# The Importance of WHOIS Data Accuracy

Adli Wahid

Security Specialist, APNIC

# Context

- Security Response (CERTs/CSIRTs) community perspective
- Feedback gathered from our security outreach activities (i.e. APCERT members)

# Security Incidents & Expected Actions

## Type of Security Incidents

- DDoS, Spam, Bruteforce, Scanning
- DDoS agents, compromised or infected computers
- Botnet Command & Control
- Phishing / Fraudulent sites
- Vulnerable or Exposed Systems

## Expected Actions

- Stop ongoing badness
- Take down / Remove
- Fix!
- Share information

# Whois

- Accuracy helps for a start
- Responsiveness
  - Stop / Mitigate on going attack
  - Reduce impact / exposure of incidents
  - Do not have to go through various loops & hoops
- Ideally
  - Ability to provide assistance or do something about it
- Reporting invalid contacts

# Conclusion

- Accuracy – Yes
  - But also Responsiveness
- Role of resource holders
  - Keeping contact accurate
  - Security Awareness
  - Policies & Procedures  in place
    - i.e. incident response, escalation
- Opportunity for outreach

# Thank You

Adli Wahid

adli@apnic.net

www.apnic.net/security