Contribution ID : **43** Type : **Standard Presentation**

Identifying DNS Open Resolvers in IPv6

Friday, 9 March 2018 11:30 (15)

Introduction

As all of you know, having DNS servers considered Open Resolvers is very negative, both for those who leave the service open, for the Internet and for online security. To read about Open Resolvers I recommend reading this link: https://www.certsi.es/blog/dns

Identifying a DNS Open Resolvers in IPv6 (open DNS servers)

Identifying Open Resolvers servers or open DNS servers in the world of IPv4 is easy, due to the short length of the IPv4 space (2 ** 32) it is relatively easy to run check every IP.
In the world of IPv6 it is virtually impossible to verify each IP address, I mean, to test IP by IP. If we try this test can last thousands of years

How is a DNS Open Resolver identified?

A recursive DNS server should only answer queries to its own clients (yes, there are few exceptions) and should reject any other. For example, the DNS servers of the ACME ISP should only respond to queries from their own clients, to no one else.
Our test consist in querying a domain name (such as www.lacnic.net) to a list of DNS servers, if the DNS server responds with a response then it is considered Open Resolver, if it returns a rejection (Query refused) or simply timed out it is not an Open Resolver.

How we find the list IPv6 resolvers?

Lacnic manages a server that can be called: Reverse Root Server, specifically the letter "D", that is, d.ip6-servers.arpa. Many queries looking information for reverse DNS goes throughout this server, in general this server ONLY receives queries from DNS servers. This is where they get IPv6 addresses from DNS queries. Since this server does not allow recursion every IP that queries this device can be considered a resolver.

Procedure & Algorithm:

.- In the server, we captured over 2.5 millions packets. We captured only v6 packets, filtered by port 53 and destined only to the IP address of the server.

.- Malformed packets, errors, etc. were discarded.

.- From the IPv6 addresses obtained in step 2 a list of unicast IP addresses is created (that is, duplicates are deleted)

.- Finally we got a list of over 800.000 resolvers (not Open resolvers yet)
A python script takes each IPv6 address from the list gotten in item 4, and queries the FQDN www.lacnic.net, verifies recursion and the status of the response. In the case of an Open Resolver, the IP is registered

.- Some manual verification is also performed, I mean, we take some results (text file) and manually check the results.

What is going to be shown

In case this paper is accepted for presentation we are going to show some this mechanism accompanied with some results & statistics

Similar publications

https://labs.ripe.net/Members/luuk_hendriks/finding-open-dns-resolvers-on-ipv6

Partial raw data:

http://stats.labs.lacnic.net/BORRAR-v6-resolvers.txt

Summary

In this presentation we will show a mechanism we used to identify IPv6 Open Resolvers in Internet. We will also present some statistics regarding this fact and possible some things TO DO for the future

Talk Duration

15 Minutes

Primary author(s) : Mr. ACOSTA, Alejandro (LACNIC)

Presenter(s) : Mr. ACOSTA, Alejandro (LACNIC)

Session Classification : Public Workshop

Track Classification : Public Workshop