DNS Abuse and Misuse

How .CO handles it

Gonzalo Romero

CISO – .CO ccTLD

2nd LACDNS Forum

Buenos Aires, ARGENTINA, June 19th, 2.015

DNS Abuse and Misuse
How .CO handles it

- We are aware of any *threat* or *issue* which may affect the *stability*, *integrity*, *reliability*, *confidence* and *image* of the .CO *community* and *systems*
- **Security**
  - ***core*** *of .CO ccTLD business and operational strategies*
  - ***Trusted*** *community building, based on responsibility, engagement and cooperation*
- .CO ccTLD **security policies**
  - *Based on "Terms and Conditions" (Registrar channel and Registrants) and "Colombian Applicable Law"*
  - ***Rapid Domain Compliance Process (RDCP)***

DNS Abuse and Misuse
.CO Rapid Domain Compliance Process

- We **validate** "*Terms and Conditions (T&C)*" **compliance** from our ***Registrants***
- **Registry Threat Mitigation Service (RTMS)**
  - *Operational workflow for RDCP violations*
  - *"**Alerts**" management regarding .CO domains / URL's*
    - Received from **trusted** sources
    - "***Incident***" follow-up: *Registry*, *channel* and *Registrants* **joint actions** (T&C)
  - ***Scope**: phishing, pharming, malware, hacking, CP, defacements*
  - *Cases "**out of the RTMS scope**"*
    - We escalate to **Colombian ITC Ministry** and **Law Enforcement Authorities (LEA's)** for their *research* and *actions* to be done.
    - "We are **not** a **LEA** and we are very conscious of it"

DNS Abuse and Misuse
RDCP / RTMS – Learned Lessons

- After five (5) years of RTMS operations
  - *97% of alerts are "non actionable"*
    - *44% are "dead links" and 56% aren't malicious when researched*
- *We review every single alert we receive*
  - *Focusing on RDCP / RTMS incident's **scope***
  - *We only notify after exhaustive investigation*
  - *.CO "special" cases (non-RTMS-scope: rogue-pharma, piracy, spam, cybersquatting, among others)*
    - *We always escalate cases to Government (ITC Ministry) and local LEA's*
    - *Colombian LEA's: our partners in cybersecurity (collaboration)*
- *Every country has its own perspective on cyber-crime.*