Recursive DNS attacks

SANOG VIII

Aug 2nd, 2006

Karachi, Pakistan

Zaeem Arshad

DANCOM Online

zaeem.arshad@dancom.net.pk

Overview

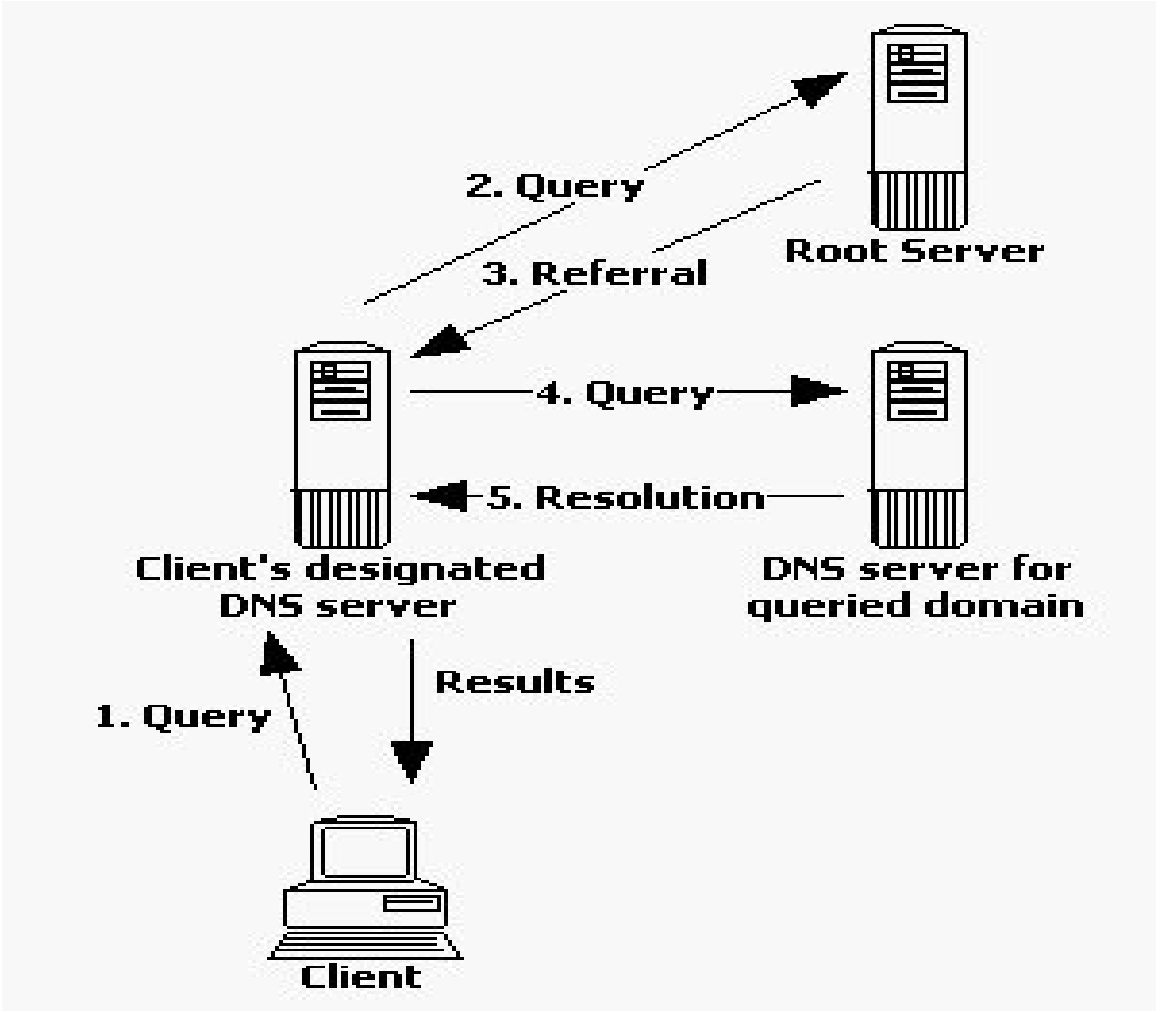
- Recursive DNS Overview
- Anatomy of an amplification attack
- Service provider considerations
- DNS software considerations

DANCOM Online

Recursive DNS

- Query other NS on client's behalf.
- Server Caches answer for quicker future lookups.
- Load is on the server rather than on the client.

Recursive DNS



Open Recursive Nameservers

- Is basically a recursive nameserver but accepts recursive queries from just anyone.

DANCOM Online

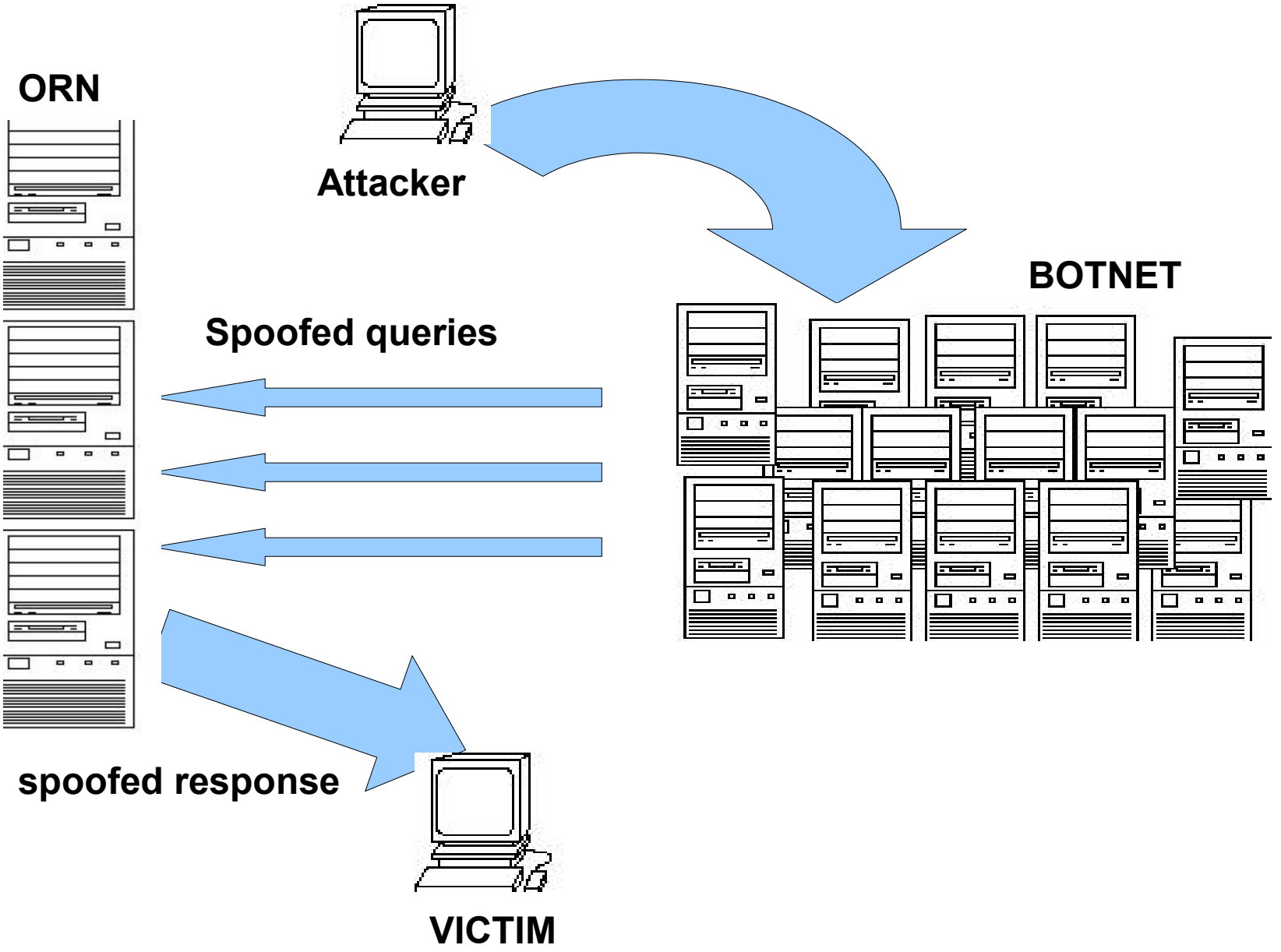
ORN as attack vectors

- Recently, ORNs have been used as amplifiers in DDoS attacks.
- These attacks are not due to any design flaw in the DNS protocol.
- DNS uses UDP and has a small query-large response behavior which is exploited by attackers.

Amplification attack

- These attacks are called amplification or reflector attacks due to their nature.
- The attacker sends a UDP query to the ORN which sends a large response to the source IP of the query.
- The source IP is spoofed as to that of the victim and all responses are sent to the victim.

Anatomy of an amplification attack



Anatomy of an amplification attack

- Attacker publishes a large record in a compromised nameserver or purposely setup nameserver.
- The drones query for the large record using their respective ORNs. The source IP of the query is modified to be that of the victim.
- The servers return the results but to the victim and not the drones.

Anatomy of an amplification attack

- Due to multiple ORNs being used, the number of queries received per NS is pretty low which doesn't raise any alarm with the operator.
- Amplification factor could be as high as 80 given many ORN support EDNS0 and other extensions to the DNS protocol.

Traffic calculation in an amplification attack

- 20,000 ORNs queried 5 times a second.
- DNS query is 68 bytes, response is 4050 bytes.
- An amplification factor of almost **60:1**
- Traffic generated towards the victim is **3Gbps** approx!.
- Traffic received per server is **2,720 bps**
- Traffic generated per server is **162 kbps**

DANCOM Online

Let's make things worse!!

- 80% of the world's NS are open recursive - CERT/CC
- Allow-recursion ACL doesn't prevent NS from returning the malicious record with a huge TTL.
- RFID, DNSSEC, IPv6, ENUM, Domain keys and SPF.

Doomsday Scenario?

- Not exactly...but if we don't start fixing the problem today, we will never be able to fix it.
- Not to be taken lightly as the attacks against BlueFrog recently has shown the power and skill of botnet operators.

Service Provider Considerations

- The distributed nature of DDoS is both its power and weakness.
- Service providers should implement Unicast RPF.
- uRPF will NOT break your network.
- Understand your DNS servers and traffic patterns.
- Implement BCP38.

Securing Nameservers

- Separate authoritative and caching servers.
- Restrict recursion to internal/trusted clients only.
- Disable recursion to external clients.
- Restrict number of simultaneous recursive clients.
- Use views to split your DNS.

General Considerations

- It is very difficult to fend off such attacks.
- Tracing the source of the attack is very difficult.
- The broadband explosion in the South Asian market makes it a lucrative target for botnet operators as well as a harvesting field of ORNs.

Questions

DANCOM Online