nic.br cgi.br | cert.br

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

cert.br nic.br cgi.br

CGI.br Members

As established by the presidential decree Nº 4.829, 03/09/2003

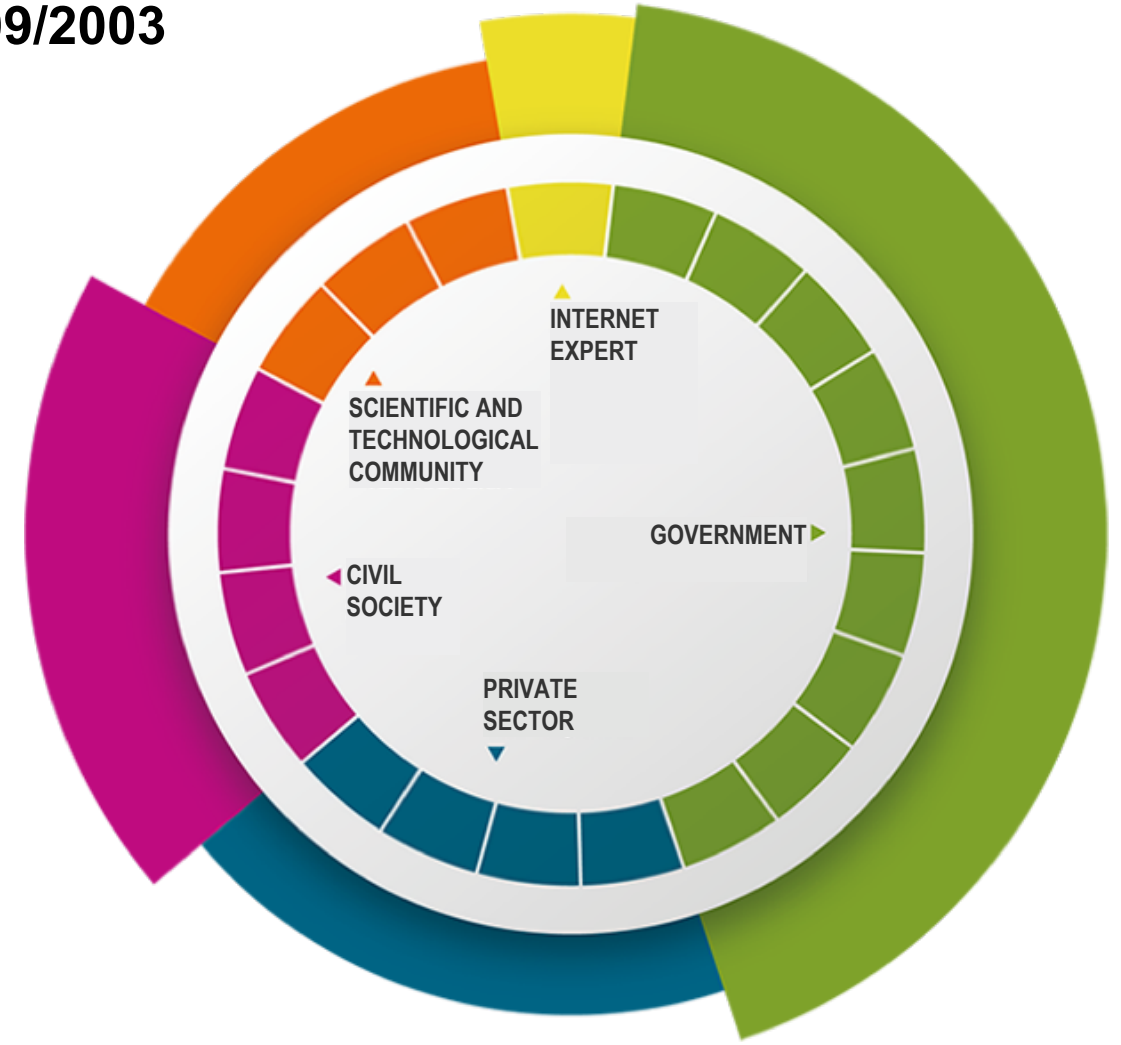
9 representatives from the Government

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)



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

AUDIT COMMITTEE

ADMINISTRATION

LEGAL

COMUNICATION

ADVISORIES:
CGI.br and PRESIDENT

EXECUTIVE BOARD

1 2 3 4 5

registro.br	cert.br	cetic.br	ceptro.br	ceweb.br	ix.br	W3C Brasil
Domain Registration IP Assignment	Security and Incident Response	Studies and Surveys About ICT use	Internet Engineering and New Projects	Web Technologies	Traffic Exchange	Web Standards

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

NIC.br:

Not for profit organization that implements all services and decisions of CGI.br.

cert.br

Incident Management	Training and Awareness	Trend Analysis
Coordination	Courses	Distributed Honeypots
Technical Analysis	Presentations	SpamPots
Support for recovery	Best Practices	Processing of threat feeds
	Meetings	

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Network

The Honeynet PROJECT

Creation:

August/1996: report with a proposed model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

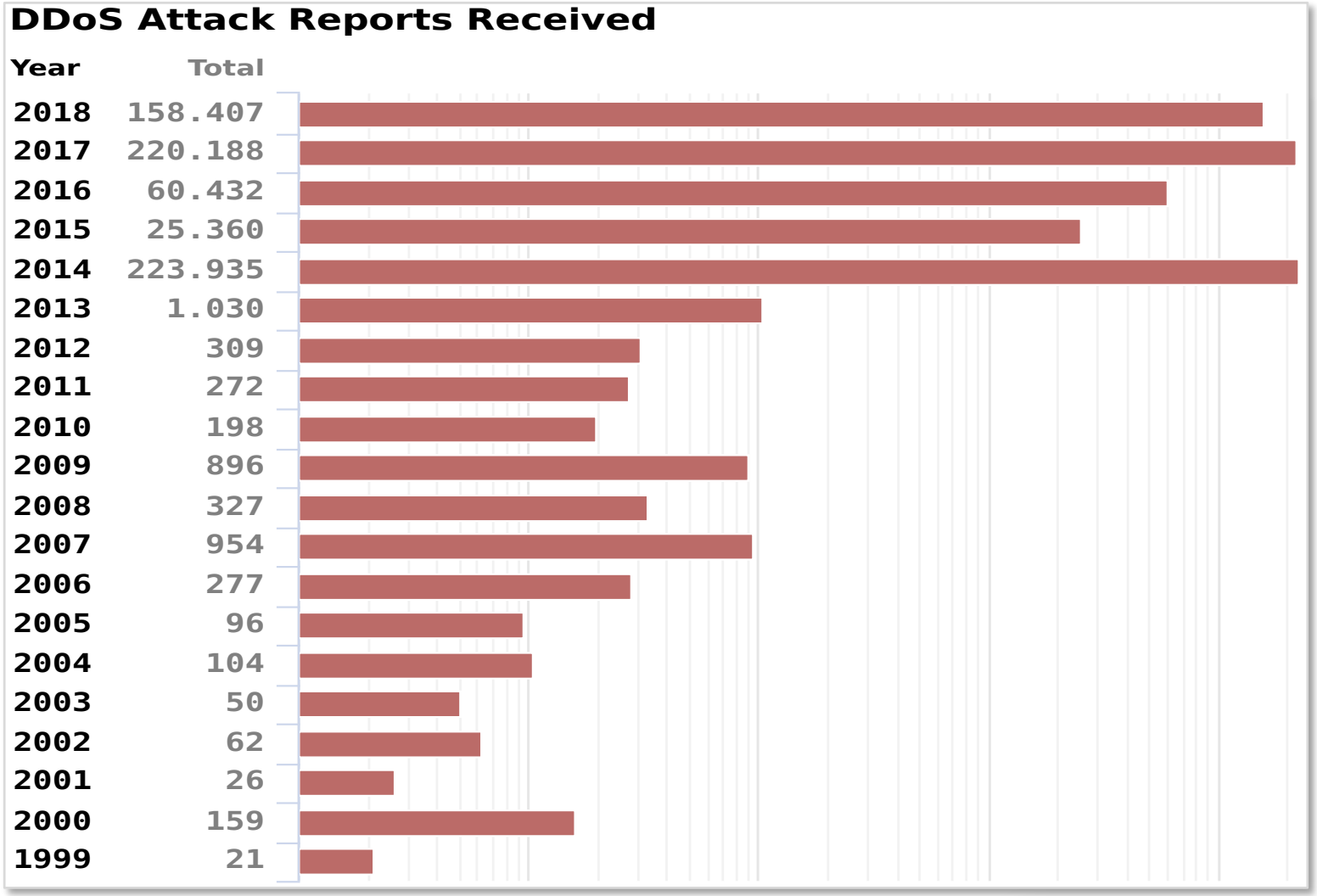
Mission

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

Incidents Reported to CERT.br:
DDoS notifications – history



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

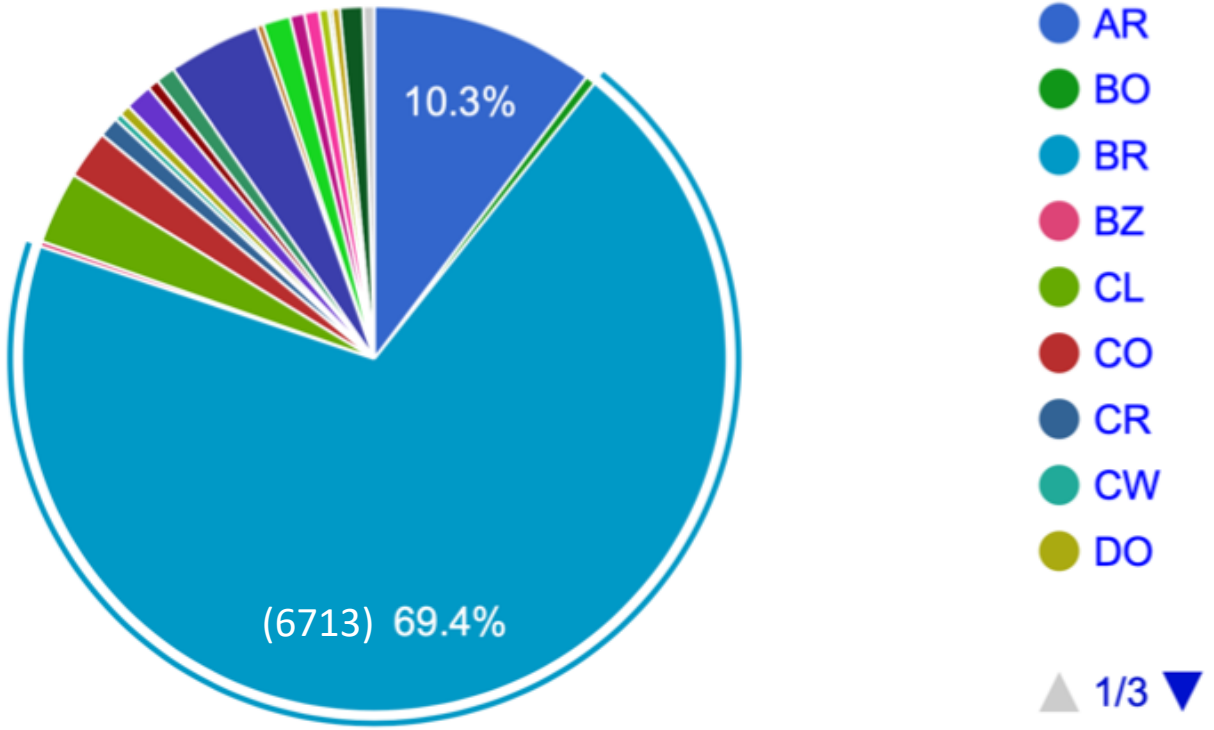
One of the biggest in the world

- #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

https://bcp.nic.br/i+seg

PROGRAMA INTERNET +SEGURA

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

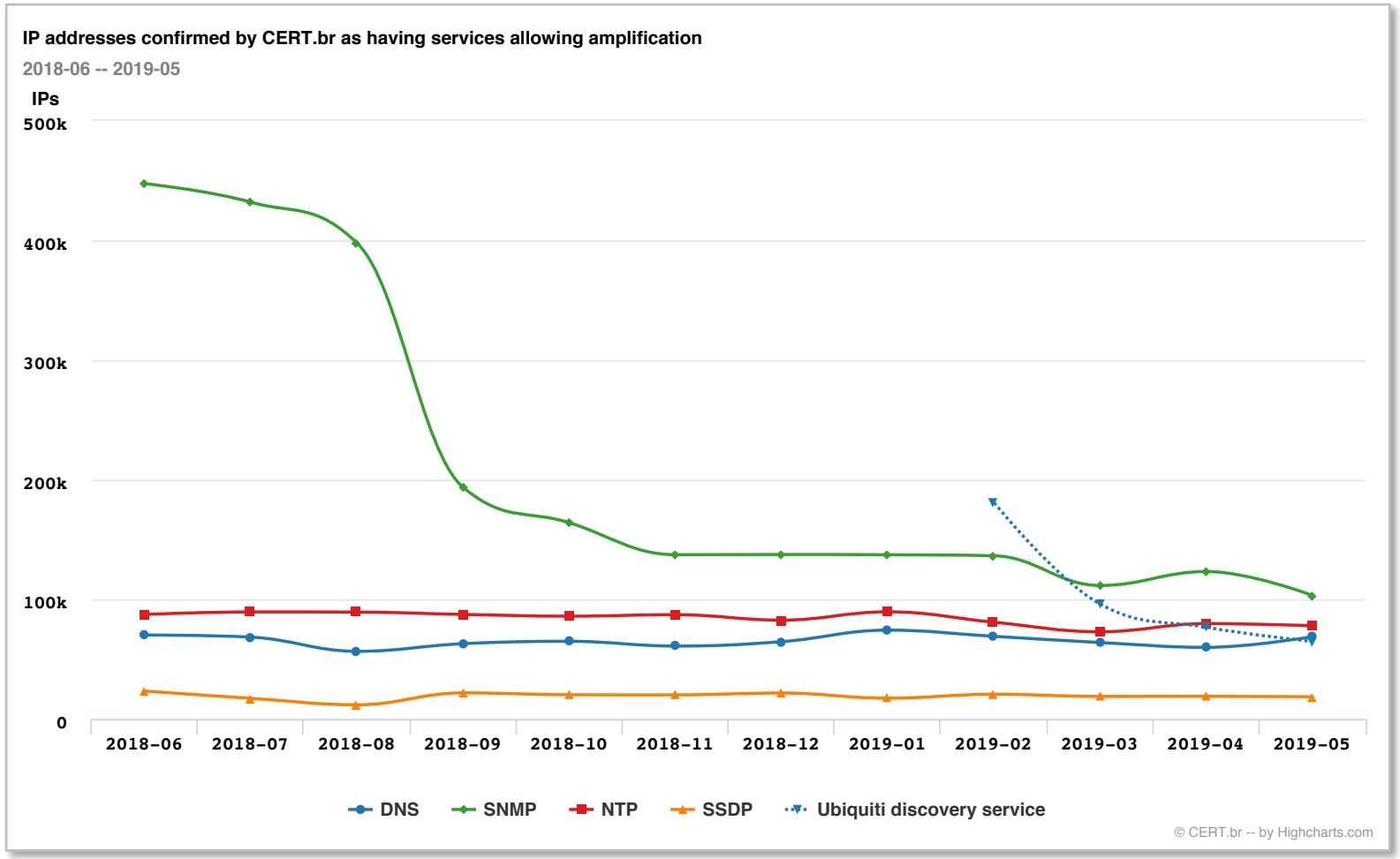
A More Secure Internet Program: Early Results – Reducing Open Services

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



https://www.cert.br/stats/amplificadores/

A More Secure Internet Program:
Early Results – Antispoofing (BCP 38) Implementation

- Higher adoption than in other countries
- Noted by CAIDA Spoofer 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 Spoofer 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

nic.br cgi.br

www.nic.br | www.cgi.br