Distributed Honeypots Project: How It's Being Useful for CERT.br

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

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

Brazilian Internet Steering Committee - CGI.br
http://www.cgi.br/

Agenda

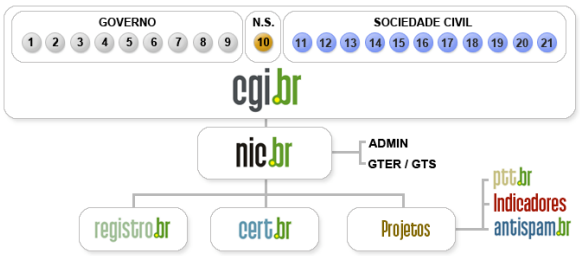
- CERT.br specific needs
  - Based on its mission and organizational structure
- The Distributed Honeypots Project
- Challenges and Requirements
- Benefits
- References

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

Among the diverse responsibilities of 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
- 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**

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

http://www.cgi.br/internacional/

CERT.br Mission

- Created in 1997 to *receive, review and respond to 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

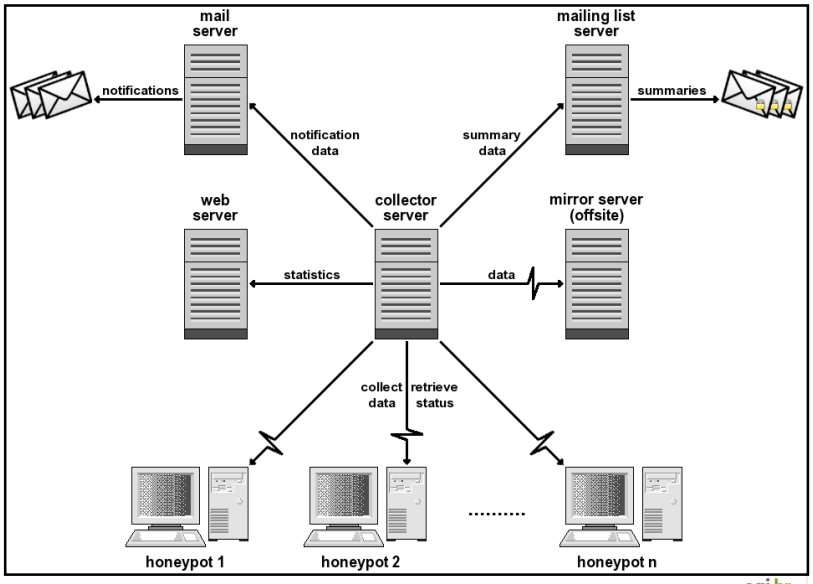
Brazilian Honeypots Alliance Distributed Honeypots Project

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
- 35 partner's 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/

Architecture

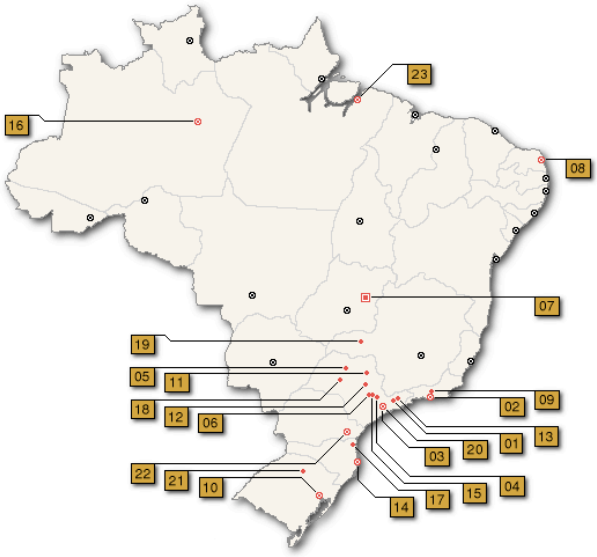


Details of the Honeypots

Currently we have 50 honeypots running:

- 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 use a netblock range (from /28 to /24)
  - 1 management IP
  - Other IPs are used to emulate the different OSs and services

Cities Where the Honeypots are Located



35 Partners of the Brazilian Honeypots Alliance

#	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, USP
04	Campinas	CenPRA, HP Brazil, 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
23	Belém	UFPA

Challenges and Requirements to Build the Network

Challenges to Find the Partners

- How to find the partners
  - Other CSIRTs
  - Known incident reporters
  - Attendees of our courses
  - People indicated by trusted partners
- After finding them, we need to convince them
  - Why they should place a honeypot in their network
  - What are the advantages that they have in sharing the information with us

Key Points to Reach and Keep a Partner

- We are not offering a “black box”
  - They have access to their honeypot
  - They can extend the honeypot configuration
- The honeypot does not capture production data
  - Only data directed to the honeypot is collected
- They can use their data freely
  - For example, as a complement to their IDS infrastructure

Key Points to Reach and Keep a Partner (2)

- We provide specific information to partners
  - Daily summaries (with honeypots’ IPs sanitized)
    - Activities seen in each honeypot
    - Combined activities seen in all honeypots
    - Correlations between activities seen in several honeypots
- All information is exchanged using an encripted mailing list

Challenges to Maintain the Project

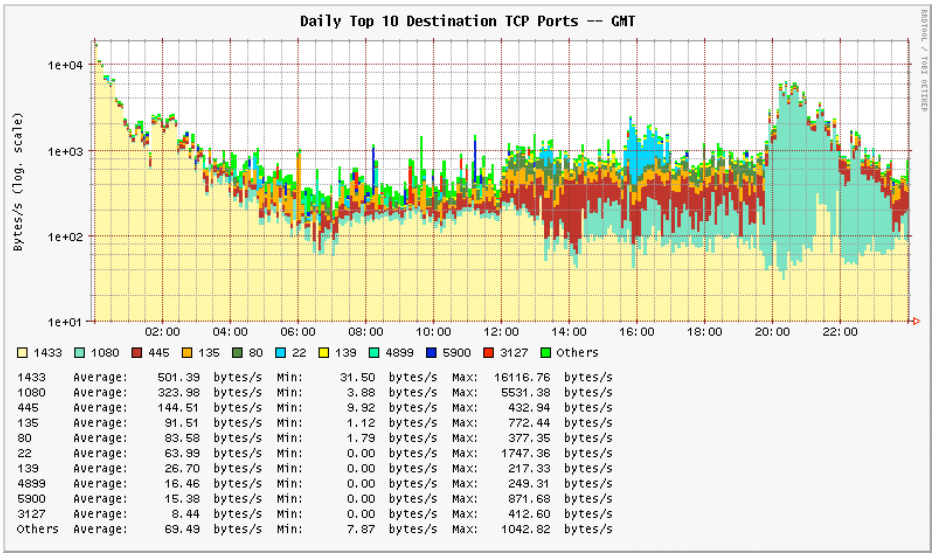
- Depend on partners' cooperation to maintain and update the honeypots
  - Harder to maintain than a "plug and play" honeypot
- The project becomes more difficult to manage as the number of honeypots grow
  - More people to coordinate with
  - PGP keys' management issues
  - Need for resources increase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

Benefits of the Project

Short Term Benefits

- Notification of networks that are originating malicious activities seen in the honeypots
- Ability to collect malware samples
  - Listeners developed for: mydoom, subseven, socks, ssh, etc.
- Ability to implement spam traps
- Produce statistics about current malicious activities
  - Very important to have a local view to compare with data collected by other projects

Public Statistics: Honeypots Flows



May 17, 2006 - http://www.honeypots-alliance.org.br/stats/

Long Term 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
  - Increase the trust
  - Create opportunities for new partnerships

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/