Incident Response and Early Warning Initiatives in Brazil

Marcelo H. P. C. Chaves
mhp@cert.br

Computer Emergency Response Team Brazil – CERT.br
http://www.cert.br/
Brazilian Internet Steering Committee
http://www.cgi.br/

Overview

- CERT.br
  - The CERT.br Sponsor
  - Mission, constituency and services
  - Initiatives
- Early Warning
  - Motivation
  - The honeypots network
  - public and private statistics and use in incident response
  - Advantages, disadvantages and future work

CGI.br / CERT.br

CGI.br – The CERT.br Sponsor

The Brazilian Internet Steering Committee (CGI.br)

- created by the Interministerial Ordinance Nº 147, of May 31st 1995
- altered by the Presidential Decree Nº 4,829, of September 3rd 2003

It is a multistakeholder organization composed of:

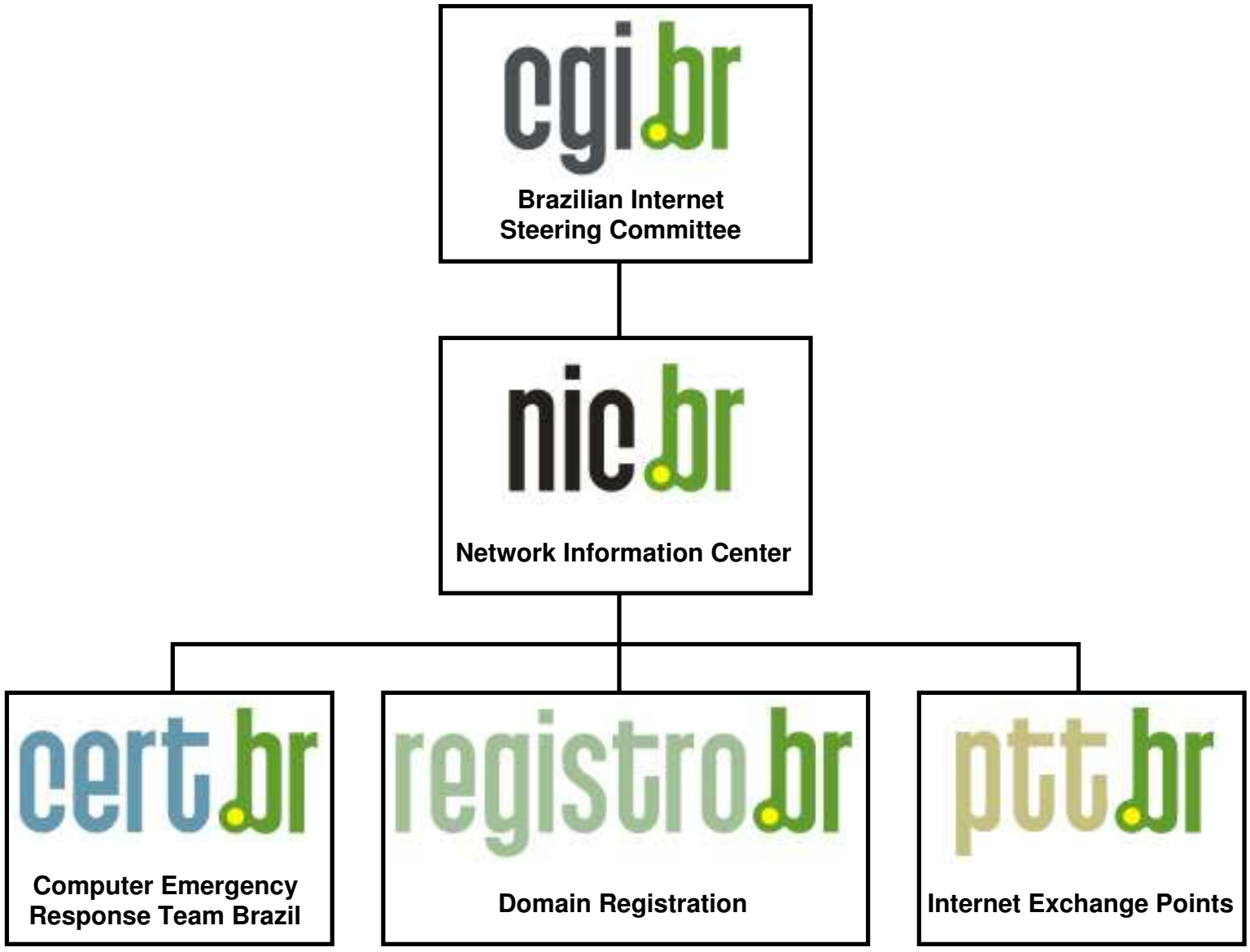
sector	representatives	number
Federal Government	**Ministries of Science and Technology, Communications, Defense, Industry, etc, and Telcos Regulatory Agency (ANATEL)**	**9**
Corporate sector	**Industry, Telcos, ISPs, users**	**4**
NGO´s	**Non–profit organizations, etc**	**4**
Sci. and Tech. Community	**Academia**	**3**
	Internet expert	**1**

CGI.br – The CERT.br Sponsor (cont.)

Brazilian Internet Steering Committe's main attributions:

- **to propose policies and procedures related to the regulation of Internet activities;**
- to recommend standards for technical and operational procedures for the Internet in Brazil;
- 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 – The CERT.br Sponsor (cont.)



CERT.br

Mission:

- An organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet.

Constituency:

- Brazil - Internet .br domain and IP addresses assigned to Brazil.

CERT.br (cont.)

Services:

- provide a focal point for reporting incidents related to Brazilian networks;
- provide coordinated support in incident response;
- establish collaborative relationships (law enforcement, service providers, telephone companies, financial sector, etc);
- increase security awareness and help new CSIRTs to establish their activities;

CERT.br is a member of FIRST http://www.first.org/

CERT.br Initiatives

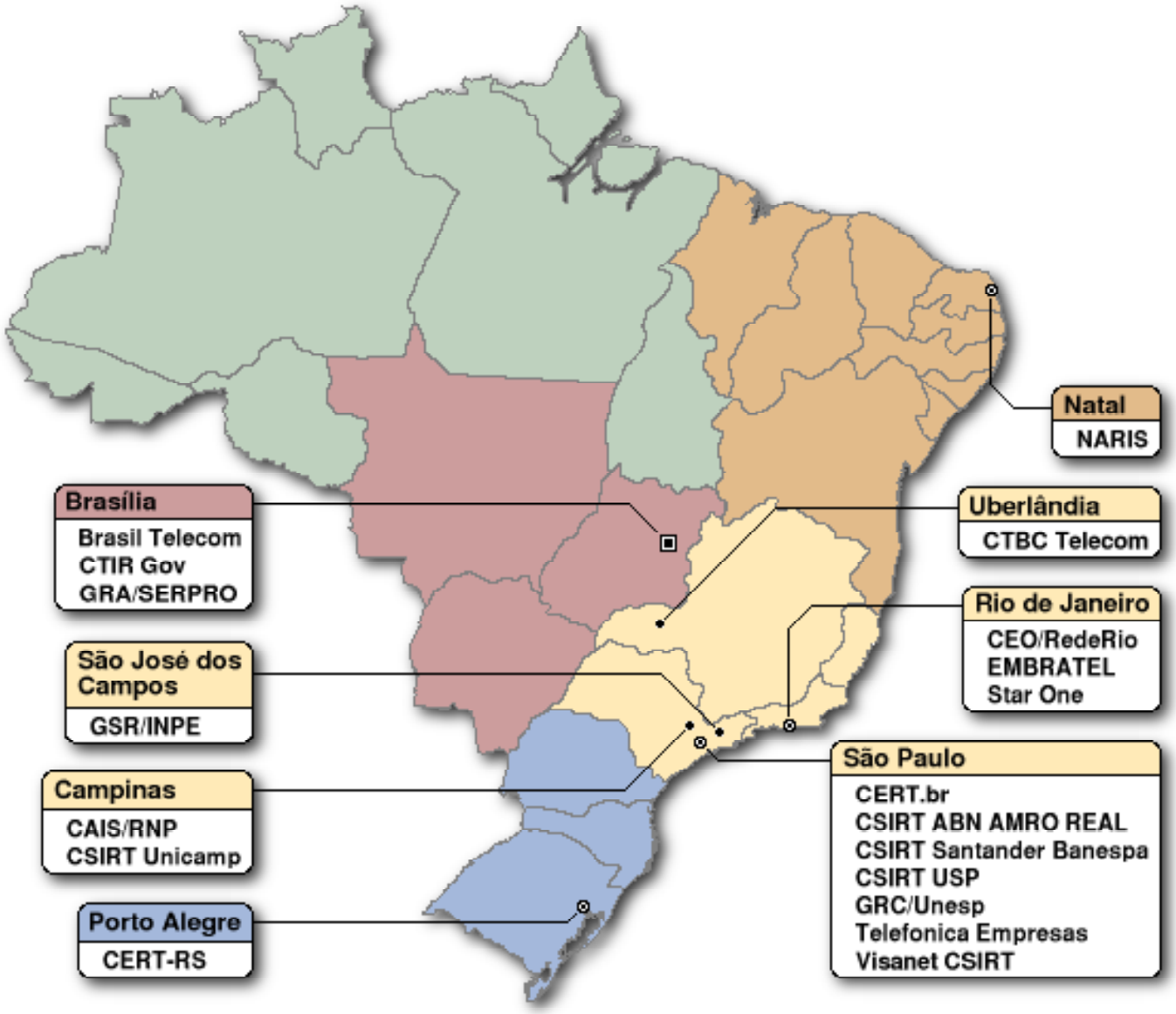
- Produce technical documents in Portuguese
- Maintain statistics (incidents and spam)
- Anti-Phishing Working Group Research Partner
  - detect malware enabled fraud
  - notify hosting sites
  - send samples to 20+ AV vendors
- Honeypots and Honeynets research
  - Honeynet Research Alliance Member
  - Brazilian Honeypots Alliance - Distributed Honeypots Project

CERT.br Initiatives (cont.)

CSIRT Development:

- Training:
  - SEI Partner for 4 CERT®/CC courses
    - Creating a Computer Security Incident Response Team
    - Managing Computer Security Incident Response Teams
    - Fundamentals of Incident Handling
    - Advanced Incident Handling for Technical Staff
  - 140+ people trained
- Help new teams' creation
- Maintain a list of Brazilian CSIRTs

Brazilian CSIRTs



http://www.cert.br/contact-br.html

CGI.br Initiatives

- sponsors 2 meetings/conferences free of charge per year, to the security and network communities (GTS/GTER)
- iNOC-DBA BR – project to stimulate Brazilian networks to join the iNOC-DBA global network
  - 100 IP phones were provided to ASNs
  - 20 IP phones were provided to CSIRTs recognized by CERT.br

iNOC-DBA – global hotline phone system which directly interconnects the Network Operations Centers and Security Incident Response Teams

CGI.br Initiatives (cont.)

Task Force on Spam (CT-Spam)

- to propose a national strategy to fight spam
- to articulate the actions among the different actors
- documents created
  - “Technologies and Policies to Fight Spam”
  - technical analysis of international antispam laws and brazilian proposals of new laws

Early Warning Initiative

Motivation

Have a national early warning capability with the following characteristics:

- Widely distributed across the country
  - in several ASNs and geographical locations
- Based on voluntary work of research partners
- High level of privacy for the members
- Useful for Incident Response

The Honeypots Network

Brazilian Honeypots Alliance –
Distributed Honeypots Project

- Coordination:
  - CERT.br – Computer Emergency Response Team Brazil
    Brazilian Internet Steering Committee
  - CenPRA Research Center
    Ministry of Science and Technology

The Honeypots Network (cont.)

- Technical requirements:
  - secure configuration
  - follow the project's standards (OS, configurations, updates, etc)
  - no data pollution
- Privacy concerns (in a NDA):
  - don't disclose IP/network information
  - don't collect production network traffic
  - don't exchange any information in clear text

The Honeypots Network (cont.)

The architecture:

- low interaction honeypots
  - OpenBSD + Honeyd
  - using a netblock range
  - emulating services (HTTP, SMTP, malwares backdoors, etc)
- a central server
  - collects logs and uploaded malware
  - performs a status check in all honeypots

The Honeypots Network (cont.)

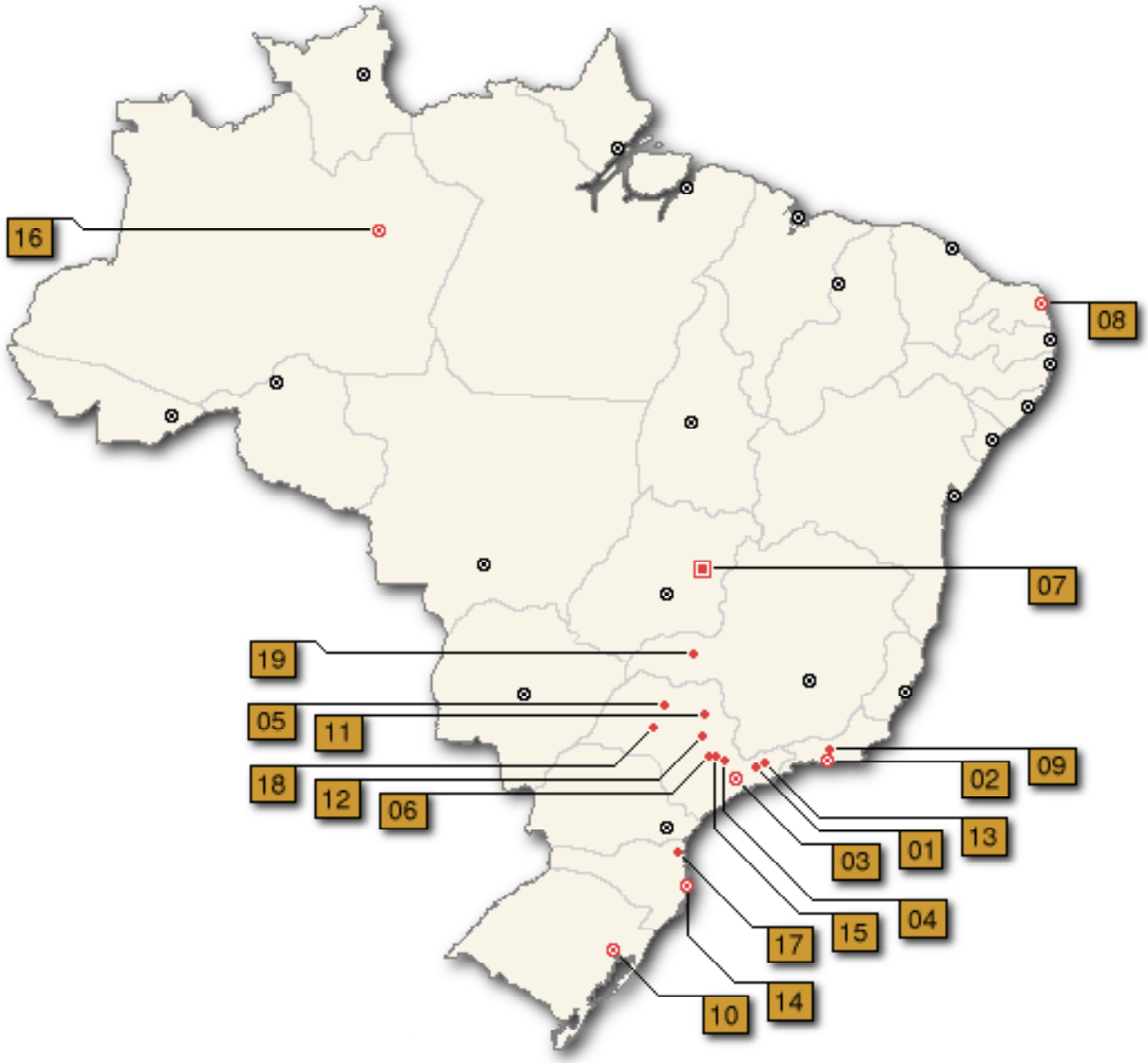
31 research partner's institutions:

- Academia, Government, Industry, Military and Telcos networks
- They provide:
  - hardware and network blocks (usually a /24)
  - maintenance of their own honeypots
- Use the data for intrusion detection purposes
  - less false positives than traditional IDSs
- Several have more than one honeypot

The Honeypots Network (cont.)

#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, USP
04	Campinas	CenPRA, ITAL, HP Brazil, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministry of Justice, TCU, UNB LabRedes
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

The Honeypots Network (cont.)



As of October, 2005

Early Warning

- Private Statistics – summaries including:
  - specific information for each honeypot
  - most active IPs, OSs, ports, protocols and Country Codes
  - correlated activities (ports and IPs)
- Public Statistics:
  - combined daily flows seen in the honeypots
  - most active OSs, TCP/UDP ports and Country Codes (CC)
    - the top ports, OSs and CCs are calculated every day

Early Warning (cont.)

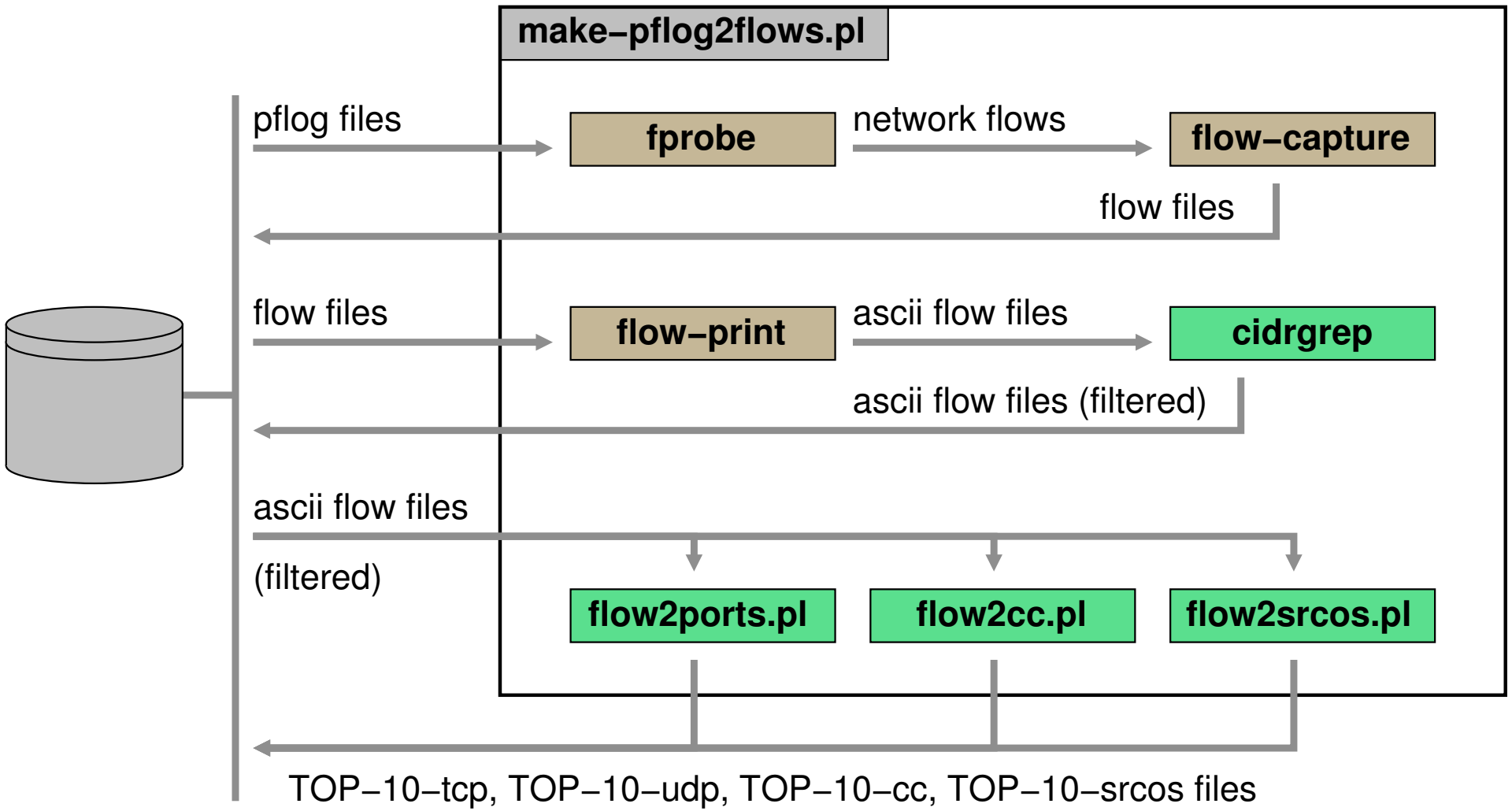
Usefulness:

- observation of trends
  - detect scans for potential new vulnerabilities
- partner institutions are detecting promptly:
  - outbreaks of new worms/bots
  - compromised servers
  - network configuration errors
- collect new signatures and new malware

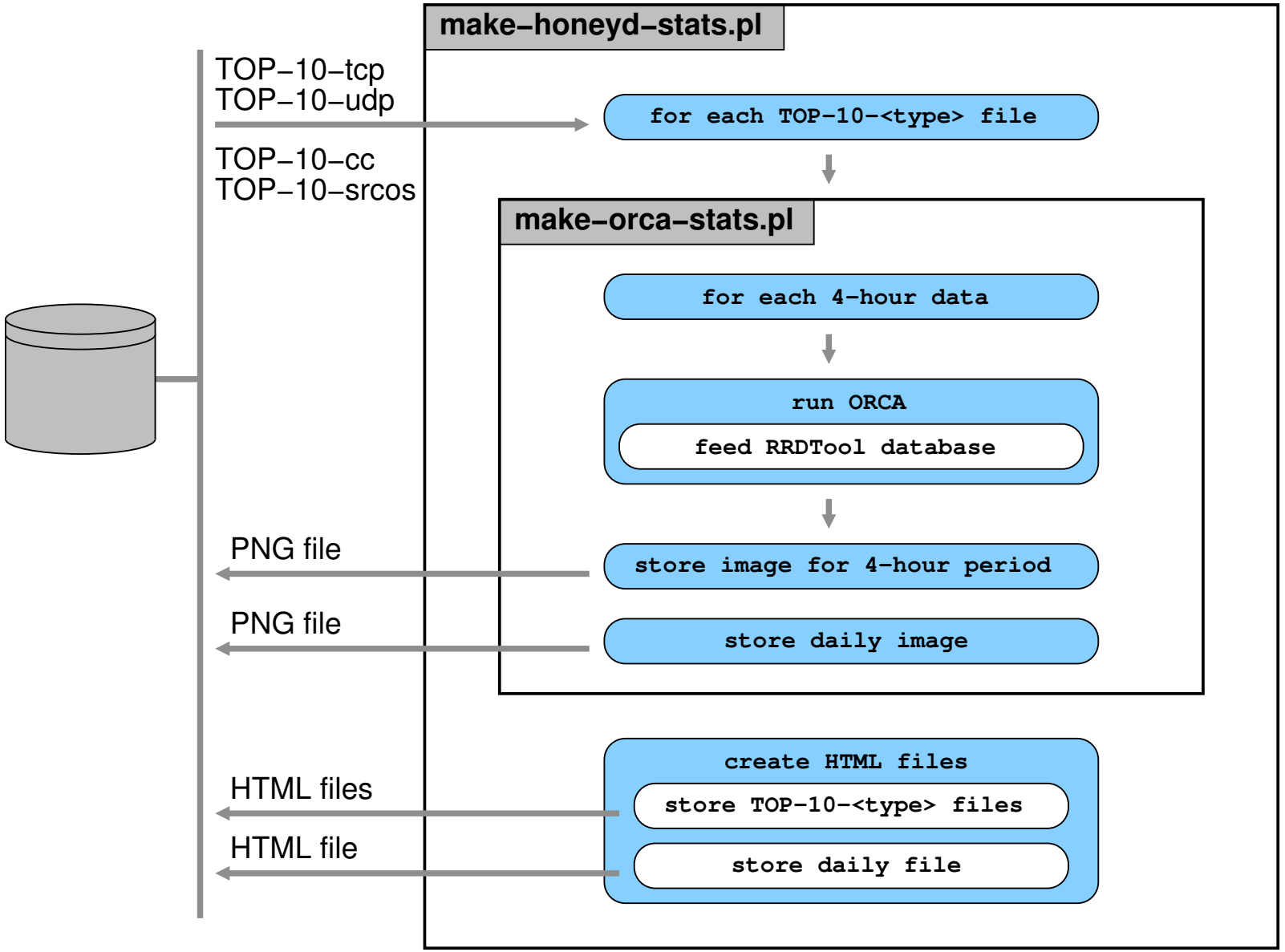
Public Statistics Generation

- convert the raw network data into flow data
- compute the amount of bytes/packets received by each port (or OS or CC)
- select the top 10 to plot
  - the remaining will be displayed as “others”
- use RRDtool and ORCA to generate the flows’ graphics
  - stack area graphics
  - logarithmic scale

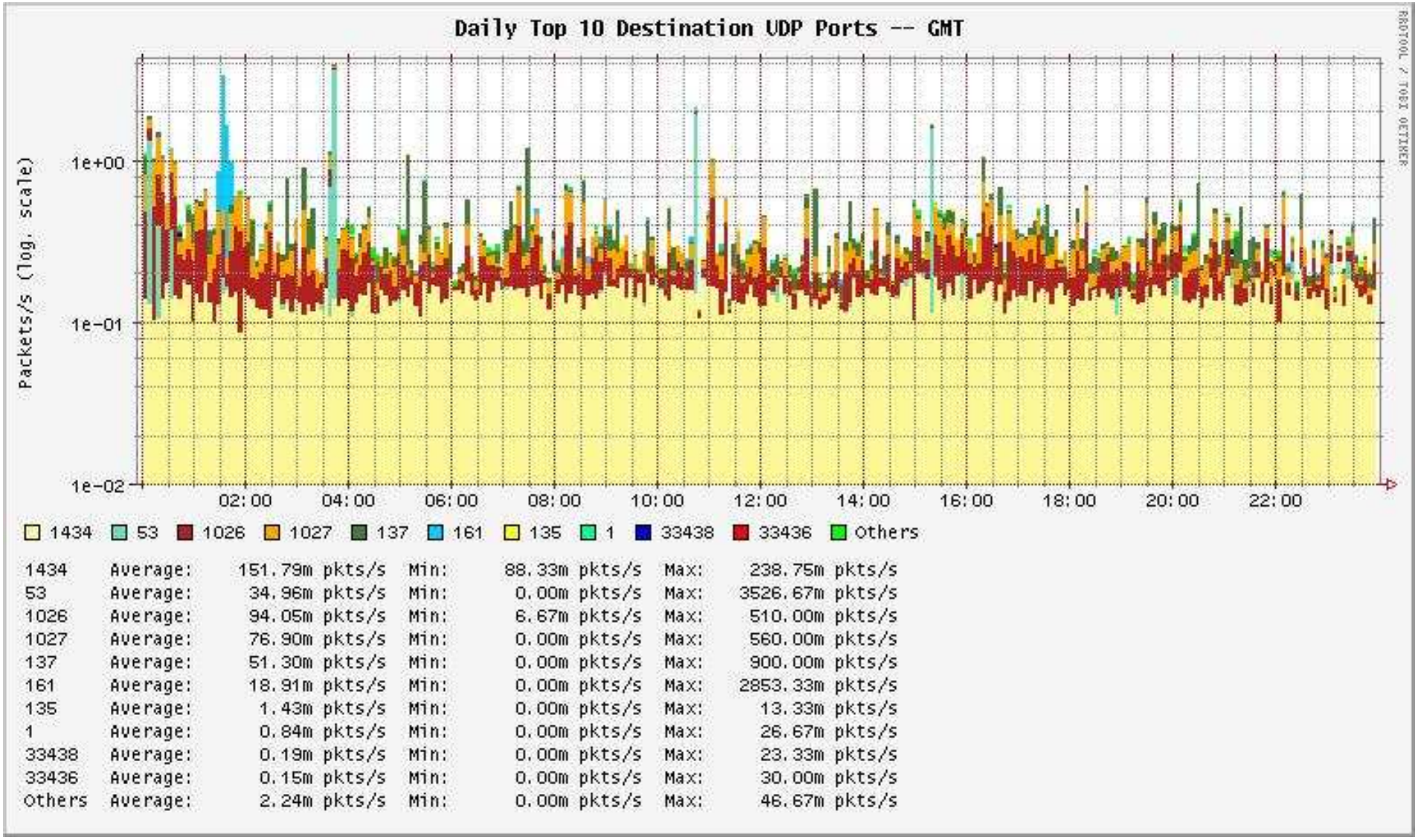
Public Statistics Generation (cont.)



Public Statistics Generation (cont.)



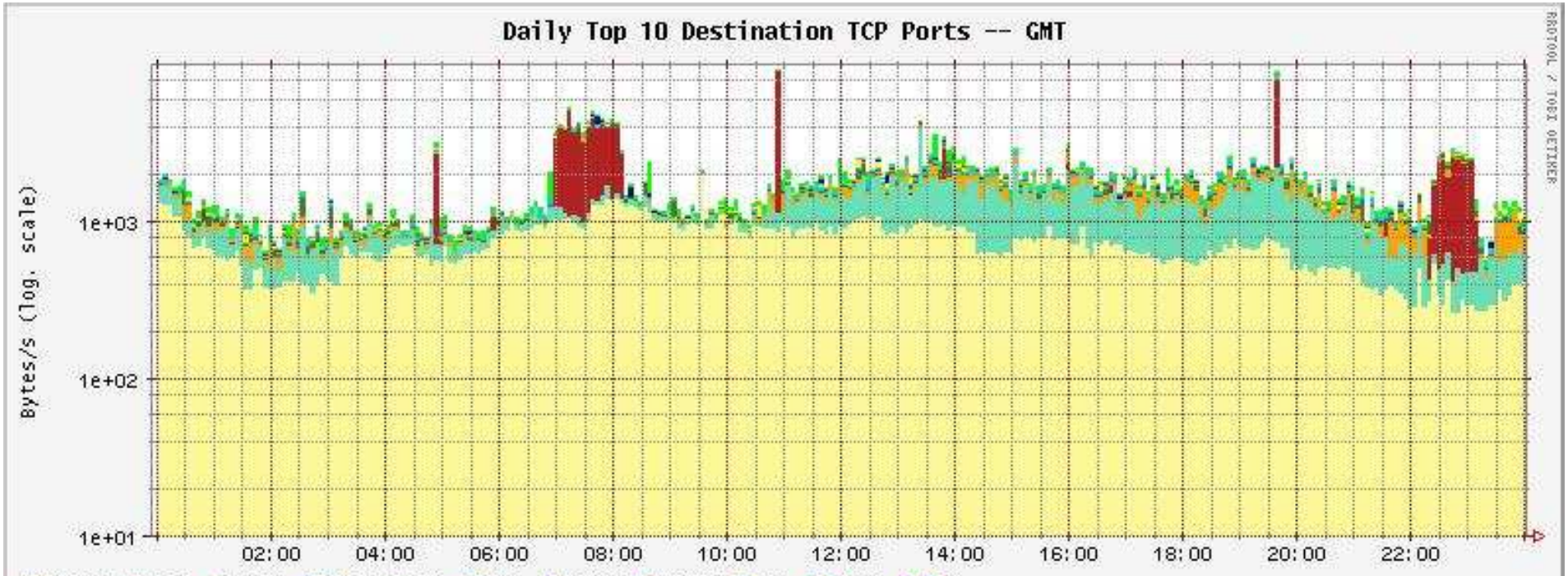
Public Statistics – Top UDP Ports



1434	Average:	151.79m pkts/s	Min:	88.33m pkts/s	Max:	238.75m pkts/s
53	Average:	34.96m pkts/s	Min:	0.00m pkts/s	Max:	3526.67m pkts/s
1026	Average:	94.05m pkts/s	Min:	6.67m pkts/s	Max:	510.00m pkts/s
1027	Average:	76.90m pkts/s	Min:	0.00m pkts/s	Max:	560.00m pkts/s
137	Average:	51.30m pkts/s	Min:	0.00m pkts/s	Max:	900.00m pkts/s
161	Average:	18.91m pkts/s	Min:	0.00m pkts/s	Max:	2853.33m pkts/s
135	Average:	1.43m pkts/s	Min:	0.00m pkts/s	Max:	13.33m pkts/s
1	Average:	0.84m pkts/s	Min:	0.00m pkts/s	Max:	26.67m pkts/s
33438	Average:	0.19m pkts/s	Min:	0.00m pkts/s	Max:	23.33m pkts/s
33436	Average:	0.15m pkts/s	Min:	0.00m pkts/s	Max:	30.00m pkts/s
Others	Average:	2.24m pkts/s	Min:	0.00m pkts/s	Max:	46.67m pkts/s

September 17, 2005

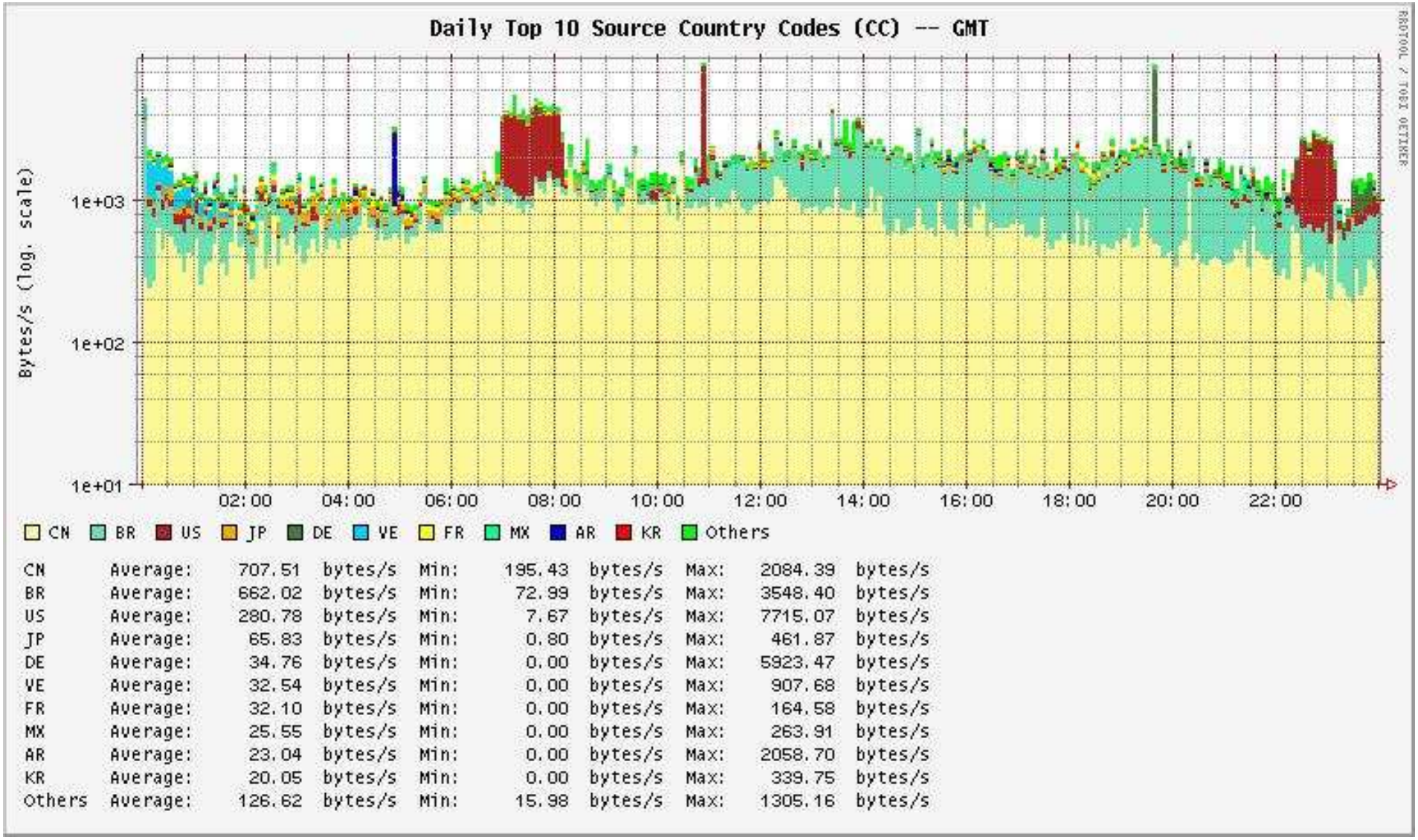
Public Statistics – Top TCP Ports



1433	Average:	730.92	bytes/s	Min:	263.89	bytes/s	Max:	1968.32 bytes/s
445	Average:	451.76	bytes/s	Min:	18.94	bytes/s	Max:	2853.51 bytes/s
3127	Average:	259.07	bytes/s	Min:	0.00	bytes/s	Max:	7684.20 bytes/s
135	Average:	124.78	bytes/s	Min:	5.99	bytes/s	Max:	871.34 bytes/s
80	Average:	55.77	bytes/s	Min:	4.01	bytes/s	Max:	389.67 bytes/s
139	Average:	50.66	bytes/s	Min:	5.28	bytes/s	Max:	249.49 bytes/s
4899	Average:	19.99	bytes/s	Min:	0.00	bytes/s	Max:	232.58 bytes/s
1025	Average:	10.42	bytes/s	Min:	0.48	bytes/s	Max:	44.41 bytes/s
22	Average:	8.75	bytes/s	Min:	0.00	bytes/s	Max:	520.95 bytes/s
5000	Average:	8.11	bytes/s	Min:	0.00	bytes/s	Max:	42.60 bytes/s
Others	Average:	58.04	bytes/s	Min:	6.91	bytes/s	Max:	970.72 bytes/s

September 21, 2005

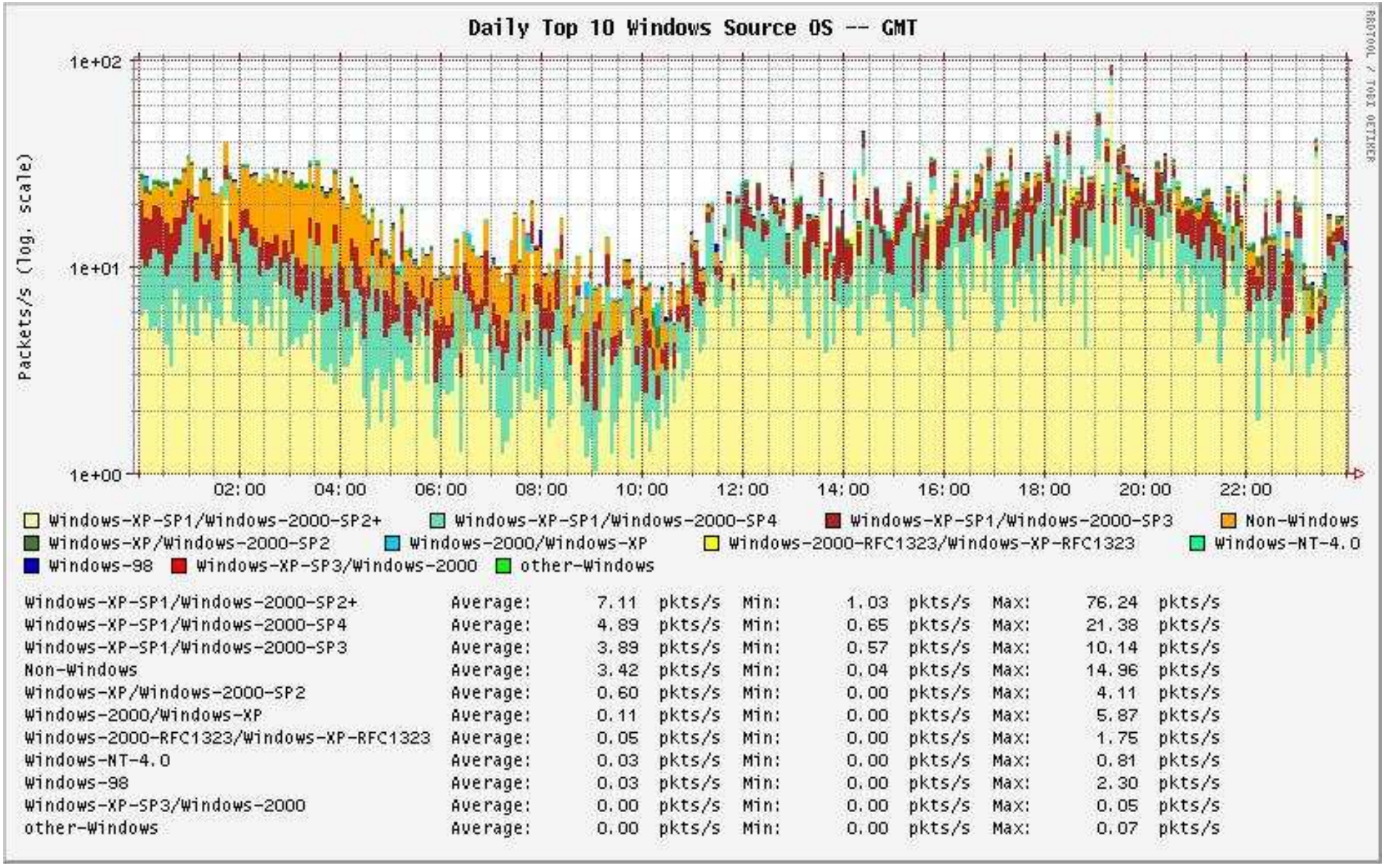
Public Statistics – Top Country Codes



CN	Average:	707.51	bytes/s	Min:	195.43	bytes/s	Max:	2084.39 bytes/s
BR	Average:	662.02	bytes/s	Min:	72.99	bytes/s	Max:	3548.40 bytes/s
US	Average:	280.78	bytes/s	Min:	7.67	bytes/s	Max:	7715.07 bytes/s
JP	Average:	65.83	bytes/s	Min:	0.80	bytes/s	Max:	461.87 bytes/s
DE	Average:	34.76	bytes/s	Min:	0.00	bytes/s	Max:	5923.47 bytes/s
VE	Average:	32.54	bytes/s	Min:	0.00	bytes/s	Max:	907.68 bytes/s
FR	Average:	32.10	bytes/s	Min:	0.00	bytes/s	Max:	164.58 bytes/s
MX	Average:	25.55	bytes/s	Min:	0.00	bytes/s	Max:	263.91 bytes/s
AR	Average:	23.04	bytes/s	Min:	0.00	bytes/s	Max:	2058.70 bytes/s
KR	Average:	20.05	bytes/s	Min:	0.00	bytes/s	Max:	339.75 bytes/s
Others	Average:	126.62	bytes/s	Min:	15.98	bytes/s	Max:	1305.16 bytes/s

September 21, 2005

Public Statistics – Top Source OS



Windows-XP-SP1/Windows-2000-SP2+	Average:	7.11	pkts/s	Min:	1.03	pkts/s	Max:	76.24 pkts/s
Windows-XP-SP1/Windows-2000-SP4	Average:	4.89	pkts/s	Min:	0.65	pkts/s	Max:	21.38 pkts/s
Windows-XP-SP1/Windows-2000-SP3	Average:	3.89	pkts/s	Min:	0.57	pkts/s	Max:	10.14 pkts/s
Non-Windows	Average:	3.42	pkts/s	Min:	0.04	pkts/s	Max:	14.96 pkts/s
Windows-XP/Windows-2000-SP2	Average:	0.60	pkts/s	Min:	0.00	pkts/s	Max:	4.11 pkts/s
Windows-2000/Windows-XP	Average:	0.11	pkts/s	Min:	0.00	pkts/s	Max:	5.87 pkts/s
Windows-2000-RFC1323/Windows-XP-RFC1323	Average:	0.05	pkts/s	Min:	0.00	pkts/s	Max:	1.75 pkts/s
Windows-NT-4.0	Average:	0.03	pkts/s	Min:	0.00	pkts/s	Max:	0.81 pkts/s
Windows-98	Average:	0.03	pkts/s	Min:	0.00	pkts/s	Max:	2.30 pkts/s
Windows-XP-SP3/Windows-2000	Average:	0.00	pkts/s	Min:	0.00	pkts/s	Max:	0.05 pkts/s
other-Windows	Average:	0.00	pkts/s	Min:	0.00	pkts/s	Max:	0.07 pkts/s

Incident Response

- Identify signatures of well known malicious/abusive activities
  - worms, bots, scans, spam and other malware
- Notify the responsible networks of the Brazilian IPs
  - with recovery tips
- Donate sanitized data of non-Brazilian IPs to other CSIRTs (e.g. Team Cymru)

Architecture advantages

- Few false positives
- Ability to collect malware samples
  - specific listeners: mydoom, kuang, subseven, etc.
- Ability to implement spam traps
- Permits the members expertise's improvement in several areas:
  - honeypots, intrusion detection, PGP, firewalls, OS hardening

Architecture disadvantages

- It's more difficult to maintain
- Usually don't catch attacks targeted to production networks
- Need the partners cooperation to maintain and update the honeypots

Future Work

- Continuously expand the network
  - 4 new partners in installation phase
  - 17 partner candidates
- Have more frequent private summaries
- Provide monthy, weekly, and hourly public statistics
- Increase data donation to trusted parties

Related Links

- This presentation
  http://www.cert.br/docs/palestras/
- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/
- Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/
- Brazilian Honeypots Alliance
  Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/
- Brazilian Honeypots Alliance Statistics
  http://www.honeypots-alliance.org.br/stats/
- The Honeynet Research Alliance
  http://project.honeynet.org/alliance/