Regular abuse-c validation
2017-02

Hervé Clément - ORANGE
Greg Mounier - EUROPOL

WHY?

- **RIPE Community committed to improving trust and safety in the IP space**

- **Accurate and validated information in RIPE database**
  - ▸ trusted environment for network operators
  - ▸ internet troubleshooting at all levels
  - ▸ help attribute malicious activities

- **Valid contact points**
  - ▸ ensuring security and reliability of networks
  - ▸ ensuring accountability of IP resource holders
  - ▸ ensuring public can resolve abusive practices
  - ▸ ensure effectiveness of existing abuse reporting systems

How did we get there?

- **2012**: ripe-563 => mandatory "abuse-c:" contact attribute

  ‣ contact info for automatic and manual reports of abusive behaviour

  ‣ abuse-c: = part of RIPE community accountability model

- **BUT no validation mechanism** => out of date and inaccurate / no valid contact point

  ‣ Undermines the objective of ripe-563

  ‣ RIPE NCC = hundreds of reports of invalid contact information

  ‣ 2011-06 impact analysis: "data accuracy will be tackled in separate policy proposal"

- **2017**: Proposal "Regular abuse-c validation" 2017-02

  ‣ complement ripe-563

  ‣ Data accuracy issues not within the scope of ripe-563

Proposal

- **Objective:**

    ▸ increase the technical reachability of abuse-c: contact

    ▸ reduce likelihood of unresponsive abuse-c: contact

- **How?**

    1. Mandate RIPE NCC <u>to validate "abuse-mailbox"</u> at least once a year

    2. Mandate RIPE NCC <u>to follow up with resource holder</u> in case contact found invalid and resolve the issue in the <u>most flexible manner</u>.

    3. Last resort : if resource holder does not cooperate => RIPE NCC could trigger ripe-676

Responsible organisation: Orange S.A.
Abuse contact info:
gestionip.ft@orange.com

```
inetnum:          92.128.0.0 - 92.128.0.255
netname:          IP2000-ADSL-BAS
descr:            BSMSO655 Montsouris Bloc 1
country:          FR
admin-c:          WITR1-RIPE
tech-c:           WITR1-RIPE
status:           ASSIGNED PA
remarks:          for hacking, spamming or security problems send mail
to
remarks:          abuse@orange.fr
mnt-by:           FT-BRX
created:          2008-03-19T13:54:24Z
last-modified:    2015-02-06T09:29:36Z
source:           RIPE
```

5

Discussion phase

- **Too costly, too bureaucratic, too "aggressive", Too much regulation!**

- **I do what I want with my resources! De-registration is property theft!**

- **Alternative: Assisted Registry Check (ARC)?**

- **Concrete procedure?**

- **Auto-response?**

- **Legacy resource holders?**

Alternative?

- Assisted Registry Check (ARC)

  ▸ help members to strengthen registry data

  ▸ cover 4 areas:
    1. registry consistency
    2. resource consistency
    3. route/rDNS consistency
    4. resource certification (RPKI)

  ▸ ARC reviews = 25-30% of memberships / year

- ARC not designed for the validation of abuse-c: contact

Procedure

- **RIPE NCC best placed to evaluate resources required**

- **Impact Analysis in 4 weeks => detailed procedure**

- **Proposed main steps:**

  1. Validate "abuse-mailbox" at least once a year => email / human interaction

  2. If no valid response within **14 days** (including bounce back + automatic response without valid contact details) = "unresponsive" => marked " invalid"

  3. RIPE NCC engage with resource holder and require to correct the issue = dialogue

  4. **2 months** (TBC) - obvious unwillingness to cooperate and resolve the issue => trigger ripe-676 procedure

Auto-response

- "Valid" <u>IF</u> leads to human interaction to say "Hello! this email is being monitored!"

- Ticket = "valid" if leads to human interaction in 14 days.

- Form = NCC to fill the form? Form not accepted as valid response?

Legacy resource holders

- Not directly impacted

- Committed to same objective of safety, accountability and trust in IP space

Version 2.0

- Feedback from the community

- Finalise version 2.0

- RIPE NCC creates impact analysis on version 2

- Kick off the review phase

Speak out!

- **Have you ever been frustrated:**

  ‣ because no valid abuse-c: / contact details to resolve abusive practice or for troubleshooting?

  ‣ by free rider attitudes: enjoy stable environment but no clean up?

- **Do you think that this proposal is:**

  ‣ common sense?

  ‣ won't resolve everything, but is a step in the right direction?

Contribute to the conversation

send an email to <u>anti-abuse-wg@ripe.net</u>

THANK YOU

herve.clement@orange.com

gregory.mounier@europol.europa.eu