Spam Metrics
Brazil

Cristine Hoepers
General Manager
cristine@cert.br

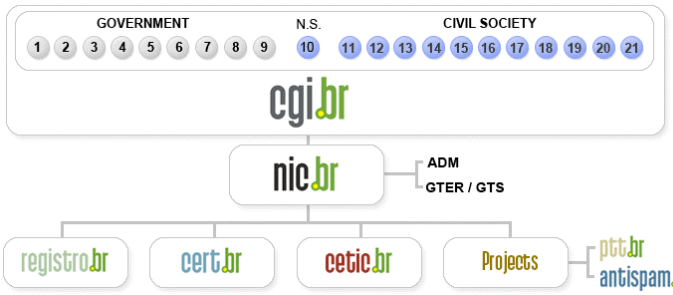
CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

CERT.br - Brazilian National CERT

- Created in 1997 to *handle computer security incidents related to networks connected to the Internet in Brazil.*
  - National focal point for reporting security incidents
  - Establish collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling
  - **Produce best practices' documents**
  - Help raise the security awareness in the country
  - **Maintain public statistics about incidents and abuse**
- APWG Research Partner - http://www.antiphishing.org/
- FIRST Full member - http://www.first.org/
- Honeynet Research Alliance Member - http://www.honeynet.org/

http://www.cert.br/mission.html

Internet Governance in Brazil: The Brazilian Internet Steering Committee – CGI.br (1/2)



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

Internet Governance in Brazil: The Brazilian Internet Steering Committee – CGI.br (2/2)

CGI.br is a multi-stakeholder organization that, among the diverse responsibilities, has the main attributions:

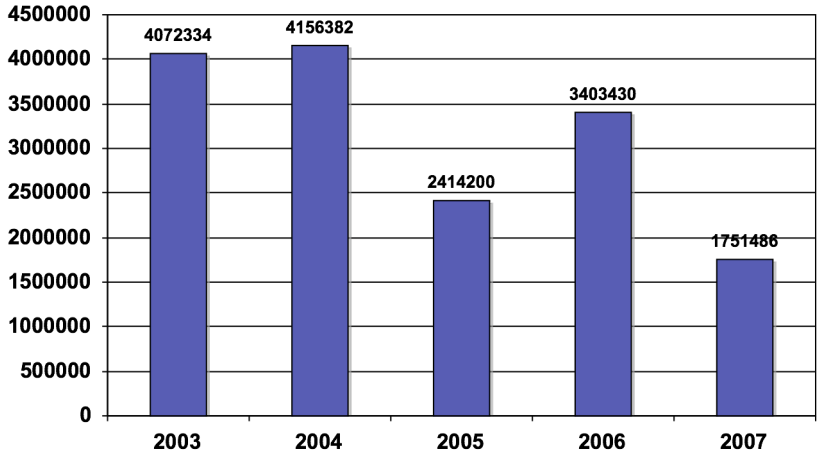
- to propose policies and procedures related to the regulation of Internet activities
- **to recommend standards for technical and operational procedures**
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the 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/internacional/

Agenda

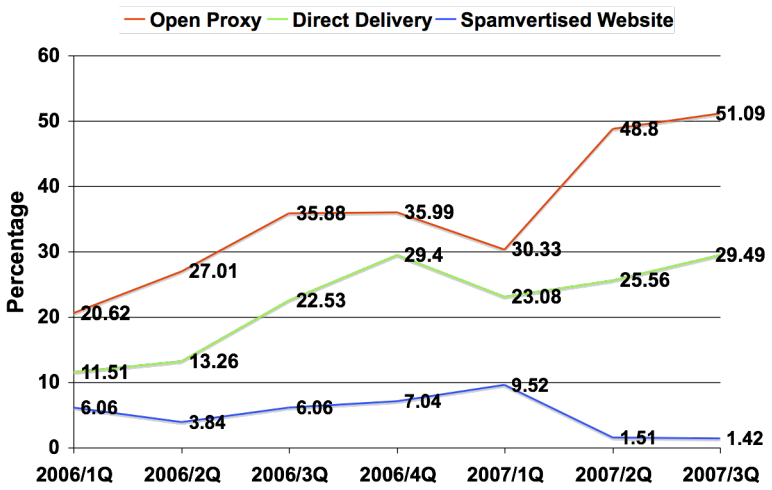
- Spam complaints to CERT.br
  - Progression since 2003
  - Common types in 2006 and 2007
- Other metrics
  - Motivations
  - Data gathered

Total Spam Complaints (2003–Sep/2007)



Source: http://www.cert.br/stats/spam/

Spam Complaints via SpamCop



Source: http://www.cert.br/stats/spam/

Other Metrics

Different Views, Different Data

- What we “hear”
  - Open proxies are not an issue anymore
  - Only botnets are used nowadays to send/relay spam
- Our data
  - Spam complaints related to open proxy abuse have increased in the past few years – just bots?
  - Spam tools still have “features” that scan for open proxies
  - Scans for open proxies are in the top 10 ports
    - in incidents reported to CERT.br
    - in our honeypots’ network statistics
      http://www.honeypots-alliance.org.br/stats/

Issues to be Addressed

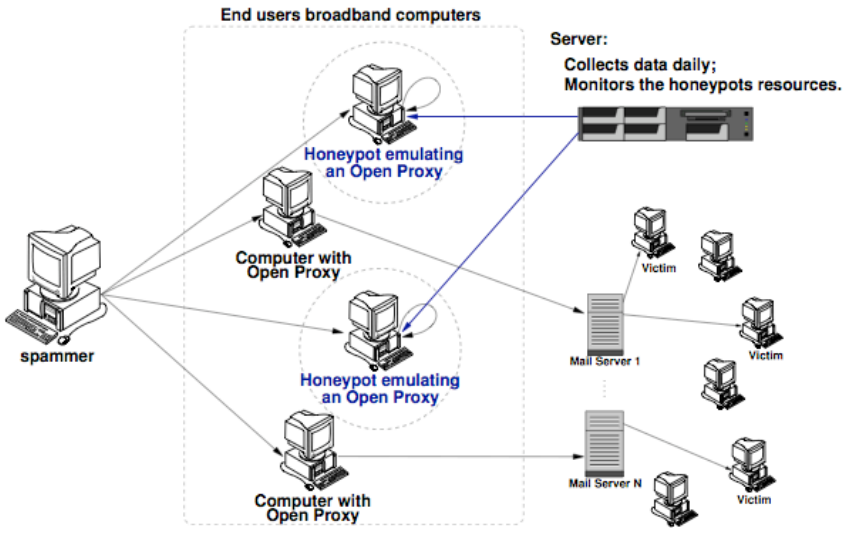
Questions raised during the Antispam Task Force work:

- How to explain bots/proxy abuse to policy makers and legislators?
- How to convince business people of possible mitigations’ needs/effectiveness?
- Who is abusing our infrastructure? And How?
- Do we have national metrics or only international?
- Any public metrics from neutral sources?
- How can we gather data and generate metrics to help the formulation of policies and the understanding of the problem?

The SpamPots Project

- Supported and sponsored by NIC.br/CGI.br
  - As part of the Anti-spam Task Force work
  - To provide some measurement of the abuse of end-user machines to send spam
- Deployment of low-interaction honeypots, emulating open proxy/relay services and capturing spam
  - 10 honeypots in 5 different broadband providers
    - 2 Cable and 3 ADSL
    - 1 home and 1 business connection each
  - Use OpenBSD, Honeyd and some custom listeners
  - Fools spammers' confirmation attempts

The Location of the Sensors

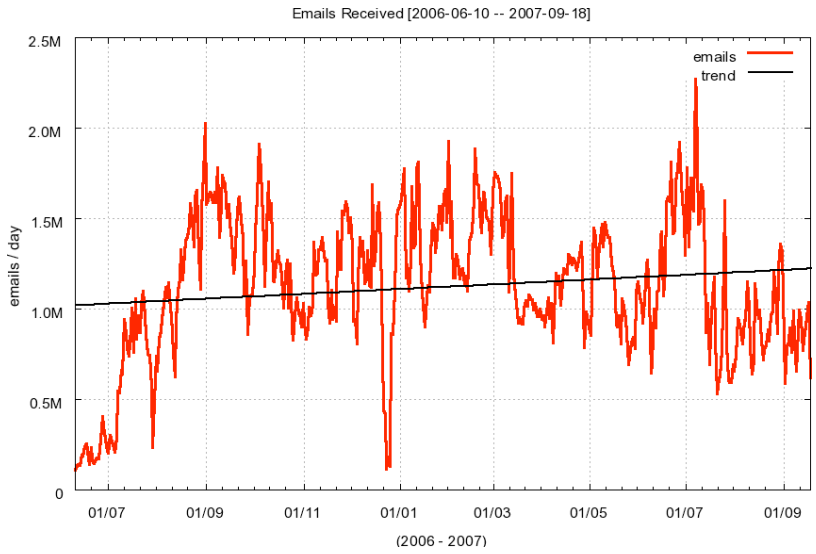


Total Data Collected by the 10 Sensors

Period: June 10, 2006 to September 18, 2007
Days: 466

Emails captured:	524,585,779
Potencial Recipients:	4,805,521,964
Average recipients/email:	≈ 9.1
Average mails/day:	≈ 1.2 Million
Unique IPs seen:	216,888
Unique Autonomous Systems (AS):	3,006
Unique Country Codes (CCs):	165

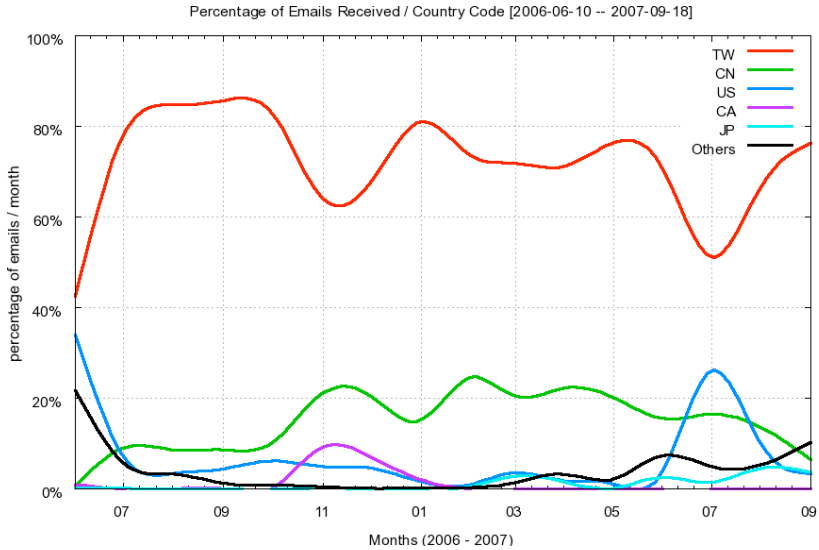
Emails Received Daily



CCs that Injected Most Spam (1/2)

#	CC	E-mails received	%
01	TW	385,189,756	73.43
02	CN	82,884,642	15.80
03	US	29,764,293	5.67
04	CA	6,684,667	1.27
05	JP	5,381,192	1.03
06	HK	4,383,999	0.84
07	KR	4,093,365	0.78
08	UA	1,806,210	0.34
09	DE	934,417	0.18
10	BR	863,657	0.16
		Subtotal:	**99.50**

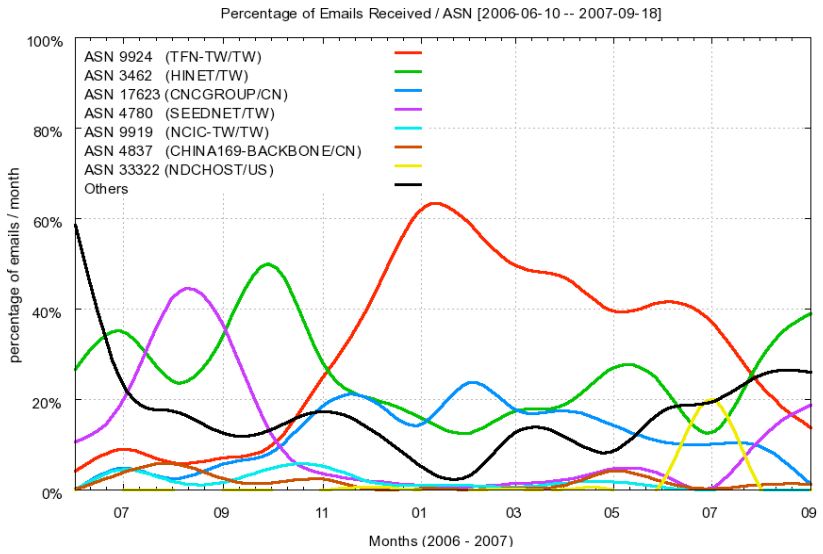
CCs that Injected Most Spam (2/2)



Top Autonomous Systems (1/2)

#	ASN	AS Name	CC	E-mails	%
01	9924	TFN-TW Taiwan Fixed Network	TW	170,998,167	32.60
02	3462	HINET Data Communication Business Group	TW	131,381,486	25.04
03	17623	CNCGROUP IP network of ShenZhen region	CN	65,214,192	12.43
04	4780	SEEDNET Digital United Inc.	TW	54,430,806	10.38
05	9919	NCIC-TW New Century InfoComm Tech Co., Ltd.	TW	9,186,802	1.75
06	4837	CHINA169-BACKBONE CNCGROUP	CN	9,025,142	1.72
07	33322	NDCHOST - Network Data Center Host, Inc.	US	8,359,583	1.59
08	4134	CHINANET-BACKBONE	CN	7,287,251	1.39
09	18429	EXTRALAN-TW Extra-Lan Technologies Co., Ltd	TW	6,746,124	1.29
10	7271	LOOKAS - Look Communications Inc.	CA	5,599,442	1.07
				Subtotal:	**89.26**

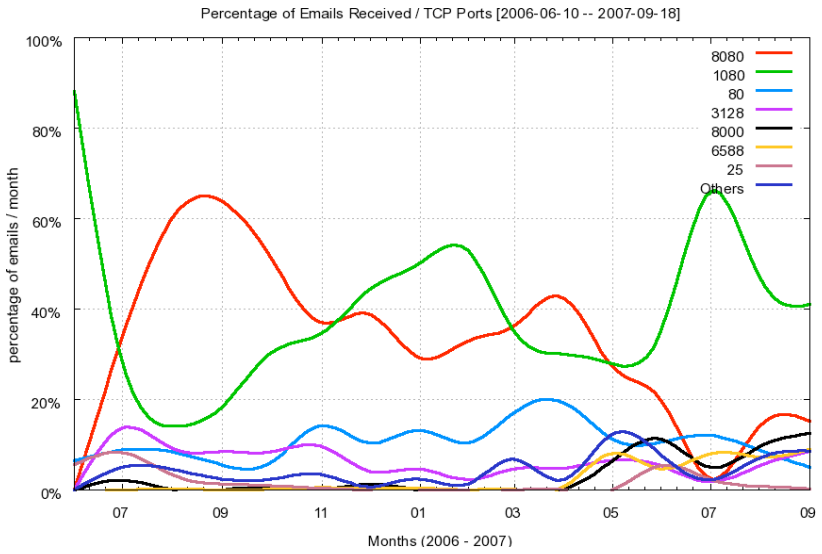
Top Autonomous Systems (2/2)



TCP Ports Abused Over the Period (1/2)

#	TCP Port	Protocol	Usual Service	%
01	1080	SOCKS	socks	37.31
02	8080	HTTP	alternate http	34.79
03	80	HTTP	http	10.92
04	3128	HTTP	Squid	6.17
05	8000	HTTP	alternate http	2.76
06	6588	HTTP	AnalogX	2.29
07	25	SMTP	smtp	1.46
08	4480	HTTP	Proxy+	1.38
09	3127	SOCKS	MyDoom Backdoor	1.00
10	3382	HTTP	Sobig.f Backdoor	0.96
11	81	HTTP	alternate http	0.96

TCP Ports Abused Over the Period (2/2)



Requests to the HTTP and SOCKS Modules

Number of requests received by the modules, divided according to connection type:

HTTP		
Type	Requests	%
connect to 25/TCP	89,496,969	97.62
connect to others	106,615	0.12
get	225,802	0.25
errors	1,847,869	2.01
total	91,677,255	100.00

SOCKS		
Type	Requests	%
connect to 25/TCP	46,776,884	87.31
connect to others	1,055,081	1.97
errors	5,741,908	10,72
total	53,573,873	100.00

Other Activities in Place

- More comprehensive spam analysis
  - Using Data Mining techniques
  - Identify:
    - patterns in language, embedded URLs, spam campaigns, etc
    - Phishing and other online crime activities
- International cooperation

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

References

- This presentation – by the end of the month
  http://www.cert.br/docs/presentations/
- CERT.br - Computer Emergency Response Team Brazil
  http://www.cert.br/
- NIC.br - Network Information Center Brazil
  http://www.nic.br/
- CGI.br - Brazilian Internet Steering Committee
  http://www.cgi.br/