CGI.br and CERT.br Initiatives in Incident Response

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

Computer Emergency Response Team Brazil – CERT.br
http://www.cert.br/
cert@cert.br

Brazilian Internet Steering Committee
http://www.cgi.br/
Overview

- about CGI.br and CERT.br
- history of Incident Response in Brazil
- CERT.br Initiatives
  - training, early warning, awareness
- CGI.br Initiatives
  - meetings/conferences for security and network communities (GTS/GTER)
  - iNOC-DBA BR
  - Task Force on Spam (CT-Spam)
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

Is a multistakeholder organization composed of:

- nine Federal Government representatives
- four representatives of the corporate sector
- four representatives of the third sector
- three representatives of the scientific and technological community
- one Internet expert
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
CSIRTs’ History 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
CSIRTs’ History in Brazil (cont.)

• August/1997: the Brazilian Research Network (RNP) created its 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
CERT.br 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
CERT.br Initiatives

CERT.br is a Software Engineering Institute Partner and has 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

140+ people trained
Brazilian Honeypots Alliance – Distributed Honeypots Project

• coordination: CERT.br and CenPRA/MCT
• 27 research partner’s institutions:
  – academia, government, industry, military and telcos networks
• widely distributed across the country
  – in several ASNs and geographical locations
• based on voluntary work of research partners
• public statistics
  – combined daily flows seen in the honeypots

http://www.honeypots-alliance.org.br/
The Honeypots Network (cont.)

Cities where the honeypots are located.
Use of the honeypots data in Incident Response

• 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
CERT.br Initiatives (cont.)

International cooperation:

- FIRST full member ([http://www.first.org/](http://www.first.org/))
- Honeynet Research Alliance member ([http://project.honeynet.org/alliance/](http://project.honeynet.org/alliance/))
  - detect malware enabled fraud
  - notify hosting sites
  - send samples to 20+ AV vendors
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
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