Prevent DNS Server from being used for a DoS attack

Using authoritative name service, DNS servers primarily advertise to the world the various records associated with the domain they serve. Because users prefer common names and networks prefer numbers, DNS servers handle the translation between what a user types in a browser—such as go4expert.com—and the actual IP address the network understands.

The task of answering a query recursively is completely different. According to a US-CERT report, between 75 and 80 percent of all DNS servers can handle recursive requests.

Recursive DNS provide answers to queries for records by asking other DNS servers and providing that response to the client that made the request. Here's an example:
1. A user enters www.go4expert.com into a Web browser.
2. The computer contacts its local DNS server to determine the IP address of www.go4expert.com.
3. The DNS server looks up www.go4expert.com in its local tables (i.e., its cache) but does not find it listed.
4. The DNS server sends a query to a root server for the IP address of www.go4expert.com.
5. The root server replies with a referral to the top-level domain (TLD) servers for www.go4expert.com.
6. The DNS server then contacts the TLD server to determine the IP address of www.go4expert.com.
7. The TLD server replies with a referral to the name server for www.go4expert.com
8. The DNS server contacts the name server for www.go4expert.com to determine the IP address.
9. The name server checks a zone file that defines a CNAME record, which shows www.go4expert.com is an alias of go4expert.com.com. DNS returns both the CNAME and the A record for go4expert.com.com
10. The DNS server sends this response to the original client: go4expert.com.com = 68.178.211.89 (with CNAME record www.go4expert.com=go4expert.com.com).
How can a recursive query become a DDoS attack? For the attack to work, the attacker needs to be in control of one DNS record.

He or she then populates the TXT field of that record with information. (The maximum size of the TXT field is approximately 4,200 bytes.) And then the fun begins. Here's how:
1. The attacker programs bots to continuously execute requests for this record against recursive DNS.
2. The bots spoof the source IP address of these requests, replacing it with the DDoS target.
3. The recursive servers take the record from the attacker-controlled zone, and send it along to the IP address they think the request came from.
Multiply this by the number of bots participating in the attack, and you've got a DDoS attack. If your DNS server is a target of this attack, your network will grind to a halt because none of its clients can resolve an IP address.

What's the solution? It's quite simple: Run two different DNS servers. Let the internal server handle all requests from your network (even recursive for your clients only).

On the external DNS server, disable recursion. With recursion disabled, the external DNS server won't send queries on behalf of other name servers or clients, which stops attackers from bouncing DoS attacks off your DNS server by querying for external zones.

Final thoughts

Open DNS recursion isn't the problem—it's a symptom of the problem. IP address spoofing is the real problem, and this spoofing provides a ready venue for DDoS, spam, and other headaches.

In my opinion, IP address verification is the answer, and the tools already exist to solve that problem. I know the Internet Engineering Task Force (IETF) is looking at the issue, but it needs to stop investigating and take action.

Source: http://www.go4expert.com/articles/prevent-dns-server-dos-attack-t3624/