Port 25 Management in Brazil: A Multi-stakeholder Effort to Reduce Direct Delivery from End User Networks

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**

Agenda

Background: the Internet Governance in Brazil

The Antispam.br efforts

- **best practices, self regulation, education**

Port 25 Management

- **What is the problem being solved**
- **Specific issues for implementation in Brazil**
  - **Antispam.br Task Force work**
  - **Results**
- **Some statistics about the situation in Latin American and Caribbean Networks**

Brazilian Legal Framework

Divides the services in 2 major categories:

- Telecommunication Providers – provide the infrastructure for data networks, and this is regulated by Anatel
  - ADSL: Telefonica, Oi, GVT, Sercomtel, CTBC
  - 3G: Claro, Oi, Sercomtel, VIVO, TIM
  - Cable: NET, TVA
- Internet Service and Content Providers – provide all "value-added" services (e-mail, hosting, etc)
  - UOL, Terra, iG, Yahoo!, Gmail, Hotmail

In other words:

- Physical Layer → regulated by Anatel (Brazilian Telecommunication Regulatory Agency)
- All Internet Services (i.e. TCP/IP) → not regulated, initiatives coordinated by CGI.br – The Brazilian Internet Steering Committee

The Brazilian Internet Steering Committee – CGI.br

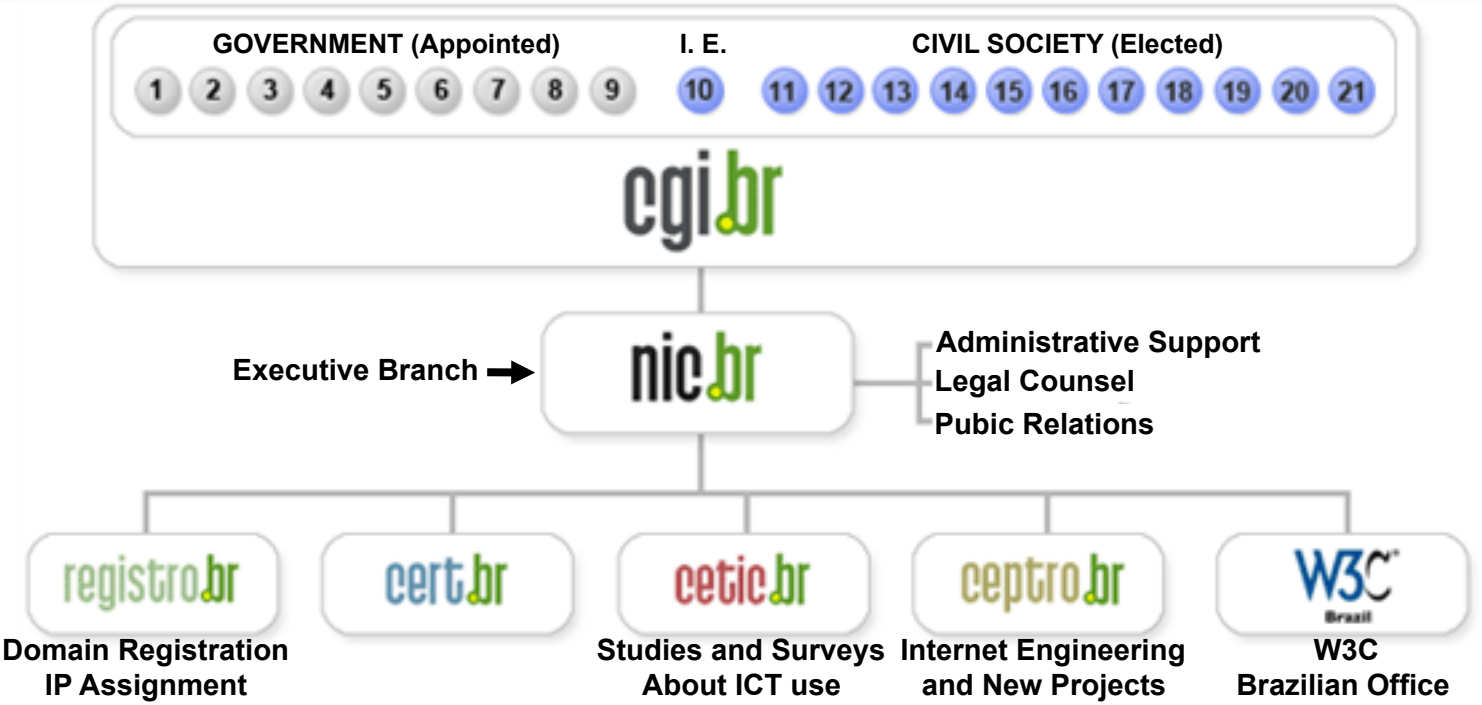
CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

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

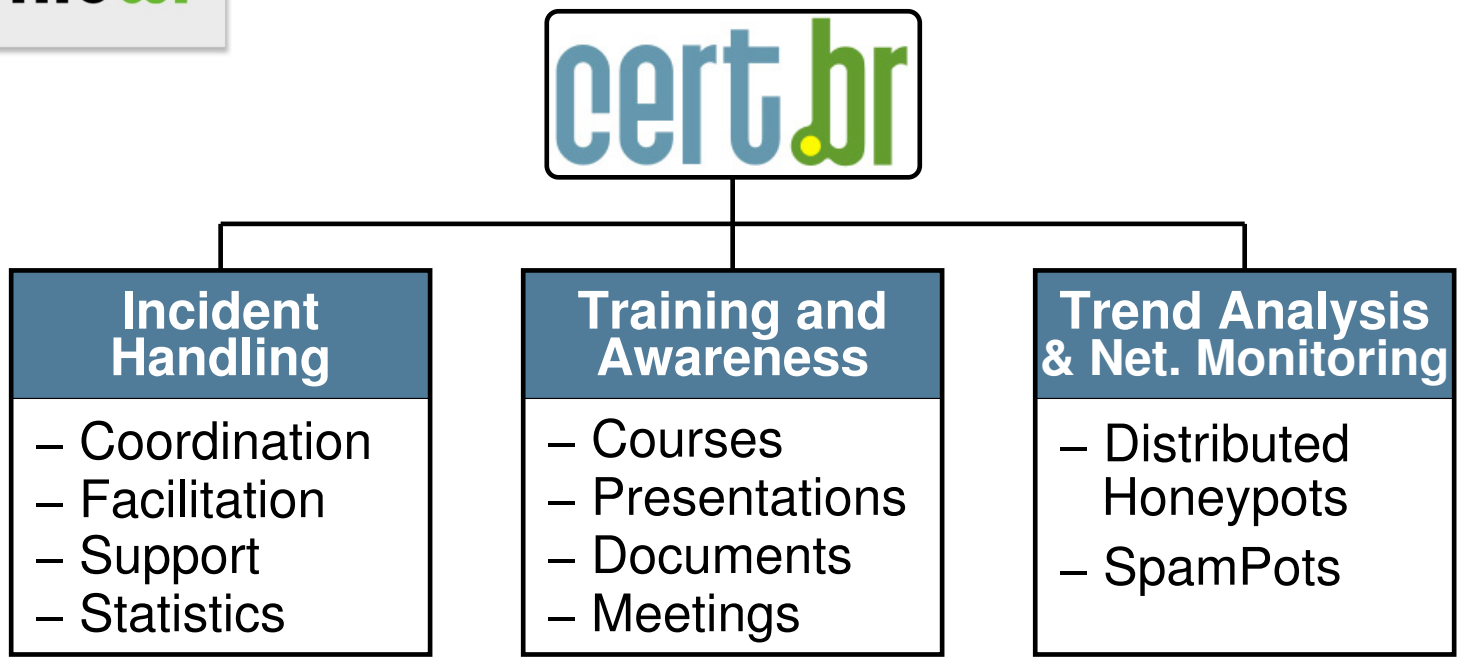
- **to propose policies and procedures related to the regulation of Internet activities**
- **to recommend standards for technical and operational procedures**
- **to establish strategic directives related to the use and development of Internet in Brazil**
- **to promote studies and recommend technical standards for the network and services' security in the country**
- **to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>**
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

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



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT

SEI Partner Carnegie Mellon

Created in 1997 to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.

- **National focal point for reporting security incidents**
- **Collect and disseminate information about threats and attack trends**
- **Increase the country's security awareness and incident handling capacity**
- **Develop collaborative relationships with other entities**
- **Help new CSIRTs to establish their activities**

http://www.cert.br/about/

Antispam.br Initiatives

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

Main activities since 2005:

Port 25 Managemet 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 (CONAR - http://www.conar.org.br)**

Best practices and awareness

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

Antispam 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 with support from 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

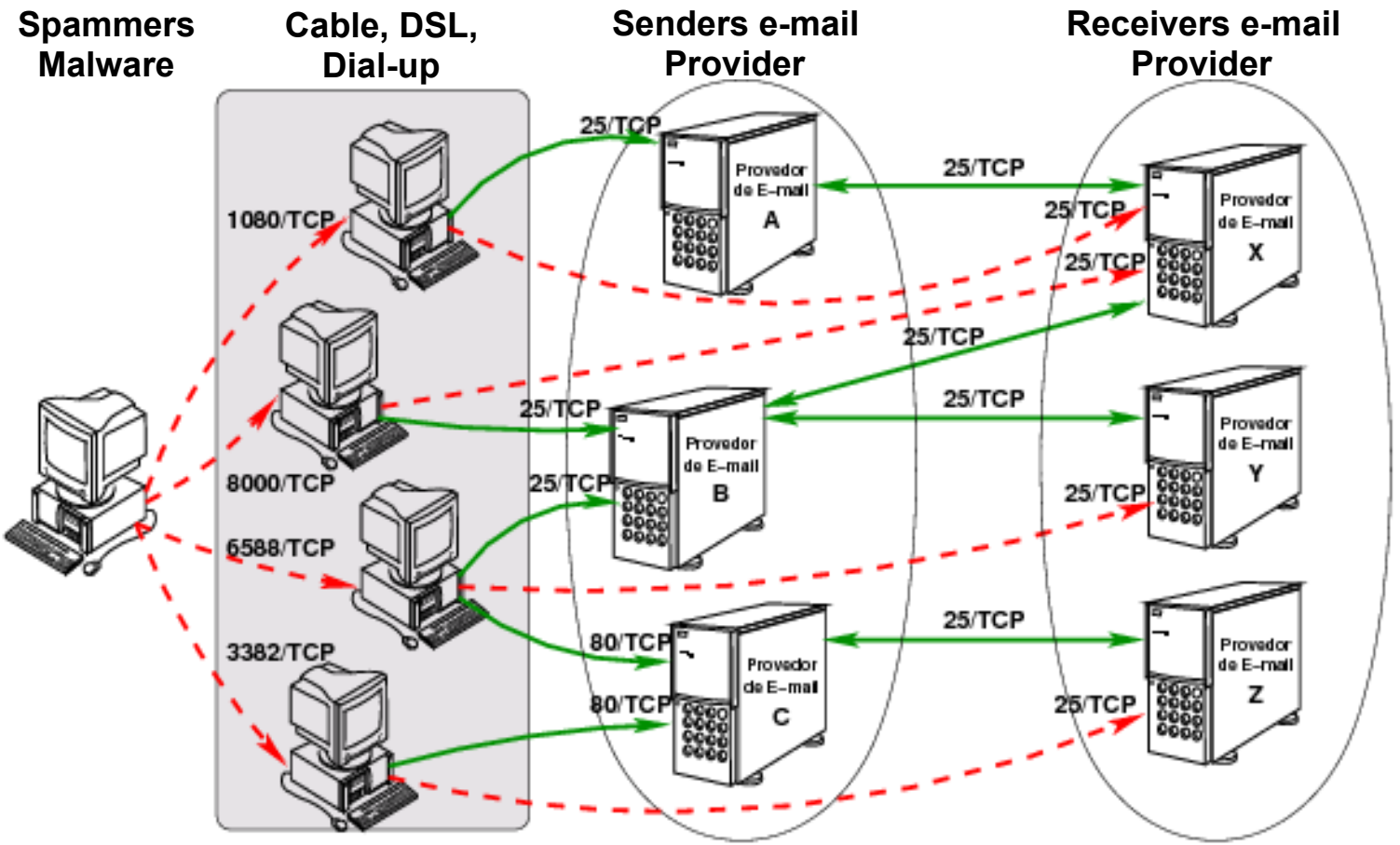
Why to create a working group as part of Antispam.br?

- **Common Goal: reduce the abuse of the Internet infrastructure in Brazil by spammers**
  - **Brazil was being appointed as a big "source" of spam**
  - **Brazilian networks were being affected negatively**
- **The adoption of port 25 management needed to be articulated among different sectors**
  - **ISPs needed first to move mail submission to a different port (587/TCP – RFC 6409) and migrate all users**
  - **Then Telcos would be able to block outgoing port 25**

What was the Problem

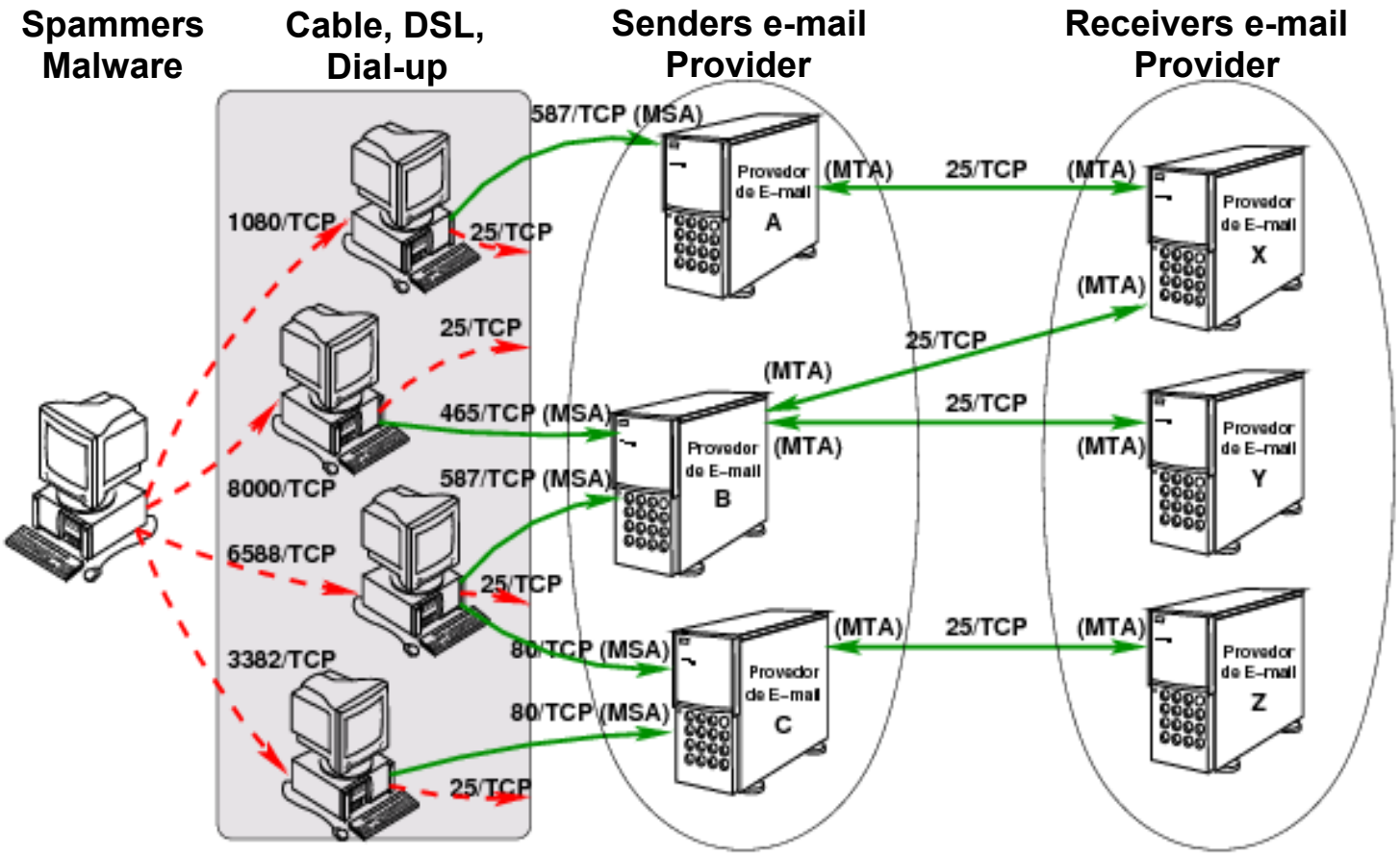
Our own studies (SpamPots Project) reinforced that:

- **more than 90% of spam leaving Brazil was originated from abroad**
- **the problem was end-user computers being abused in different ways**



What is Port 25 Management

- It is the enforcement of the differentiation between message submission and message transport
- stops direct delivery of spam by blocking outgoing connections to port 25
- must be applied only at end user networks



Port 25 Management Working Group Members

Who was involved

- Coordinated by CGI.br – with technical coordination by CERT.br/ NIC.br
- Initial players: Telcos, 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

Regular Meetings to Negotiate Port 25 Mgmt Adoption

- Agree on a coordinated effort for adoption:
  - 1st: ISPs offering Message Submission services and changing at least 90% of their clients' configuration
  - 2nd:Telcos blocking outbound port 25 traffic – residential/3G networks only
- A formal implementation agreement was signed
  - CGI.br, NIC.br, Anatel, Telcos and ISP Associations
  - The consumer protection associations supported formally the agreement
- Once the agreement was signed, NIC.br/CERT.br started a national awareness campaign about
  - the importance of these measures
  - the impact on the consumers
  - part of the Antispam.br Campaign

Campaign Main Banner

Graphic Explanations about the Change

1. Historicamente, tanto a troca de mensagens entre servidores de e-mail quanto a submissão de e-mails de clientes para o seu provedor sempre foram feitas pela porta 25. Essa característica é abusada por spammers, que usam computadores de todo o mundo se fazendo passar por servidores de e-mail.

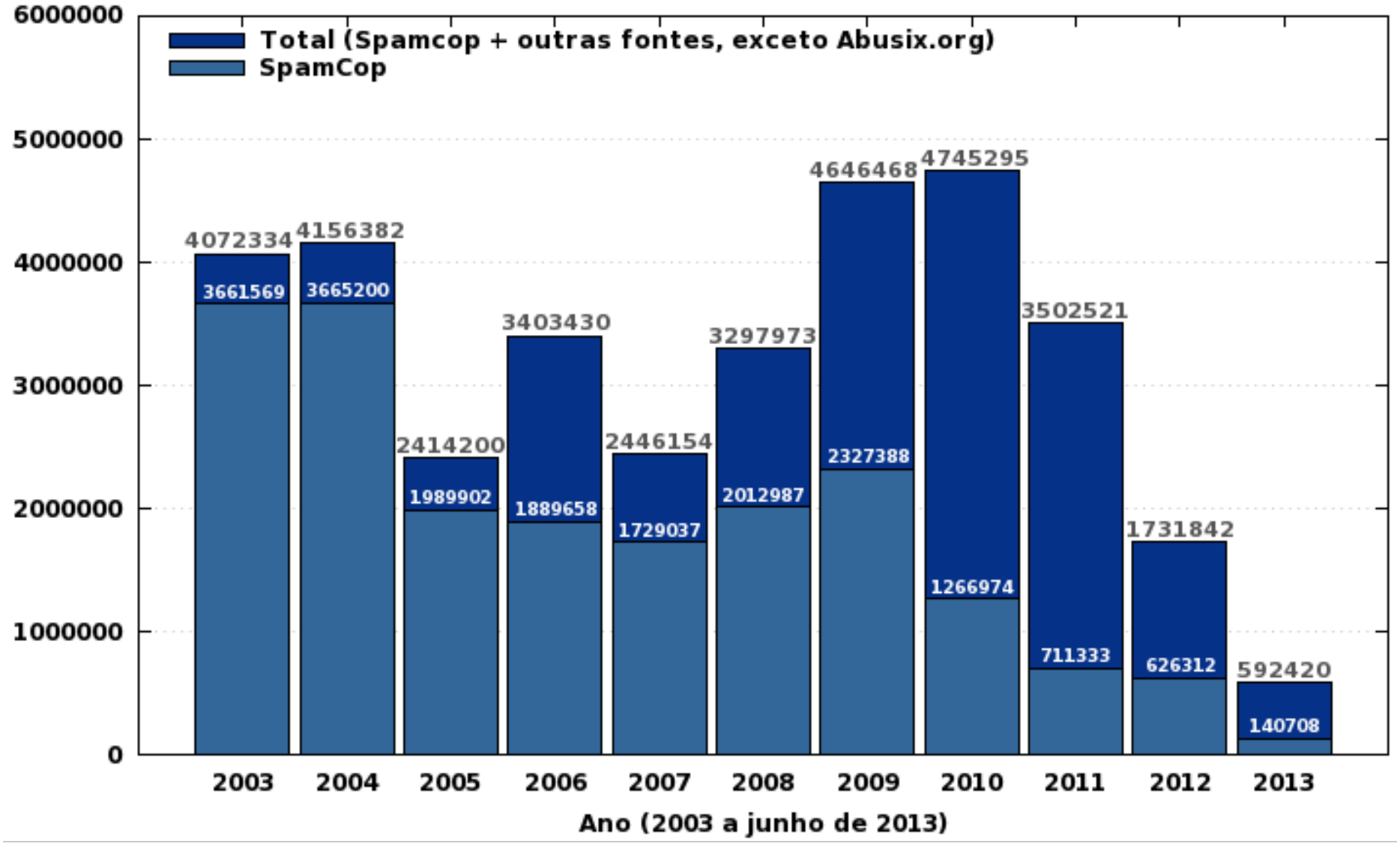
2. O Brasil tem sido classificado como um dos países com o maior número de máquinas sendo abusadas ou infectadas por códigos maliciosos que

3. Com a troca da configuração do programa cliente de e-mails para a porta 587, adotada em vários países nos últimos anos, as redes que fornecem acesso residencial podem impedir conexões com destino à porta 25, cessando o abuso sem afetar o consumidor.

4. A troca de mensagens entre servidores continua ocorrendo na porta 25.

Results

Reduction of Spam Complaints sent to CERT.br

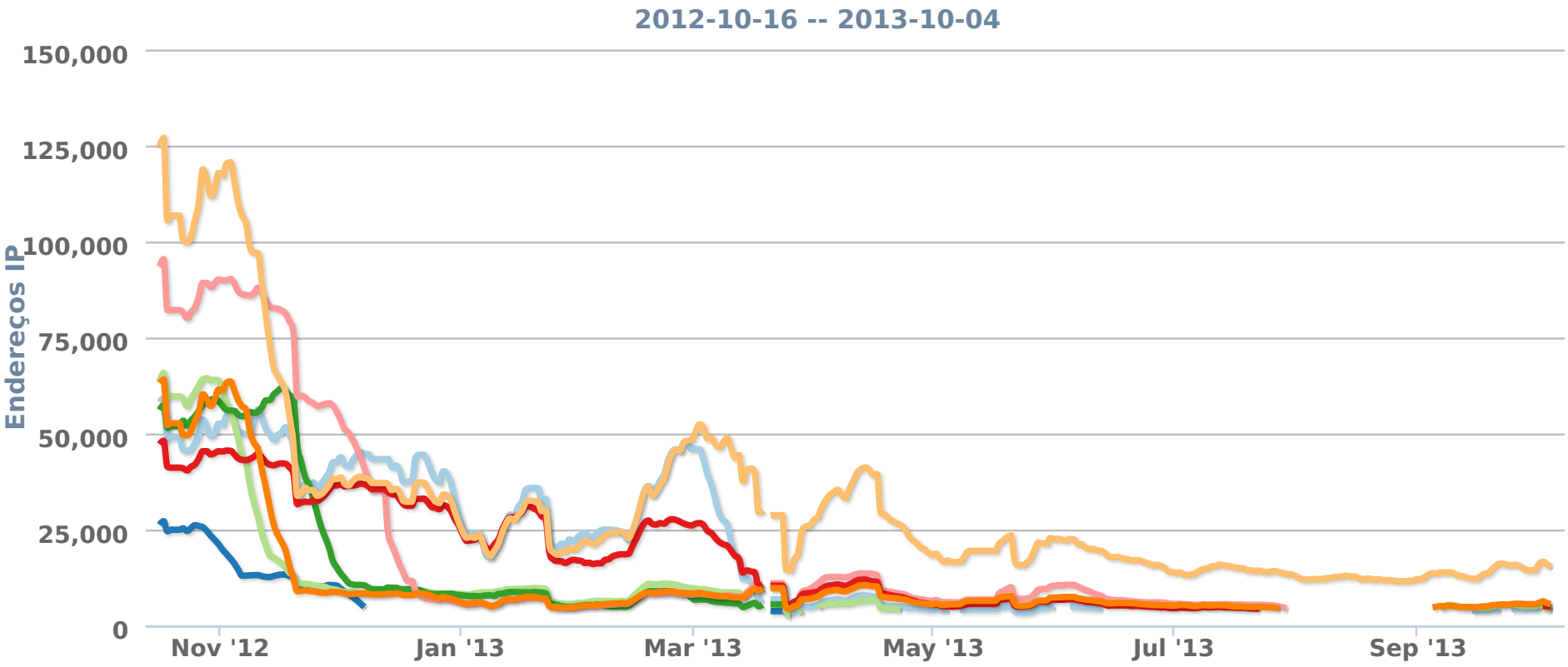


From CBL 1st in 2009 to 25th in 2013

The deadline for the implementation was March 2013

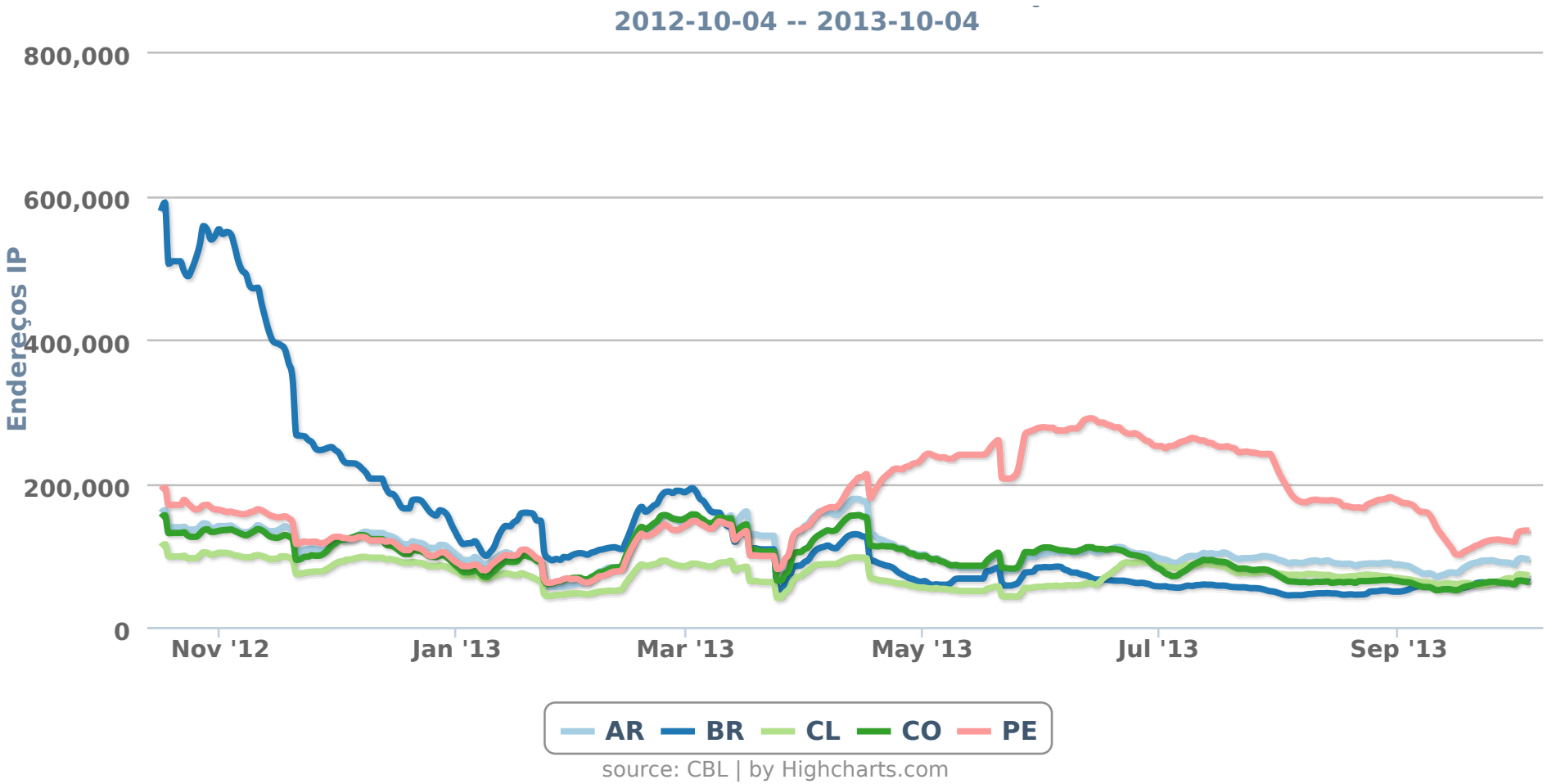
Source of data: Spamhaus CBL (Composite Blocking List) Statistics
http://cbl.abuseat.org/statistics.html

Evolution of the Main Brazilian ASNs in CBL Top 200



CBL Statistics for other LAC Countries

Comparison of the top 5 LAC Countries in CBL – by Listed IPs



Top 20 LAC in CBL – as of October 04, 2013

Rank	CC	IPs Listed	Rank	CC	%network infected
10	PE	134006	5	PE	2.29
16	AR	93836	19	BO	1.02
22	CL	71925	23	DO	0.76
24	CO	62595	29	CL	0.63
25	BR	62144	37	UY	0.47
28	MX	44842	38	GT	0.46
50	UY	16141	39	AR	0.41
54	BO	12808	41	CO	0.38
56	VE	11779	45	PR	0.28
65	DO	9255	50	HN	0.26
67	EC	7939	51	PY	0.25
71	PA	6972	48	PA	0.23
93	PY	2465	63	EC	0.21
96	PR	2100	67	SV	0.19
100	CR	1759	71	VE	0.18
105	HT	1345	79	MX	0.15
115	TT	920	101	CR	0.06
120	SV	744	102	BR	0.06
140	AN	311	104	AN	0.05
151	GY	140	110	NI	0.04

http://cbl.abuseat.org/country.html http://cbl.abuseat.org/countryinfections.html

References

- **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/
- **Antispam.br**
  http://www.antispam.br/

Questions?

Dr. Cristine Hoepers
<cristine@cert.br>

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