WHOIS ACCURACY AND PUBLIC SAFETY

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

• Public Safety Uses of WHOIS
• Current WHOIS accuracy challenges
• Case example involving inaccurate WHOIS
• Lay the ground for mutually beneficial policy on WHOIS accuracy
USES of WHOIS

Not only RIR community, but public uses of WHOIS:

• ACCOUNTABILITY: Ensuring IP address holders are properly registered so individuals, consumers and the public are empowered to resolve abusive practices that impact safety and security

• Ensuring the security and reliability of the network

• Assisting businesses, consumer groups, healthcare organizations and other organizations in combating abuse and fraud

• Finding information about potential bad actors using IP number resources

• Complying with national, civil and criminal due process laws
PUBLIC SAFETY USE OF WHOIS

• WHOIS lookups 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
THE PROBLEM

System program problem detected
Do you want to report the problem now?

Cancel  Report problem...
THE PROBLEM

• **IP Address Chain of Custody Inaccuracy Issue:**
  - Sub-allocations are not documented to the last downstream provider -> leads to inaccuracy
  - Each RIR tends to have different policies and requirements for what information to retain regarding sub-allocations

• **Problem only expanding** as IP becomes more ubiquitous in devices
  - IOT expansion
  - IPv6
  - IETF MODERN Protocol

• **Seeking industry solution**
  - Work with RIPE community for best solution
Failure to get accurate WHOIS information can present the following challenges:

- **Inability to quickly identify resources** used in abusive activities

- **Inability to serve legal process** to the party responsible for the resources - finding jurisdiction for suspects & victims

- **Waste of time of investigators and network operators**: Investigators go from ISP to ISP to serve legal notice

- **More abuse: IP hijacking**...
CASE STUDY
7.8 Million customer details
95.168.177.xx

on 8/09/16 at 02:02:58 EST
1) Perform a WHOIS lookup of 95.168.177.xx

- Inferno listed as the host
- RIPE handle MC21407-RIPE
- German address given for LEASEWEB
- Also a RIPE person object listing a UK contact
- Abuse contact for Inferno identified

RIPE record returned on a /24 Inferno CIDR
2) Query the RIPE database for John Doe & NIC MC21407-RIPE
3) Research RIPE records for Inferno (by provider name, contact and address)
Another contact and country - more contacts can be found if you keep looking...

<table>
<thead>
<tr>
<th>person:</th>
<th>Tom Smith</th>
</tr>
</thead>
<tbody>
<tr>
<td>address:</td>
<td>12 Knez Mihailova</td>
</tr>
<tr>
<td>address:</td>
<td>apt. 18</td>
</tr>
<tr>
<td>address:</td>
<td>Belgrade</td>
</tr>
<tr>
<td>address:</td>
<td>11000</td>
</tr>
<tr>
<td>address:</td>
<td>Serbia</td>
</tr>
<tr>
<td>remarks:</td>
<td>**** Inferno Solutions Customer ****</td>
</tr>
<tr>
<td>remarks:</td>
<td>Please report abuse incidents to <a href="mailto:abuse@inferno.name">abuse@inferno.name</a></td>
</tr>
<tr>
<td>remarks:</td>
<td>Messages sent to other contact addresses may not be acted upon.</td>
</tr>
<tr>
<td>phone:</td>
<td>+1 619 664 2664</td>
</tr>
<tr>
<td>e-mail:</td>
<td><a href="mailto:mail@inferno.name">mail@inferno.name</a></td>
</tr>
<tr>
<td>abuse-mailbox:</td>
<td><a href="mailto:abuse@inferno.name">abuse@inferno.name</a></td>
</tr>
<tr>
<td>nic-hdl:</td>
<td>SA4597-RIPE</td>
</tr>
<tr>
<td>mnt-by:</td>
<td>NETDIRECT-MNT</td>
</tr>
<tr>
<td>created:</td>
<td>2008-10-10T15:14:23Z</td>
</tr>
<tr>
<td>last-modified:</td>
<td>2010-04-28T09:22:05Z</td>
</tr>
<tr>
<td>source:</td>
<td>RIPE</td>
</tr>
</tbody>
</table>

RIPE Database Software Version 1.87.4
4) Identify Inferno RIPE member records for the registered address to serve legal process on

- 2 person objects
- 2 UK addresses
- 1 Serbian Address
- 1 US contact phone number
5) Research inferno.name by website and domain WHOIS records
New company name and address of 3NT listed on the website
New contact name of JOE BLOGGS (Registrant) at new UK address on the domain WHOIS
Corporate Address
DALTON HOUSE 60,
WINDSOR AVENUE,
SW19 2RR,
LONDON
United Kingdom
+442081333030

Quick Contact
Name
Email-ID
submit
Despite listing Dalton House as a 3NT listed address, they are not officially registered there.
6) Research RIPE records for JOE BLOGGS & 3NT
More company and country locations for JOE BLOGGS

Address in Belize - different company

Swedish contact number
7) New RIPE members list query using 3NT as the selector

Corporate UK name and address now identified?
8) Query Google Maps against Inferno / 3NT UK registered addresses

10 Great Russell Street is a drop address !!!
Dalton House could be a server location or another drop / false address?
9) Query UK Companies House Information for JOE BLOGGS to reveal Darl Telecom and find more company identities.

British Virgin Islands and Panama are also found in more Companies House Records attributed to JOE BLOGGS.
(sobbing hysterically)
Inferno Summary

➡ Still not 100% sure where or who to serve legal process on or the real provider name

➡ The common UK address for Inferno / 3NT is a suspected drop address (10 Great Russel St.)

➡ Multiple RIPE member records and handles act as good intelligence to give LE a lead, but...

➡ Accuracy of records is questionable and is seen across different open source entries

➡ RIPE member list records and RIPE IP object records are hard to link together

➡ Multiple company address and country registrations point to 3 different continents
CONCLUSION

• We want to work with the RIPE Community and network operators to develop a policy that would address some of these concerns.

• Mutual interest to act.

• Suggestion:
  
  ➡ Require registration of all IP sub-allocations to downstream provider so entire chain of sub-allocations are accurately reflected in WHOIS.
Thank you

gregory.mounier@europol.europa.eu