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

Henrique Faulhaber, Board Member
Brazilian Internet Steering Committee – CGI.br

Dr. Cristine Hoepers, General Manager
CERT.br / NIC.br

Brazilian Internet Steering Committee - **CGI.br**
Network Information Center Brazil - **NIC.br**
Computer Emergency Response Team Brazil - **CERT.br**

Agenda

Port 25 management

- What is the problem being solved
- What is port 25 management
- Major benefits

A multistakeholder initiative

- Specific issues for implementation in Brazil
- Antispam.br Task Force work

Results

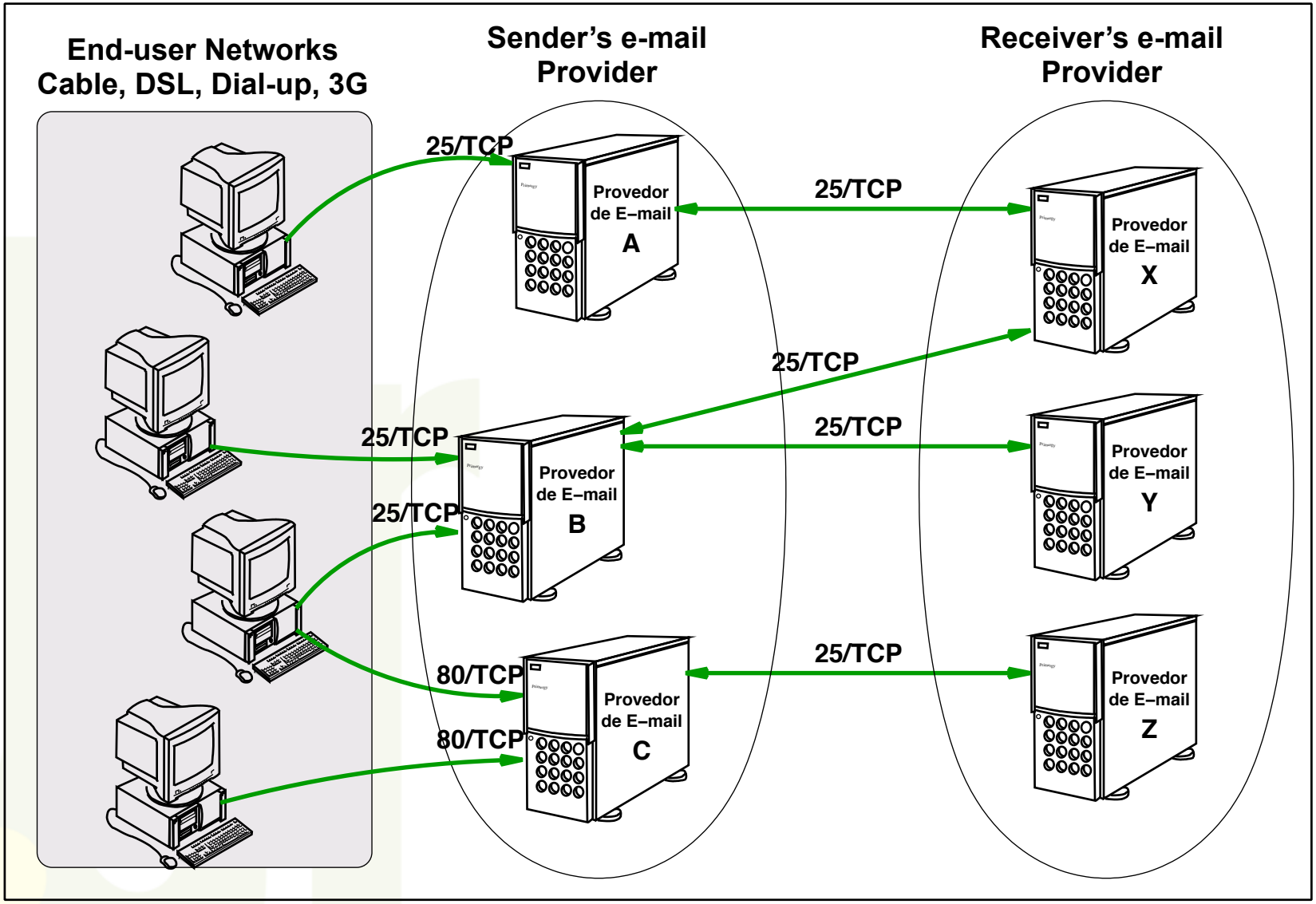
What is the Problem Port 25 Management Solves

- 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
    - used to deliver spam directly to the recipients' e-mail server
- Common Goal: to 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

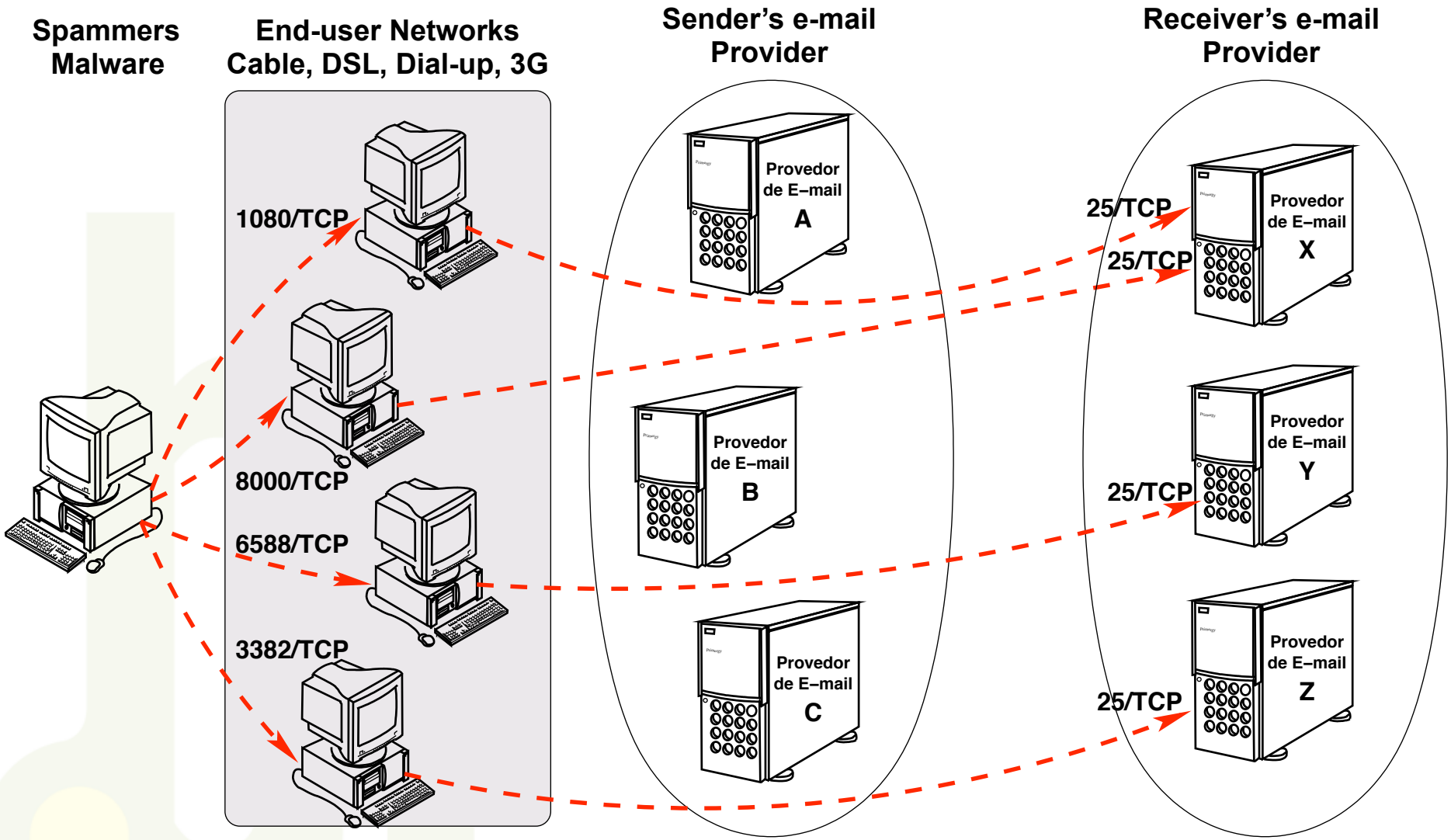
Port 25 Management in a nutshell

- 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
- In Brazil 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

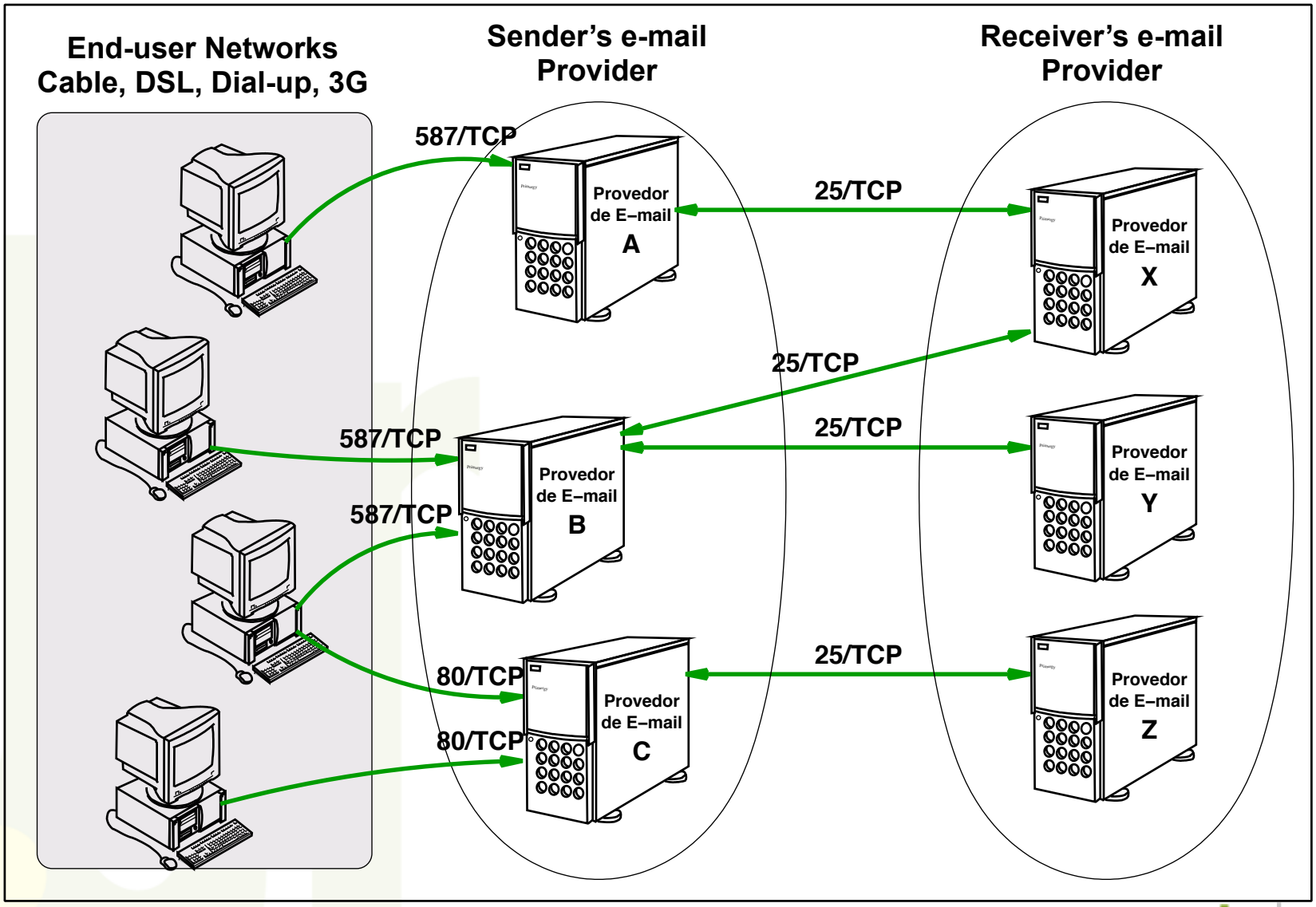
Message Submission Before Port 25 Management



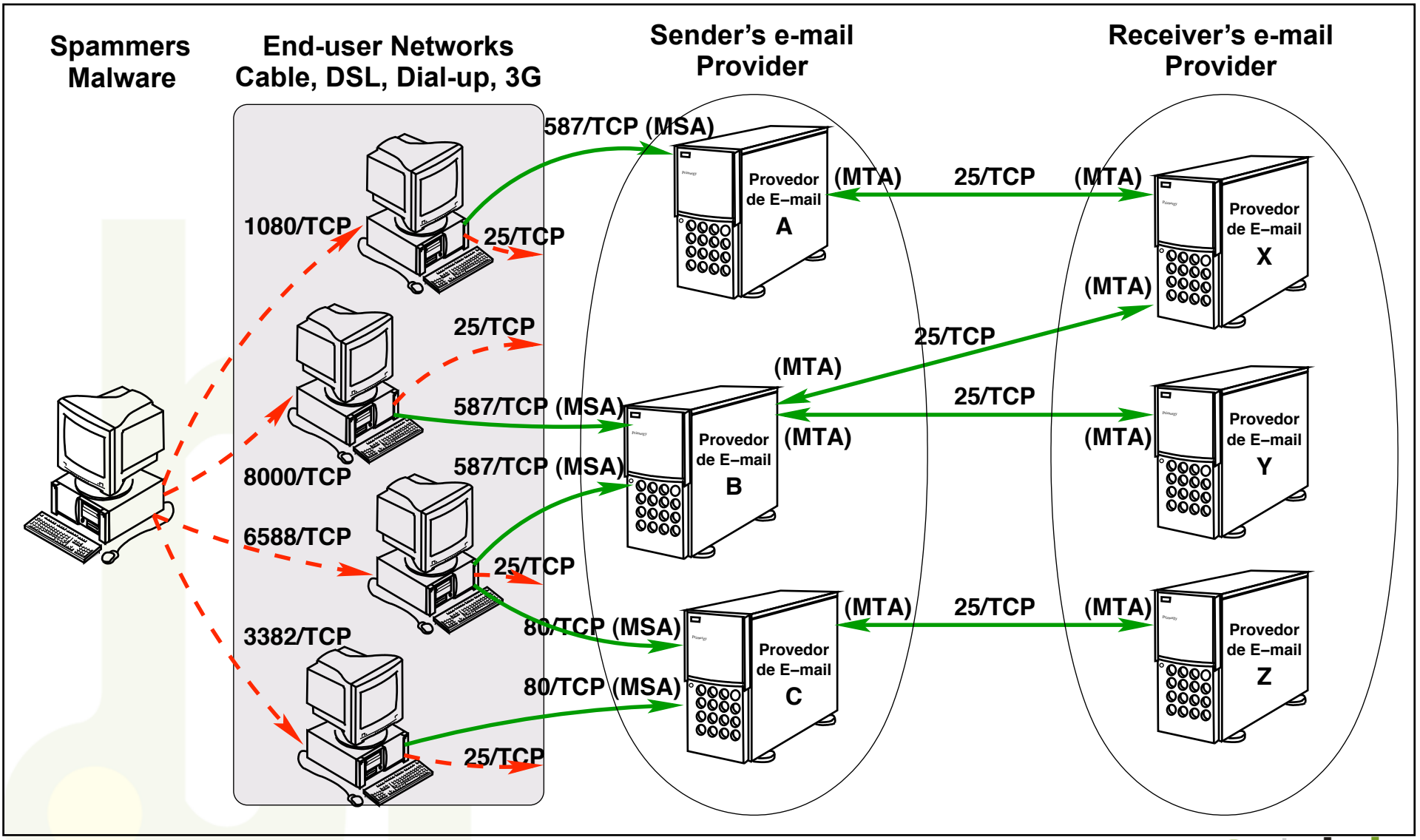
How Spammers Abuse End-user Infected Computers



Message Submission After Port 25 Management



How Port 25 Management Stops Direct Delivery



Major Benefits

- Acts before the spam enters the network
  - less effort on spam filtering and operational costs
- Decreases the number of Brazilian IP ranges in blacklists
- Makes harder the abuse of the infected computers to send phishing and malware related spams
- Reduces the “value” of the infected machines in the underground market, as it can’t be used for direct delivery

A Multistakeholder Initiative

The Brazilian Internet Steering Committee – CGI.br

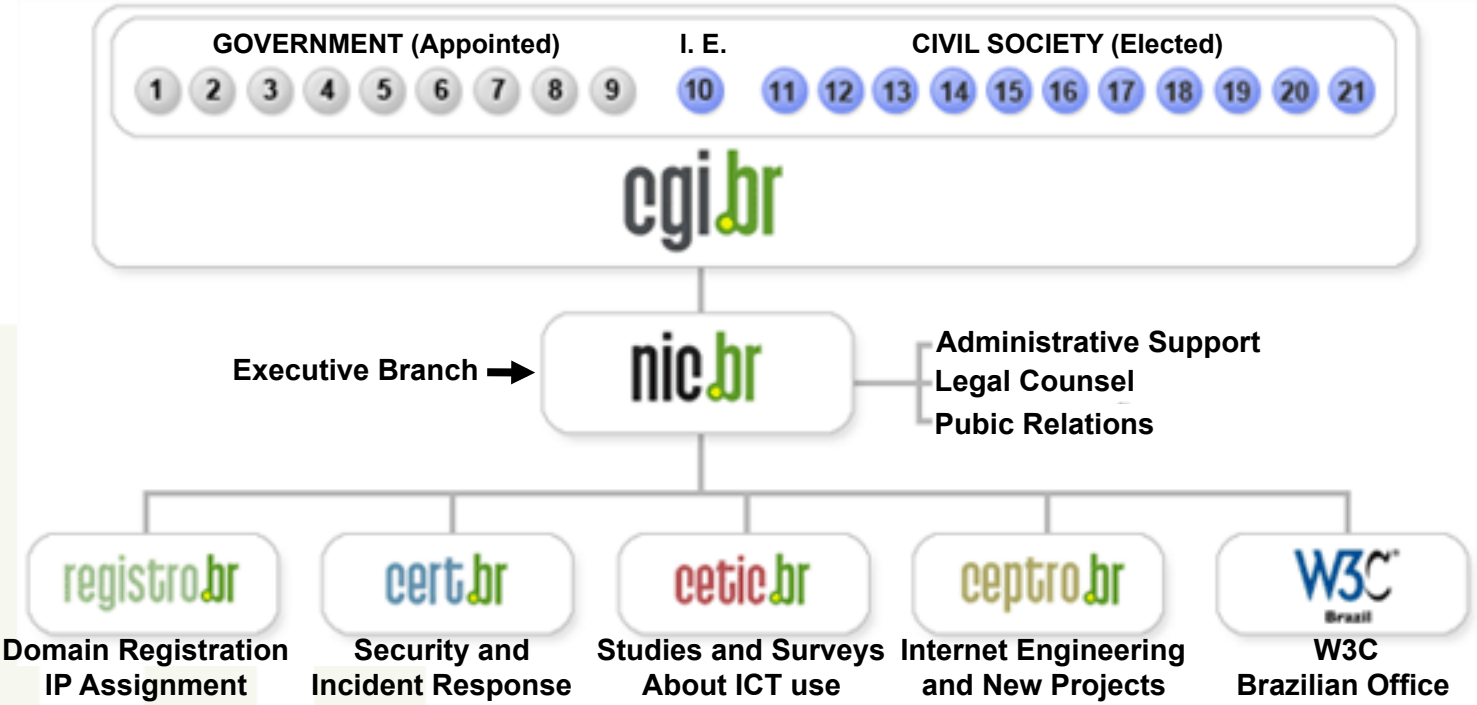
CGI.br is a multistakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

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

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 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

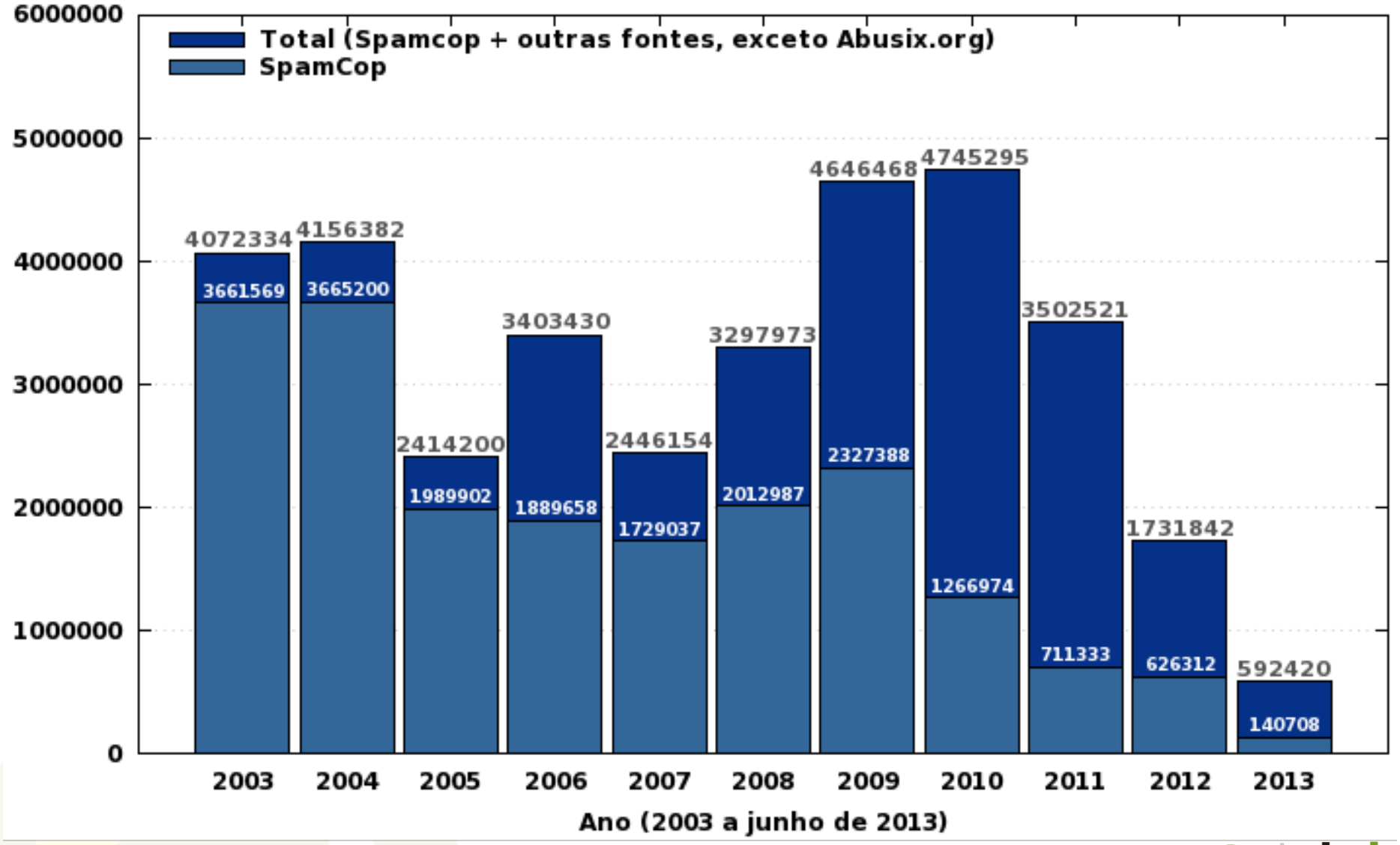
3. Com a troca da configuração do programa cliente de e-mails para a porta 587, adotada em vários países nos últimos anos, as redes que fornecem acesso residencial podem impedir conexões com destino à porta 25, cessando o abuso sem afetar o consumidor.

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

antispam.br cgi.br

Results

Reduction of Spam Complaints sent to CERT.br

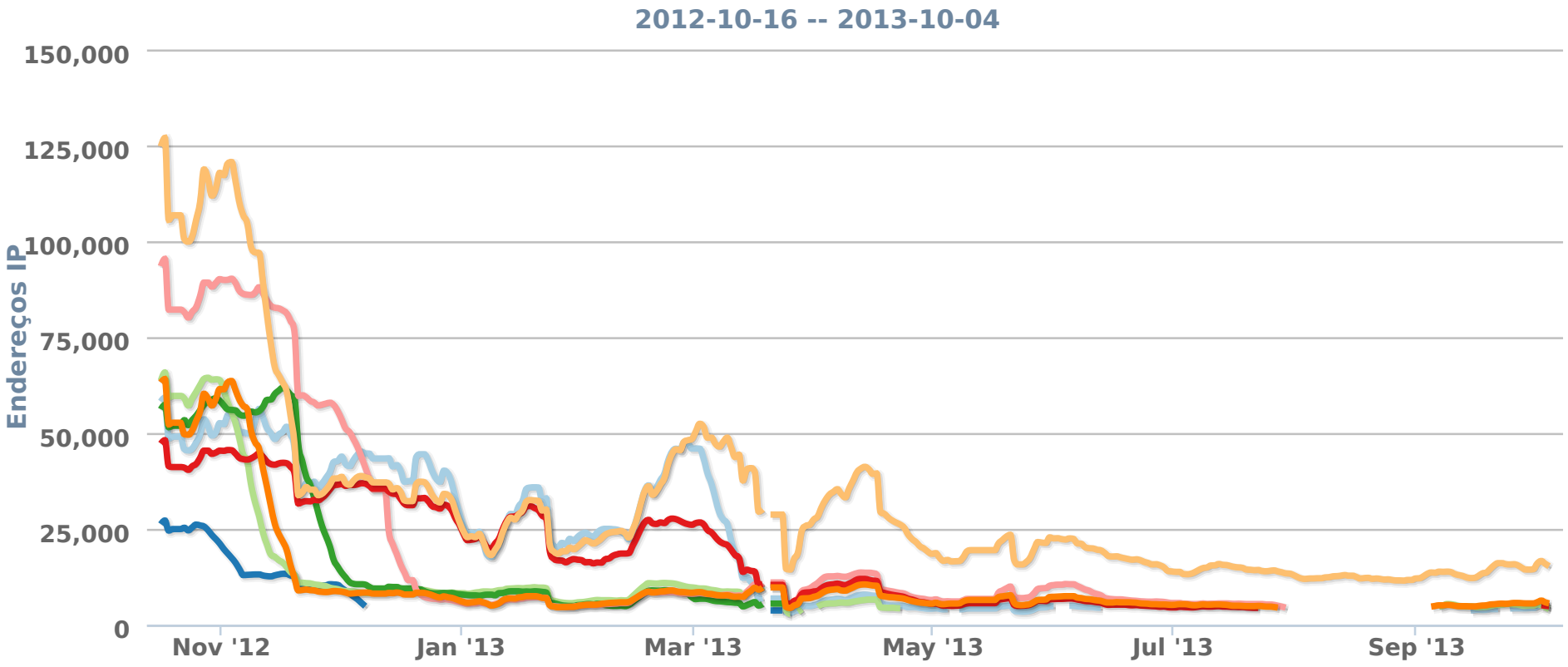


From CBL 1st in 2009 to 25th in 2013

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



References

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

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

- **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

Questions?

- **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/