The Brazilian Honeypots Alliance

Cristine Hoepers
General Manager
cristine@cert.br

Klaus Steding-Jessen
Technical Manager
jessen@cert.br

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

Questions Asked by the Organizers

- What motivated the project?
- What kind of data is collected?
- How is the data collected?
- What are the data sharing agreements or restrictions?
- How is the data used?

Agenda

- CERT.br mission and its relation with project's motivations
- The Brazilian Honeypots Alliance
- Architecture
- Data collection
- Data usage
- Benefits and challenges

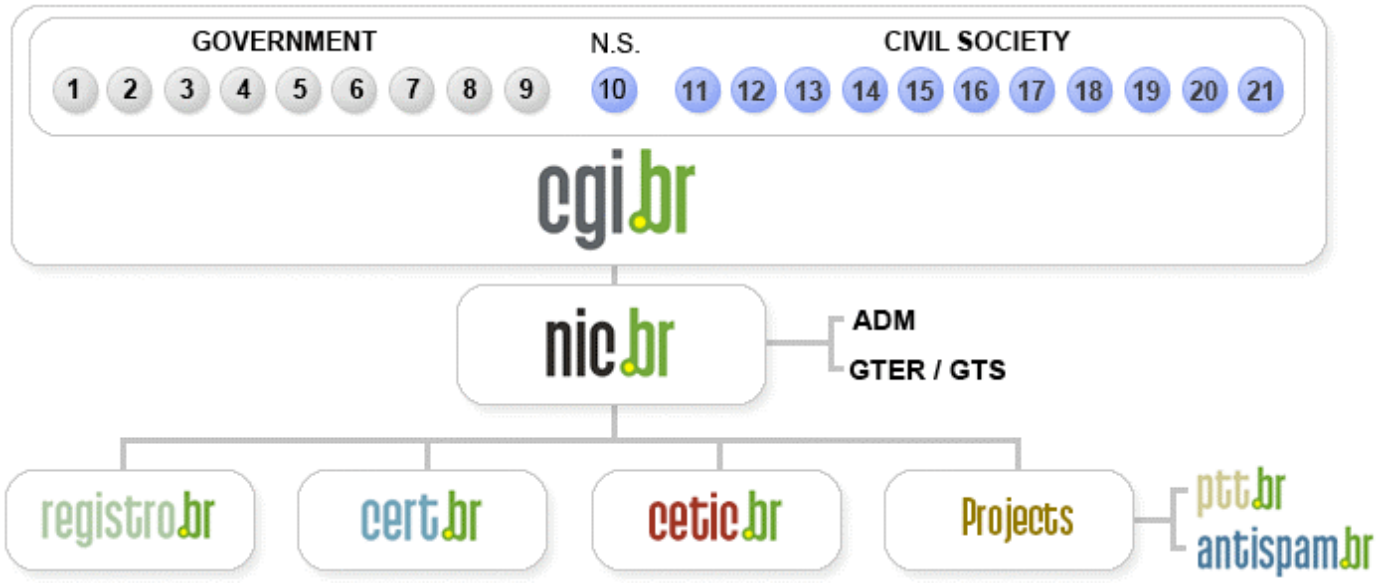
Our Parent Organization:
The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization that, among the diverse responsibilities, has 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/internacional/

Brazilian Internet Steering Committee (CGI.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 Mission

- Created in 1997 to *handle computer security incident reports and activities related to networks connected to the Internet in Brazil.*
  - National focal point for reporting security incidents
  - Establish collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling
  - Produce best practices' documents
  - Help raise the security awareness in the country

http://www.cert.br/mission.html

Brazilian Honeypots Alliance
Distributed Honeypots Project

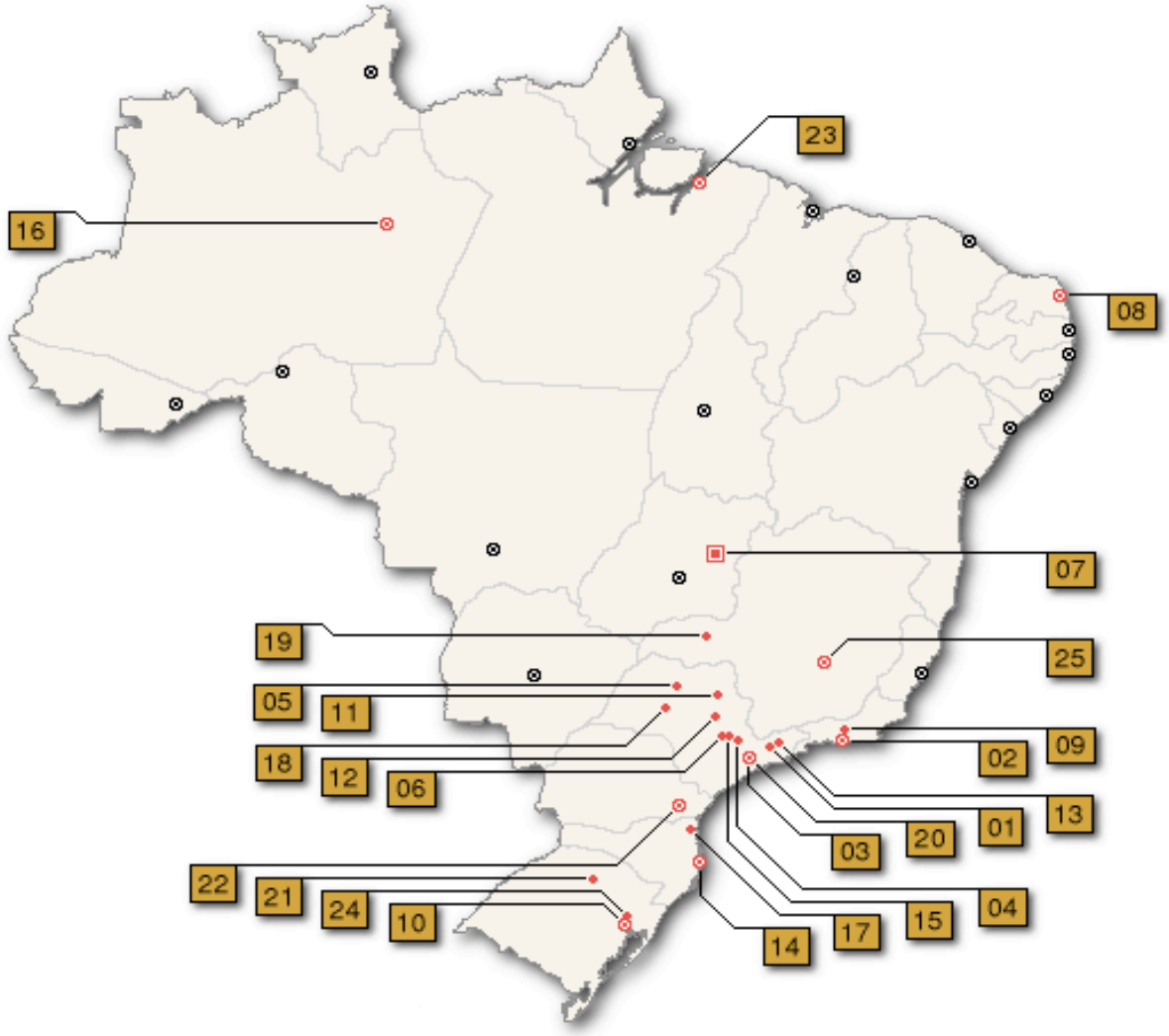
Main objective: to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 37 partner institutions:
  - Academic, government, industry, telecom and military networks
- Widely distributed across the country
- Based on voluntary work
- Maintain public statistics

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

- Honeynet Research Alliance Member since June 2002
  http://honeynet.org/alliance/

Cities Where the Honeypots are Located



Partner Institutions (April/2007)

#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-Rio, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, UOL, USP
04	Campinas	CenPRA, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministry of Justice, TCU, UNB LabRedes
08	Natal	UFRN
09	Petrópolis	LNCC
10	Porto Alegre	CERT-RS
11	Ribeirão Preto	USP
12	São Carlos	USP
13	Taubaté	UNITAU
14	Florianópolis	UFSC DAS
15	Americana	VIVAX
16	Manaus	VIVAX
17	Joinville	UDESC
18	Lins	FPTE
19	Uberlândia	CTBC Telecom
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	PoP-PR, PUC PR
23	Belém	UFPA
24	São Leopoldo	Unisinos
25	Belo Horizonte	Diveo

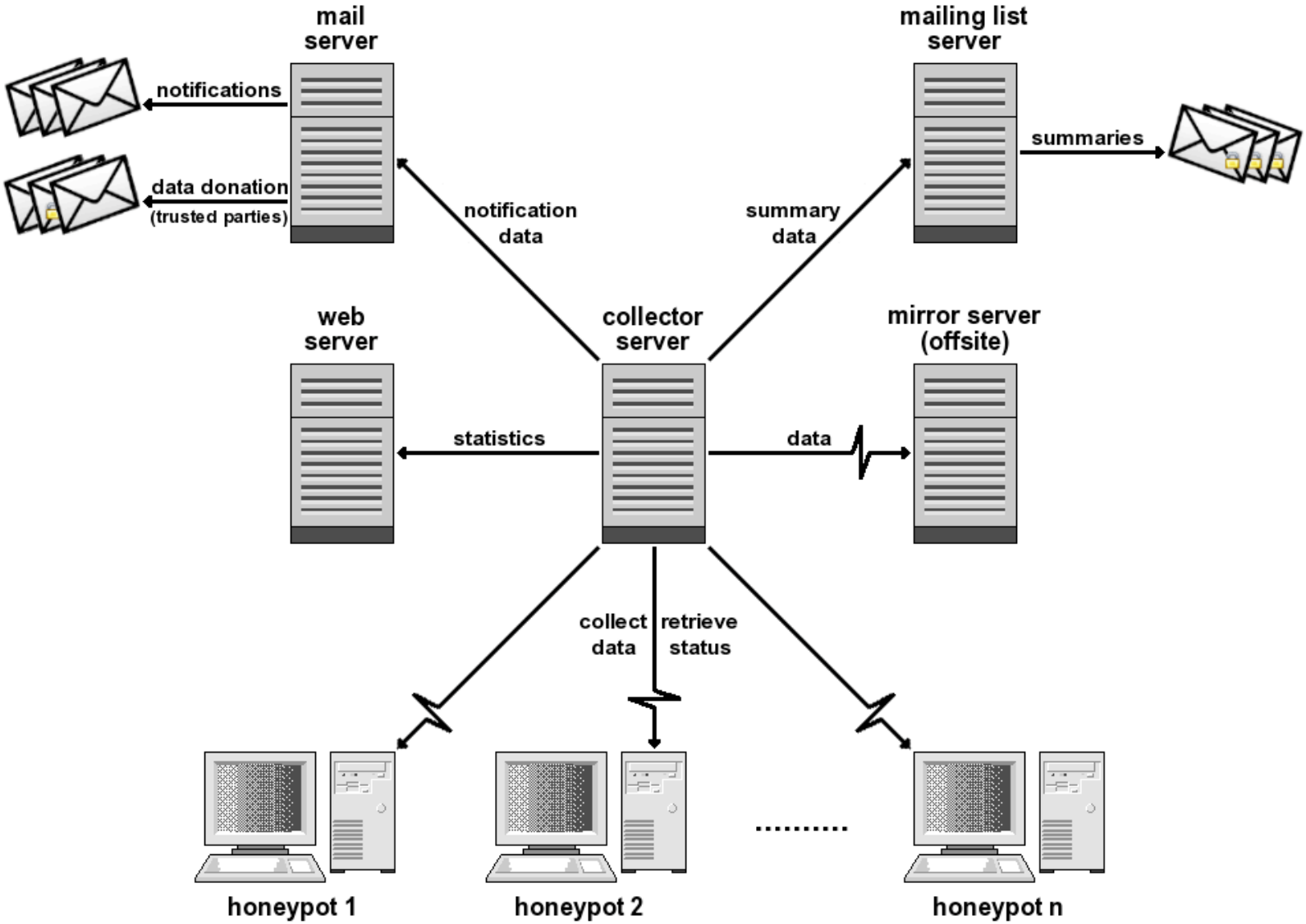
Main Characteristics of the Project

- Partners do not receive a “black box”
  - They have access to their honeypot
  - They can extend the honeypot’s configuration
- The honeypot does not capture production data
  - Only data directed to the honeypot is collected
- They can internally use the data captured by their own honeypot
  - As a complement to their IDS infrastructure
  - To detect infected machines, etc

Details of the Honeypots

- OpenBSD as the base Operating System (OS)
- Honeyd
  - Emulates different OSs
  - Runs listeners to emulate services (IIS, ssh, smtp, etc)
- Proxy arp using `arpd`
- Payload logged using `pf`
- Each honeypot uses a netblock range (from /28 to /24)
  - 1 management IP
  - Other IPs are used to emulate different OSs and services
- Ability to collect malware samples
  - Listeners developed for: mydoom, subseven, socks, ssh, etc.
- Ability to implement spam traps

Architecture



Relationship With the Partners (1/2)

- Partners are:
  - Other CSIRTs
  - Known incident reporters
  - Organizations that have attended our courses
  - Organizations introduced by trusted partners
- Partners provide:
  - Hardware
  - IP range
  - Time to configure/run the honeypot

Relationship With the Partners (2/2)

- CERT.br provides daily encrypted summaries to partners (without honeypots' IPs):
  - Activities seen in each honeypot
  - Combined activities seen in all honeypots
  - Correlations between activities seen in several honeypots
- Confidentiality issues:
  - Only coordination knows all the honeypots' locations
  - Coordination doesn't disclose the honeypots's location/address
  - Partners adhere to a Confidentiality Agreement:
    - Don't disclose the honeypot's location/address
    - Don't share any information without the coordination consent

CERT.br Use of Data

- Notification of Brazilian networks that are originating malicious activities seen in the honeypots
- Data donation to trusted parties
- Produce public statistics about current malicious activities
  - Very important to have a local view to compare with data collected by other projects (SANS Storm Center, Arakis, ISDAS, etc)

Other Benefits

- Allow members to improve their expertise in several areas:
  - Honeypots, intrusion detection, firewalls, OS hardening, PGP, etc
- Improve CERT.br relationship with the partners
  - Enhance trust
  - Create opportunities for new partnerships

Challenges to Maintain the Project

- Depend on partners' cooperation to maintain and update the honeypots
  - Harder to maintain than a "plug-and-play" honeypot
- The project becomes more difficult to manage as the number of honeypots grow
  - More people to coordinate with
  - PGP keys' management issues
  - Increasing need for resources (disk space, bandwidth, etc)
  - Some honeypots start to present hardware problems

References

- Brazilian Honeypots Alliance
  http://www.honeypots-alliance.org.br/

- Previous presentations about the project
  http://www.cert.br/presentations/

- Several papers presented at other conferences
  http://www.honeynet.org.br/papers/

- CERT.br
  http://www.cert.br/