

CERT.br

Incident Handling and Network Monitoring Activities

Cristine Hoepers
General Manager
`cristine@cert.br`

Computer Emergency Response Team Brazil - **CERT.br**

Network Information Center Brazil - **NIC.br**
Brazilian Internet Steering Committee - **CGI.br**

Agenda

- **Our Organization and Mission**
 - **Brazilian Internet Governance**
- **CERT.br Incident Handling activities**
 - **Reactive**
 - **Proactive**
 - **Network Monitoring**

The Brazilian Internet Steering Committee - CGI.br

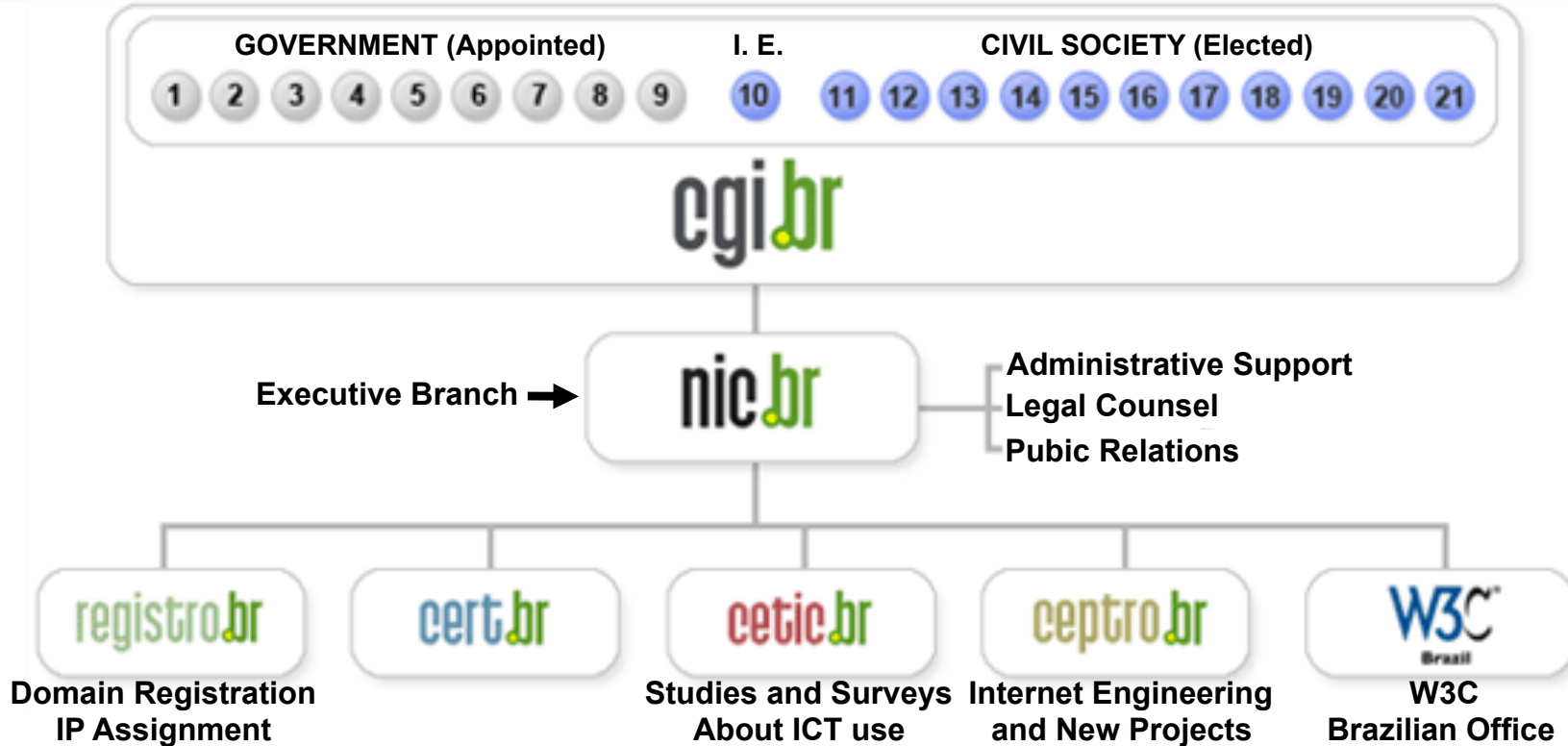
CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

Among the diverse responsibilities reinforce 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 recommend 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

Early Developments on 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 recommendation²**
- **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 constituency⁵**

¹<http://www.nic.br/grupo/historico-gts.htm>

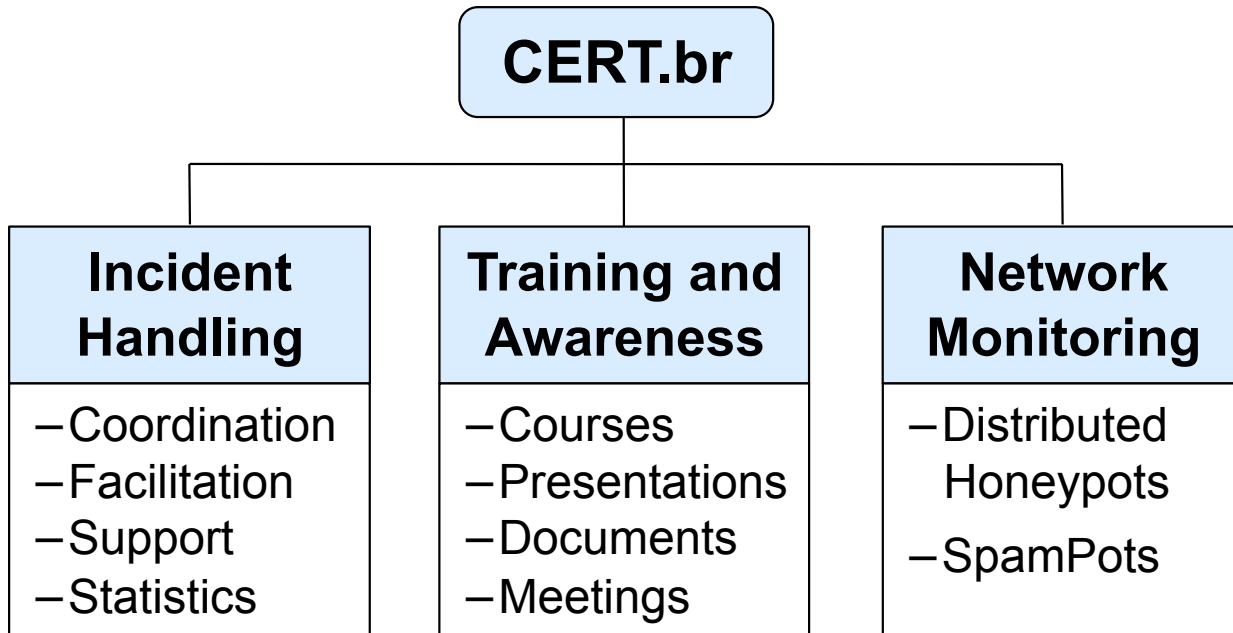
²<http://www.nic.br/grupo/gts.htm>

³http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf

⁴<http://www.cert-rs.tcche.br/cert-rs.html>

⁵<http://www.ctir.gov.br>

CERT.br Activities



Staff:

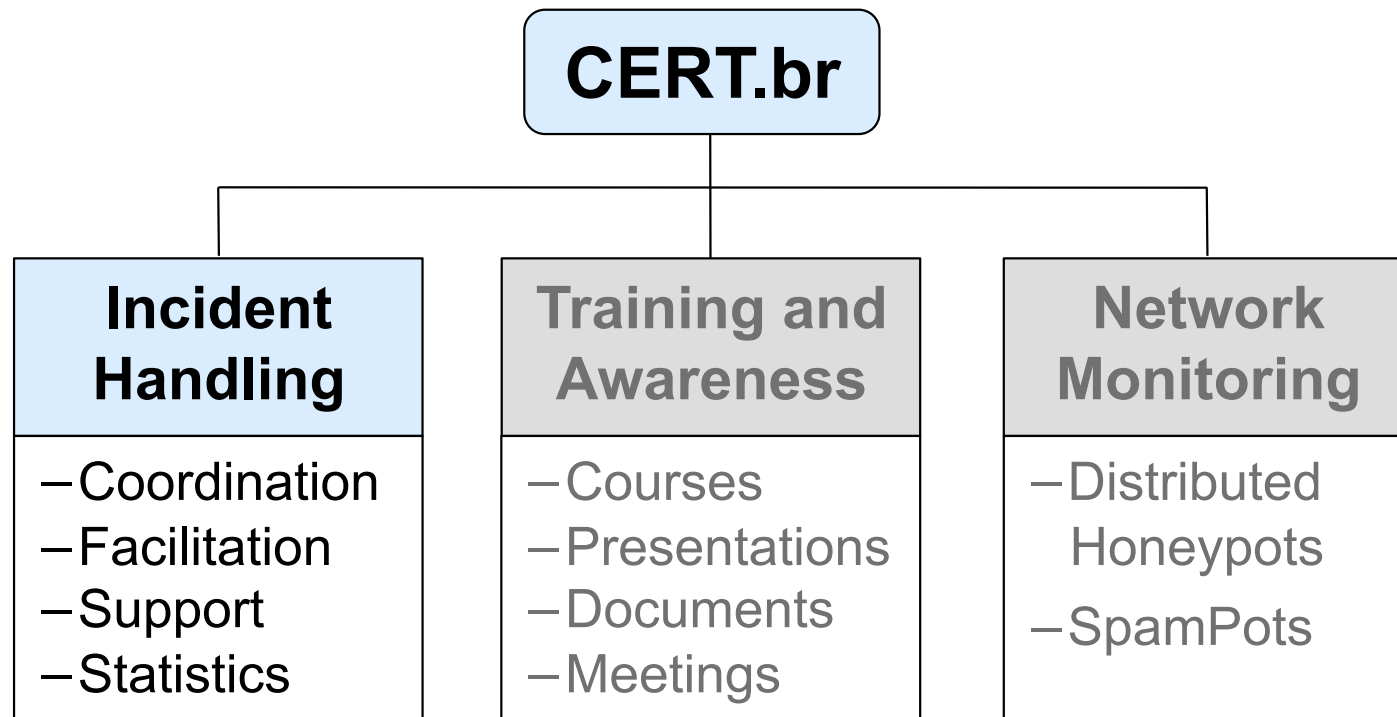
- 8 Security Analysts
 - 2 with PhD
 - 4 with MSc

Staff background:

- Computer Science or Engineering degrees
- System Administration
- Network Security

Staff shared with NIC.br/ CGI.br:

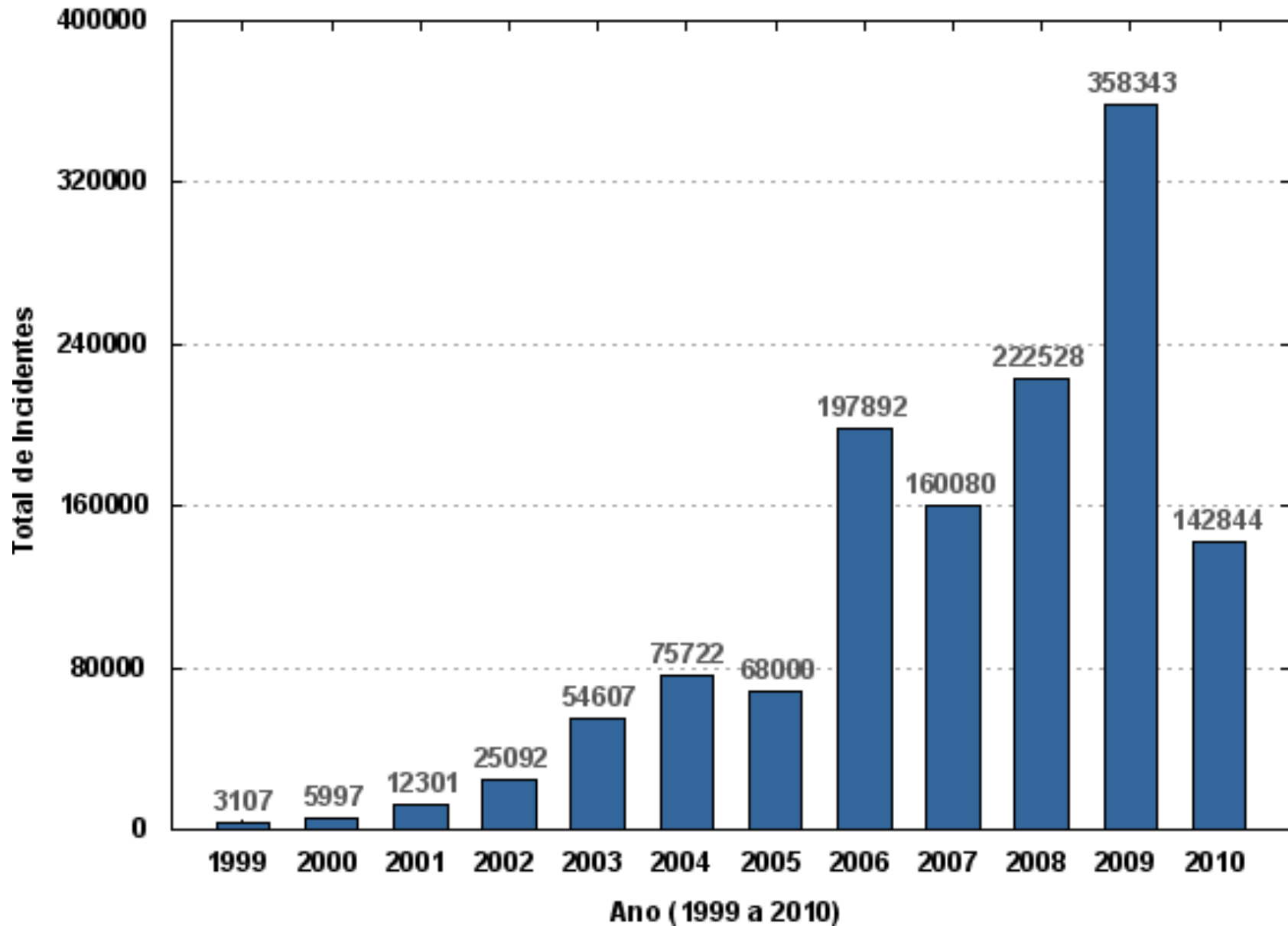
- Administrative Support
- Legal department
- Public Relations
- 24/7 Data Center and Network Operations Support



CERT.br Incident Handling Activities

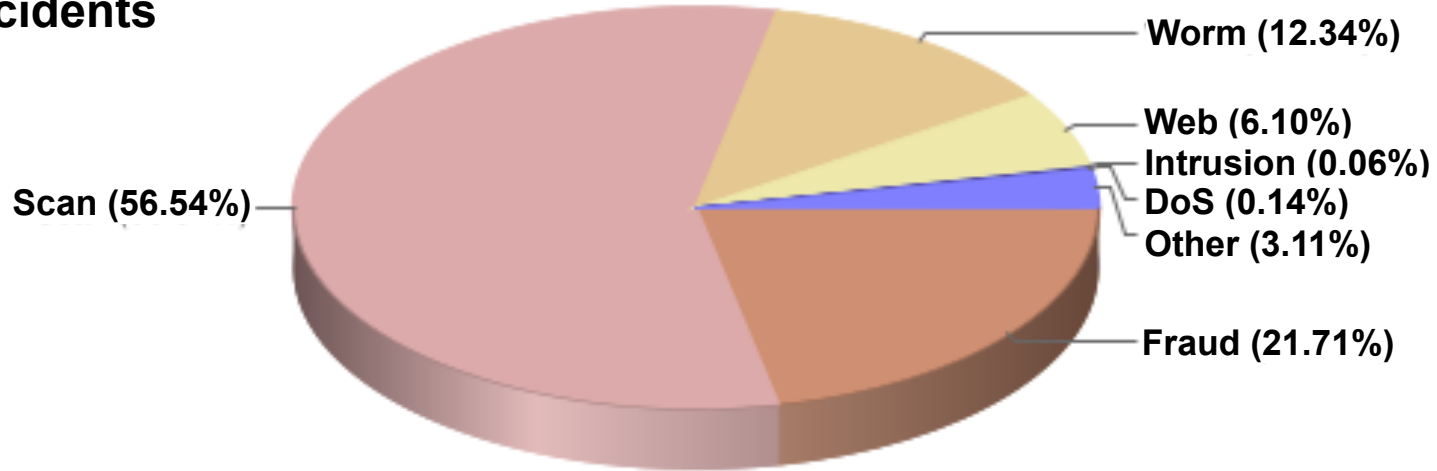
- **Provides a focal point for incident notification in the country**
- **Provides the coordination and necessary support for organizations involved in incidents**
- **Supports the analysis of compromised systems and their recovery process**
- **Establishes collaborative relationships with other entities,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

Incidents Reported to CERT.br – 1999-2010

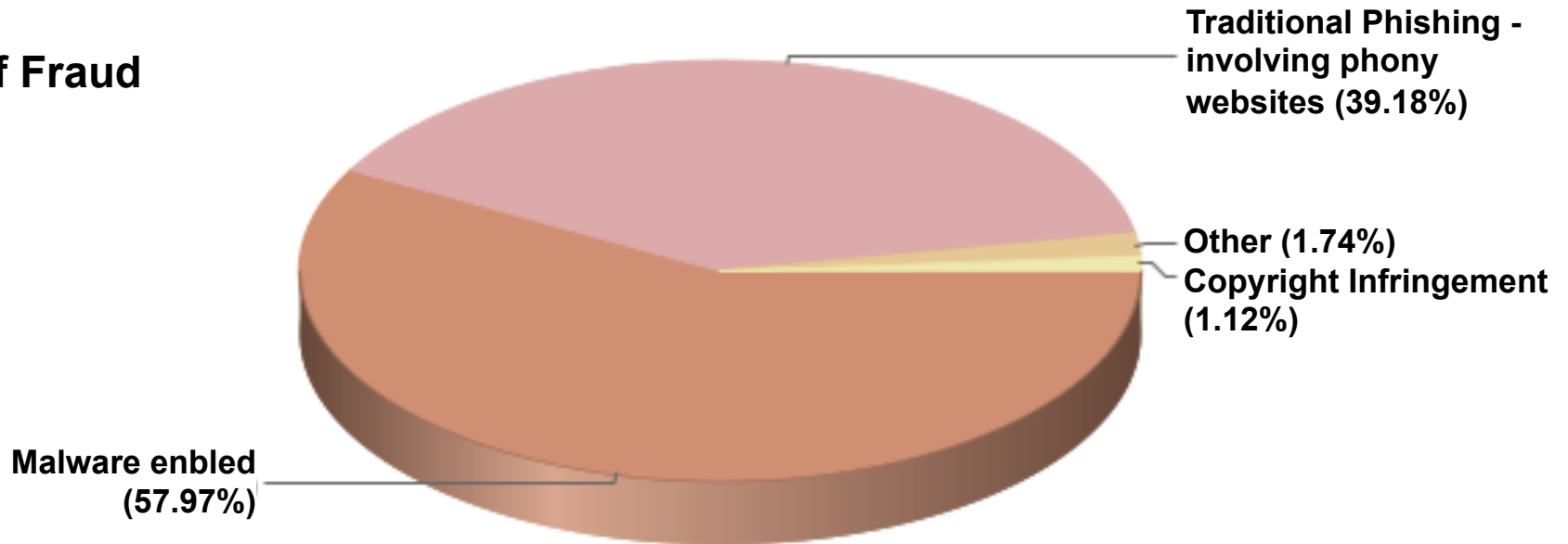


Incidents Reported to CERT.br in 2010

Types of Incidents



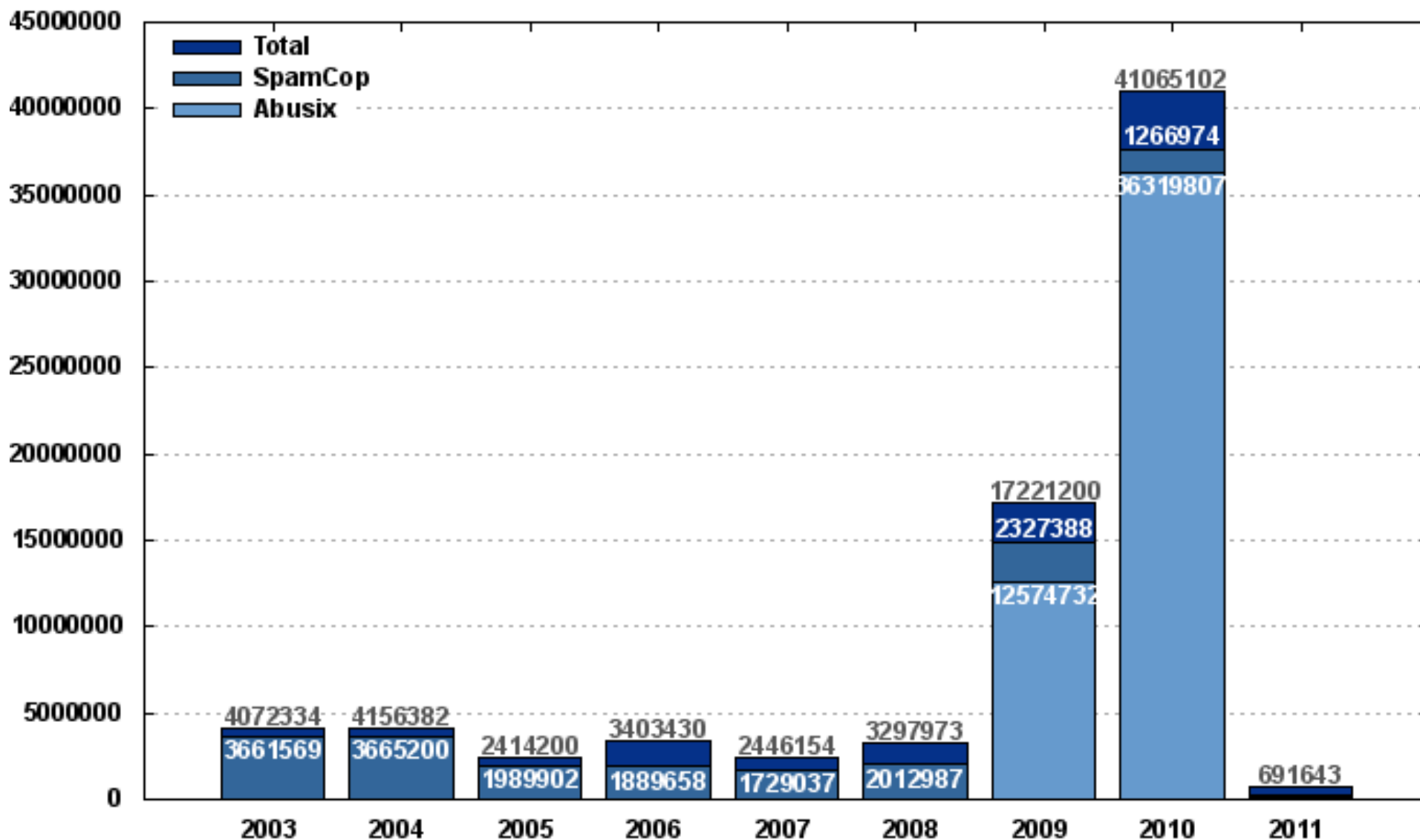
Types of Fraud



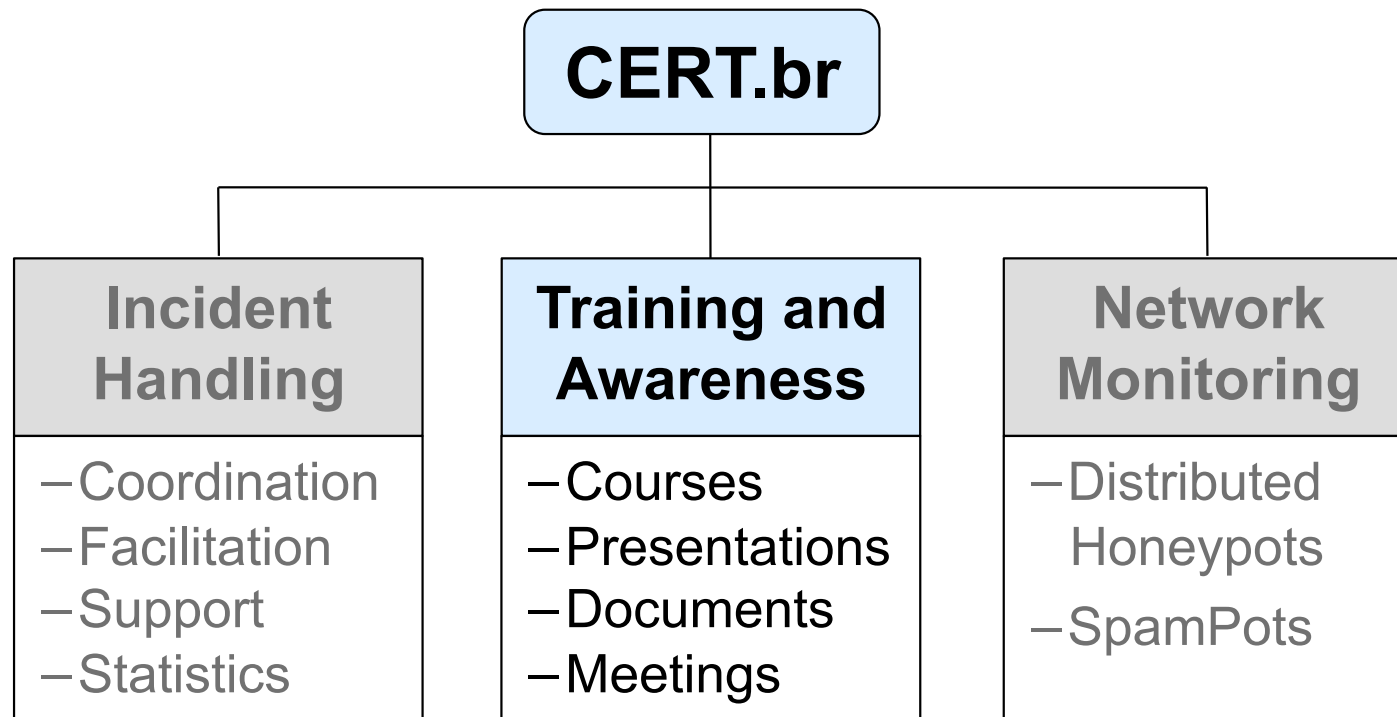
<http://www.cert.br/stats/incidentes/>

Spams Reported to CERT.br – 2003-Feb/2011

Mainly botnets and open proxies at broadband networks



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



Establishment of new CSIRTs

- **Help new Computer Security Incident Response Teams (CSIRTs) to establish their activities**
 - meetings, training and presentations at conferences
- ***SEI/CMU Partner* since 2004, delivers in Brazil the following CERT® Program courses:**

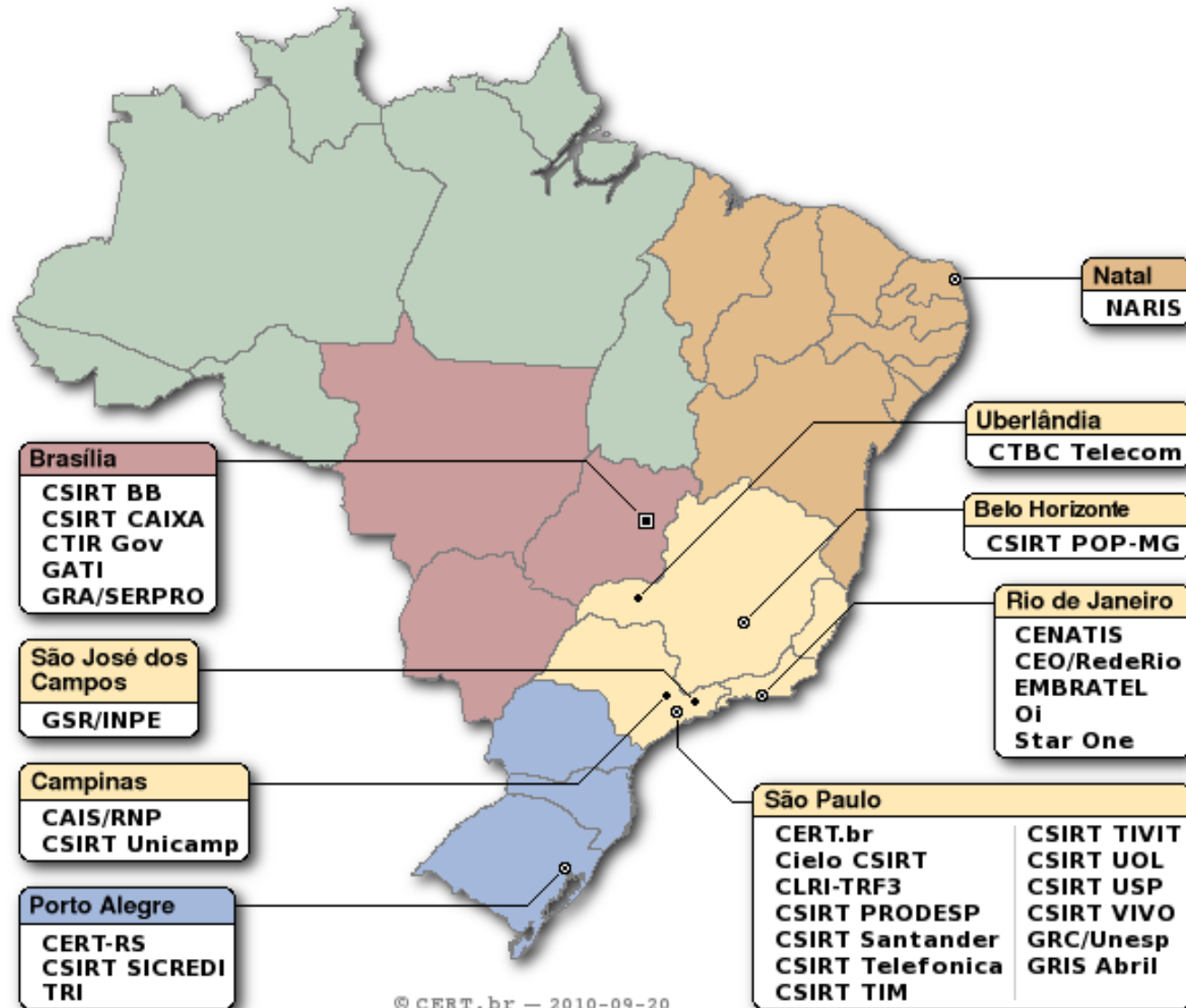


- <http://www.cert.br/courses/>
 - ***Overview of Creating and Managing CSIRTs***
 - ***Fundamentals of Incident Handling***
 - ***Advanced Incident Handling for Technical Staff***
- **400+ security professionals trained in Brazil**
- ***Overview of Creating and Managing CSIRTs* workshop delivered at 2008, 2009 and 2010 LACNIC Conferences, with permission of SEI/CMU**

Brazilian CSIRTs as of March/2011

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/>

Internet Security Best Practices – for End Users

“*Cartilha de Segurança para Internet*”

<http://cartilha.cert.br/>

The screenshot shows the website interface for the Internet Security Best Practices manual. At the top, there are navigation links: [Início](#), [Dicas](#), [Download](#), [Checklist](#), [Glossário](#), and [Livro](#). The main heading is **Cartilha de Segurança para Internet 3.1**. A **Novidade** box states that version 3.1 is available and has been edited like a book. Below this is a table of contents listing parts I through VIII, a checklist, and a glossary. A 'Dica do Dia' (Tip of the Day) section provides advice on using wireless networks. A 'Licença de Uso' (License) section lists contact, acknowledgments, revisions, and notices. A search bar is located at the bottom right.

Novidade: já está disponível a versão 3.1 da Cartilha de Segurança para Internet, que passou a ser editada também como **livro**.

A Cartilha de Segurança para Internet contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

- Parte I: Conceitos de Segurança
- Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
- Parte III: Privacidade
- Parte IV: Fraudes na Internet
- Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)
- Parte VI: Spam
- Parte VII: Incidentes de Segurança e Uso Abusivo da Rede
- Parte VIII: Códigos Maliciosos (*Malware*)
- Checklist
- Glossário

Dica do Dia

Se utilizar redes sem fio, verifique se seus equipamentos já suportam WPA (Wi-Fi Protected Access) e utilize-o sempre que possível.

[Saiba mais](#)

Licença de Uso

- Contato
- Agradecimentos
- Revisões
- Avisos

[antispam.br](#)

Busca

Antispam.br

Website and cartoons about spam and security

<http://www.antispam.br/>



Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | Antispam.br | PTT.br

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br

nic.br Núcleo de Informação e Coordenação

cgi.br Registro CERT.br

Tipos de spam

[Botar]

Fraudes

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os fraudadores têm utilizado amplamente e-mails com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os e-mails que recebem e ao utilizarem serviços de comércio eletrônico ou Internet Banking.

Sumário

Tipos de spam

[Botar]

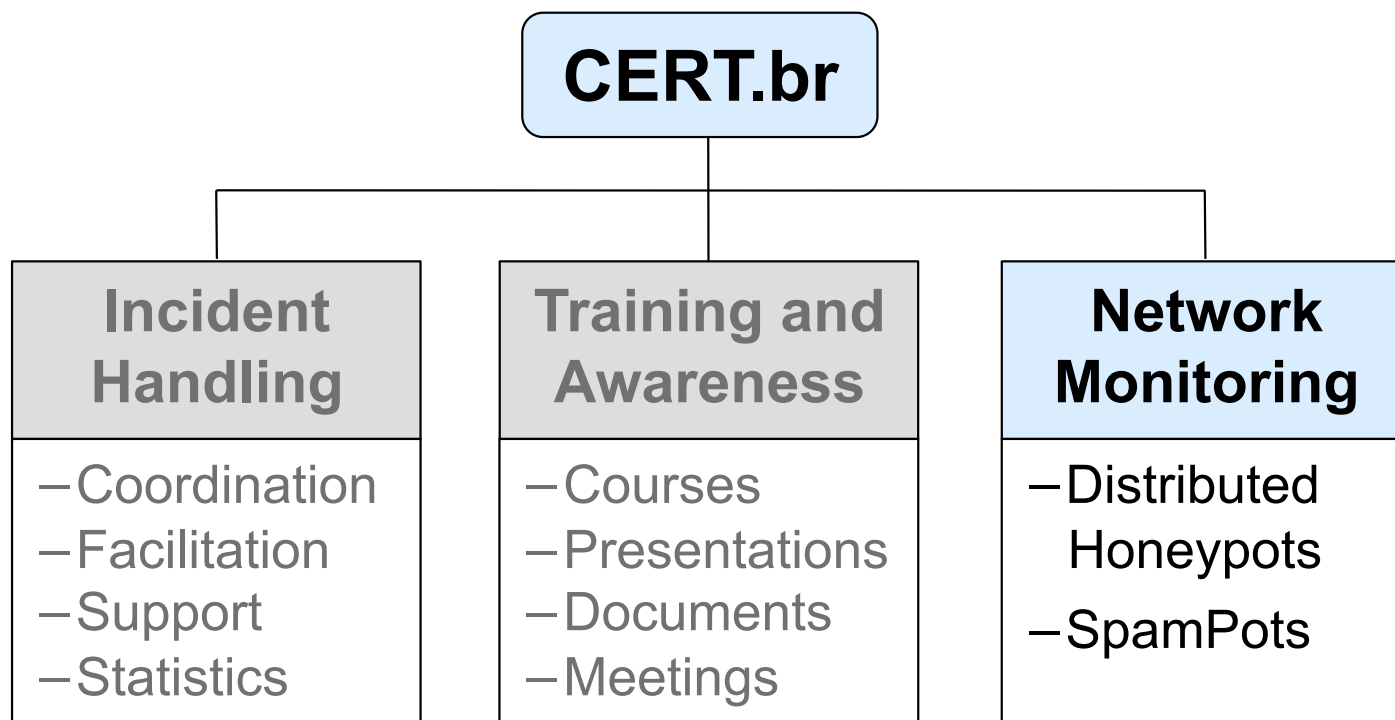
Códigos maliciosos

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em spams enviados por fraudadores.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- **Backdoor:** Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- **Spyware:** Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma

<http://www.antispam.br/videos/english/>



Use of Honeypots for Network Monitoring

CERT.br honeyTARG

Computer Emergency Response Team Brazil

honeypots for Threats and Abuse passive Reconnaissance and information Gathering

honeyTARG

This site contains statistics, papers and general information about CERT.br activities regarding the use of low-interaction honeypots for *Abuse and Threat Analysis*.

Currently we have the following projects:

- Spampots
- Distributed Honeypots for Attack Trend Analysis

SpamPots Project

The [Spampots Project](#) uses low-interaction honeypots to gather data related to the abuse of the Internet infrastructure by spammers. The main goals are:

- measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
- help develop the spam characterization research
- measure the abuse of network infrastructure to send spam
- develop better ways to

Distributed Honeypots

CERT.br maintains the [Distributed Honeypots Project](#), whose objective is to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet space.

The data produced by the project include

- Daily summaries to project partners, with detailed information about the traffic observed in each honeypot;
- A system to notify CSIRTs of networks that generate attacks against the honeypots;
- The following public statistics:

Flows

[Daily statistics](#) for the network flow data directed to honeypots from the Distributed Honeypots Project

TCP/UDP Port Summary

[Port summary statistics](#) for TCP/UDP traffic data directed to honeypots from the Distributed Honeypots Project.

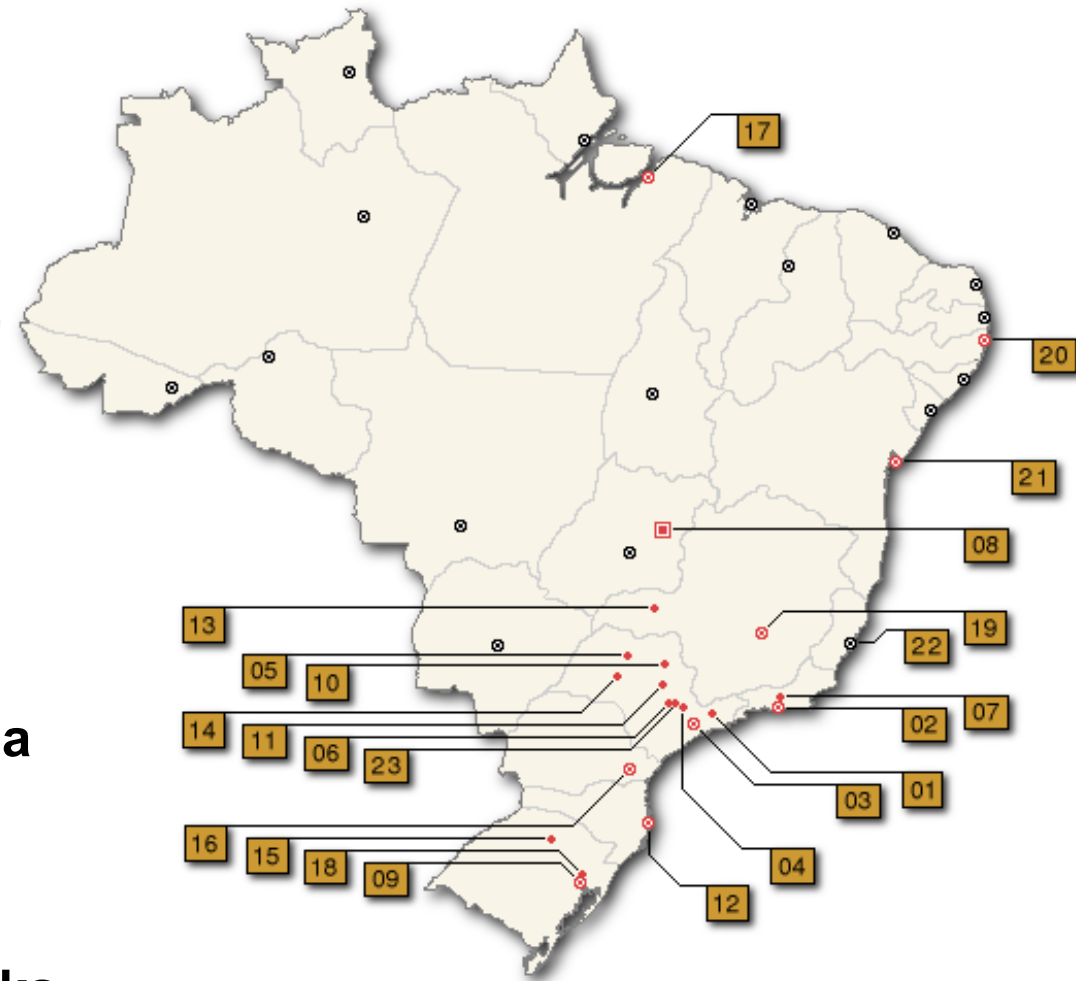
Brazilian Distributed Honeypots Project

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

- **Sensors distributed in 22 cities**
- **Hosted by 46 Partners in**
 - **government, energy, financial, ISPs, academia**
- **Based on voluntary work**
- **Transparent configuration**
 - **no “black-box”**
- **No production data is captured**
- **Each partner can use its sensor as a complement to its own IDS**

Data collected is used to

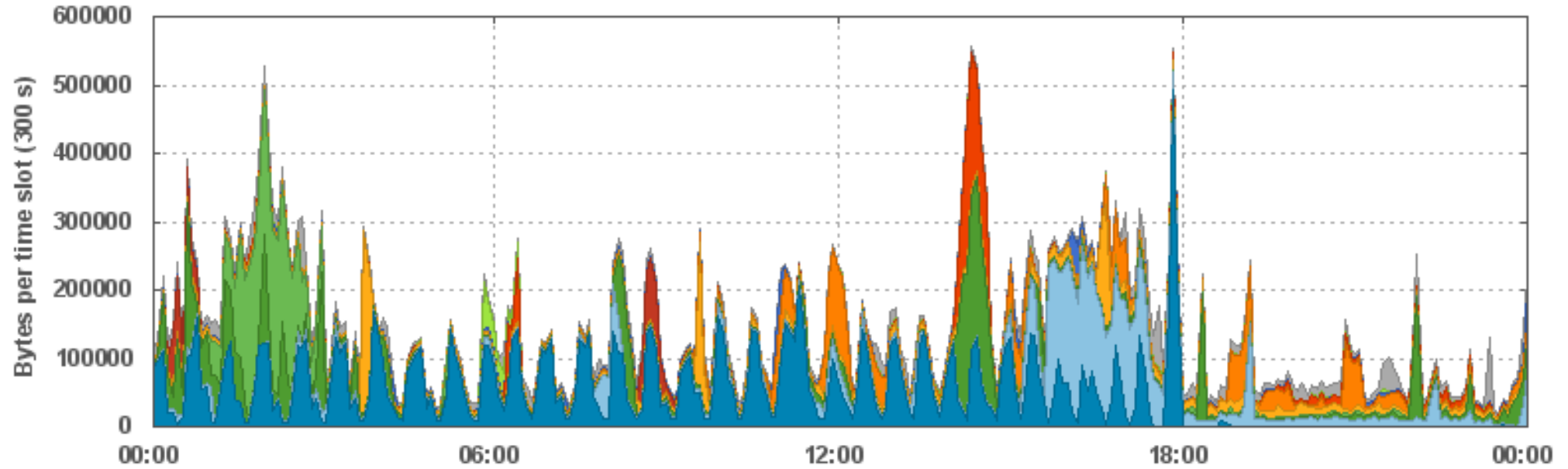
- **Notify networks that originate attacks**
- **Donate data to other National CSIRTs**
- **Generate public statistics/trends**



<http://honeytarg.cert.br/honeypots/>

Public Statistics – Country Codes originating Attacks

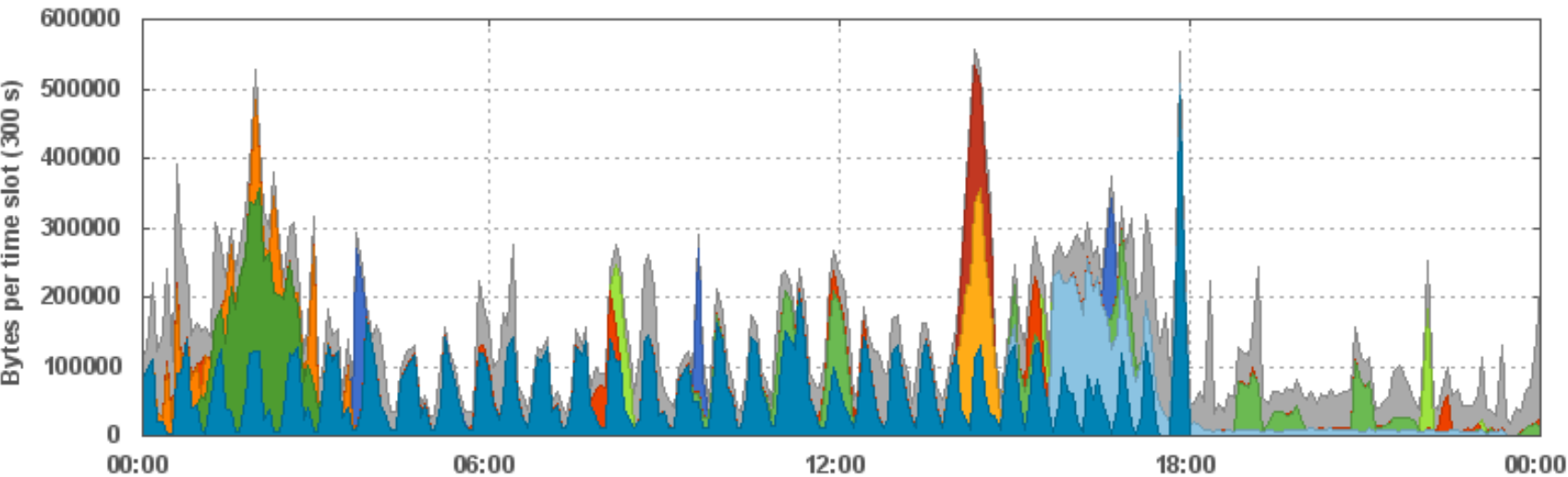
Source Country Codes (CC) -- 2011-03-04 GMT



#	Key	CC	Name	Total	Max	Avg
01		DE	Germany	14.37 MB 33.14 %	1.64 KB/s	166.30 B/s
02		CN	China	6.24 MB 14.38 %	752.61 B/s	72.19 B/s
03		US	United States	5.70 MB 13.16 %	772.56 B/s	66.02 B/s
04		MX	Mexico	3.70 MB 8.54 %	779.91 B/s	42.85 B/s
05		BR	Brazil	3.54 MB 8.16 %	904.43 B/s	40.97 B/s
06		RU	Russian Federation	2.89 MB 6.66 %	412.92 B/s	33.44 B/s
07		JP	Japan	1.58 MB 3.65 %	734.93 B/s	18.31 B/s
08		PL	Poland	820.12 KB 1.89 %	294.33 B/s	9.49 B/s
09		TW	Taiwan, Province of China	649.69 KB 1.50 %	207.70 B/s	7.52 B/s
10		EU	NA	379.51 KB 0.88 %	228.13 B/s	4.39 B/s
11		Others		3.49 MB 8.04 %	309.69 B/s	40.36 B/s

Public Statistics – ASes originating Attacks

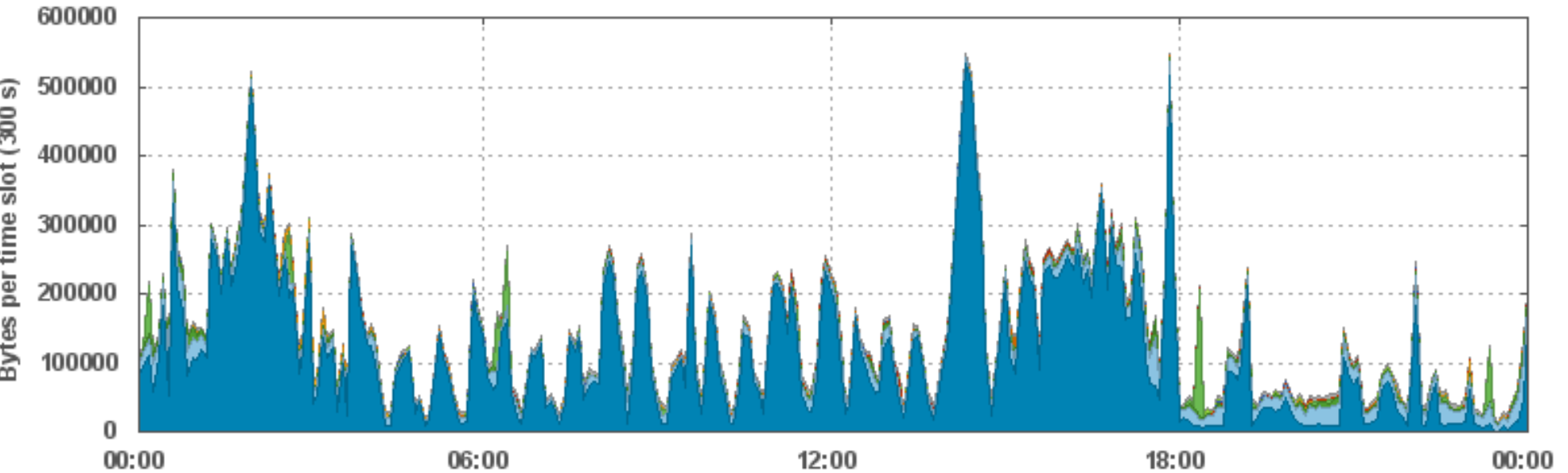
Source AS Numbers (ASN) -- 2011-03-04 GMT



#	Key	ASN	Name	CC	Total	Max	Avg
01		8972	PLUSSERVER-AS PlusServer AG, G...	DE	14.16 MB 32.66 %	1.64 KB/s	163.89 B/s
02		4835	CHINANET-IDC-SN China Telecom ...	CN	3.55 MB 8.19 %	743.61 B/s	41.08 B/s
03		6503	Axtel, S.A.B. de C.V.	MX	3.32 MB 7.66 %	779.91 B/s	38.43 B/s
04		12768	ER-TELECOM-AS JSC ER-Telecom	RU	2.45 MB 5.64 %	408.31 B/s	28.32 B/s
05		8001	NET-ACCESS-CORP - Net Access C...	US	1.40 MB 3.24 %	758.00 B/s	16.25 B/s
06		46475	LIMESTONENETWORKS - Limestone ...	US	1.24 MB 2.85 %	669.49 B/s	14.32 B/s
07		4134	CHINANET-BACKBONE No.31,Jin-ro...	CN	1.20 MB 2.76 %	268.80 B/s	13.87 B/s
08		9371	SAKURA-C SAKURA Internet Inc.	JP	1.01 MB 2.34 %	731.37 B/s	11.73 B/s
09		27664	CTBC MultimAdia	BR	998.47 KB 2.30 %	869.11 B/s	11.56 B/s
10		33657	CMCS - Comcast Cable Communica...	US	778.74 KB 1.80 %	568.75 B/s	9.01 B/s
11		Others			13.25 MB 30.56 %	711.43 B/s	153.38 B/s

Public Statistics – Top TCP Ports Scanned

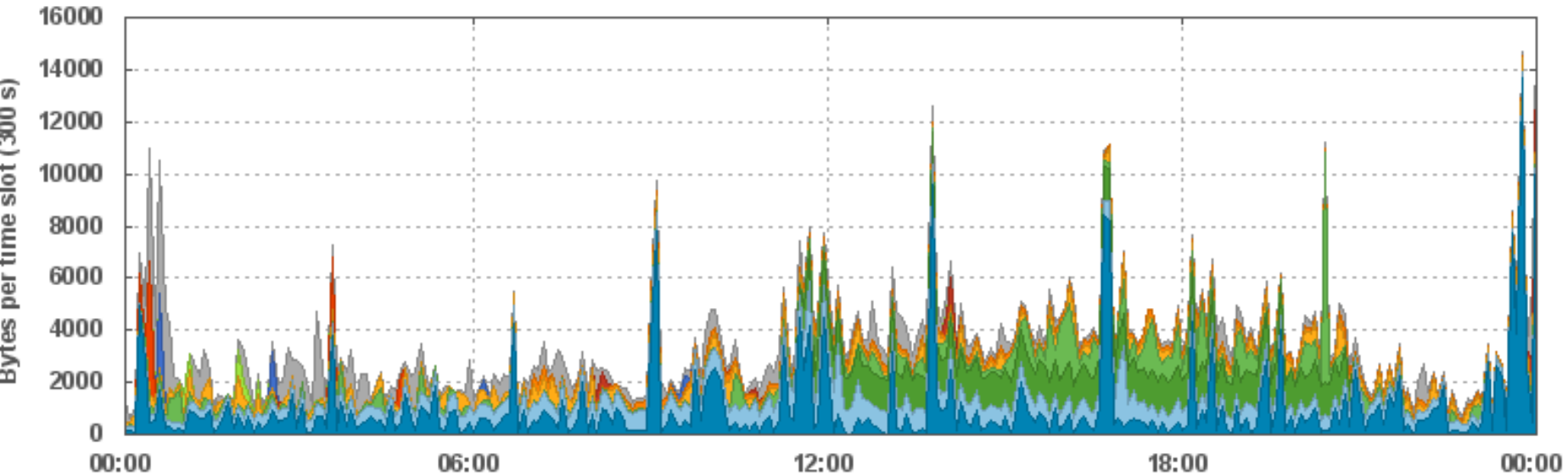
Destination TCP Ports -- 2011-03-04 GMT



#	Key	Port	Name	Total	Max	Avg
01	■	22	SSH (Secure Shell)	33.20 MB 80.07 %	1.77 KB/s	384.24 B/s
02	■	445	Microsoft-DS Active Directory	4.26 MB 10.27 %	224.78 B/s	49.28 B/s
03	■	139	NETBIOS Session Service	1.01 MB 2.44 %	87.04 B/s	11.70 B/s
04	■	9988	Rbot/SpyBot	709.86 KB 1.71 %	602.90 B/s	8.22 B/s
05	■	80	HTTP (Hypertext Transfer Protocol)	218.09 KB 0.53 %	69.23 B/s	2.52 B/s
06	■	1433	Microsoft SQL Server	142.71 KB 0.34 %	59.49 B/s	1.65 B/s
07	■	4899	Radmin (remote administration tool)	99.53 KB 0.24 %	14.83 B/s	1.15 B/s
08	■	135	Microsoft RCP	95.22 KB 0.23 %	38.12 B/s	1.10 B/s
09	■	1080	SOCKS	92.35 KB 0.22 %	19.72 B/s	1.07 B/s
10	■	5900	VNC (Virtual Network Computing)	74.83 KB 0.18 %	19.85 B/s	0.87 B/s
11	■	Others		1.56 MB 3.77 %	45.54 B/s	18.09 B/s

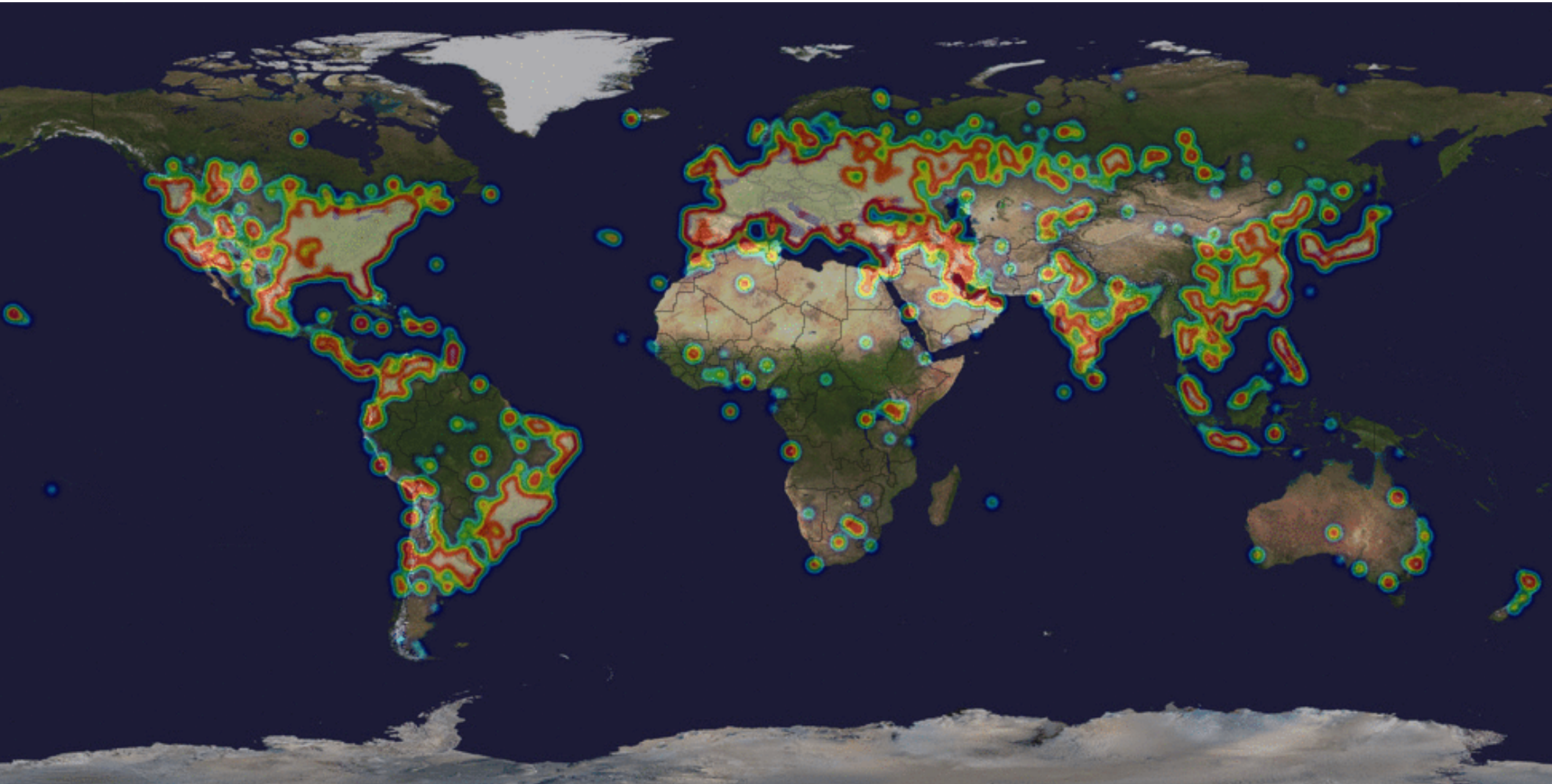
Public Statistics – Top UDP Ports Scanned

Destination UDP Ports -- 2011-03-04 GMT



#	Key	Port	Name	Total	Max	Avg
01	■	5060	SIP (Session Initiation Protocol)	288.78 KB 29.28 %	45.68 B/s	3.34 B/s
02	■	53	DNS (Domain Name System)	175.77 KB 17.82 %	10.41 B/s	2.03 B/s
03	■	161	SNMP (Simple Network Management Protocol)	141.68 KB 14.36 %	4.22 B/s	1.64 B/s
04	■	137	NETBIOS Name Service	101.30 KB 10.27 %	29.25 B/s	1.17 B/s
05	■	1434	Microsoft SQL Monitor	76.68 KB 7.77 %	4.80 B/s	0.89 B/s
06	■	21665	n/a	38.14 KB 3.87 %	1.67 B/s	0.44 B/s
07	■	36135	n/a	9.80 KB 0.99 %	16.92 B/s	0.11 B/s
08	■	35623	n/a	7.36 KB 0.75 %	6.07 B/s	0.09 B/s
09	■	39207	n/a	5.37 KB 0.54 %	9.38 B/s	0.06 B/s
10	■	4903	n/a	4.96 KB 0.50 %	3.38 B/s	0.06 B/s
11	■	Others		136.49 KB 13.84 %	17.00 B/s	1.58 B/s

Public Statistics – Next Month: Heat Maps



SpamPots Project

CERT.br honeyTARG – SpamPots Project

http://honeytarg.cert.br/spampots/

Reader ↻

Google

honeyTARG

SpamPots Project



The Spampots Project, coordinated by CERT.br, uses low-interaction honeypots to gather data related to the abuse of the Internet infrastructure by spammers. The main goals are:

- measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
- help develop the spam characterization research
- measure the abuse of network infrastructure to send spam
- develop better ways to
 - identify phishing and malware
 - identify botnets via the abuse of open proxies and relays

Data Mining Research



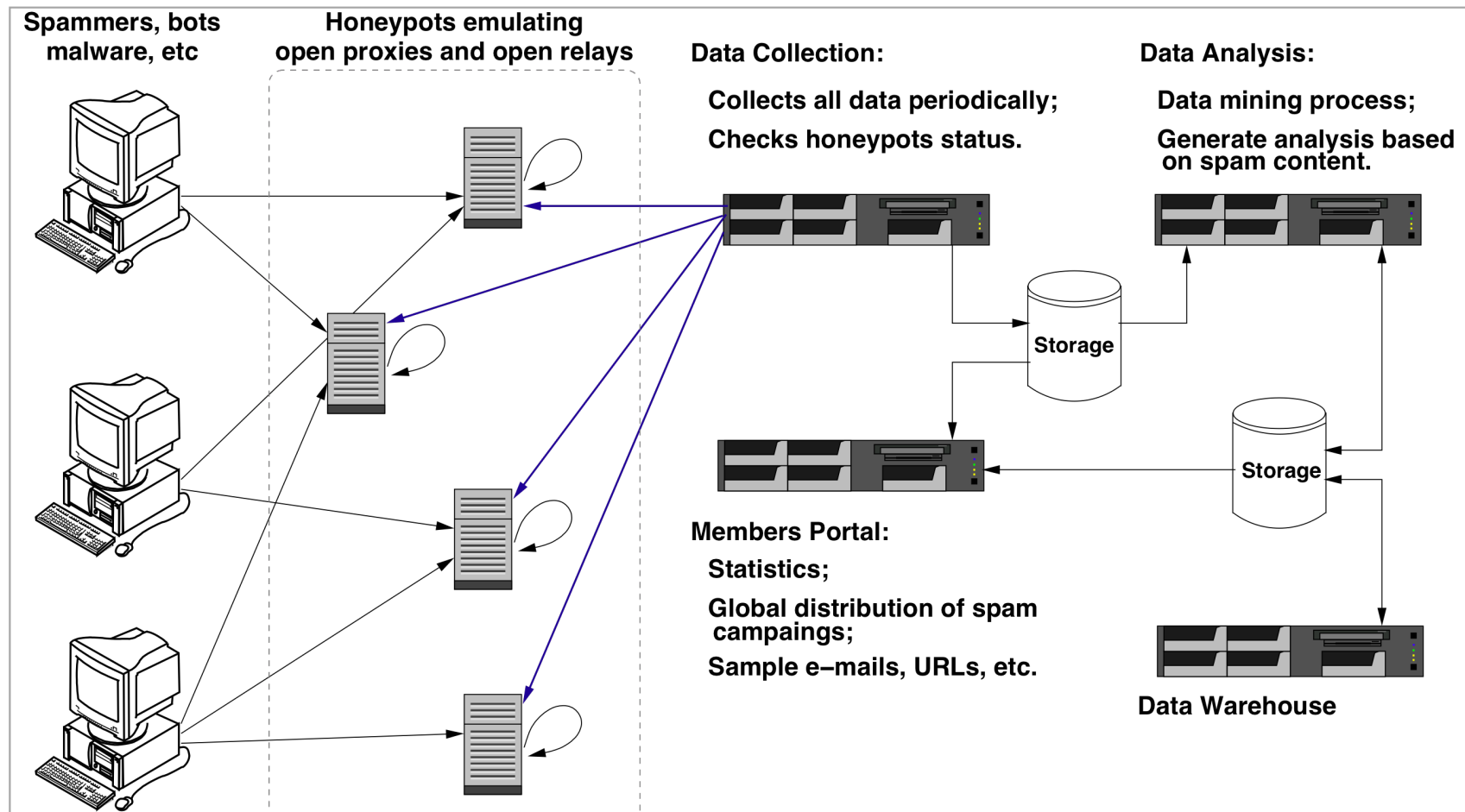
The spam characterization and data mining research, SpamMining, is being developed by the e-Speed Laboratory, from the Federal University of Minas Gerais (UFMG)

Papers in English

- **Exploring the Spam Arms Race to Characterize Spam Evolution**
 Pedro H. Calais Guerra, Dorgival Guedes, Wagner Meira Jr., Cristine Hoepers, Marcelo H. P. C. Chaves, Klaus Steding-Jessen.
 Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS'10), 2010, Redmond, USA.
[PDF File](#) (240 KB)
- **Spam Miner: A Platform for Detecting and Characterizing Spam Campaigns (demo paper)**
 Pedro H. Calais Guerra, Douglas Pires, Marco Túlio Ribeiro, Dorgival Guedes, Wagner Meira Jr., Cristine Hoepers, Marcelo H. P. C. Chaves, Klaus Steding-Jessen.
 International Conference on Knowledge Discovery and Data Mining (KDD'09), 2009, Paris, France.
[PDF File](#) (400 KB)
- **Spamming Chains: A New Way of Understanding Spammer Behavior**
 Pedro H. Calais Guerra, Dorgival Guedes, Wagner Meira Jr., Cristine Hoepers, Marcelo H. P. C. Chaves, Klaus Steding-Jessen.

SpamPots Project – Overview of the Architecture

- **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), CSIRT UTPL (EC), SURFcert (NL), TWCERT/CC (TW), University of Washington (US), CSIRT Antel (UY)



SpamPots Project Objectives

Better understand the abuse of the Internet infrastructure by spammers

- **Measure the problem from a different point of view: abuse of infrastructure X spams received at the destination**
- **Help develop the spam characterization research**
- **Measure the abuse of end-user machines to send spam**
- **Use the spam collected to improve antispam filters**
- **Develop better ways to**
 - **identify phishing and malware**
 - **identify botnets via the abuse of open proxies and relays**

We provide a grant to the e-Speed Laboratory of the Federal University of Minas Gerais (UFMG) to develop research with the data collected

Improving cooperation in spam fighting

- **Provide data to trusted parties**
- **Help their constituency to identify infected machines**
- **Identify malware and scams targeting their constituency**
- **Currently providing data about spams coming from networks assigned to**
 - **JP - to JADAC / IJ / JPCERT/CC / Min. of Communications – had a workshop in Brazil with representatives from these organizations and local ISPs and network providers to discuss how to reduce spam and network abuse**
 - **TW - to NCC-TW – they are using the data to shutdown spammers infrastructures**

Links

- **CGI.br – Brazilian Internet Steering Committee**
<http://www.cgi.br/>
- **NIC.br – Network Information Center Brazil**
<http://www.nic.br/>
- **CERT.br – Computer Emergency Response Team Brazil**
<http://www.cert.br/>
- **honeyTARG – honeypots for Threats and Abuse passive Reconnaissance and information Gathering**
<http://honeytarg.cert.br/>