



nic.br egi.br

cert.br

**CARIS Workshop**  
June 19, 2015  
Berlin, DE

# CERT.br Use of Honeypots for Network Monitoring and Incident Response

**Cristine Hoepers**  
General Manager  
[cristine@cert.br](mailto:cristine@cert.br)

**Klaus Steding-Jessen**  
Technical Manager  
[jessen@cert.br](mailto:jessen@cert.br)

**cert.br nic.br cgi.br**



**Brazilian Internet Steering Committee**

- multi-stakeholder council that coordinates all Internet related activities in Brazil.



**Incident Handling**

- Coordination
- Facilitation
- Support
- Statistics

**Training and Awareness**

- Courses
- Presentations
- Documents
- Meetings

**Trend Analysis & Net. Monitoring**

- Distributed Honeypots
- SpamPots

**CERT.br mission**

- National focal point for reporting security incidents
- **Collect and disseminate information about threats and attack trends**
- **Increase the country's security awareness and incident handling capacity**
- Help new CSIRTs to establish their activities



# Network Monitoring: Motivation and Challenges

## Motivation

- incident reports only reflect what organizations are already looking at
- trend reports are usually
  - produced by vendors
  - based on data we don't know where and how was collected
- the goal:
  - have a picture of malicious activity in the Brazilian IPv4 Internet space
  - start having “weather stations” in Brazilian networks

## Challenges

- protect privacy and possible sensitiveness of data
- transparency
- gather partner organizations to share information

# Network Monitoring: Use of Honeypots

**2001 – Researched the technology**

**2003 – Started to use low-interaction honeypots for network monitoring**

## Pros

- no production data collected
- very low risk to the hosting organizations (than high-interaction)
- gather more details about attacks than darknets/telescopes/etc
  - payloads available if listeners are used
  - collect malware in some cases

## Cons

- do not detect targeted attacks
- are focused on attacks that abuse/spread through the network

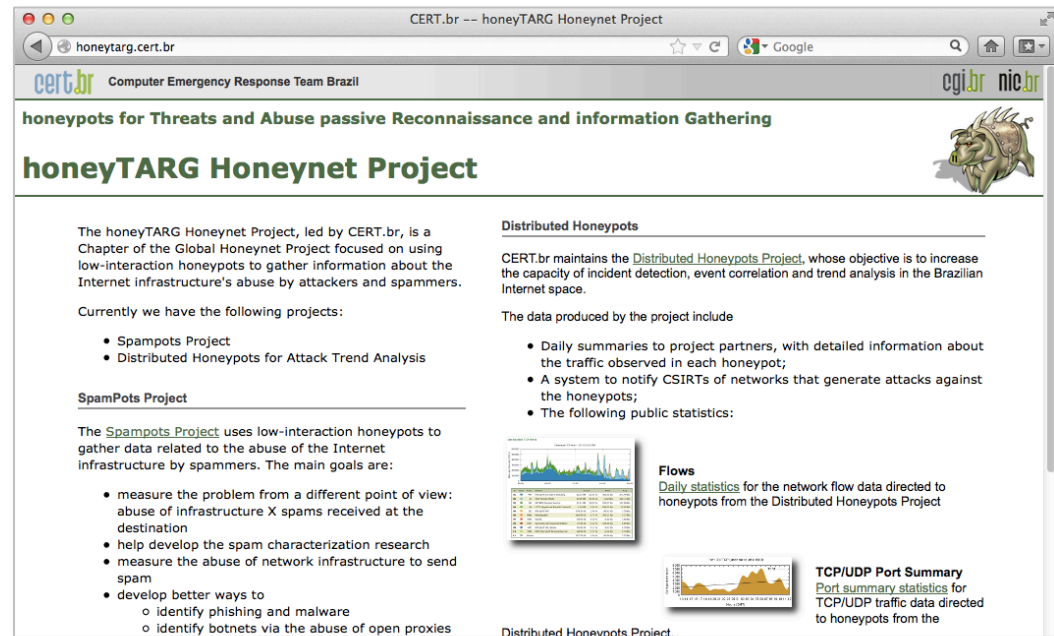
# Network Monitoring: honeyTARG Honeynet Project

- **Brazilian Distributed Honeydumps**

- National
- Focused on network attacks

- **SpamPots**

- International
- Focused on the abuse of networks by spammers and fraudsters



The screenshot shows a web browser window displaying the honeyTARG Honeynet Project website. The browser's address bar shows 'honeytarg.cert.br'. The website header includes the CERT.br logo and the text 'Computer Emergency Response Team Brazil'. The main heading is 'honeyTARG Honeynet Project' with a sub-heading 'honeypots for Threats and Abuse passive Reconnaissance and information Gathering'. The page content is organized into two columns. The left column describes the project's goals and lists current projects: 'Spampots Project' and 'Distributed Honeydumps for Attack Trend Analysis'. The right column describes the 'Distributed Honeydumps' project, its objectives, and the data it produces. It includes a section for 'Flows' with a line graph and a section for 'TCP/UDP Port Summary' with a bar chart. The website also features logos for 'cgi.br' and 'nic.br' in the top right corner.

CERT.br -- honeyTARG Honeynet Project

honeytarg.cert.br

cert.br Computer Emergency Response Team Brazil cgi.br nic.br

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 Honeydumps 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
  - identify phishing and malware
  - identify botnets via the abuse of open proxies

### Distributed Honeydumps

CERT.br maintains the Distributed Honeydumps 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 Honeydumps Project

#### TCP/UDP Port Summary

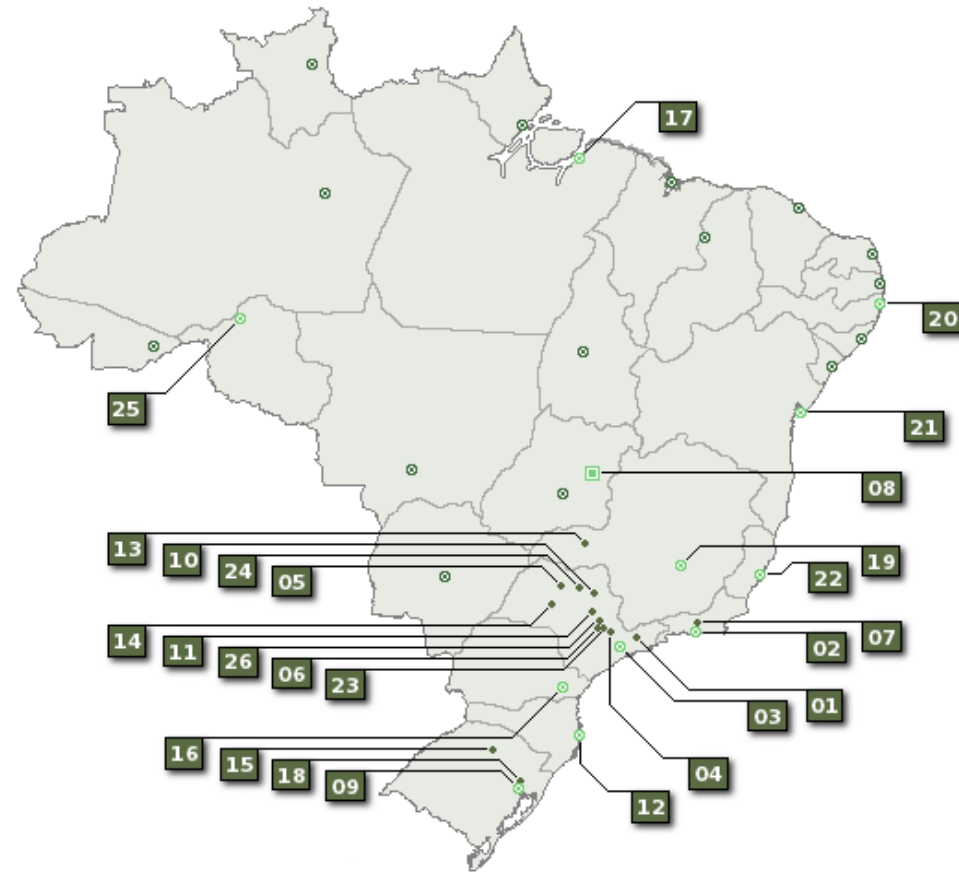
Port summary statistics for TCP/UDP traffic data directed to honeypots from the Distributed Honeydumps Project

# Brazilian Distributed Honey Pots Project

- 55 Sensors in 22 cities hosted by 49 Partners in
  - government, energy, financial, ISPs, academia
- Data is collected to a central server at CERT.br
- Based on voluntary work and resources
- Transparent configuration
  - no “black-box”
  - no production data is captured

## Data collected is used to

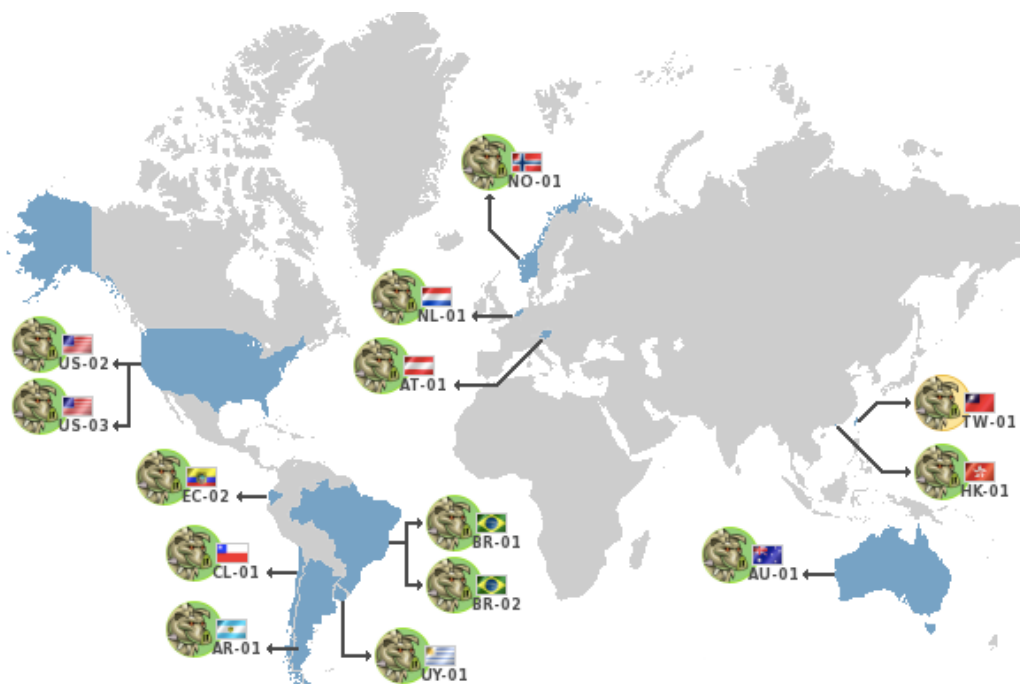
- Notify networks that originate attacks
  - focus on Brazilian networks
- Donate data to other National CSIRTs and to trusted partners
- Generate public statistics/trends
  - partners have access to more info



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

# SpamPots Project

- **Collect data in the “middle” of the spam path**
  - emulate open proxies/relays
- **Fund research on spam characterization**
- **Share spam campaign information with regulators/investigators**
- **Provide metrics to policy makers**



Sensors deployed in 12 countries, with the invaluable help of these organizations:

- CSIRT UNLP (AR)
- AusCERT (AU)
- CERT.at (AT)
- CSIRT USP (BR)
- CLCERT (CL)
- CSIRT CEDIA (EC)
- HKCERT (HK)
- SurfCERT (NL)
- Shadowserver (NO and US)
- TWCERT (TW)
- University of Alabama at Birmingham (US)
- CSIRT ANTEL (UY)



# Spampots Project Members Portal: Month / Quarter / Semester / Year Stats

- IP addresses
- Messages per IP
- Change Over Time
- Total
- Country Codes
- AS Numbers

---

- Spampots Comparison**
- By Period
- Spam Volume grid chart
- Messages per IP grid chart
- Change Over Time
- Spams & IPs grid chart

---

- Tables
- raw data

---

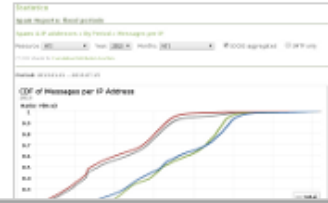
- back



**HISTOGRAM OF SPAM VOLUME, BY PERIOD**  
 Histogram of spam volume by period, which can be months, quarters, semesters or years. Also shows the spam volume by protocol for the whole period, and corresponding percentages. It can be filtered by resource, selecting all spampots, an specific one, or a country that hosts an spampot. The histogram can also be filtered by protocol.



**HISTOGRAM OF IP ADDRESSES, BY PERIOD**  
 Histogram of IP addresses by period, which can be months, quarters, semesters or years. It can be filtered by resource, selecting all spampots, an specific one, or a country that hosts an spampot. The histogram can also be filtered by protocol.



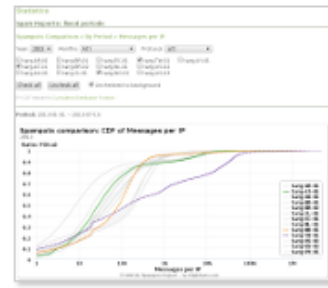
**CDF OF MESSAGES PER IP, BY PERIOD**  
 Cumulative Distribution Function (CDF) of messages per IP address in a given period.



**SPAM VOLUME PER SPAMPOT, BY PERIOD**  
 Comparison of spam volume per spampot, for a given period. It can be filtered by protocol, and sorted by volume.



**SPAM VOLUME PER SPAMPOT, BY PERIOD (grid chart)**  
 Grid chart comparing the spam volume by protocol of each spampot, for a given period. The graphics displayed can be bars, columns or pie charts.



**CDF OF MESSAGES PER IP PER SPAMPOT, BY PERIOD**  
 Comparison of the cumulative distribution function (CDF) of messages per IP address by spampots, for a given period. It can be filtered by protocol. Obs. The unchecked spampots' curves can be kept on the background, by marking the corresponding checkbox.



**CDF OF MESSAGES PER IP PER SPAMPOT, BY PERIOD (grid chart)**

# Spampots Project Members Portal: Database Query Interface

From: 2015-06-01

To: 2015-06-17

Spampot: All

- Graphs to show:
- Total
  - Spampots comparison
  - Country Codes
  - Autonomous Systems

Region: ripencc

CC\*: AD,AE,AL

ASN\*: All

Top N: 5

Protocol: All

Grouped by: day

- Chart options:
- SOCKS aggregated
  - SMTP only
  - Smooth lines
  - Show markers

Submit Defaults

## Statistics

### Spam Reports: database query interface

#### GRAPHICS

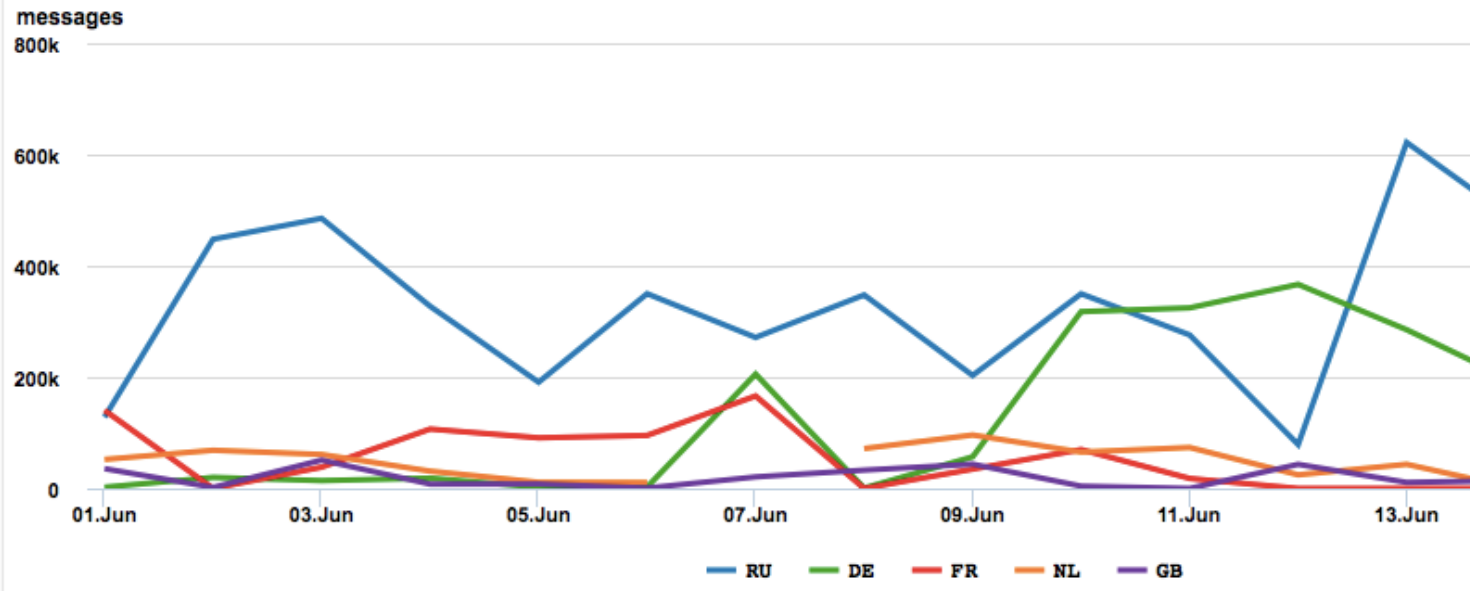
Available data: from 2012-01-01 to 2015-06-17

Selected data: from 2015-06-01 to 2015-06-17

Observed date range: from 2015-06-01 to 2015-06-17

#### Top 5 Country Codes: spam volume / day

2015-06-01 -- 2015-06-17 (Region: ripencc)



© CERT.br (Spampots Project) -- by Highcharts.com

# Thank You

[www.cert.br](http://www.cert.br)

 [cristine@cert.br](mailto:cristine@cert.br)

 [jessen@cert.br](mailto:jessen@cert.br)

 [@certbr](https://twitter.com/certbr)

June 19, 2015

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)