DNS Spoofing

Info: https://tools.ietf.org/html/rfc5452

When certain steps are taken, it is feasible to «spoof» the current deployed majority of resolvers with carefully crafted and timed DNS packets. Once spoofed, a caching server will repeat the data it wrongfully accepted, and make its clients contact the wrong, and possibly malicious, servers.

To understand how this process works it is important to know what makes a resolver accept a response.

The following sentence in Section 5.3.3 of [RFC1034] presaged the present problem:

The resolver should be highly paranoid in its parsing of responses. It should also check that the response matches the query it sent using the ID field in the response.

DNS data is to be accepted by a resolver if and only if:

1. The question section of the reply packet is equivalent to that of a question packet currently waiting for a response.
2. The ID field of the reply packet matches that of the question packet.
3. The response comes from the same network address to which the question was sent.
4. The response comes in on the same network address, including port number, from which the question was sent.

In general, the first response matching these four conditions is accepted.

If a third party succeeds in meeting the four conditions before the response from the authentic nameserver does so, it is in a position to feed a resolver fabricated data. When it does so, we dub it an «attacker», attempting to spoof in fake

data.

All conditions mentioned above can theoretically be met by a third party, with the difficulty being a function of the resolver.