Cybersecurity and Incident Response Initiatives: Brazil and Americas

Cristine Hoepers
cristine@cert.br

Computer Emergency Response Team Brazil – CERT.br

http://www.cert.br/

Brazilian Internet Steering Committee – CGI.br

http://www.cgi.br/

Overview

- about CGI.br and CERT.br
- discussion of the panel main questions
- how Brazil is dealing with
  - spam
  - phishing
  - user's education
- comments on future threats

CGI.br

The Brazilian Internet Steering Committee (CGI.br)

- created by the Interministerial Ordinance Nº 147, of May 31st 1995
- altered by the Presidential Decree Nº 4,829, of September 3rd 2003

It is a multistakeholder organization composed of:

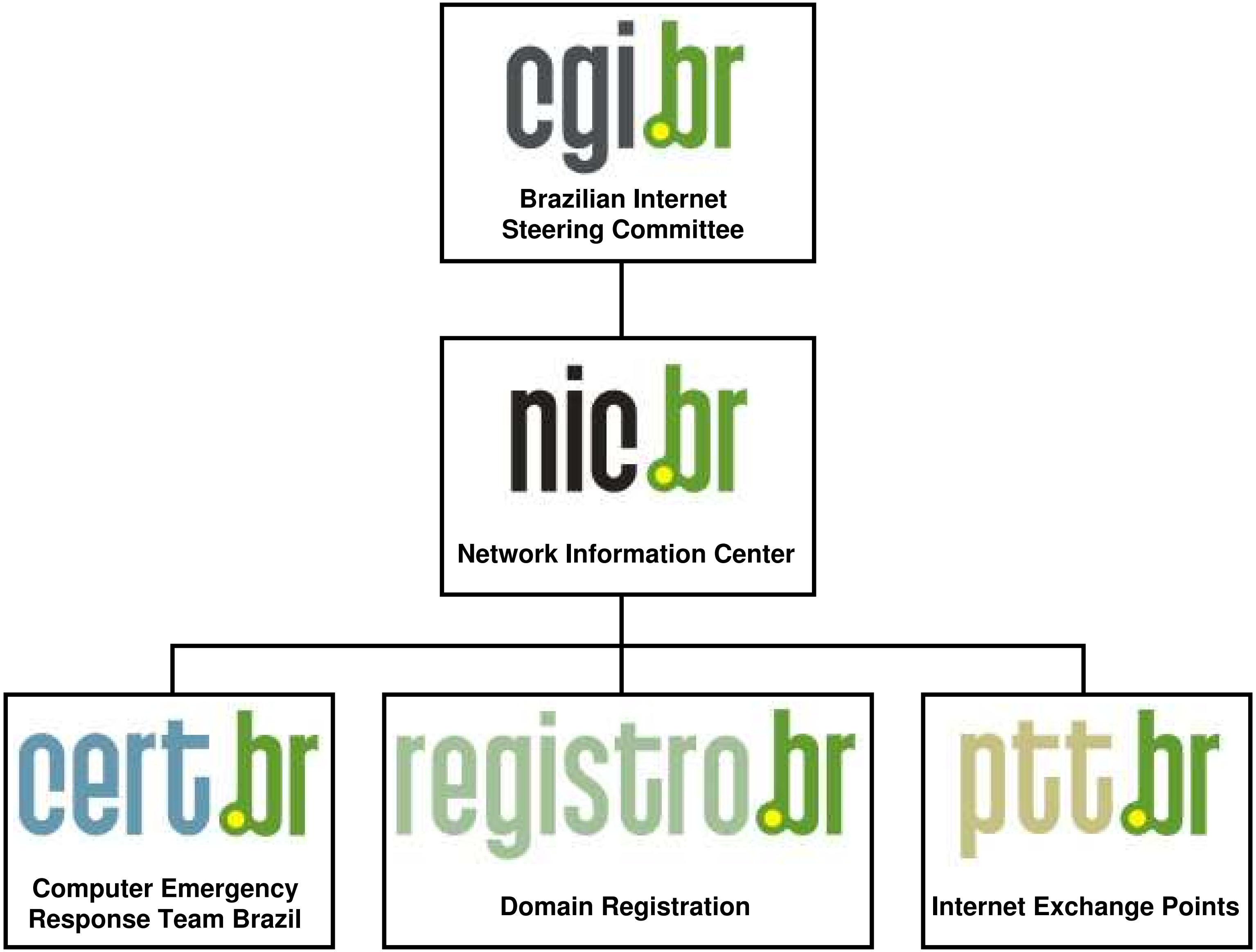
sector	representatives	number
Federal Government	Ministries of Science and Technology, Communications, Defense, Industry, etc, and Telcos Regulatory Agency (ANATEL)	9
Corporate sector	Industry, Telcos, ISPs, users	4
NGO´s	Non–profit organizations, etc	4
Sci. and Tech. Community	Academia	3
	Internet expert	1

CGI.br (cont.)

Among the diverse responsibilities of the CGI.br, the main attributions are:

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

CGI.br (cont.)



Brazilian Internet Steering Committee

Network Information Center

Computer Emergency Response Team Brazil

Domain Registration

Internet Exchange Points

CERT.br Main Activities

- provide a focal point for reporting incidents related to Brazilian networks (.br domain and IPs assigned to Brazil)
- produce security best practices documents in Portuguese
  - for end users (`http://cartilha.cert.br/`)
  - for network and system administrators (`http://www.cert.br/docs/seg-adm-redes/`)
- maintain statistics (incidents and spam)
- increase security awareness and help new CSIRTs to establish their activities

What guidelines should be followed for establishing Cybersecurity at the national level?

Incident Response Development in Brazil

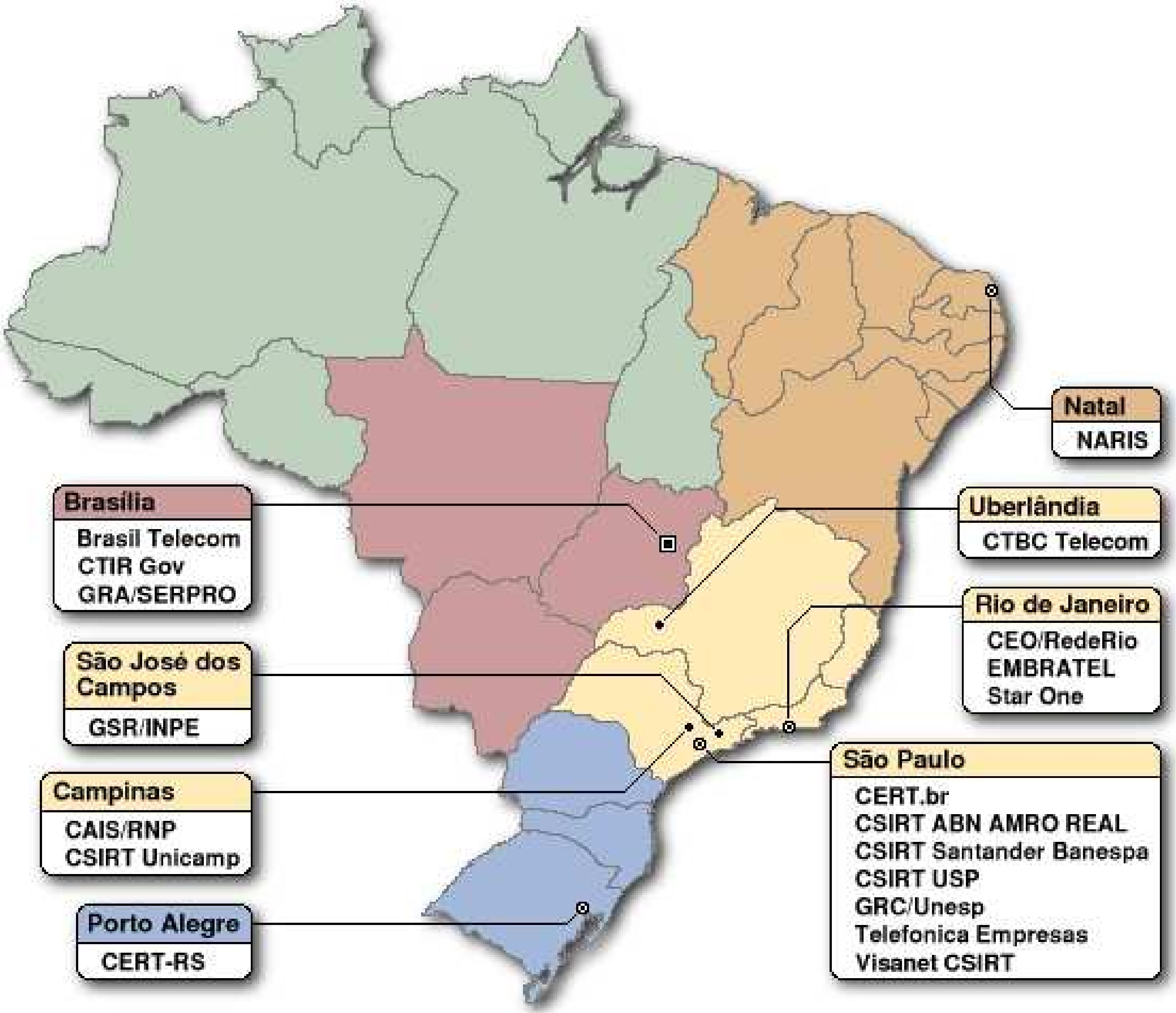
- August/1996: CGI.br released the document: “Towards the Creation of a Security Coordination Center in the Brazilian Internet.” (*)
  - to be a neutral organization
  - to act as a focal point for security incidents in Brazil
  - to facilitate information sharing and incident handling
- June/1997: CGI.br created CERT.br (at that time called NBSO – NIC BR Security Office)

(*) http://www.nic.br/grupo/historico-gts.htm

Incident Response Development in Brazil (cont.)

- August/1997: the Brazilian Research Network (RNP) created it's own CSIRT (CAIS), followed by the Rio Grande do Sul State that created the CERT-RS
- 1999: other institutions including Universities and Telecommunication Companies announced their CSIRTs
- 2000: CERT.br started a CSIRT Development program based on speeches and meetings with key institutions
- 2003: more than 20 CSIRTs formed. Started a CSIRT contact Directory at CERT.br, available at: `http://www.cert.br/contact-br.html`
- 2004: the CTIR Gov was created, with the Brazilian Federal Government Networks as their constituency.

Brazilian CSIRTs



http://www.cert.br/contact-br.html

Training in Incident Response

To raise the national capability in Incident Response

CERT.br/CGI.br are a SEI/CMU Partner and have licensed 4 CERT/CC courses to deliver in Brazil:

- Creating a Computer Security Incident Response Team
- Managing Computer Security Incident Response Teams
- Fundamentals of Incident Handling
- Advanced Incident Handling for Technical Staff

160+ people trained

To promote Cybersecurity at the national level it is necessary to gain trust, collaborate and raise awareness

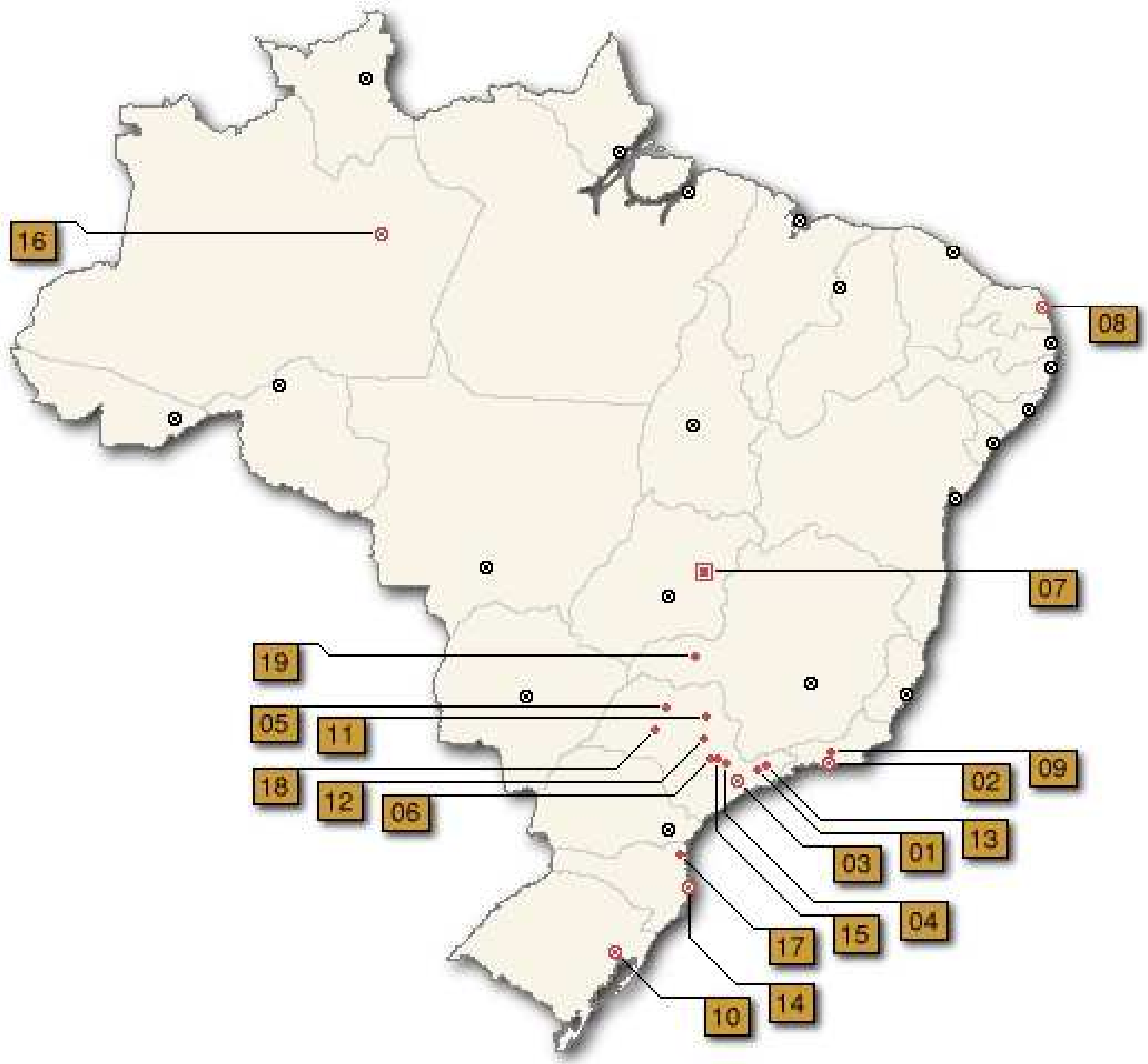
CERT.br Initiatives

Brazilian Honeypots Alliance – Distributed Honeypots Project

- 27 research partner's institutions:
  - academia, government, industry, military and telcos networks
- widely distributed across the country
- based on voluntary work of research partners
- public statistics
- identify signatures of well known malicious/abusive activities
  - worms, bots, scans, spam and other malware
  - notify the responsible networks of the Brazilian IPs with recovery tips
- donate sanitized data of non-Brazilian IPs to other CSIRTs

http://www.honeypots-alliance.org.br/

The Honeypots Network (cont.)



Cities where the honeypots are located.

CGI.br Initiatives

- sponsors 2 meetings/conferences free of charge per year, to the security and network communities (GTS/GTER)
- iNOC-DBA BR – project to stimulate Brazilian networks to join the iNOC-DBA global network
  - 100 IP phones where provided to ASNs
  - 20 IP phones where provided to CSIRTs recognized by CERT.br

iNOC-DBA – global hotline phone system which directly interconnects the Network Operations Centers and Security Incident Response Teams

How well-prepared is the Americas region?

The Inter-American Cyber Incident Response Network

- to stablish a hemisphere-wide network of cyber security incident response contact points
- cooperation must make it possible to:
  - stablish CSIRTs in each of the Member States
  - strengthen the hemisphere's CSIRTs
  - make use of existing subregional mechanisms
- more details at:

  http://www.cicte.oas.org/English/Cyber.htm

What are the appropriate forums for regional and international co-operation?

There is no single forum

CERT.br International cooperation:

- FIRST full member (http://www.first.org/)
- Honeynet Research Alliance member (http://project.honeynet.org/alliance/)
- Anti-Phishing Working Group Research Partner (http://www.antiphishing.org/)

Other International forums

- APCERT (http://www.apcert.org/)
- TF-CSIRT (http://www.terena.nl/tech/task-forces/tf-csirt/)
- EGC (http://www.bsi.de/certbund/EGC/index_en.htm/)

What is the best approach for dealing with spam and "phishing"?

CGI.br Task Force on Spam (CT-Spam)

- to propose a national strategy to fight spam
- to articulate the actions among the different actors
- documents created
  - “Technologies and Policies to Fight Spam”
  - technical analysis of international antispam laws and brazilian proposals of new laws
- this task force is creating a national website with trustworthy information, and is effectively involving all sectors
- CERT.br is coordinating with AusCERT and GOVCERT.NL – sharing technical information and lessons learned

Actions Against Phishing

- cooperation between CERT.br and the Financial Sector to understand the threat and mitigations techniques
- user's education is the key
  - site with information for end users (http://cartilha.cert.br/)
- CERT.br is focused on technical issues
  - detect malware enabled fraud
  - notify hosting sites
  - send samples to 20+ AV vendors

What future threats are on the horizon?

Future Threats

- continuously increase in automation
- maintain the focus on the final user
  - increase in the number of users with broadband
  - machines infected with bots/worms and used for spam, phishing, DDoS and other attacks
- “botnet effect” in other devices (cellphones, PDAs, etc)
- time between the discovery of a vulnerabilty and the automated exploitation will be even shorter
  - no reasonable time to react
  - update/patch/anti-virus solutions no longer viable
- crimes will continue to increase in the Internet

Final Considerations

For a real improvement in the long term:

- the IT industry need to change its mindeset
  - have secure systems by default
  - change the development cycle, with focus on secure coding and testing
- it is important to promote education on secure desing and programming at universities;
- it is necessary to teach “online ethics” to children
  - so they don’t become script kiddies and get involved with criminals