Cooperation Initiatives Among Diverse Sectors

Cristine Hoepers
General Manager
cristine@cert.br

Computer Emergency Response Team Brazil - **CERT.br**

Network Information Center Brazil - **NIC.br**
Brazilian Internet Steering Committee - **CGI.br**

Agenda

- Cooperation within our mission
- Informal cooperation
  - Malware and phishing
    - banks, AV companies, browser vendors
  - Compromised and infected machines identification
    - CSIRTs with national responsibility, ISPs, botnet research organizations
- Formal cooperation with ISPs and Telcos
  - Regulatory issues
    - Telecommunication Infrastructure Providers
    - Internet Service and Content Providers

The Brazilian Internet Steering Committee - CGI.br

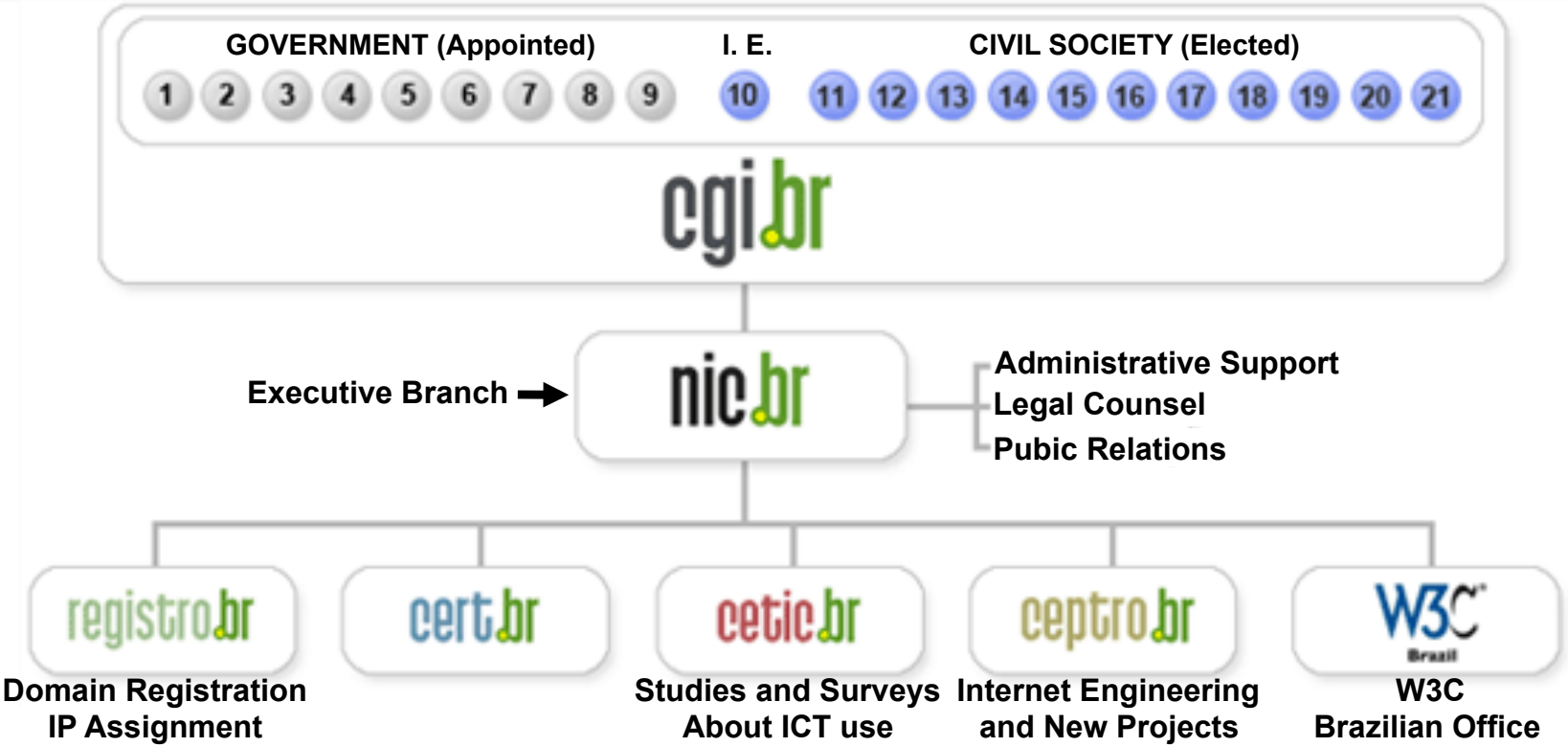
CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

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 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/

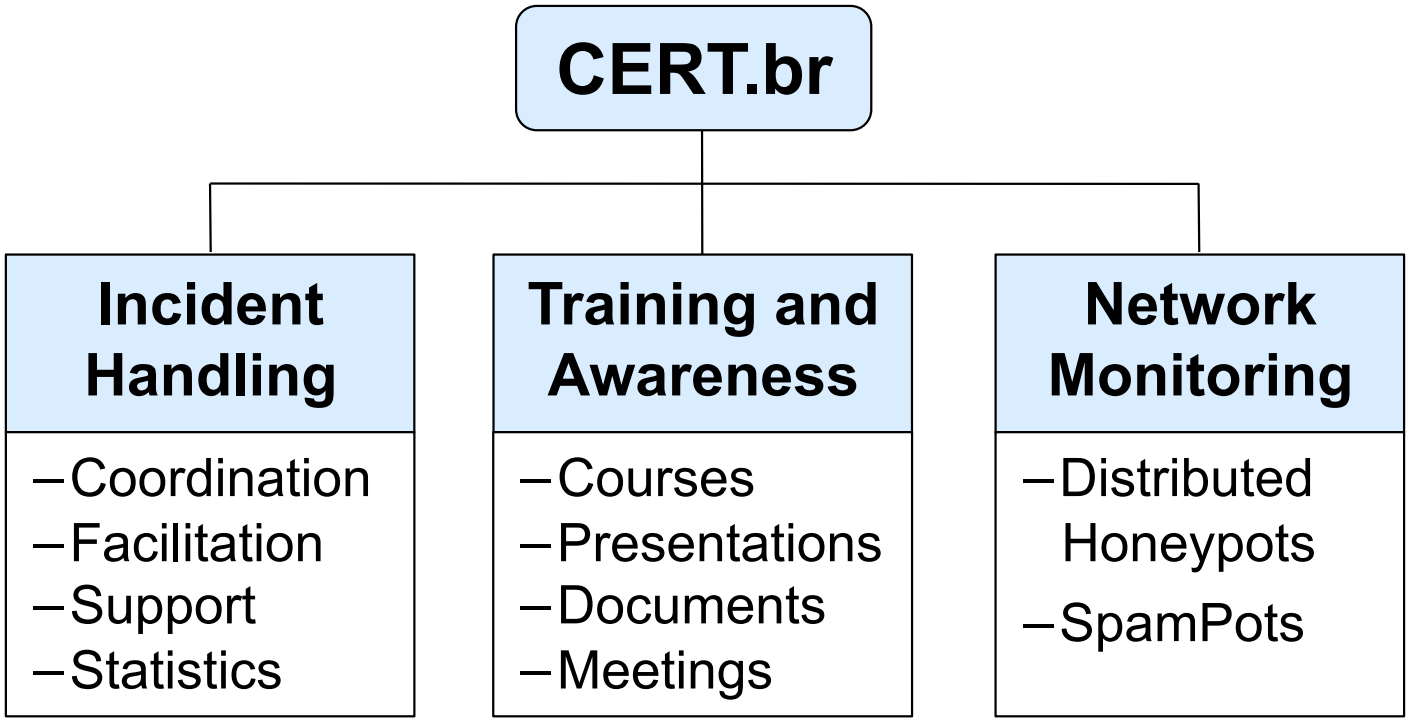
CGI.br and NIC.br Structure



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

CERT.br Activities



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

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

Informal Cooperation

Improve Incident Handling Capacity and Cooperation

Get the players involved

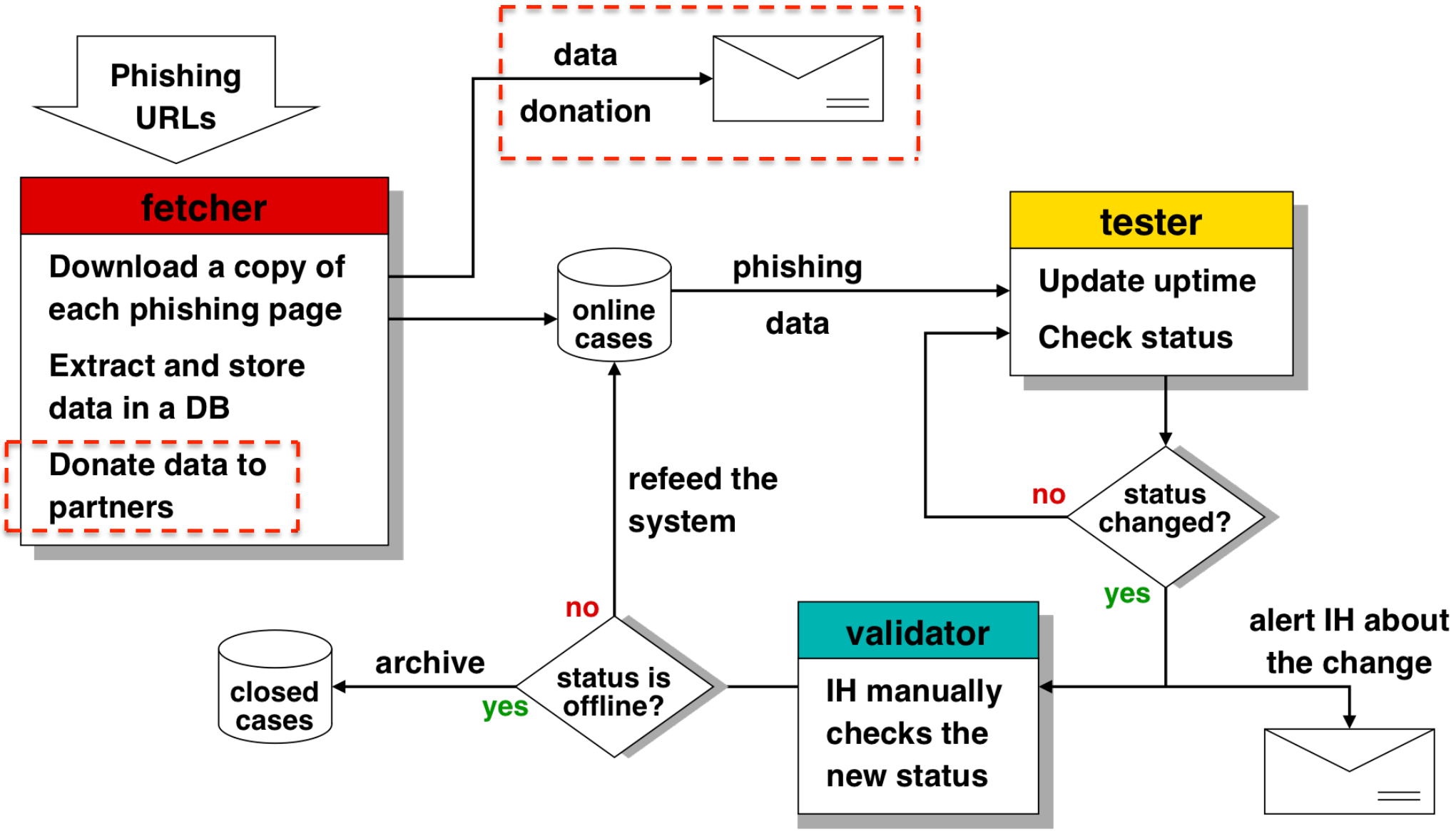
- Regular meetings with the Financial Sector CSIRTs
- Individual meetings with CSIRTs and SOCs of diverse sectors
  - to identify problems in the incident response process
  - to establish better communication and prioritization of reports among CSIRTs
  - to help improve the processes to grow effectiveness

Protect the Internet Users and Organizations

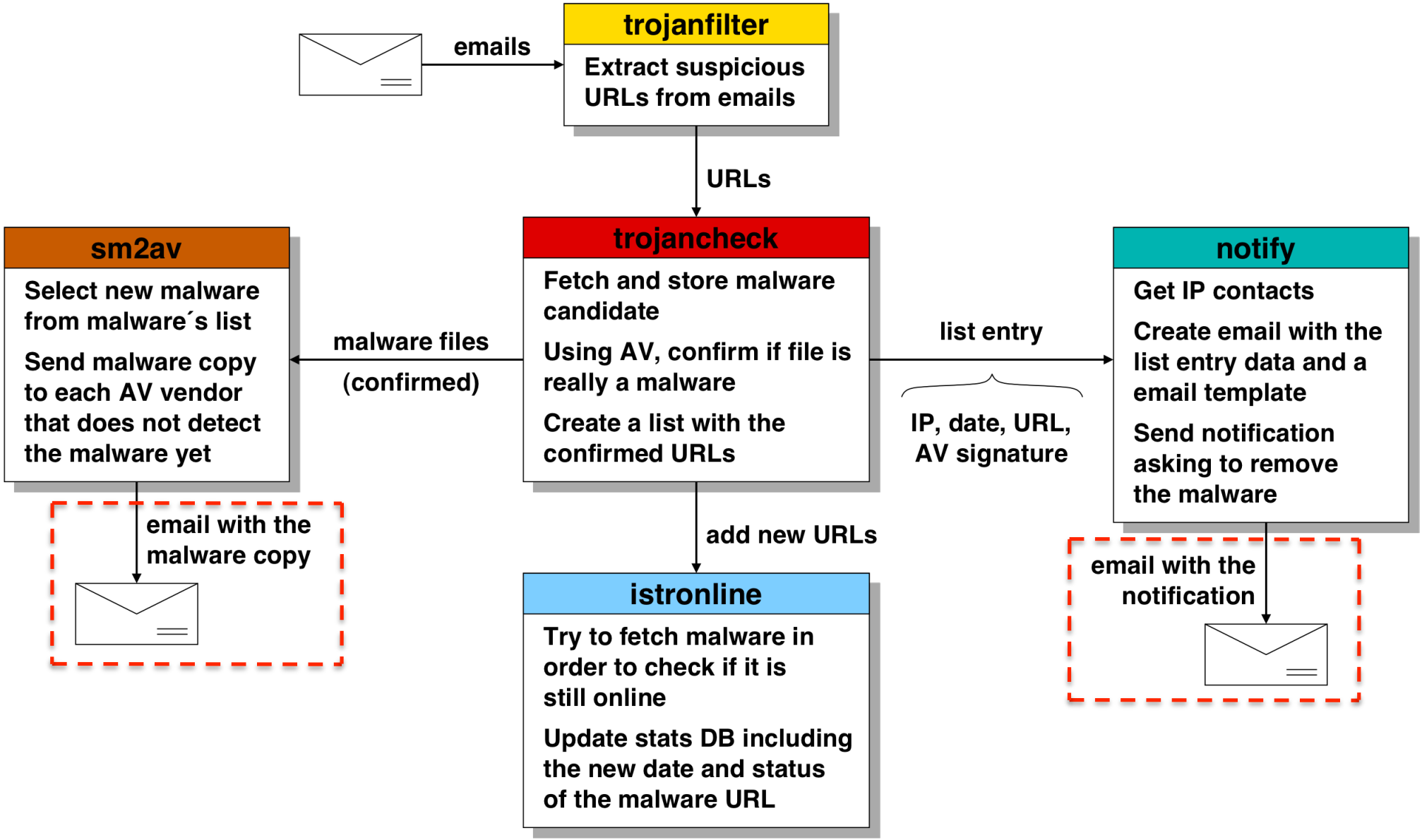
- Reduce the window of exposure
- Notify compromised networks
- Improve the effectiveness of tools

Malware and phishing

Online Phishing Monitoring and Notification System



Banking Malware Notification and Submission System



Malware and Phishing Cases Handled in 2010

327.245 reports, that were categorized in:

Phishing

- Cases: 7960
- Unique page contents: 3611
- IPs hosting phishing: 3494
- Countries hosting content: 96

Banking Malware

- Unique new samples: 5333
- Unique URLs: 7298
- IPs hosting malware: 2553
- Countries hosting malware: 72

Actions

- Notify sites hosting phishing for takedown
- Send the URLs to phishing protection products: Firefox, IIS, Yahoo!, Trendmicro and UOL

Actions

- Notify sites hosting malware for takedown
- Send malware to 35+ AV vendors
- Send malware to the institutions affected

Some Results of Working to reduce the response time

Average uptime of phishing cases: 8d 10h 25m

Cases Hosted in IPs allocated to Brazil

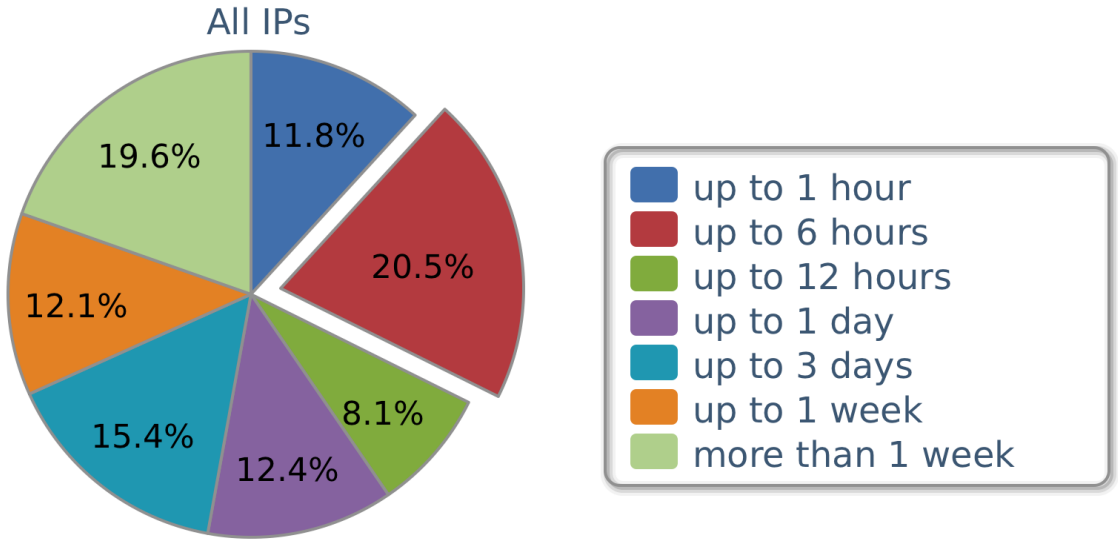
- **average uptime: 4d 01h 47m**
- **47% were taken down up to 12 hours after the first report**

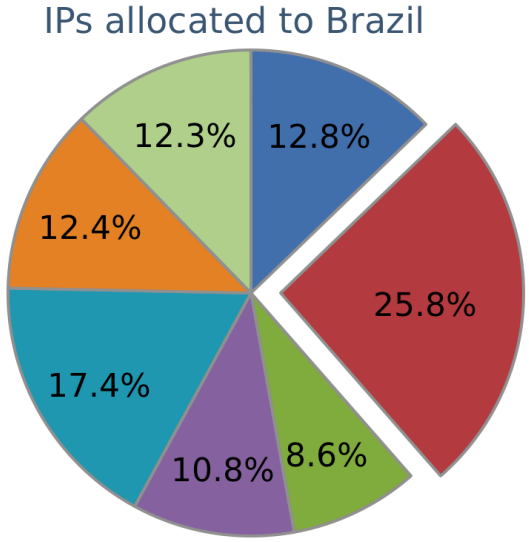
Cases Hosted in IPs allocated to other countries

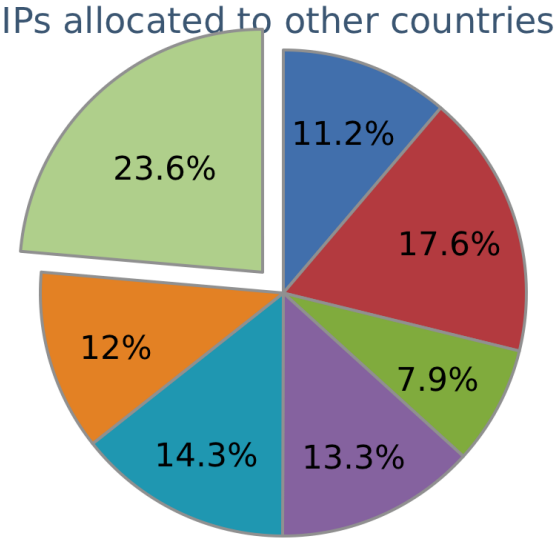
- **average uptime: 10d 20h 24m**
- **50% took more than 2 days to be taken down**

The difference:

- **Language barriers, lack of contacts in other countries**
- **Helping networks to be more effective brought our numbers down**

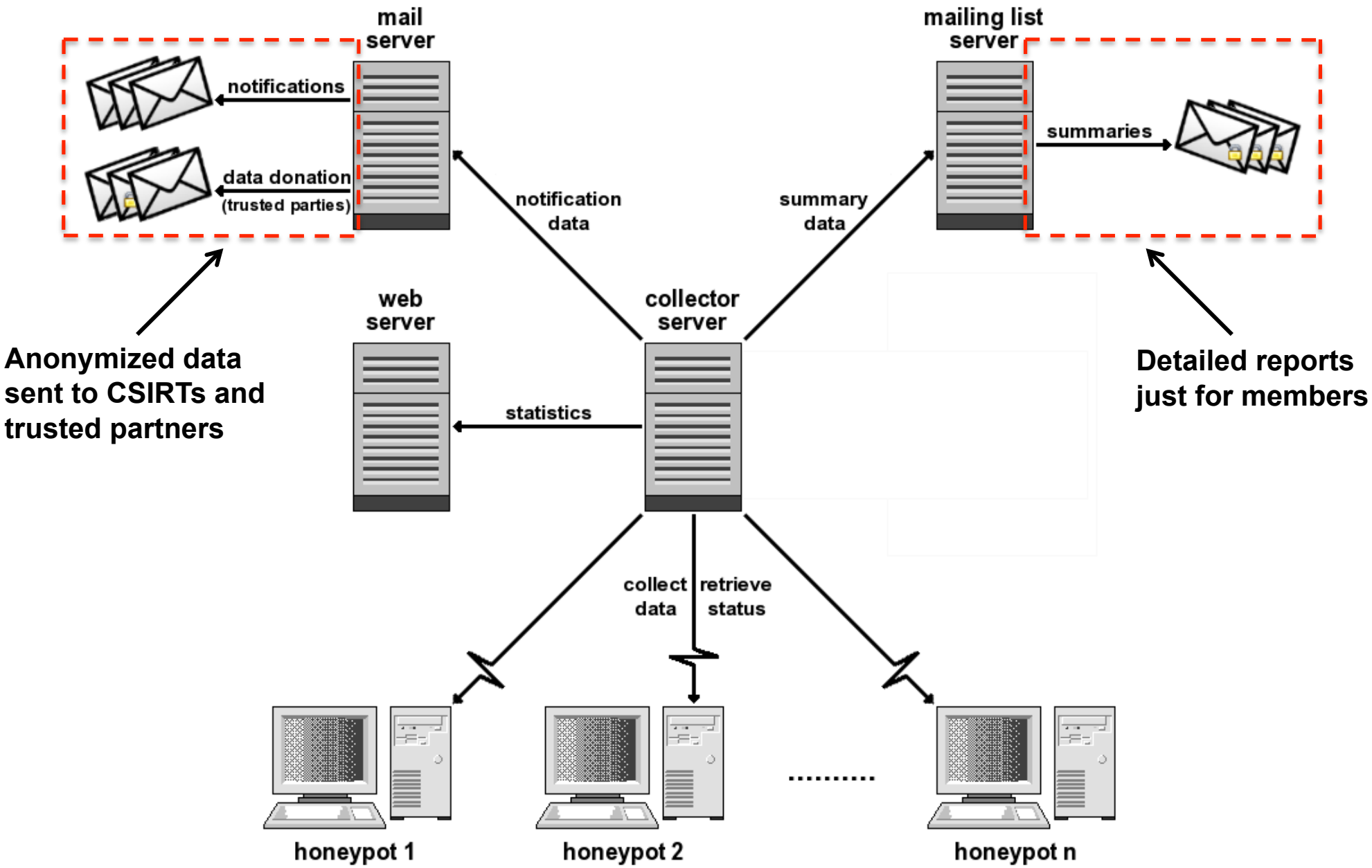






Compromised and Infected Machines Identification

Architecture of the Network of Honeypots



Uses of the Data to Help the Community

Individual Incident Notifications

- Only for IPs allocated to Brazil
- Sent to whois contacts and CSIRTs (when one exists)
- With anonymized logs
- Includes a description of the problem, how to identify compromised machines, how to recover, etc

Daily donation of anonymized data

- To CSIRTs with national responsibility
  - All traffic coming from IPs allocated to the given country
- To organizations that share data with ISPs
  - Team Cymru (SSH brute force attacks and some botnet traffic)
  - Shadowserver Foundation and Arbor ATLAS (SSH brute force attacks)

Formal Cooperation with Telcos and ISPs: Port 25 Management Working Group 2005—present

Telecommunications Legal Framework

Divides the services in 2 major categories:

- **Telecommunication Providers – provide the infrastructure for data networks, and this is regulated by Anatel**
  - **ADSL: Telefonica, Oi, GVT, Sercomtel, CTBC**
  - **3G: Claro, Oi, Sercomtel, VIVO, TIM**
  - **Cable: NET, TVA**
- **Internet Service and Content Providers – provide all "value-added" services (e-mail, hosting, etc)**
  - **UOL, Terra, iG, Yahoo!, Gmail, Hotmail**

In other words:

- **Physical Layer → regulated by Anatel (Brazilian Telecommunication Regulatory Agency)**
- **All Internet Services (i.e. TCP/IP) → not regulated, initiatives coordinated by CGI.br**

What is needed for cooperation among diverse sectors

- A common goal upon which to cooperate
- Identify who should be involved in any specific initiative
- Consider sensitive issues that can impact the participation of the different players

- One single framework involving everybody is usually pointed in Conferences and Workshops as the ultimate goal

- Real life is much harder
  - People tend not to openly share problems with people they don't know
  - Sometimes organizations won't talk about problems if there is police or regulators involved
    - Other times their presence is important for success – need to find a balance
  - Before any cooperation really starts there is a lot of finger pointing

Anti-spam Task Force – Port 25 Management Working Group

- Common Goal: reduce the abuse of the Internet infrastructure in Brazil by spammers
  - Brazil is being appointed as a big “source” of spam
  - Brazilian networks are being affected negatively
- Who is involved
  - Initially: Telcos, ISPs and Associations of these sectors, Anatel, the CGI.br representatives for these sectors and CERT.br
  - Players identified in further meetings: Federal Prosecutor’s Office, Consumer Defense organizations and Ministry of Justice
- Sensitive issues:
  - Competitive issues among ISPs and Telcos
  - No one would admit how big the problem really is and what is the real impact for the infrastructure or the consumers

The problem was not clear to all involved

- Who is abusing our infrastructure? And how?
- Are there any national metrics or only international?
- How can we gather data and generate metrics to help the formulation of policies and the understanding of the problem?
- How to convince business people of possible mitigation measures needs/effectiveness?
  - Port 25 management, e-mail reputation, etc
- We had to research the problem and produce “neutral metrics”
  - SpamPots Project was created
  - 10 sensors (honeypots) were deployed in 5 broadband providers in Brazil (cable and ADSL)
  - We then had data to point to right countermeasures

Regular Meetings to Negotiate Countermeasures

- Port 25 Management in Brazil depends on a coordinated effort:
  - Telcos blocking outbound port 25 traffic
  - ISPs offering Message Submission services and changing their clients' configuration
- Text of a formal implementation agreement is being finished
- Waiting for Ministry of Justice to inform the level of involvement they'll have
- Anatel, Telcos and ISP Associations will sign the agreement
- Once the agreement is signed, NIC.br/CERT.br will start a national awareness campaign about
  - the importance of these measures
  - the impact on the consumers

Final Considerations

- More frequently than not, organizations only know there is a problem because someone shared information
- There are lots of examples of informal cooperation out there
- Every small step counts

Links

- CGI.br – Brazilian Internet Steering Committee
  http://www.cgi.br/
- NIC.br – Network Information Center Brazil
  http://www.nic.br/
- CERT.br – Computer Emergency Response Team Brazil
  http://www.cert.br/
- honeyTARG – honeypots for Threats and Abuse passive Reconnaissance and information Gathering
  http://honeytarg.cert.br/
- Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction
  http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf