Identifying DNS Open Resolvers in IPv6

Dario Gomez dario at lacnic dot net
Alejandro Acosta alejandro at lacnic dot net
What is all this about?

Simple: as you know identifying Open Recursive DNS Servers in the IPv4 world is very easy, we needed to tried a different approach in IPv6
Ok., too much talk. What is the approach you previously mentioned!

**Step 1**

- **tcpdump (getting the pcap file)**
- **Pcap file processing, some basic sanity check, scp, rsync (bash)**
- **Processing, cleaning and publishing of the data (python3)**
- **Checking open resolvers IPv6 by IPv6 address (python3)**
What are going to be the final results

.- # of IPv6 Resolvers identified
.- % of IPv6 Resolvers identified per RIR
.- % of IPv6 OPEN IPv6 Resolvers identified
.- % of IPv6 OPEN IPv6 Resolvers identified by RIR
.- We also expect to identify some more information
## Summary of the results

<table>
<thead>
<tr>
<th>RIR</th>
<th>Total</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>arin</td>
<td>1892</td>
<td>51</td>
</tr>
<tr>
<td>lacnic</td>
<td>46</td>
<td>3</td>
</tr>
<tr>
<td>ripe</td>
<td>3211</td>
<td>38</td>
</tr>
<tr>
<td>afrinic</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>apnic</td>
<td>173</td>
<td>17</td>
</tr>
</tbody>
</table>

Total IPv6 DNS servers: 3211

Open IPv6 DNS servers: 38
Graphs (½)

IPv6 Resolvers: Open vs Closed

IPv6 Open Resolvers by RIR
Graphs (2/2)

# de resolvers por pais

BR
4,531 (76.9%)

# de resolvers abiertos por pais

BR
131 (54.8%)
Miscellaneous finding

Number of resolvers per /64:

2001:xxxx:xxxx:2/64 62
2a02:xxxx:0:xxxx/64 38
2a02:xxxx:0:xxxx/64 38
2001:xxxx:52:xxxx/64 34
2a02:xxxx:0:xxxx/64 32
What we were looking for
What we were looking for

30-09-2018|NO|2001:xxxx:yyyy::53| recursion Timed out while resolving with |****|arin|CA
30-09-2018|NO|2001:xxxx:yyyy::26| recursion Timed out while resolving with |****|arin|CA
30-09-2018|NO|2001:xxxx:yyyy::21| recursion Timed out while resolving with |****|arin|CA
30-09-2018|NO|2001:xxxx:yyyy:16c4| recursion Looks like query refused when resolving with |****|arin|US
30-09-2018|NO|2001:xxxx:yyyy:16c5| recursion Looks like query refused when resolving with |****|arin|US
What we were looking for

Dear [Name] S.A. de C.V. (4-LACNIC):


It may have undesirable consequences on the Internet because it may participate in an attack against a selected target, causing a Denial of Service (DOS) attack. It generates large UDP responses to spoofed queries, with those responses becoming fragmented because of their size.

We strongly recommend to reconfiguring your resolver. Here are some ways that may help you:

- To only serve your customers and not respond to outside IP addresses (in BIND, this is done by defining a limited set of hosts in "allow-query;;")

options {

    allow-query {
        192.168.196.0/24;
        2001:db8::/32;
    }
}

What we were looking for (good news)

*We do have evidence of ISPs that have fixed their servers!!*
Next steps

- Integration with main Lacnic system (milacnic)
- Automation of some stats in our portal
- Publish in open data format some statistics
- Recently trying to find squats prefixes with a recursive DNS
Questions / Comments