Finding Open DNS Resolvers

Duane Wessels
The Measurement Factory
wessels@measurement-factory.com

June 2, 2005

Open Resolvers/Recursion

- An *open resolver* is a DNS server that provides DNS recursion for clients outside of its own organization.
- Sometimes, authoritative servers are unintentionally also configured for recursion.
- Sometimes, recursive servers don't have any ACLs.
- Similar to SMTP relays and open proxies.

Problems with Open Recursion

- Open recursion enables poisoning of vulnerable nameservers.
- Recent DDOS amplification attacks.
- DNS cache spying.
- Abuse of resources in general.
- There are benefits as well...

The RA Bit

- The DNS message header has a "Recursion Available" bit.
- Not always accurate.
- Nameserver policy or controls may allow or deny particular queries.
- Packet filters may prevent recursion.
- Missing or different root hints.
- Implementation bugs.

How to Test for Openness

- Setup a "fake" authoritative server for a zone.
- Select target IP address to test.
- Send a query for a name in the zone that you know will not be cached.
- Encrypt target address in the query name, in case target host has multiple addresses.
- If authoritative server receives a valid query, the target is open.
- Periodically re-test targets.

Finding Targets

- Addresses that query our real authoritative servers.
- Authoritative servers taken from Additional section of DNS queries.
- Addresses submitted for testing via Web page.
- Authoritative servers seem to be the best source of open resolvers.

What We Found

- Currently tracking about 350,000 open resolvers.
- About 50% of addresses we test are open.

Unexpected Results

- CoDoNS Beehive nameservers automatically refresh expired RRs.
- When our fake authoritative server crashed or stopped, we received AAAA/A6 query storms, presumably from BIND 8.3.[2-4] bug #1503.

Future Work

- Web interface to see open resolvers based on CIDR network
- Periodic reports grouped by AS# or RIR Ids.
- Looking for more sources of targets to probe.

The End