nic.br cgi.br cert.br

LACNIC 25 – CSIRTs Meeting

Havana, Cuba

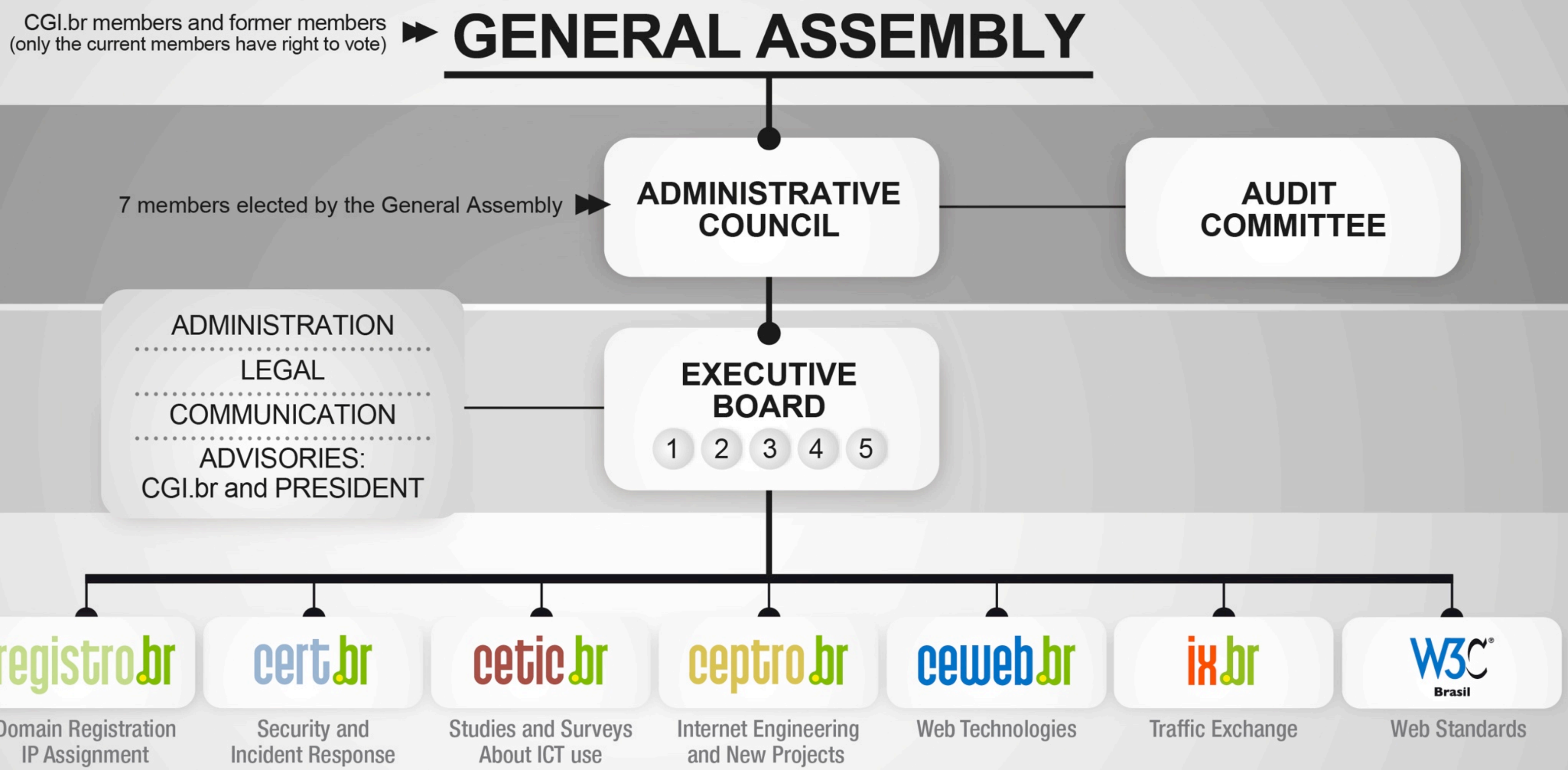
May 4th, 2016

DDoS Atacks:
Detection, Analysis and Mitigation

Lucimara Desiderá
lucimara@cert.br

Klaus Steding-Jessen
jessen@cert.br

cert.br nic.br 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

AUDIT COMMITTEE

ADMINISTRATION

LEGAL

COMMUNICATION

ADVISORIES:
CGI.br and PRESIDENT

EXECUTIVE BOARD

1 2 3 4 5

registro.br
Domain Registration
IP Assignment

cert.br
Security and
Incident Response

cetic.br
Studies and Surveys
About ICT use

ceptro.br
Internet Engineering
and New Projects

ceweb.br
Web Technologies

ix.br
Traffic Exchange

W3C Brasil
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

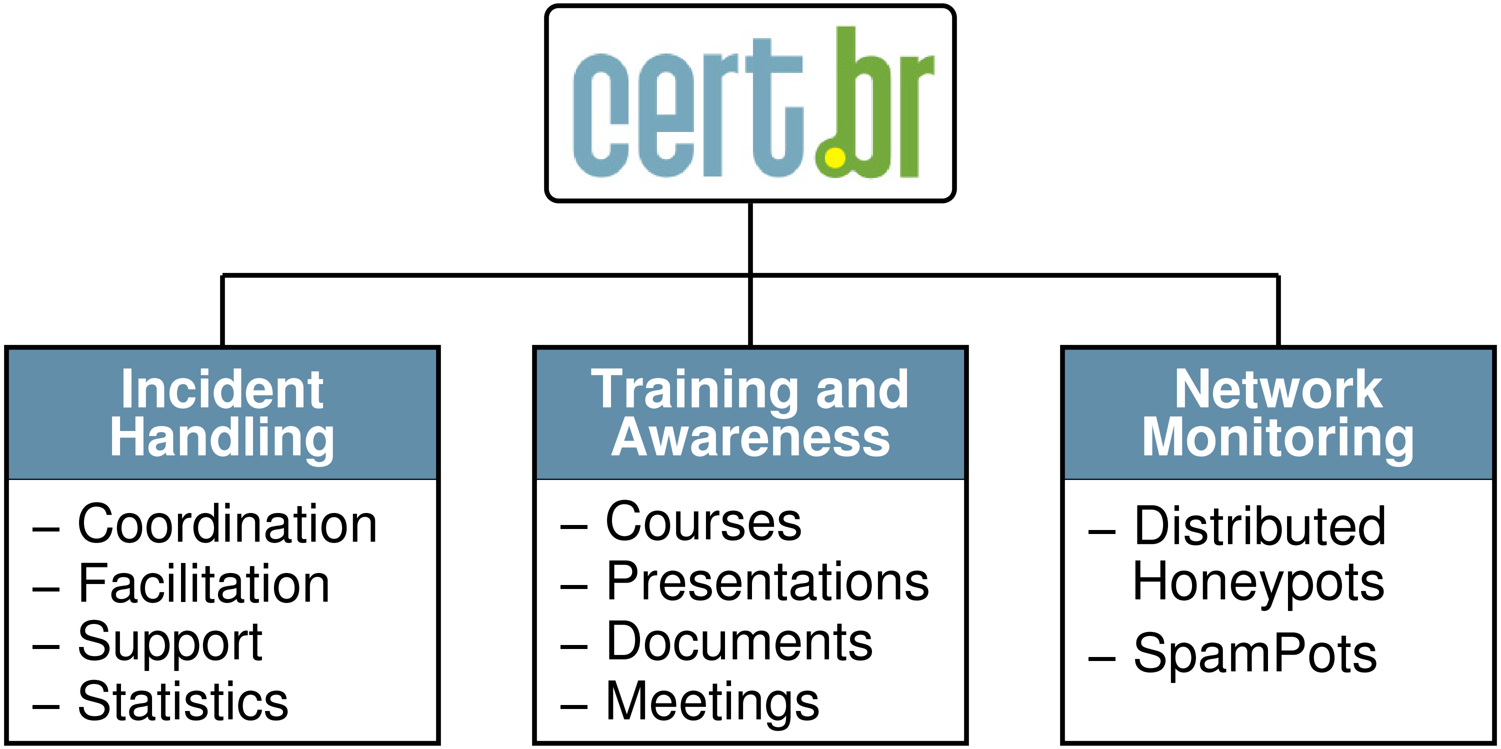
Internet Governance in Brazil:
The Brazilian Internet Steering Committee – CGI.br

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 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/about/

CERT.br Activities



Incident Handling

- Coordination
- Facilitation
- Support
- Statistics

Training and Awareness

- Courses
- Presentations
- Documents
- Meetings

Network Monitoring

- Distributed Honeypots
- SpamPots

http://www.cert.br/about/

DDoS Atacks: Challenges

cert.br nic.br cgi.br

Challenges:

- It's not possible to avoid them
  - Anyone can be a target
- Countless networks/systems being abused to perpetrate attacks:
  - DNS open resolvers, lack of antispoofing implementation, unnecessary services enabled, unpatched systems, weak passwords, etc
- Attacks are getting more harmful:
  - reflective
  - mixed techniques
- CERT.br 2014: more than 200 times increase in DDoS notifications

How to make things better?

GOAL:

- **help to understand the attack types in order to choose the right mitigation strategy**
- **compile a set (not exhaustive) of good practices:**
  - **avoid networks and systems from being abused to perpetrate attacks**
  - **how to handle DDoS attacks**
    - prepare
    - detect
    - analyze
    - mitigate

Document ***"Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)"***

http://www.cert.br/docs/whitepapers/ddos/

Some highlights

Document highlights – Main topics

- Main targets and motivations for the attacks
- How attacks are executed
- Attack Types
  - Application layer attacks
  - Resource exhaustion attacks
  - Volumetric attacks
- How to avoid your network and systems from being abused to perpetrate attacks
  - End users
  - Web application developers
  - Network administrators
  - ISPs
- How to handle DDoS attacks
  - Preparation
  - Detection and Analysis
  - Mitigation
  - Post mortem

Don't contribute to the problem: **Best Practices to avoid being abused (1/2)**

Implement *anti-spoofing* (BCP38)

- https://tools.ietf.org/html/bcp38
- http://spoofer.caida.org/
- http://bcp.nic.br/

DNS

- Enable recursion for your network only
- On authoritative servers:
  - Disable Recursion
  - Consider implementing *Response Rate Limit* (RRL)

NTP

- Consider using a simpler implementation
  - OpenNTPD
- Uptade to version 4.2.7 or superior
- Disable the *monitor* function in `ntpd.conf`

Don’t contribute to the problem: **Best Practices to avoid being abused (2/2)**

SNMP

- Use version 3 if possible
- Don’t use the *Public* community

Other protocols

- Enable only when necessary

Preparation

Adopt proactive measures

- become an Autonomous System
  - more than one route to the Internet
  - control over your own routing policy
- over provisioning
  - have physical links/ports with more capacity than contracted
  - service scalability (web, e-mail, etc)
- make sure your contracts allow bandwidth flexibility in case of attacks
- implement network segregation for critical services
- reduce the visibility of internal systems and services
- establish contacts with the technical team from your upstream to have help in case of emergency
- train the technical network team to implement mitigation techniques

Detection

Monitor your network traffic – in and out

- this allows the identification of:
  - changes in the network use patterns
  - detection of connections to botnet C&C

"Intrusion Detection"

- IDS / IPS, Firewall, Antivirus

"Extrusion Detection"

- Netflows, Honeypots, Passive DNS
- Handling abuse and incident notifications
- Data Feeds (Team Cymru, ShadowServer, other CSIRTs)

Mitigation

Improve your infrastructure

- more bandwidth
- services and routers with more capacity

Traffic filtering by source IP or port

- firewall, IPSes, switches and routers

Use rate-limiting and ACLs in routers and switches

Contact your upstream

- apply filters, blackholing / sinkholing
- DDoS mitigation services ("clean pipe")

If you have an AS, consider using Team Cymru's UTRS

- http://www.team-cymru.org/UTRS/

Contract mitigation services

- may affect the confidentiality of information

Move to a CDN (*Content Delivery Network*)

Thank You

www.cert.br

lucimara@cert.br   jessen@cert.br   @certbr

May 04th, 2016

nic.br cgi.br

www.nic.br | www.cgi.br