A National Early Warning Capability Based on a Network of Distributed Honeypots

Cristine Hoepers, Klaus Steding-Jessen
Luiz Eduardo R. Cordeiro, Marcelo H. P. C. Chaves
{cristine,jessen,cordeiro,mhp}@cert.br

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

Overview

- Motivation
- The honeypots network
- Early Warning
- Use in Incident Response
- Advantages and disadvantages
- Future work

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 (formerly NBSO)
    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.)

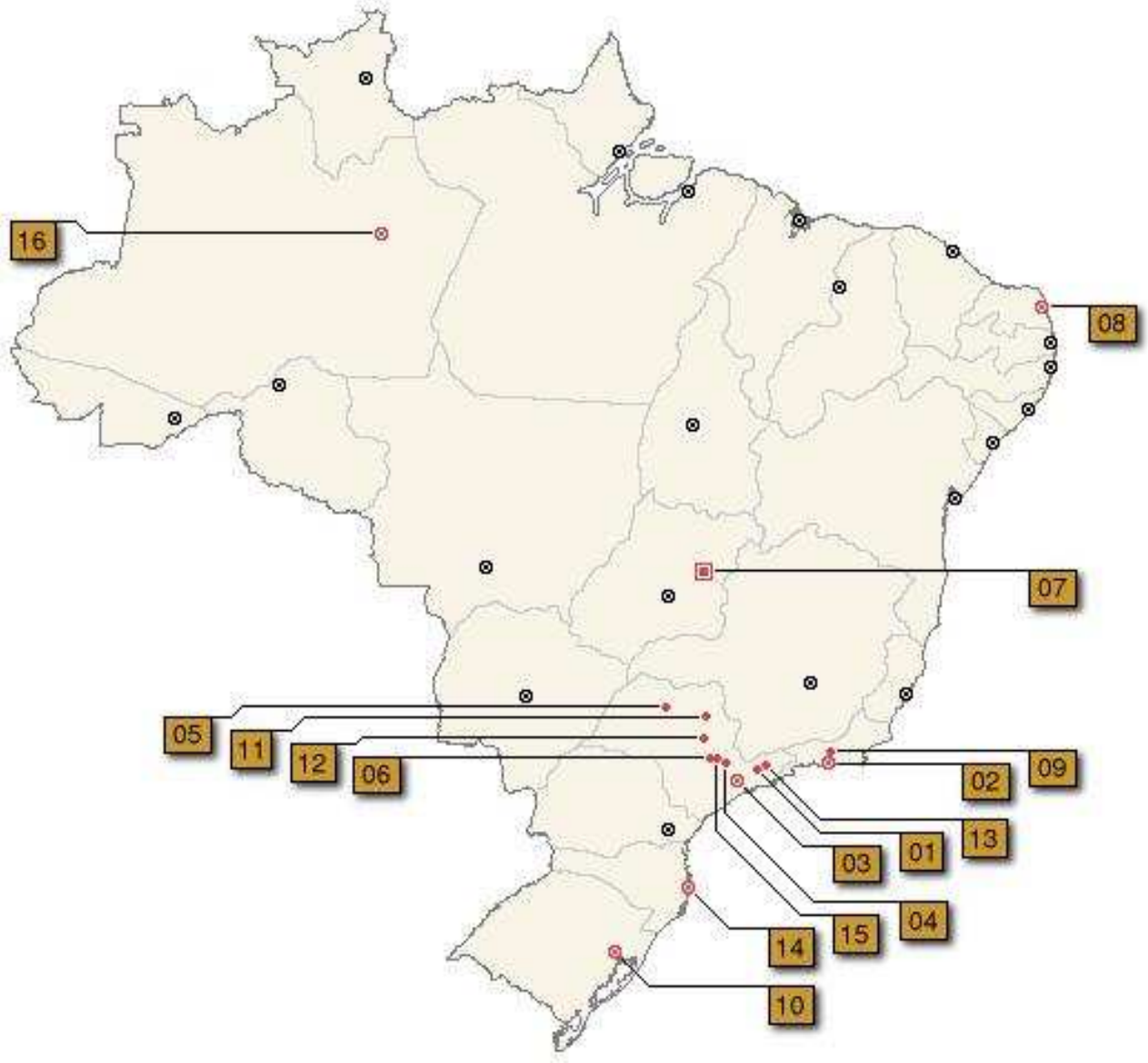
26 research partner's institutions:

- 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, 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.)

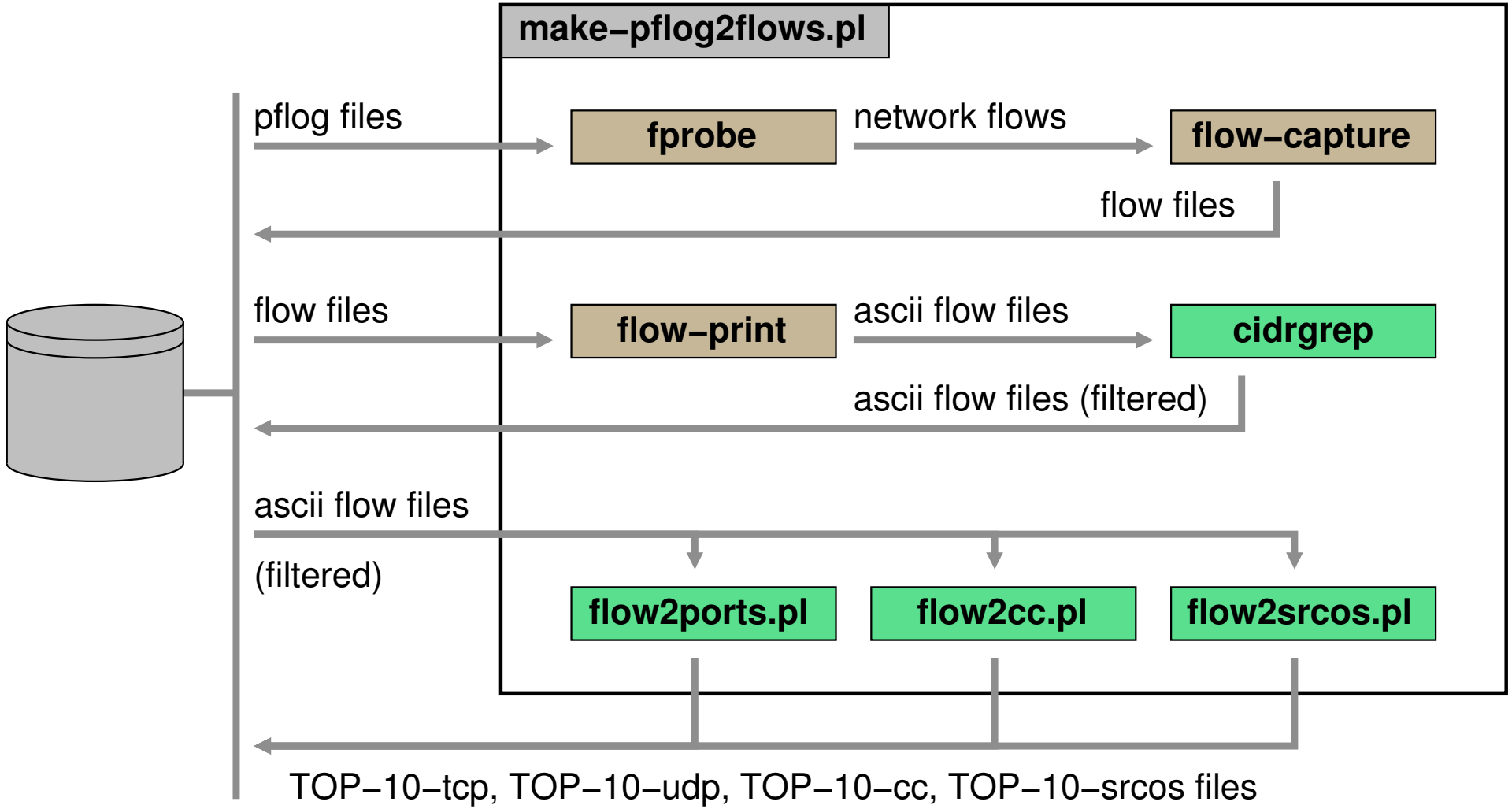
Usefulness:

- 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

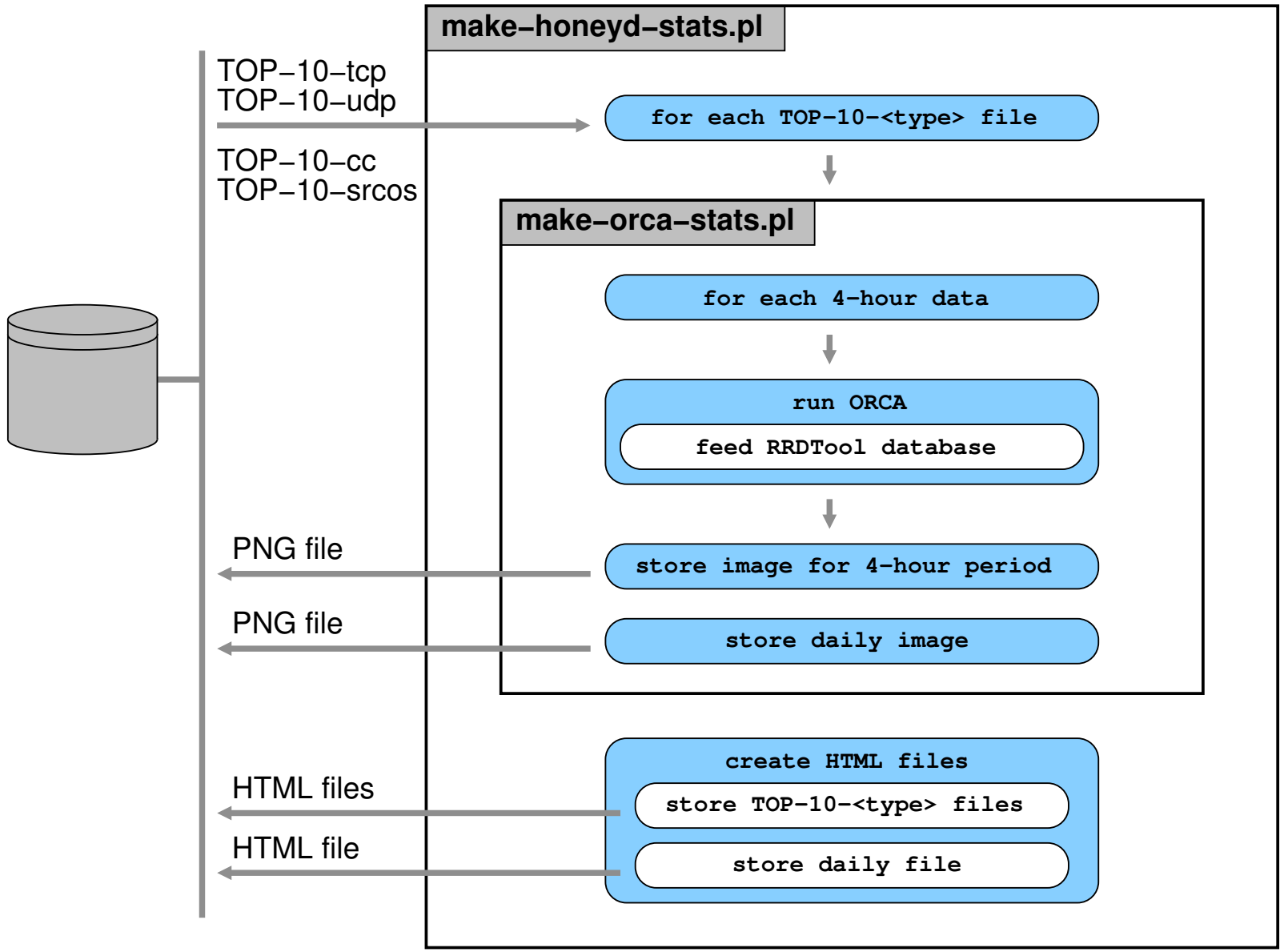
Public Statistics Generation

- 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

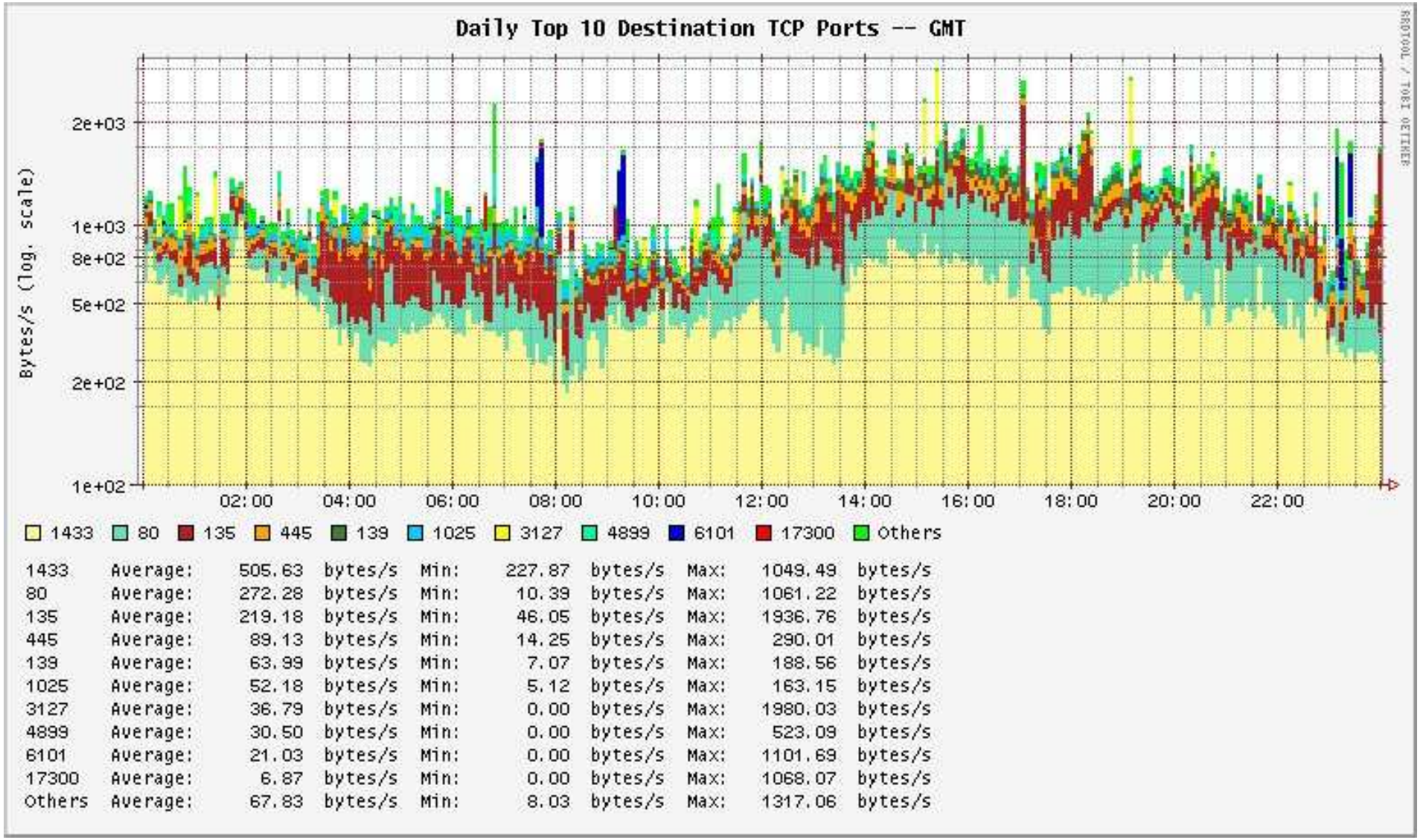
Public Statistics Generation (cont.)



Public Statistics Generation (cont.)



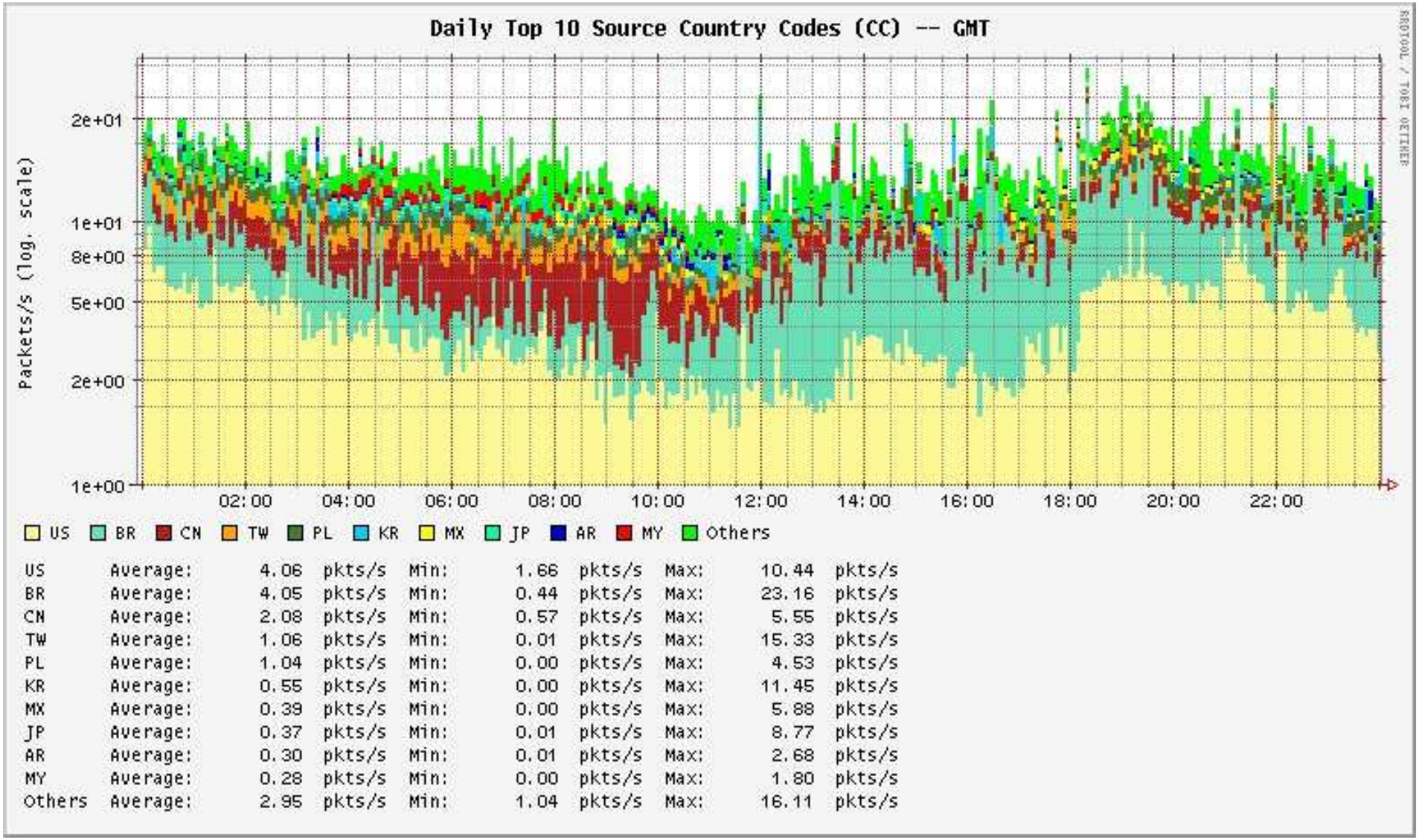
Public Statistics – Top TCP Ports



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

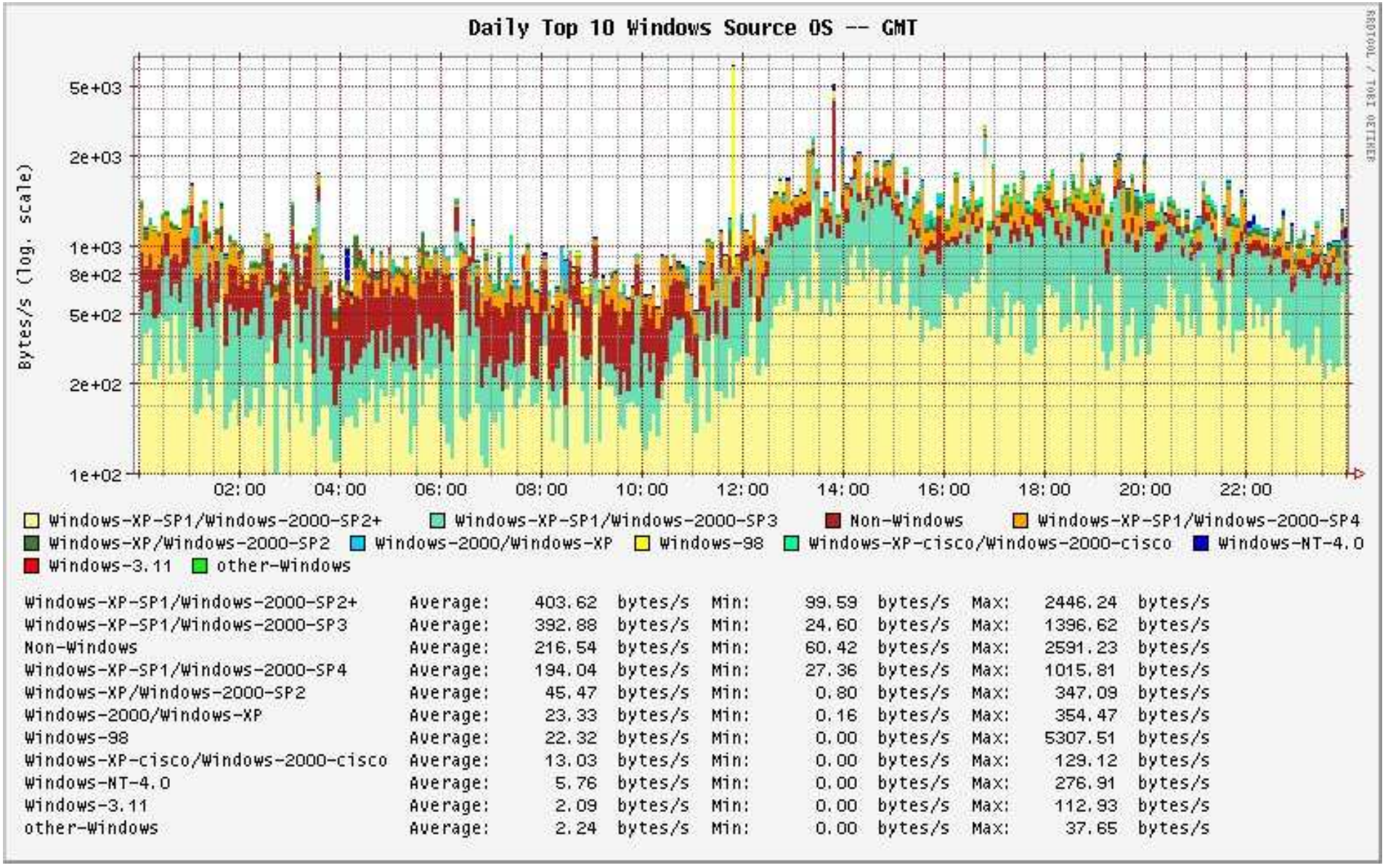
Public Statistics – Top Country Codes



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

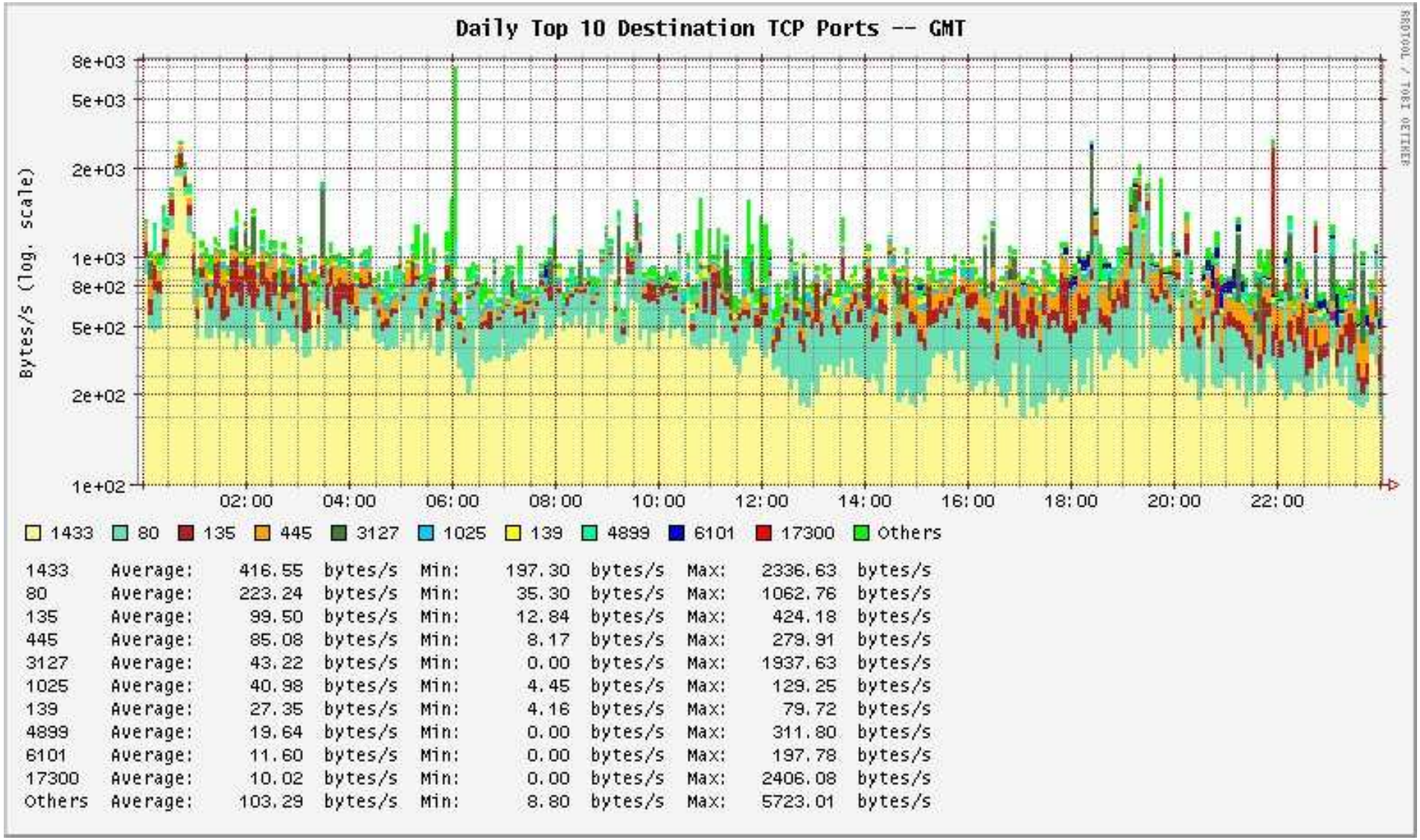
June 17, 2005

Public Statistics – Top Source OS



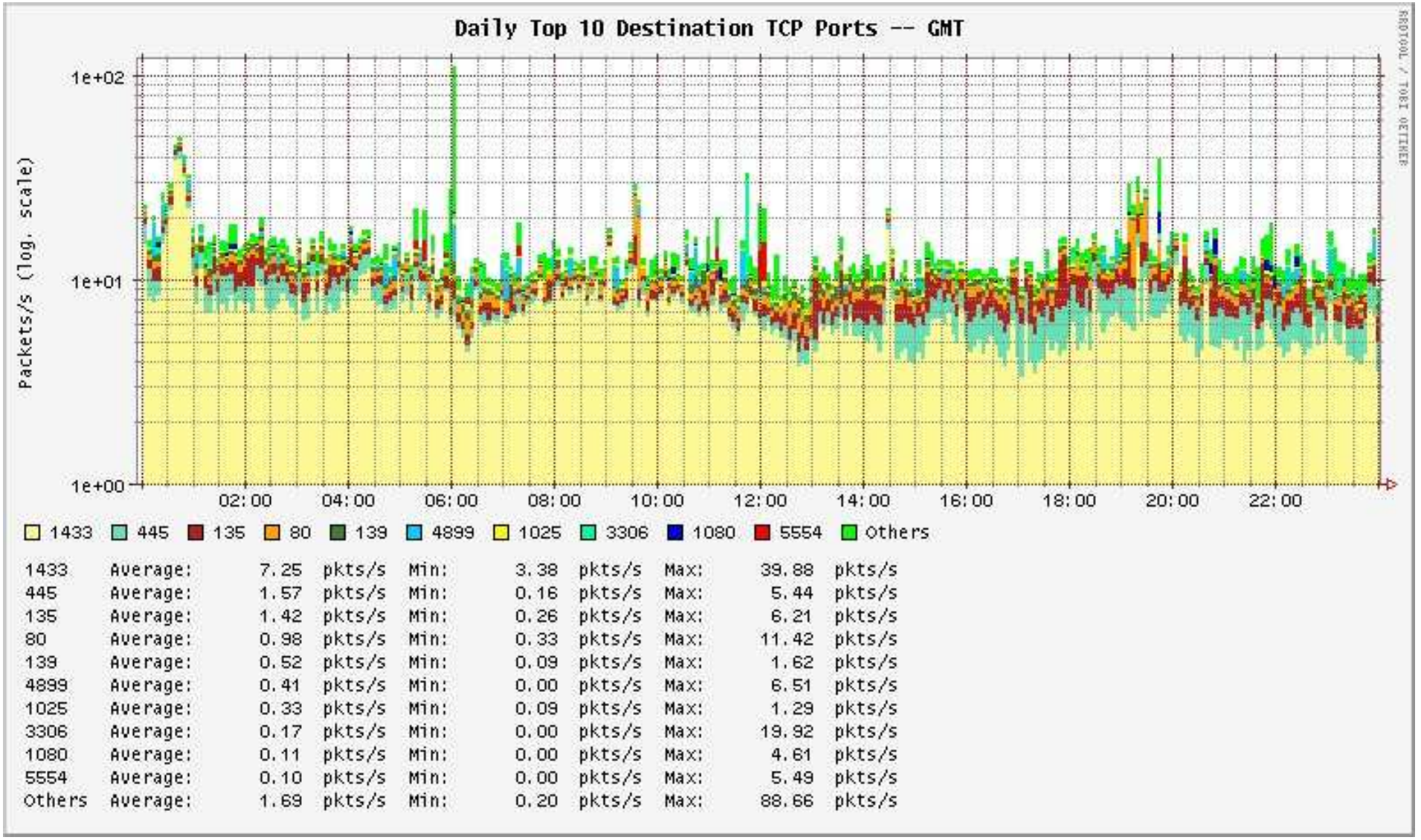
Windows-XP-SP1/Windows-2000-SP2+	Average:	403.62	bytes/s	Min:	99.59	bytes/s	Max:	2446.24 bytes/s
Windows-XP-SP1/Windows-2000-SP3	Average:	392.88	bytes/s	Min:	24.60	bytes/s	Max:	1396.62 bytes/s
Non-Windows	Average:	216.54	bytes/s	Min:	60.42	bytes/s	Max:	2591.23 bytes/s
Windows-XP-SP1/Windows-2000-SP4	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

Public Statistics – Correlation



June 12, 2005

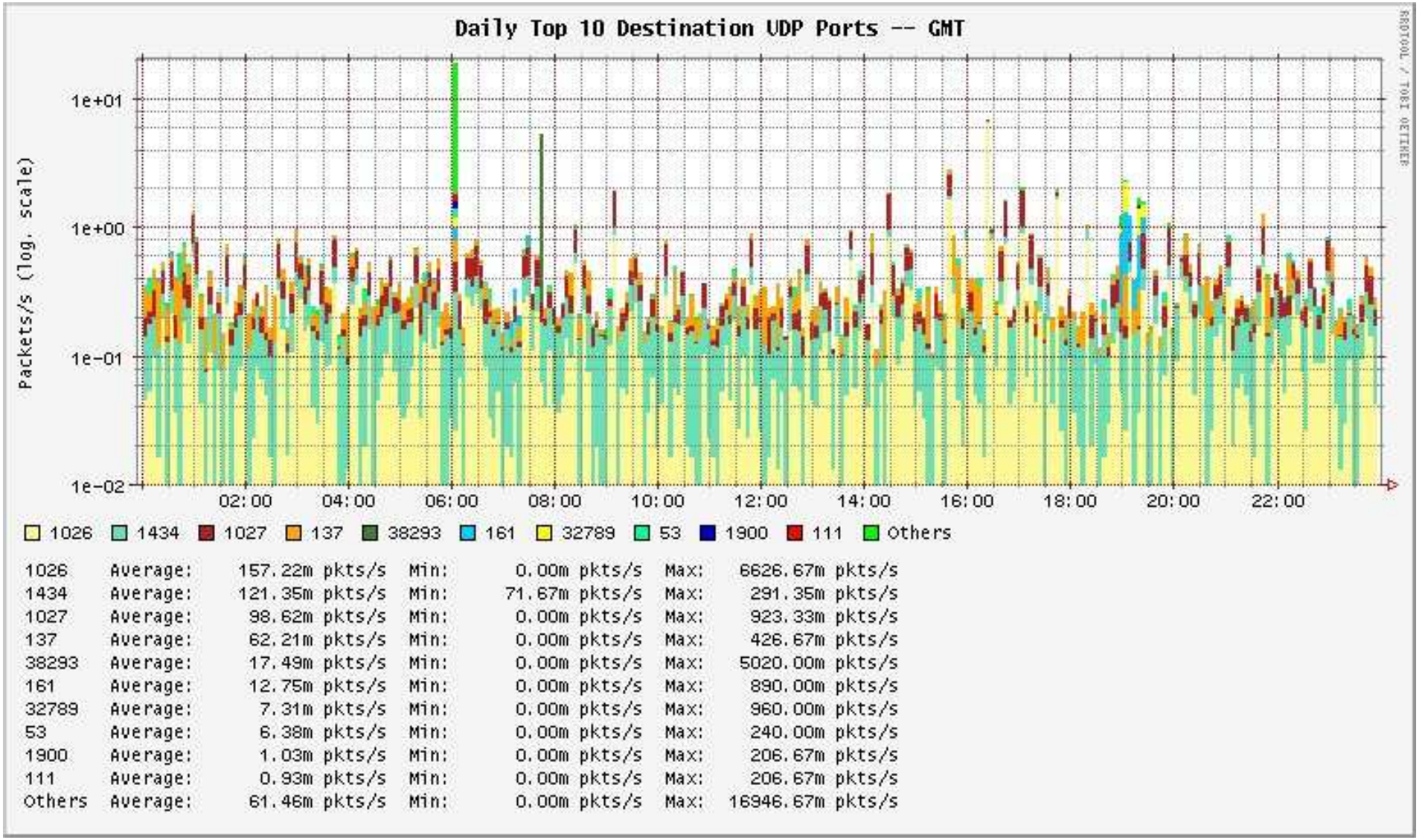
Public Statistics – Correlation (cont.)



1433	Average:	7.25	pkts/s	Min:	3.38	pkts/s	Max:	39.88 pkts/s
445	Average:	1.57	pkts/s	Min:	0.16	pkts/s	Max:	5.44 pkts/s
135	Average:	1.42	pkts/s	Min:	0.26	pkts/s	Max:	6.21 pkts/s
80	Average:	0.98	pkts/s	Min:	0.33	pkts/s	Max:	11.42 pkts/s
139	Average:	0.52	pkts/s	Min:	0.09	pkts/s	Max:	1.62 pkts/s
4899	Average:	0.41	pkts/s	Min:	0.00	pkts/s	Max:	6.51 pkts/s
1025	Average:	0.33	pkts/s	Min:	0.09	pkts/s	Max:	1.29 pkts/s
3306	Average:	0.17	pkts/s	Min:	0.00	pkts/s	Max:	19.92 pkts/s
1080	Average:	0.11	pkts/s	Min:	0.00	pkts/s	Max:	4.61 pkts/s
5554	Average:	0.10	pkts/s	Min:	0.00	pkts/s	Max:	5.49 pkts/s
Others	Average:	1.69	pkts/s	Min:	0.20	pkts/s	Max:	88.66 pkts/s

June 12, 2005

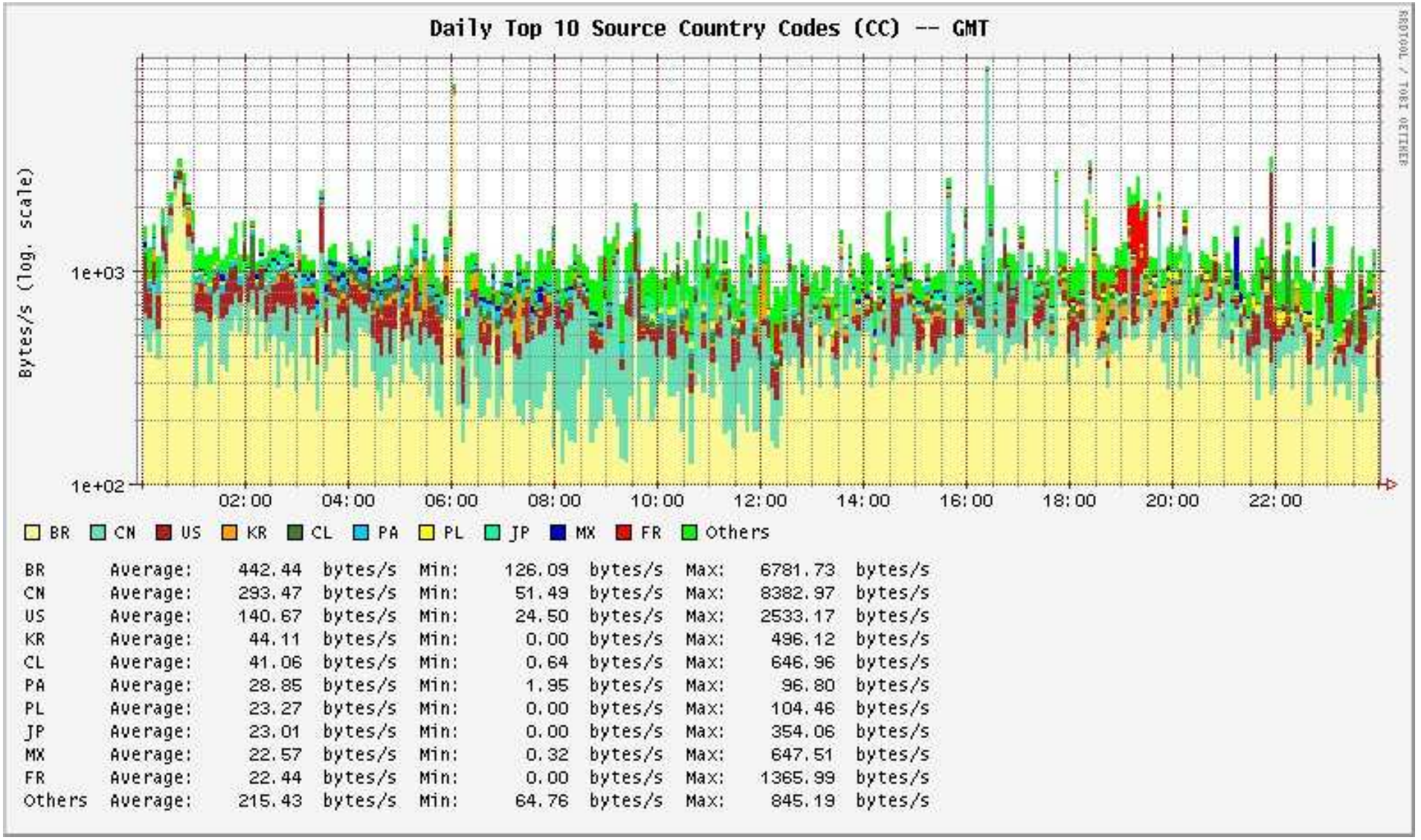
Public Statistics – Correlation (cont.)



1026	Average:	157.22m pkts/s	Min:	0.00m pkts/s	Max:	6626.67m pkts/s
1434	Average:	121.35m pkts/s	Min:	71.67m pkts/s	Max:	291.35m pkts/s
1027	Average:	98.62m pkts/s	Min:	0.00m pkts/s	Max:	923.33m pkts/s
137	Average:	62.21m pkts/s	Min:	0.00m pkts/s	Max:	426.67m pkts/s
38293	Average:	17.49m pkts/s	Min:	0.00m pkts/s	Max:	5020.00m pkts/s
161	Average:	12.75m pkts/s	Min:	0.00m pkts/s	Max:	890.00m pkts/s
32789	Average:	7.31m pkts/s	Min:	0.00m pkts/s	Max:	960.00m pkts/s
53	Average:	6.38m pkts/s	Min:	0.00m pkts/s	Max:	240.00m pkts/s
1900	Average:	1.03m pkts/s	Min:	0.00m pkts/s	Max:	206.67m pkts/s
111	Average:	0.93m pkts/s	Min:	0.00m pkts/s	Max:	206.67m pkts/s
Others	Average:	61.46m pkts/s	Min:	0.00m pkts/s	Max:	16946.67m pkts/s

June 12, 2005

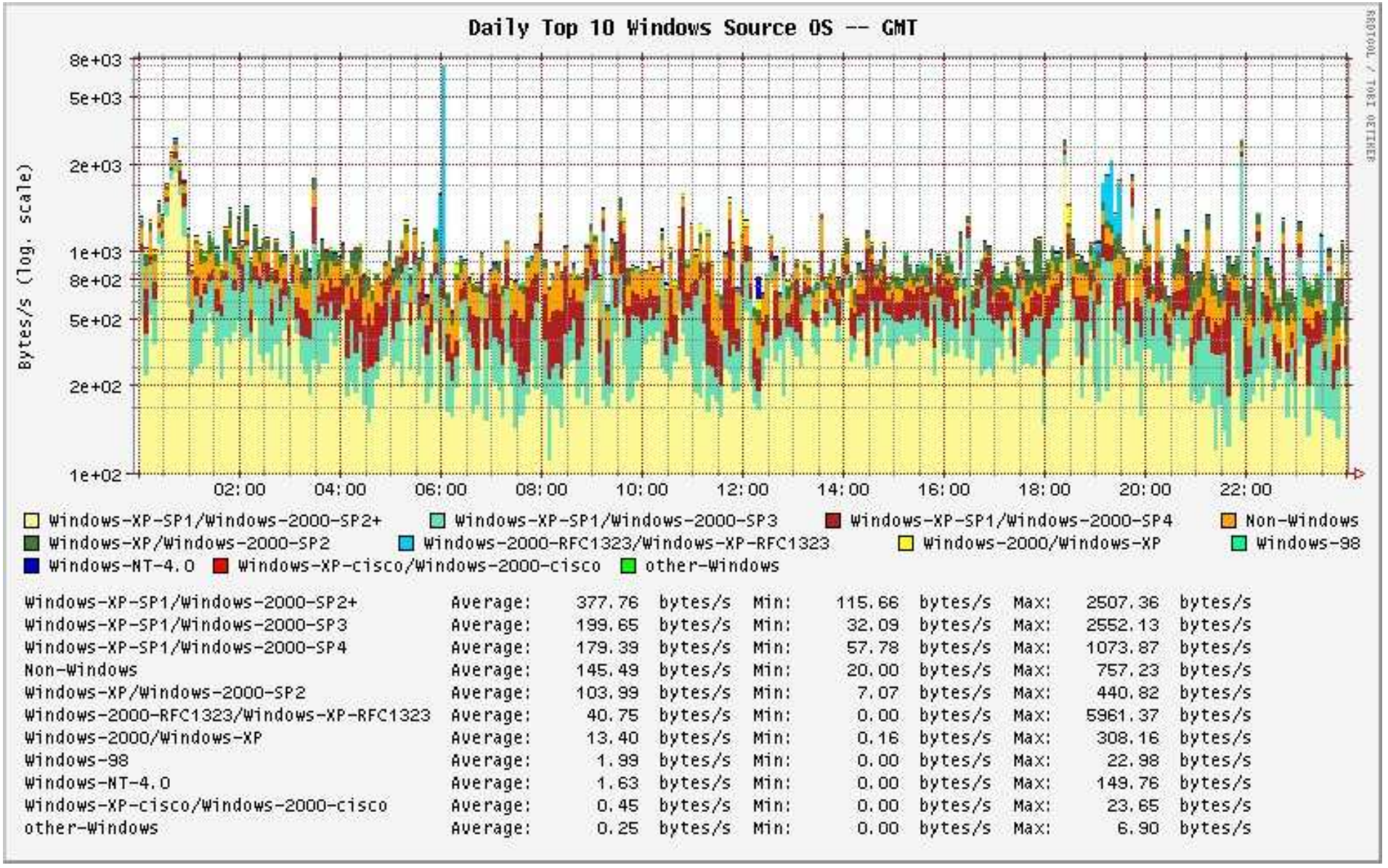
Public Statistics – Correlation (cont.)



BR	Average:	442.44	bytes/s	Min:	126.09	bytes/s	Max:	6781.73 bytes/s
CN	Average:	293.47	bytes/s	Min:	51.49	bytes/s	Max:	8382.97 bytes/s
US	Average:	140.67	bytes/s	Min:	24.50	bytes/s	Max:	2533.17 bytes/s
KR	Average:	44.11	bytes/s	Min:	0.00	bytes/s	Max:	496.12 bytes/s
CL	Average:	41.06	bytes/s	Min:	0.64	bytes/s	Max:	646.96 bytes/s
PA	Average:	28.85	bytes/s	Min:	1.95	bytes/s	Max:	96.80 bytes/s
PL	Average:	23.27	bytes/s	Min:	0.00	bytes/s	Max:	104.46 bytes/s
JP	Average:	23.01	bytes/s	Min:	0.00	bytes/s	Max:	354.06 bytes/s
MX	Average:	22.57	bytes/s	Min:	0.32	bytes/s	Max:	647.51 bytes/s
FR	Average:	22.44	bytes/s	Min:	0.00	bytes/s	Max:	1365.99 bytes/s
Others	Average:	215.43	bytes/s	Min:	64.76	bytes/s	Max:	845.19 bytes/s

June 12, 2005

Public Statistics – Correlation (cont.)



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
  - 9 new partners in installation phase
- Have more frequent private summaries
- Provide hourly public statistics
- Increase data donation to trusted parties

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/