GFCE Triple-I Capacity Building | The Internet Infrastructure Security Day
La Paz, BO | August 5, 2019
National Program
“For a More Secure Internet”

Lucimara Desiderá, M.Sc.
Security Analyst
lucimara@cert.br
As established by the presidential decree Nº 4.829, 03/09/2003

9 representatives from the Government
- Ministry of Science, Technology and Innovation (coordination)
- Ministry of Communications
- Presidential Cabinet
- Ministry of Defense
- Ministry of Development, Industry and Foreign Trade
- Ministry of Planning, Budget and Management
- National Telecommunication Agency
- National Council for Scientific and Technological Development
- National Council of State Secretariats for Science, Technology and Information

12 representatives from private sector & civil society
- Private Sector (4)
  - Internet access and content providers
  - Telecommunication infrastructure providers
  - Hardware, telecommunication and software industries
  - Enterprises that use the Internet
- Civil Society (4)
  - Scientific and technological community (3)
  - Internet Expert (1)
NIC.br: Not for profit organization that implements all services and decisions of CGI.br.

CGI.br members and former members (only the current members have right to vote) → GENERAL ASSEMBLY

7 members elected by the General Assembly → ADMINISTRATIVE COUNCIL

ADMINISTRATION
LEGAL
COMMUNICATION
ADVISORIES: CGI.br and PRESIDENT

EXECUTIVE BOARD

1 Chief Executive Officer
2 Administrative and Financial Director
3 IT and Services Director
4 Director of Special Projects and Development
5 Consulting Director for CGI.br activities

AUDIT COMMITTEE

registr obr
Security and Incident Response
Studies and Surveys About ICT use
Internet Engineering and New Projects
Web Technologies
Traffic Exchange
Web Standards
Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Focus of the Activities

- National focal point for security incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase the capacity of incident detection, event correlation and trend analysis in the country
- Transfer the acquired knowledge through courses, best practices and awareness materials

Creation:

August/1996: report with a proposed model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br

June/1997: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office) based on the report’s recommendations

1https://www.nic.br/grupo/historico-gts.htm | 2https://www.nic.br/pagina/gts/157
Incidents Reported to CERT.br: DDoS notifications – history

<table>
<thead>
<tr>
<th>Year</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>158,407</td>
</tr>
<tr>
<td>2017</td>
<td>220,188</td>
</tr>
<tr>
<td>2016</td>
<td>60,432</td>
</tr>
<tr>
<td>2015</td>
<td>25,360</td>
</tr>
<tr>
<td>2014</td>
<td>223,935</td>
</tr>
<tr>
<td>2013</td>
<td>1,030</td>
</tr>
<tr>
<td>2012</td>
<td>309</td>
</tr>
<tr>
<td>2011</td>
<td>272</td>
</tr>
<tr>
<td>2010</td>
<td>198</td>
</tr>
<tr>
<td>2009</td>
<td>896</td>
</tr>
<tr>
<td>2008</td>
<td>327</td>
</tr>
<tr>
<td>2007</td>
<td>954</td>
</tr>
<tr>
<td>2006</td>
<td>277</td>
</tr>
<tr>
<td>2005</td>
<td>96</td>
</tr>
<tr>
<td>2004</td>
<td>104</td>
</tr>
<tr>
<td>2003</td>
<td>50</td>
</tr>
<tr>
<td>2002</td>
<td>62</td>
</tr>
<tr>
<td>2001</td>
<td>26</td>
</tr>
<tr>
<td>2000</td>
<td>159</td>
</tr>
<tr>
<td>1999</td>
<td>21</td>
</tr>
</tbody>
</table>
Brazilian ISPs Ecosystem

Cetic.br National ISPs Survey
- Total ISPs (estimated): 6618
- Respondents: 2177
- 75% have 1000 clients or less

https://www.cetic.br/pesquisa/provedores/

IX.br SP
One of the biggest in the world
- #1 in participants (1467)
- #3 in traffic – both average (3.5T) and peak (5.1T)

https://www.pch.net/ixp/dir

≈700 ASes use MikroTik as core router

LACNIC ASN Allocation Stats

http://www.lacnic.net/en/web/lacnic/estadisticas-asignacion
We need a healthier ecosystem:
**National Initiative – A More Secure Internet Program**

**Objectives:**

- Reduce Denial of Service attacks originating in Brazilian networks
- Reduce the Prefix Hijacking, Route Leak, and IP Spoofing
- Reduce the vulnerabilities and configuration failures in network elements
- Create a culture of security

**Incentive to adopt best practices:**

- Hardening
- Close open services
- Routing Security
- Anti-spoofing (BCP 38)

**Joint initiative:**

- NIC.br/CGI.br, ISOC and ISPs, Hosting and Telco Associations

https://bcp.nic.br/i+seg
A More Secure Internet Program: Early Results – Reducing Open Services

Focusing more on the top 5:
- The top 1 (SNMP) reduced from 500K IPs to 100K
  - most in the big Telcos
- Ubiquity devices became abused recently
  - mostly on small ISPs

Common denominator in most of them:
- They are low cost CPEs (home routers)
- with bad factory defaults and do not allow changes most of the time
A More Secure Internet Program:
Early Results – Antispoofing (BCP 38) Implementation

- Higher adoption than in other countries
- Noted by CAIDA Spoof Project

Matthew Luckie mjl at caida.org
Mon May 13 23:01:57 -03 2019

- Previous message (by thread): [GTER] Governança de Internet - SSIG 2019 - Ao vivo
- Next message (by thread): [GTER] BCP38 deployment in Brazil
- Messages sorted by: [date] [thread] [subject] [author]

Hi,

I am wondering if you can help me understand why it is that Brazil, as a country, seems to be active in deploying BCP38. When I look at the monthly reports that CAIDA's Spoof Project sends to GTER, there are often 5-6 networks that have deployed BCP38 in the past month. This is more than in other countries / regions.

https://eng.registro.br/pipermail/gter/2019-May/076685.html
Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Work developed by the LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

Joint Publication of
- M³AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editor: Lucimara, LAC-AAWG Chair / CERT.br

Currently available in:
- English, Japanese and Korean

New translations to be released soon:
- Portuguese, Spanish, French and German

www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP
Gracias!
Thank You!

www.cert.br

@ lucimara@cert.br  @certbr

August 5, 2019