously, most of these also go back through a Forwarder.

# Open Target, Reply not received



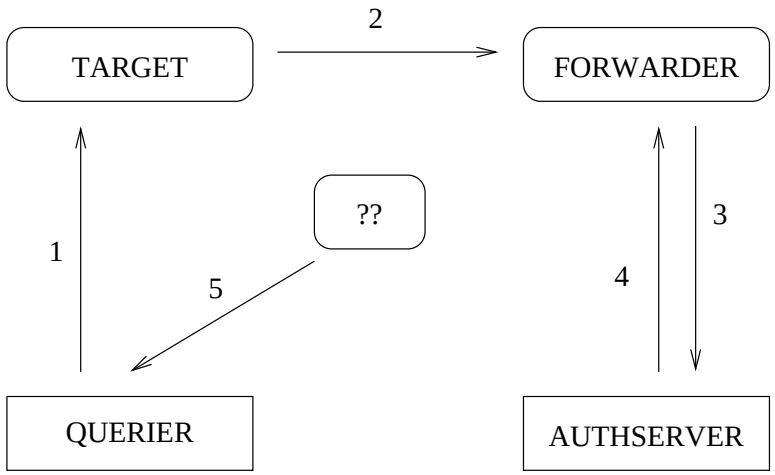

- In about **16.7%** of cases, we detect an Open Target at the Authserver, but do not receive a Reply at the Querier.
- Almost all of these go through a Forwarder.
- We do not know exactly where the Reply is blocked or dropped.

# Open Target, Reply from Forwarder




- In **0.3%** of cases, a Reply comes back from the Forwarder, instead of the Target!

# Open Target, Reply from Elsewhere




- In **3.2%** of cases, a Reply comes back from an address that is neither the Target, nor the Forwarder!!
- Maybe an intermediate Forwarder that we can't otherwise detect?

# Other Funny Stuff

# Changed Peer Port

- Among both Open and Closed Replies, 20.5% of them came back from a different UDP port!

```
00:13:06.485388 IP 192.172.226.156.58969 > 70.16.160.28.53:  19685+ A? 4701fd92.1ca01046.openresolvers.org. (59)
00:13:06.811389 IP 70.16.160.28.50455 > 192.172.226.156.58969: UDP, length: 75

00:13:06.521399 IP 192.172.226.156.53098 > 71.250.125.67.53:  19703+ A? 4701fd92.437dfa47.openresolvers.org. (59)
00:13:06.866600 IP 71.250.125.67.50740 > 192.172.226.156.53098: UDP, length: 75

00:13:06.645365 IP 192.172.226.156.56570 > 72.68.160.115.53:  19765+ A? 4701fd92.73a04448.openresolvers.org. (59)
00:13:06.978899 IP 72.68.160.115.50881 > 192.172.226.156.56570: UDP, length: 75
```

- Surprisingly common.
- Broken NAT?

# Changed Answers

- Authserver always answers with 127.0.0.3.
- Found 49 cases like this, out of 671,329 Open Targets.

```
00:31:16.941316 IP 192.172.226.156.52254 > 83.105.70.17.53:  53297+ A? 470201d4.11466953.openresolvers.org. (59)
00:31:17.106875 IP 194.159.187.34.48213 > 192.172.226.156.53:  11026 A? 470201d4.11466953.openresolvers.org. (59)
00:31:17.106974 IP 192.172.226.156.53 > 194.159.187.34.48213:  11026* 1/1/0 A 127.0.0.3 (97)
00:31:17.136243 IP 83.105.70.17.53 > 192.172.226.156.52254:  53297*- 1/1/1 A 62.6.38.125 (115)
```

# Reply before Query

- Found 698 cases (out of 671,329 open Targets) where the Querier received a Reply *before* the Authserver received the Query.
- In most of these 698 cases, the Reply code is REFUSED, SERVFAIL, or NOERROR with unexpected RDATA.
- In 76 of the 698 cases, the Querier got multiple Replies (ie, SERVFAIL first, followed by NOERROR later).
- However, in 8 cases, we got only the expected reply!!
- Cache hits?
- Pcap drops?

# Reply before Query Examples

```
05:55:17.697746 IP 192.172.226.156.50591 > 88.254.24.227.53:  18639+ A? 47024dc5.e318fe58.openresolvers.org. (59)
05:55:18.638869 IP 88.254.24.227.53 > 192.172.226.156.50591:  18639 1/1/0 A 127.0.0.3 (97)
05:55:18.778398 IP 212.175.13.113.32795 > 192.172.226.156.53:  14859% [1au] A? 47024dc5.e318fe58.openresolvers.org. (
05:55:18.779217 IP 192.172.226.156.53 > 212.175.13.113.32795:  14859* 1/1/1 A 127.0.0.3 (108)

07:52:15.233964 IP 192.172.226.156.53403 > 87.11.30.44.53:  46081+ A? 4702692f.2c1e0b57.openresolvers.org. (59)
07:52:15.817325 IP 87.11.30.44.53 > 192.172.226.156.53403:  46081 1/0/0 A 127.0.0.3 (75)
07:52:15.930076 IP 85.37.17.47.35586 > 192.172.226.156.53:  34621 A? 4702692f.2c1e0b57.openresolvers.org. (59)
07:52:15.930226 IP 192.172.226.156.53 > 85.37.17.47.35586:  34621* 1/1/0 A 127.0.0.3 (97)

13:13:34.860064 IP 192.172.226.156.62698 > 196.20.35.213.53:  24263+ A? 4702b47e.d52314c4.openresolvers.org. (59)
13:13:37.763541 IP 196.20.35.213.53 > 192.172.226.156.62698:  24263* 1/1/0 A 127.0.0.3 (97)
13:13:50.022256 IP 212.122.224.11.49152 > 192.172.226.156.53:  45289% [1au] A? 4702b47e.d52314c4.openresolvers.org. (
13:13:50.022418 IP 192.172.226.156.53 > 212.122.224.11.49152:  45289* 1/1/1 A 127.0.0.3 (108)
```

- In both cases the Forwarder is forwarding for many Targets.
- These look like cache hits (note no "*" by first reply query ID).
- 212.175.13.113 and 212.122.224.11 fingerprint as ISC BIND 9.2.3rc1 – 9.4.0a0
- 85.37.17.47 fingerprints as Nominum CNS

# Unexpected queries with same ID

```
> tcpdump -n -r 20071002.pcap dst host 192.172.226.156 and dst port 53 | grep -i a.root-servers.net
reading from file 20071002.pcap, link-type EN10MB (Ethernet)
00:20:07.665907 IP 123.100.2.222.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
00:22:34.732517 IP 211.88.12.253.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
00:29:06.559121 IP 218.201.39.107.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
00:47:19.587712 IP 210.51.171.54.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
00:55:04.302365 IP 211.157.104.192.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
00:55:24.926496 IP 61.183.175.44.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
00:55:46.175108 IP 121.14.3.113.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
01:04:25.205090 IP 210.82.118.226.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
01:07:19.102576 IP 210.73.64.55.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
01:10:25.703951 IP 58.211.140.126.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
01:18:32.574520 IP 202.10.64.69.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
04:17:07.579403 IP 210.51.170.65.53 > 192.172.226.156.53:  40162+ A? a.root-servers.net. (44)
```

- Probe host sends queries for *a.root-servers.net*, but it should not receive them
- Note all have the same query ID!
- These addresses could not be fingerprinted (timeout errors).
- Malware? Buggy CPE?

The End