WHOIS Accuracy and Public Safety

Objectives

- Public Safety Uses of WHOIS
- Current WHOIS accuracy challenges
- Case examples involving inaccurate WHOIS
- Introduction of principles of a globally coordinated WHOIS accuracy policy

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 stale data
  - Each RIR tends to have different policies and requirements for what information to retain regarding sub-allocations

- **Problem expanding**
  - IPv6 – ISPs may never come back to the RIR for more space, may not register sub-allocations
  - IETF MODERN Protocol – shift to VoIP
  - IOT

- **Seeking industry solution**
  - Work with ARIN community for best solution

CHALLENGES

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

- Inability of public safety agencies to quickly identify resources used in abusive activities
- Misdirected legal requests can waste both public safety agencies' and network operator's time and resources
- IP address hijacking resulting in the potential use of those number resources for criminal activity

Case Examples

CASE EXAMPLE

- In July 2013, security organization contacted LEA reporting COMPANY A stealing IP addresses to send millions of spam emails
- COMPANY A alleged to be one of the largest spammers in history, hijacked hundreds of thousands of IP Addresses
- COMPANY A found inaccurate and outdated WHOIS information and went through a series of registration record modifications pretending to be the original registrant to start large spamming campaigns

From: CA Business Ops Manger Sent: Monday, February 11, 2013 10:25 AM ***To: CA Manager*** ***CC: CA Tech. Ops Mgr***	"Just got the logins to the domain. Working on setting everything up now. Will have an email/LOA to you soon from @surfa.net"

DEA CASE EXAMPLE

Time doesn't always amount to money, it sometimes equates to lives.

All investigations touch the internet. As stated earlier, a Whois query is most often the first step in an investigation. The following are drug overdose statistics for the past few months.

- July 27, 2016: over 200 overdoses in less than 1 month in the Akron, Ohio area.
- August 15, 2016: 27 overdoses in a 4 hour period in the Huntingdon, WV area.
- August 29, 2016: 174 overdoses over a 6 day period in the Cincinnati, Ohio area.
- October 20, 2016: nine (9) overdoes deaths this month in Delray Beach, Florida.

In these instances, public safety organizations have to work as quickly as possible to establish a pattern of life and determine the source of supply for the narcotics.

CANADIAN PERSPECTIVE

- R v. Spencer decision
- NCECC – 19,000 complaints to date this year
  - Vast majority refer to IPs sharing child pornography
  - WHOIS is the first step to find jurisdiction and where to send requests
- WHOIS is also used to search for victims - recent file had 33,000 Canadian IP addresses affected by ransomware
- In March 2016 investigation into a man extorting a young female for nude and sexualized videos
  - Took four production orders, and three months, to obtain the suspect's information
  - Three production orders would have been avoided if the WHOIS was up to date with accurate downstream ISP
  - Arrest in June 2016, but extended delay meant the suspect could continue to extort her and others

Policy Proposal

Policy Proposal 2017

- **Policy principles**
  - Require registration of all IP sub-allocations to downstream ISPs so entire chain of sub-allocations are accurately reflected in WHOIS
  - Will 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?

Way Forward

- **Globally 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 and Spanish Guardia Civil – to be done next week
  - AfriNIC: Mauritius Police and African Union – to be done Dec. 2016

- **Introduce unified Policy Proposal in Spring 2017**
  - Draft with the help of all 5 RIR communities
  - Submit at RIR meetings in Spring 2017

- **Seeking industry assistance**
  - Collaborate with ARIN/RIR communities for industry-led solution

GOALS

- Work with all 5 RIRs between now and Spring 2017 to develop community-supported WHOIS accuracy policy
- Introduce globally coordinated policy in each RIR region by Spring 2017
- Implementation by Fall 2017

THANK YOU