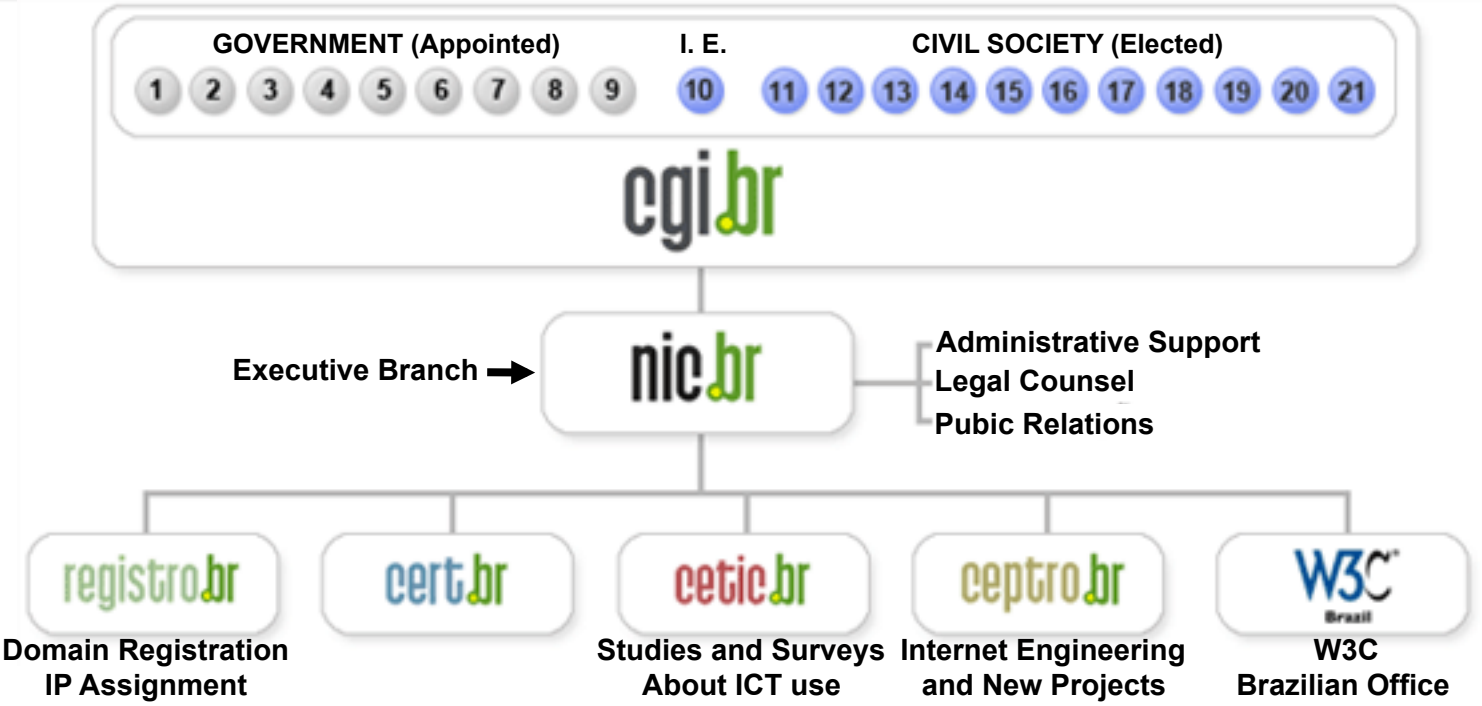
Anti-botnet Initiatives

Lucimara Desiderá
lucimara@cert.br

Computer Emergency Response Team Brazil - CERT.br
Network Information Center Brazil - NIC.br
Brazilian Internet Steering Committee - CGI.br

CGI.br and NIC.br Structure



1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – National Forum of Estate Science and Technology Secretaries
10 – Internet Expert

11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

The Brazilian Internet Steering Committee - CGI.br

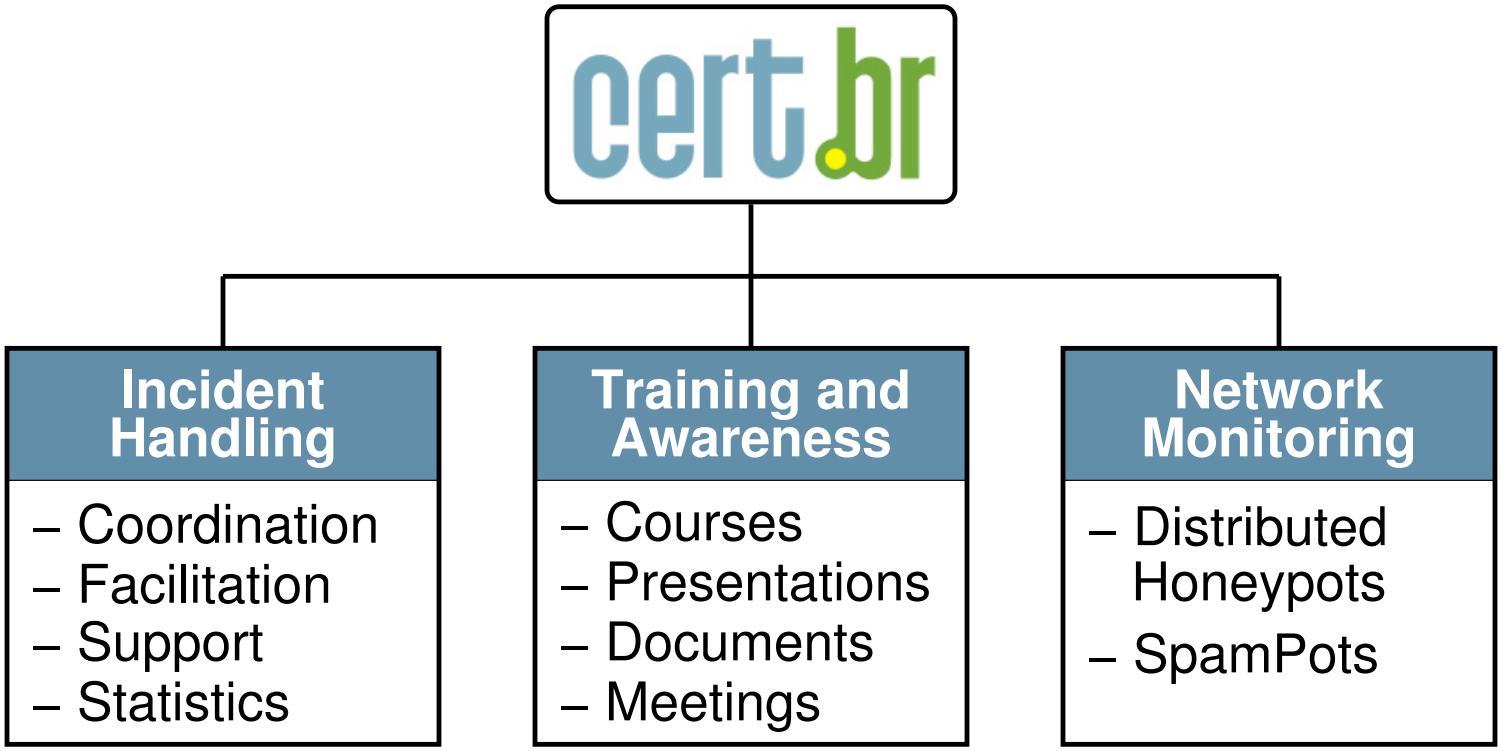
CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

Among the diverse responsibilities reinforced by the Presidential Decree 4.829, 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 recommend 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/english/

CERT.br Activities



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

The Honeynet PROJECT

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

Agenda

- Current mitigation focus
- Mitigation activities in Brazil
- Next steps

Current Mitigation Techniques

Focus in disrupting the C&C communications

- **DNS-based Countermeasures**
- **Takedown of Command-and-Control Server**
- **Packet Filtering on Network and Application Level**

Focus on blocking the attacks perpetrated by zombies

- **Blacklisting of infected computers**
- **Port 25 management**

Mitigation Activities in Brazil (1/2)

- **CGI.br Port 25 Management / Antispam.br campaign**
  - **Brazil is no longer in the CBL "Top 10" (from 1st to 20th)**
    http://cbl.abuseat.org/country.html
    http://www.nic.br/imprensa/clipping/2013/midia182.htm

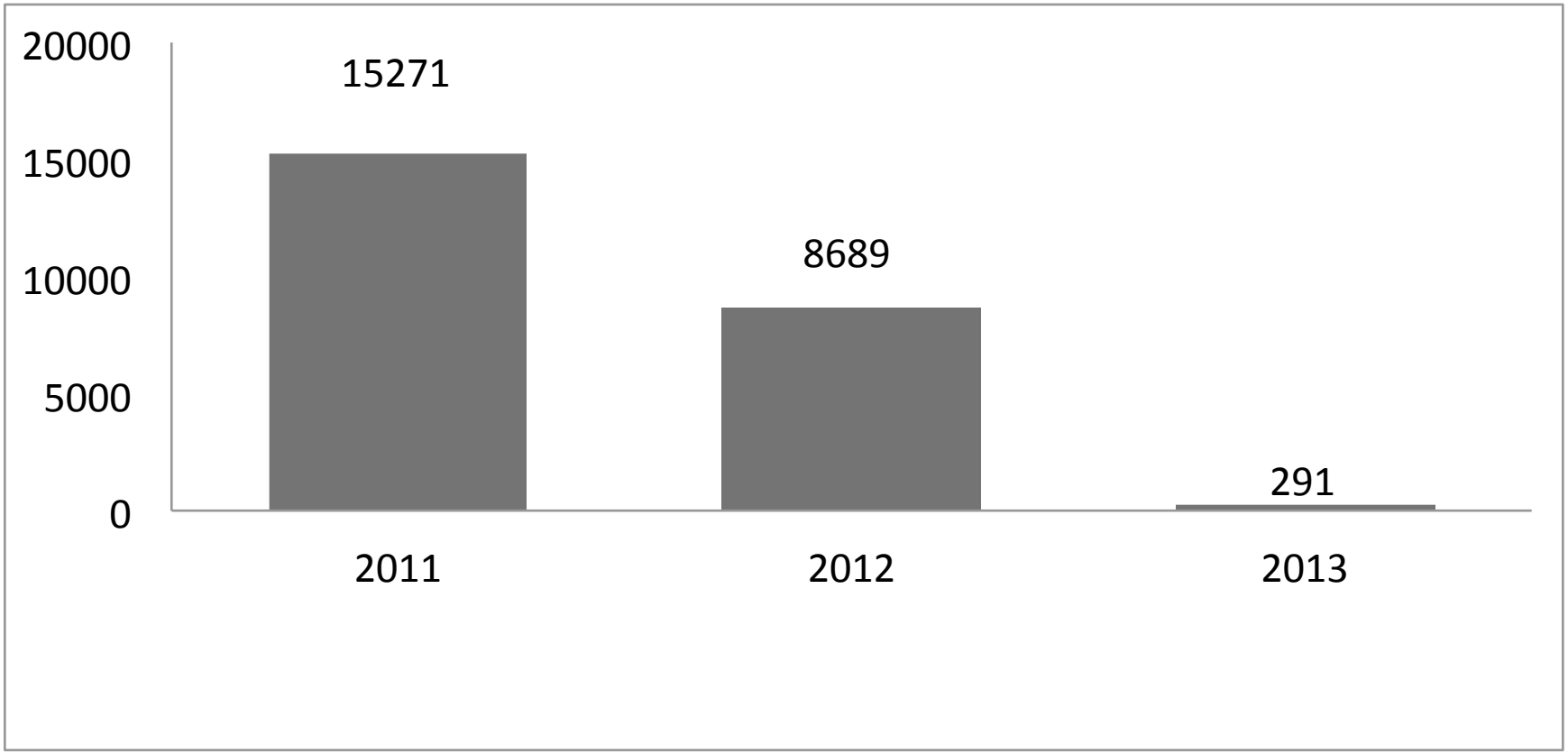
- **Registro.br actions against malicious domains**
  - **E.g. blocking the registration of domains to be used by Conficker variants**

- **CERT.br notification of network activities related to bot propagation**
  - **seen in our honeypots network**

- **CERT.br notification of bots seen in C&Cs**
  - **as part of takedown operations**

Mitigation Activities in Brazil (2/2)

Notifications sent as part of the cooperation with takedown operations



Future: Need to focus on remediation

- Current mitigation techniques are not enough
  - end users are still infected

- Best practices already being discussed
  - RFC 6561: Recommendations for the Remediation of Bots in ISP Networks
  - Having ISP engaged in
    - Education
    - Detection
    - Notification
    - Remediation
    - Collaboration

International Initiatives

- iCODE – Australia
- Botfrei.de – Germany
- Irish Anti-Botnet Initiative (Botfree.ie) – Ireland
- Cyber Clean Center (CCC) – Japan
- Cyber Curing System / e-Call Center 118 – Korea
- Anti-Botnet Working Group – Netherlands
- Abuse Information Exchange – Netherlands
- Autoreporter – Finland
- U.S. Anti-Bot Code of Conduct (ABCs) for ISPs – USA
- Malware Free Switzerland – Switzerland
- Advanced Cyber Defence Centre / Botfree.eu – European Union

Questions?

Lucimara Desiderá

lucimara@cert.br

- **CGI.br - Brazilian Internet Steering Committee**
  http://www.cgi.br/
- **NIC.br**
  http://www.nic.br/
- **CERT.br**
  http://www.cert.br/