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
10. Internet Expert

GOVERNMENT (Appointed)

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

CIVIL SOCIETY (Elected)

19. Academia
20. Academia
21. Academia

I. E.

Administrative Support
Legal Counsel
Public Relations

Executive Branch
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 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 (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 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:**
  - 1\(^{st}\): ISPs offering Message Submission services and changing at least 90% of their clients’ configuration
  - 2\(^{nd}\): 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
Configura a porta de envio de suas mensagens para 587!

Com a Gerência da Porta 25, o Brasil vai reduzir o volume de spams enviados em nosso país.

Você ajuda o Brasil a melhorar a Internet e ainda evita dores de cabeça.

Conheça neste site mais detalhes do Gerenciamento da Porta 25.

Afinal, quem tem que ficar de fora são os spams, e não você!
Graphic Explanations about the Change

COMO É HOJE
PARA QUEM USA LEITORES DE E-MAIL
(Outlook, Thunderbird, etc.)

1. SPAMMER
de: spammer@endereço.falso
para: vítima1@terra
vítima2@gmail
vítima3@yahoo
vítima4@uol

2. USUÁRIO COM OUTLOOK OU THUNDERBIRD
de: usuário@gmail
para: fulano@terra

REDE DA OPERADORA

INTERNET

3. YAHOO!
25

UOL
25

TERRA
25

GMAIL
25

[conta/senha]

COMO VAI FICAR
PARA QUEM USA LEITORES DE E-MAIL
(Outlook, Thunderbird, etc.)

1. SPAMMER

INTERNET

2. USUÁRIO COM OUTLOOK OU THUNDERBIRD

[conta/senha]

3. UOL
25

TERRA
25

GMAIL
25

4. TERRA
25
587

INTERNET

4. NÃO HÁ MUDANÇA NO USO DA PORTA 25 PARA COMUNICAÇÃO ENTRE SERVIDORES DE E-MAIL

Históricamente, 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.

O Brasil tem sido classificado como um dos países com o maior número de máquinas sendo abusadas ou infectadas por códigos maliciosos que queiram se passar por servidores de e-mail.

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.

A troca de mensagens entre servidores continua ocorrendo na porta 25.
Results
Reduction of Spam Complaints sent to CERT.br

<table>
<thead>
<tr>
<th>Year</th>
<th>Total (Spamcop + outras fontes, exceto Abusix.org)</th>
<th>SpamCop</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>40,723,344</td>
<td>36,615,69</td>
</tr>
<tr>
<td>2004</td>
<td>41,563,824</td>
<td>36,652,00</td>
</tr>
<tr>
<td>2005</td>
<td>24,142,003</td>
<td>19,899,02</td>
</tr>
<tr>
<td>2006</td>
<td>34,034,300</td>
<td>18,896,58</td>
</tr>
<tr>
<td>2007</td>
<td>24,461,540</td>
<td>17,290,37</td>
</tr>
<tr>
<td>2008</td>
<td>32,979,730</td>
<td>20,129,87</td>
</tr>
<tr>
<td>2009</td>
<td>46,464,680</td>
<td>23,273,88</td>
</tr>
<tr>
<td>2010</td>
<td>47,452,950</td>
<td>12,669,74</td>
</tr>
<tr>
<td>2011</td>
<td>35,025,210</td>
<td>7,113,33</td>
</tr>
<tr>
<td>2012</td>
<td>17,318,422</td>
<td>6,263,12</td>
</tr>
<tr>
<td>2013</td>
<td>5,924,200</td>
<td>1,407,08</td>
</tr>
</tbody>
</table>

Joint CITEL, ITU and the Internet Society Workshop on Combating Spam – Mendoza, Argentina, October 07, 2013
From CBL 1\textsuperscript{st} in 2009 to 25\textsuperscript{th} 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

2012-10-16 -- 2013-10-04

Endereços IP

Source: CBL | by Highcharts.com
CBL Statistics for other LAC Countries
Comparison of the top 5 LAC Countries in CBL – by Listed IPs

2012-10-04 -- 2013-10-04

source: CBL | by Highcharts.com
## Top 20 LAC in CBL – as of October 04, 2013

<table>
<thead>
<tr>
<th>Rank</th>
<th>CC</th>
<th>IPs Listed</th>
<th>%network infected</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>PE</td>
<td>134006</td>
<td>2.29</td>
</tr>
<tr>
<td>16</td>
<td>AR</td>
<td>93836</td>
<td>1.02</td>
</tr>
<tr>
<td>22</td>
<td>CL</td>
<td>71925</td>
<td>0.76</td>
</tr>
<tr>
<td>24</td>
<td>CO</td>
<td>62595</td>
<td>0.63</td>
</tr>
<tr>
<td>25</td>
<td>BR</td>
<td>62144</td>
<td>0.47</td>
</tr>
<tr>
<td>28</td>
<td>MX</td>
<td>44842</td>
<td>0.46</td>
</tr>
<tr>
<td>50</td>
<td>UY</td>
<td>16141</td>
<td>0.38</td>
</tr>
<tr>
<td>54</td>
<td>BO</td>
<td>12808</td>
<td>0.28</td>
</tr>
<tr>
<td>56</td>
<td>VE</td>
<td>11779</td>
<td>0.26</td>
</tr>
<tr>
<td>65</td>
<td>DO</td>
<td>9255</td>
<td>0.25</td>
</tr>
<tr>
<td>67</td>
<td>EC</td>
<td>7939</td>
<td>0.23</td>
</tr>
<tr>
<td>71</td>
<td>PA</td>
<td>6972</td>
<td>0.21</td>
</tr>
<tr>
<td>93</td>
<td>PY</td>
<td>2465</td>
<td>0.19</td>
</tr>
<tr>
<td>96</td>
<td>PR</td>
<td>2100</td>
<td>0.18</td>
</tr>
<tr>
<td>100</td>
<td>CR</td>
<td>1759</td>
<td>0.15</td>
</tr>
<tr>
<td>105</td>
<td>HT</td>
<td>1345</td>
<td>0.15</td>
</tr>
<tr>
<td>115</td>
<td>TT</td>
<td>920</td>
<td>0.06</td>
</tr>
<tr>
<td>120</td>
<td>SV</td>
<td>744</td>
<td>0.06</td>
</tr>
<tr>
<td>140</td>
<td>AN</td>
<td>311</td>
<td>0.05</td>
</tr>
<tr>
<td>151</td>
<td>GY</td>
<td>140</td>
<td>0.04</td>
</tr>
</tbody>
</table>

[http://cbl.abuseat.org/country.html](http://cbl.abuseat.org/country.html)  
[http://cbl.abuseat.org/countryinfections.html](http://cbl.abuseat.org/countryinfections.html)
References

- Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction

- OECD Anti-Spam Toolkit of Recommended Policies and Measures

- 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/"