WHOIS ACCURACY

San Jose, Costa Rica

September 29, 2016

USES OF WHOIS

Not only RIR community, but public uses of WHOIS:

- Ensuring IP address holders worldwide are properly registered so individuals, consumers and the public are empowered to resolve abusive practices that impact safety and security
- Assuring the security and reliability of the network
- Assisting businesses, consumer groups, healthcare organizations and other organizations in combating abuse
- Assisting organizations responsible for the safety of the general public

PUBLIC SAFETY USE OF WHOIS

- WHOIS searches are **one of many tools** investigators use in addition to:
  - Routing tables/services
  - Commercially available tools
  - Internally developed tools and services

- However, WHOIS is the most common **starting point** for most investigations

ISSUE AT HAND

- **IP Address Chain of Custody Accuracy Issue**
  - Sub-allocation information of ISPs many times removed from original delegation can be inaccurate and old data
  - Each RIR tends to have different policies and requirements for what information to retain regarding sub-allocations

- **Problem expanding**
  - IPv6
  - IETF MODERN Protocol
  - IOT

- **Seeking industry solution**
  - Work with LACNIC community to for best solution

CHALLENGES

From a public safety perspective, failure to have accurate WHOIS information can present the following challenges:

- Ability of public safety agencies to quickly identify resources used in abusive activities
- Wasted network operator resources dedicated to responding to potentially misdirected legal requests
- Domain and IP address hijacking resulting in the potential use of those domain names and number resources for criminal activity

Case Examples

Chief Erick Lewis Hernández
Judicial Cyber Investigative Section
San Jose, Costa Rica

CONCLUSION

Goal: Work with all 5 RIRs on WHOIS accuracy to ISP closest to the bad actor

Other RIR efforts:

ARIN: DEA, FBI and RCMP

RIPE NCC: Europol and Spanish Guardia Civil

AfriNIC: African Union

APNIC: Sri Lanka Police

THANK YOU

Supervisory Special Agent Thomas Walden
Section Chief Technical Support Section
Office of Investigative Technology