Security in the .CO ccTLD

Gonzalo Romero

CSO - .CO Internet

ICANN Meeting # 48

Buenos Aires, ARGENTINA, November 17-21, 2.013

Agenda

- Motivation
- Security Policies
- Knowledge Transfer and Cooperation Action
- Malicious Activities Monitoring
- Challenges
- Q & A

Our Motivation

- As ***Administrators*** of the ".CO" ccTLD, we are committed to
  - *Protect the integrity, stability and reliability of the IT and services of the ccTLD, as well as its image and reputation worldwide*

- As an ***entity which manages Internet services***, our duties and responsibilities are
  - *Offer Quality and Value-Added services*
  - *Participate and contribute with efforts, activities and initiatives which aim to maintain the "Security, Stability and Resilience (SSR)" of the Internet global ecosystem.*

Security Policies

- Price($) = component **deterrent** to malicious/abusive/illegal domain name registrations
- Good practices on IT, Security and Business Continuity
- An innovative *Malicious Activities Monitoring (MAM)* process
  - *Security, Positioning and **Reputation** of the ccTLD (globally)*
- **Registrars** accreditation includes "*Values y Purposes*"
  - ***Security** = "Added-Value" for .CO Registrants*
- Active global, regional and in-country participation in security initiatives, projects, joint efforts and communities
- Continuous support to In-country and Regional efforts
  - *Knowledge Transfer and Security awareness*
  - *Joint IT projects and awareness campaigns with private and public entities*

Knowledge Transfer and Cooperation Action

- **CO-DNS – "Our DNS .*CO*mmunity"**
  - *"DNS Tec and Sec Day" – annual event since 2.011*
  - *Active participation and commitment with National, Regional and Global community*
    - Support and collaboration to certify national CERT's/CSIRT's to FIRST.ORG
    - Cooperate action with public and private entities
      - Colombian ITC Ministry (MinTIC), National Defense Ministry (MDN), National CERT (Col-CERT), National Police, Presidency, CSIRT-CCIT, RENATA (academic network), among others
    - Cooperation agreements and joint initiatives in cyber-security with organizations, enterprises and communities worldwide
      - Microsoft, APWG, NCMEC, DNS-OARC, RSA-AFCC, WEF, PHISHLABS, among others

Malicious Activities Monitoring (MAM)

- .CO zone permanent monitoring (DNS, URL's)
  - *Feeds provided by several (trusted) parties*
  - *Alerts to validate and research*
    - Phishing, Pharming, Malware distribution, Malicious hacking, defacements, CP
  - *NeuStar CERT: incident research and notification workflow*
  - *Work with Registrars and Registrants given a timeline (6-24h) to resolve, or risk to SH the domain*
- .CO Registrars, URL Shortener Registrants and subdomain owners
  - *Handle incident notifications based on "Terms and Conditions (TOS)"*
  - *Cooperative action*
- Special cases (CP, Rogue-Pharma, content, piracy, Spam)
  - *Forward to Colombian LEA's (under cooperation agreements) for research and actions.*

Only 4 of the 330 ccTLD's have a process like this

Security – Challenges

- Cybersquatting and Registration TOS/AOS violations/infringements:
  - *Proactive monitoring of hourly .CO domain name registrations*
  - *ccTLD Manager contacts Registrant reminding ccTLD "policies and terms":*
    - "*Registration and use of a domain name will comply with all Registry applicable policies and will not infringe on or violate the intellectual property or other rights of any 3rd party or otherwise violate applicable law*"
    - *"It's the sole responsibility of Registrant to ensure this representation and warranty is true as of the time it is made (i.e. upon registration) and continues to remain true at all times thereafter during the life of the registration"*
      - **Law-Enforcement working with ICANN accredited Registrars to strengthen Registry-Registrar Agreements**
    - *If not sure whether registration and/or use of Domain Names infringes on or violates someone else's rights, please consult with a qualified attorney*
      - **UDRP**: http://www.cointernet.co/domain/policies-procedures/dispute-resolution-co-domains
    - *Use of .CO domain names in a manner that may threaten the stability, integrity or security of the .CO registry and/or of any of our registrar partners – and/or that may put the safety and/or security of any registrant or user at risk also is strictly prohibited*
      - **RDCP**: http://www.cointernet.co/domain/global-responsibility/rapid-domain-compliance

¡Thank you!