Monitoring the Abuse of Open Proxies for Sending Spam

Klaus Steding-Jessen

jessen@cert.br

CERT.br – Computer Emergency Response Team Brazil

NIC.br – Network Information Center Brazil

CGI.br – Brazilian Internet Steering Committee

About CERT.br

Created in 1997 to receive, review and respond to computer security incident reports and activities related to networks connected to the Internet in Brazil.

- National focal point for reporting security incidents
- Establishes collaborative relationships with other entities
- Helps new CSIRTs to establish their activities
- Provides training in incident handling
- Provides statistics and best practices' documents
- Helps raise the security awareness in the country

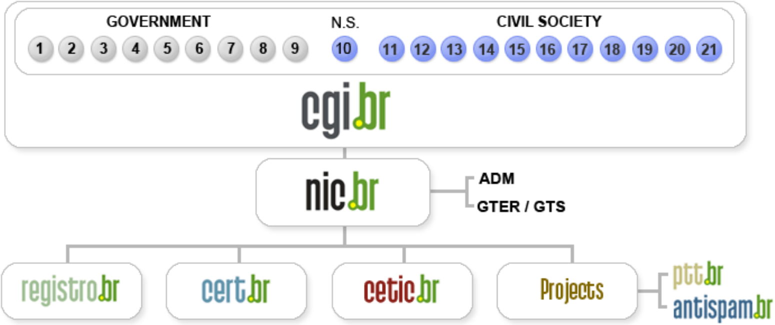
`http://www.cert.br/mission.html`

Our Parent Organization: CGI.br

Among the diverse responsibilities of The Brazilian Internet Steering Committee – CGI.br, the main attributions are:

- to propose policies and procedures related to the regulation of the 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 (IPs) and the registration of domain names using <.br>
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

CGI.br Structure



GOVERNMENT
1 2 3 4 5 6 7 8 9

N.S.
10

CIVIL SOCIETY
11 12 13 14 15 16 17 18 19 20 21

cgi.br

nic.br

ADM
GTER / GTS

registro.br

cert.br

cetic.br

Projects

ptt.br
antispam.br

01- Ministry of Science and Technology
02- Ministry of Communications
03- Presidential Cabinet
04- Ministry of Defense
05- Ministry of Development, Industry and Foreign Trade
06- Ministry of Planning, Budget and Management
07- National Telecommunications Agency
08- National Council of Scientific and Technological Development
09- National Forum of Estate Science and Technology Secretaries
10- Internet Expert

11- Internet Service Providers
12- Telecom Infrastructure Providers
13- Hardware and Software Industries
14- General Business Sector Users
15- Non-governamental Entity
16- Non-governamental Entity
17- Non-governamental Entity
18- Non-governamental Entity
19- Academia
20- Academia
21- Academia

Agenda

- Motivation
- The SpamPots Project
  - Open Proxy Abuse Scenario
  - Architecture
  - Honeypots
  - Server
- Statistics
- Future Work
- References

Motivation

The Nature of the Problem

- Spam is a source of
  - malware/phishing
  - decrease in productivity
  - increase in infrastructure costs

- Congress and regulators
  - Are pressed by the general public to “do something about it”
  - Have several questionable law projects to consider
  - Don’t have data that show the real spam scenario

Motivation (2)

Different Views, Different Data

- What we "hear"
  - Open proxies are not an issue anymore
  - Only botnets are used nowadays to send/relay spam
  - Brazil is a big "source" of spam
- Our data
  - Spam complaints related to open proxy abuse have increased in the past few years
  - Scans for open proxies are always in the top 10 ports in our honeypots' network statistics

    `http://www.honeypots-alliance.org.br/stats/`

Motivation (3)

Still Lots of Questions

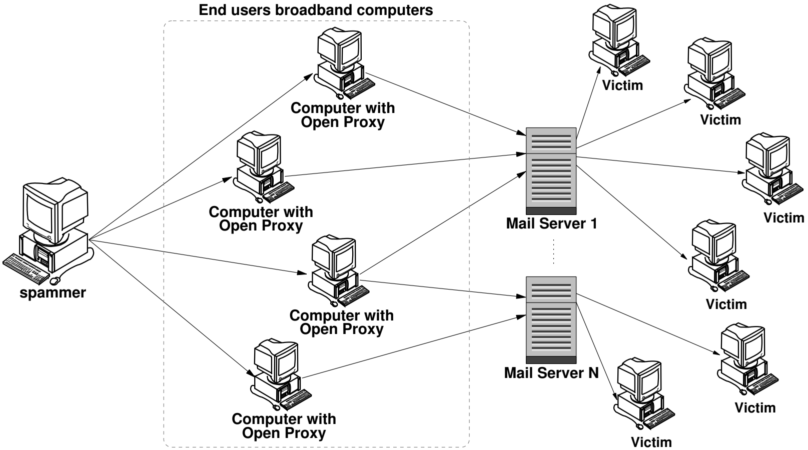
- How to convince business people of possible mitigation measures needs/effectiveness?
  - Port 25 management, e-mail reputation, etc
- Who is abusing our infrastructure? And How?
- Do we have national metrics or only international?
- How can we gather data and generate metrics to help the formulation of policies and the understanding of the problem?

Need to better understand the problem and have more data about it

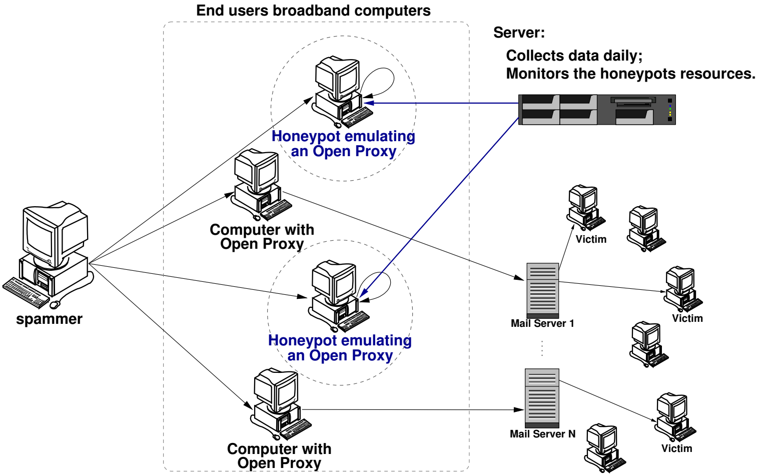
The SpamPots Project

- Supported by the CGI.br/NIC.br
  - as part of the Anti-spam Commission work
- Deployment of 10 low-interaction honeypots, emulating open proxy/relay services and capturing spam
- Installed on Brazilian ADSL/cable networks, for 15 months
  - 5 broadband providers, 1 home and 1 business connection each
- Measure the abuse of end-user machines to send spam

Open Proxy Abuse Scenario



Architecture


End users broadband computers
Server:
Collects data daily;
Monitors the honeypots resources.
Honeypot emulating an Open Proxy
Computer with Open Proxy
spammer
Honeypot emulating an Open Proxy
Computer with Open Proxy
Victim
Mail Server 1
Victim
Mail Server N
Victim

Honeypots

- OpenBSD as the base OS
  - good proactive security features
  - pf packet filter: stateful, integrated queueing (ALTQ), port redirect
  - logs in libpcap format: allows passive fingerprinting
- Honeyd emulating services
  - Niels Provos' SMTP and HTTP Proxy emulator (with minor modifications)
  - SOCKS 4/5 emulator written by ourselves
  - pretends to connect to the final SMTP server destination and starts receiving the emails
  - doesn't deliver the emails
- Fools spammers' confirmation attempts

Server

- Collects and stores data from honeypots
  - initiates transfers through ssh connections
  - uses rsync over ssh to copy spam from the honeypots
- Performs status checks in all honeypots
  - daemons, ntp, disk space, load, rsync status
- Web page interface
  - honeypot status
  - emails stats: daily, last 15min
  - MRTG: bandwidth, ports used, emails/min, etc

Statistics

Statistics

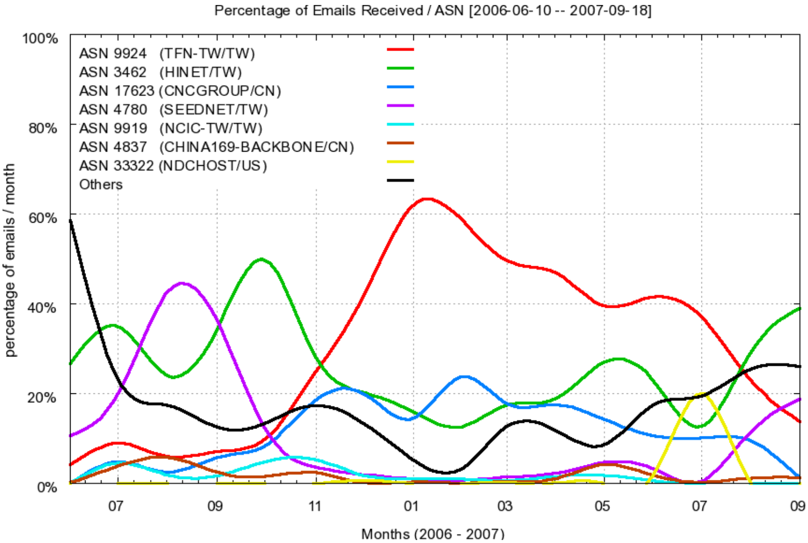
period	2006-06-10 to 2007-09-18
days	466
emails	524.585.779
avg. emails/day	1.125.720
recipients	4.805.521.964
avg. recpts/email	$\approx$ 9,2
unique IPs	216.888
unique ASNs	3006
unique CCs	165

Top ASNs sending spam

- Top 10 emails/ASN:

#	ASN	ASN Name	Emails	%
01	9924	TFN-TW (TW)	170.998.167	32,60
02	3462	HINET (TW)	131.381.486	25,04
03	17623	CNCGROUP (CN)	65.214.192	12,43
04	4780	SEEDNET (TW)	54.430.806	10,38
05	9919	NCIC-TW (TW)	9.186.802	1,75
06	4837	CHINA169 (CN)	9.025.142	1,72
07	33322	NDCHOST (US)	8.359.583	1,59
08	4134	CHINANET (CN)	7.287.251	1,39
09	18429	EXTRALAN (TW)	6.746.124	1,29
10	7271	LOOKAS (CA)	5.599.442	1,07

Top ASNs sending spam (2)

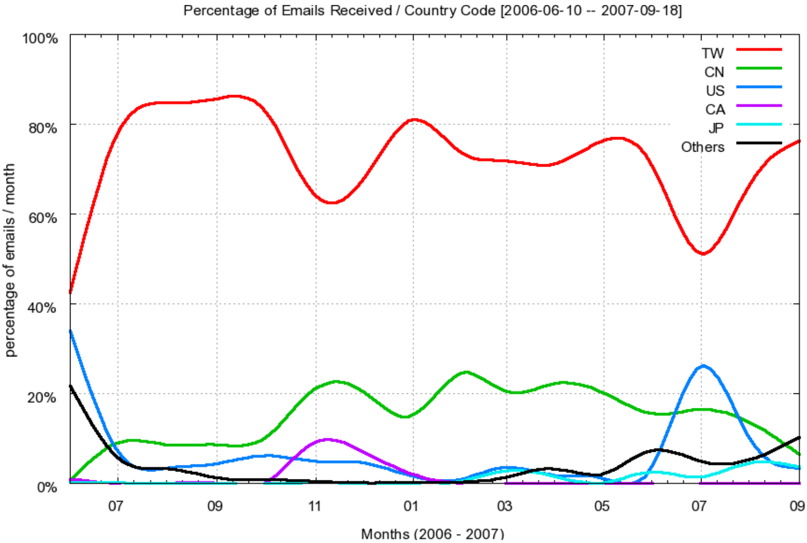


Top CCs sending spam

- Top 10 emails/CC:

#	CC	Emails	%
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

Top CCs sending spam (2)

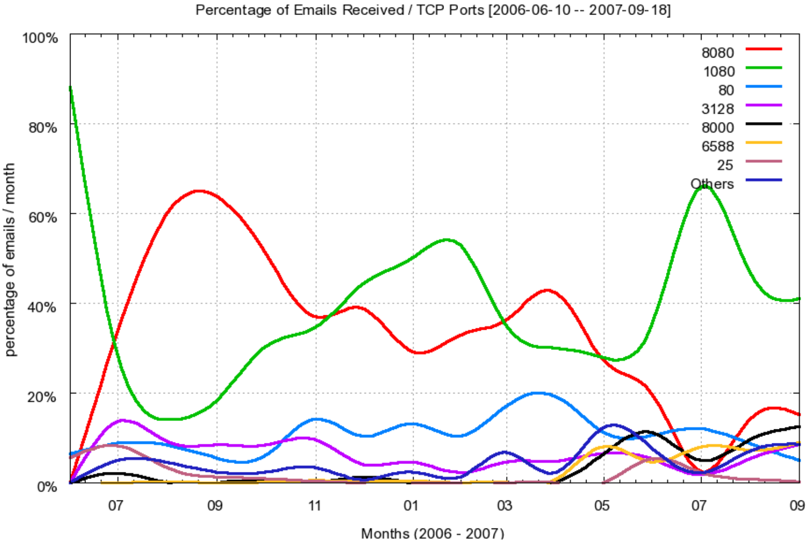


Top TCP ports used

- TCP ports used:

#	TCP Port	protocol	used by	%
01	1080	SOCKS	socks	37,31
02	8080	HTTP	alt http	34,79
03	80	HTTP	http	10,92
04	3128	HTTP	Squid	6,17
05	8000	HTTP	alt 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	1,00
10	3382	HTTP	Sobig.f	0,96
11	81	HTTP	alt http	0,96

Top TCP ports used (2)



Request Types

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

Future Work

Future Work

- Comprehensive spam analysis
  - using Data Mining techniques
  - determine patterns in language, embedded URLs, etc
  - phishing and other online crime activities
- Propose best practices to ISPs
  - port 25 management
  - proxy abuse monitoring
- International cooperation

References

- This presentation can be found at:
  http://www.cert.br/docs/presentations/
- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/
- OpenBSD
  http://www.openbsd.org/
- Honeyd
  http://www.honeyd.org/
- Brazilian Honeypots Alliance
  http://www.honeypots-alliance.org.br/