DNS: Refusing UDP-based ANY

Edward Lewis
ed.lewis@neustar.biz
NANOG 57 Lightening Talk Submission
February XX, 2013

neustar.

The Problem

- For over a year there has been suspicious traffic directed at DNS servers, typified by UDP-based ANY queries
  - NANOG 56 had a DNS-track panel discuss one such attack
  - The incidence of “ANY” attacks is rising (not just repeats)
- UltraDNS sees this attack as a DDoS using our servers to amplify and reflect traffic to addresses of intended victims
- The impact of the attack is
  - Need for DDoS mitigation (work, delay)
  - Higher costs (bills) for everyone, not just the intended victims

Mitigations

- Adding capacity
  - Assumes we are the intended victim
  - For a reflection attack, more capacity means more to abuse
- Response Rate Limiting
  - Effective, but an in-line activity and scales “only so much”
- Refusing (UDP-based) ANY (RCODE=REFUSED)
  - Rationale is that this these queries have come to be more useful in abuse than in earnest operations

Storyline

- Late December 2012
  - REFUSED to answer UDP-based ANY, leaving TCP open
  - Received and noted complaints, along with suggested “fixes”
- Working on response-rate-limiting solution
  - Viewed as an interim step, suspending “REFUSED”
- Long term we want to turn off UDP-based ANY responses
  - For a number of reasons

UDP-based ANY Uses

- Domain Name pre-delegation checks
  - Some TLD do DNS “health checks”
- Mail forwarders
  - Collecting IPv4 and IPv6 addresses as well as mail data

- Suggested fixes
  - They varied, indicating there’s no “easy” protocol flag bit to set to “fix” all of this

Why a Lightening Talk?

- We want to start a conversation about the issue of eliminating UDP-based ANY queries
  - We feel that the functionality has become more of a security burden than a useful tool
  - We know there are some legitimate (earnest) uses of the query but there are alternatives
- We are picking on UDP-based ANY queries because they are in use. There other large response that can be used in amplification (DNSSEC related) but there are other mitigations for those records. “ANY” is an across-the-DNS problem