Incident Handling in Brazil

Cristine Hoepers
cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - **CERT.br**

Núcleo de Informação e Coordenação do Ponto br - **NIC.br**
Comitê Gestor da Internet no Brasil - **CGI.br**

Agenda

- Brazilian Internet Governance
- A brief history of CSIRTs in Brazil
- CERT.br activities

Internet Governance in Brazil

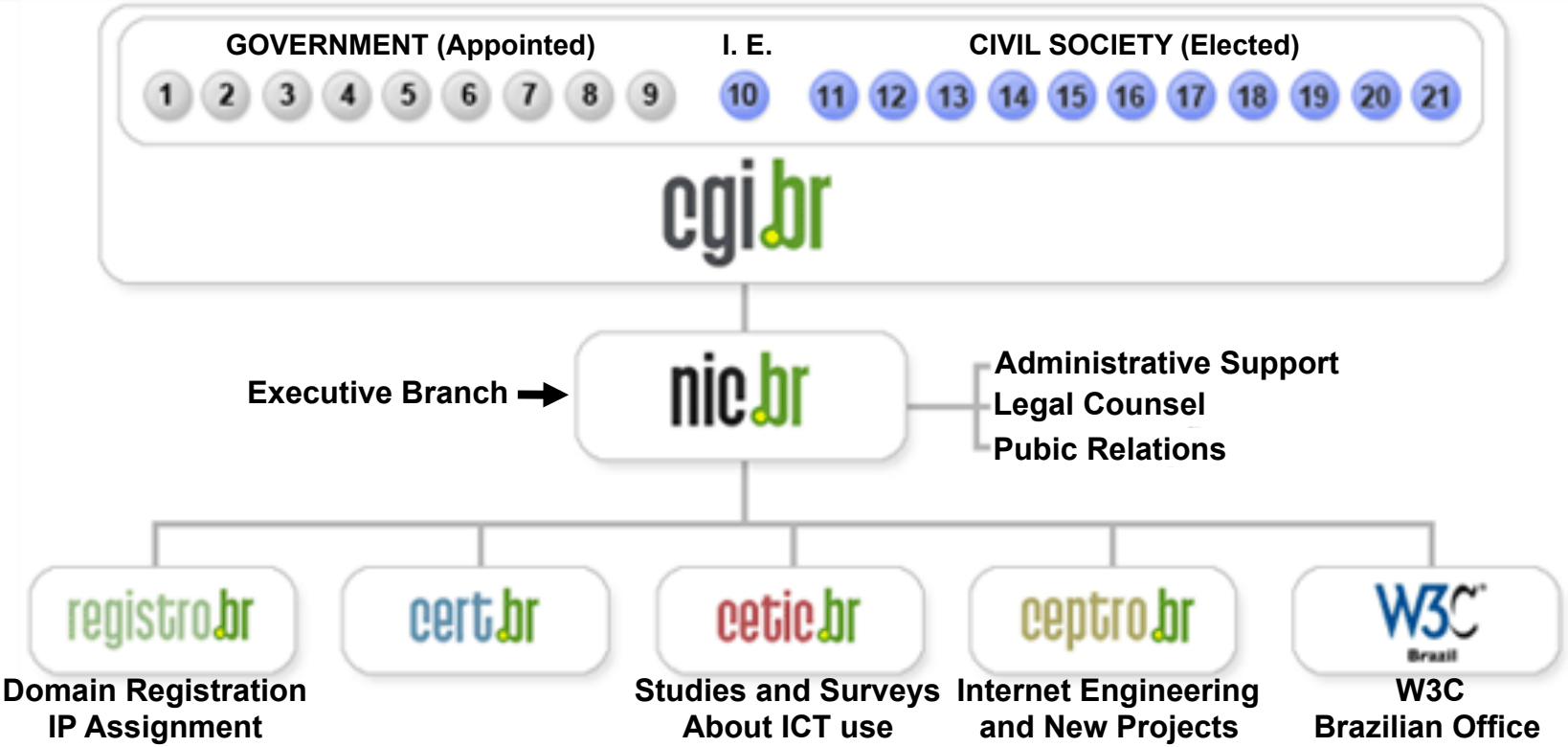
The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization created in 1995 that, among the diverse responsibilities established 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

A Brief History of Incident Handling in Brazil

Development of Incident Handling in Brazil

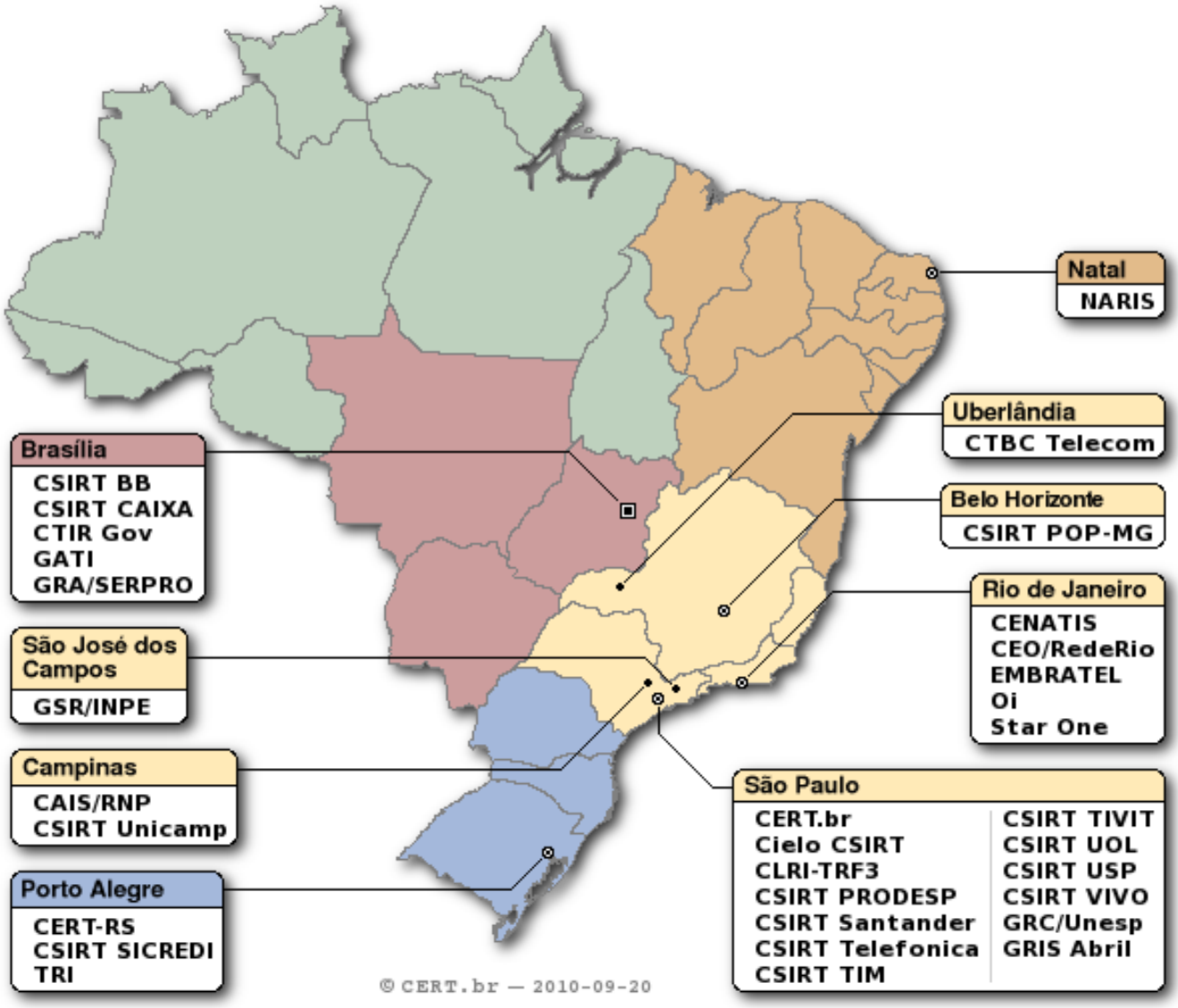
- August/1996: CGI.br released the report: "*Towards the Creation of a Security Coordination Center for the Brazilian Internet*."[1]
- June/1997: CGI.br created CERT.br (at that time called NBSO), as a CSIRT with national responsibility, based on the report's recommendation[2]
- August/1997: the Brazilian Research Network (RNP) created it's own CSIRT (CAIS) [3], followed by the Rio Grande do Sul Academic Network (CERT-RS)[4]
- 1999: other institutions, including Universities and Telecommunication Companies started forming their CSIRTs
- 2003/2004: task force to discuss the structure of a CSIRT for the Federal Government Administration
- 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 as of November/2010

32 teams with services announced to the public

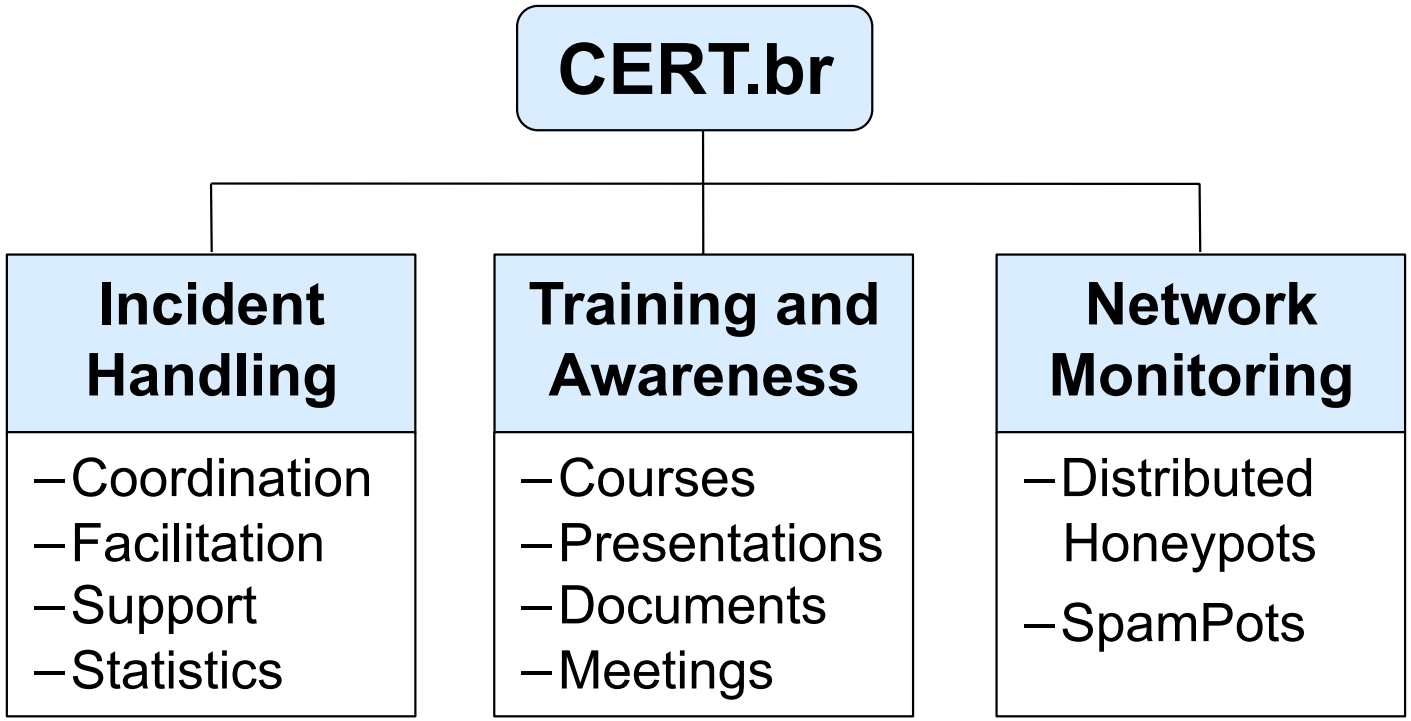
Sector	CSIRTs
National Responsibility	CERT.br, CTIR Gov
Government	CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO
Financial Sector	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Research & Education	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC/UNESP, TRI
Other Sectors	CSIRT TIVIT, GRIS Abril



http://www.cert.br/csirts/brazil/

CERT.br Activities

CERT.br Activities

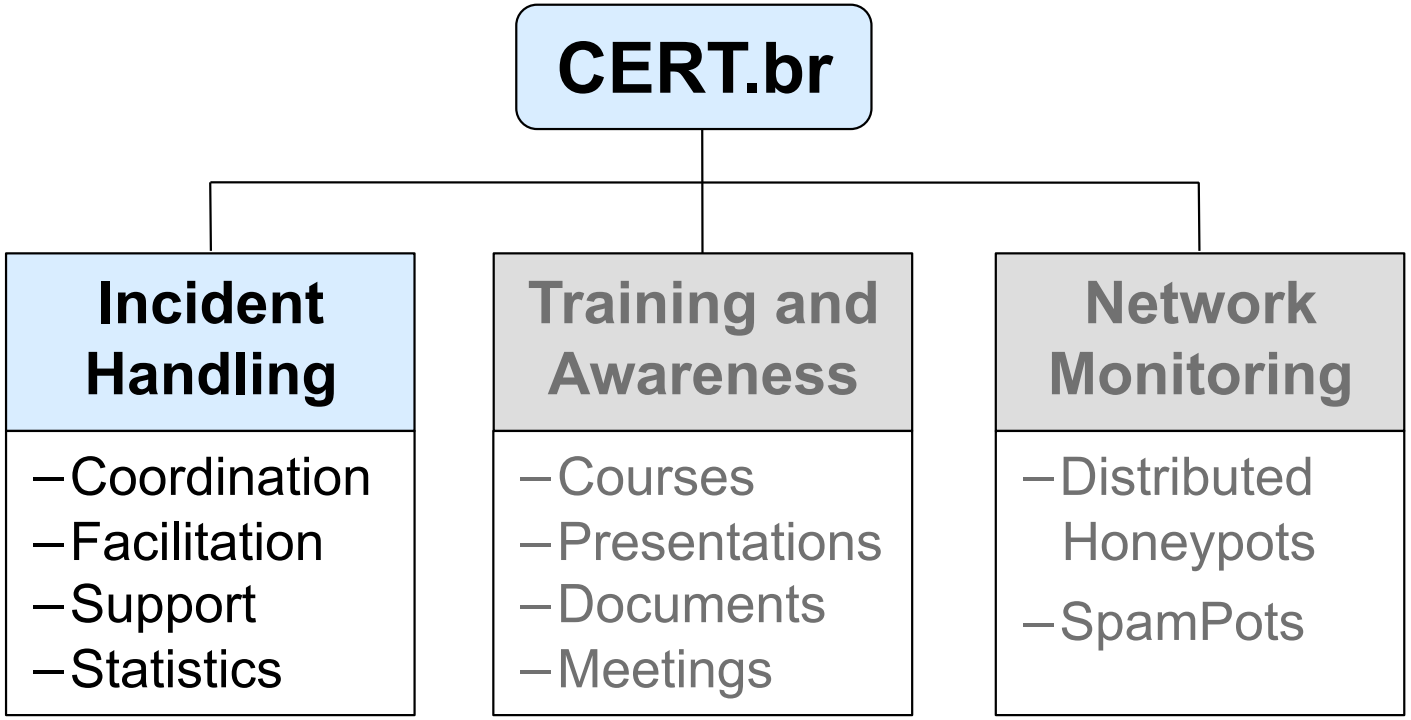


FIRST Improving Security Together MEMBER

Anti-Phishing Working Group APWG

SEIPartner CERT Courses

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


CERT.br
Incident Handling
– Coordination
– Facilitation
– Support
– Statistics
Training and Awareness
– Courses
– Presentations
– Documents
– Meetings
Network Monitoring
– Distributed Honeypots
– SpamPots

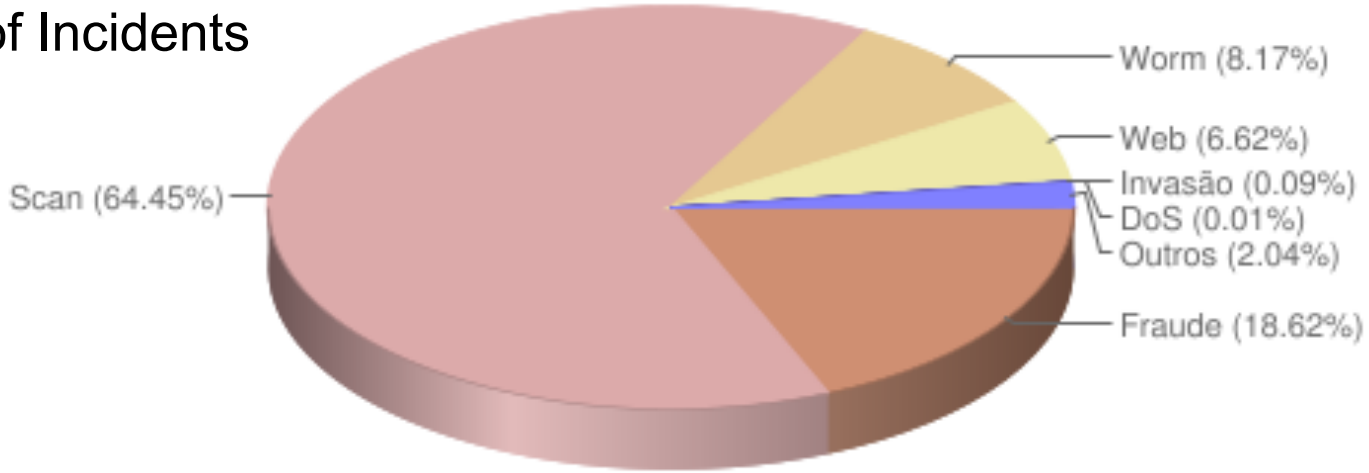
CERT.br Incident Handling Activities

- Provides a focal point for incident notification in the country
- Provides the coordination and necessary support for organizations involved in incidents
- Supports the analysis of compromised systems and their recovery process
- Establishes collaborative relationships with other entities, such as other CSIRTs, Universities, ISPs and telecommunication companies
- Maintains public statistics of incidents handled and spam complaints received

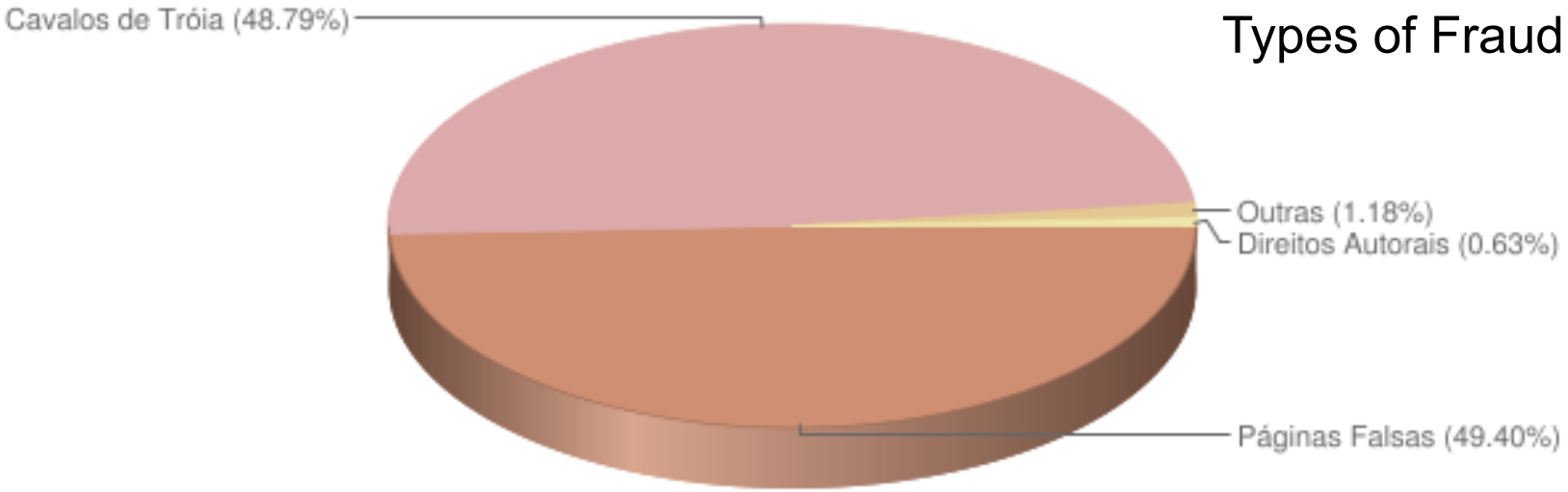
Incidents Reported to CERT.br

- **2010 Jan-Sep: 101156**

Types of Incidents

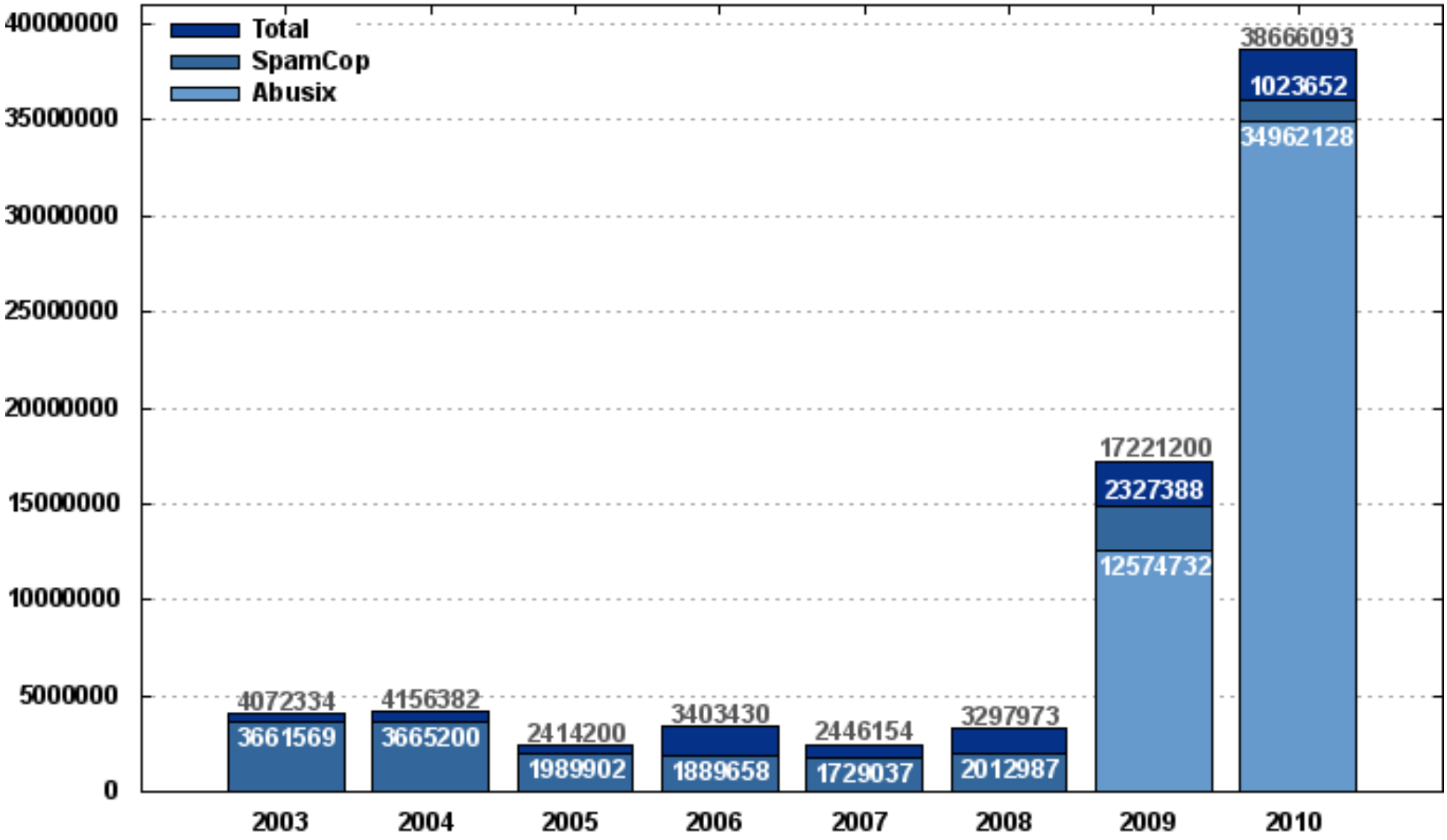


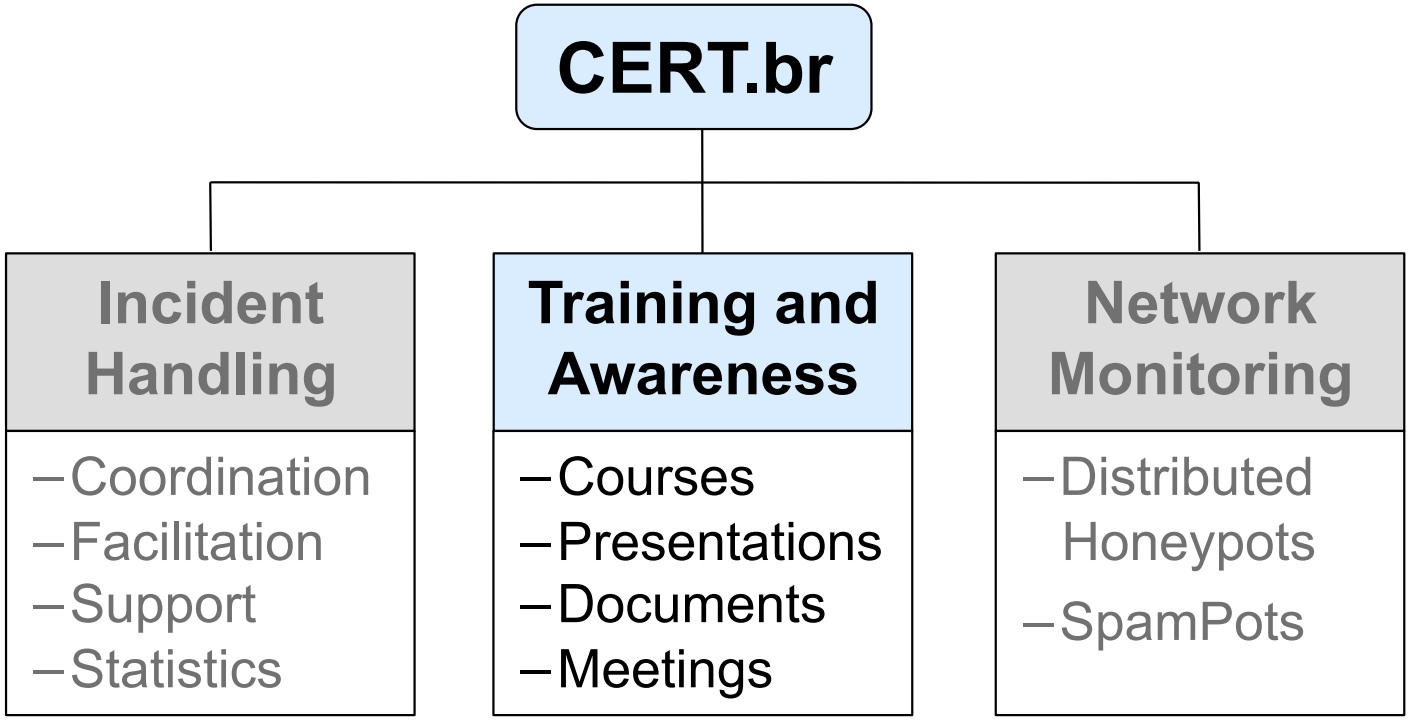
Types of Fraud



Spams Reported to CERT.br

Mainly botnets and open proxies at broadband networks




CERT.br
Incident Handling
– Coordination
– Facilitation
– Support
– Statistics
Training and Awareness
– Courses
– Presentations
– Documents
– Meetings
Network Monitoring
– Distributed Honeypots
– SpamPots

Establishment of new CSIRTs

- **Helps new Computer Security Incident Response Teams (CSIRTs) to establish their activities**
  - **meetings, presentations at conferences and training**
- ***SEI/CMU Partner* since 2004, delivers in Brazil the following CERT® Program courses:**
  - **http://www.cert.br/courses/**
    - ***Information Security for Technical Staff***
    - ***Overview of Creating and Managing CSIRTs***
    - ***Fundamentals of Incident Handling***
    - ***Advanced Incident Handling for Technical Staff***
  - **400+ security professionals trained in Brazil**
  - ***Overview of Creating and Managing CSIRTs* workshop delivered at 2008, 2009 and 2010 LACNIC Conferences**

Internet Security Best Practices – for End Users

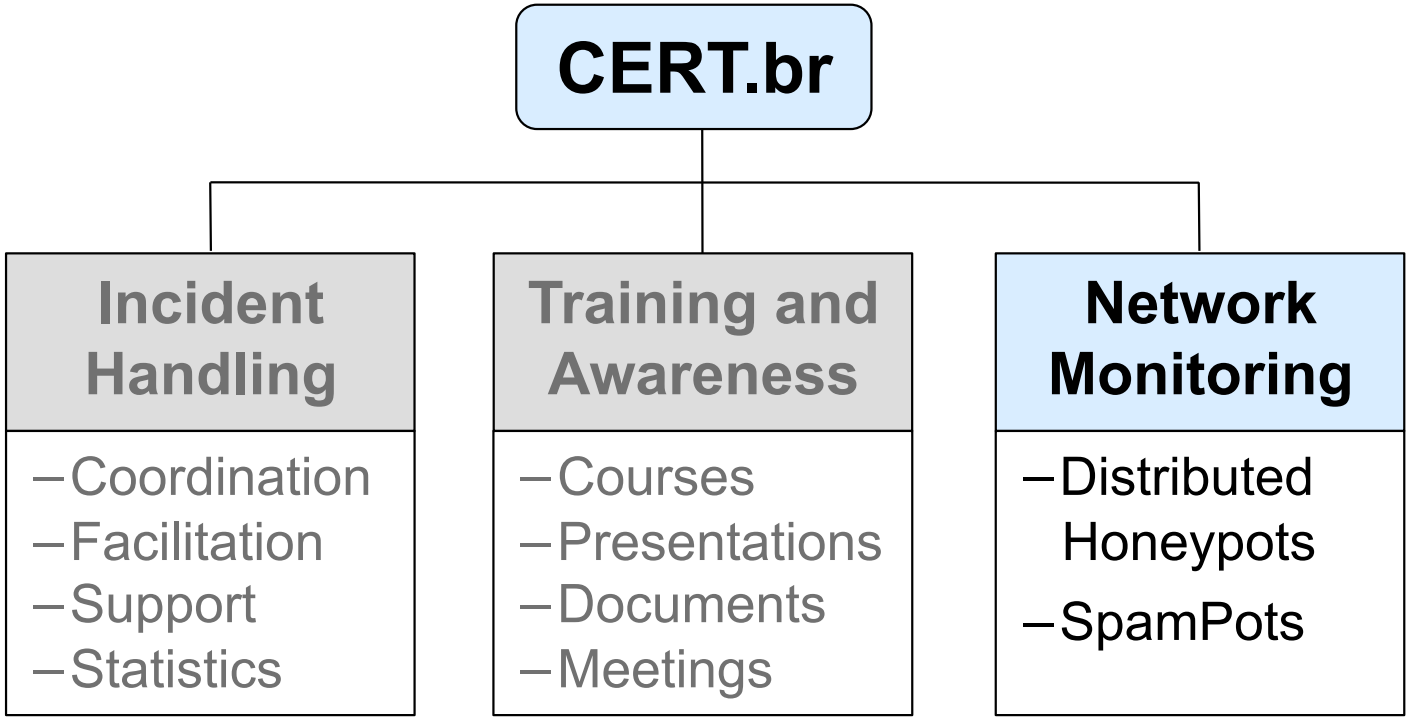
"*Cartilha de Segurança para Internet*"

http://cartilha.cert.br/

Antispam.br

Website and Cartoons about spam and Security

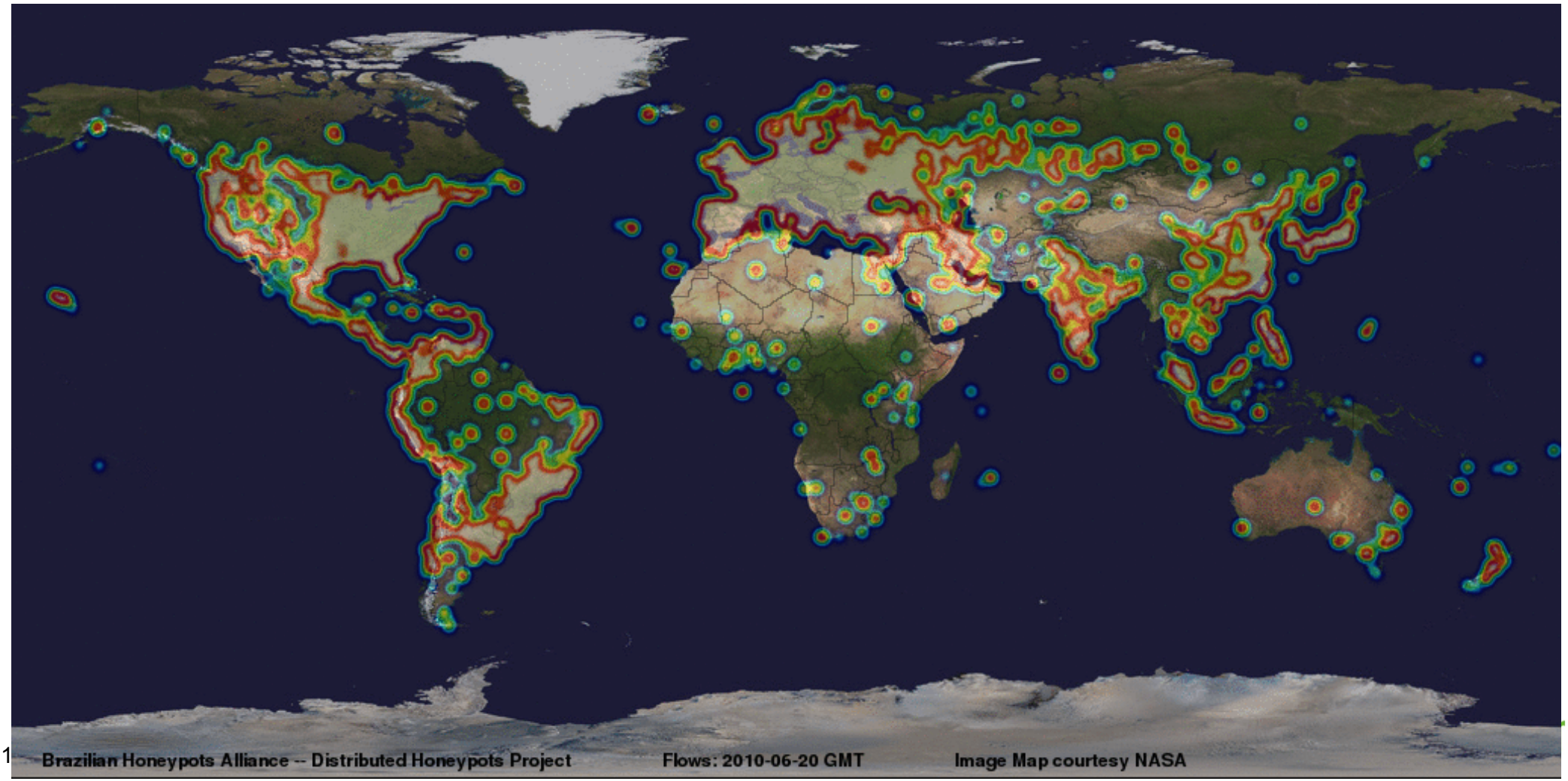
http://www.antispam.br/


CERT.br
Incident Handling
– Coordination
– Facilitation
– Support
– Statistics
Training and Awareness
– Courses
– Presentations
– Documents
– Meetings
Network Monitoring
– Distributed Honeypots
– SpamPots

Monitoring Attacks Directed to Brazil

Brazilian Distributed Honeypots Network

Partners: ADG, ANSP, Banco do Brasil, Banco Real, BNDES, Brasil Telecom, CBPF, CenPRA, CERT.br, CERT-RS, CSIRT PoP-MG, CTBC Telecom, CTIR Gov, Diveo, Durand, Embratel, EMPREL, Fiocruz, FPTE, Furnas, HC FMUSP, INPE, ITA, ITAL, LOCAWEB, LNCC, Ministério da Justiça, Onda, PoP-ES, PoP-PR, PRODESP, PUCPR, PUC-RIO, RedeRio, TCU, TIVIT, TRI, UFBA, UFSC DAS, UNESP, UNICAMP, UOL, UPF, USP e Unisinos.



SpamPots Project

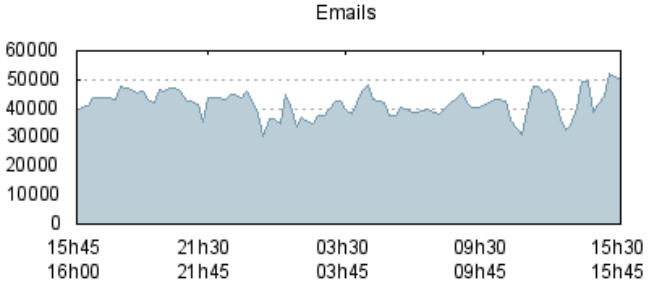
- **Network of Honeypots emulating open proxies and SMTP servers**
- **Capturing 8 million spams/day, on average**

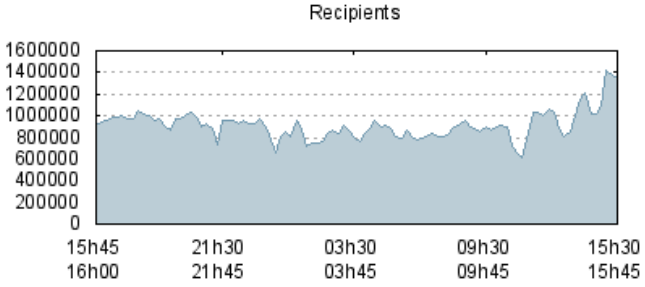
Sensors in cooperation with:

- CERT.at (AT),
- AusCERT (AU),
- CSIRT-USP (BR),
- CLCERT (CL),
- Loja Unversity (EC),
- SURFcert (NL),
- TWCERT/CC (TW),
- U. of Washington (US),
- CSIRT Antel (UY),
- Trend Micro (MX)

SpamPots Project – Statistics

Graphics showing the number of emails & recipients over the last 24 hours (in chunks of 15 minutes).





Country Codes

top

Top 15 Country Codes sorted by emails

#	CC	description	emails	(%)	recipients	(%)	connections	proto	spampots
1	TW	Taiwan, Province of China	17,122	34.43	392,592	29.29	8,114	HTTP, SMTP, S4, S5	8
2	US	United States	10,157	20.43	384,439	28.68	2,722	HTTP, SMTP	5
3	CN	China	6,460	12.99	84,369	6.29	867	HTTP, SMTP, S4, S5	8
4	BR	Brazil	2,969	5.97	102,366	7.64	904	SMTP	6
5	RU	Russian Federation	1,575	3.17	53,637	4.00	445	SMTP, S4, S5	7
6	DE	Germany	1,089	2.19	25,714	1.92	130	HTTP, SMTP, S4, S5	5
7	JP	Japan	911	1.83	1,797	0.13	173	SMTP, S4, S5	4
8	IN	India	875	1.76	28,647	2.14	330	SMTP, S4, S5	6
9	UA	Ukraine	715	1.44	24,288	1.81	213	SMTP	6
10	TH	Thailand	712	1.43	24,326	1.81	246	SMTP	6
11	HK	Hong Kong	660	1.33	14,134	1.05	259	HTTP, SMTP, S4, S5	6
12	FR	France	538	1.08	8,047	0.60	458	SMTP	4
13	CO	Colombia	537	1.08	18,280	1.36	161	SMTP, S4, S5	6
14	KR	Korea, Republic of	472	0.95	12,027	0.90	122	SMTP, S4	7
15	AR	Argentina	351	0.71	11,824	0.88	131	SMTP, S4	7
16	others (59)		4,584	9.22	153,844	11.48	1,193	HTTP, SMTP, S4, S5	—
Total			**49,727**	**100.00**	**1,340,331**	**100.00**	**16,468**		

Other NIC.br/CGI.br Activities Related to Internet Security

Training, Networking and Information Sharing

- **Regular Meetings**
  - Financial Sector
  - ISPs, Telecommunication Companies, their Associations and the Brazilian Communications Regulatory Agency
  - Law enforcement and other Legal entities
- **CEPTRO.br Courses**
  - Autonomous System Administration
  - IPv6 Network Administration
- **GTER and GTS Meetings**
  - Attendance is free and the event is transmitted via Internet
  - Held twice a year
  - Case studies and tutorials

Stability of Critical Internet Components

- NTP.br – maintains atomic clocks and provides Stratum 1 servers
- PTT.br – Internet eXchange points at major metropolitan areas in Brazil
- Registro.br
  - Hosts four DNS Root Server's mirrors
  - Mirrors of `.br` hosted overseas
  - DNSSEC supported at `.br` ccTLD
    - Free online training
      http://registro.br/suporte/tutoriais/dnssec.html
    - `.jus.br` and `.b.br` require DNSSEC

Links

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do Ponto br**
  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/