Query Storm affecting .CL

Mauricio Vergara Ereche
<mave@nic.cl>
OARC/ccNSO Meeting 2011
The phenomenon seen

• Since the beginning of 2011, we've received lots of unusual traffic in our servers.
• Most of the “extra” queries follows a common pattern:
  – Ask for the MX type
  – Bit RD turned on
  – Almost every query is a NXDOMAIN
  – Transaction ID starting with 0x0 (lower than 256)
A little example (first week seen)

Queries by QType
From Jan 03, 2011, 09:11:58 To Jan 03, 2011, 10:11:58 CLST

A: 60%
MX: 15%
AAAA: 14%
ANY: 2%

A: 15%
MX: 80%
AAAA: 3%
ANY: 0.3%
A little example (first week seen)
A little example (first week seen)
But then... it started to increase
The TOP-10 hitters?

<table>
<thead>
<tr>
<th>T-10 by IP</th>
<th>T-10 by ASN</th>
<th>T-10 by country</th>
</tr>
</thead>
<tbody>
<tr>
<td>95.79.165.0</td>
<td>6849</td>
<td>UA</td>
</tr>
<tr>
<td>212.94.96.113</td>
<td>9050</td>
<td>RU</td>
</tr>
<tr>
<td>93.105.123.139</td>
<td>6697</td>
<td>RO</td>
</tr>
<tr>
<td>178.137.18.68</td>
<td>6147</td>
<td>PE</td>
</tr>
<tr>
<td>94.230.167.239</td>
<td>9198</td>
<td>IT</td>
</tr>
<tr>
<td>212.182.115.131</td>
<td>19429</td>
<td>CO</td>
</tr>
<tr>
<td>84.60.185.254</td>
<td>12715</td>
<td>ES</td>
</tr>
<tr>
<td>89.216.144.251</td>
<td>3269</td>
<td>KZ</td>
</tr>
<tr>
<td>194.44.220.206</td>
<td>16735</td>
<td>BR</td>
</tr>
<tr>
<td>193.110.165.118</td>
<td>9121</td>
<td>US</td>
</tr>
</tbody>
</table>

# of unique IPs: ~500k
(sampled over 12 hours captures on *.nic.cl servers)
Distribution
What have they been asking for

- **Ascii to hex?**
  - 01c15bb2.cl.
  - 01c2f8f1.cl.
  - 01c3318e.cl.
  - 01c34ab2.cl.
  - 01c36640.cl.
  - 01c39260.cl.

- **Malformed list?**
  - 08b.cl.
  - 08biennial.cl.
  - 08family.cl.
  - 08g.cl.
  - 08q.cl.
  - 097lider.cl.
  - 09ales.cl.
  - 09atencion.cl.
  - 09coolman.cl.
  - 09family.cl.

- **dictionary?**
  - zurih-chile.cl.
  - zurik-chile.cl.
  - zuro1999.cl.
  - zur-ofubo.cl.

- **Final users?**
  - 79-17-112.adsl.terra.cl.
  - 79-40-89.adsl.terra.cl.
  - 78-67-20-190.adsl.tie.cl.
  - xxx-23d7036f.adsl.terra.cl.
  - xxx-23dba370.adsl.terra.cl.
  - bd063ee.cpe.telmex.com.cl
  - 2005.cpe.telmex.com.cl
  - xlr9cp15q7.cpe.telmex.com.cl
  - d86dd4.cpe.telmex.com.cl
  - 32b0b9c6.cpe.telmex.com.cl
  - 2fcb5a43a79b496.cpe.telmex.com.cl
What have we done?

- Re-distribute traffic between nodes in our self-managed anycast clouds (AS-path prepending).
- Disable temporary logging on BIND servers.
- Change our last unicast to an anycast one.
- Improve our BW, QPS and conntrack monitors and alerts.
- Contact other TLDs and associates to gather more info
Things learn on the way

- International BW almost topped on main site
- iptables filter `udp/tcp 53 vs raw table`
- IDS can trigger block/stop traffic on some ISPs
- *Small packets* flood on border routers on some ISPs could do some nasty things
Some things to think about it...

• To filter packets costs more than just give the answer.
• Over provisioning is one of the keys.
• DNS service providers that rates you by per-query basis, could be extremely expensive.
• ISP contracts must be prepared to give you more BW under emergency
• This is a spam botnet? Or something else?