A Wild IPv6 Attack Appears!

IEPG @ IETF101

Wes George - Neustar
wesgeorge@puck.nether.net

“First” IPv6 DoS Attack?

Almost certainly not, and we all knew IPv6 attacks were coming, but not **when.**

- Lots of attack vectors that are protocol agnostic, easier to (ab)use than IPv6-specific ones
- Code that follows best practices will use IPv6 when available
- Arbor PR from 2012, but few public details around type/scale of attack

But…

- It is the first one I’ve seen and been able to analyze

IPv6 DNS – Good, Bad, Ugly

Good:

- Lots of recursive DNS servers with IPv6 addresses on the backend
- 1900+ unique querying hosts from ~450 ASNs, 65 countries (Cymru)

Bad:

- IPv6 Open Resolvers are a thing now
  - 400+ seen in the sample I analyzed

Ugly:

- People are (still) using 6to4 to do their own DNS recursion
  - 442 unique querying hosts seen (~22% of total)
  - 238 open resolvers responding to queries on 2002::/16 IPs

Open Resolver Hunting, version 6.0

- Can’t scan the IP range for things that respond on port 53 like we do with IPv4
  - But we do have some useful data we can mine
- People with lots of DNS servers can pull a periodic report of unique IPv6 query sources
- Attempt to query them (dig batch mode, etc)
- Make a list of those that respond, aggregated by prefix
- Aggregate that list from multiple sources and host it somewhere useful (openresolverproject.org?)

See also from DNS-OARC: https://indico.dns-oarc.net/event/28/session/11/contribution/43/material/slides/0.pdf

IPv6 Open DNS Resolvers – Questions

- Do DNS education and best practice documents cover IPv6?
- Do we need changes in DNS server default configurations for IPv6?
- Is this a real problem, or a minority of bad configuration?
- Any interest in trying to build lists of Open Resolvers?
- Are 6to4 sources:
  - IPv4 open resolvers that just happen to be behind 6to4 gateways?
  - DNS servers purposely configured to listen on a 6to4 address?
  - Specifically being used for attacks?
- Reject DNS queries from 2002::/16 and just let it fall back to IPv4?