# honeyTARG Chapter Activities

**Marcelo Chaves**
**`mhp@cert.br`**

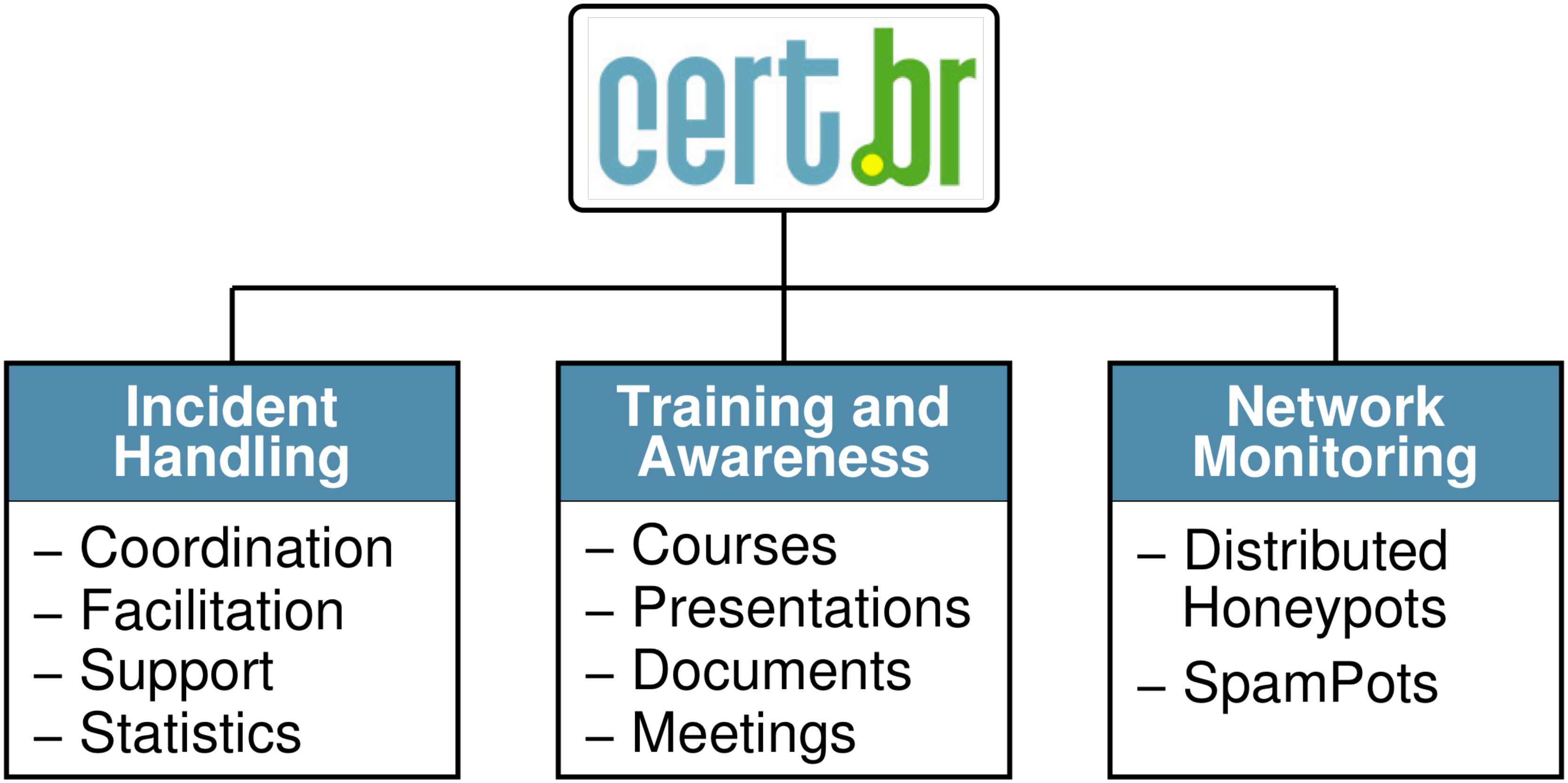
Computer Emergency Response Team Brazil - **CERT.br**

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

# Agenda

- Our Organization and Mission
- Chapter activities
  - Distributed Honeypots Project
  - SpamPots Project

# CERT.br Activities



cert.br

**Incident Handling**

- – Coordination
- – Facilitation
- – Support
- – Statistics

**Training and Awareness**

- – Courses
- – Presentations
- – Documents
- – Meetings

**Network Monitoring**

- – Distributed Honeypots
- – SpamPots

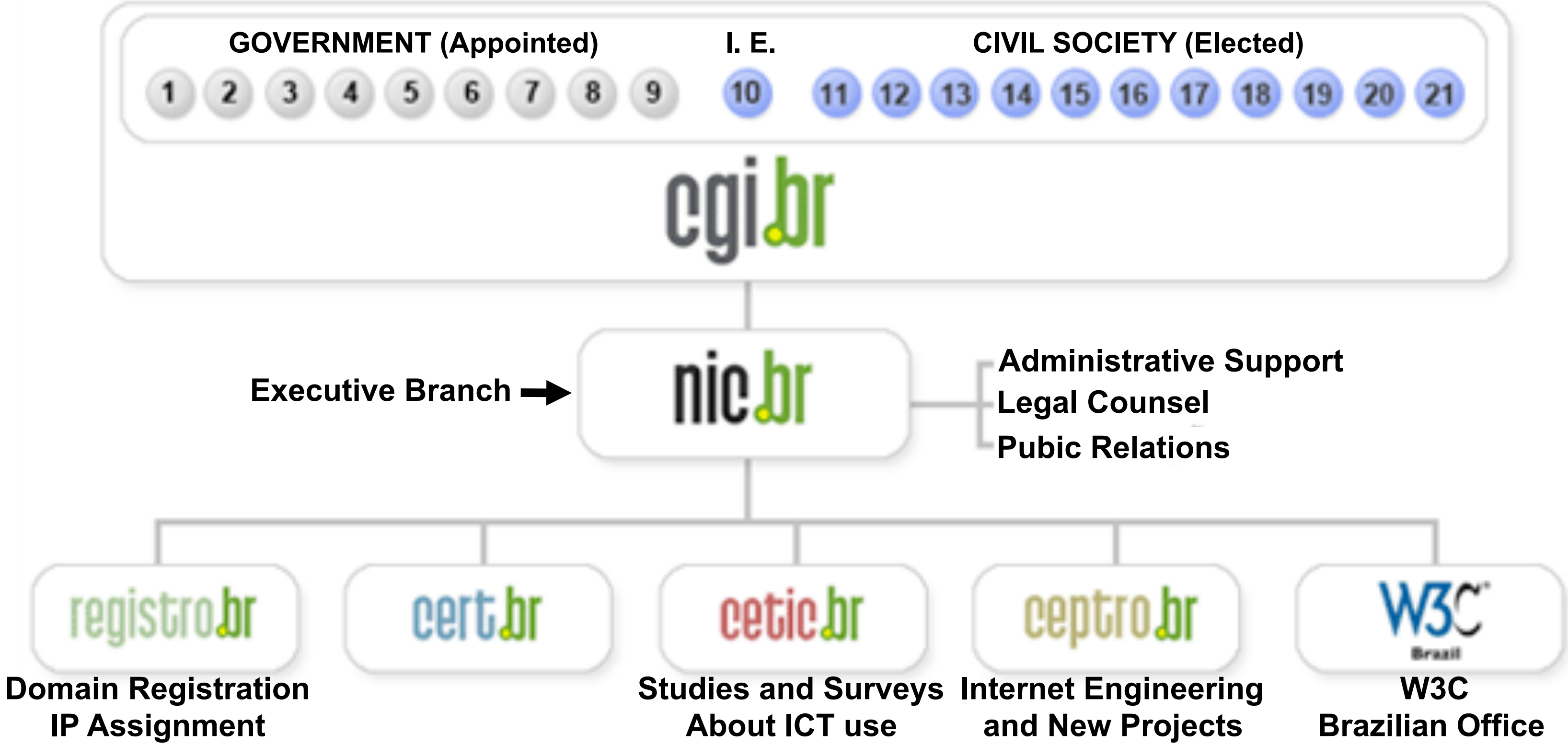
FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon.

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

# CGI.br and NIC.br Structure



GOVERNMENT (Appointed)

I. E.

CIVIL SOCIETY (Elected)

Executive Branch

Administrative Support

Legal Counsel

Pubic Relations

Domain Registration
IP Assignment

Studies and Surveys
About ICT use

Internet Engineering
and New Projects

W3C
Brazilian Office

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

# 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.

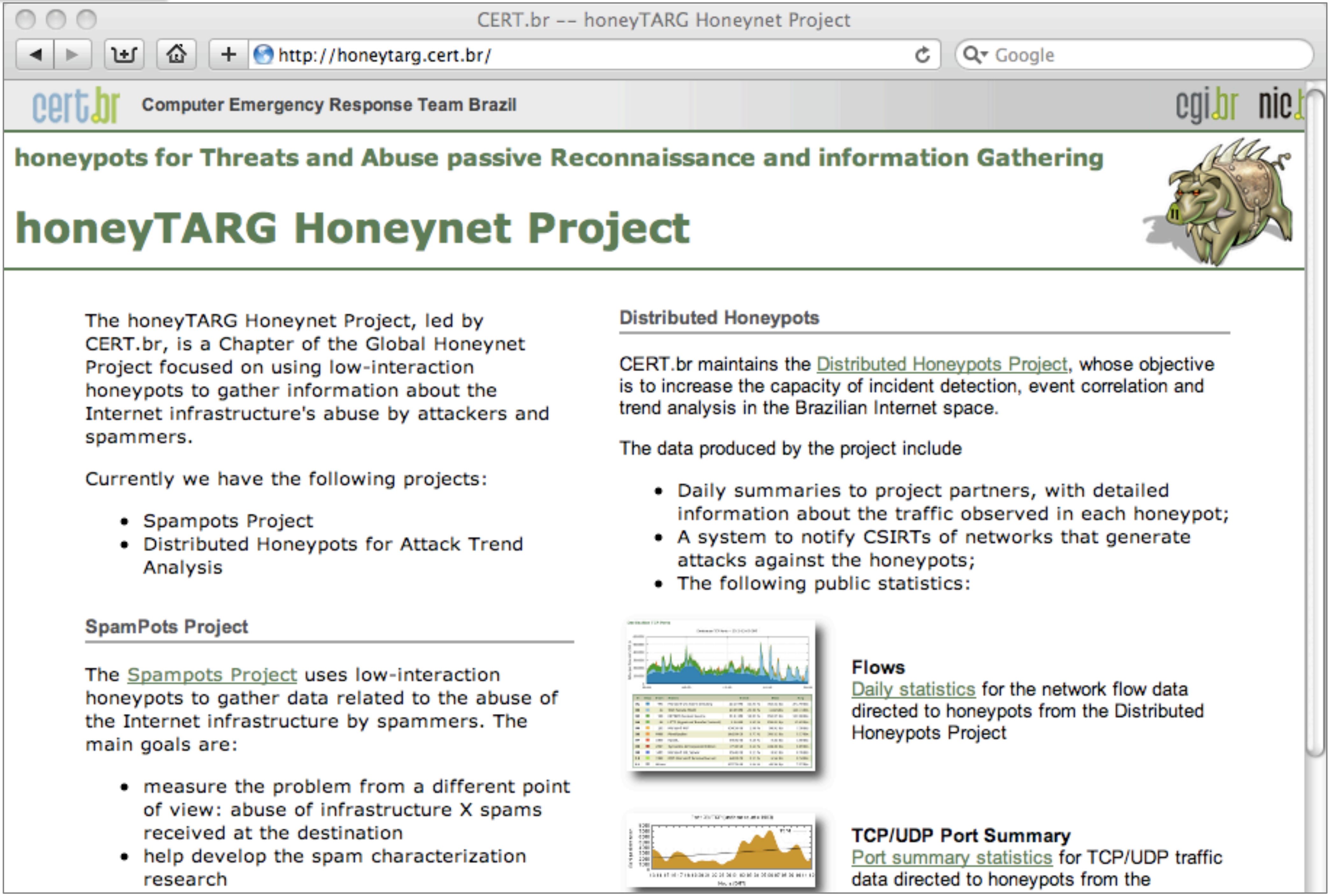
Among the diverse responsibilities reinforced by the Presidential Decree 4.829, has as the main attributions:

- 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/

Núcleo de Informação e Coordenação do Ponto BR

# Use of Honeypots for Network Monitoring


CERT.br -- honeyTARG Honeynet Project
http://honeytarg.cert.br/
Google
Computer Emergency Response Team Brazil

honeypots for Threats and Abuse passive Reconnaissance and information Gathering

## honeyTARG Honeynet Project

The honeyTARG Honeynet Project, led by CERT.br, is a Chapter of the Global Honeynet Project focused on using low-interaction honeypots to gather information about the Internet infrastructure's abuse by attackers and spammers.

Currently we have the following projects:

- Spampots Project
- 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

### 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

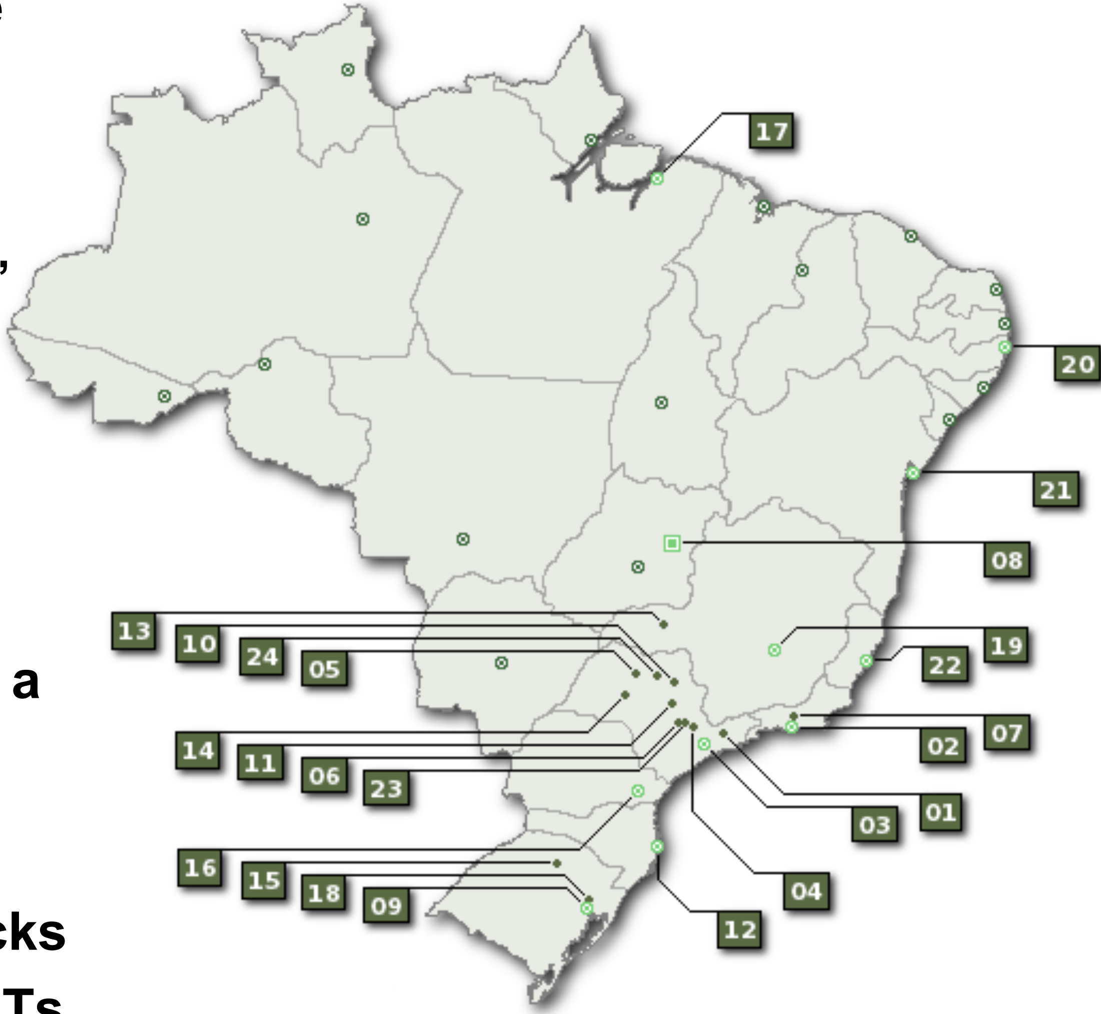
# Brazilian Distributed Honeypots Project

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

- 51 sensors distributed in 22 cities
- Hosted by 41 Partners in
  - government, energy, telecom, 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

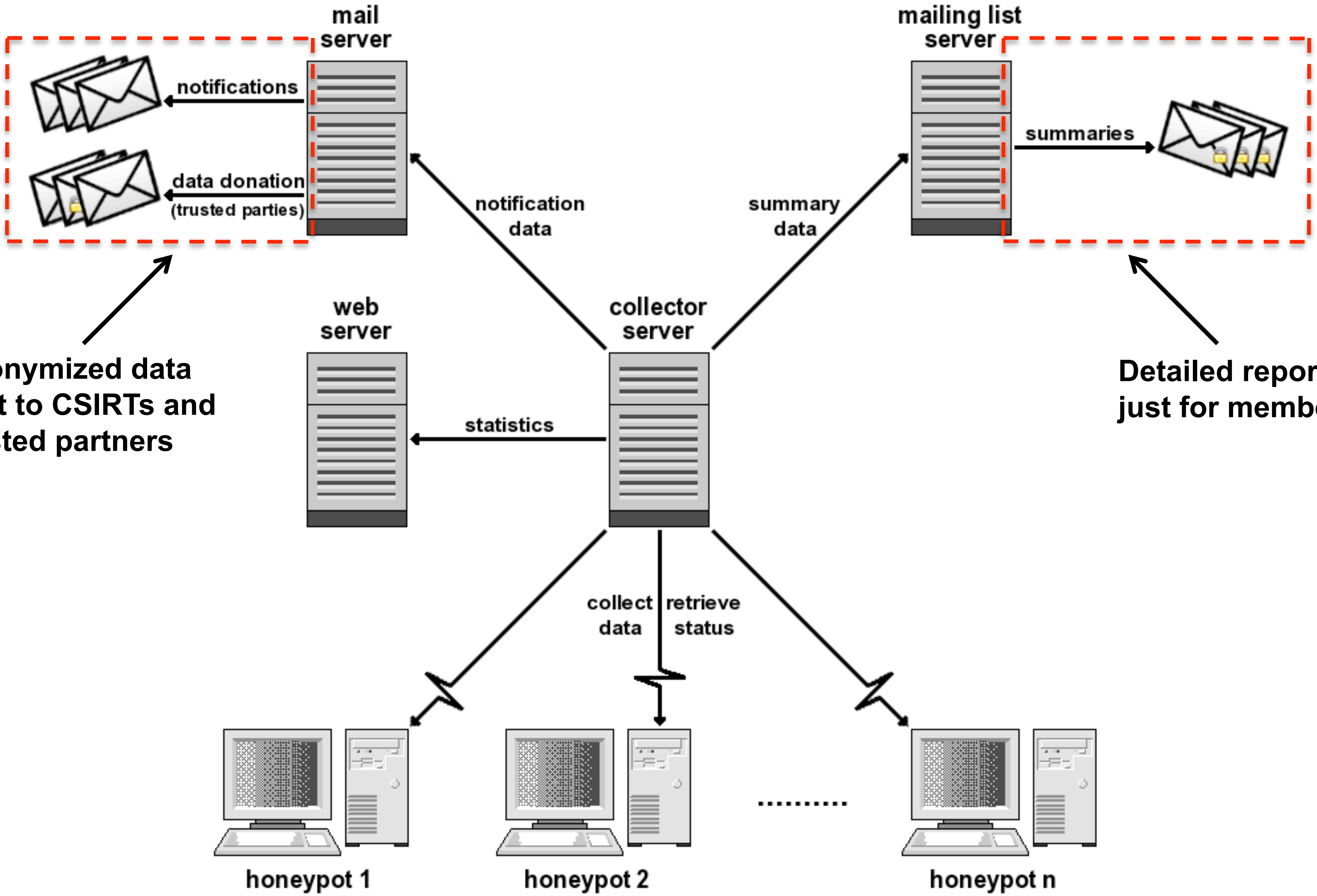
Data collected is used to

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



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

# Architecture of the Network of Honeypots



Anonymized data sent to CSIRTs and trusted partners

Detailed reports just for members

# Uses of the Data to Help the Community

## Individual Incident Notifications

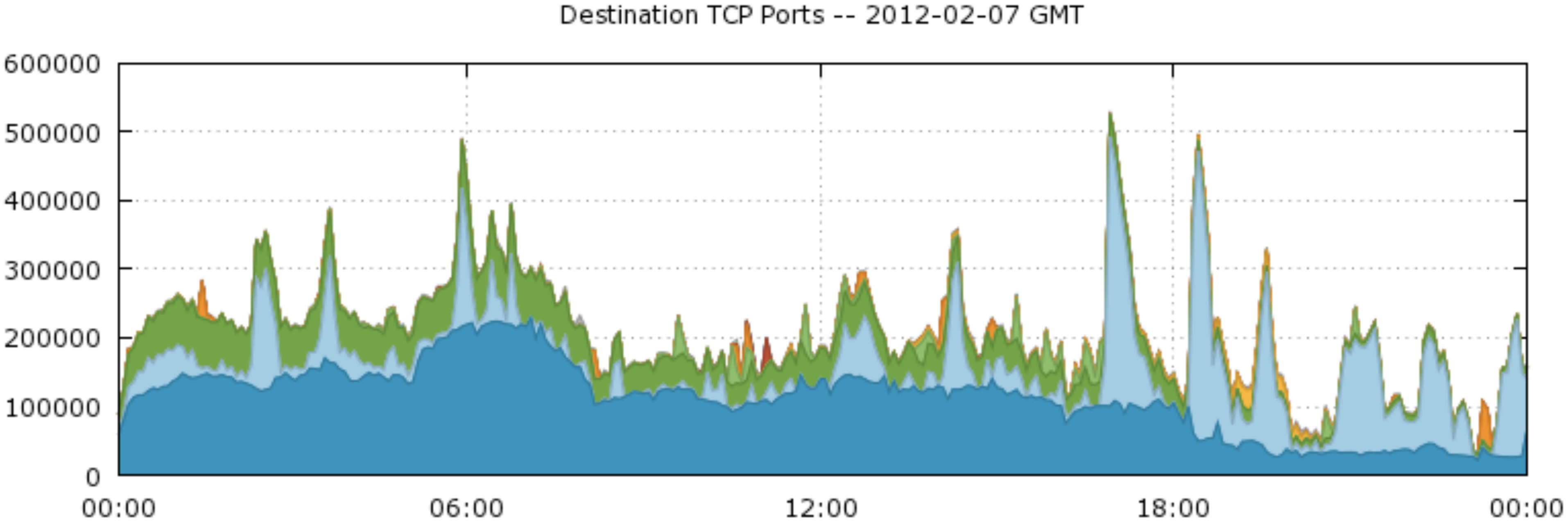
- Only for IPs allocated to Brazil
- Sent to whois contacts and CSIRTs (when one exists)
- With anonymized logs
- Includes a description of the problem, how to identify compromised machines, how to recover, etc

## Daily donation of anonymized data

- To CSIRTs with national responsibility
  - All traffic coming from IPs allocated to the given country
- To organizations that share data with ISPs
  - Team Cymru (SSH brute force attacks and some botnet traffic)
  - Shadowserver Foundation (SSH brute force attacks)
  - Arbor ATLAS (SSH brute force attacks)

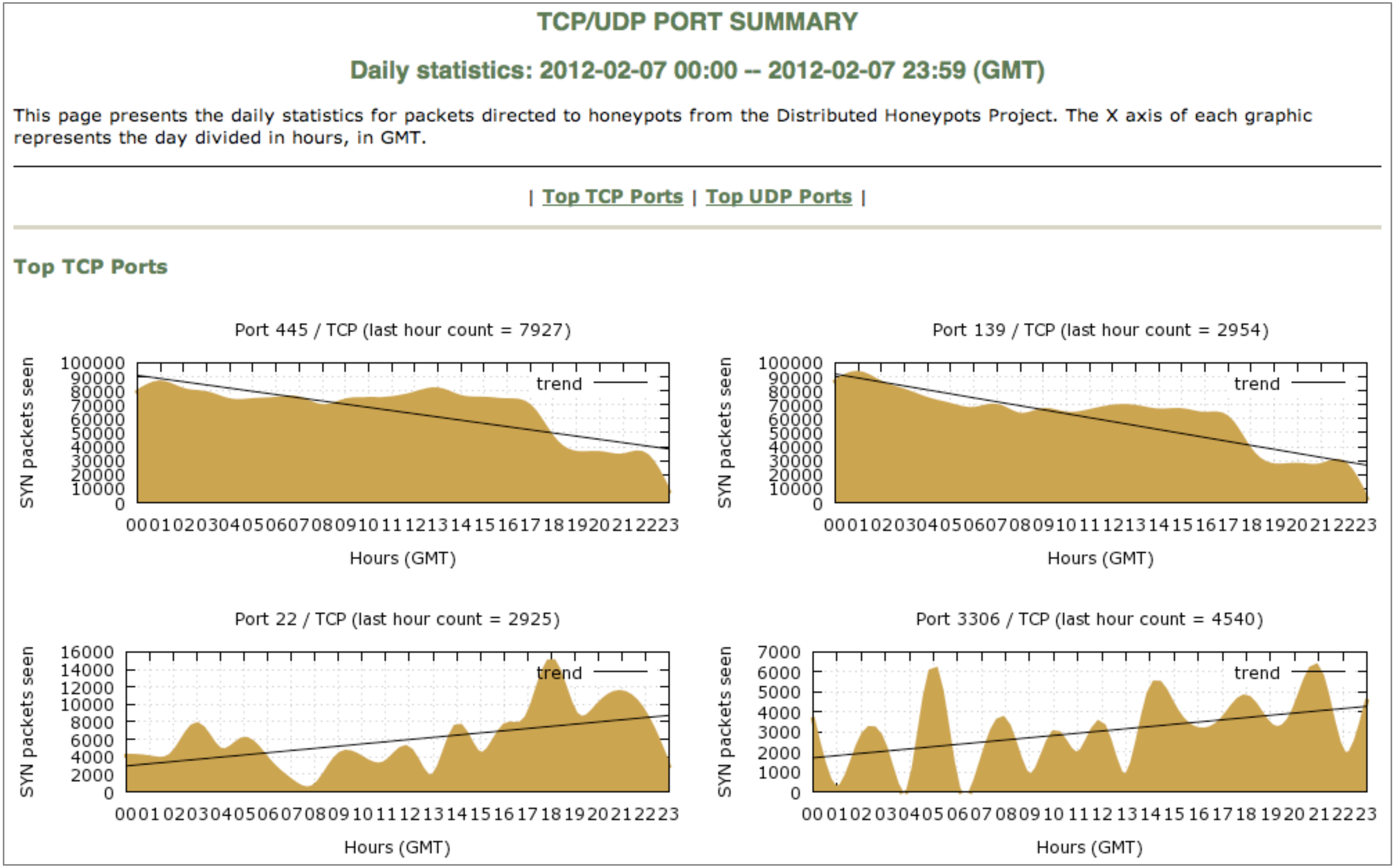
Núcleo de Informação e Coordenação do Ponto BR

# Public Statistics: Flows - Top TCP Destination Ports


Destination TCP Ports -- 2012-02-07 GMT

| # | Key | Port | Name | Total | | Max | Avg |
|---|---|---|---|---|---|---|---|
| 01 | 🟦 | 445 | Microsoft-DS Active Directory | 32.10 MB | 52.95 % | 762.52 B/s | 371.49 B/s |
| 02 | 🟦 | 22 | SSH (Secure Shell) | 13.89 MB | 22.90 % | 1.41 KB/s | 160.71 B/s |
| 03 | 🟩 | 139 | NETBIOS Session Service | 11.41 MB | 18.82 % | 250.07 B/s | 132.08 B/s |
| 04 | 🟩 | 80 | HTTP (Hypertext Transfer Protocol) | 1.18 MB | 1.95 % | 239.61 B/s | 13.65 B/s |
| 05 | 🟧 | 135 | Microsoft RCP | 654.55 KB | 1.08 % | 98.91 B/s | 7.58 B/s |
| 06 | 🟧 | 9988 | Rbot/SpyBot | 464.09 KB | 0.77 % | 195.51 B/s | 5.37 B/s |
| 07 | 🟥 | 3306 | MySQL | 94.31 KB | 0.16 % | 9.22 B/s | 1.09 B/s |
| 08 | 🟥 | 2967 | Symantec AV Corporate Edition | 77.32 KB | 0.13 % | 134.36 B/s | 0.89 B/s |
| 09 | 🟦 | 1433 | Microsoft SQL Server | 65.41 KB | 0.11 % | 8.61 B/s | 0.76 B/s |
| 10 | 🟩 | 3389 | RDP (Microsoft Terminal Server) | 64.03 KB | 0.11 % | 6.56 B/s | 0.74 B/s |
| 11 | ⬜ | Others | | 627.70 KB | 1.04 % | 42.34 B/s | 7.27 B/s |

# Public Statistics: Port Summary



## TCP/UDP PORT SUMMARY

### Daily statistics: 2012-02-07 00:00 -- 2012-02-07 23:59 (GMT)

This page presents the daily statistics for packets directed to honeypots from the Distributed Honeypots Project. The X axis of each graphic represents the day divided in hours, in GMT.

| Top TCP Ports | Top UDP Ports |

### Top TCP Ports

Port 445 / TCP (last hour count = 7927)

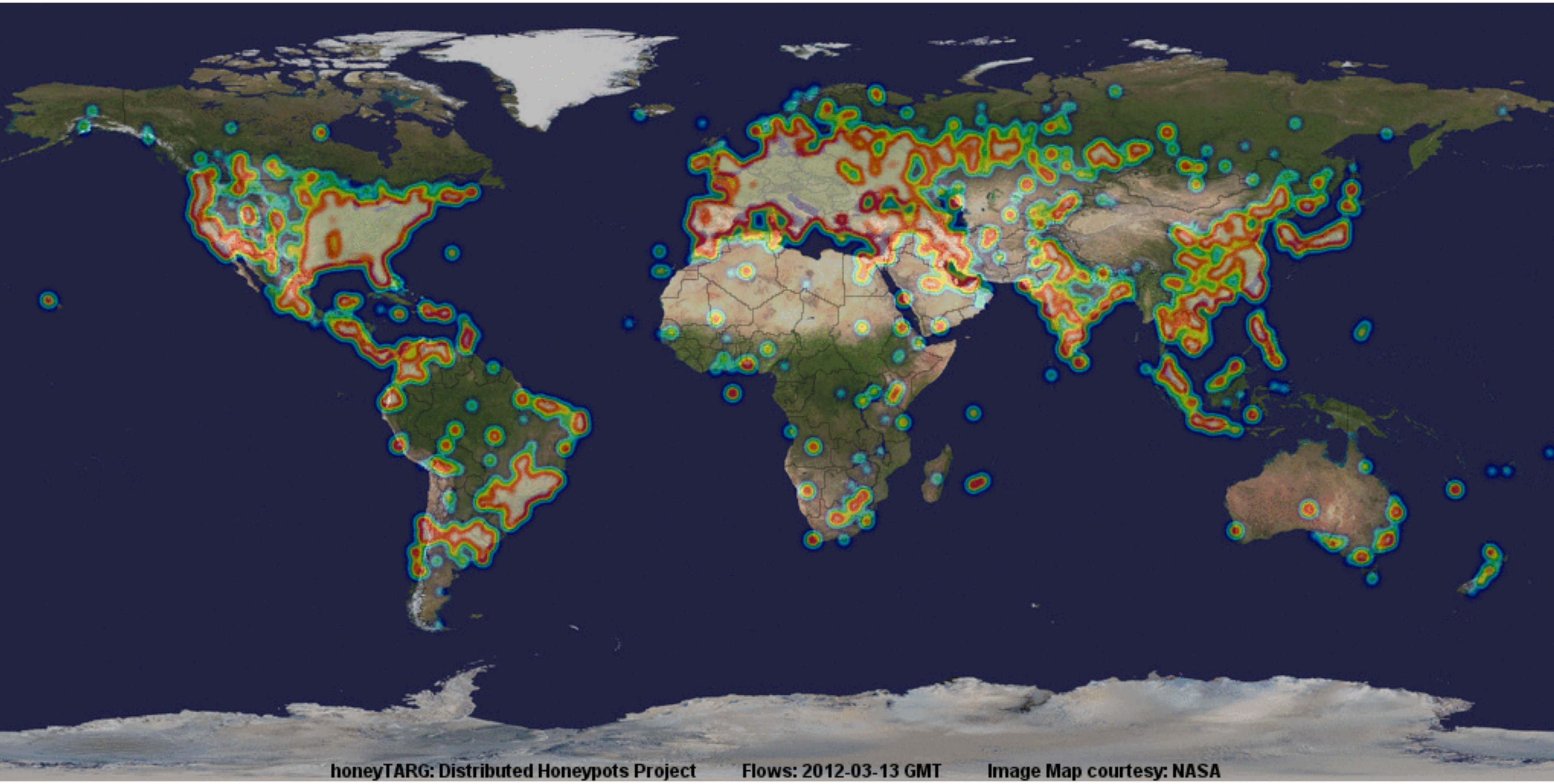
Port 139 / TCP (last hour count = 2954)

Port 22 / TCP (last hour count = 2925)

Port 3306 / TCP (last hour count = 4540)

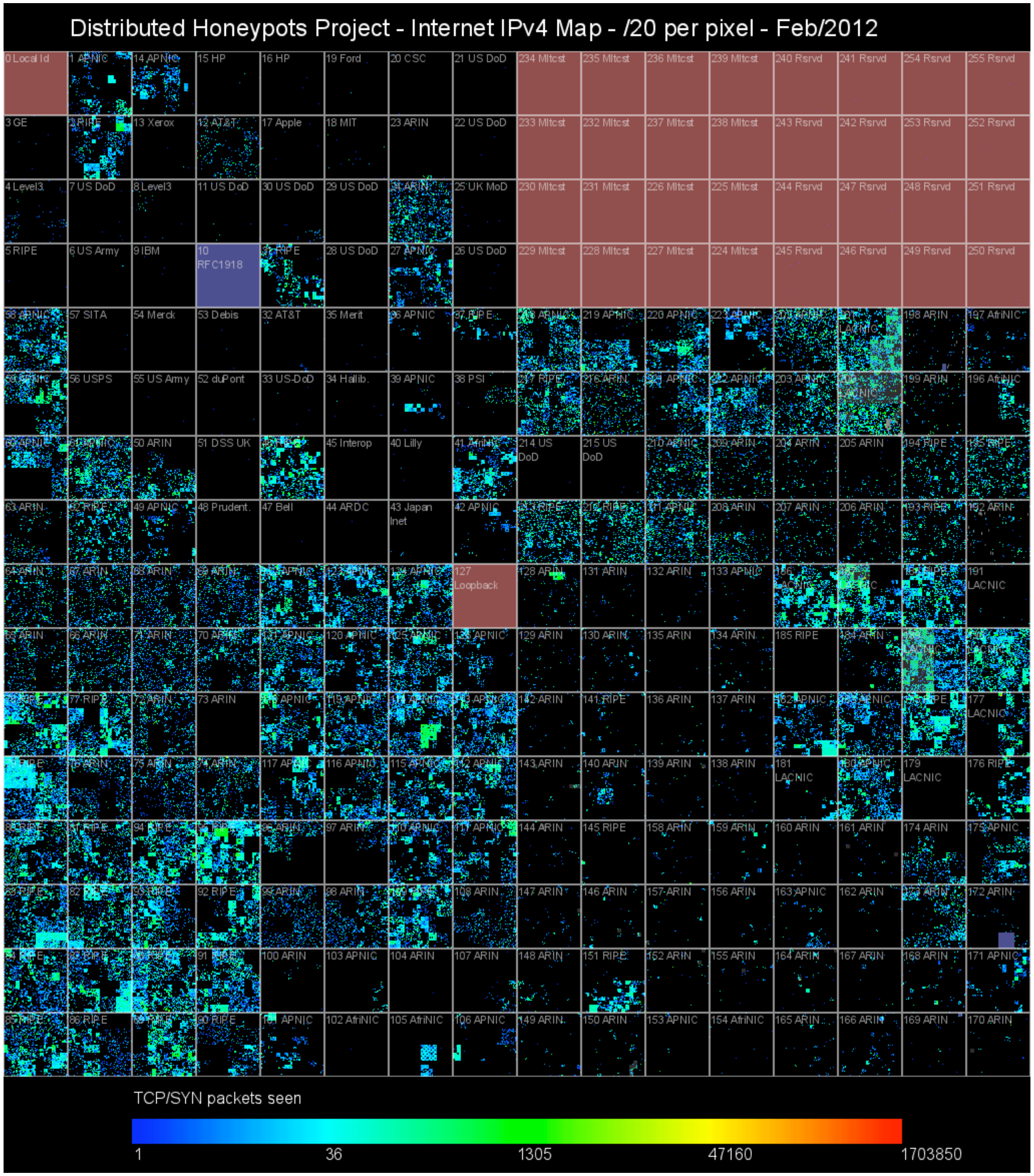
# Public Statistics: Heat Maps (future work)

- Daily image based on flows directed to the honeypots
- Daily animated GIF based on syn packets seen by the honeypots (1-hour frame)

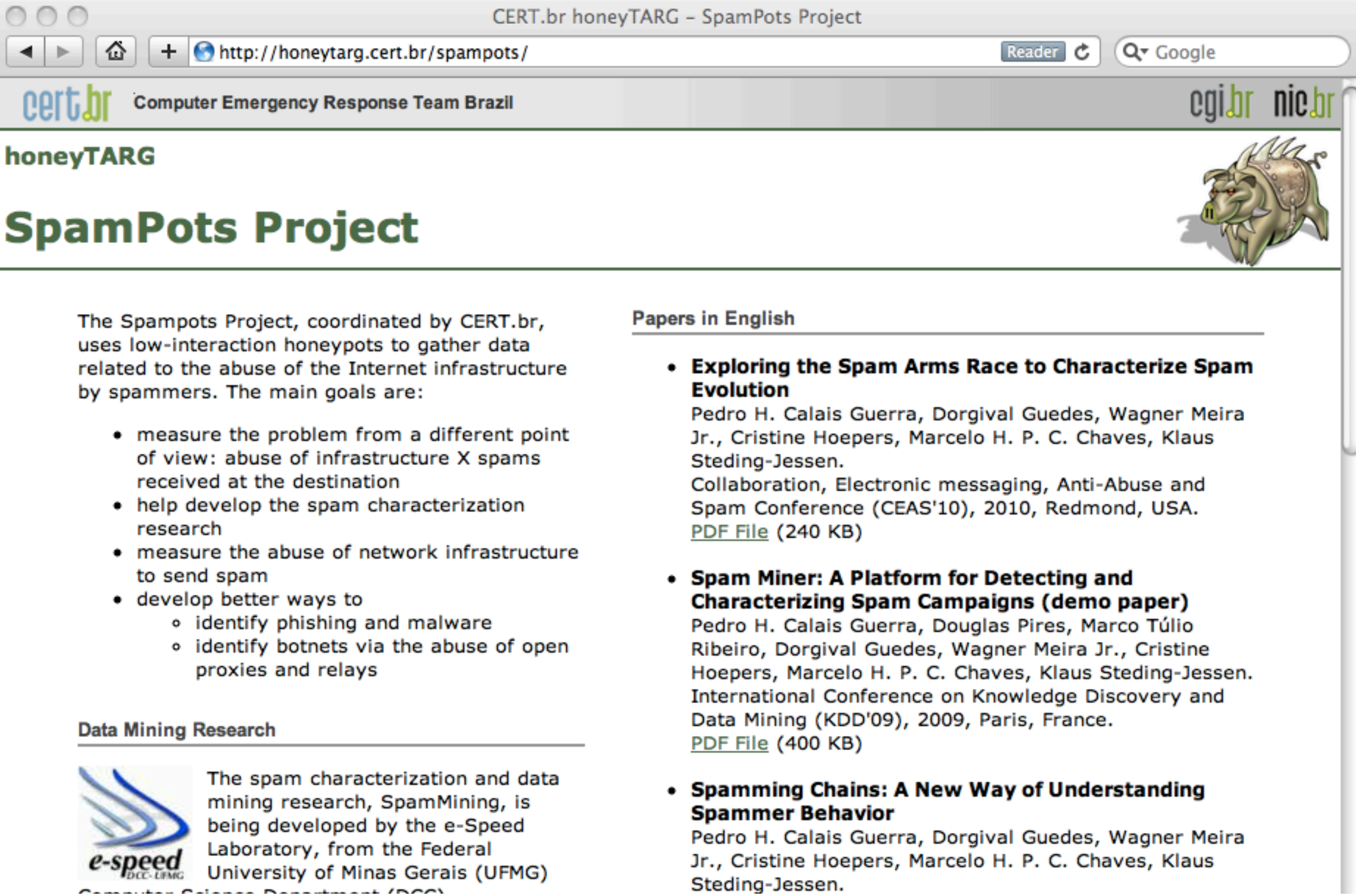


Núcleo de Informação e Coordenação do Ponto BR

# Public Statistics: Hilbert Map (future work)



# SpamPots Project


CERT.br honeyTARG – SpamPots Project
http://honeytarg.cert.br/spampots/
Reader
Google
Computer Emergency Response Team Brazil
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) Computer Science Department (DCC)

### 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.

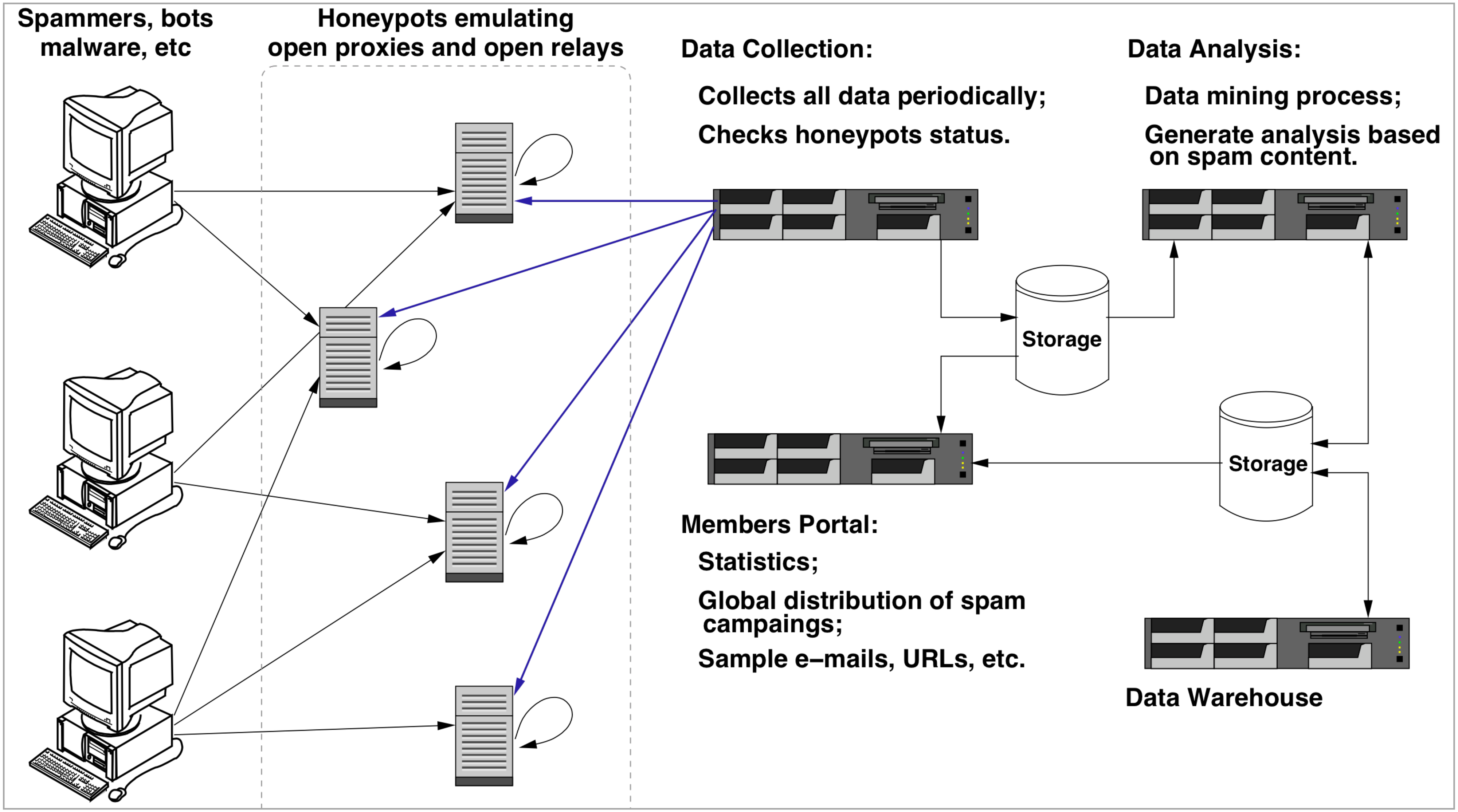
# SpamPots Project

- **Network of Honeypots emulating open proxies and SMTP servers**
- **Capturing 11 million spams/day, on average**
- **Active sensors: AT (**CERT.at**), AU (**AusCERT**), BR (**CERT.br and CSIRT-USP**), CL (**CLCERT**), EC (**CSIRT UTPL**), NL (**SURFcert**), TW (**TWCERT/CC**), UY (**CSIRT Antel**)**
- **Sensor candidates: AE (**aeCERT**), AR (**CSIRT Banelco and Univ. de La Plata**), DE (**Telekom-CERT**), GR (**FORTH, ICS**), MY (**MyCERT**), PL (**CERT Polska**), TH (**ThaiCERT**), TN (**TunCERT**), UK (**OX-CERT**), US (**UAB**)** and **ZA (**via SURFcert**)**

**Objectives:**

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

# SpamPots Project – Overview of the Architecture



Spammers, bots malware, etc

Honeypots emulating open proxies and open relays

Data Collection:

Collects all data periodically;

Checks honeypots status.

Data Analysis:

Data mining process;

Generate analysis based on spam content.

Members Portal:

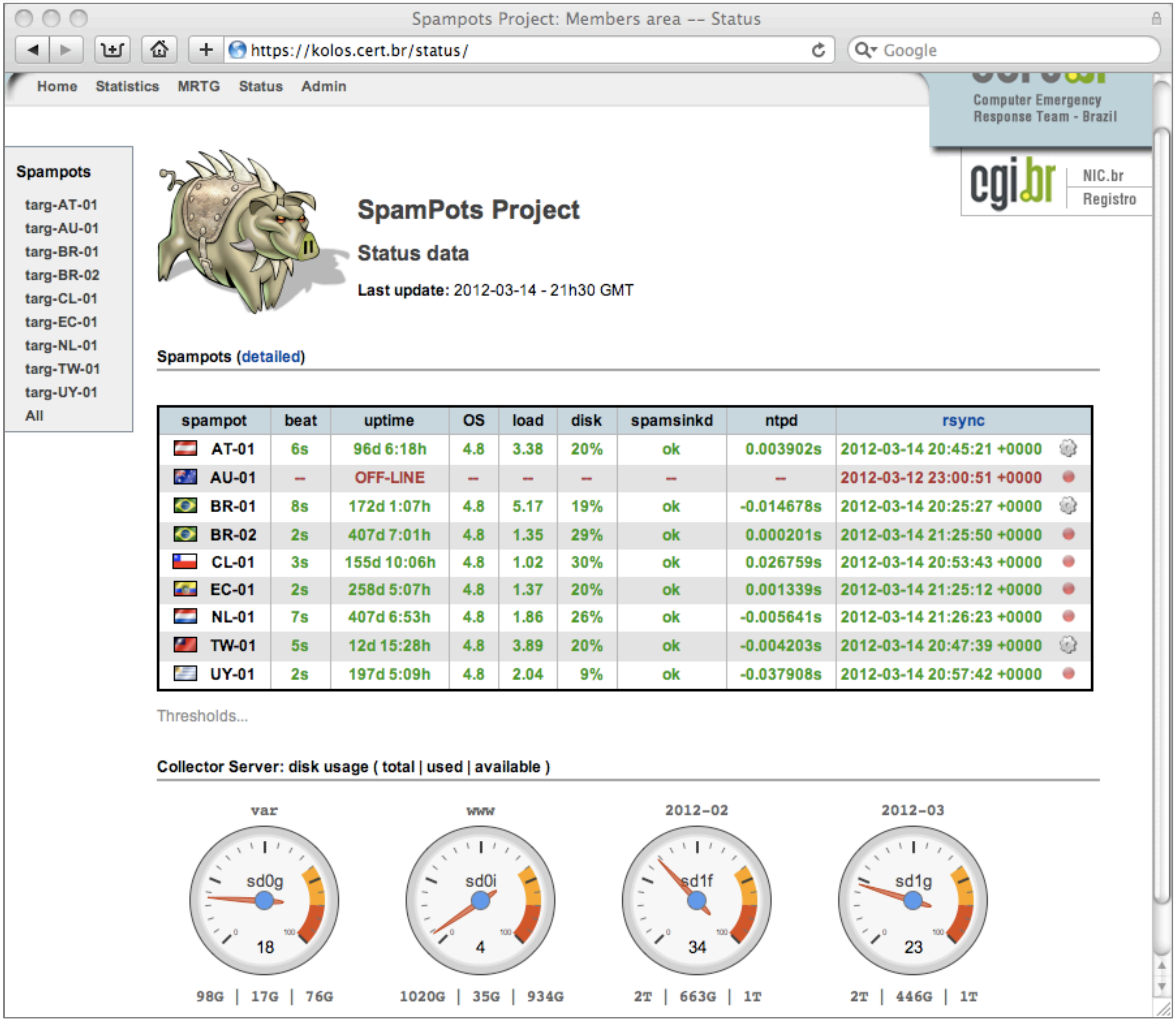
Statistics;

Global distribution of spam campaings;

Sample e–mails, URLs, etc.

Data Warehouse

# Spampots Project: Infrastructure monitoring



## SpamPots Project

### Status data

**Last update:** 2012-03-14 - 21h30 GMT

**Spampots (detailed)**

| spampot | beat | uptime | OS | load | disk | spamsinkd | ntpd | rsync |
|---|---|---|---|---|---|---|---|---|
| AT-01 | 6s | 96d 6:18h | 4.8 | 3.38 | 20% | ok | 0.003902s | 2012-03-14 20:45:21 +0000 ⚙ |
| AU-01 | – | OFF-LINE | – | – | – | – | – | 2012-03-12 23:00:51 +0000 ● |
| BR-01 | 8s | 172d 1:07h | 4.8 | 5.17 | 19% | ok | -0.014678s | 2012-03-14 20:25:27 +0000 ⚙ |
| BR-02 | 2s | 407d 7:01h | 4.8 | 1.35 | 29% | ok | 0.000201s | 2012-03-14 21:25:50 +0000 ● |
| CL-01 | 3s | 155d 10:06h | 4.8 | 1.02 | 30% | ok | 0.026759s | 2012-03-14 20:53:43 +0000 ● |
| EC-01 | 2s | 258d 5:07h | 4.8 | 1.37 | 20% | ok | 0.001339s | 2012-03-14 21:25:12 +0000 ● |
| NL-01 | 7s | 407d 6:53h | 4.8 | 1.86 | 26% | ok | -0.005641s | 2012-03-14 21:26:23 +0000 ● |
| TW-01 | 5s | 12d 15:28h | 4.8 | 3.89 | 20% | ok | -0.004203s | 2012-03-14 20:47:39 +0000 ⚙ |
| UY-01 | 2s | 197d 5:09h | 4.8 | 2.04 | 9% | ok | -0.037908s | 2012-03-14 20:57:42 +0000 ● |

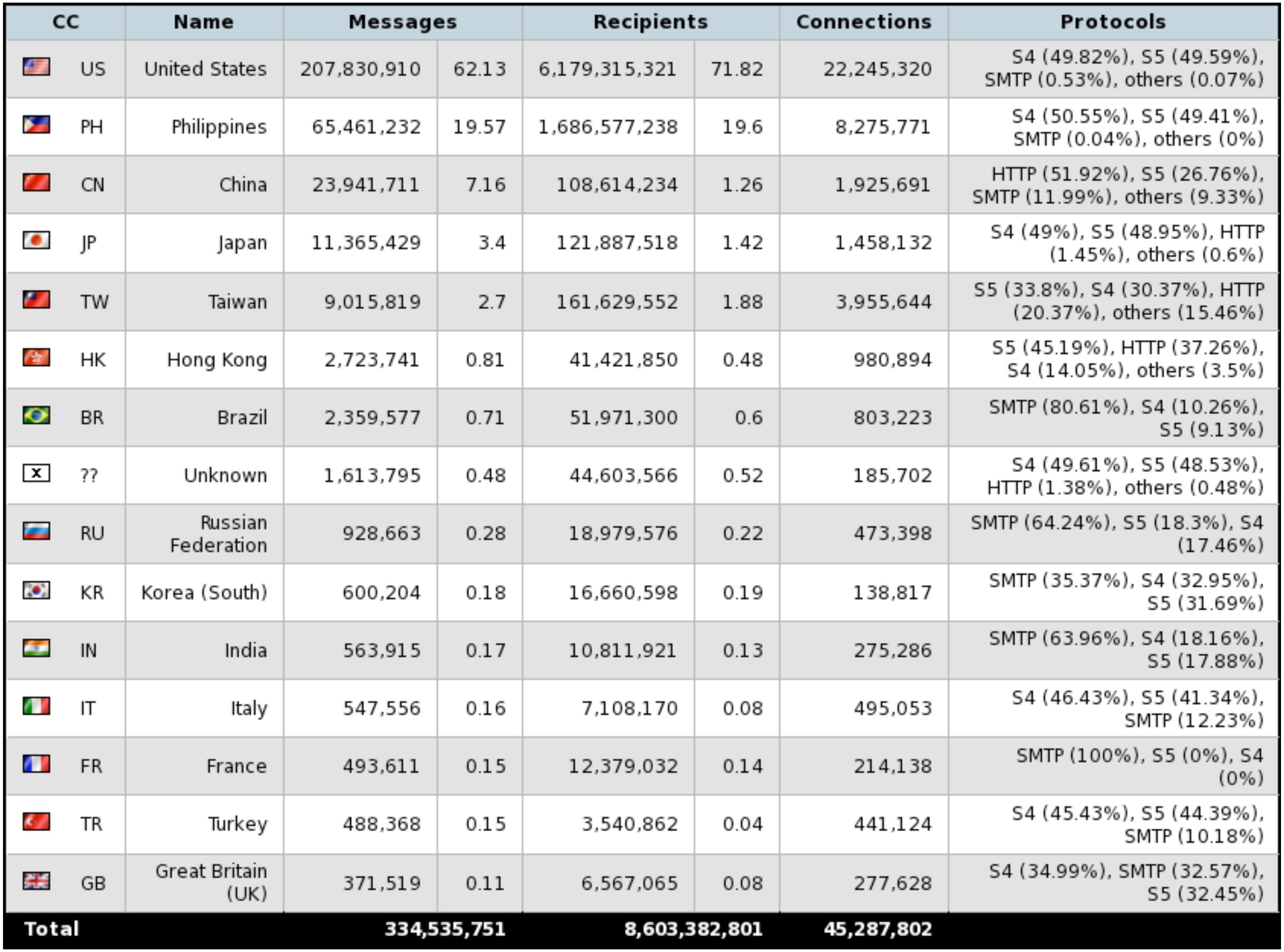
Thresholds...

**Collector Server: disk usage ( total | used | available )**

| var | www | 2012-02 | 2012-03 |
|---|---|---|---|
| sd0g<br>18 | sd0i<br>4 | sd1f<br>34 | sd1g<br>23 |
| 98G \| 17G \| 76G | 1020G \| 35G \| 934G | 2T \| 663G \| 1T | 2T \| 446G \| 1T |

# Spampots Project: Data Mining Portal (1/2)

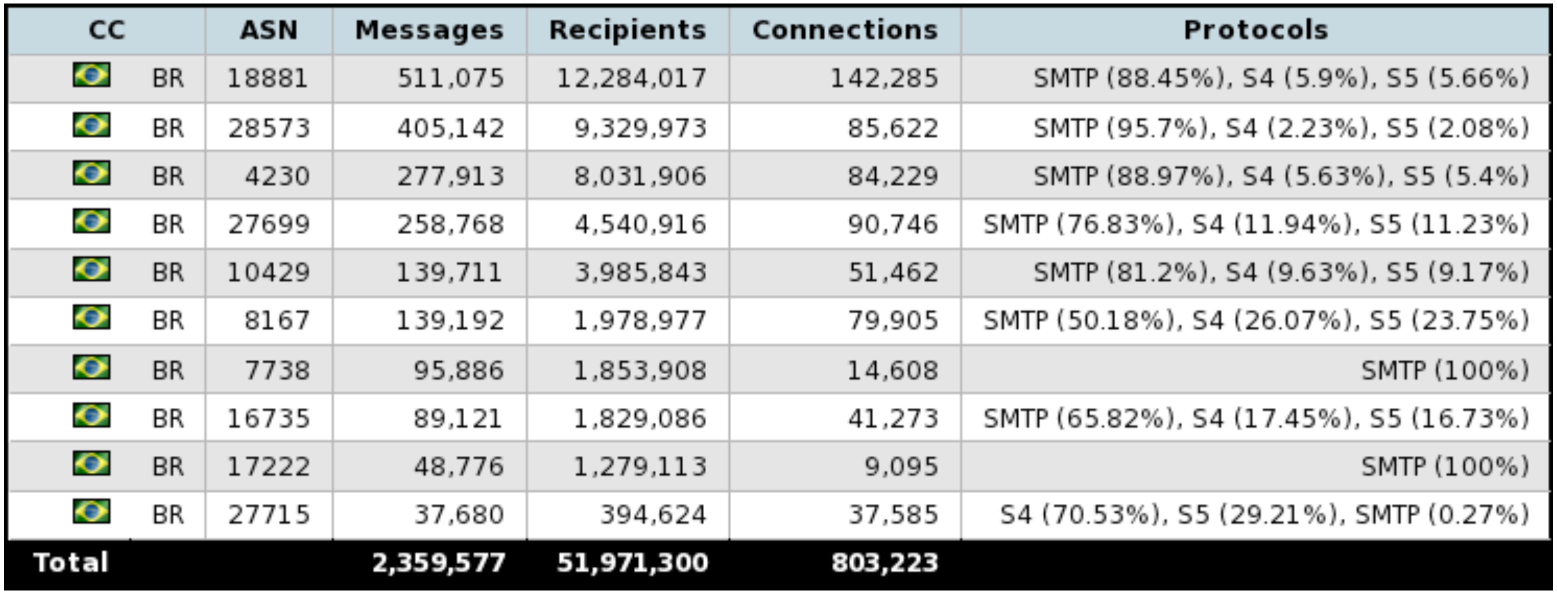
## February 2012: top 15 country codes



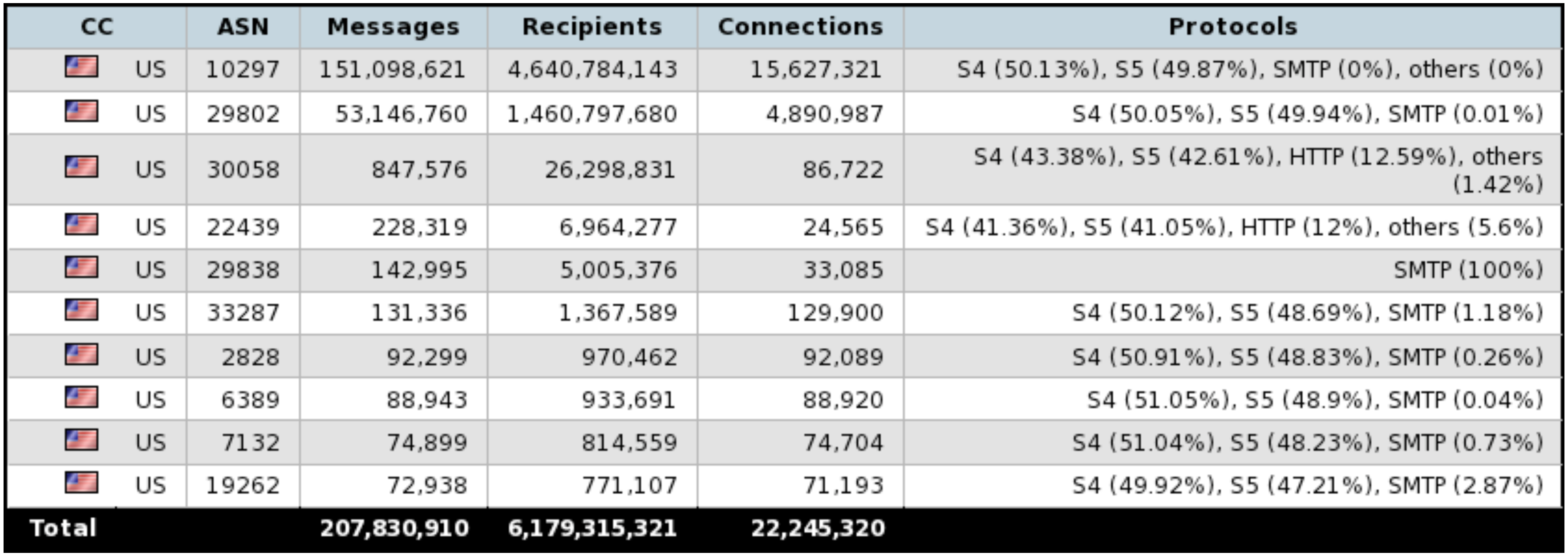
| CC | Name | Messages | | Recipients | | Connections | Protocols |
|---|---|---|---|---|---|---|---|
| US | United States | 207,830,910 | 62.13 | 6,179,315,321 | 71.82 | 22,245,320 | S4 (49.82%), S5 (49.59%), SMTP (0.53%), others (0.07%) |
| PH | Philippines | 65,461,232 | 19.57 | 1,686,577,238 | 19.6 | 8,275,771 | S4 (50.55%), S5 (49.41%), SMTP (0.04%), others (0%) |
| CN | China | 23,941,711 | 7.16 | 108,614,234 | 1.26 | 1,925,691 | HTTP (51.92%), S5 (26.76%), SMTP (11.99%), others (9.33%) |
| JP | Japan | 11,365,429 | 3.4 | 121,887,518 | 1.42 | 1,458,132 | S4 (49%), S5 (48.95%), HTTP (1.45%), others (0.6%) |
| TW | Taiwan | 9,015,819 | 2.7 | 161,629,552 | 1.88 | 3,955,644 | S5 (33.8%), S4 (30.37%), HTTP (20.37%), others (15.46%) |
| HK | Hong Kong | 2,723,741 | 0.81 | 41,421,850 | 0.48 | 980,894 | S5 (45.19%), HTTP (37.26%), S4 (14.05%), others (3.5%) |
| BR | Brazil | 2,359,577 | 0.71 | 51,971,300 | 0.6 | 803,223 | SMTP (80.61%), S4 (10.26%), S5 (9.13%) |
| ☒ ?? | Unknown | 1,613,795 | 0.48 | 44,603,566 | 0.52 | 185,702 | S4 (49.61%), S5 (48.53%), HTTP (1.38%), others (0.48%) |
| RU | Russian Federation | 928,663 | 0.28 | 18,979,576 | 0.22 | 473,398 | SMTP (64.24%), S5 (18.3%), S4 (17.46%) |
| KR | Korea (South) | 600,204 | 0.18 | 16,660,598 | 0.19 | 138,817 | SMTP (35.37%), S4 (32.95%), S5 (31.69%) |
| IN | India | 563,915 | 0.17 | 10,811,921 | 0.13 | 275,286 | SMTP (63.96%), S4 (18.16%), S5 (17.88%) |
| IT | Italy | 547,556 | 0.16 | 7,108,170 | 0.08 | 495,053 | S4 (46.43%), S5 (41.34%), SMTP (12.23%) |
| FR | France | 493,611 | 0.15 | 12,379,032 | 0.14 | 214,138 | SMTP (100%), S5 (0%), S4 (0%) |
| TR | Turkey | 488,368 | 0.15 | 3,540,862 | 0.04 | 441,124 | S4 (45.43%), S5 (44.39%), SMTP (10.18%) |
| GB | Great Britain (UK) | 371,519 | 0.11 | 6,567,065 | 0.08 | 277,628 | S4 (34.99%), SMTP (32.57%), S5 (32.45%) |
| **Total** | | **334,535,751** | | **8,603,382,801** | | **45,287,802** | |

# Spampots Project: Data Mining Portal (2/2)

## February 2012: top 10 ASNs per country code



| CC | | ASN | Messages | Recipients | Connections | Protocols |
|---|---|---|---|---|---|---|
| 🇧🇷 | BR | 18881 | 511,075 | 12,284,017 | 142,285 | SMTP (88.45%), S4 (5.9%), S5 (5.66%) |
| 🇧🇷 | BR | 28573 | 405,142 | 9,329,973 | 85,622 | SMTP (95.7%), S4 (2.23%), S5 (2.08%) |
| 🇧🇷 | BR | 4230 | 277,913 | 8,031,906 | 84,229 | SMTP (88.97%), S4 (5.63%), S5 (5.4%) |
| 🇧🇷 | BR | 27699 | 258,768 | 4,540,916 | 90,746 | SMTP (76.83%), S4 (11.94%), S5 (11.23%) |
| 🇧🇷 | BR | 10429 | 139,711 | 3,985,843 | 51,462 | SMTP (81.2%), S4 (9.63%), S5 (9.17%) |
| 🇧🇷 | BR | 8167 | 139,192 | 1,978,977 | 79,905 | SMTP (50.18%), S4 (26.07%), S5 (23.75%) |
| 🇧🇷 | BR | 7738 | 95,886 | 1,853,908 | 14,608 | SMTP (100%) |
| 🇧🇷 | BR | 16735 | 89,121 | 1,829,086 | 41,273 | SMTP (65.82%), S4 (17.45%), S5 (16.73%) |
| 🇧🇷 | BR | 17222 | 48,776 | 1,279,113 | 9,095 | SMTP (100%) |
| 🇧🇷 | BR | 27715 | 37,680 | 394,624 | 37,585 | S4 (70.53%), S5 (29.21%), SMTP (0.27%) |
| **Total** | | | **2,359,577** | **51,971,300** | **803,223** | |



| CC | | ASN | Messages | Recipients | Connections | Protocols |
|---|---|---|---|---|---|---|
| 🇺🇸 | US | 10297 | 151,098,621 | 4,640,784,143 | 15,627,321 | S4 (50.13%), S5 (49.87%), SMTP (0%), others (0%) |
| 🇺🇸 | US | 29802 | 53,146,760 | 1,460,797,680 | 4,890,987 | S4 (50.05%), S5 (49.94%), SMTP (0.01%) |
| 🇺🇸 | US | 30058 | 847,576 | 26,298,831 | 86,722 | S4 (43.38%), S5 (42.61%), HTTP (12.59%), others (1.42%) |
| 🇺🇸 | US | 22439 | 228,319 | 6,964,277 | 24,565 | S4 (41.36%), S5 (41.05%), HTTP (12%), others (5.6%) |
| 🇺🇸 | US | 29838 | 142,995 | 5,005,376 | 33,085 | SMTP (100%) |
| 🇺🇸 | US | 33287 | 131,336 | 1,367,589 | 129,900 | S4 (50.12%), S5 (48.69%), SMTP (1.18%) |
| 🇺🇸 | US | 2828 | 92,299 | 970,462 | 92,089 | S4 (50.91%), S5 (48.83%), SMTP (0.26%) |
| 🇺🇸 | US | 6389 | 88,943 | 933,691 | 88,920 | S4 (51.05%), S5 (48.9%), SMTP (0.04%) |
| 🇺🇸 | US | 7132 | 74,899 | 814,559 | 74,704 | S4 (51.04%), S5 (48.23%), SMTP (0.73%) |
| 🇺🇸 | US | 19262 | 72,938 | 771,107 | 71,193 | S4 (49.92%), S5 (47.21%), SMTP (2.87%) |
| **Total** | | | **207,830,910** | **6,179,315,321** | **22,245,320** | |

# 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 / IIJ / JPCERT/CC / Min. of Communications
  - TW: to NCC-TW

# 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/