Using Honeypots to Monitor Spam and Attack Trends

Marcelo H. P. C. Chaves

mhp@cert.br

CERT.br – Computer Emergency Response Team Brazil

NIC.br – Network Information Center Brazil

CGI.br – Brazilian Internet Steering Committee

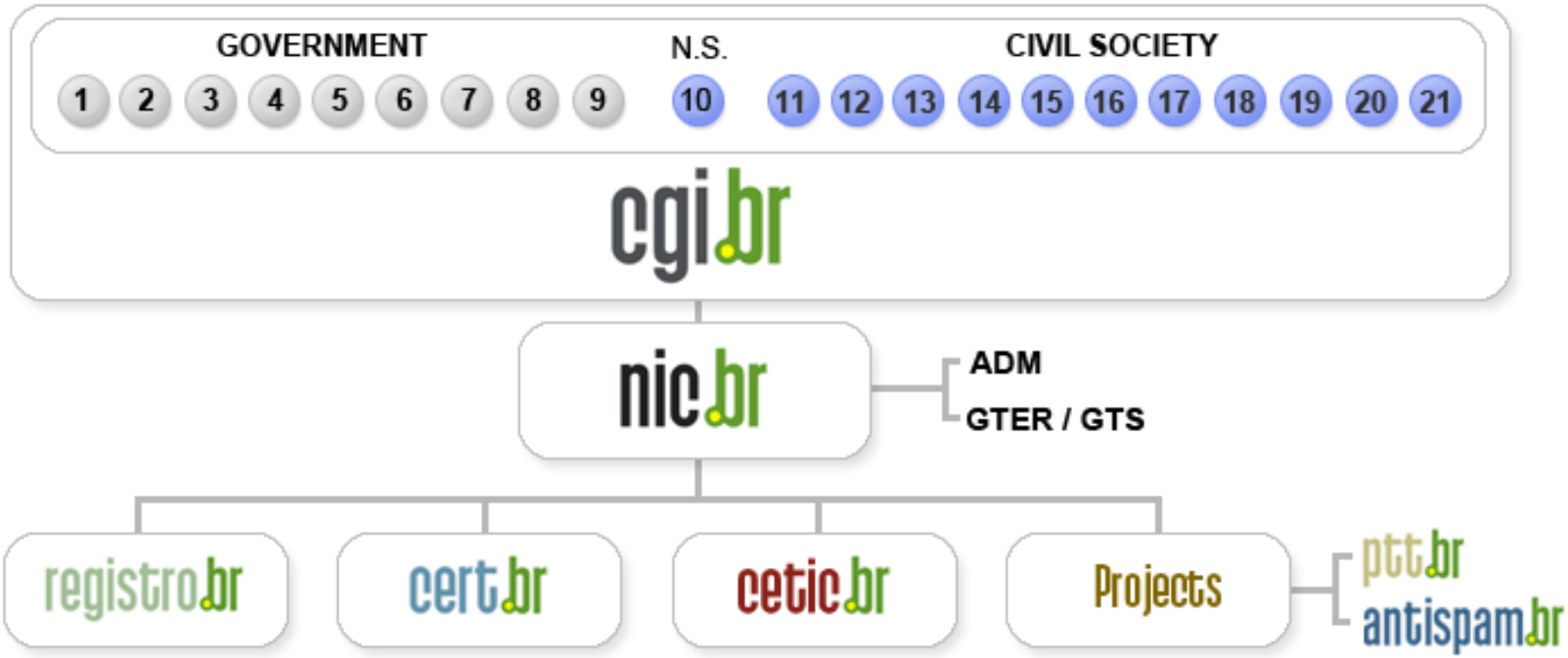
About CERT.br

Created in 1997 to handle 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

CGI.br Structure



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- Telecommunication 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

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**

Agenda

- Timeline
- The Distributed Honeypots Project
  - Objective
  - Architecture
  - Key Points, Benefits and Disavantages
  - Statistics
- The SpamPots Project
  - Objectives and Structure
  - Architecture
  - Statistics
  - Next Steps
- References

Timeline

- March/2002
  - Honeynet.BR project first honeynet deployed
- June/2002
  - Joined the Honeynet Research Alliance
- September/2003
  - The “Brazilian Honeypots Alliance – Distributed Honeypots Project” was started

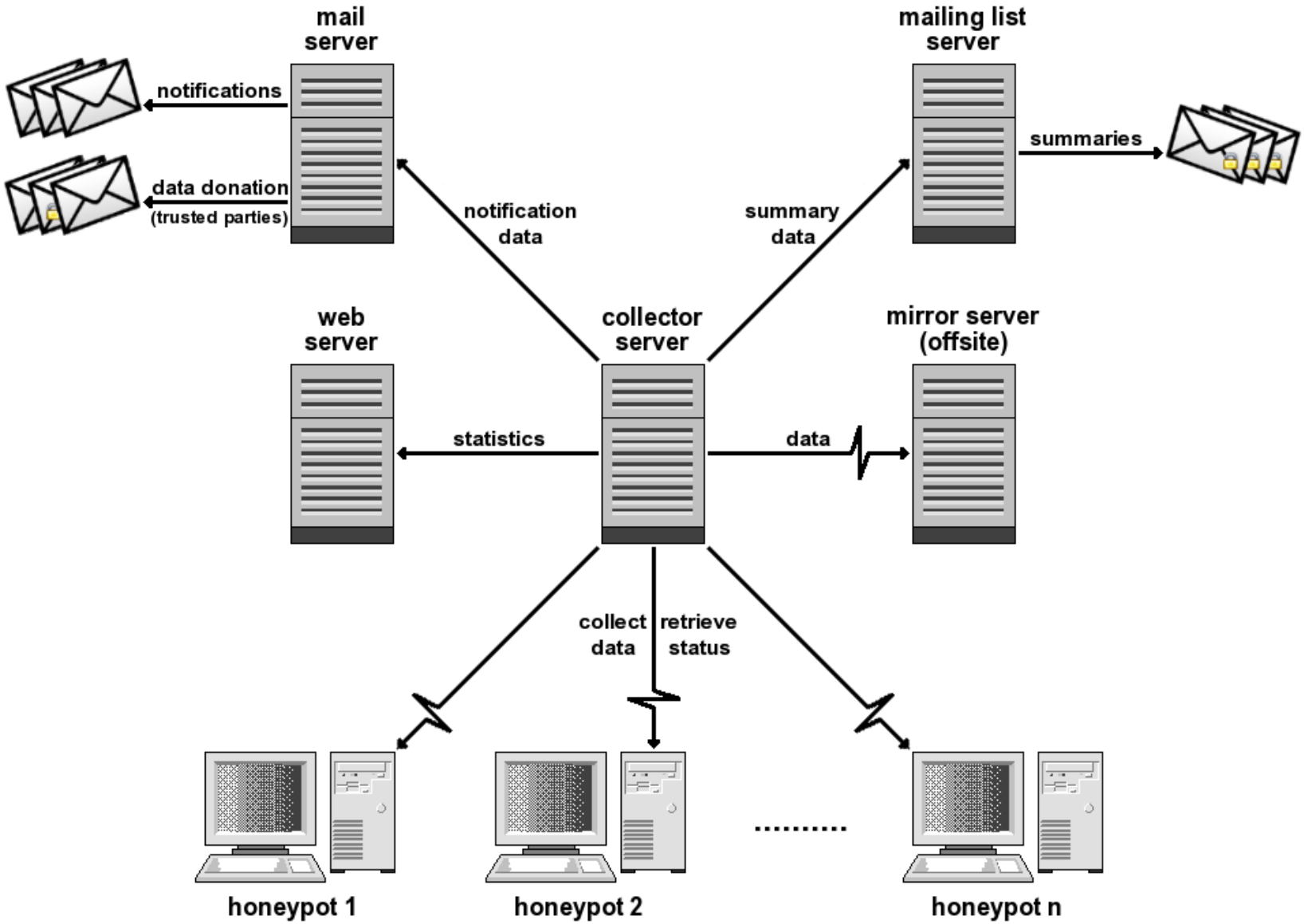
Brazilian Honeypots Alliance
Distributed Honeypots Project

Main Objective

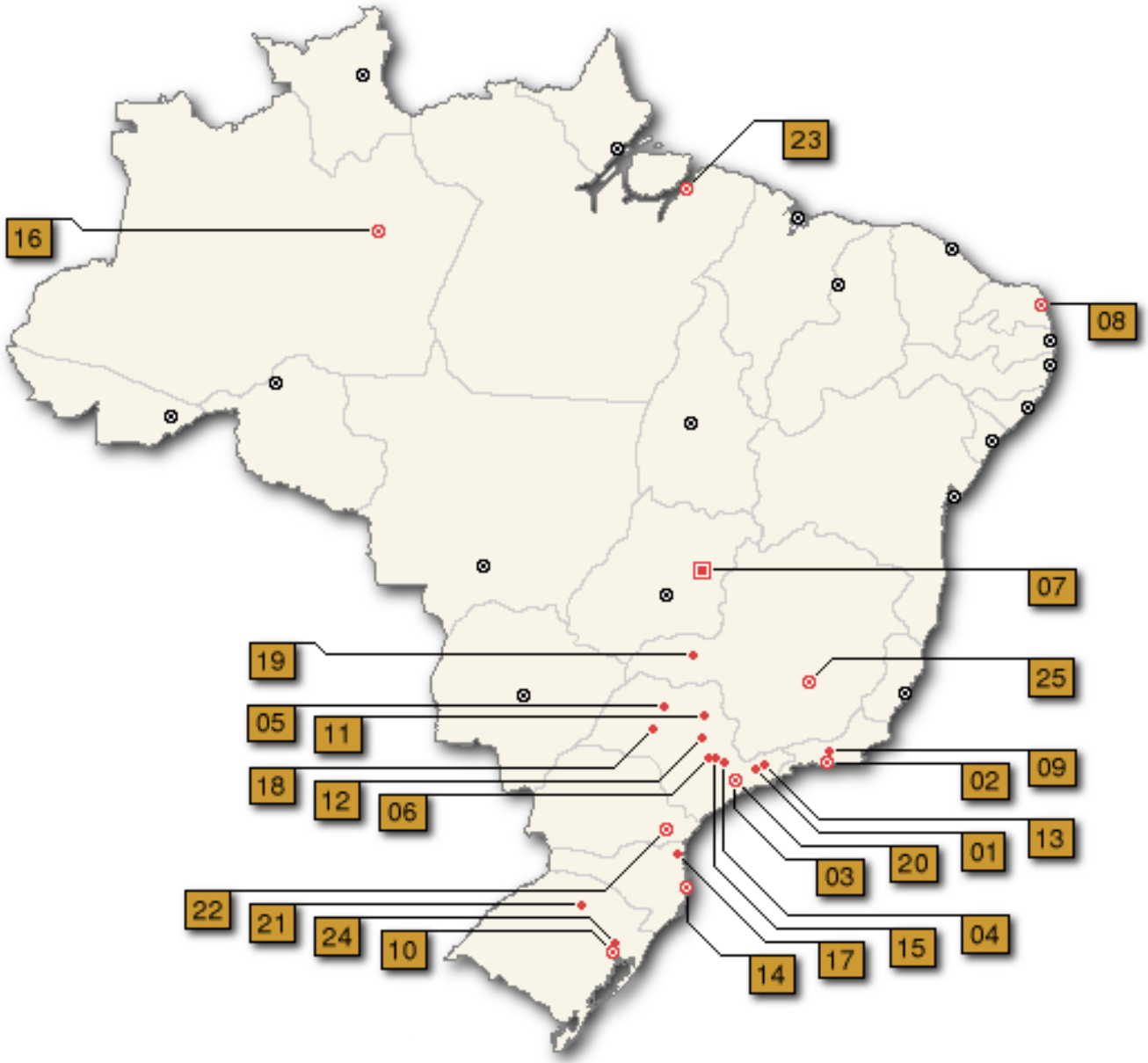
Increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 39 partner's institutions:
  - Academic, government, industry, telecom and military networks
- Widely distributed across the country
- Based on voluntary work
- Honeypots based on OpenBSD and Honeyd
- Maintain public statistics
  http://www.honeypots-alliance.org.br/

Architecture



Cities Where the Honeypots are Located



39 Partners of the Brazilian Honeypots Alliance

#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, TIVIT, UNESP, UOL, USP
04	Campinas	CenPRA, ITAL, UNICAMP
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Banco do Brasil, Brasil Telecom, Ministério da Justiça, TCU
08	Natal	UFRN
09	Petrópolis	LNCC
10	Porto Alegre	CERT-RS
11	Ribeirão Preto	USP
12	São Carlos	USP
13	Taubaté	UNITAU
14	Florianópolis	UFSC DAS
15	Americana	VIVAX
16	Manaus	VIVAX
17	Joinville	UDESC
18	Lins	FPTE
19	Uberlândia	CTBC Telecom
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	Onda, PoP-PR, PUCPR
23	Belém	UFPA
24	São Leopoldo	Unisinos
25	Belo Horizonte	Diveo

Key Points to Keep and Reach Partners

We are not offering a “black box”

- They have access to their honeypots
- They can extend the honeypot configuration

The honeypot does not capture production data

- Only data directed to the honeypot is collected

They can use their data freely

- For example, as a complement to their IDS infrastructures

We provide specific information to partners

- Daily summaries (sanitized) – each, combined, correlated

Info exchanged with an encrypted mailing list

Benefits and Disavantages

Short Term Benefits

- Few false positives, low cost and low risk
- Networks originating malicious activities notified
- Production of stats and ability to collect malware samples

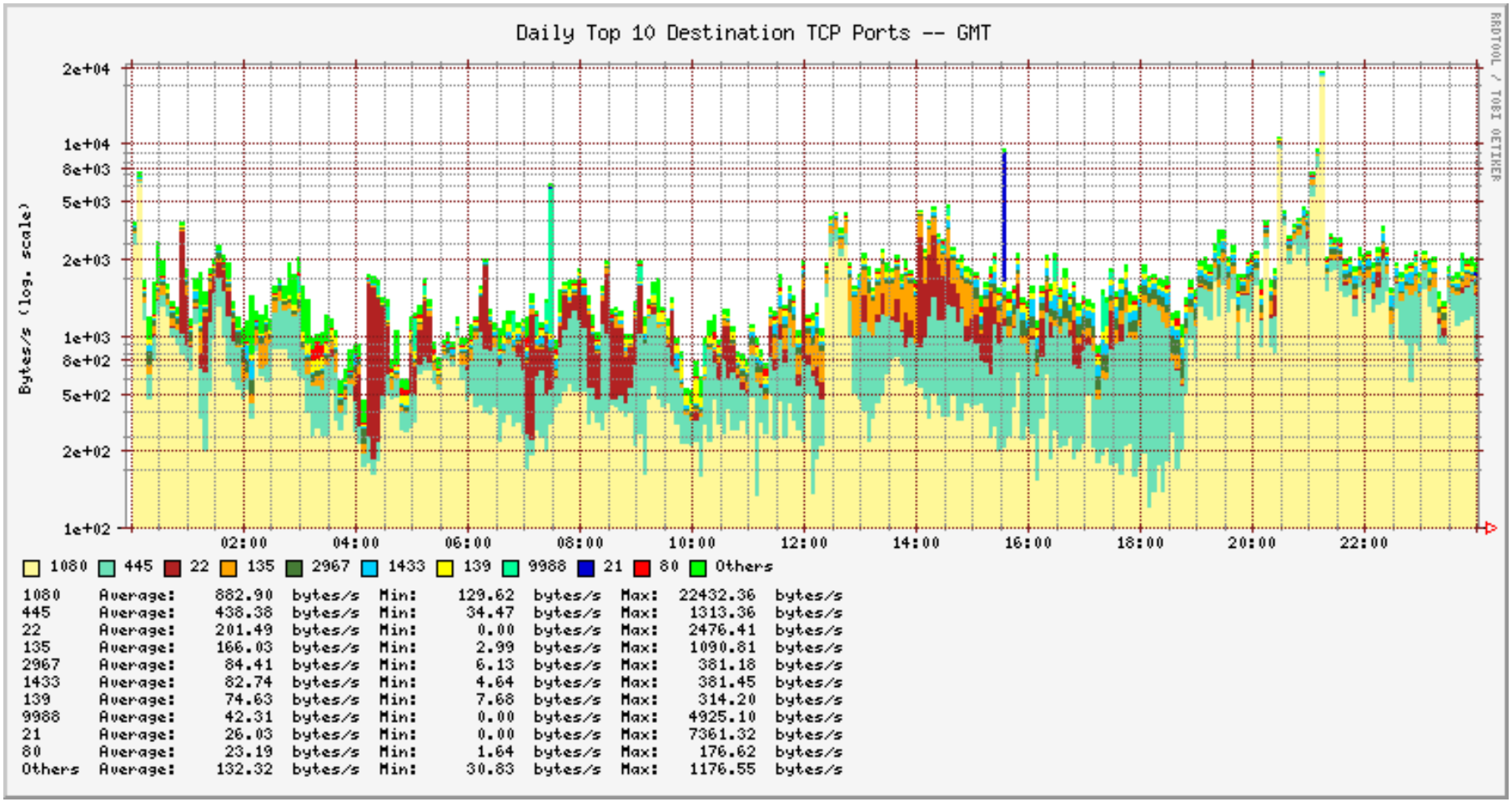
Long Term Benefits

- Allow members to improve their expertise in several areas: honeypots, firewall, IDS, OS hardening, PGP, etc
- Improve CERT.br's relationship with the partners

Disavantages

- Harder to maintain than a "plug and play" honeypot
- Honeypots usually don't catch attacks targeted to production networks
- Information gathered is limited

Public Statistics: Honeypots Flows

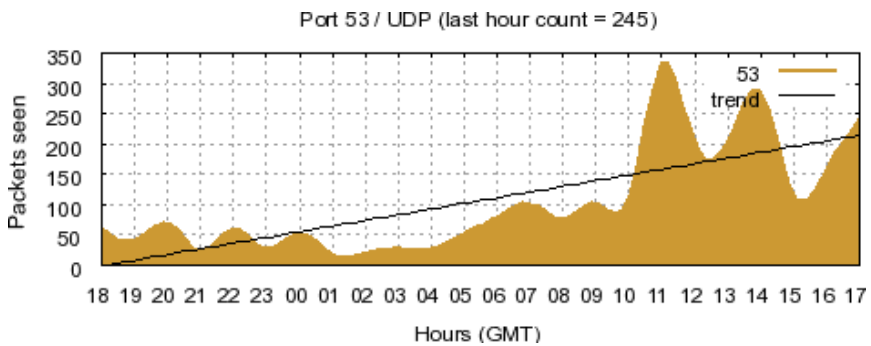


August 08, 2007 – http://www.honeypots-alliance.org.br/stats/

Public Statistics: Port summary (coming soon)

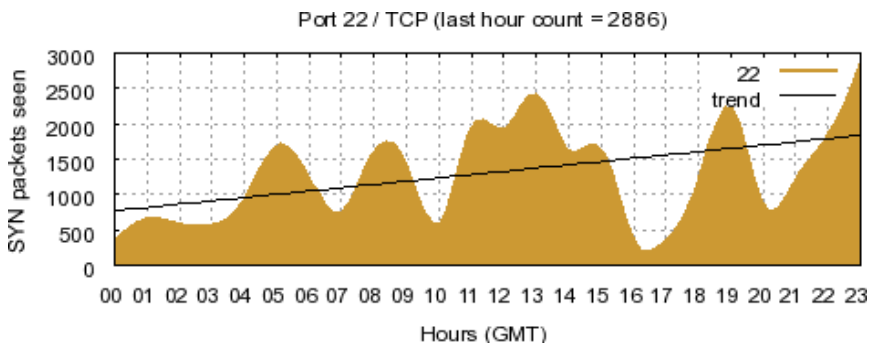
- Hourly

17: 2007-08-12 18:00 – 2007-08-13 17:59 (GMT)



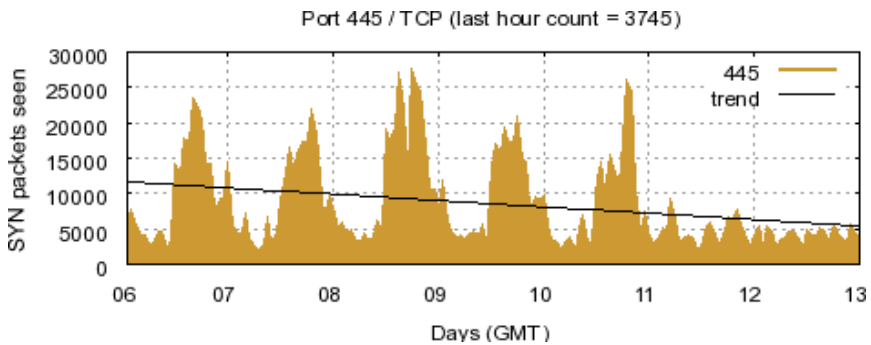
- Daily

12: 2007-08-12 00:00 – 2007-08-12 23:59 (GMT)



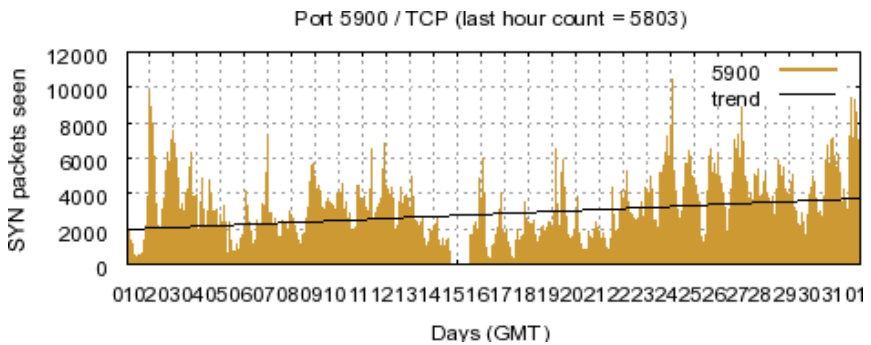
- Weekly

32: 2007-08-06 00:00 – 2007-08-12 23:59 (GMT)



- Monthly

07: 2007-07-01 00:00 – 2007-07-31 23:59 (GMT)



The SpamPots Project

Using Honeypots to Measure the Abuse of End-User Machines to Send Spam

Objectives and Structure

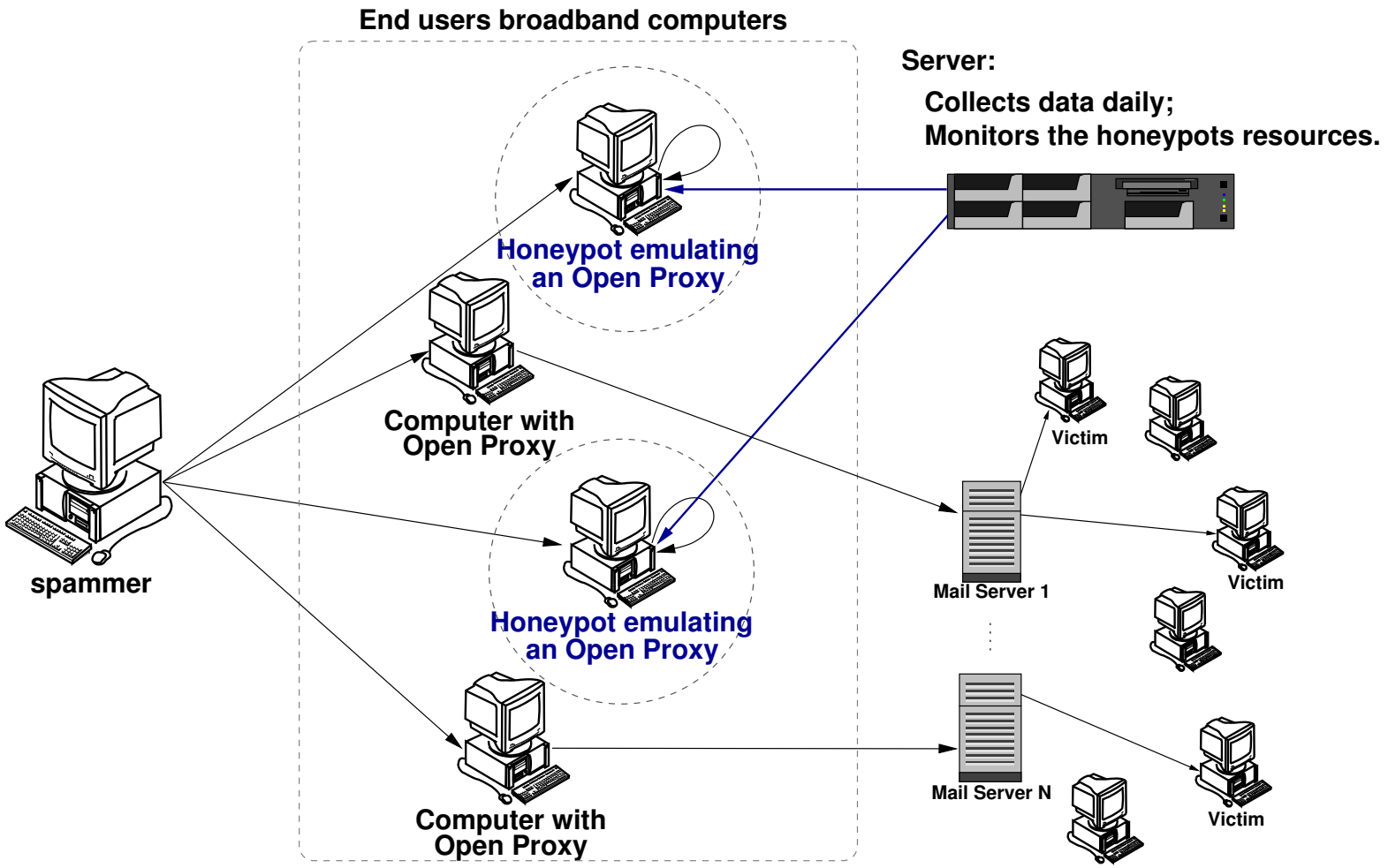
Objectives

- Better understand the abuse of end-user machines to send spam
  - source, different types, language, etc
- Generate metrics to help the formulation of policies

Structure

- Supported by CGI.br/NIC.br Anti-spam Commission
- 10 honeypots in 5 different broadband providers
  - 1 residential an 1 business connection each
  - based on OpenBSD and Honeyd
  - emulate open proxy/relay services and capture spam
  - do **not** deliver the emails

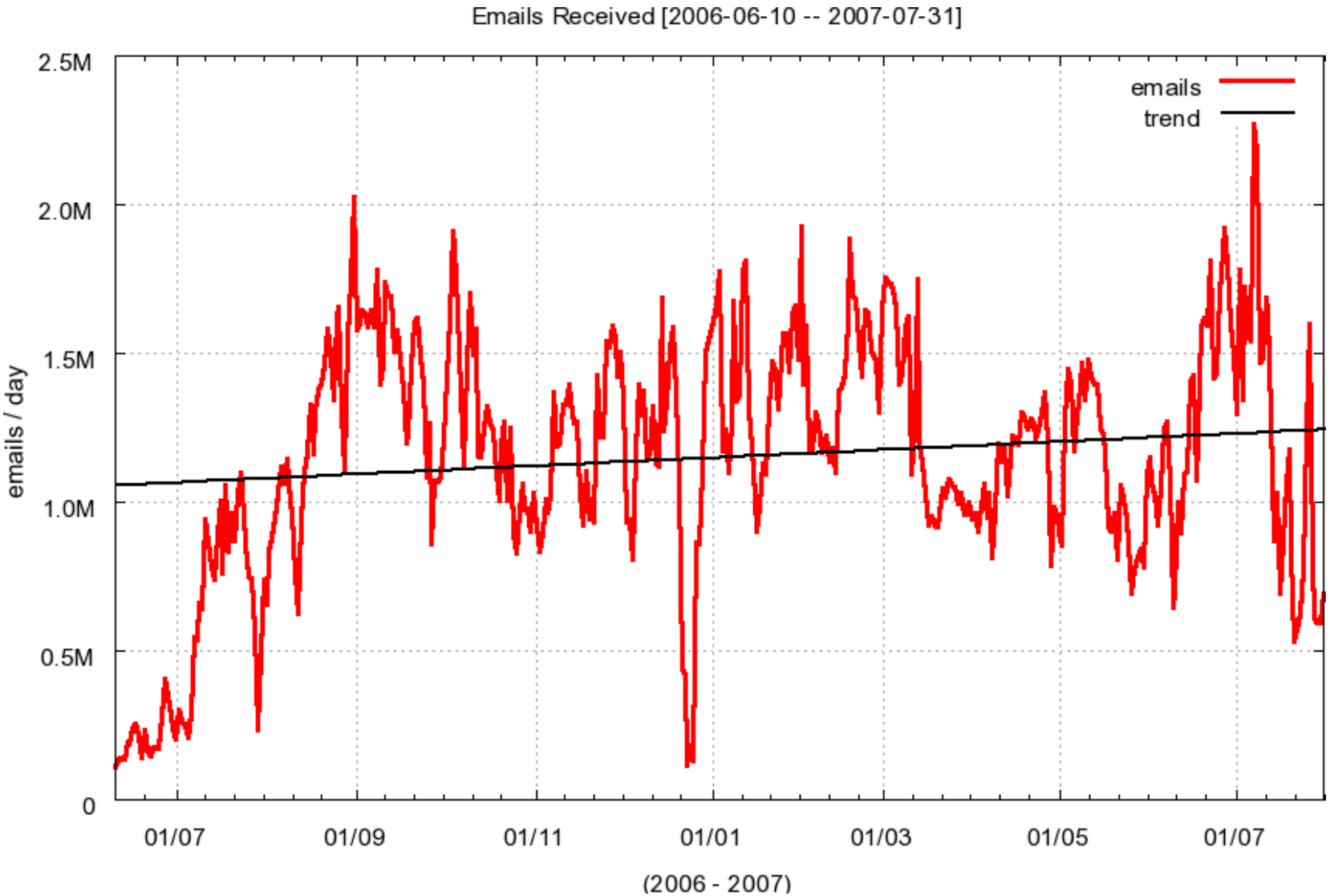
Architecture



Statistics: The Big Picture

period	2006-06-10 to 2007-07-31
days	417
emails captured	480.120.724
recipients	4.307.010.941
avg. recpts/email	$\approx$ 8.97
avg. emails/day	1.151.368
unique IPs seen	209.327
unique ASNs	2.966
unique CCs	164

Statistics: Spams captured / day

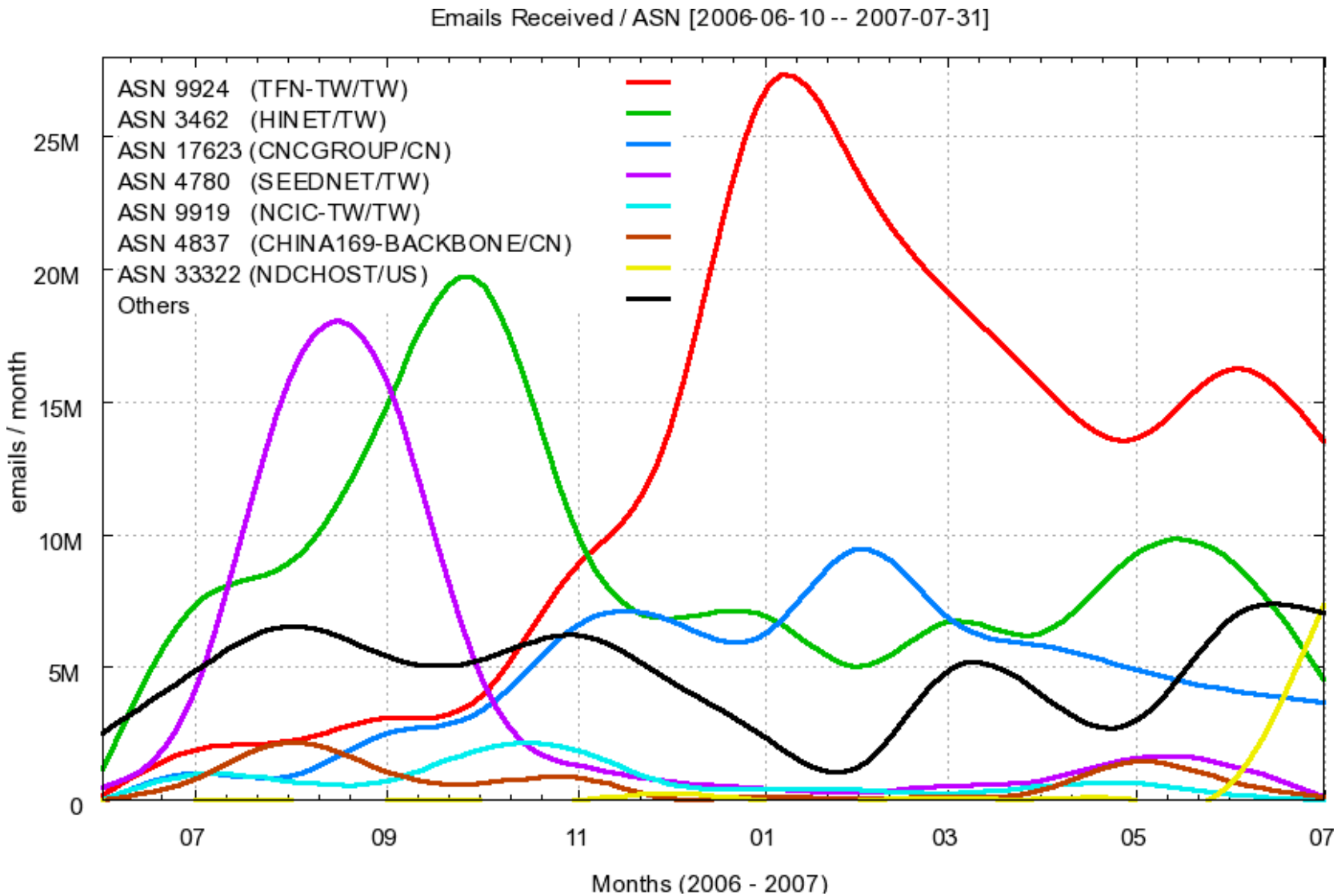


Statistics: Most frequent ASNs

- Top 10 emails/ASN:

#	ASN	AS Name	%
01	9924	TFN-TW Taiwan Fixed Network / TW	33.77
02	3462	HINET Data Communication / TW	24.35
03	17623	CNCGROUP-SZ CNCGROUP / CN	12.97
04	4780	SEEDNET Digital United / TW	10.04
05	9919	NCIC-TW / TW	1.91
06	4837	CHINA169-BACKBONE CNCGROUP / CN	1.77
07	33322	NDCHOST / US	1.73
08	4134	CHINANET-BACKBONE / CN	1.29
09	7271	LOOKAS - Look Communications / CA	1.17
10	18429	EXTRALAN-TW / TW	1.08

Statistics: Most frequent ASNs (2)

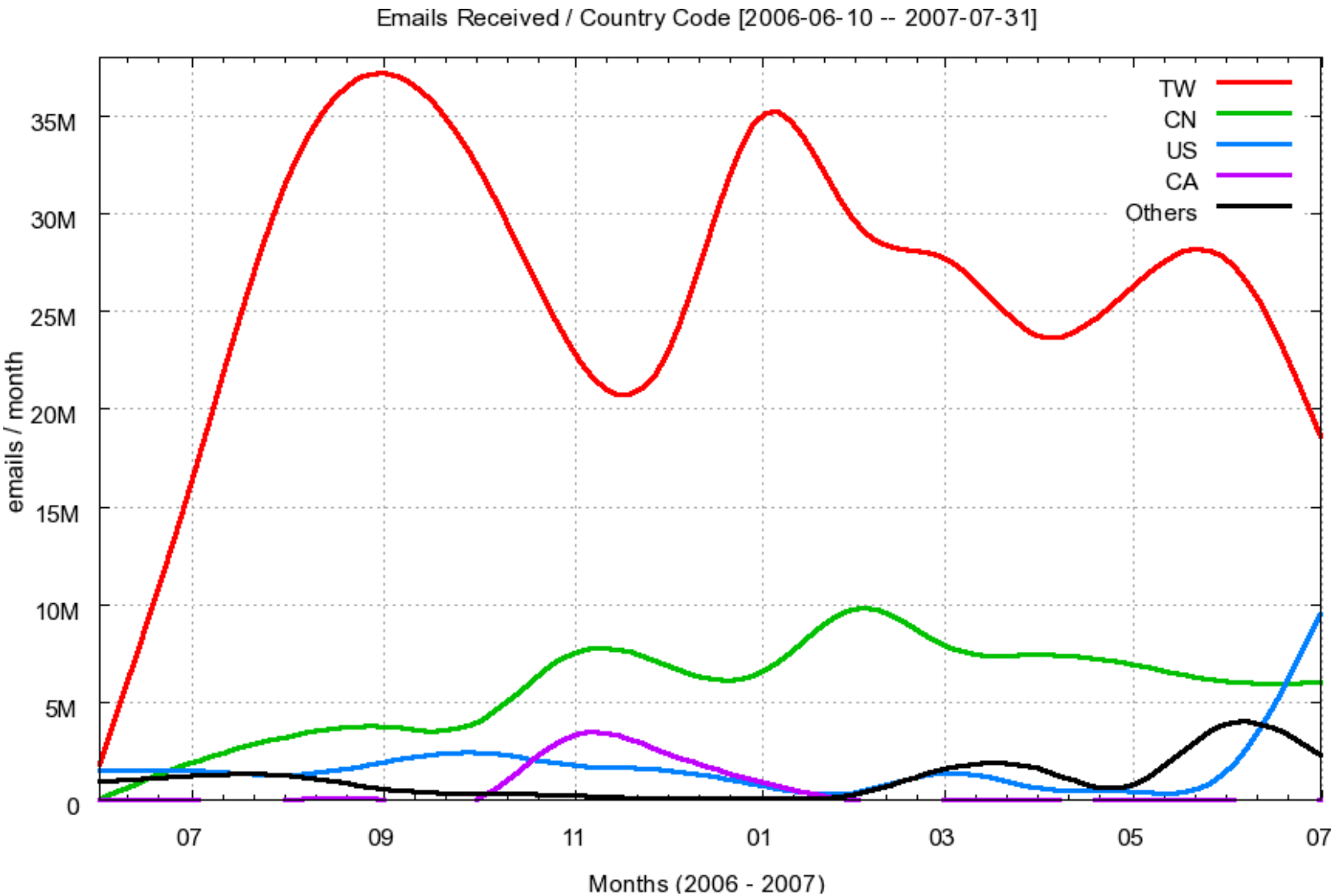


Statistics: Most frequent CCs

- Top 10 emails/CC:

#	emails	CC	%
01	354.042.709	TW	73.74
02	77.922.019	CN	16.23
03	26.384.260	US	5.50
04	6.680.596	CA	1.39
05	3.712.431	KR	0.77
06	3.491.197	JP	0.73
07	3.085.048	HK	0.64
08	932.330	DE	0.19
09	771.130	BR	0.16
10	617.714	UA	0.13

Statistics: Most frequent CCs (2)



Next Steps

- 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

- Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/
- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/
- Brazilian Honeypots Alliance – Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/
- Honeynet.BR
  http://www.honeynet.org.br/
- Previous presentations about the projects
  http://www.cert.br/presentations/
- Several papers presented at other conferences
  http://www.honeynet.org.br/papers/
- SpamPots Project white paper (in Portuguese)
  http://www.cert.br/docs/whitepapers/spampots/