Incident Handling and Internet Security in Brazil

Cristine Hoepers
<cristine@cert.br>

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Computer Emergency Response Team Brazil
http://www.cert.br/

Comitê Gestor da Internet no Brasil
Brazilian Internet Steering Committee
http://www.cgi.br/

Agenda

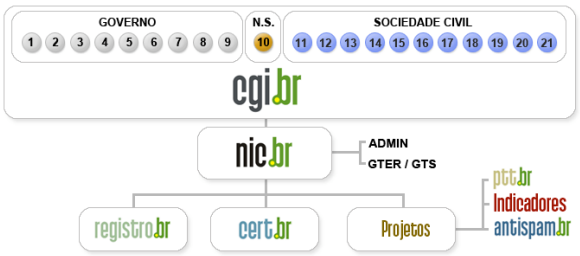
- CERT.br
  - Mission
  - CGI.br Structure
- History of Incident Response in Brazil
- CERT.br Activities
  - Training, Early Warning, Awareness, Partnerships, etc
- Other Initiatives Related to Security
- References

CERT.br

- 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
  - Forum of Incident Response and Security Teams (FIRST) Full member (http://www.first.org/membership/)

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

The Brazilian Internet Steering Committee (CGI.br)



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

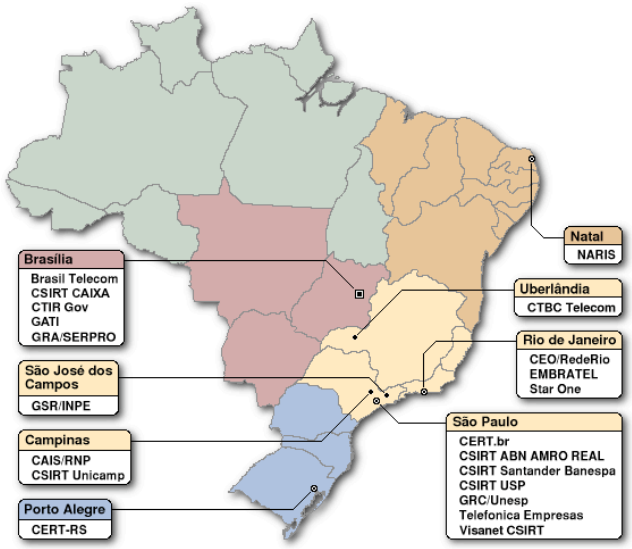
http://www.cgi.br/internacional/

History of CSIRTs in Brazil

- **August/1996**: CGI.br released the document: “Towards the Creation of a Security Coordination Center for the Brazilian Internet.”[1]
- **June/1997**: CGI.br created CERT.br (at that time called NBSO - NIC BR Security Office), based on the report’s recommendation[2]
- **August/1997**: the Brazilian Research Network (RNP) created it’s own CSIRT (CAIS)[3], followed by the *Rio Grande do Sul* State, that created CERT-RS[4]
- **1999**: other institutions, including Universities and Telecommunication Companies announced their CSIRTs
- **2003**: more than 20 CSIRTs formed
- **2004**: CTIR Gov was created, with the Brazilian Federal Government Administration as their constituency[5]

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm
[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/cert-rs.html
[5] http://www.ctir.gov.br

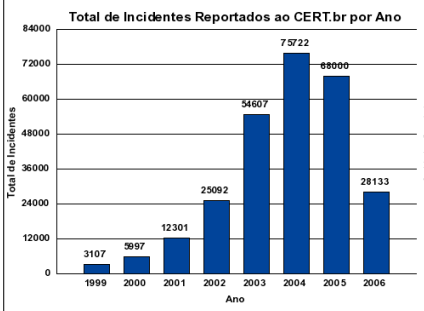
Brazilian CSIRTs

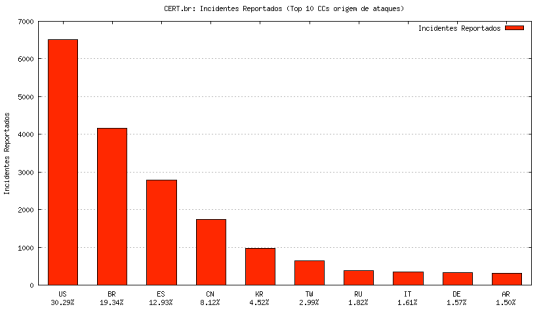


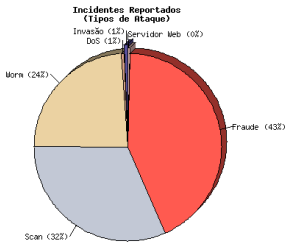
http://www.cert.br/contact-br.html

CERT.br Activities

Incident Handling and Statistics







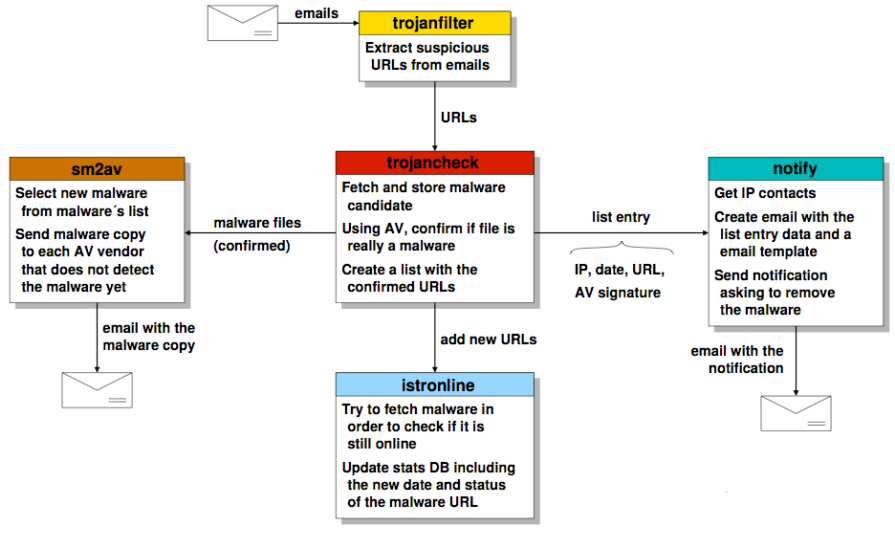
http://www.cert.br/stats/incidentes/

http://www.cert.br/stats/spam/

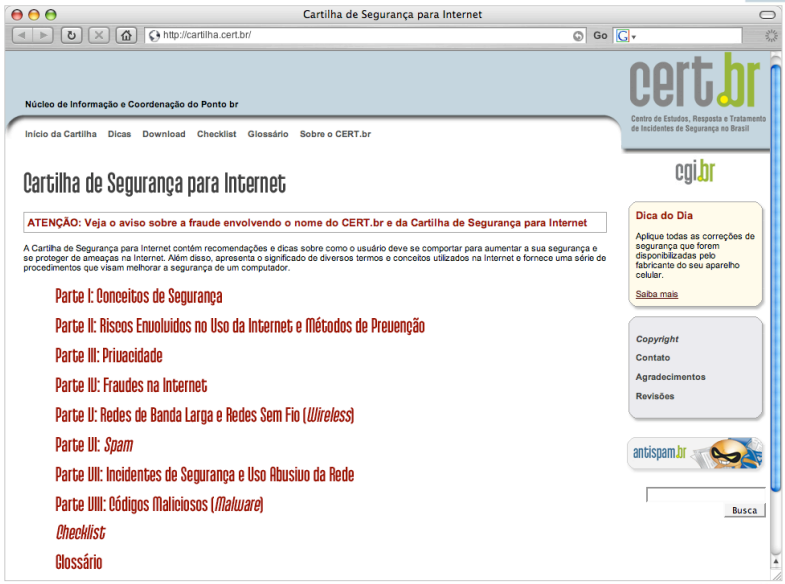
Anti-Fraud Activities

- In Brazil fraud is almost all based on malicious codes disseminated through social engineering
- CERT.br and Financial Institutions:
  - Share technical details about crimeware, new social engineering techniques, malicious codes, etc
  - CERT.br:
    - Notifies sites hosting crimeware related to frauds
    - Coordinates with international sites and CSIRTs to take down the crimeware sites
    - Send new crimeware (trojans, keyloggers, etc) to 24 anti-virus vendors
    - Anti-Phishing Working Group (APWG) Research Partner http://www.antiphishing.org/

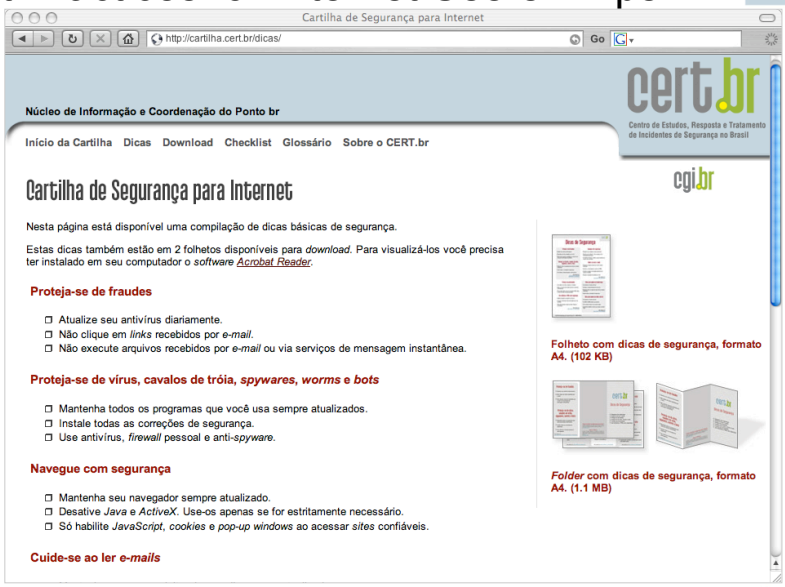
Trojan Notification System



Best Practices for Internet Users



Best Practices for Internet Users - Tips



Trend Analysis and Early Warning

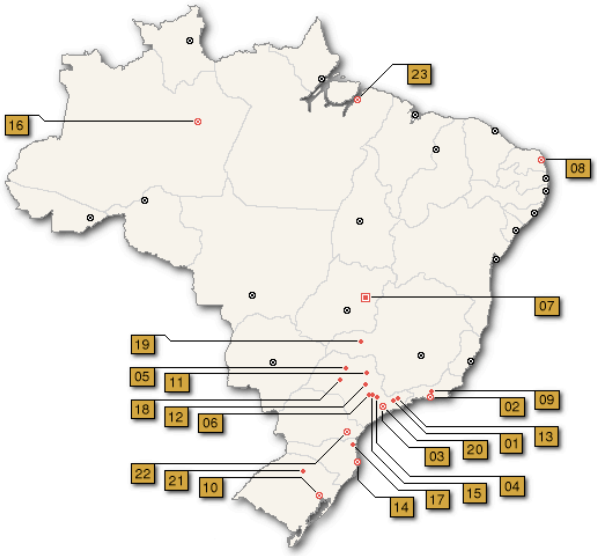
Brazilian Honeypots Alliance - Distributed Honeypots Project

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/

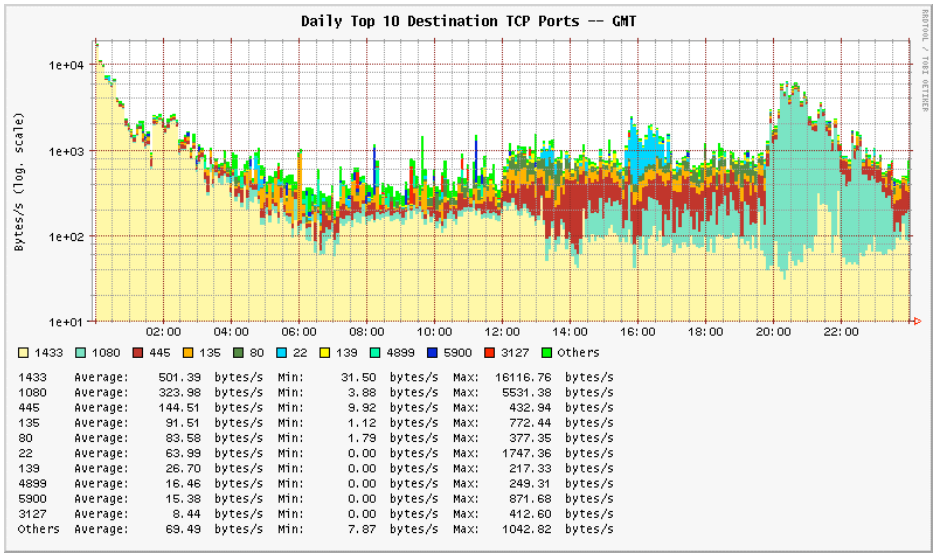
Cities Where the Honeypots are Located



Partners of the Brazilian Honeypots Alliance

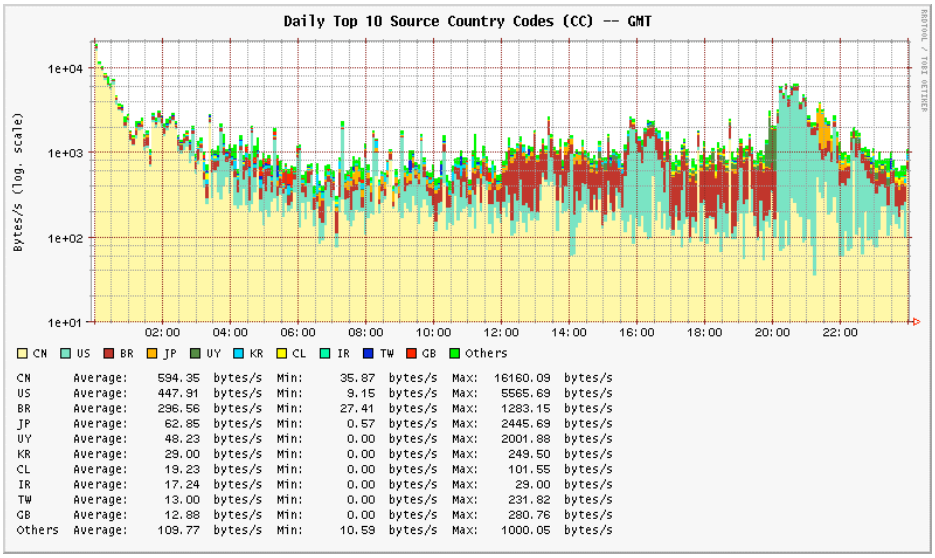
#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, USP
04	Campinas	CenPRA, HP Brazil, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil 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

Honeypots Flows - Top Destination TCP Ports



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

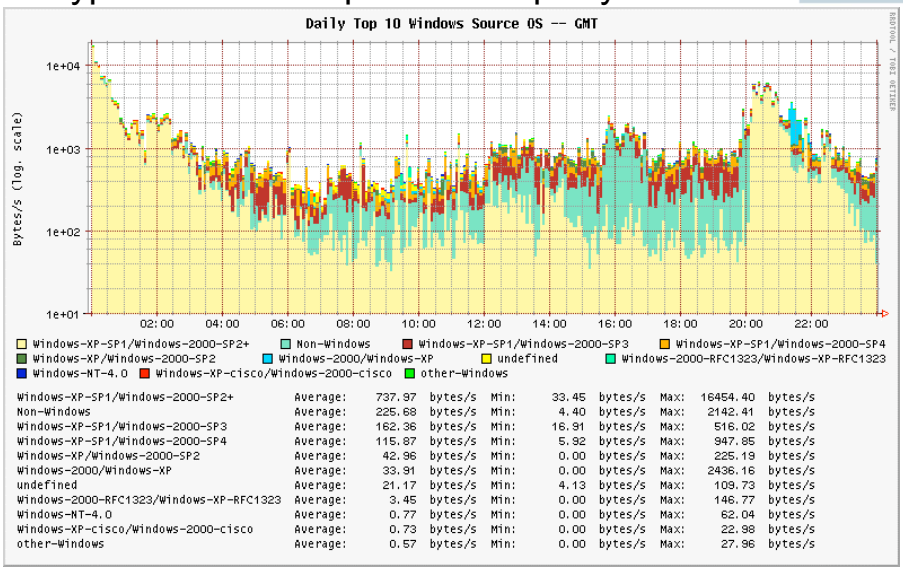
Honeypots Flows - Top Source Country Codes



CN	Average:	594.35	bytes/s	Min:	35.87	bytes/s	Max:	16160.09	bytes/s
US	Average:	447.91	bytes/s	Min:	9.15	bytes/s	Max:	5565.69	bytes/s
BR	Average:	296.56	bytes/s	Min:	27.41	bytes/s	Max:	1283.15	bytes/s
JP	Average:	62.85	bytes/s	Min:	0.57	bytes/s	Max:	2445.69	bytes/s
UY	Average:	48.23	bytes/s	Min:	0.00	bytes/s	Max:	2001.88	bytes/s
KR	Average:	29.00	bytes/s	Min:	0.00	bytes/s	Max:	249.50	bytes/s
CL	Average:	19.23	bytes/s	Min:	0.00	bytes/s	Max:	101.55	bytes/s
IR	Average:	17.24	bytes/s	Min:	0.00	bytes/s	Max:	29.00	bytes/s
TW	Average:	13.00	bytes/s	Min:	0.00	bytes/s	Max:	231.82	bytes/s
GB	Average:	12.88	bytes/s	Min:	0.00	bytes/s	Max:	280.76	bytes/s
Others	Average:	109.77	bytes/s	Min:	10.59	bytes/s	Max:	1000.05	bytes/s

May 17, 2006 - http://www.honeypots-alliance.org.br/stats/
LACNIC IX - Network Security Event - May 2006

Honeypots Flows - Top Source Op. Systems



Windows-XP-SP1/Windows-2000-SP2+	Average:	737.97	bytes/s	Min:	33.45	bytes/s	Max:	16454.40	bytes/s
Non-Windows	Average:	225.68	bytes/s	Min:	4.40	bytes/s	Max:	2142.41	bytes/s
Windows-XP-SP1/Windows-2000-SP3	Average:	162.36	bytes/s	Min:	16.91	bytes/s	Max:	516.02	bytes/s
Windows-XP-SP1/Windows-2000-SP4	Average:	115.87	bytes/s	Min:	5.92	bytes/s	Max:	947.85	bytes/s
Windows-XP/Windows-2000-SP2	Average:	42.96	bytes/s	Min:	0.00	bytes/s	Max:	225.19	bytes/s
Windows-2000/Windows-XP	Average:	33.91	bytes/s	Min:	0.00	bytes/s	Max:	2436.16	bytes/s
undefined	Average:	21.17	bytes/s	Min:	4.13	bytes/s	Max:	109.73	bytes/s
Windows-2000-RFC1323/Windows-XP-RFC1323	Average:	3.45	bytes/s	Min:	0.00	bytes/s	Max:	146.77	bytes/s
Windows-NT-4.0	Average:	0.77	bytes/s	Min:	0.00	bytes/s	Max:	62.04	bytes/s
Windows-XP-cisco/Windows-2000-cisco	Average:	0.73	bytes/s	Min:	0.00	bytes/s	Max:	22.98	bytes/s
other-Windows	Average:	0.57	bytes/s	Min:	0.00	bytes/s	Max:	27.96	bytes/s

May 17, 2006 - http://www.honeypots-alliance.org.br/stats/
LACNIC IX - Network Security Event - May 2006

Support for new CSIRTs

- Help new CSIRTs to establish their activities
  - Meetings, presentations to C-level managers, training, etc
- SEI[SM]/CMU Partner, licensed to deliver CERT® Program courses in Brazil:
    - Creating a Computer Security Incident Response Team
    - Managing Computer Security Incident Response Teams
    - Fundamentals of Incident Handling
    - Advanced Incident Handling for Technical Staff
  - 160+ incident handlers trained

http://www.cert.br/cursos/

Other CGI.br Initiatives Related to Security

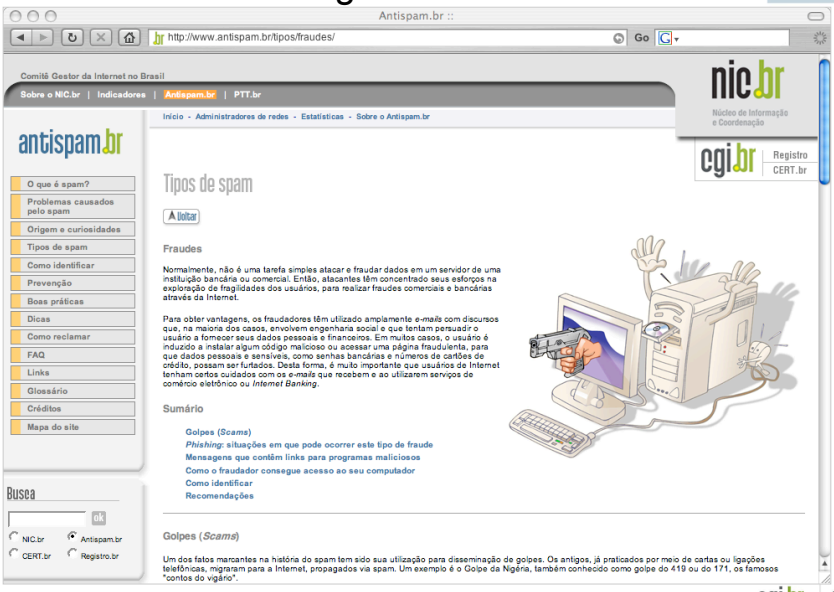
CGI.br Anti-Spam Comission

- Created by CGI.br to articulate, with all players, viable solutions to reduce the spam problem
  http://www.cgi.br/sobre-cg/antispam.htm
- Produced material that include tips for preventing from security problems coming through email
  - All material available at the www.antispam.br site
- CERT.br helped to produce 2 documents
  - Technologies and Policies to Fight Spam
  - Technical Analysis of Anti-spam Legislation

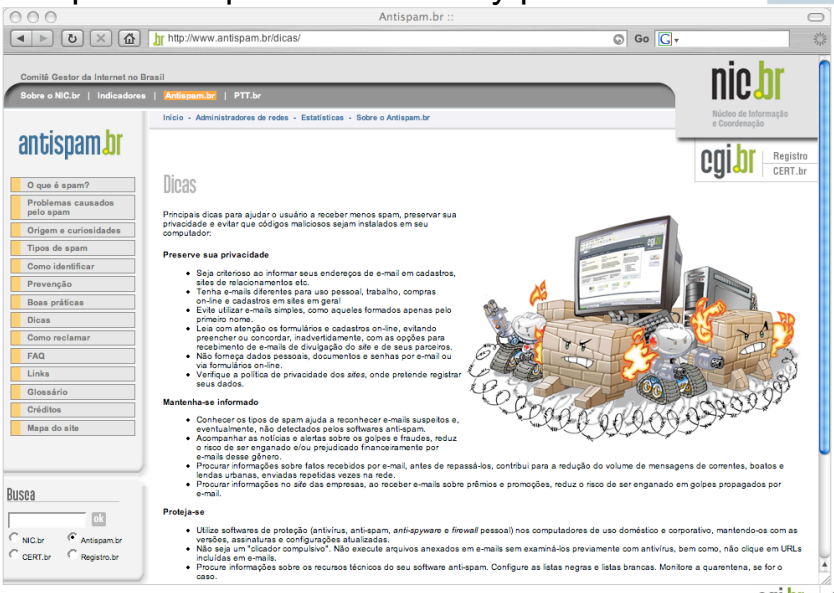
The antispam.br website

Malicious codes and their relation to emails

Frauds that come through emails



Tips to prevent spam and security problems



CGI.br Indicators

- Survey on the Use of Information and Communication Technologies In Brazil 2005
- Includes indicators about security and spam
  - **Households**: security problems encountered, security measures adopted, antivirus updating frequency, frequency they receive spam, time spent with spam, etc.
  - **Enterprises**: identified IT security problems, security measures adopted, antivirus updating frequency, technologies adopted for secure communication, etc.

http://www.nic.br/indicadores/

http://www.nic.br/indicadores/indicadores.pdf

References

- This presentation
  http://www.cert.br/docs/palestras/
  http://www.cert.br/docs/presentations/
- CSIRT development references (English and Portuguese)
  http://www.cert.br/csirts/
- Best Practices in Portuguese:
  - Tips for home users (*Cartilha de Segurança para Internet*)
    http://cartilha.cert.br/
  - Security Best Practices for System and Network Administrators
    (*Práticas de Segurança para Administradores de Redes Internet*)
    http://www.cert.br/seg-adm-redes/
- SEI℠/CMU CERT® Program Courses delivered by CERT.br
  http://www.cert.br/cursos/
- CERT.br Statistics
  http://www.cert.br/stats/
- Comitê Gestor da Internet - CGI.br: http://www.cgi.br/
- CGI.br Indicators: http://www.nic.br/indicadores/

References (cont)

CSIRTs around the world:

- FIRST Member Teams
  http://www.first.org/about/organization/teams/
- National Computer Emergency Response Teams
  http://www.cert.org/csirts/national/contact.html
- TI Directory of European CSIRTs
  http://www.ti.terena.nl/teams/
- APCERT Member Teams
  http://www.apcert.org/about/structure/members.html
- Brazilian CSIRTs Contact Information
  http://www.cert.br/contact-br.html