Use of Honeypots for Network Monitoring and Situational Awareness

Cristine Hoepers
cristine@cert.br

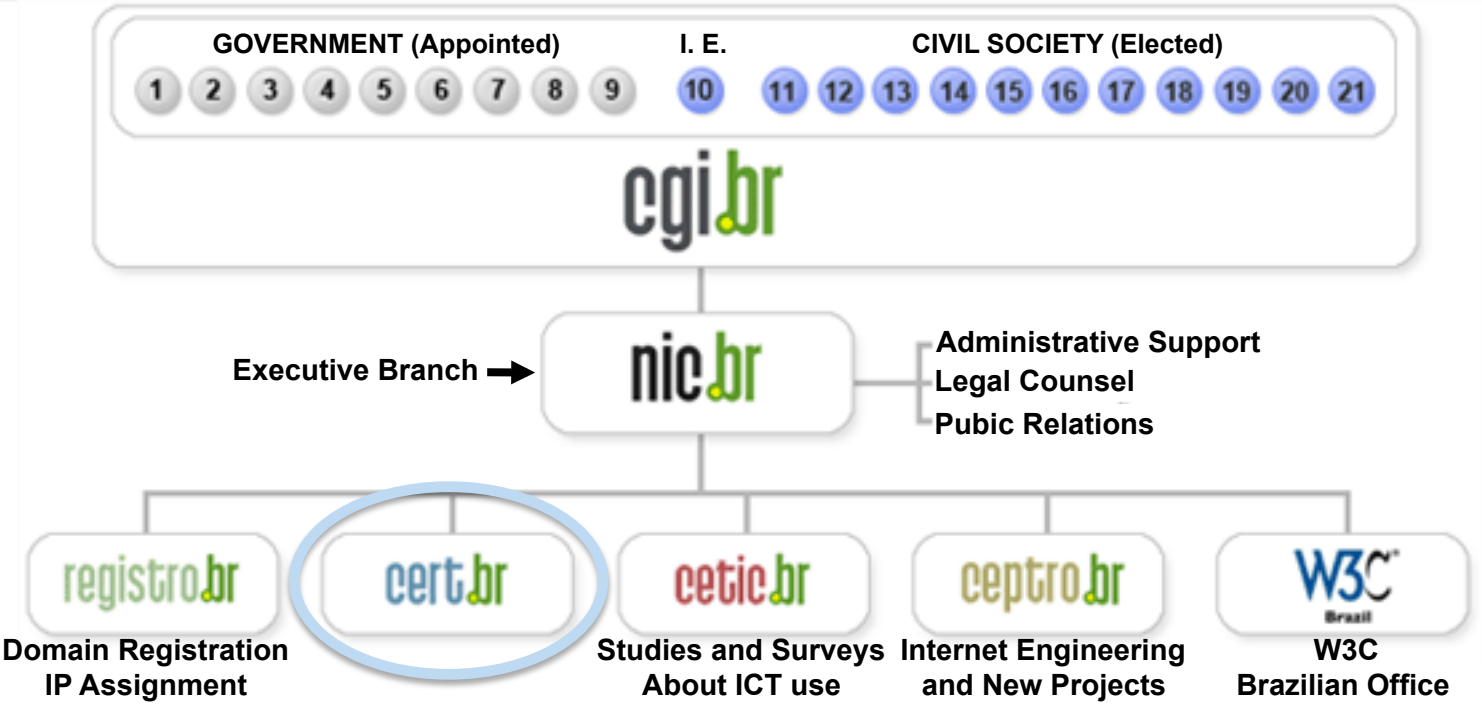
Computer Emergency Response Team Brazil - **CERT.br**

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

Agenda

- Our Mission
  - and its relation with network monitoring and situational awareness
- Why use honeypots
- How we are using honeypots
  - Distributed Honeypots Project
  - SpamPots Project

CGI.br, NIC.br and CERT.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

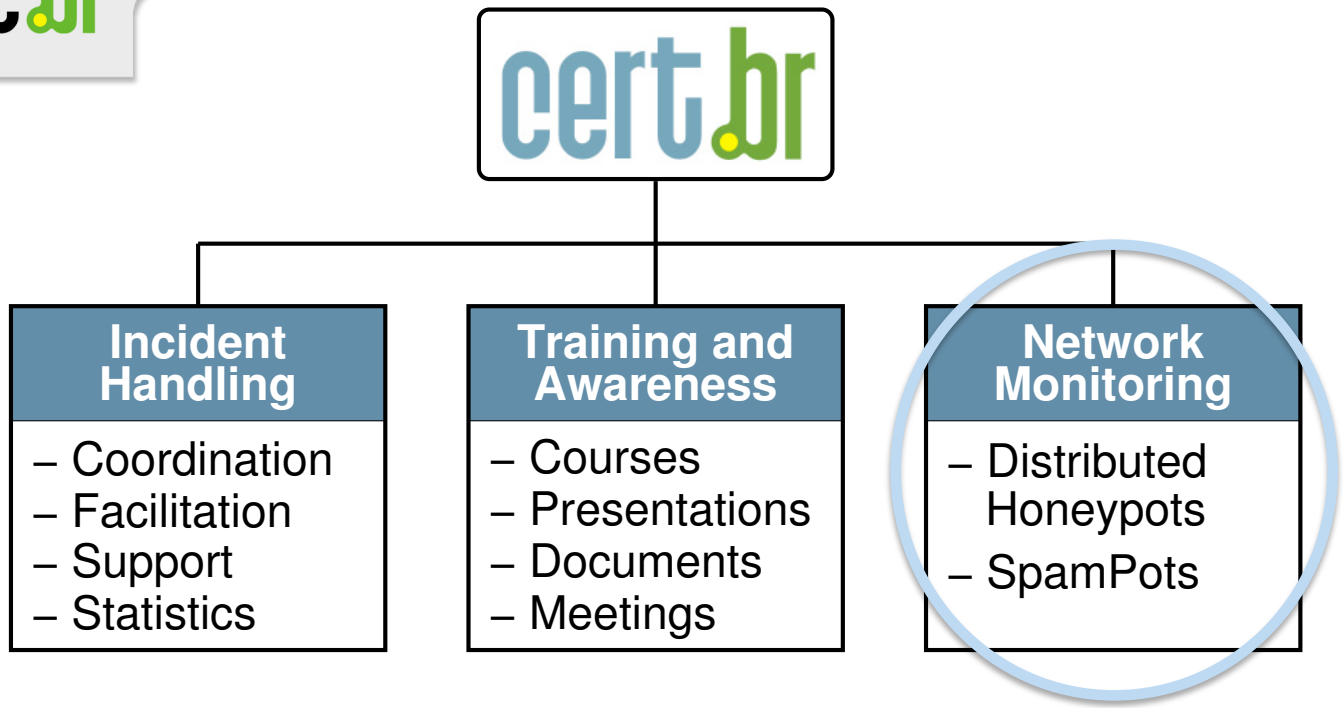
The Brazilian Internet Steering Committee - CGI.br

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/



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT

SEI Partner Carnegie Mellon

Created in 1997 to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.

- **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**
- **Develop collaborative relationships with other entities**
- **Help new CSIRTs to establish their activities**

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

Why use honeypots

There are Several Ways to Collect Data for Network Monitoring and Situational Awareness

- Flows
- Darknets
- Several security tools
  - firewalls, IDS, etc
- Honeypots
  - low- and high-interaction
- Data feeds
  - comercial and free

But not all of them can be used to collect data that needs to be shared outside an organization

As a National CERT we have Specific Needs

- **Privacy**
  - the network is not ours
  - we don't want or need to have access to production traffic
- **Scalability**
  - no extra processing or costs should be imposed on the participant's network
  - easy maintenance
- **Low risk**
  - we can't introduce risks on the participant's network
- **Data about attacks against Brazilian networks**
  - need of "neutral" data
  - collected locally

We Decided to Use Low-Interaction Honeypots

- **The data captured is**
  - **limited, as there is no real compromise of a system/application**
  - **more detailed than that collected on darknets**
  - **enough to determine trends and provide comparability with global statistics**

	Low-Interaction	High-Interaction
Installation	Easy	More difficult
Maintenance	Easy	Time consuming
Risk	Low	High
Need Control	No	Yes
Data gathering	Limited	Extensive
Interaction	Emulated services	Full control

How we are using honeypots

The Honeynet Project honeyTARG Chapter

CERT.br -- honeyTARG Honeynet Project

honeytarg.cert.br Reader

cert.br 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

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

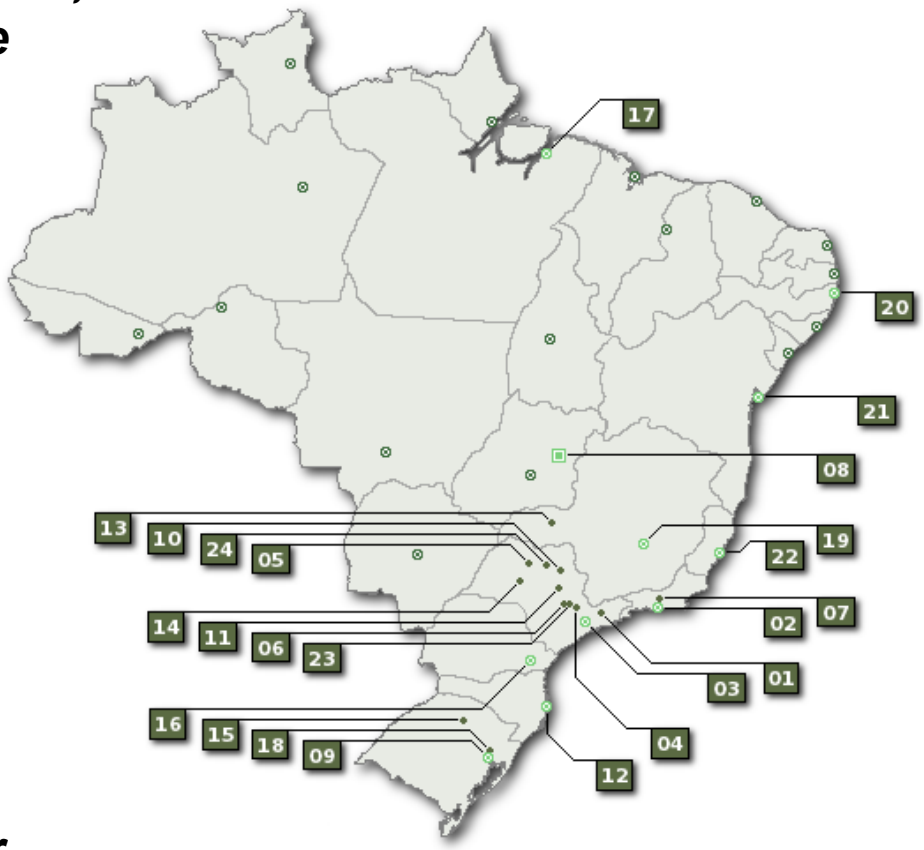
Daily statistics for the network flow

Brazilian Distributed Honeypots Project

Goal

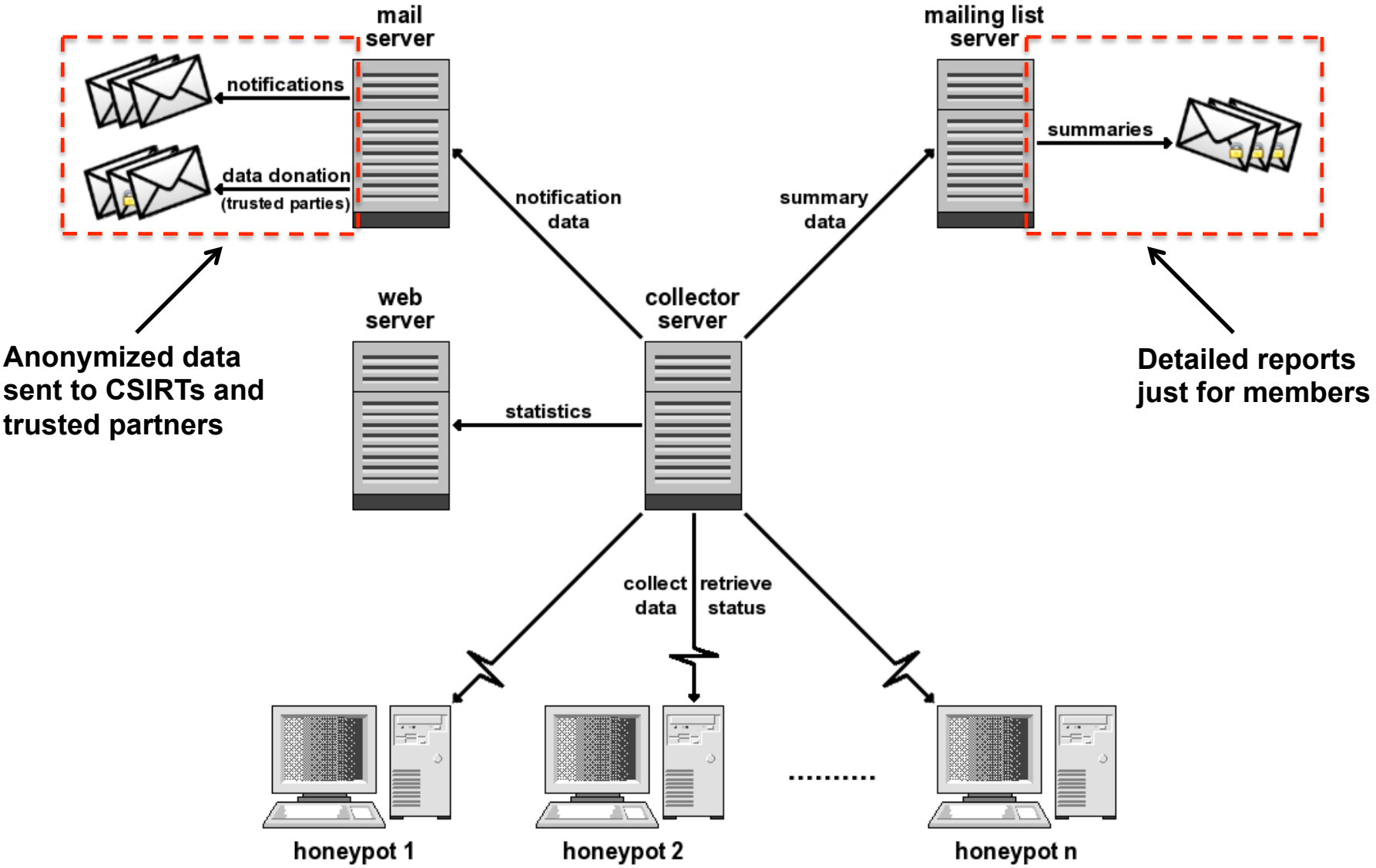
to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet space

- Established in 2003
- 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 customize its sensor and use it as a complement to its own IDS



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

Architecture of the Network of Honeypots



Uses of the Data to Help the Community

Public statistics/trends

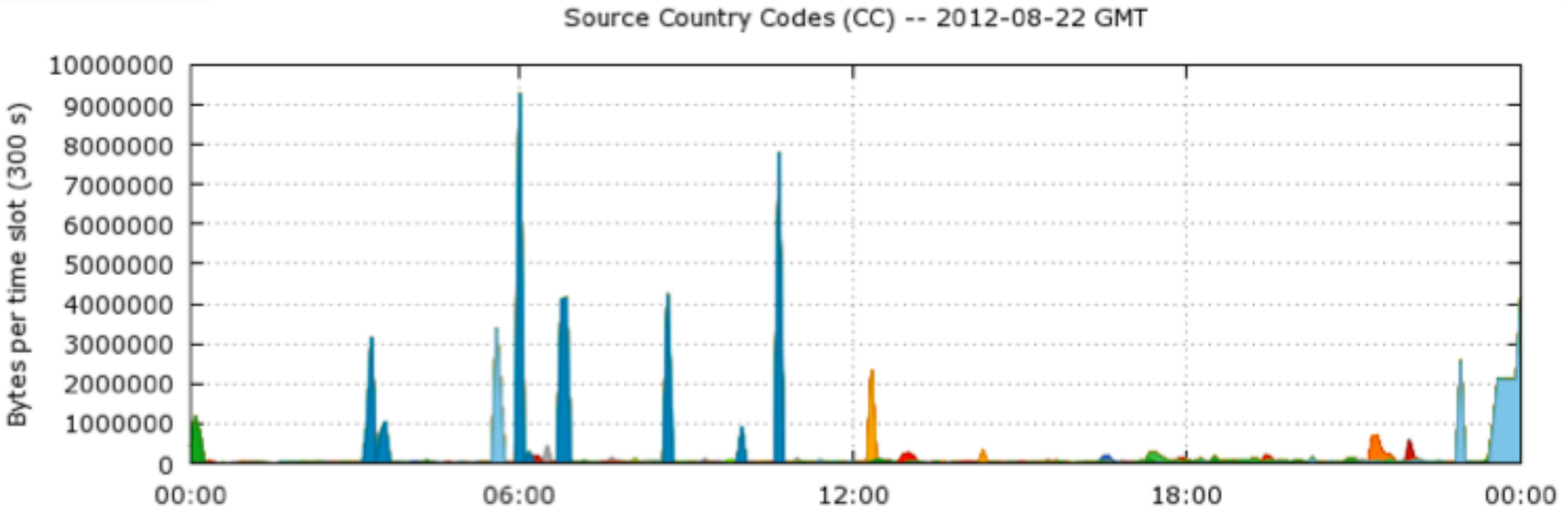
Individual Incident Notifications

- 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

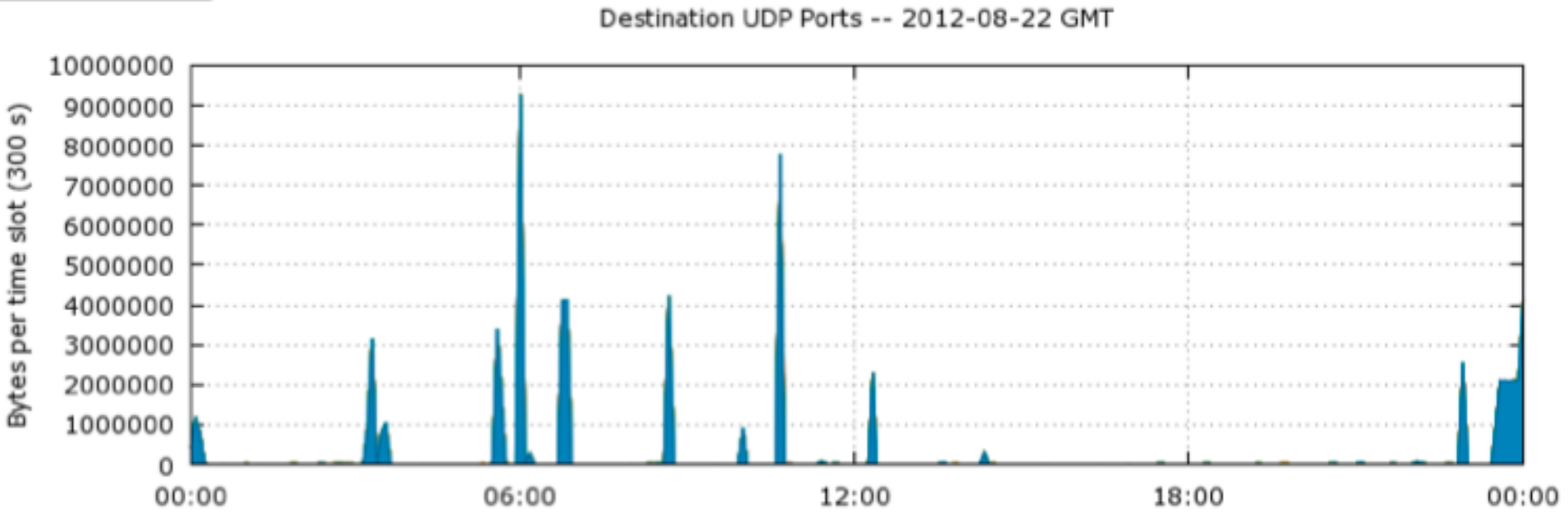
- To CSIRTs with national responsibility
  - All traffic coming from IPs allocated to the given country
- To organizations that share data with ISPs
  - Team Cymru (SSH brute force, SIP attacks and some botnet traffic)
  - Shadowserver Foundation (SSH brute force attacks)
  - Arbor ATLAS (SSH brute force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

Public Statistics: Flows – Source Country codes



#	Key	CC	Name	Total		Max	Avg
01		DE	Germany	36.63 MB	44.67 %	30.91 KB/s	423.96 B/s
02		US	United States	24.74 MB	30.16 %	13.68 KB/s	286.31 B/s
03		CN	China	4.75 MB	5.79 %	3.93 KB/s	54.95 B/s
04		PA	Panama	3.03 MB	3.69 %	843.79 B/s	35.02 B/s
05		MY	Malaysia	2.67 MB	3.25 %	7.66 KB/s	30.87 B/s
06		NL	Netherlands	2.02 MB	2.47 %	2.10 KB/s	23.41 B/s
07		BR	Brazil	1.82 MB	2.21 %	761.66 B/s	21.02 B/s
08		RU	Russian Federation	952.75 KB	1.16 %	1.76 KB/s	11.03 B/s
09		GB	United Kingdom	602.74 KB	0.73 %	604.51 B/s	6.98 B/s
10		FR	France	493.87 KB	0.60 %	389.45 B/s	5.72 B/s

Public Statistics: Flows – UDP Attacks



#	Key	Port	Name	Total		Max	Avg
01		5060	SIP (Session Initiation Protocol)	65.01 MB	99.27 %	30.92 KB/s	752.47 B/s
02		1434	Microsoft SQL Monitor	74.74 KB	0.11 %	3.11 B/s	0.87 B/s
03		53	DNS (Domain Name System)	35.51 KB	0.05 %	12.45 B/s	0.41 B/s
04		1900	ssdp (SSDP)	17.93 KB	0.03 %	22.13 B/s	0.21 B/s
05		137	NETBIOS Name Service	16.68 KB	0.03 %	15.03 B/s	0.19 B/s
06		32760	n/a	13.64 KB	0.02 %	0.91 B/s	0.16 B/s
07		32761	n/a	13.56 KB	0.02 %	0.83 B/s	0.16 B/s
08		17185	n/a	13.07 KB	0.02 %	22.33 B/s	0.15 B/s
09		39455	n/a	10.99 KB	0.02 %	9.49 B/s	0.13 B/s

We also have Details not Available in Flows or Darknets

```
U 2010/09/28 22:54:07.491696 89.47.63.183:59317 -> network_server:5060
  OPTIONS sip:100@network_server SIP/2.0..Via: SIP/2.0/UDP 127.0.1.1:5060;bra
  nch=z9hG4bK-3932320937;rport..Content-Length: 0..From: "sipvicious"<sip:100
  @1.1.1.1>; tag=6338616232316238313363340132333530383633323634..Accept: appl
  ication/sdp..User-Agent: friendly-scanner..To: "sipvicious"<sip:100@1.1.1.1
  >..Contact: sip:100@127.0.1.1:5060..CSeq: 1 OPTIONS..Call-ID: 3655079754140
  81403837664..Max-Forwards: 70....

U 2010/09/30 23:50:21.236653 67.21.82.4:45018 -> network_server:5060
  INVITE sip:96626653000@network_server SIP/2.0..Via: SIP/2.0/UDP 67.21.82.4:
  45018;rport;branch=z9hG4bK051C0283E05B4BF182275668E1F3BD15..From: 102 <sip:
  102@network_server>;tag=129156506..To: <sip:96626653000@network_server>..Co
  ntact: <sip:102@67.21.82.4:45018>..Call-ID: 3A1309F9-9FAC-4BE3-8B7E-9294496
  D1E08@192.168.1.3..CSeq: 9999 INVITE..Max-Forwards: 70..Content-Type: appli
  cation/sdp..User-Agent: X-PRO build 1101..Content-Length: 312....v=0..o=102
   4272671 4272671 IN IP4 67.21.82.4..s=X-PRO..c=IN IP4 67.21.82.4..t=0 0..m=
  audio 45020 RTP/AVP 0 8 3 18 98 97 101..a=rtpmap:0 pcmu/8000..a=rtpmap:8 pc
  ma/8000..a=rtpmap:3 gsm/8000..a=rtpmap:18 G729/8000..a=rtpmap:98 iLBC/8000.
  .a=rtpmap:97 speex/8000..a=rtpmap:101 telephone-event/8000..a=fmtp:101 0-15
  ..
```

Public Statistics: Port Summary – Trends

TCP/UDP PORT SUMMARY

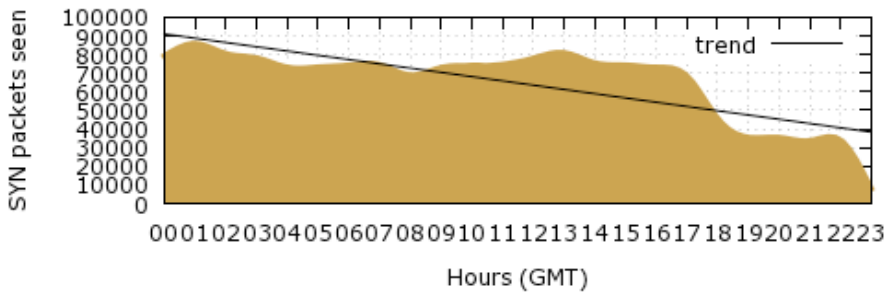
Daily statistics: 2012-02-07 00:00 -- 2012-02-07 23:59 (GMT)

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.

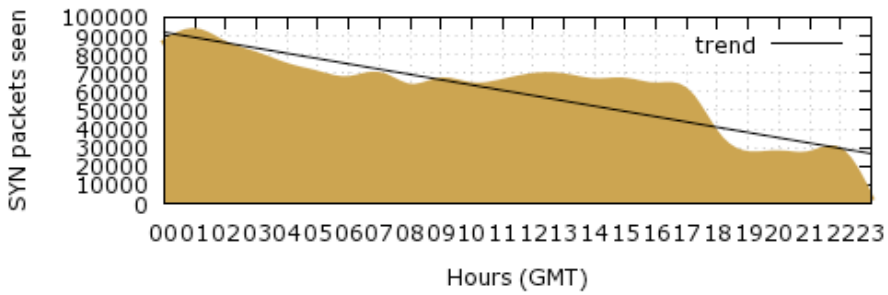
| Top TCP Ports | Top UDP Ports |

Top TCP Ports

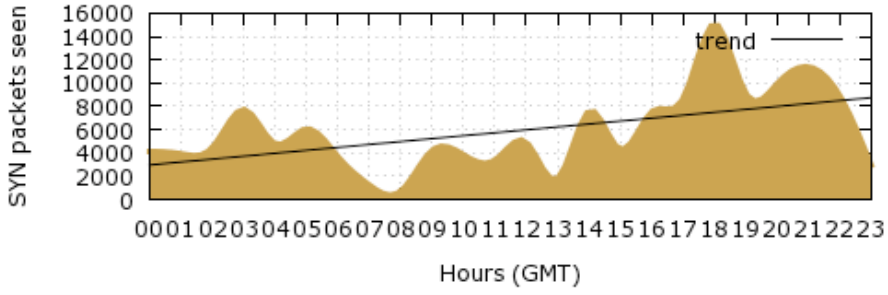
Port 445 / TCP (last hour count = 7927)



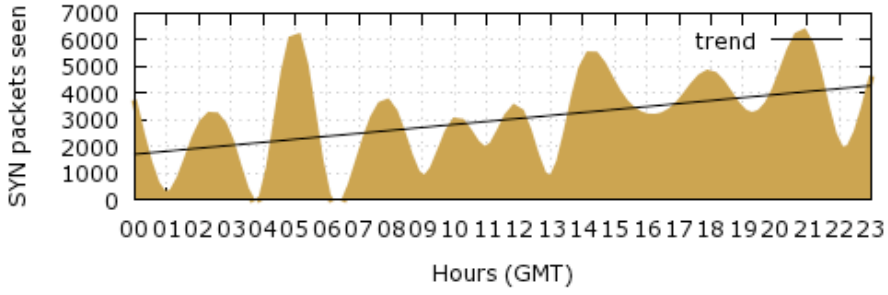
Port 139 / TCP (last hour count = 2954)



Port 22 / TCP (last hour count = 2925)



Port 3306 / TCP (last hour count = 4540)



SpamPots Project

CERT.br honeyTARG – SpamPots Project

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

cert.br Computer Emergency Response Team Brazil — egi.br nic.br

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)

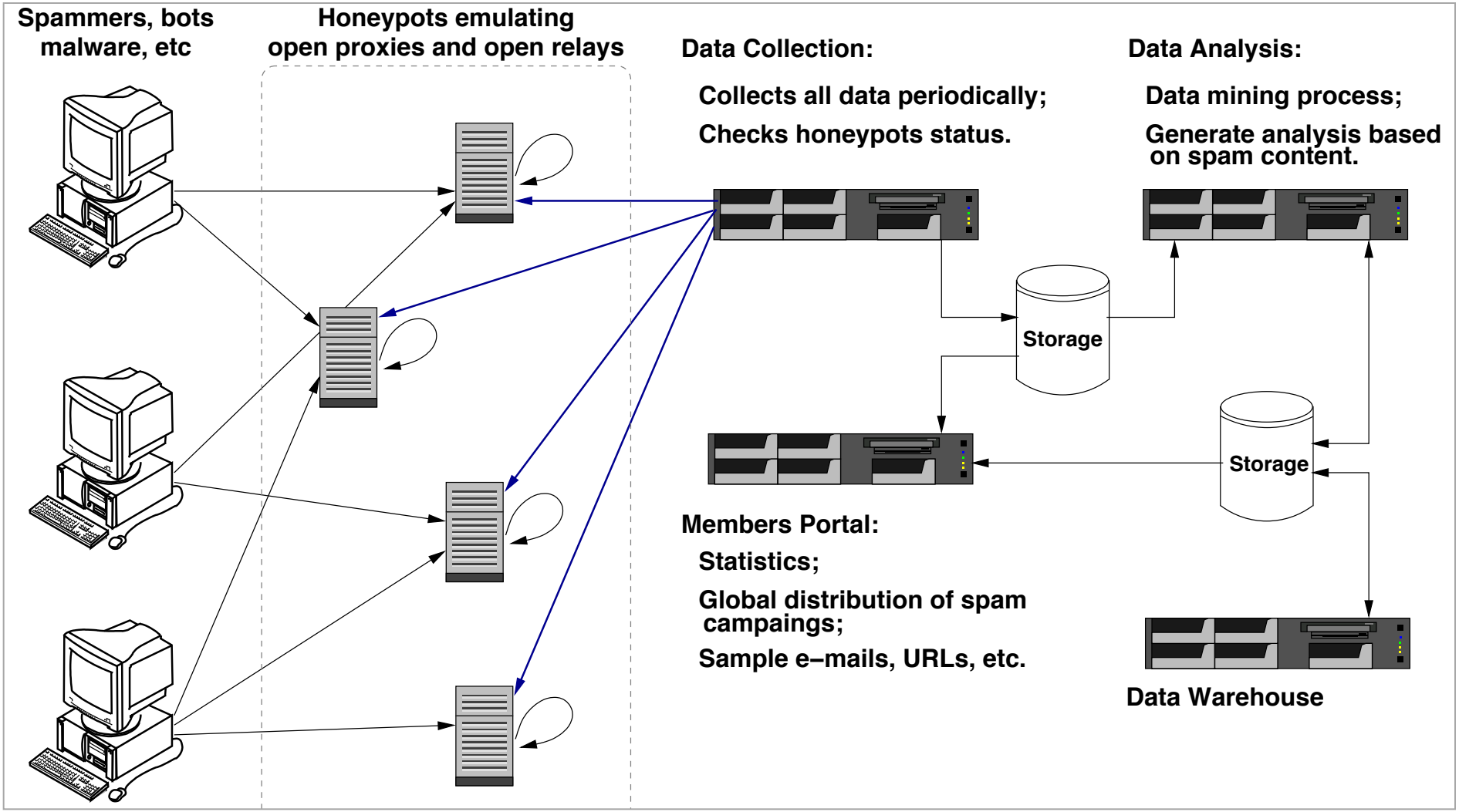
Papers in English

- **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



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)

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**
- **Propose policies and techniques to mitigate the abuse of the infrastructure**

Data mining research in partnership with the e-speed Laboratory, from UFMG (Federal University of Minas Gerais)

Spams Captured in August 29, 2012

Honeypots' location

spampot	CCs	ASNs	CIDRs	IPs	emails (%)		recipients (%)		connections	proto	ports
AT-01	81	425	775	1,344	1,181,825	10.56	35,819,646	10.96	160,883	HTTP, SMTP, S4, S5	multi (6)
AU-01	86	528	1,024	1,760	855,636	7.64	27,499,520	8.41	181,910	HTTP, SMTP, S4, S4a, S5	multi (4)
BR-01	85	511	987	2,069	614,829	5.49	20,708,352	6.34	135,256	SMTP, S4, S5	1080, 25
BR-02	33	123	253	929	1,864,521	16.66	54,947,676	16.81	280,605	HTTP, SMTP, S4, S5	multi (5)
CL-01	41	156	339	969	151,376	1.35	3,734,873	1.14	77,913	HTTP, SMTP, S4, S4a, S5	multi (5)
EC-01	72	411	932	4,217	734,013	6.56	11,864,692	3.63	321,407	HTTP, SMTP, S4, S5	multi (6)
NL-01	42	160	319	649	2,182,979	19.50	67,153,381	20.55	244,009	HTTP, SMTP, S4, S5	multi (4)
TW-01	44	176	432	1,029	2,985,828	26.67	85,971,804	26.31	409,510	HTTP, SMTP, S4, S5	multi (7)
UY-01	86	528	1,041	1,482	623,223	5.57	19,124,015	5.85	85,239	HTTP, SMTP, S4, S5	multi (5)
All	**92**	**666**	**1,547**	**5,547**	**11,194,230**	**100.00**	**326,823,959**	**100.00**	**1,896,732**	**HTTP, SMTP, S4, S4a, S5**	**multi (8)**

All the data was collected in a 24-hour period, in the 9 honeypots emulating Open Proxies and Open Relays

- **Total e-mails captured:** **11.194.230**
- **Potential victims of the spams:** **326.823.959**
  (Average of 30 recipients/e-mail)
- **Protocols abused by spammers:** **HTTP, SMTP, SOCKS 4/4a, SOCKS 5**
- **Unique IPs:** **5.547**

Top Countries Abusing Open Proxies and Open Relays

	CC	description	emails (%)		recipients (%)		connections	proto (%)	spampots
1	US	United States	5,992,587	53.53	188,955,930	57.82	909,203	HTTP (19.86), SMTP (2.35), S4 (38.91), S5 (38.87)	9
2	PH	Philippines	1,983,340	17.72	49,352,063	15.10	224,884	HTTP (21.50), SMTP (0.48), S4 (39.20), S5 (38.82)	9
3	TW	Taiwan, Province of China	1,121,568	10.02	32,755,550	10.02	171,710	HTTP (3.09), SMTP (12.17), S4 (42.41), S5 (42.34)	9
4	CN	China	636,237	5.68	12,149,932	3.72	91,195	HTTP (25.78), SMTP (59.64), S4 (3.49), S4a (1.39), S5 (9.70)	9
5	BR	Brazil	343,552	3.07	8,925,378	2.73	165,480	HTTP (0.61), SMTP (66.05), S4 (15.57), S5 (17.77)	9
6	RU	Russian Federation	164,648	1.47	5,451,144	1.67	41,625	SMTP (95.33), S4 (2.28), S5 (2.39)	9
7	KR	Korea, Republic of	76,229	0.68	2,421,441	0.74	24,528	SMTP (87.47), S4 (6.08), S5 (6.46)	9
8	UA	Ukraine	61,446	0.55	2,024,894	0.62	12,453	SMTP (99.13), S4 (0.43), S5 (0.44)	9
9	IN	India	59,874	0.53	1,859,111	0.57	17,042	SMTP (90.61), S4 (4.66), S5 (4.73)	9
10	GB	United Kingdom	52,129	0.47	1,673,259	0.51	16,394	SMTP (88.79), S4 (5.45), S5 (5.76)	8
11	IT	Italy	43,787	0.39	779,763	0.24	29,670	SMTP (67.85), S4 (16.24), S5 (15.90)	9
12	DE	Germany	42,146	0.38	1,383,770	0.42	8,664	SMTP (97.83), S4 (1.06), S5 (1.11)	9
13	NL	Netherlands	37,215	0.33	1,245,812	0.38	8,514	SMTP (97.49), S4 (1.21), S5 (1.30)	9
14	IR	Iran, Islamic Republic of	32,461	0.29	1,049,467	0.32	8,552	SMTP (93.31), S4 (3.23), S5 (3.47)	9
15	FR	France	30,795	0.28	1,014,317	0.31	8,008	SMTP (94.82), S4 (2.50), S5 (2.68)	9
16	MX	Mexico	28,304	0.25	913,371	0.28	8,154	SMTP (91.67), S4 (4.12), S5 (4.21)	9
17	RO	Romania	26,175	0.23	458,925	0.14	3,391	SMTP (100.00)	7
18	ID	Indonesia	24,565	0.22	822,220	0.25	5,597	SMTP (97.96), S4 (0.97), S5 (1.07)	9
19	CA	Canada	23,907	0.21	831,693	0.25	5,365	SMTP (100.00)	7
20	HK	Hong Kong	22,920	0.20	433,421	0.13	11,601	HTTP (41.39), SMTP (26.11), S4 (17.75), S4a (0.00), S5 (14.75)	9
21	VN	Vietnam	22,123	0.20	773,615	0.24	5,242	SMTP (100.00)	6
22	AR	Argentina	21,036	0.19	679,513	0.21	6,003	SMTP (92.31), S4 (3.81), S5 (3.87)	8
23	CO	Colombia	20,484	0.18	701,494	0.21	4,658	SMTP (100.00)	9

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

Questions?

Cristine Hoepers
cristine@cert.br

- **CGI.br - Brazilian Internet Steering Committee**
  http://www.cgi.br/
- **NIC.br**
  http://www.nic.br/
- **CERT.br**
  http://www.cert.br/
- **honeyTARG – honeypots for Threats and Abuse passive Reconnaissance and information Gathering**
  http://honeytarg.cert.br/

cert.br 15 YEARS