Impact of abuse-c

Bengt Gördén

Resilans
abuse-c

- abuse-c is a service to the end user
- Our customers should have their own abuse contact information
- In case they don't, we are the intermediate abuse-mailbox for them but the goal is to get everyone in the RIPE-db with correct abuse-c
Acceptable use policy

- Our AUP says our customers should answer within 24h upon contact from us
ABUSE POLICY

● SPAM
  - To generate or facilitate unsolicited bulk commercial email
  - To imitate, or impersonate another person or to use his, her or its email address, or to create false accounts for the purpose of sending spam
  - To engage in data mining or harvesting from websites to find email addresses
  - To send unauthorized mail via open third-party servers
  - To send emails to users who have requested to be removed from a mailing list
ABUSE POLICY

- Resilans AB further does not accept the following activities related to delegated addresses:
  - To intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature.
  - Attacks such as DDoS or other disruptive activity affecting or preventing others to use services/communications.
  - To be unreachable at your abuse-address, tech-c or admin-c. Replies must be given within 24 hours after the initial contact from us.
  - The customer must comply with Swedish law.
• We started out to implement RIPE-563 in spring 2013
• About one thousands role objects were created
• Created automatic role objects if the customer didn't reply with their own
• In late summer we started to get more and more abuse complaints
• SPAM/Viruses/DDoS/harvesting emails/.....
• Started to gather statistics from different trap-systems to see what's actually going on
Detailed statistics

- Harvesting email
- Email spam
- Dictionary attacks
- Comment spam
Lot of work to get different organizations on the Internet to use the abuse-c.

- A **lot** doesn't bother reading the reply to check abuse-c for correct info
- If they wanted a reply why do they have `<no-reply@willnotread.com>`
- A lot of those who automate check for abuse contact info can't do whois with -b
- Many have cached old abuse-maiboxes info
Worst offenders in that respect is the representatives of copyright holders

- They respond when their board of the company gets email
- They don’t change cached contact info upon request
- They sure don't know what a LIR is
Blacklists
Blacklists

- If resource holders don't respond to complaints they run the risk of ending up in a blacklist of some sort
- There are myriads of blacklists
  - 203 lists in 117 domains
- Some examples
  - blogspambl justspam spamcannibal spamcop spameatingmonkey spamgrouper spamhaus spamlab spamlookup spamrats spam-rbl spamstinks stopspam
- The most well known would be Spamhaus with Spamcop and SORBS in second place
Blacklist from Spamhaus

- XBL / SBL / PBL / DBL / ZEN
  - Exploits Block List
  - Spamhaus Block List
  - Policy Block List
  - Domain Block List
  - ZEN = All inclusive

- Different views of who to block
SBL

- Good service, if run correctly
- To get de-listed you need to send in a request for removal
- This is acted upon manually
A specific Spamhaus block

- Feb 27 2014
- Spamhaus blocked 3 /16 and 3 /19
  - Without warning us
  - Without warning our customers
- A lot of our customers ended up as collateral damage in SBL
What we tried to do

- We've asked to talk to them over the phone
- We invited them to come to us
- We're prepared to visit them
- We did ask to get a feed from them so we can be proactive
- We've asked them to come to RIPE meetings
- All of the above were turned down or ignored
- We had to wait for them to read their email from us, which they had blocked
Example

• They even copy and pasted wrong prefixes
  
  – An example: Spamhaus says that these IP-numbers were used to spam
    192.71.8.22
    192.71.8.101
    192.71.8.127
    192.71.8.137
    192.71.8.184

• “Logically” they blocked 194.71.8.0/24
Hello resilans.se Abuse Desk,
This is an automated message from the Spamhaus Block List (SBL) database to advise you that the IP below has been added to sbl.spamhaus.org:

IP/cidr: 194.71.226.0/24
Problem: Dirty block, huge ranges given to spammers
SBL Ref: SBL214437

- The City Government of Gothenburg
- 194.71.226.0/24 wasn't even routed
- Was it hijacked?
- Can't find it in any historical BGPdb (BGPlay etc.)
Is everything in SBL correct?
Check it yourself

- http://www.spamhaus.org/sbl/listings/ripe
- http://www.spamhaus.org/sbl/listings/arin
- http://www.spamhaus.org/sbl/listings/apnic
- http://www.spamhaus.org/sbl/listings/lacnic
- http://www.spamhaus.org/sbl/listings/afrinic
- http://www.spamhaus.org/sbl/listings/amazon.com
- http://www.spamhaus.org/sbl/listings/google.com
Blocked prefixes for RIR

![Graph showing blocked prefixes for RIR]
Some been there a while

<table>
<thead>
<tr>
<th>RIPE</th>
<th>ARIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  2003</td>
<td>1  2002</td>
</tr>
<tr>
<td>1  2006</td>
<td>12 2003</td>
</tr>
<tr>
<td>2  2007</td>
<td>3  2004</td>
</tr>
<tr>
<td>4  2008</td>
<td>2  2005</td>
</tr>
<tr>
<td>32 2009</td>
<td>1  2006</td>
</tr>
<tr>
<td>44 2010</td>
<td>2  2007</td>
</tr>
<tr>
<td>48 2011</td>
<td>8  2008</td>
</tr>
<tr>
<td>47 2012</td>
<td>16 2009</td>
</tr>
<tr>
<td>61 2013</td>
<td>91 2010</td>
</tr>
<tr>
<td>38 2014</td>
<td>92 2011</td>
</tr>
<tr>
<td></td>
<td>20 2012</td>
</tr>
<tr>
<td></td>
<td>116 2013</td>
</tr>
<tr>
<td></td>
<td>128 2014</td>
</tr>
</tbody>
</table>
Fight spam with DoS

- But when innocent users gets affected it's a denial of service attack
Incident reports

• We published an incident report 24h later

• Four days later Spamhaus did the same
What to do?

• We need legal certainty
  – Spamhaus tells you “you can sue as all you want, we don't care”
  – If they think your a spam haven, they don't care what your arguments are
Suggestions

• Arbitration of blocked IP resources
  – Is it possible through RIPE-NCC?
  – Swedish: The National Board for Consumer Disputes

• Make our own blacklist that operates within some European law

• Get the rest of the RIR to adopt similar solution as abuse-c
  – Is it possible?
Questions?