# Network Abuse Handling in CNNIC and JPNIC

Terence Zhang, CNNIC

Izumi Okutani, JPNIC

# Contents

- Whois operated by NIRs
- IRT object in NIR Whois
- Network abuse handling as an NIR
- Observation from abuse handling in an NIR
- Abuse Handling in an ISP
  - Example
  - Observation
- Issues about Abuse Handling with Whois contacts
- Future Considerations

# Whois operated by NIRs

- Whois operations vary by NIRs
- CNNIC and JPNIC run our own Whois in our own languages
- We mirror with APNIC Whois to have consistent information
- Most ISPs in our economies refer to NIR Whois to view information in their own language

# IRT object in NIR Whois

- Situation varies depending on NIRs
- CNNIC WHOIS has IRT object, but it’s not mandatory
  - According to survey, most network-abuse contact is the same as tech-c
- JPNIC WHOIS doesn't have IRT object
  - Based on community's feedback
  - Our community felt more needs for correctness of POCs than creating a new object

# Network abuse handling as an NIR

- Our main role is to provide whois query services and to maintain the Whois database
- We require member organizations register valid contact details in the whois database, but we don't verify if those contact is valid
- When we receive network abuse complaints, we advice to contact POCs of upstream ISP and the network in question (in JPNIC)
  - JPNIC receive about  500 comlaints per week
  - Responds to 70-100, takes about  1.5h-2h of our HM's time per week

# Observation from abuse handling in an NIR

- People send complaints by machines, so always the same people send us e-mails, even if we advice them to contact the upstream ISP
- Some ISPs consider abuse handling as additional cost, and do not wish to register an effective POC
- Small enterprises do not have staff who can handle complaints in English
- LIRs wish to exchange POCs with each other rather than make it public privacy reasons, avoid spam

An example from JPNIC

# An Example of Abuse Handling in an ISP

- Keep whois contacts up to date, and have an agreement with their customers
  - Not to use their network service to perform abuse activities like spamming,hacking and phishing
- When they receive spamming complaint
  - they will notify the email server administrator to investigate
- When they receive complaint about phishing activities:
  - they will do some basic analysis like whois query to verify, if they confirm that's phishing, they will block the phishing server's IP, and contact the server owner to further investigate.
- When they receive complaint about hacking activities:
  - they will check their log to verify, if they confirm the hacking activity, they will block the server's IP, and contact the server owner to further investigate.

An example from an ISP in China

# Observation from abuse handling in an ISP in China

- Most organizations in China tend to strengthen their network security mechanism (software or hardware) to prevent hacking and filter spam
- Also there are widely recognized software to automatically check about phishing if you are visiting major banking or online-shopping web sites
- Hence there are not many people choose to complaint to ISP or registry about network abuse activities

Observation from an ISP in China

# Issues about Abuse Handling with Whois contacts

- Whois POCs are not always considered as an effective way for reaching an appropriate POCs in its current state

- Registering POCs generate spams for ISPs, which lowers the motivation to register effective POCs

# Future Considerations

- Is there an effective way to exchange POCs without generating spams?
  - There is a talk about privately exchanging PKIs between POCs for our major operators for IRR in Japan
  - allow LIR portable to share POC info between LIRs?
- Would co-ordination with local CERTS be useful?
  - Registries simply provides POCs and not involved in co-ordination between parties, but sometimes this is requested especially due to language problem
- Do we need a mechanism to ensure updating reachable POCs in WHOIS?
  - we do garbage collections of registered objects in JPIRR