A Multistakeholder Effort to Reduce Spam – The Case of Brazil

Dr. Cristine Hoepers
cristine@cert.br

Computer Emergency Response Team Brazil - **CERT.br**

Network Information Center Brazil - **NIC.br**
Brazilian Internet Steering Committee - **CGI.br**

Internet Governance in Brazil

The Brazilian Internet Steering Committee – CGI.br

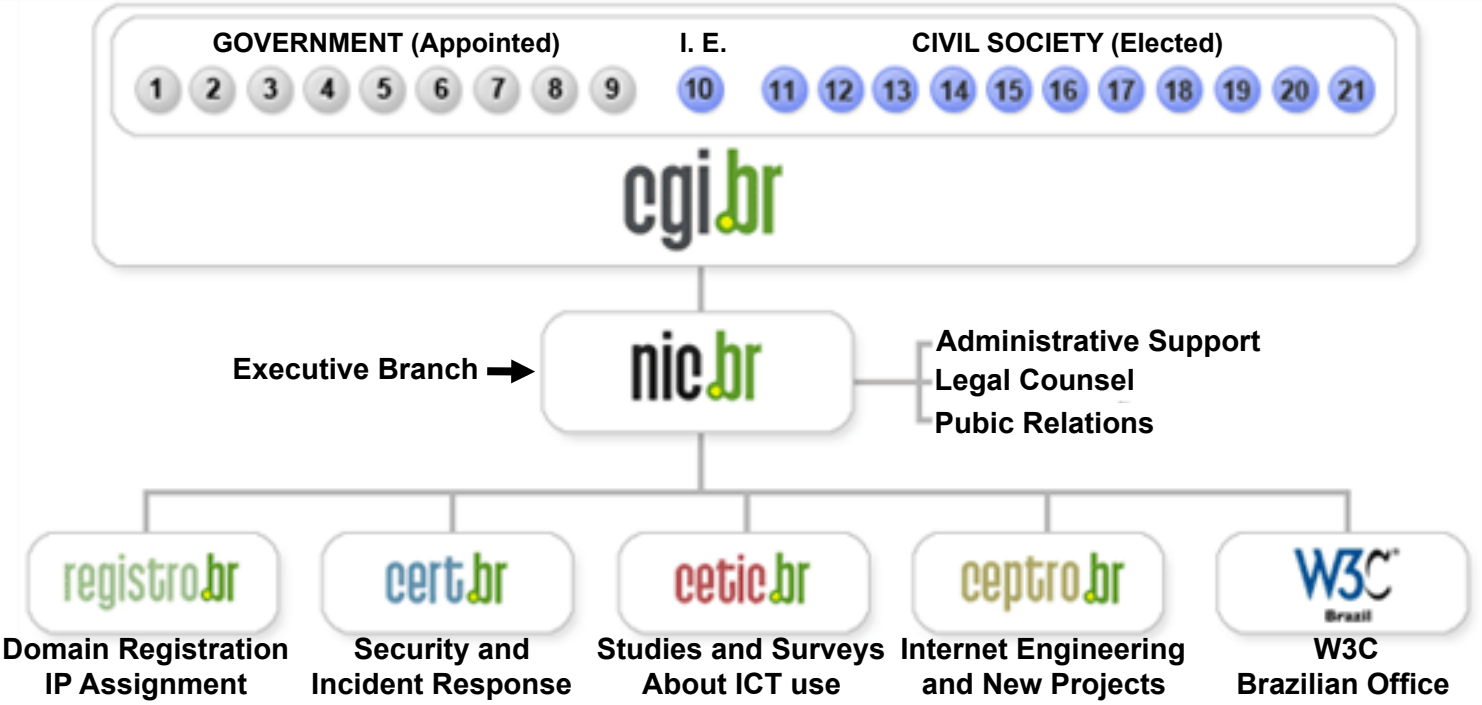
- **a multi-stakeholder organization**
- **created in 1995 to coordinate all Internet related activities in Brazil**

Among the diverse responsibilities reinforced by the Presidential Decree 4.829, it has as attribution:

- **to propose policies and procedures related to the regulation of Internet activities**
- **to recommend standards for technical and operational procedures**
- **to promote studies and recommend technical standards for the network and services' security in the country**

http://www.cgi.br/english/

CGI.br and NIC.br Structure



1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – National Forum of Estate Science and Technology Secretaries
10 – Internet Expert

11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

Anti-Spam Initiatives in Brazil – Historical Perspective

- **Early 2000's: Network operators changed contracts and established Acceptable Use Policies (AUP) forbidding spam**
  - **drastic reduction in spammers' operations in the country (that used to sell open relays and hosting services for international spammers)**
- **Mid 2000's: Brazil continually rising in the rankings of top spamming countries**
  - **needed to determine which really were the problems:**
    - **Local spammers?**
    - **Bullet proof services for international spammers?**
    - **Open relays?**
    - **Open proxies and/or infected machines (botnets/zombies)?**
    - **Bad practices of e-mail marketing?**
  - **need to involve multiple stakeholders to determine which policies and technical actions could actually be effective, depending on the problem**
- **2005: Anti-spam Task Force (CT-Spam) created by CGI.br**
  - **brought together technical community, ISPs, network operators, academia, e-mail marketing associations, legal advisors and regulators**

CT-Spam Initial Findings

- CERT.br abuse reports showed that
  - more than 80% of spam was due to open proxies (maybe botnets)
  - almost all remaining spam was direct delivery (probably botnets)
- We established the SpamPots Project and produced independent metrics about how the the Brazilian Broadband Infrastructure was being abused by spammers who used open proxies and botnets
  - result: international spammers, abusing Brazilian networks to send spams to victims in other countries
- There was a residual amount of complaints from bad e-mail marketing practices
- There were no indications of big spammers' operations inside the country anymore (hosting advertisement, selling delivery services)
- Decision was reached to start several working groups to act on each specific problem

Antispam.br Initiatives

Antispam.br is maintained by NIC.br/CGI.br, with technical coordination from CERT.br.

Main activities since 2005:

Port 25 Management working group (discussed in length in a bit)

Study on legal framework

- **evaluated bill proposals in Congress**
- **created a report with a new text of legislation proposed to Congress**

Email Marketing Self Regulation initiative (http://capem.org.br)

- **Involved ISPs, e-mail marketing associations and consumer rights organizations**
- **Builds upon the success of self regulation framework already in place for other marketing sectors (e.g. CONAR - http://www.conar.org.br)**

Best practices and awareness

- **ISPs and Telecom operators (http://www.antispam.br/admin/)**
  - **technical best practices: DKIM&SPF (DMARC), Greylisting, etc**
- **End users**

Anti-Spam and Security Awareness

Antispam.br website and cartoon videos about spam and security

http://www.antispam.br/videos/english/

"Secure Internet" Portal

- Points to all public awareness initiatives in the country

http://www.internetsegura.br/

INTERNET SEGURA.BR

Internet Security Best Practices for End Users

PT: "*Cartilha de Segurança para Internet*"
http://cartilha.cert.br/

ES: Translation in partnership with ISOC:
"*Cartilla de Seguridad para Internet*"
http://cartilla.cert.br/

- **support material for trainers and teachers**
- **booklets, stickers and slides distributed to parties interested in promoting security campaigns**

Port 25 Management Working Group

Why to create a working group as part of Antispam.br?

- **Common Goal: reduce the abuse of the Internet infrastructure in Brazil by spammers**
  - **reduce direct delivery and the abuse of open proxies**
  - **Brazilian networks were being affected negatively**
- **The adoption of port 25 management needed to be articulated among different sectors, mainly**
  - **E-mail providers needed first to move mail submission to a different port (587/TCP – RFC 6409) and migrate all users**
  - **Then Telecom companies would be able to block outgoing port 25 traffic**

Port 25 Management Working Group Members

Who was involved

- Coordinated by CGI.br – with technical coordination by CERT.br/ NIC.br
- Initial players: Telecoms, ISPs and Associations of these sectors, Anatel (Telecom regulator), the CGI.br representatives for these sectors
- Players identified in further meetings: Federal Prosecutor's Office, Consumer Defense organizations and Ministry of Justice
- A formal implementation agreement was signed
  - CGI.br, NIC.br, Anatel, Telecoms and ISP Associations
  - The consumer protection associations formally supported the agreement

Main Results

- **Port 25 management: Brazil is not listed anymore as a top source of spam on lists that keep track of direct delivery / open proxy originated spam**
- **E-mail marketing self-regulation: the board created after the code of practice was adopted is working with the major marketing companies**
- **Awareness campaigns: this is an ongoing effort, specially considering the security aspect**
- **Legislation proposals: still being discussed in Congress – the proposed text was the base for a new text now being considered**

References

- **Antispam.br – Summary of Anti-Spam Efforts in Brazil**
  http://www.antispam.br/en/

- **Internet Society Anti-Spam Technology & Issues**
  http://www.internetsociety.org/spam

- **Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction**
  http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf

- **OECD Anti-Spam Toolkit of Recommended Policies and Measures**
  http://www.oecd-ilibrary.org/science-and-technology/oecd-anti-spam-toolkit-of-recommended-policies-and-measures_9789264027176-en

- **SpamPots Project**
  http://honeytarg.cert.br/spampots/

Dr. Cristine Hoepers
<cristine@cert.br>

- **CERT.br – Computer Emergency Response Team Brazil**
  http://www.cert.br/
- **NIC.br – Brazilian Network Information Center**
  http://www.nic.br/
- **CGI.br – Brazilian Internet Steering Committee**
  http://www.cgi.br/