A Resolver Reputation System (ResRep)

June 4, 2014

CENTR Jamboree, R&D workshop
Marco Davids
The goal of the project:

• To investigate if assigning some sort of reputation to resolvers can help in mitigating abuse.

• To gather experience on data-science (analyzing ‘bigdata’).
How?

By ‘fingerprinting’ specific resolver-behavior.

<table>
<thead>
<tr>
<th>ver</th>
<th>hlen</th>
<th>TOS</th>
<th>pkt len</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>identification</td>
<td>flg</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>protocol</td>
<td>header cksum</td>
<td></td>
</tr>
</tbody>
</table>

**Source IP address**

**Destination IP address**

**Source port**

**Destination port**

**UDP length**

**UDP cksum**

**Query ID**

**0**

**Opcode**

**ATRR ACAA Z**

**rcode**

**Question count**

**Answer count**

**Authority count**

**Addl. Record count**

**DNS question or answer data**

**IP Header**

**UDP Header**

**DNS Data**
Theoretical situation:

Normal resolvers:
- Large ISP’s.
- Home users (privacy-issue).
- ‘Domainers’ (on the edge).
- Validating (or not).
- In sensor-networks (RIPE Atlas DNSmon etc.).
In reality

Malicious systems:
- Spam-runs.
- Cutwail and other spambotnets.
- DNS-amplification DDoS with *spoofed* addresses.
- Open resolvers.

But also:
- Legacy software, or poorly configured software.
- Things we do not yet fully understand.
Some examples of what we look at...

• Ratio between ANY / non-ANY queries.
• REFUSED (asking for .com for example).
• Only asking second-level.
• Triggering TC-bit (RRL truncated answers).
• Only use TCP.
• Relatively many NXDOMAIN’s.
As well as…

• Relatively many MX-queries?
• Are they large resolvers?
• Do they visit us regularly?
• Are they home-resolvers (exclude them for privacy reasons).
• Are they validating?
• Do they respect our TTL?
• Do they only use source port 53?
Etc.
Example:

| 170 | 0iil69fqh.nl | 11 |
| 171 | 7nvg0qi3767875.nl | 11 |
| 172 | 7ko183.nl | 11 |
| 173 | 7io3k704uwt12.nl | 11 |
| 174 | 0hzs32a.nl | 11 |
| 175 | 7b8pk1002221z.nl | 11 |
| 176 | 75o56a3p1.nl | 11 |
| 177 | 99u9xh6z7a2e7.nl | 11 |
| 178 | 7qzh3.nl | 11 |
| 179 | 0jse8h49oxh.nl | 11 |
| 180 | 0n5j077wso9.nl | 11 |
| 181 | 0j3qd.nl | 11 |
| 182 | 7k7zv.nl | 11 |
| 183 | 7n4dmq81111a4.nl | 11 |
| 184 | 73q42q8n.nl | 11 |
| 185 | 0k3yi8.nl | 11 |
| 186 | 77r0vvg4.nl | 11 |
| 187 | 7dt80.nl | 11 |
| 188 | 7ew5140.nl | 11 |
| 189 | 99w1cx335rp.nl | 11 |
Resolver Reputation System:

1. Eerste niveau
2. Tweede niveau
3. Titel

Resolver bij ISP

Authoritative DNS voor .nl

.nl Registry

Labs Netwerk

ResRep

Vragen en antwoorden
Example of first prototype

```sql
SELECT SUM(qps_refused) AS sum_refused
FROM 'resolvers_daily'
WHERE qps_refused = 0
AND qps_refused = qps_tot
GROUP BY ip
ORDER BY sum_refused DESC
LIMIT 0, 30
```
Looking closer

```
SELECT * FROM `resolvers_reputation` WHERE `ip` = '217.121.39.05' LIMIT 0, 30
```

![Database query result showing IP addresses with associated metadata](image)

![Ziggo logo](image)
Example of ongoing attack

```
marco@triton:/projects/resrep/attack$ sudo tshark -i eth1 host 217.121.248.251
[sudo] password for marco:
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:45: dofile has been disabled.
Running as user "root" and group "root". This could be dangerous.
```

Capturing on eth1

```
    0.000000 217.121  --> 193.
    0.000211 193.176  --> 217.12
    21.031298 193.176  --> 217.12
    46.359113 217.121  --> 193.
    46.359216 193.176  --> 217.12
    70.366468 217.121  --> 193.
    70.366575 193.176  --> 217.12
   135.462973 217.121  --> 193.
   135.464059 193.176  --> 217.12
   148.473951 217.121  --> 193.
   148.474115 193.176  --> 217.12
   169.505099 217.121  --> 193.
   169.505144 193.176  --> 217.12
   179.518297 217.121  --> 193.
   179.518310 193.176  --> 217.12
  264.763477 217.121  --> 193.
  264.763649 193.176  --> 217.12
311.015623 217.121  --> 193.
311.015694 193.176  --> 217.12
```
In retrospective

```sql
select qname from dns.packet
where src="217.121.XXX.XXX"
limit 500
```
Ultimate situation:

-Vragen en antwoorden

.nl Registry

Labs Netwerk

AbuseHUB

Authoritative DNS voor .nl

ResRep

AbuseHUB

Ziggo
What have we found so far...

• More ‘resolvers’ than anticipated (~4 million).
• ~750000 seem ‘suspicious’ (possibly only tip of the iceberg).
• Various remarkable findings.
  • botnets sending spam, DDoS-traffic, a number of unknown phenomenon's.
• Also some things we hoped for, but didn’t encounter.
Lessons learned:

• Profiling and defining ‘security metrics’ is quite complicated.
  • But can produce interesting results (needle in the haystack).

• Derived behavior, there’s a fair change of false positives.
  • Results so far are probably only complementary on other measurements, but we would like more.

• We see only systems that are contacting our DNS, obviously.
Tell me please:

• Are you involved in similar projects?
• Do you have any opinions about this project?
• Any other feedback, suggestions, proposals?
VOEG EEN FOTO IN:

1. Verwijder de bestaande foto en klik op het icoon, om een foto in te voegen:

2. Zoek de gewenste foto en dubbelklik hierop.

3. Staat de apeelding er niet goed in? Selecteer de foto, klik 'Format' in het lint en selecteer 'Crop'.

4. Als de apeelding boven het tekstvak verschijnt, kun je de slide re睡egen. Selecteer hiervoor de dia met een rechtermuisklik en selecteer 'Reset slide'.

Thank you!

Marco Davids
marco.davids@sidn.nl

@marcodavids

sidn.nl | sidnlabs.nl