WHOIS ACCURACY and PUBLIC SAFETY

AAWG - 26/10/2016

Gregory Mounier
Head of Outreach
European Cybercrime Centre (EC3)
EUROPOL

OBJECTIVES

- Update: Public Safety Uses of WHOIS
- Current WHOIS accuracy challenges
- Example
- Suggestions for policy proposal?

ACCESS

- Access to the RIPE Database is available to **anyone** provided the Terms and Conditions are followed (art. 2 RIPE Database Terms and Conditions).

USES

Security and reliability of the network:

- **Ensuring the uniqueness of Internet number resource usage**
- **Facilitating coordination between network operators** (network problem resolution, outage notification etc.)

Accountability :

- Providing information about the Registrant and Maintainer of Internet number resources when the resources are **suspected of being used for unlawful activities**, to parties who are authorised under the law to receive such information (art. 3 RIPE Database Terms and Conditions)

- In practice: Assisting, public safety organisations, businesses, consumer groups, individuals in **combating abuse and fraud and seeking redress.**

PUBLIC SAFETY USE OF WHOIS

- WHOIS lookups are **one of the tools** investigators use in addition to:
  - Routing tables/services
  - Commercially available tools

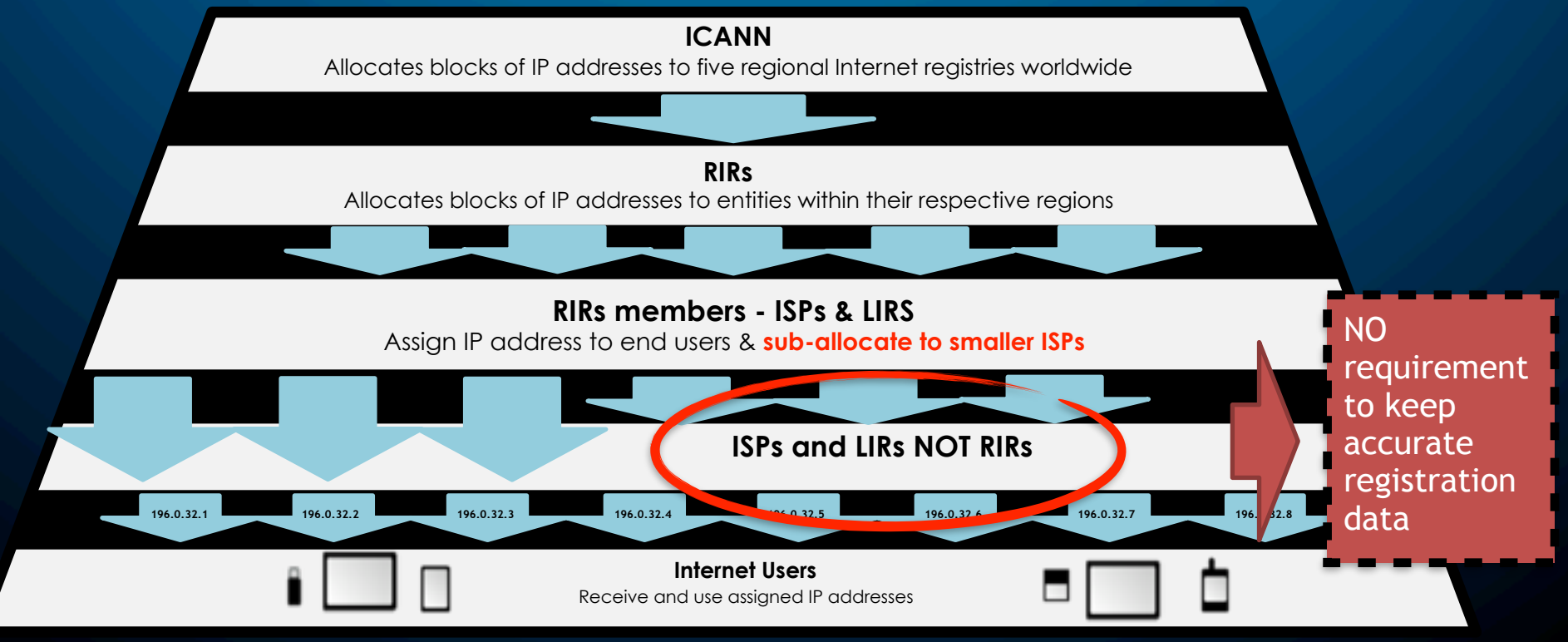
- However, WHOIS is the most common **starting point** for most investigations

PROBLEM

IP Address Chain of Custody Inaccuracy Issue:

- Sub-allocations are not properly documented -> leads to outdated data
- Each RIR tends to have different policies and requirements for what information to retain regarding sub-allocations

IP Address Chain of Custody Inaccuracy Issue



RIPE NCC POLICY FRAMEWORK

- **Section 4 of the IPv4 Address Allocation and Assignment Policies:**
  - ✓ **Registration data** (range, **contact information**, status etc.) must be correct at all time (i.e. they have to be maintained)
- **Art 6.1 of the RIPE NCC Standard Service Agreement**
  - ✓ Members acknowledge and adhere to RIPE Policy
- **Art 6.3 Standard Service Agreement: In case of non-compliance**
  - ✓ **Suspension**
  - ✓ **Deregister**

SUB-ALLOCATION

- **Section 5.4 - IPv4 Address Allocation and Assignment Policies:**
  - ✓ LIR is contractually responsible for ensuring the address space allocated to it is used in accordance with RIPE community's policies.
  - ✓ It is recommended that LIRs have contracts **requiring downstream network operators to follow the RIPE community's policies when those operators have sub-allocations.**

- **COMPLIANCE?**

CHALLENGES

- **Inability to serve legal process** to the party responsible for the resources
- **Inability to quickly identify resources** used in abusive activities
- **Waste of time of investigators and network operators:**
  - Investigators go from ISP to ISP to serve legal order
  - Network operators need to answer request for information not relevant
- **IP hijacking** resulting in those resources used for criminal activities

WHAT WE WOULD NEED

- **WHO and WHERE (ISP) to serve a legal order on?**
- **REAL ADDRESS of the last downstream provider** in allocation of a suspected IP address = ISP closest to the subject

WHAT WE DON'T WANT

- **We're not looking for end-user data, we can't get it without a warrant.**

CASE STUDY

BACKGROUND:

- Supermarket chain - IT systems compromised - 7.8 million customer details
- Network intrusion - SQL injection attack
- Log files - IP address 95.168.XXX.XX

GOAL:

- **Serve legal process on the ISP** to attribute the attack to a named subscriber
- Conduct open source research to **identify the address of the Hosting Provider**

Information on the provider in the RIPE database:

- 3 different addresses in the UK
- 1 address in Serbia
- 1 address in Belize

- 1 US phone number
- 1 Swedish phone number
- 1 UK phone number

POLICY PROPOSAL

Policy principles

- Require registration of all IP sub-allocations to downstream ISPs so entire chain of sub-allocations are accurately reflected in WHOIS
- NOT disclose end-user information but instead focus on downstream ISP providing connectivity to the end-user
- Benefits to the entire community
  - Provides both public and private sector communities with effective incident response
- Ways to ensure adherence to policy requirements
  - Incentives?
  - Compliance?

WAY FORWARD

- **Coordinated Effort with RIRs and Public Safety Organizations**
  - LACNIC: Costa Rican Police and DEA – done Sept. 2016
  - APNIC: Sri Lanka Police – done Oct. 2016
  - ARIN: DEA, RCMP and FBI – done Oct 2016
  - RIPE NCC: Europol – NOW
  - AfriNIC: Mauritius Police and African Union – to be done Dec. 2016

- **Introduce individual Policy Proposals in Spring 2017**
  - Not global policy via NRO
  - Draft with the help of all 5 RIR communities
  - Submit at RIR meetings in Spring 2017

- **Seeking industry assistance**
  - Collaborate with RIPE/RIR communities for industry-led solution
  - Task force? Brainstorming?

RIPE 73
24 - 28 OCT 2016
MADRID, SPAIN

EUROPOL

Thank you

gregory.mounier@europol.europa.eu