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

Klaus Steding-Jessen

jessen@cert.br

CERT.br – Computer Emergency Response Team Brazil

NIC.br – Network Information Center Brazil

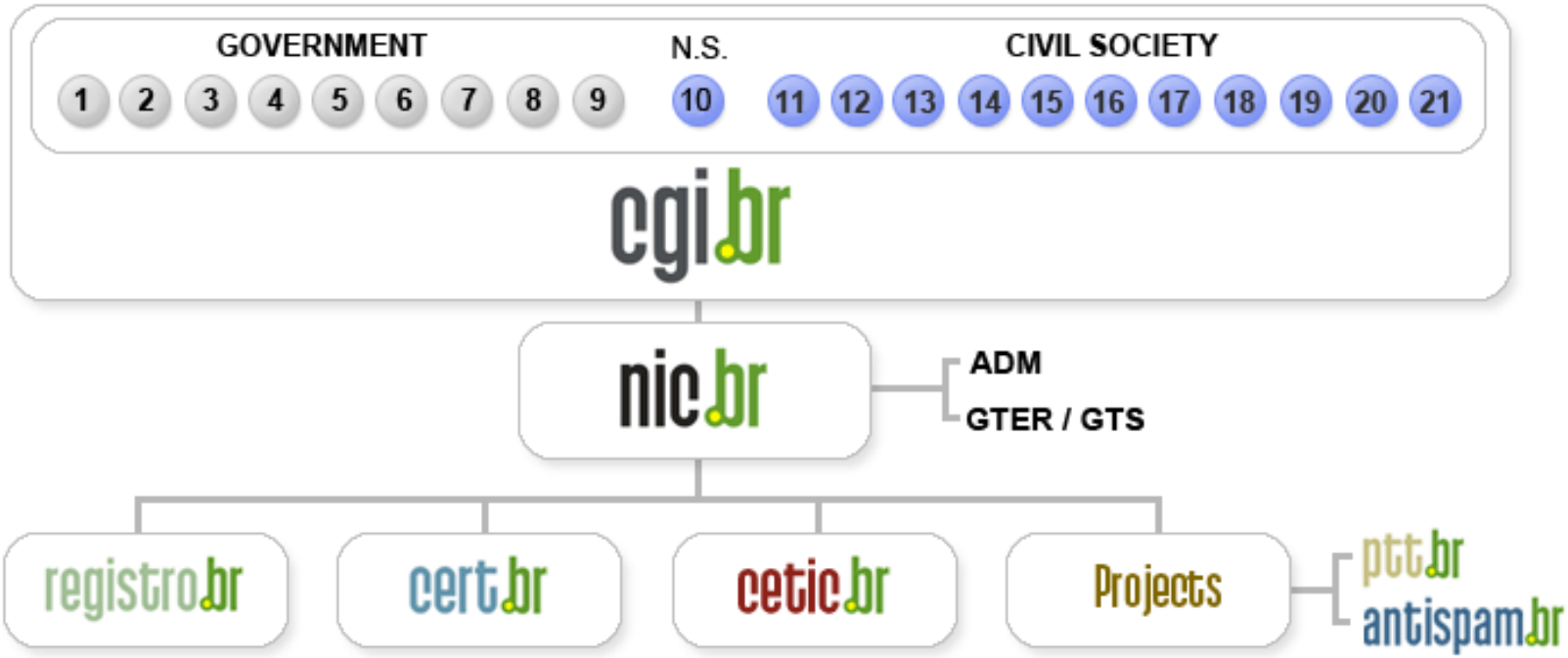
CGI.br – Brazilian Internet Steering Committee

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



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

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

Agenda

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

Motivation

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

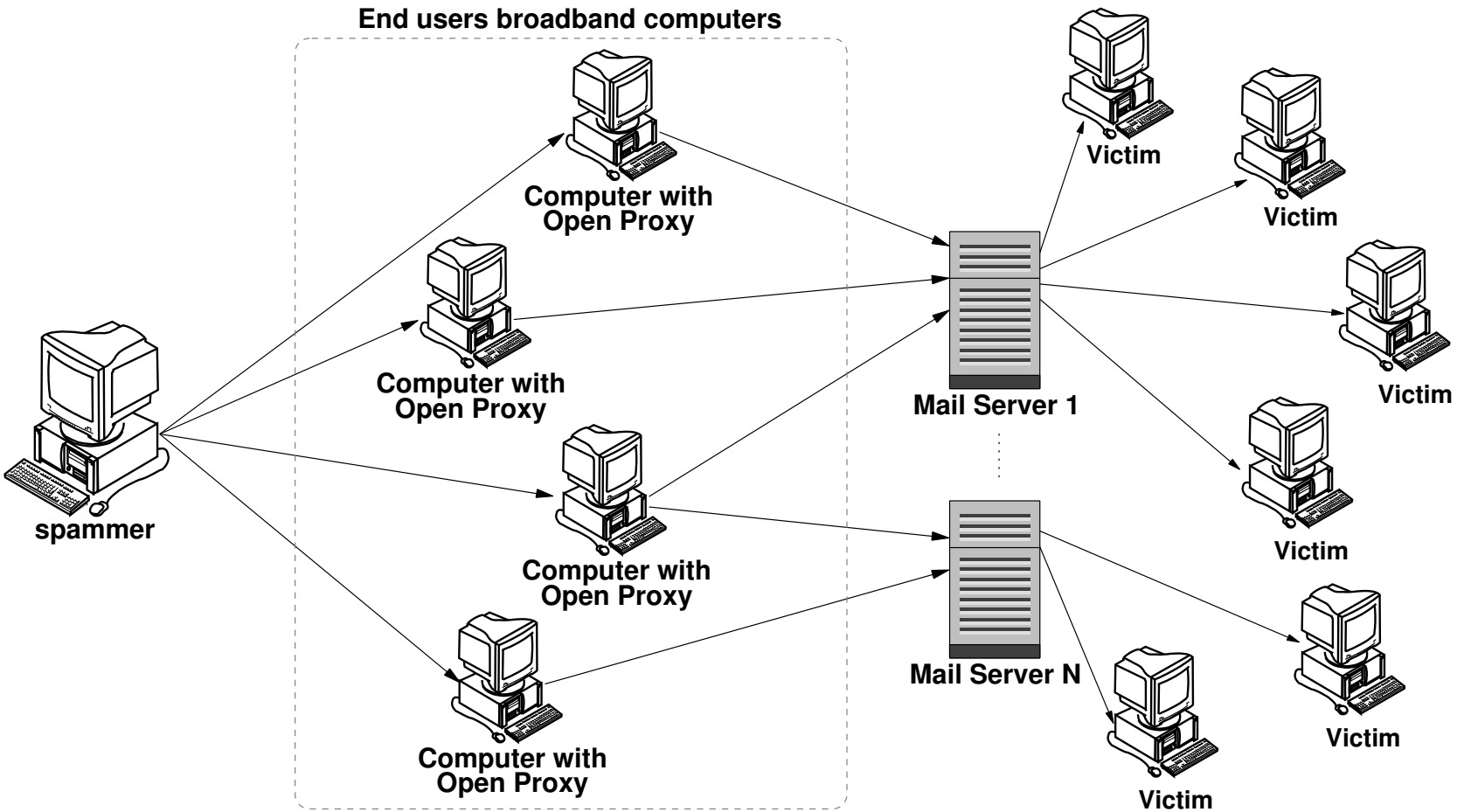
Motivation (2)

- Brazil is usually listed as a big source of spam
  - is it really the source or is it just being abused by others?
- **Need to better understand the problem and have more data about it**
  - generate metrics that can help the formulation of policies

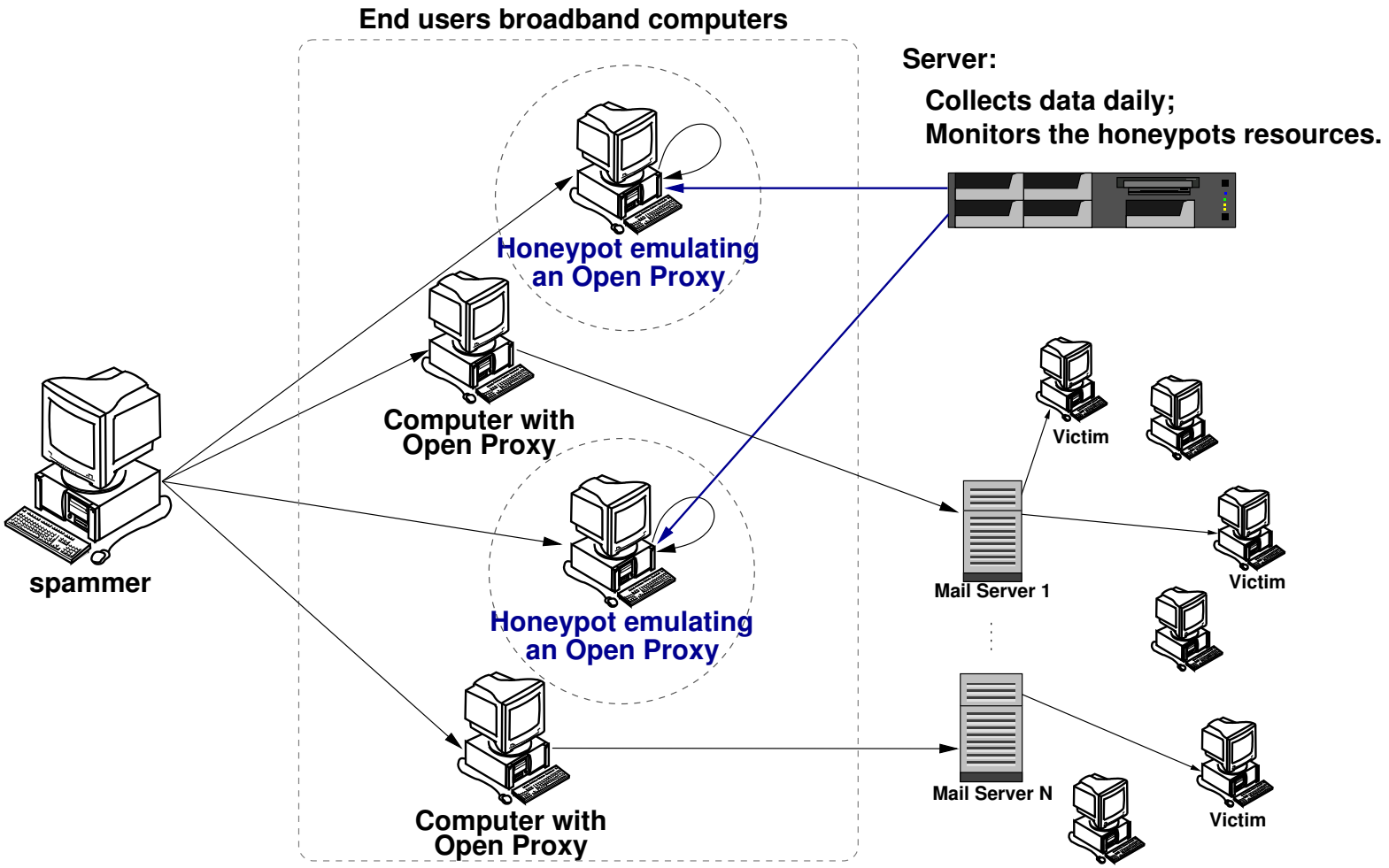
The SpamPots Project

- 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 one year
  - 5 broadband providers, 1 residential and 1 business connection each
- Measure the abuse of end-user machines to send spam

Open Proxy Abuse Scenario



Architecture



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

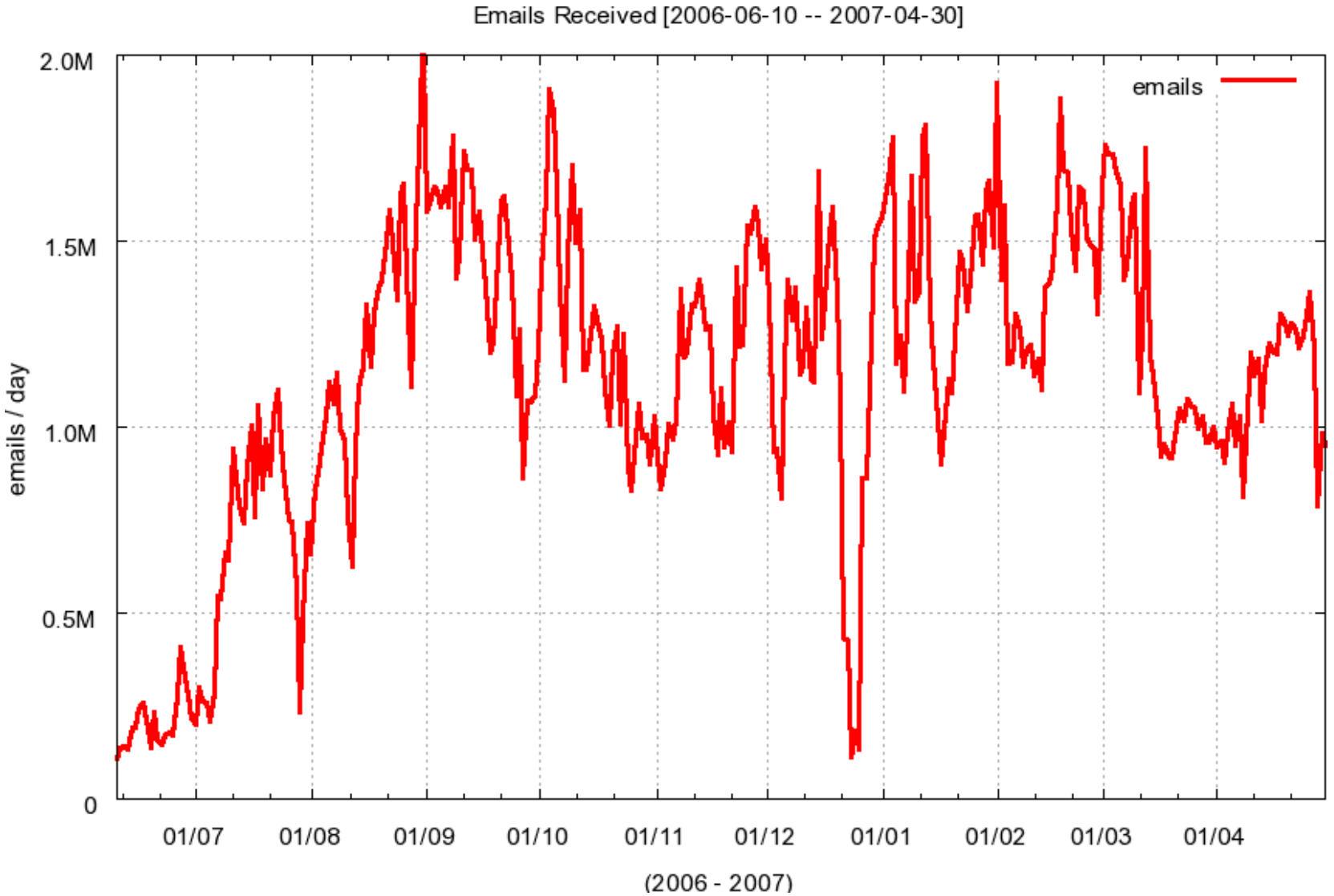
- Collects and stores data from honeypots
  - initiates transfers through ssh connections
  - uses rsync over ssh to copy spam from the honeypots
- Performs status checks in all honeypots
  - daemons, ntp, disk space, load, rsync status
- Web page interface
  - honeypot status
  - emails stats: daily,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

Statistics

Statistics

period	2006-06-10 to 2007-04-30
days	325
emails	$\approx$ 370M
recipients	$\approx$ 3.2G
avg. recpts/email	$\approx$ 8.9
unique IPs	$\approx$ 160K
unique ASNs	2813
unique CCs	157

Spams captured / day

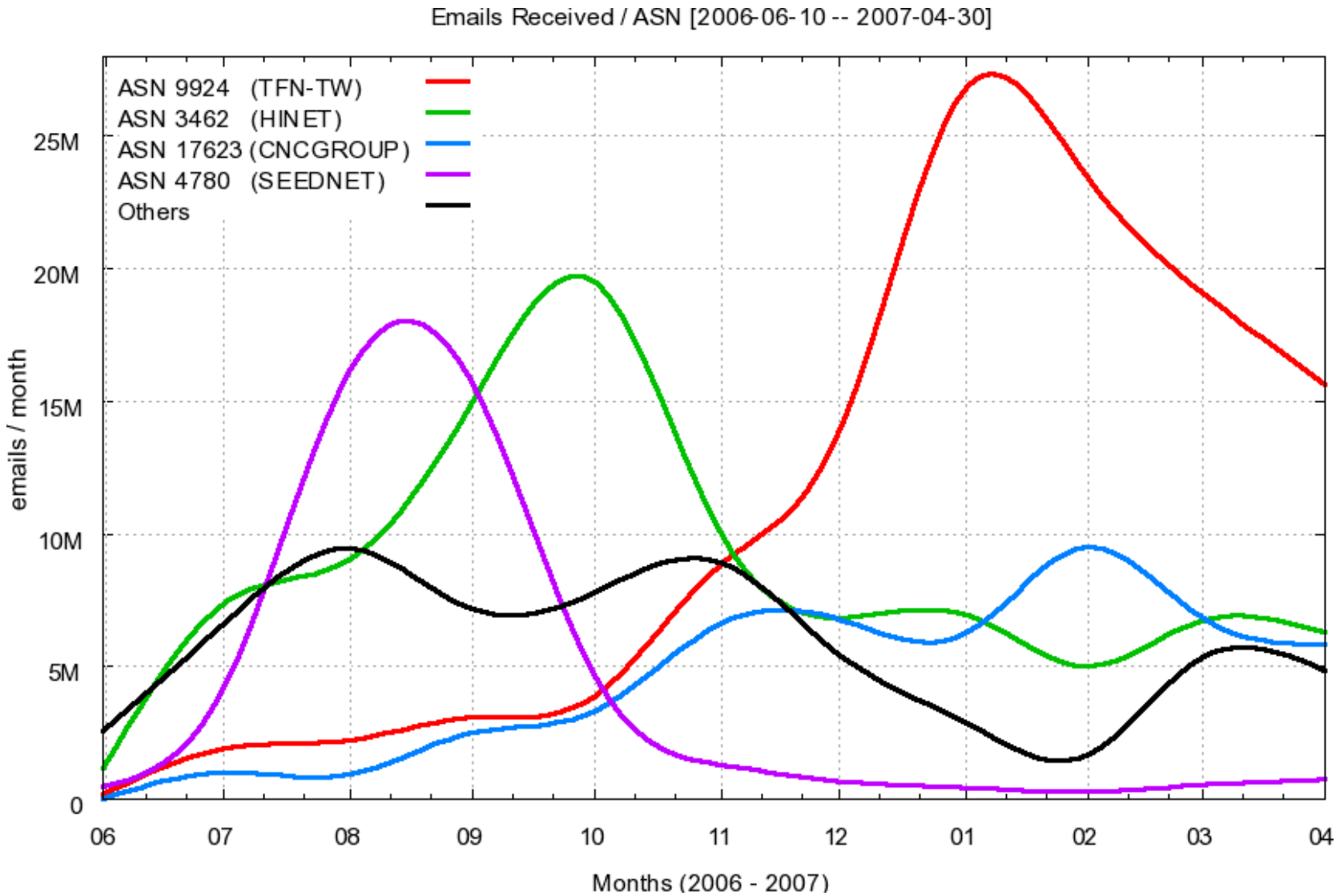


Top ASNs sending spam

- Top 10 emails/ASN:

#	ASN	ASN Name	%
01	9924	TFN-TW Taiwan Fixed Network	32.08
02	3462	HINET Data Communication	25.41
03	17623	CNCGROUP-SZ CNCGROUP	13.37
04	4780	SEEDNET Digital United	12.21
05	9919	NCIC-TW	02.25
06	4837	CHINA169-BACKBONE CNCGROUP	01.69
07	7271	LOOKAS - Look Communications	01.51
08	7482	APOL-AS Asia Pacific On-line	00.98
09	18182	SONET-TW Sony Network Taiwan	00.96
10	18429	EXTRALAN-TW	00.89

Top ASNs sending spam (2)

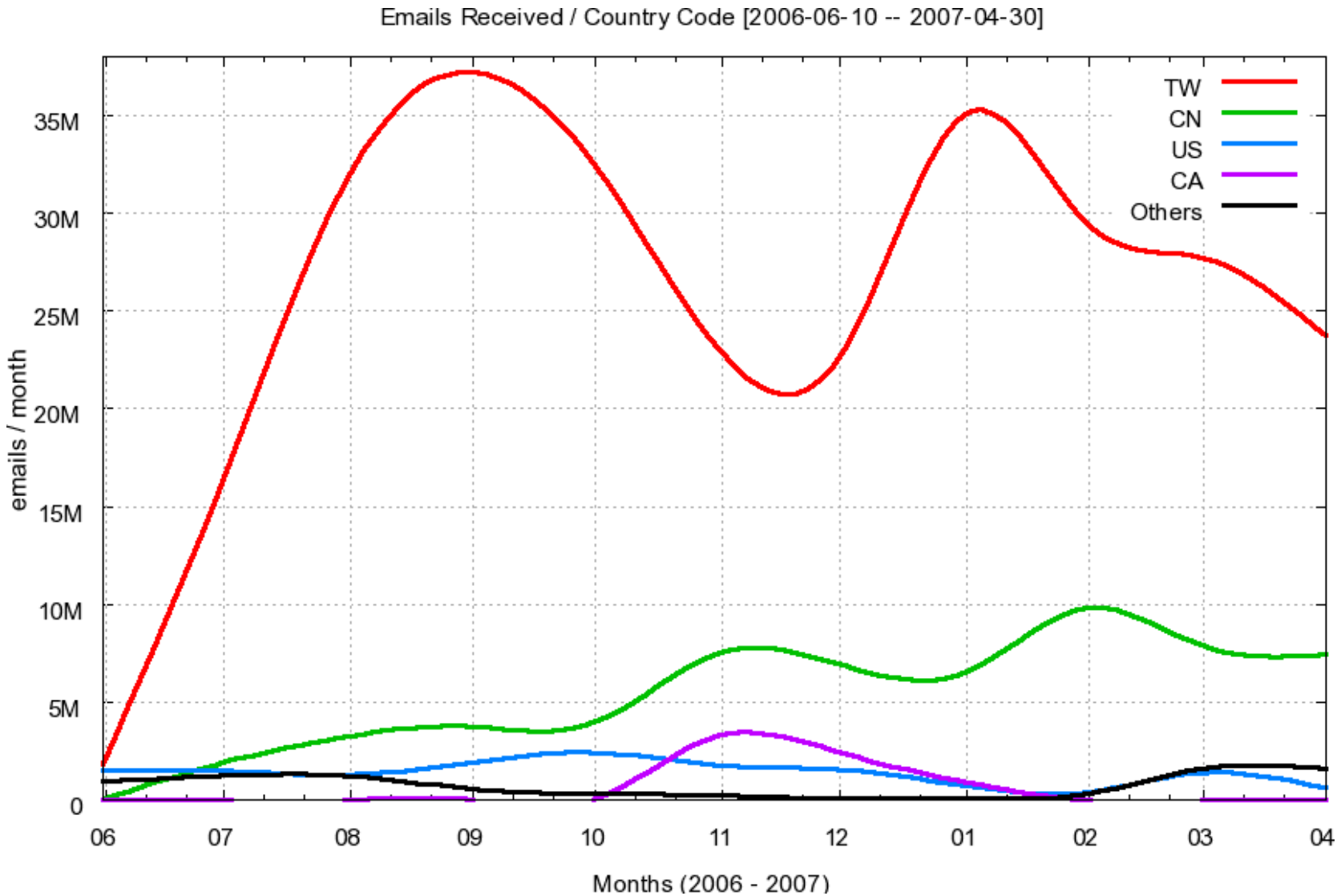


Top CCs sending spam

- Top 10 emails/CC:

#	emails	CC	%
01	281601310	TW	76.05
02	58912303	CN	15.91
03	14939973	US	04.03
04	6677527	CA	01.80
05	1935648	KR	00.52
06	1924341	JP	00.52
07	816072	HK	00.22
08	776245	DE	00.21
09	642446	BR	00.17
10	355622	PA	00.10

Top CCs sending spam (2)

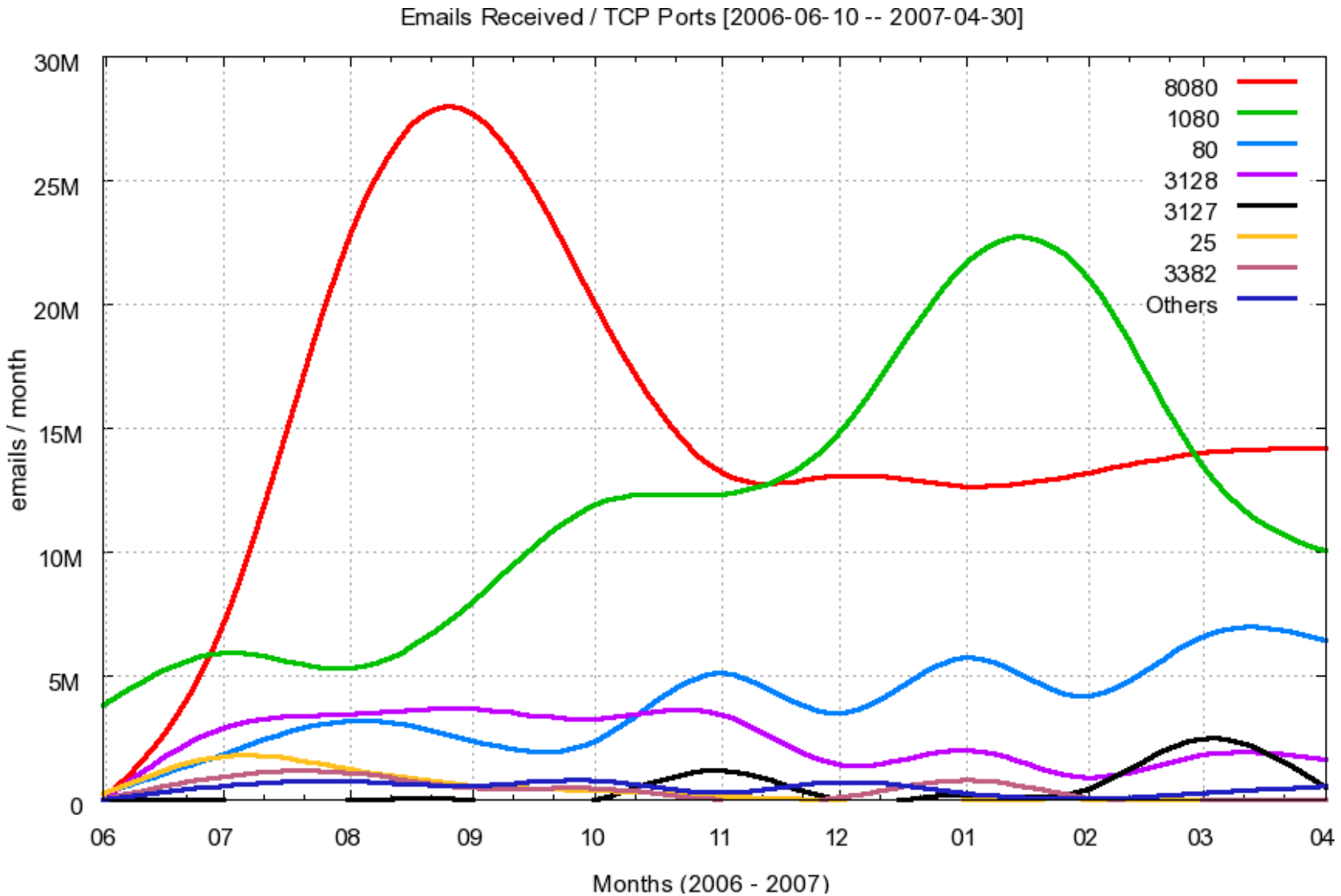


Top TCP ports used

- TCP ports used:

#	TCP Port	protocol	used by	%
01	8080	HTTP	alt http	42.68
02	1080	SOCKS	socks	34.66
03	80	HTTP	http	11.22
04	3128	HTTP	Squid	06.61
05	3127	SOCKS	MyDoom	01.28
06	25	SMTP	smtp	01.18
07	3382	HTTP	Sobig.f	01.07
08	81	HTTP	alt http	00.51
09	8000	HTTP	alt http	00.37
10	6588	HTTP	AnalogX	00.27
11	4480	HTTP	Proxy+	00.15

Top TCP ports used (2)



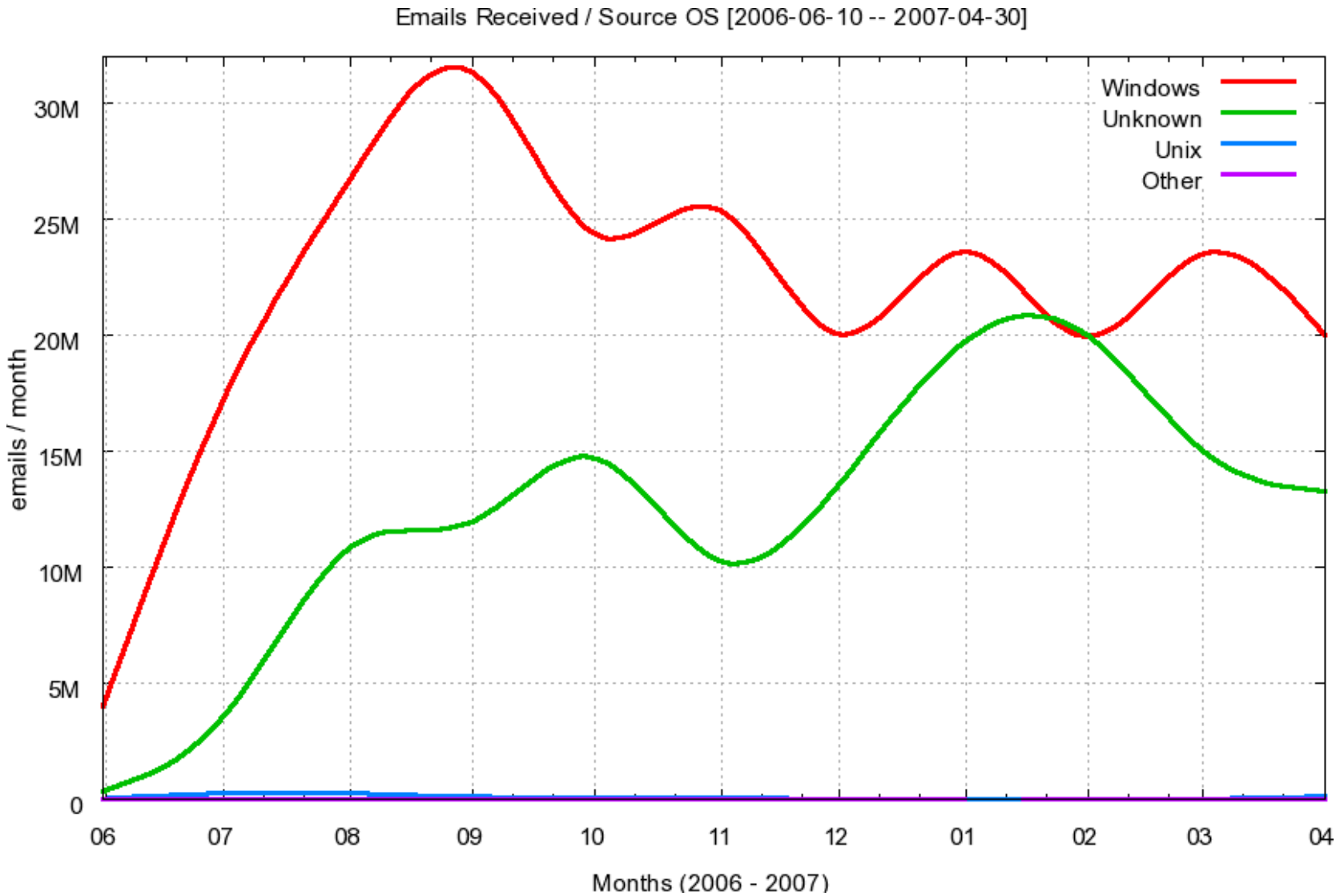
Top Source OS used

- `tcpdump/pf.os` used to fingerprint the OS of hosts originating IPv4 TCP connections

#	emails	Src OS	%
01	235990984	Windows	63.74
02	133276691	Unknown	36.00
03	945642	Unix	00.26
04	50096	Other	00.01

http://www.openbsd.org/cgi-bin/man.cgi?query=pf.os

Top Source OS used (2)



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/