Incident Response Initiatives in Brazil

Klaus Steding-Jessen
jessen@cert.br

Computer Emergency Response Team Brazil – CERT.br
http://www.cert.br/

Brazilian Internet Steering Committee
http://www.cgi.br/

Overview

- Incident Response
  - CERT.br
  - History
  - Initiatives
  - Brazilian CSIRTs
  - Early Warning

CERT.br

Mission:

- A 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 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 Sponsor

The Brazilian Internet Steering Committee (CGI.br)

- Multilateral Committee created in 1995
  - 10 members from the government, including: Ministries of Science and Technology, Communications, Defense, Industry, and the Telecommunications Regulatory Agency (Anatel)
  - 11 members from the civil society and private sector, including: industry, telcos, ISPs, academia and third sector

CERT.br Sponsor (cont.)

Brazilian Internet Steering Committe's main attributions are:

- to foment the development of Internet services;
- to recommend technical standards and procedures for the Brazilian Internet;
- to coordinate the attribution of IP addresses and the registration of domain names;
- to collect, organize and disseminate information to the Brazilian Internet community.

How CERT.br was created

- August/1996: CGI.br released the document: "Towards the Creation of a Security Coordination Center in the Brazilian Internet."
  - to be a neutral organization
  - to act as a focal point for security incidents in Brazil
  - to facilitate information sharing and incident handling
- June/1997: They created NBSO/Brazilian CERT
- May/2005: NBSO changed its name to:
  - CERT.br

    Computer Emergency Response Team Brazil

CERT.br Sponsor (cont.)

CERT.br Initiatives

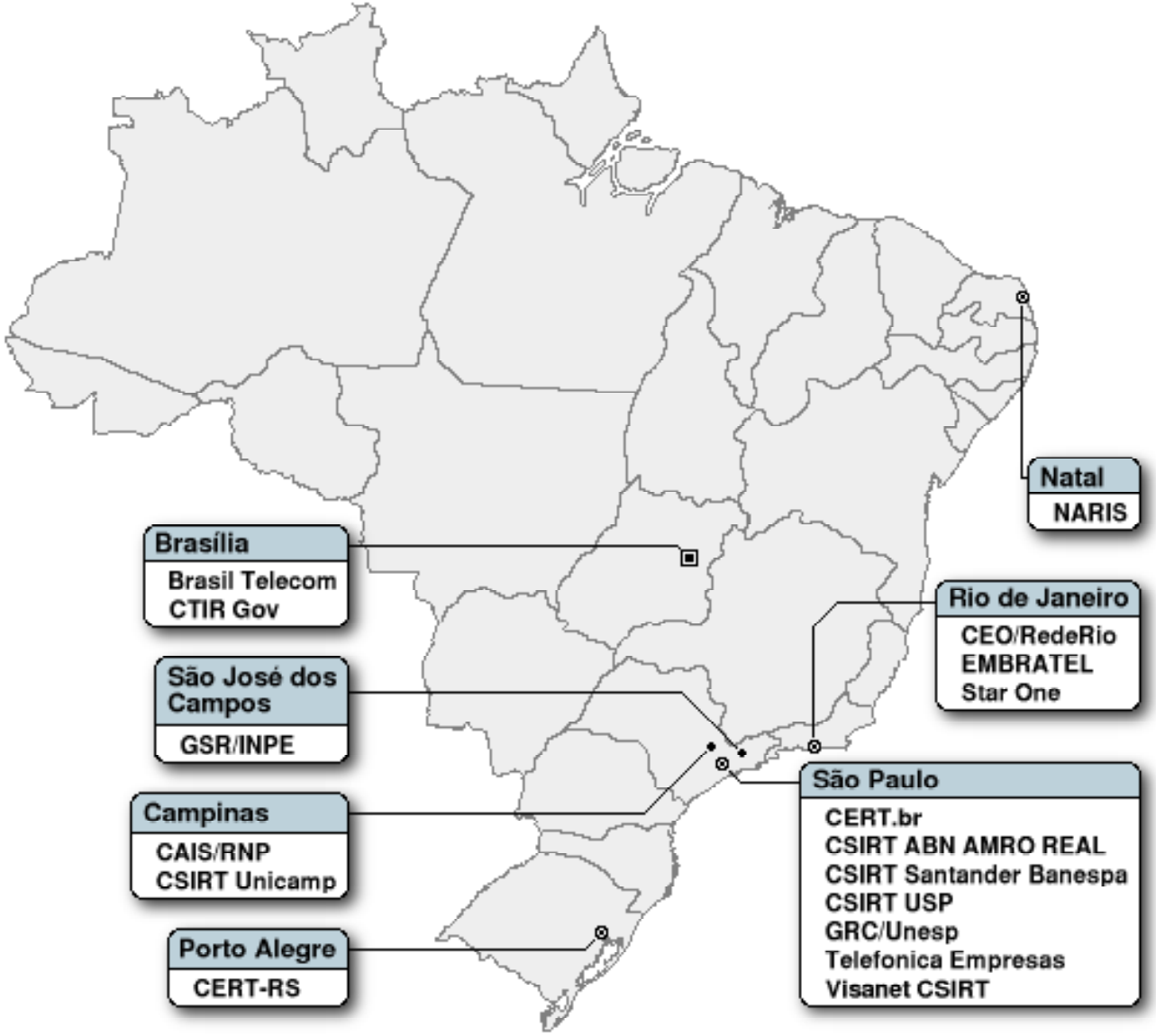
- Produce technical documents in Portuguese
- Maintain statistics (incidents and spam)
- Anti-Phishing Working Group Research Partner
  - detect malware enabled fraud
  - notify hosting sites
  - send samples to 20+ AV vendors
- Honeypots and Honeynets research
  - Honeynet Research Alliance Member
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

CERT.br Initiatives (cont.)

CSIRT Development

- iNOC-DBA – IP phones distributed to all CSIRTs
- Training
  - SEI Partner for 4 CERT®/CC courses
  - 100+ people trained
- Help new teams' creation
- Maintain a list of Brazilian CSIRTs

Brazilian CSIRTs



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

Early Warning

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

A distributed networks of honeypots was chosen

The Honeypots Network

Brazilian Honeypots Alliance –
Distributed Honeypots Project

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

The Honeypots Network (cont.)

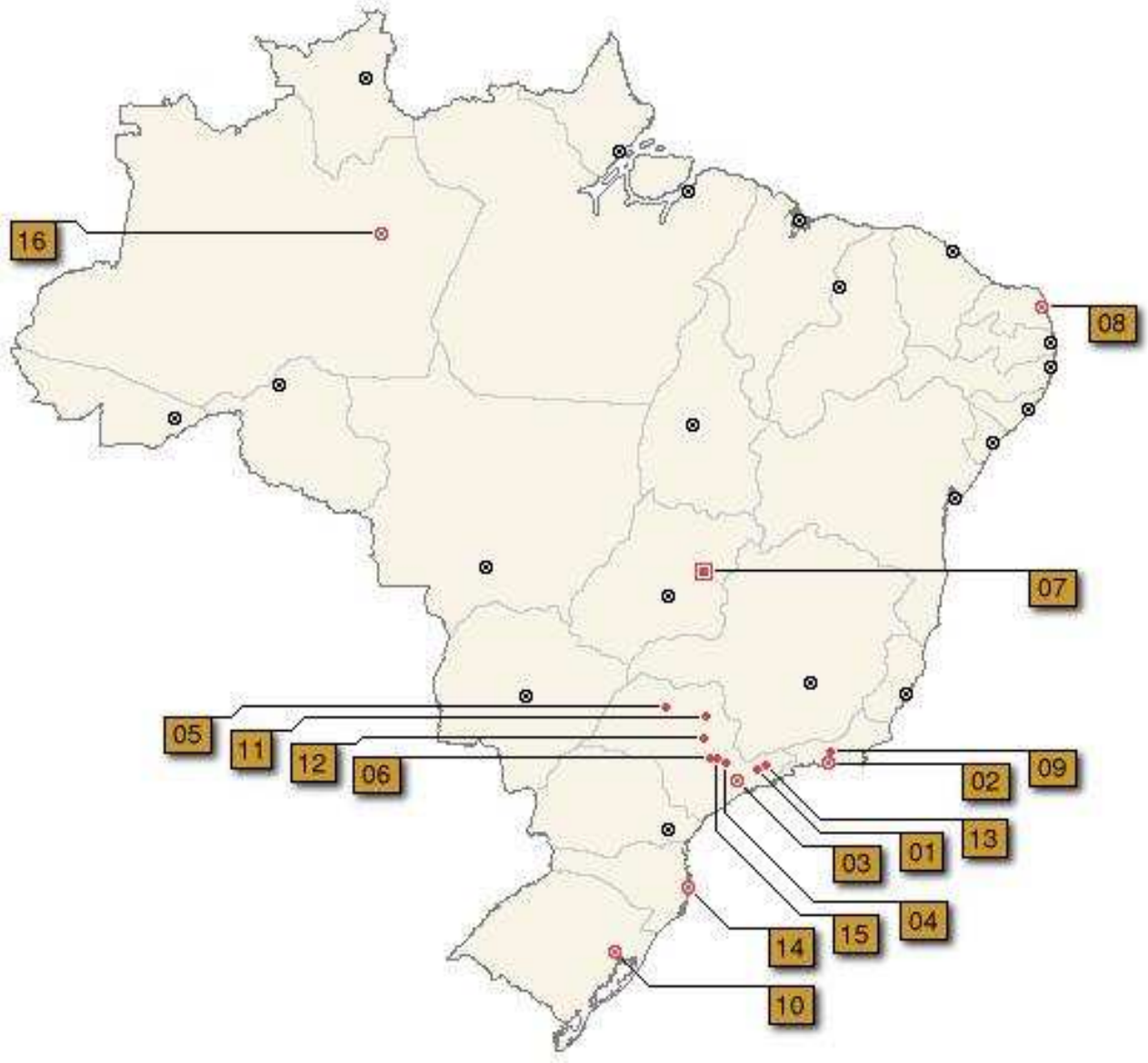
26 research partner's institutions:

- 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, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, USP
04	Campinas	CenPRA, HP Brazil, UNICAMP
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

The Honeypots Network (cont.)



As of June, 2005

Early Warning

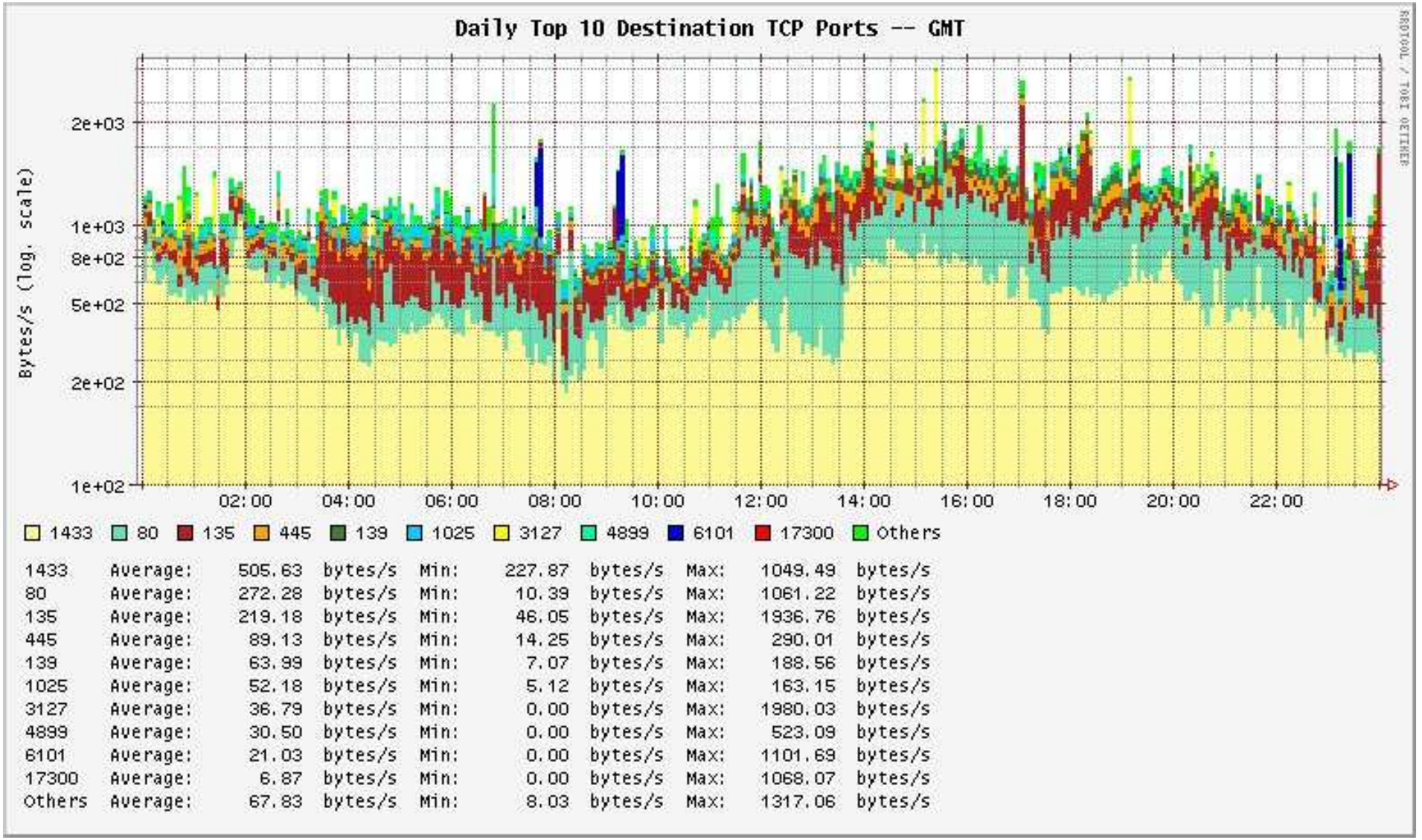
- Private Statistics – summaries including:
  - specific information for each honeypot
  - most active IPs, Operating Systems, ports, protocols and Country Codes
  - correlated activities (ports and IPs)
- Public Statistics
  - combined daily flows seen in the honeypots
  - most active Operating Systems,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

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

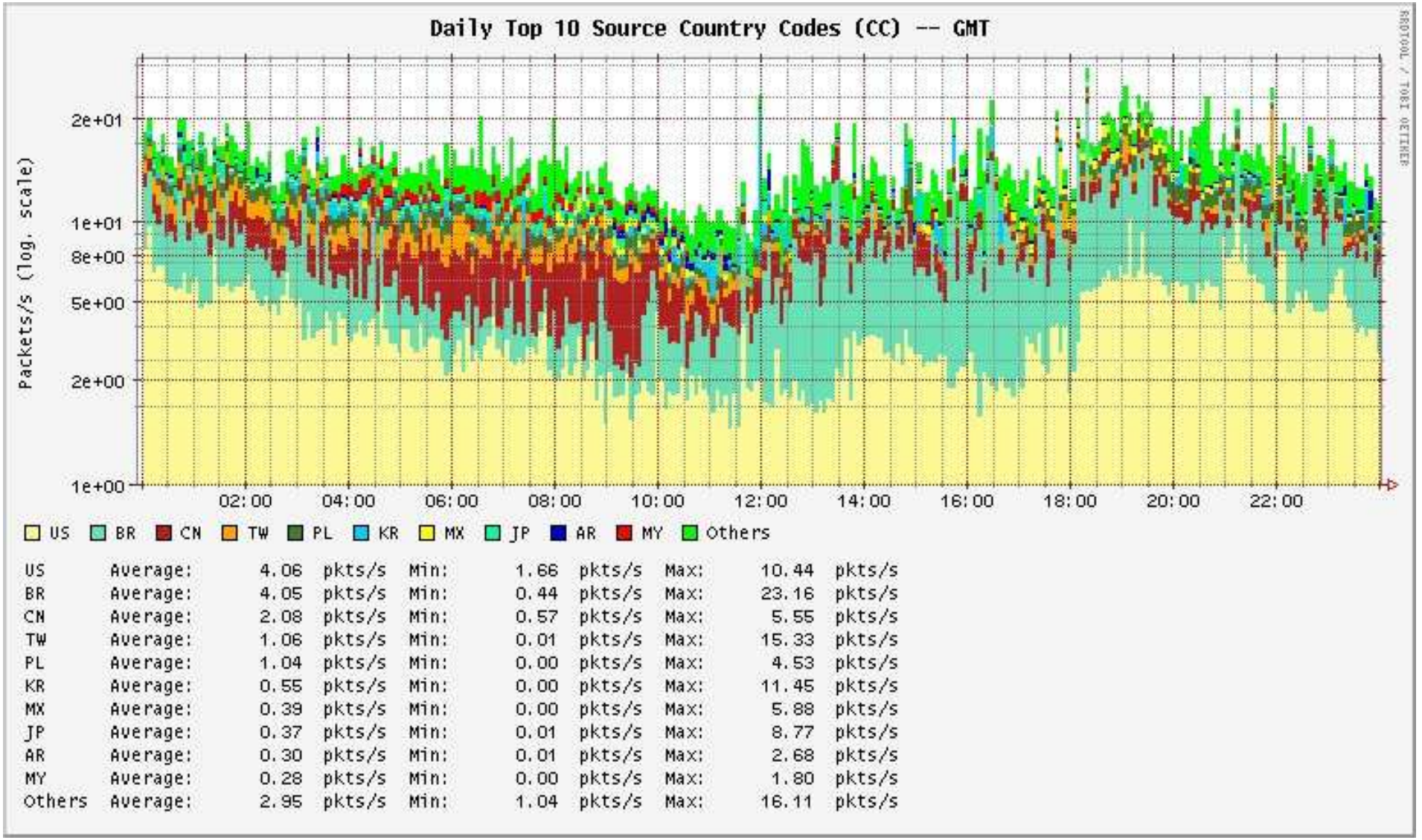
Public Statistics – Top TCP Ports



1433	Average:	505.63	bytes/s	Min:	227.87	bytes/s	Max:	1049.49 bytes/s
80	Average:	272.28	bytes/s	Min:	10.39	bytes/s	Max:	1061.22 bytes/s
135	Average:	219.18	bytes/s	Min:	46.05	bytes/s	Max:	1936.76 bytes/s
445	Average:	89.13	bytes/s	Min:	14.25	bytes/s	Max:	290.01 bytes/s
139	Average:	63.99	bytes/s	Min:	7.07	bytes/s	Max:	188.56 bytes/s
1025	Average:	52.18	bytes/s	Min:	5.12	bytes/s	Max:	163.15 bytes/s
3127	Average:	36.79	bytes/s	Min:	0.00	bytes/s	Max:	1980.03 bytes/s
4899	Average:	30.50	bytes/s	Min:	0.00	bytes/s	Max:	523.09 bytes/s
6101	Average:	21.03	bytes/s	Min:	0.00	bytes/s	Max:	1101.69 bytes/s
17300	Average:	6.87	bytes/s	Min:	0.00	bytes/s	Max:	1068.07 bytes/s
Others	Average:	67.83	bytes/s	Min:	8.03	bytes/s	Max:	1317.06 bytes/s

June 15, 2005

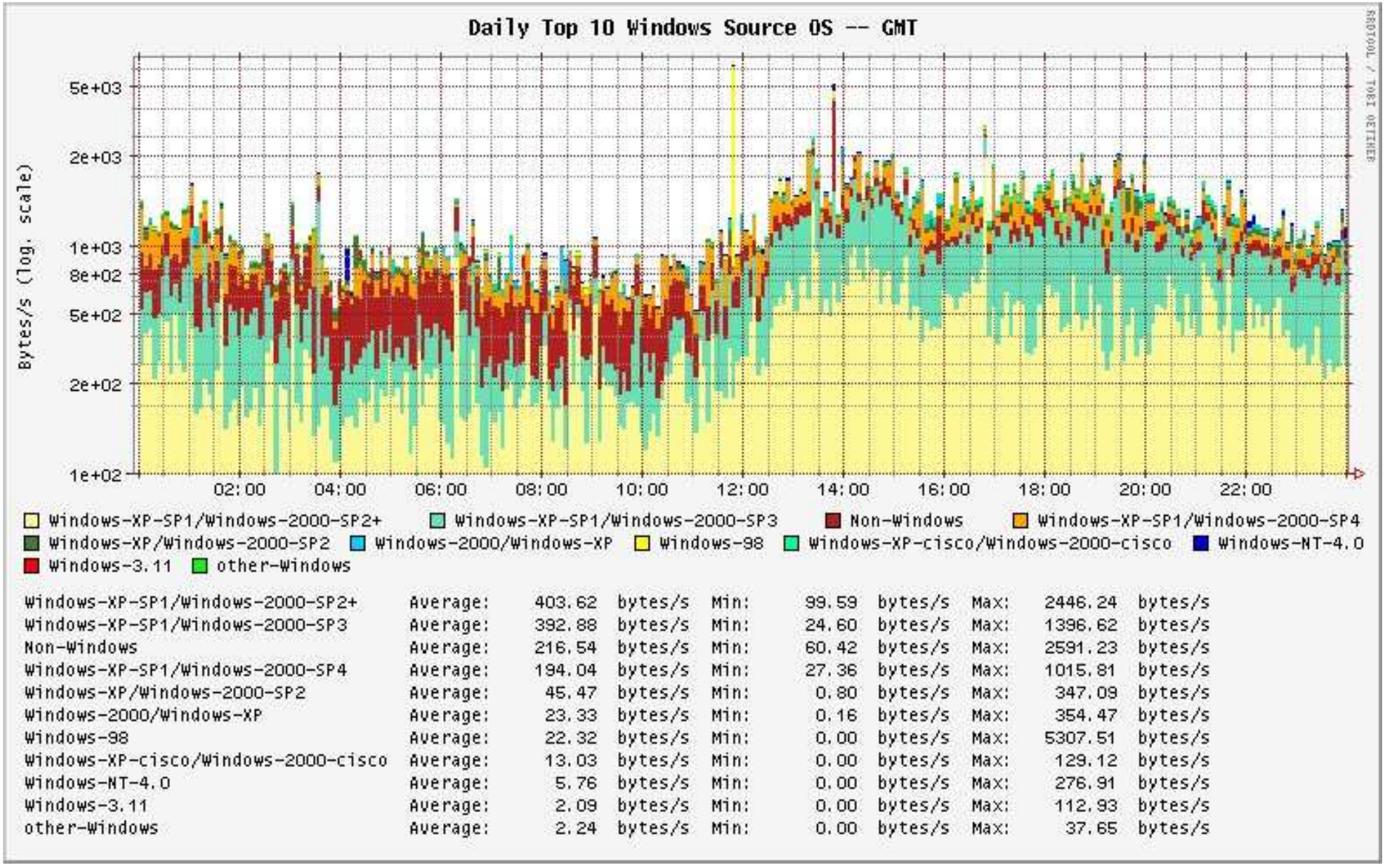
Public Statistics – Top Country Codes



US	Average:	4.06	pkts/s	Min:	1.66	pkts/s	Max:	10.44 pkts/s
BR	Average:	4.05	pkts/s	Min:	0.44	pkts/s	Max:	23.16 pkts/s
CN	Average:	2.08	pkts/s	Min:	0.57	pkts/s	Max:	5.55 pkts/s
TW	Average:	1.06	pkts/s	Min:	0.01	pkts/s	Max:	15.33 pkts/s
PL	Average:	1.04	pkts/s	Min:	0.00	pkts/s	Max:	4.53 pkts/s
KR	Average:	0.55	pkts/s	Min:	0.00	pkts/s	Max:	11.45 pkts/s
MX	Average:	0.39	pkts/s	Min:	0.00	pkts/s	Max:	5.88 pkts/s
JP	Average:	0.37	pkts/s	Min:	0.01	pkts/s	Max:	8.77 pkts/s
AR	Average:	0.30	pkts/s	Min:	0.01	pkts/s	Max:	2.68 pkts/s
MY	Average:	0.28	pkts/s	Min:	0.00	pkts/s	Max:	1.80 pkts/s
Others	Average:	2.95	pkts/s	Min:	1.04	pkts/s	Max:	16.11 pkts/s

June 17, 2005

Public Statistics – Top Source OS



Windows-XP-SP1/Windows-2000-SP2+	Average:	403.62	bytes/s	Min:	99.59	bytes/s	Max:	2446.24 bytes/s
Windows-XP-SP1/Windows-2000-SP3	Average:	392.88	bytes/s	Min:	24.60	bytes/s	Max:	1396.62 bytes/s
Non-Windows	Average:	216.54	bytes/s	Min:	60.42	bytes/s	Max:	2591.23 bytes/s
Windows-XP-SP1/Windows-2000-SP4	Average:	194.04	bytes/s	Min:	27.36	bytes/s	Max:	1015.81 bytes/s
Windows-XP/Windows-2000-SP2	Average:	45.47	bytes/s	Min:	0.80	bytes/s	Max:	347.09 bytes/s
Windows-2000/Windows-XP	Average:	23.33	bytes/s	Min:	0.16	bytes/s	Max:	354.47 bytes/s
Windows-98	Average:	22.32	bytes/s	Min:	0.00	bytes/s	Max:	5307.51 bytes/s
Windows-XP-cisco/Windows-2000-cisco	Average:	13.03	bytes/s	Min:	0.00	bytes/s	Max:	129.12 bytes/s
Windows-NT-4.0	Average:	5.76	bytes/s	Min:	0.00	bytes/s	Max:	276.91 bytes/s
Windows-3.11	Average:	2.09	bytes/s	Min:	0.00	bytes/s	Max:	112.93 bytes/s
other-Windows	Average:	2.24	bytes/s	Min:	0.00	bytes/s	Max:	37.65 bytes/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

Related Links

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