# LEA Side Event @ ICANN62

## *Internal Report*

Place: Panama City @ICANN62

Dates:

Prepared by: Carlos Martinez (carlos@lacnic.net)

# Agencies and Key People Present

*This listing may be incomplete*

- Interpol Regional Bureaus
  - Mr. Adrian Acosta (Argentina)
  - <>
- Republic of Panama Prosecutors' Office
- Crowdstrike (https://www.crowdstrike.com/)
- Shadowserver (https://www.shadowserver.org/wiki/)
- INCIBE (https://www.incibe.es/)
  - National Cybersecurity Institute, a Spanish organization co-financed by the Spanish Government and some actors from the private sector.
- LACTLD (the organization grouping most of the America's TLD operators)
- OAS (Organization of American States)
- .CO Internet (Operator of Colombia's .CO TLD)
- LACNIC
  - *Carlos Martinez*
- ICANN
  - *Carlos Alvarez*

# Agenda Overview

The program was quite long (three days!). The full agenda (in Spanish) is distributed together with this document. Worth highlighting are:

- Cooperation challenges when dealing with trans-border crime
- Dark/Deep web  and blockchain
- Three talks dealing with malicious activity in the DNS
- Two talks on threat intelligence
- Material on IPv6 introduced by LACNIC in the agenda

# General Comments

- Among the LEA officers present there was low awareness of the RIR system and the RIR's role in operating WHOIS and reverse DNS, even though they use both in their investigative work.
- Lack of adequate interpretation of WHOIS output remains an issue.
- Awareness of RDAP is still very low (only one officer attending had heard of it)
- Awareness of Bulk-WHOIS-like services is also very low.
- Several questions were received regarding what could be done to improve WHOIS accuracy.
    - In most cases, after being asked, their main complain is that their emails go unanswered. I highlighted that this doesn't necessarily mean that the registry is inaccurate but rather that the emails are received at non-monitored inboxes.
    - *Still I believe here they have a point. In fact, LACNIC has received a policy proposal asking for better abuse POC validation, which we will start implementing as soon as the Board ratifies it*
- Several questions were made regarding "*who else can we contact if the WHOIS contact does not answer emails or refuses to comply with a request for information and takedown*".
    - There was a lively debate in the room on this topic. Some of the officers present were of the idea that in this cases they would use some form of warrant against a hosting company or an ISP. Others realized that this doesn't work when you deal with cross-border incidents.
    - I suggested that contacting upstream ISPs or carriers in some cases can help "*convincing*" user or hosting site. I offered to share information regarding where to identify upstreams and how to interpret sites like http://bgp.he.net or similar.
- The IPv4 exhaustion / IPv6 talk was very well received and sparked a lot of comments and questions from the audience.
    - Many of the LEA officers present had had investigations stalled due to a suspect being hidden behind some form of carrier-grade NAT.
    - They complain that operators rarely take the time (or prefer not to) to explain why following a user behind the CGN is complex and time consuming.
    - It seems that ISPs are deploying CGNs in less than optimal ways, making an already difficult problem even harder.
- As closing remark I suggested the idea that LEAs stand to gain more if they work within the governance structures of the Internet instead of trying to fight with it. I believe this is a concept we need to point out more frequently.

# Material Presented by LACNIC

LACNIC presented a talk which highlights the challenges that the exhaustion of IPv4 poses to law enforcement agencies.

This talk gives a brief introduction to the RIR system and to how IP space is managed. It then illustrates the current crossroads most ISPs are finding themselves in, where they have to deploy CGN boxes and to decided whether to deploy IPv6 alongside said CGNs.

The need for source port logging is also highlighted. The slide deck used is distributed together with this report.