# Reporting Network Abuse and APNIC Whois Database Accuracy

Aftab A. Siddiqui

# Introduction

- The APNIC Whois Database is a publicly searchable database detailing address usage within the Asia Pacific region. The results of any search are provided purely for operational purposes (such as finding the authoritative contact for a troublesome machine)

Source: www.apnic.net[1]

# Reporting Network Abuse

**Use the APNIC Whois Database to obtain network contacts**

Å You can use the APNIC Whois Database to obtain the registration details of the IP addresses APNIC has delegated. If the those IP addresses have been further assigned to other networks, you may also see the registration details of these assignments.

Source: www.apnic.net[2]

# Reporting Network Abuse

Contact The Network

- The **admin-c**, **tech-c**, and **mnt-irt** fields contain details for the objects associated with the contact details for the network administrators responsible.
- You will find the person, role, and/or irt objects listed in the results generated.

Source: www.apnic.net[2]

# Reporting Network Abuse

- Currently many Operators, Investigator/Law Enforcement Agencies, End-User and other institutions are using whois database to fetch contact details to identify and share abuse cases and other security problems.
- Currently the growing amount of abuse reports are sent to tech-c, admin-c or mnt-irt contacts, as encouraged on the APNIC website.[2]

# Reporting Network Abuse

- Whois database data accuracy has been a big issue for years now. There have been several approaches to get better data accuracy within whois information all over the world.
- There are two main reasons for data inaccuracy in whois:

a) Wrong data is published to camouflage illegal actions.

b) b) Wrong data is published because object owners forget to update the whois information as changes occur within their organization (staff changes, etc.)

Source: prop-084 [3]

# Reporting Network Abuse

- Currently the only mechanism available is to report the invalid contact to APNIC.
- APNIC notify the member to update the record.

# Solution

- As per the ARIN Number Resource Policy Manual section 3.6.1:
  - Annual Whois POC Validation:

  During ARIN's annual Whois POC validation, an email will be sent to every POC in the Whois database. Each POC will have a maximum of 60 days to respond with an affirmative that their Whois contact information is correct and complete.

  Unresponsive POC email addresses shall be marked as such in the database. If ARIN staff deems a POC to be completely and permanently abandoned or otherwise illegitimate, the POC record shall be marked invalid. ARIN will maintain, and make readily available to the community, a current list of number resources with no valid POC; this data will be subject to the current bulk Whois policy.

# Solution

- 4342 IRT Object exist out of 4714 members.
- 4164 members created IRT object via MyAPNIC.
- During 2014 on average APNIC received around 100 invalid contact reports.

Source: APNIC Secretariat

# Solution

- In July 2010 similar to ARIN policy a proposal (prop-084) “Frequent whois information update request” was proposed by Tobias Knecht (author of IRT-Object prop).
- In August 2011 the proposal was withdrawn by the author as it did not reach consensus in the policy-sig.

# Solution?

- Is there any problem?
- Are we comfortable with Invalid object Reporting only?
- What to do with contact reported as invalid?
- Is annual contact validation a solution?
- How the process will work?
- What will be the repercussion if I don't validate my contact on time?

Thank You

# Links

1. http://www.apnic.net/apnic-info/whois_search/using-whois
2. http://www.apnic.net/apnic-info/whois_search/using-whois/abuse-and-spamming/reporting-abuse-and-spam
3. http://www.apnic.net/ data/assets/file/0006/22857/prop-084-v002.txt