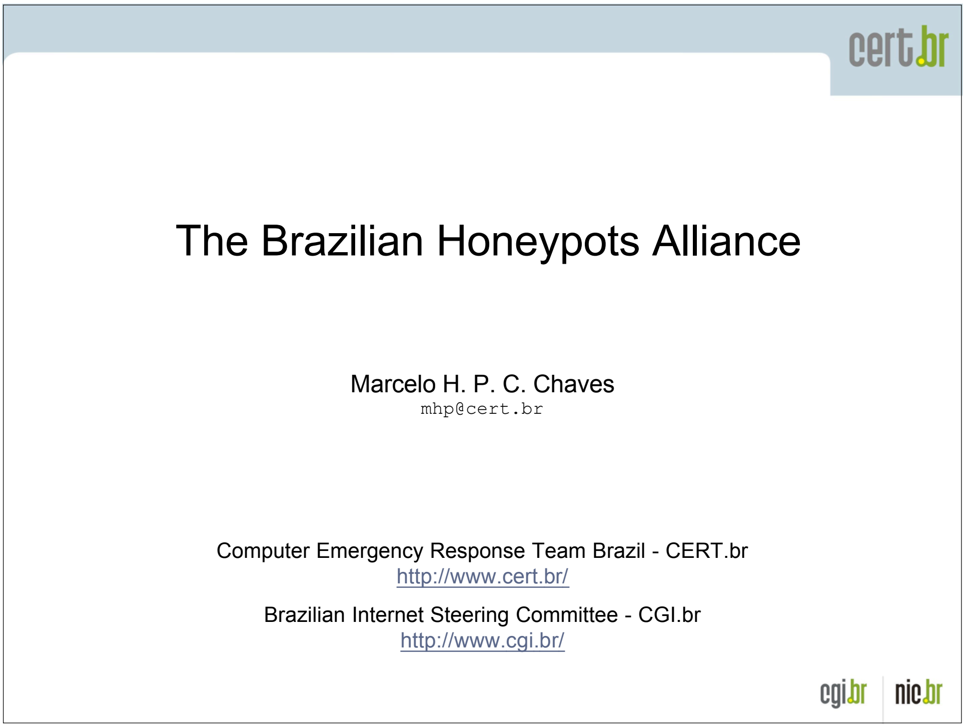
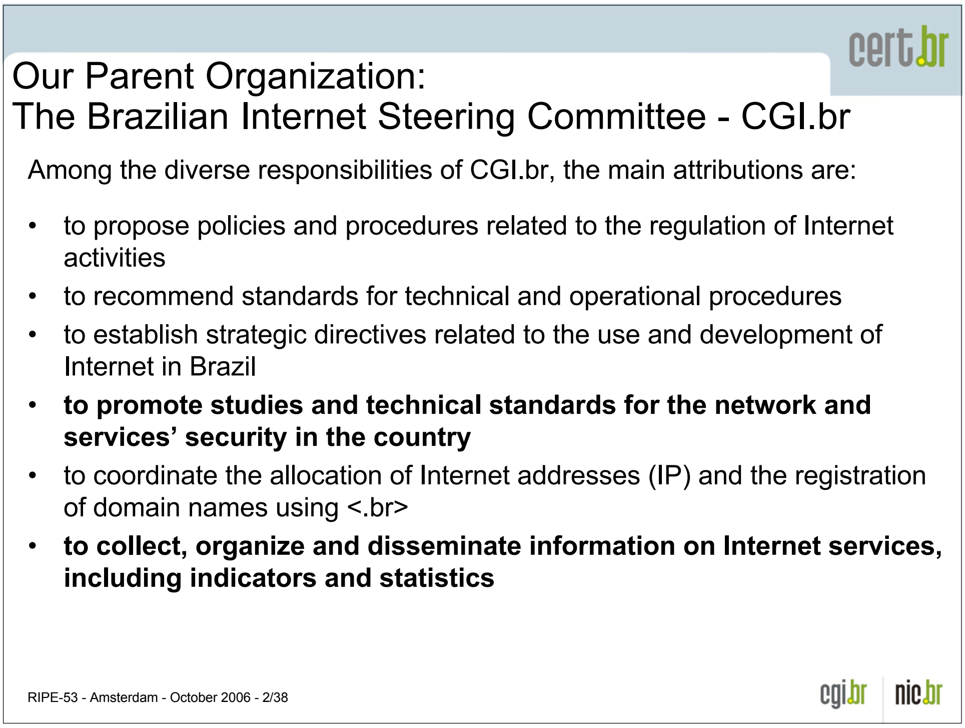


The Brazilian Honeypots Alliance

Marcelo H. P. C. Chaves
mhp@cert.br

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

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

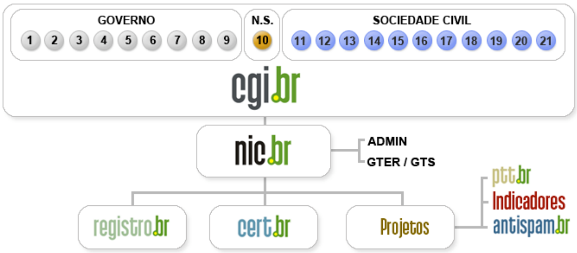


Our Parent Organization: The Brazilian Internet Steering Committee - CGI.br

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

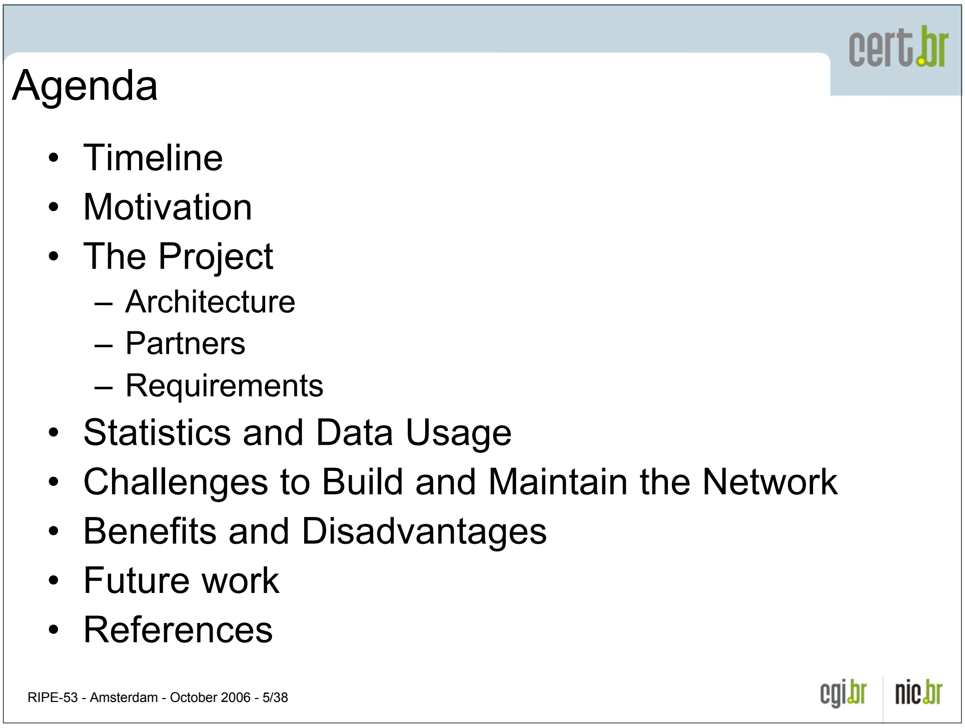
11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 –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

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

CERT.br Mission

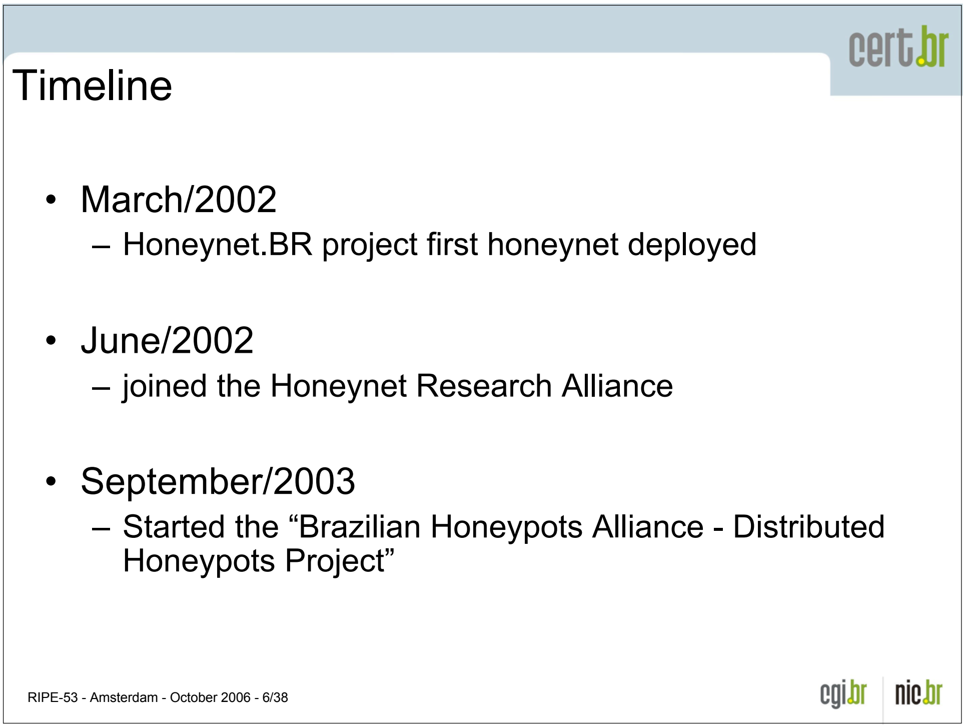
- Created in 1997 to *receive, review and respond to computer security incident reports and activities related to networks connected to the Internet in Brazil.*
  – National focal point for reporting security incidents
  – Establish collaborative relationships with other entities
  – Help new CSIRTs 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



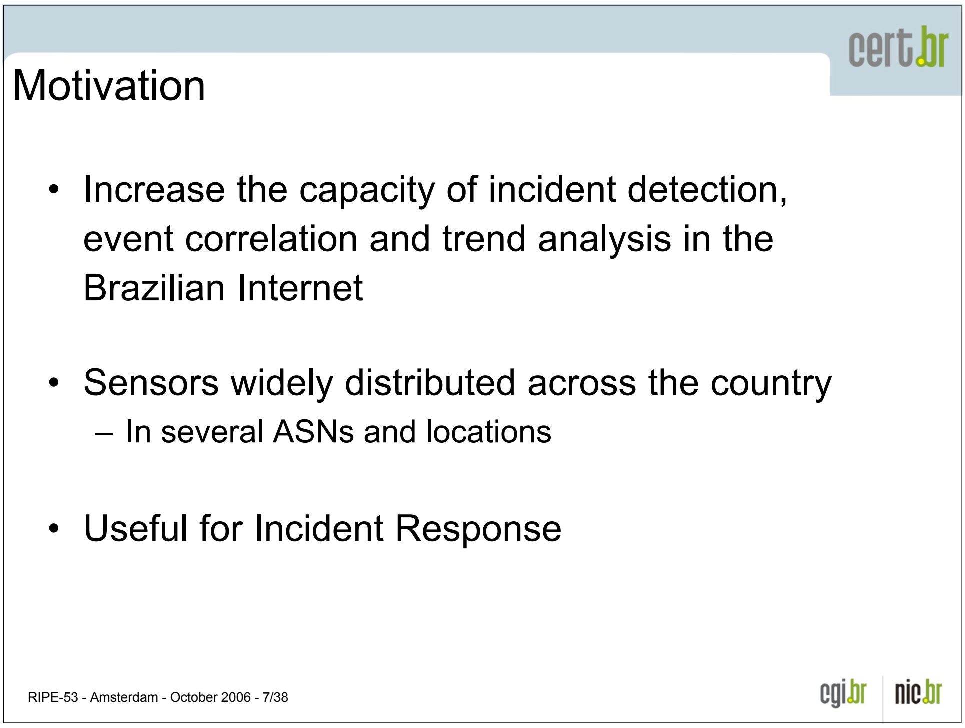
Agenda

- Timeline
- Motivation
- The Project
  - Architecture
  - Partners
  - Requirements
- Statistics and Data Usage
- Challenges to Build and Maintain the Network
- Benefits and Disadvantages
- Future work
- References



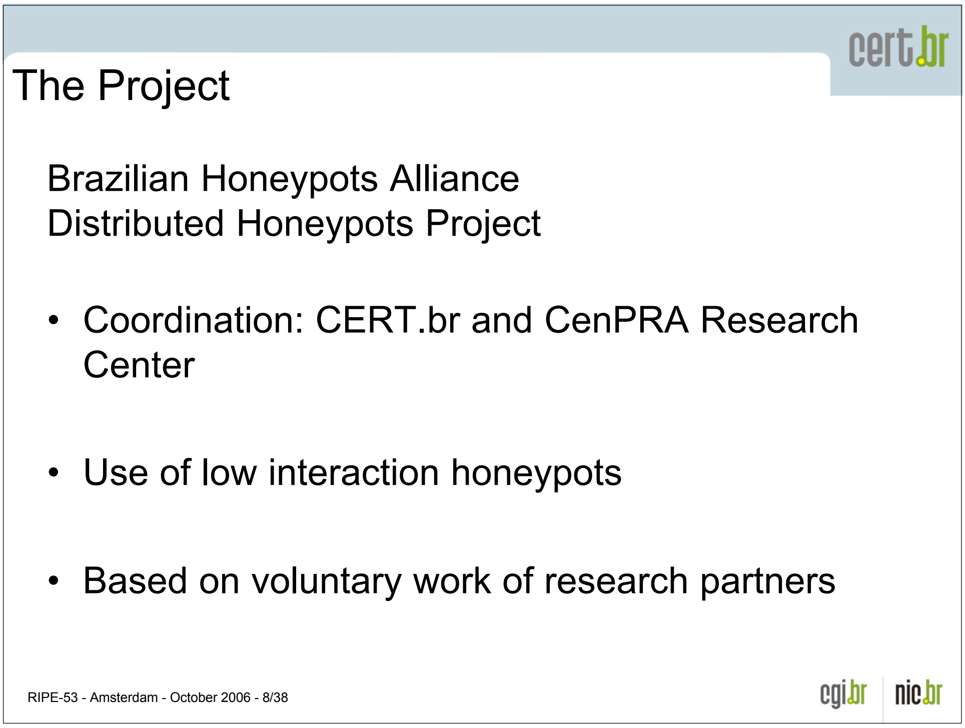
Timeline

- March/2002
  - Honeynet.BR project first honeynet deployed
- June/2002
  - joined the Honeynet Research Alliance
- September/2003
  - Started the “Brazilian Honeypots Alliance - Distributed Honeypots Project”



Motivation

- Increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet
- Sensors widely distributed across the country
  - In several ASNs and locations
- Useful for Incident Response

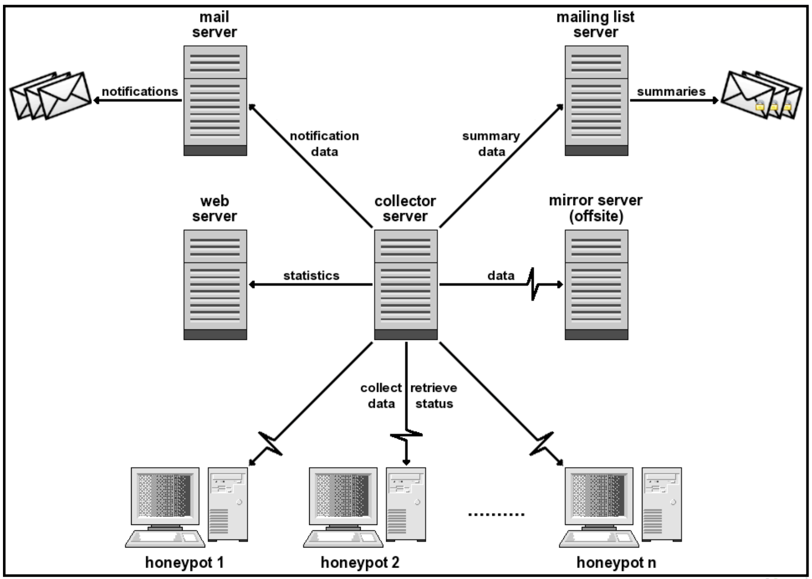


The Project

Brazilian Honeypots Alliance
Distributed Honeypots Project

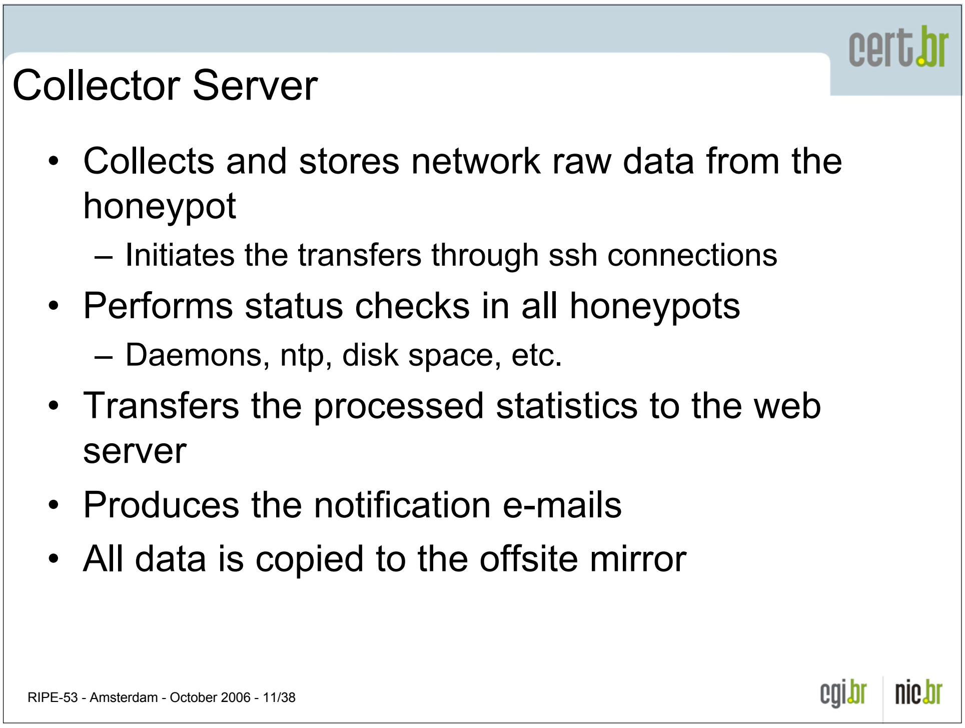
- Coordination: CERT.br and CenPRA Research Center
- Use of low interaction honeypots
- Based on voluntary work of research partners

Architecture



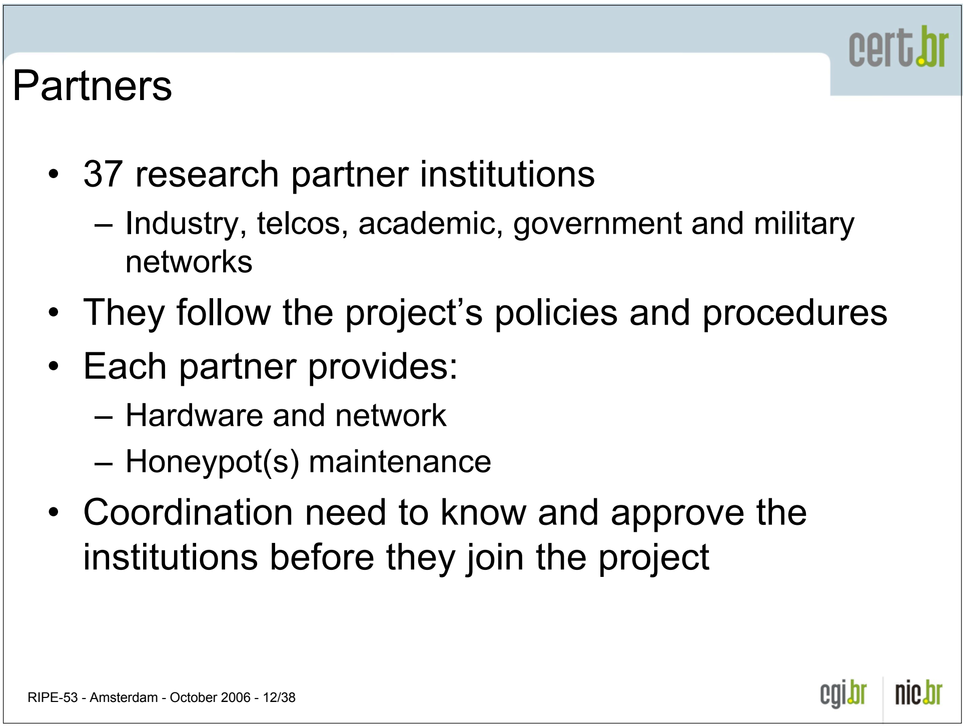
Low Interaction Honeypots

- OpenBSD as the base Operating System (OS)
- Honeyd
  - Emulates different OSs
  - Runs listeners to emulate services (IIS, ssh, sendmail, etc)
- Proxy arp using `arpd`
- Payload logged using `pf`
- Use a netblock range (from /28 to /24)
  - 1 management IP
  - Other IPs are used to emulate the different OSs and services



Collector Server

- Collects and stores network raw data from the honeypot
  - Initiates the transfers through ssh connections
- Performs status checks in all honeypots
  - Daemons, ntp, disk space, etc.
- Transfers the processed statistics to the web server
- Produces the notification e-mails
- All data is copied to the offsite mirror



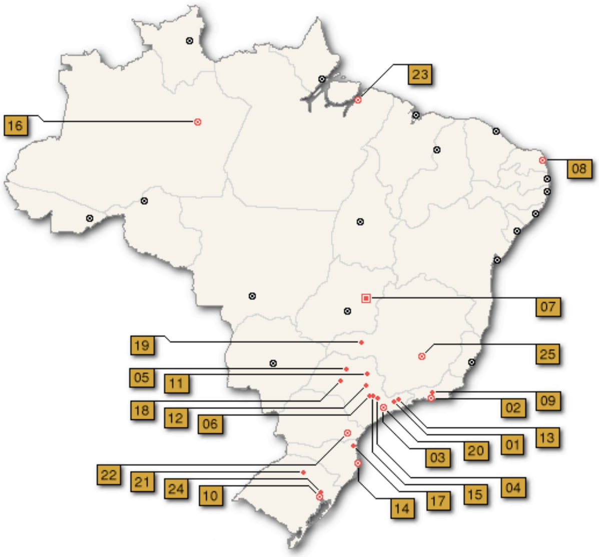
Partners

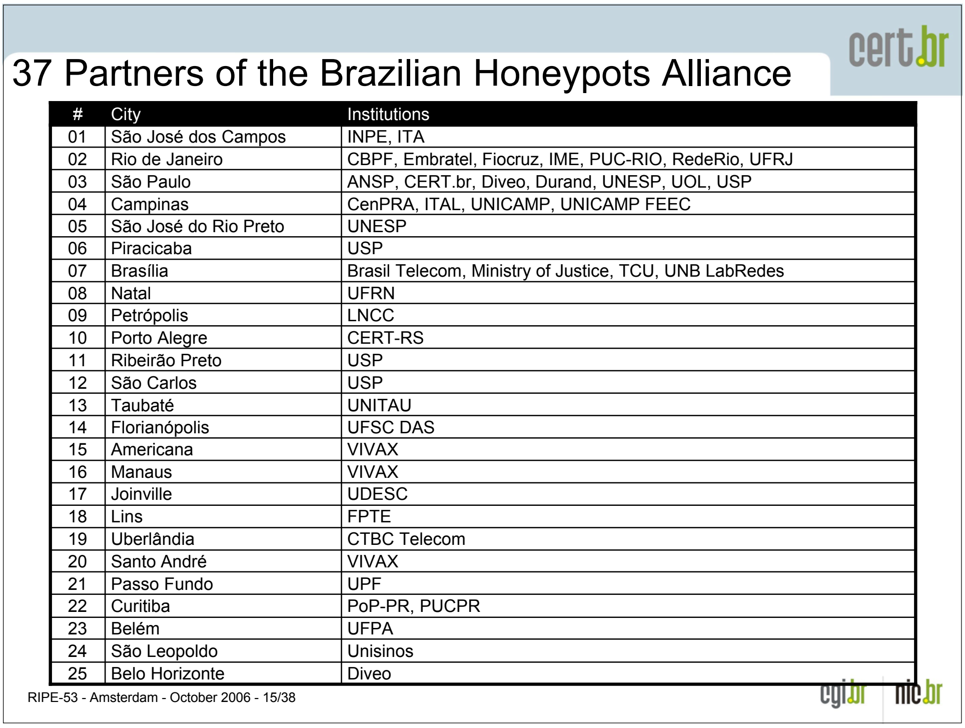
- 37 research partner institutions
  - Industry, telcos, academic, government and military networks
- They follow the project's policies and procedures
- Each partner provides:
  - Hardware and network
  - Honeypot(s) maintenance
- Coordination need to know and approve the institutions before they join the project

Partner Requirements

- Follow the project’s standards (OS, basic secure configuration, updates, etc)
- No data pollution
- Permit all traffic to/from the honeypot
- Don’t disclose IP/network
  - All network and IP information must be sanitized
- Don’t collect production traffic
- Don’t exchange any information in clear text

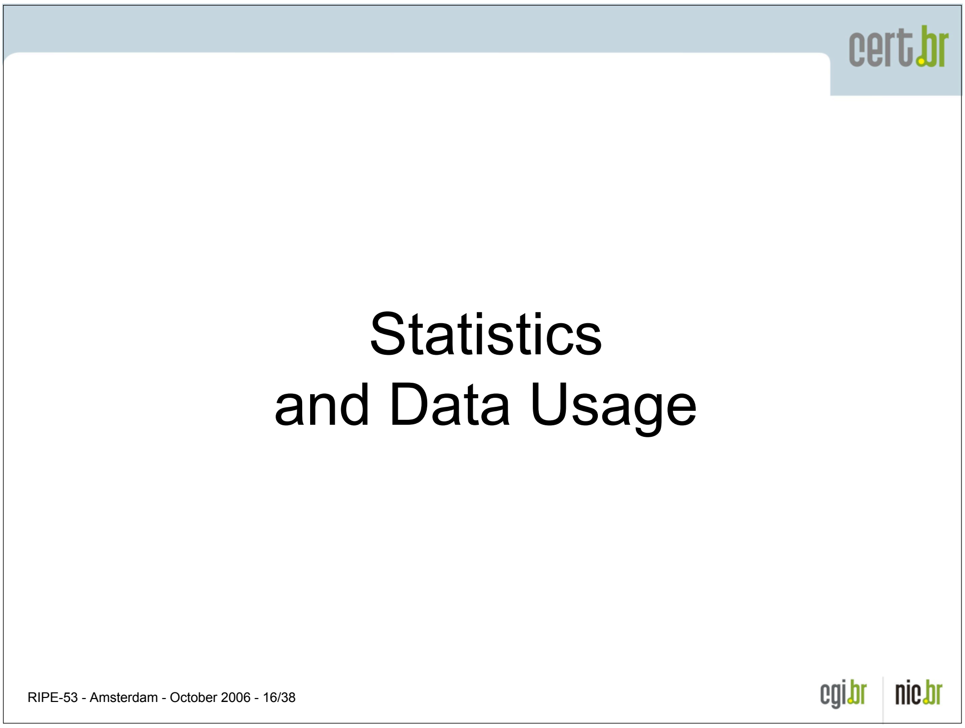
Cities Where the Honeypots are Located



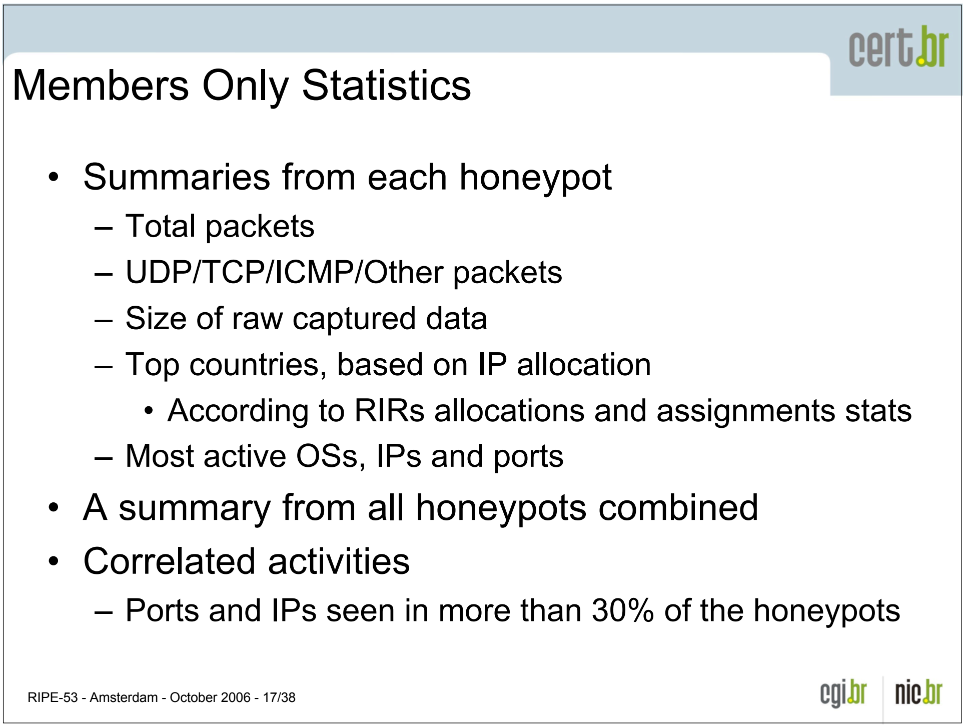


37 Partners of the Brazilian Honeypots Alliance

#	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, 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, PUCPR
23	Belém	UFPA
24	São Leopoldo	Unisinos
25	Belo Horizonte	Diveo

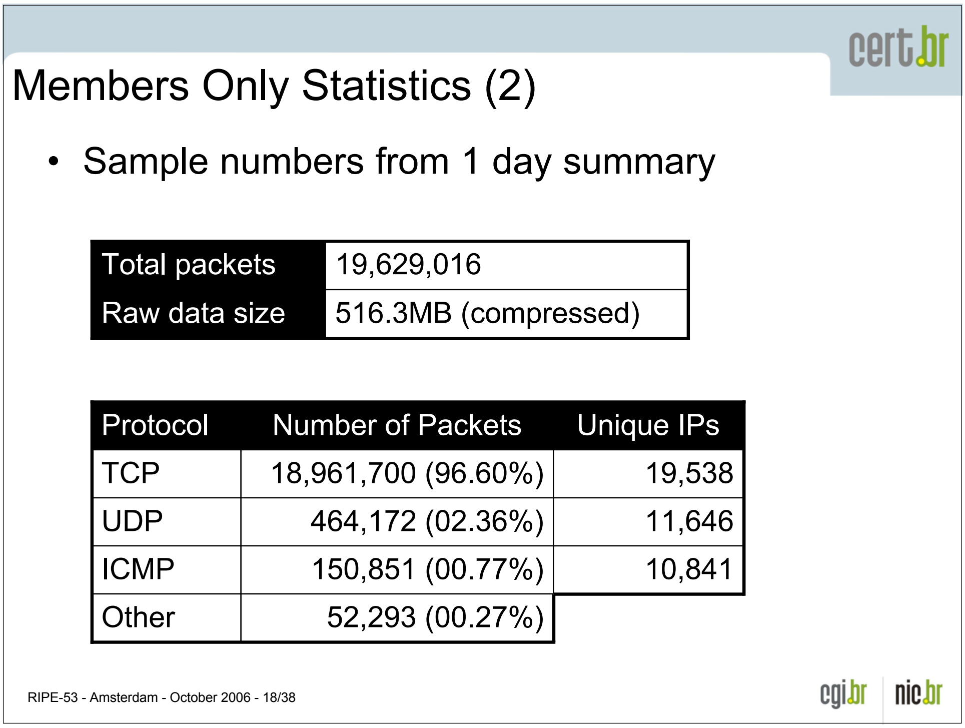


Statistics and Data Usage



Members Only Statistics

- Summaries from each honeypot
  - Total packets
  - UDP/TCP/ICMP/Other packets
  - Size of raw captured data
  - Top countries, based on IP allocation
    - According to RIRs allocations and assignments stats
  - Most active OSs, IPs and ports
- A summary from all honeypots combined
- Correlated activities
  - Ports and IPs seen in more than 30% of the honeypots



Members Only Statistics (2)

- Sample numbers from 1 day summary

Total packets	19,629,016
Raw data size	516.3MB (compressed)

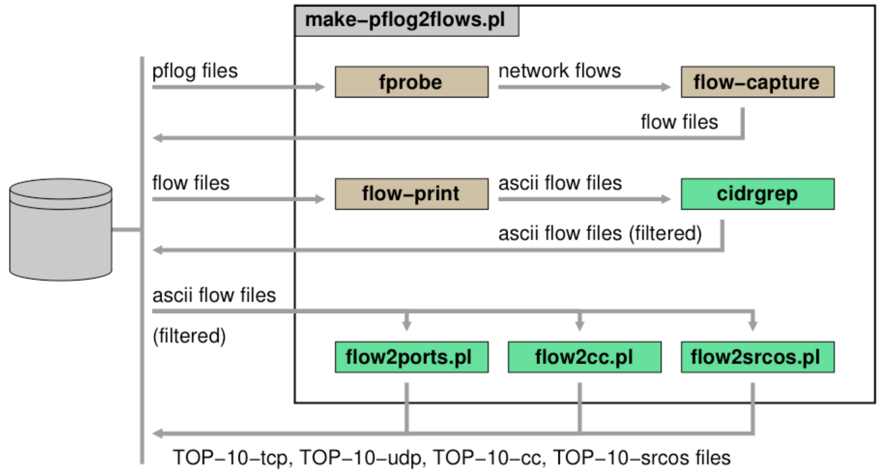
Protocol	Number of Packets	Unique IPs
TCP	18,961,700 (96.60%)	19,538
UDP	464,172 (02.36%)	11,646
ICMP	150,851 (00.77%)	10,841
Other	52,293 (00.27%)	

Public Statistics

- Flows from data collected in all honeypots
- Most active OSs, TCP/UDP ports and countries
  - Packets/s and bytes/s
  - Daily and 4-hour periods
- Available at:

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

Public Statistics Generation



make–pflog2flows.pl

pflog files

fprobe

network flows

flow–capture

flow files

flow files

flow–print

ascii flow files

cidrgrep

ascii flow files (filtered)

ascii flow files

(filtered)

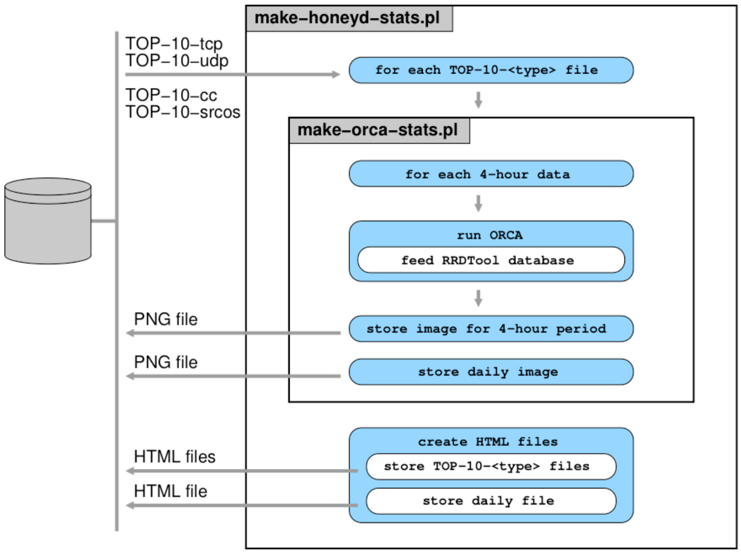
flow2ports.pl

flow2cc.pl

flow2srcos.pl

TOP–10–tcp, TOP–10–udp, TOP–10–cc, TOP–10–srcos files

Public Statistics Generation (2)



make–honeyd–stats.pl

TOP–10–tcp
TOP–10–udp

TOP–10–cc
TOP–10–srcos

for each TOP–10–<type> file

make–orca–stats.pl

for each 4–hour data

run ORCA

feed RRDTool database

PNG file

store image for 4–hour period

PNG file

store daily image

HTML files

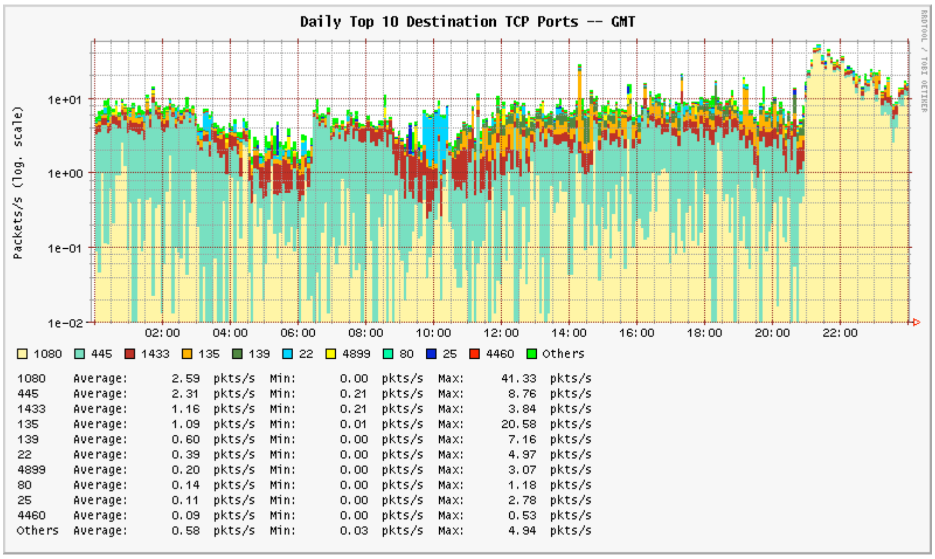
create HTML files

store TOP–10–<type> files

HTML file

store daily file

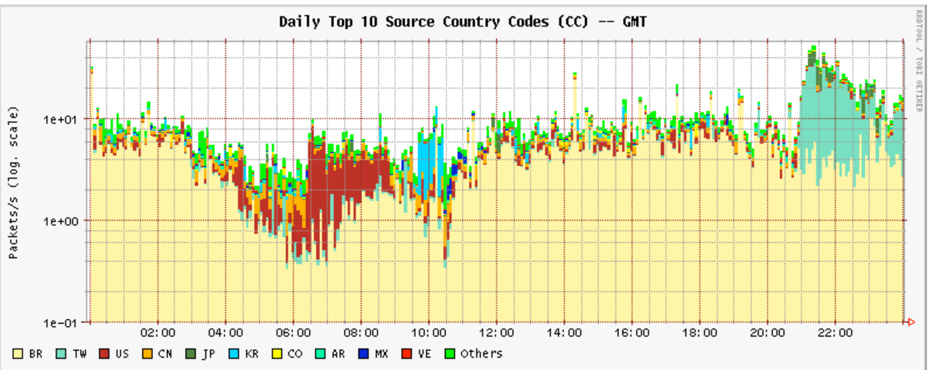
Public Stats (honeypots flows): Top TCP Ports



```
1080    Average:     2.59  pkts/s  Min:     0.00  pkts/s  Max:    41.33  pkts/s
445     Average:     2.31  pkts/s  Min:     0.21  pkts/s  Max:     8.76  pkts/s
1433    Average:     1.16  pkts/s  Min:     0.21  pkts/s  Max:     3.84  pkts/s
135     Average:     1.09  pkts/s  Min:     0.01  pkts/s  Max:    20.58  pkts/s
139     Average:     0.60  pkts/s  Min:     0.00  pkts/s  Max:     7.16  pkts/s
22      Average:     0.39  pkts/s  Min:     0.00  pkts/s  Max:     4.97  pkts/s
4899    Average:     0.20  pkts/s  Min:     0.00  pkts/s  Max:     3.07  pkts/s
80      Average:     0.14  pkts/s  Min:     0.00  pkts/s  Max:     1.18  pkts/s
25      Average:     0.11  pkts/s  Min:     0.00  pkts/s  Max:     2.78  pkts/s
4460    Average:     0.09  pkts/s  Min:     0.00  pkts/s  Max:     0.53  pkts/s
Others  Average:     0.58  pkts/s  Min:     0.03  pkts/s  Max:     4.94  pkts/s
```

August 21, 2006 - http://www.honeypots-alliance.org.br/stats/

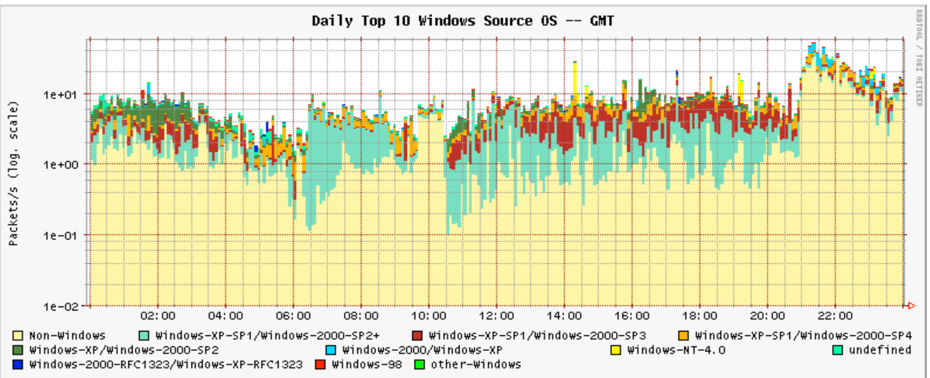
Public Stats (honeypots flows): Top CC



```
BR      Average:      4.43  pkts/s  Min:      0.34  pkts/s  Max:     28.32  pkts/s
TW      Average:      2.03  pkts/s  Min:      0.00  pkts/s  Max:     30.06  pkts/s
US      Average:      0.88  pkts/s  Min:      0.04  pkts/s  Max:      7.65  pkts/s
CN      Average:      0.60  pkts/s  Min:      0.17  pkts/s  Max:      2.81  pkts/s
JP      Average:      0.45  pkts/s  Min:      0.00  pkts/s  Max:     12.68  pkts/s
KR      Average:      0.30  pkts/s  Min:      0.00  pkts/s  Max:      4.36  pkts/s
CO      Average:      0.16  pkts/s  Min:      0.00  pkts/s  Max:      2.05  pkts/s
AR      Average:      0.15  pkts/s  Min:      0.00  pkts/s  Max:      1.30  pkts/s
MX      Average:      0.11  pkts/s  Min:      0.00  pkts/s  Max:      2.32  pkts/s
VE      Average:      0.11  pkts/s  Min:      0.01  pkts/s  Max:      0.68  pkts/s
Others  Average:      0.85  pkts/s  Min:      0.04  pkts/s  Max:      4.47  pkts/s
```

August 21, 2006 - http://www.honeypots-alliance.org.br/stats/

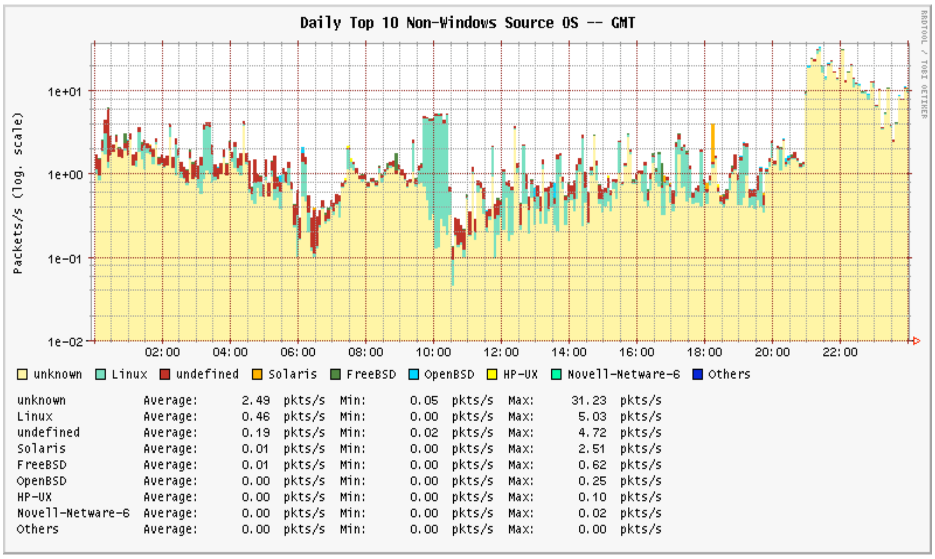
Public Stats (honeypots flows): Top Win Src.OS



```
Non-Windows                              Average:    2.98  pkts/s  Min:     0.10  pkts/s  Max:    33.54  pkts/s
Windows-XP-SP1/Windows-2000-SP2+         Average:    1.89  pkts/s  Min:     0.11  pkts/s  Max:    11.37  pkts/s
Windows-XP-SP1/Windows-2000-SP3          Average:    1.51  pkts/s  Min:     0.01  pkts/s  Max:     8.11  pkts/s
Windows-XP-SP1/Windows-2000-SP4          Average:    1.11  pkts/s  Min:     0.12  pkts/s  Max:     9.74  pkts/s
Windows-XP/Windows-2000-SP2              Average:    0.90  pkts/s  Min:     0.00  pkts/s  Max:    11.26  pkts/s
Windows-2000/Windows-XP                  Average:    0.42  pkts/s  Min:     0.00  pkts/s  Max:    12.77  pkts/s
Windows-NT-4.0                           Average:    0.20  pkts/s  Min:     0.00  pkts/s  Max:    17.83  pkts/s
undefined                                Average:    0.19  pkts/s  Min:     0.02  pkts/s  Max:     4.72  pkts/s
Windows-2000-RFC1323/Windows-XP-RFC1323  Average:    0.03  pkts/s  Min:     0.00  pkts/s  Max:     2.60  pkts/s
Windows-98                               Average:    0.02  pkts/s  Min:     0.00  pkts/s  Max:     2.53  pkts/s
other-Windows                            Average:    0.00  pkts/s  Min:     0.00  pkts/s  Max:     0.08  pkts/s
```

August 21, 2006 - http://www.honeypots-alliance.org.br/stats/

Public Stats (honeypots flows): Top Non-Win Src.OS

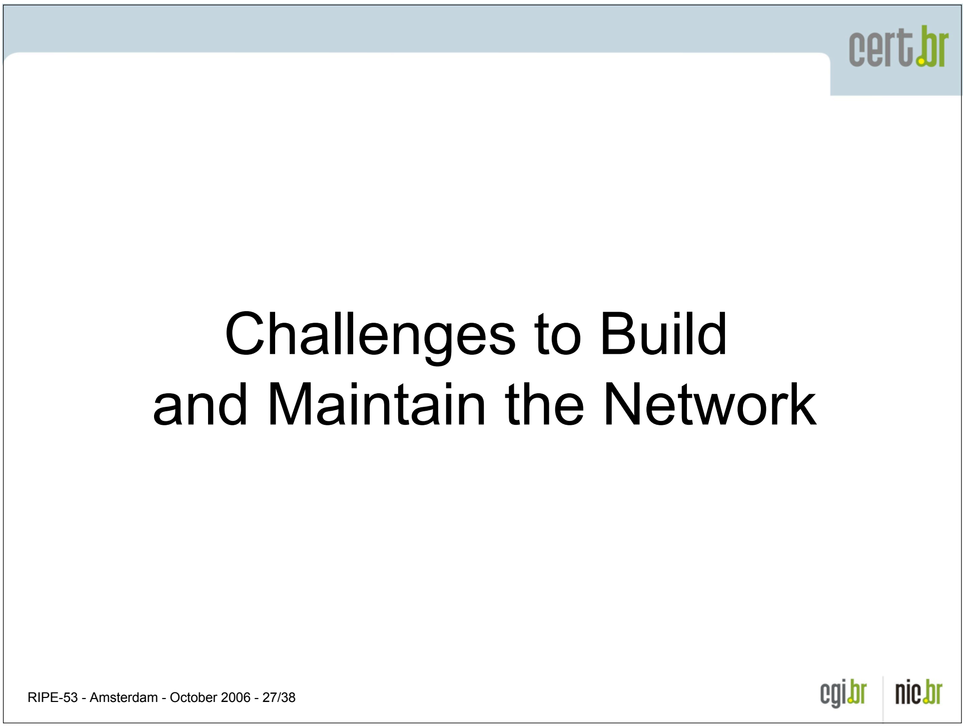


```
unknown          Average:    2.49  pkts/s  Min:    0.05  pkts/s  Max:    31.23  pkts/s
Linux            Average:    0.46  pkts/s  Min:    0.00  pkts/s  Max:     5.03  pkts/s
undefined        Average:    0.19  pkts/s  Min:    0.02  pkts/s  Max:     4.72  pkts/s
Solaris          Average:    0.01  pkts/s  Min:    0.00  pkts/s  Max:     2.51  pkts/s
FreeBSD          Average:    0.01  pkts/s  Min:    0.00  pkts/s  Max:     0.62  pkts/s
OpenBSD          Average:    0.00  pkts/s  Min:    0.00  pkts/s  Max:     0.25  pkts/s
HP-UX            Average:    0.00  pkts/s  Min:    0.00  pkts/s  Max:     0.10  pkts/s
Novell-Netware-6 Average:    0.00  pkts/s  Min:    0.00  pkts/s  Max:     0.02  pkts/s
Others           Average:    0.00  pkts/s  Min:    0.00  pkts/s  Max:     0.00  pkts/s
```

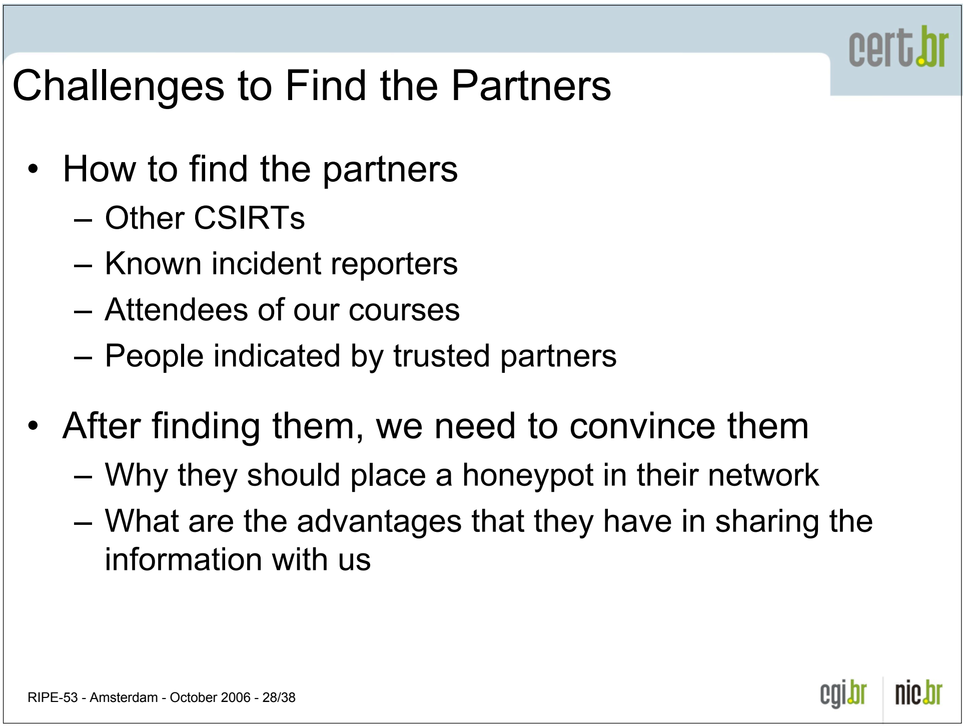
August 21, 2006 - http://www.honeypots-alliance.org.br/stats/

Data Usage

- Partners:
  - Observe trends and scans for new vulnerabilities
  - Detect promptly:
    - Outbreaks of new worms/bots
    - Compromised servers
    - Network configuration errors
- Incident response (CERT.br):
  - Identify well known malicious/abuse activities
    - Worms, bots, scans, spams and malware in general
  - Notify the Brazilian networks’ contacts
    - including recovery tips

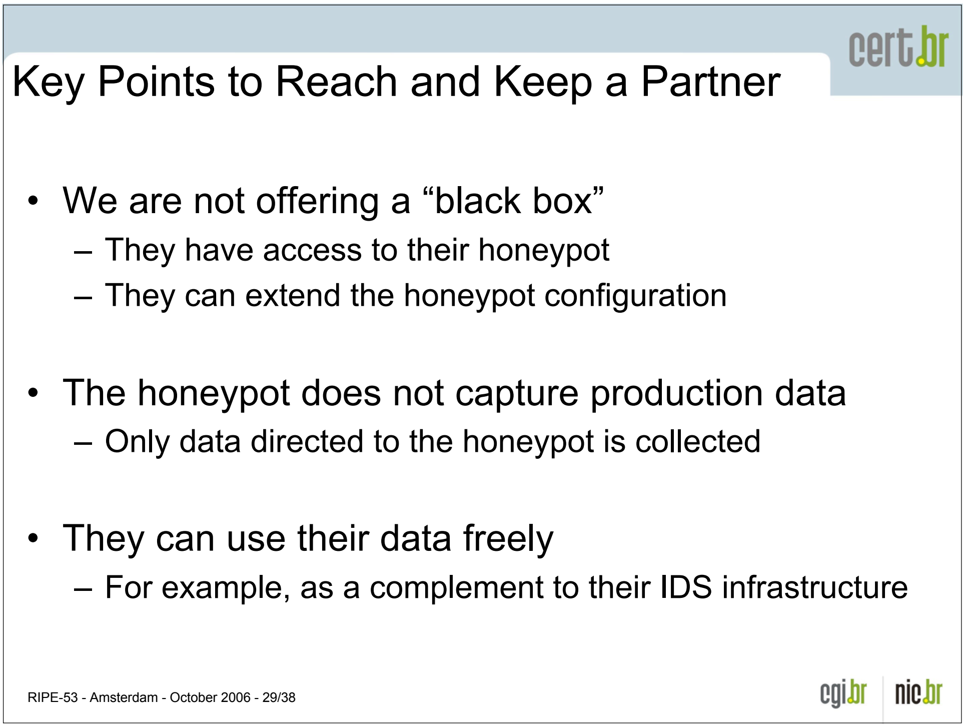


Challenges to Build and Maintain the Network



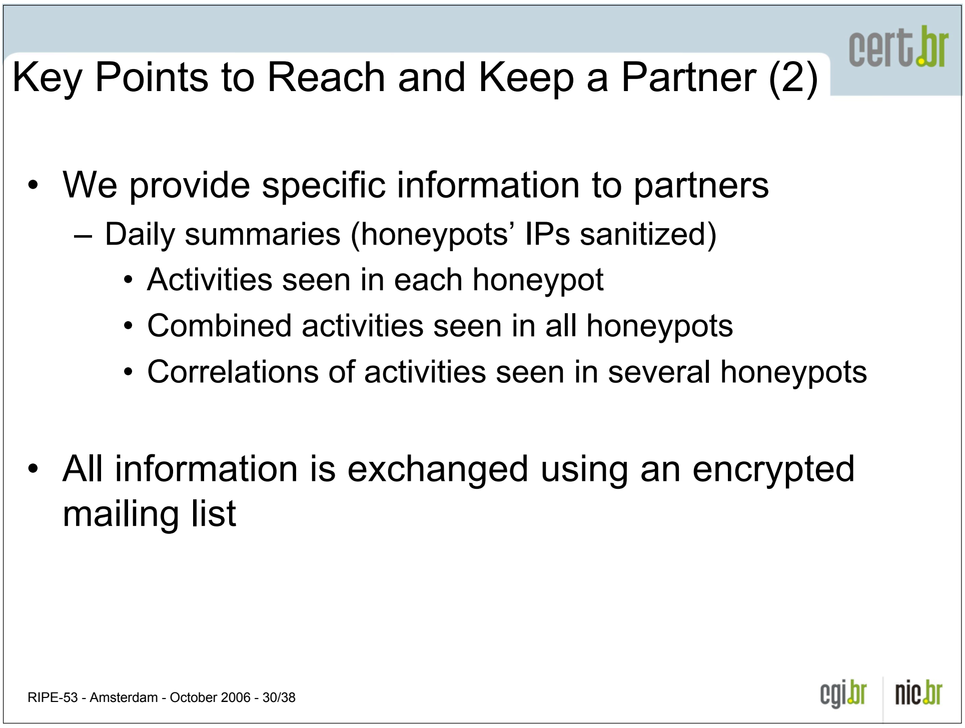
Challenges to Find the Partners

- 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



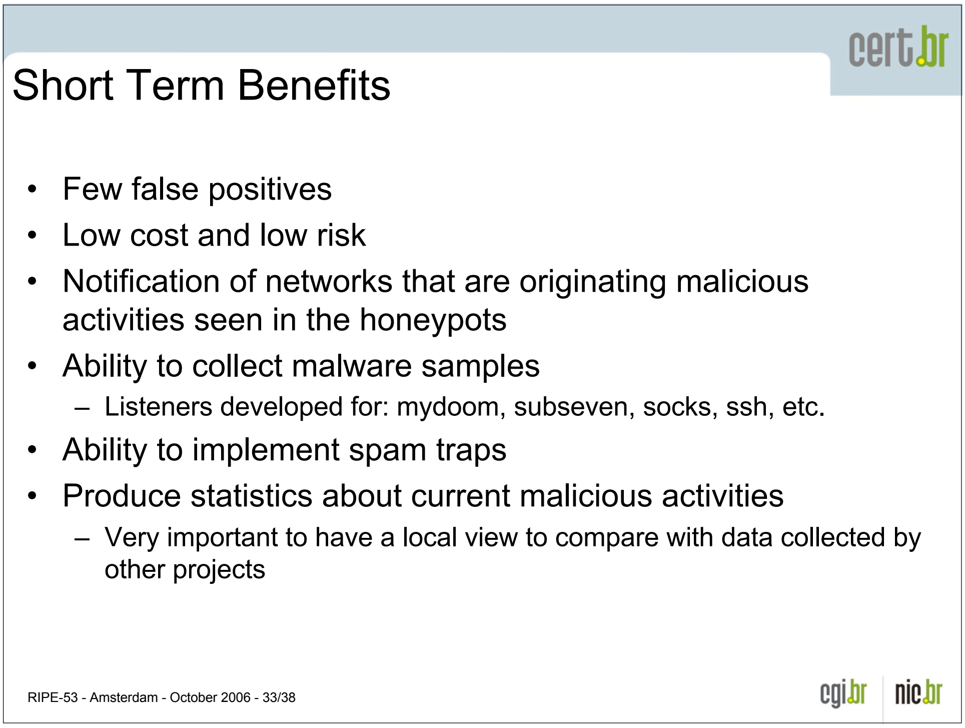
Key Points to Reach and Keep a Partner (2)

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

Challenges to Maintain the Project

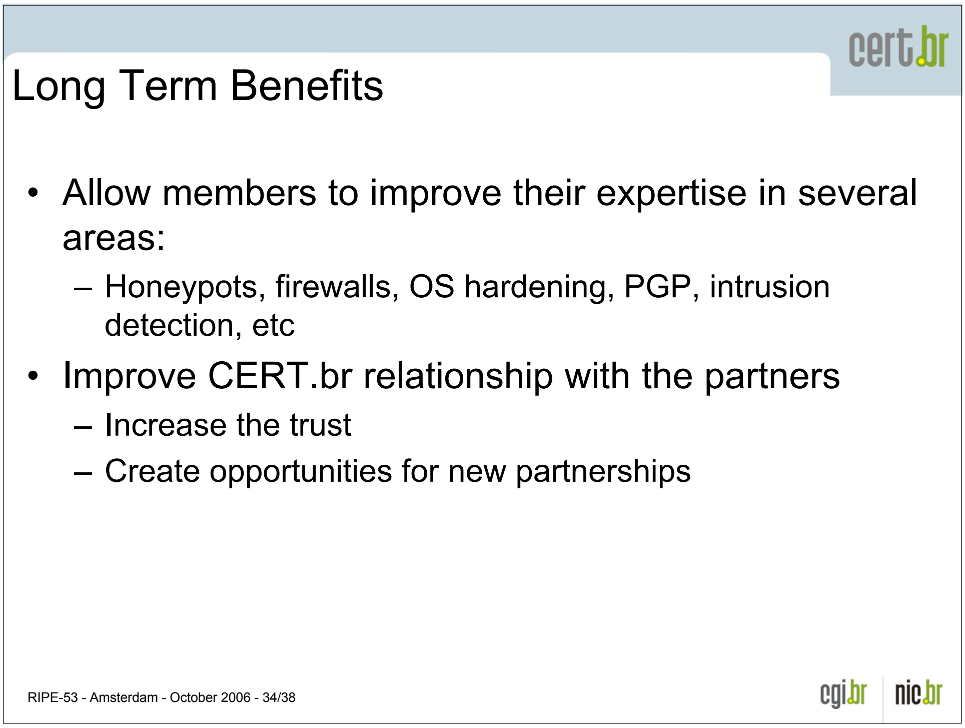
- Depend on partners' cooperation to maintain and update the honeypots
  - Harder to maintain than a "plug and play" honeypot
- The project becomes more difficult to manage as the number of honeypots grow
  - More people to coordinate with
  - PGP keys' management issues
  - More resources needed (disk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

Benefits of the Project and Disavantages of the Architecture



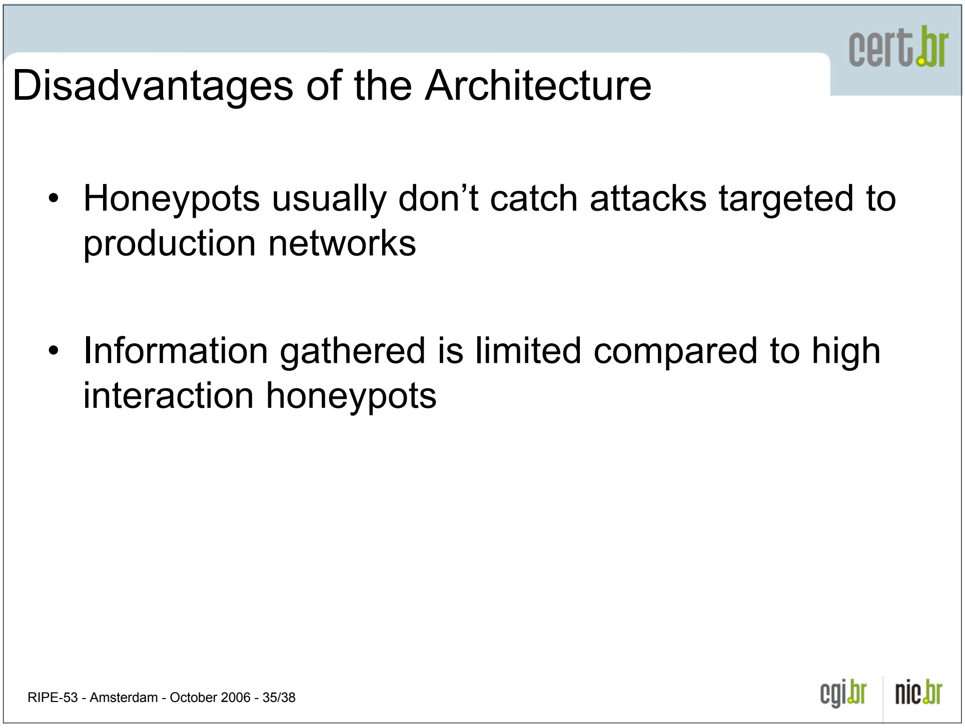
Short Term Benefits

- Few false positives
- Low cost and low risk
- 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



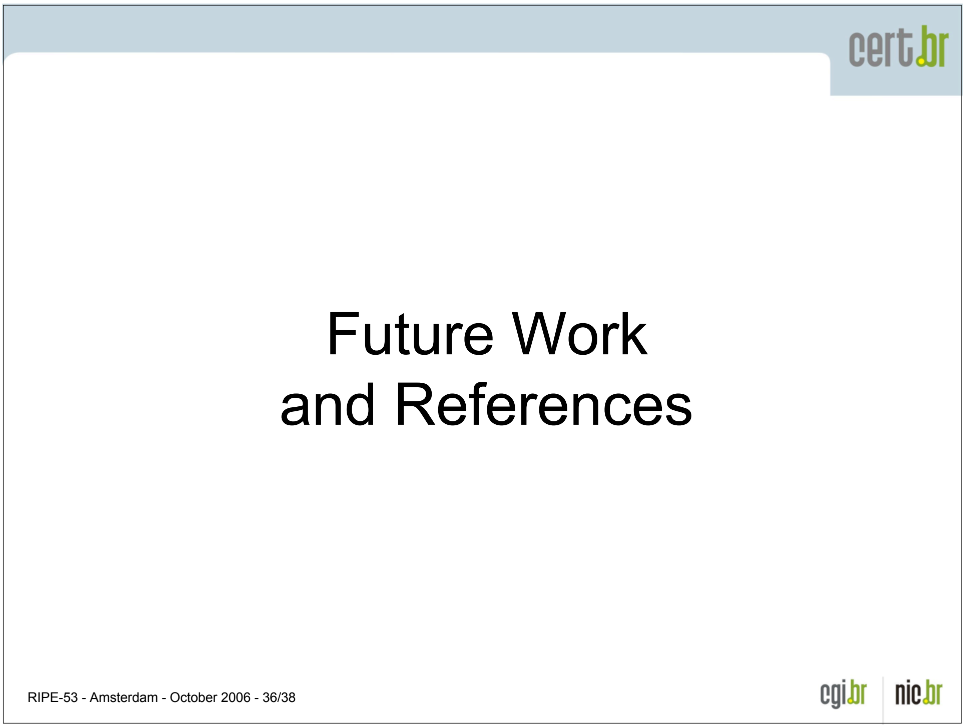
Long Term Benefits

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

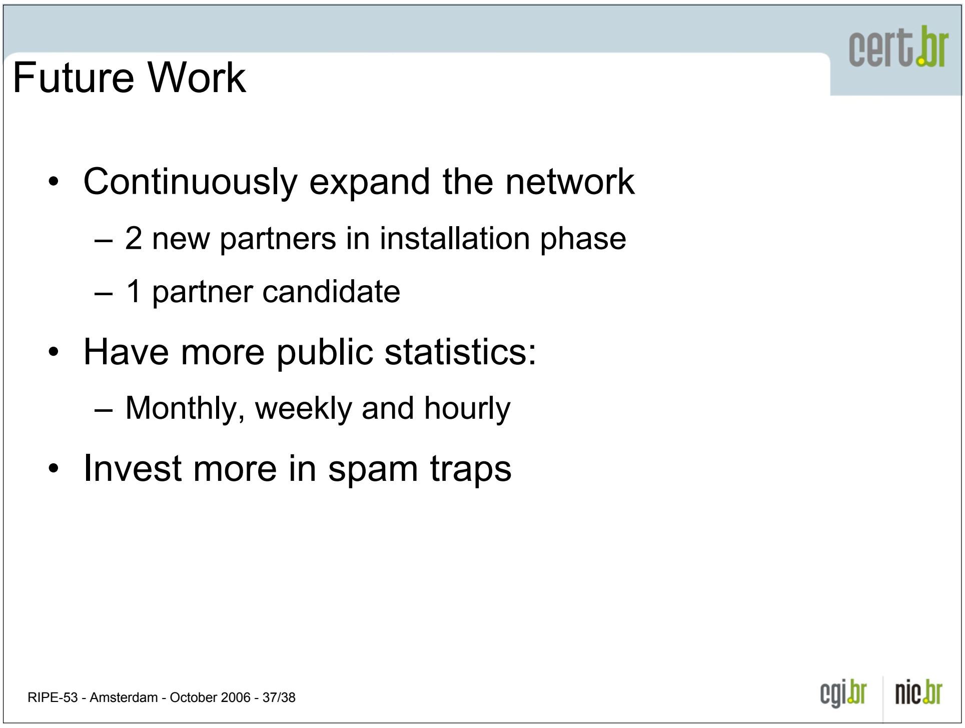


Disadvantages of the Architecture

- Honeypots usually don’t catch attacks targeted to production networks
- Information gathered is limited compared to high interaction honeypots

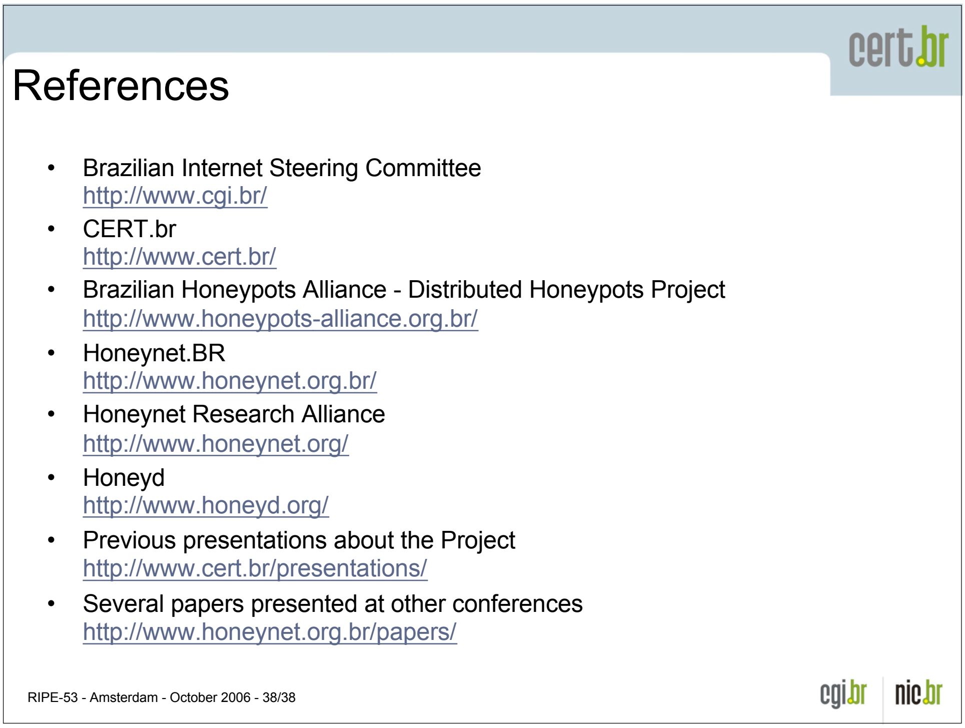


Future Work and References



Future Work

- Continuously expand the network
  - 2 new partners in installation phase
  - 1 partner candidate
- Have more public statistics:
  - Monthly, weekly and hourly
- Invest more in spam traps



References

- Brazilian Internet Steering Committee
  http://www.cgi.br/
- CERT.br
  http://www.cert.br/
- Brazilian Honeypots Alliance - Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/
- Honeynet.BR
  http://www.honeynet.org.br/
- Honeynet Research Alliance
  http://www.honeynet.org/
- Honeyd
  http://www.honeyd.org/
- Previous presentations about the Project
  http://www.cert.br/presentations/
- Several papers presented at other conferences
  http://www.honeynet.org.br/papers/