

# Honeynet.BR and the National Early Warning Capability Based on a Network of Distributed Honeypots

Cristine Hoepers

[cristine@cert.br](mailto:cristine@cert.br)

Computer Emergency Response Team Brazil – CERT.br

<http://www.cert.br/>

Brazilian Internet Steering Committee

<http://www.cgi.br/>

# Overview

---

- Honeynet.BR
  - objectives and requirements
  - architecture overview
- Early warning using honeypots
  - Motivation
  - The honeypots network
  - Advantages and disadvantages
  - Future work

# Honeynet.BR Objectives

---

- Monitor current attacks and intrusions
- Collect data
- Develop new tools
- Use in Incident Response

# Implementation Decisions

---

## Requirements:

- Low-cost and reliability
- High quality data control mechanism

## Decisions:

- Use of Free Software
- Store data in a well-known format (`libpcap`)

# Architecture Overview

---

- 2 honeynets in different address spaces
- Use of OpenBSD for data control and data collection
- Several honeypots with different OSs and applications
- Developed Honeynet Maintenance Procedures and Tools

# Alerts and Summaries

---

- Alerts
  - outgoing packets originating from the honeynet
  - shell commands
- Daily summaries
  - statistics (top ports, protocols, number of packets, etc)
  - snort alerts

# Use in Incident Response

---

## Understand constituency threats:

- Detection of attacks
- Better understanding of ongoing activities
- Compare activities with incident reports

## Help the community:

- Alert networks that originate malicious activity
- New rootkits are used to update `chkrootkit` tool

# Lessons Learned

---

- Needs good containment mechanisms
- Can be time consuming
  - use of scripts can minimize the problem
- Correlate honeynet data and incident reports
  - clarify attacks
  - add more information
  - help to identify false positives



# Early Warning Using Honeypots

# 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.)

---

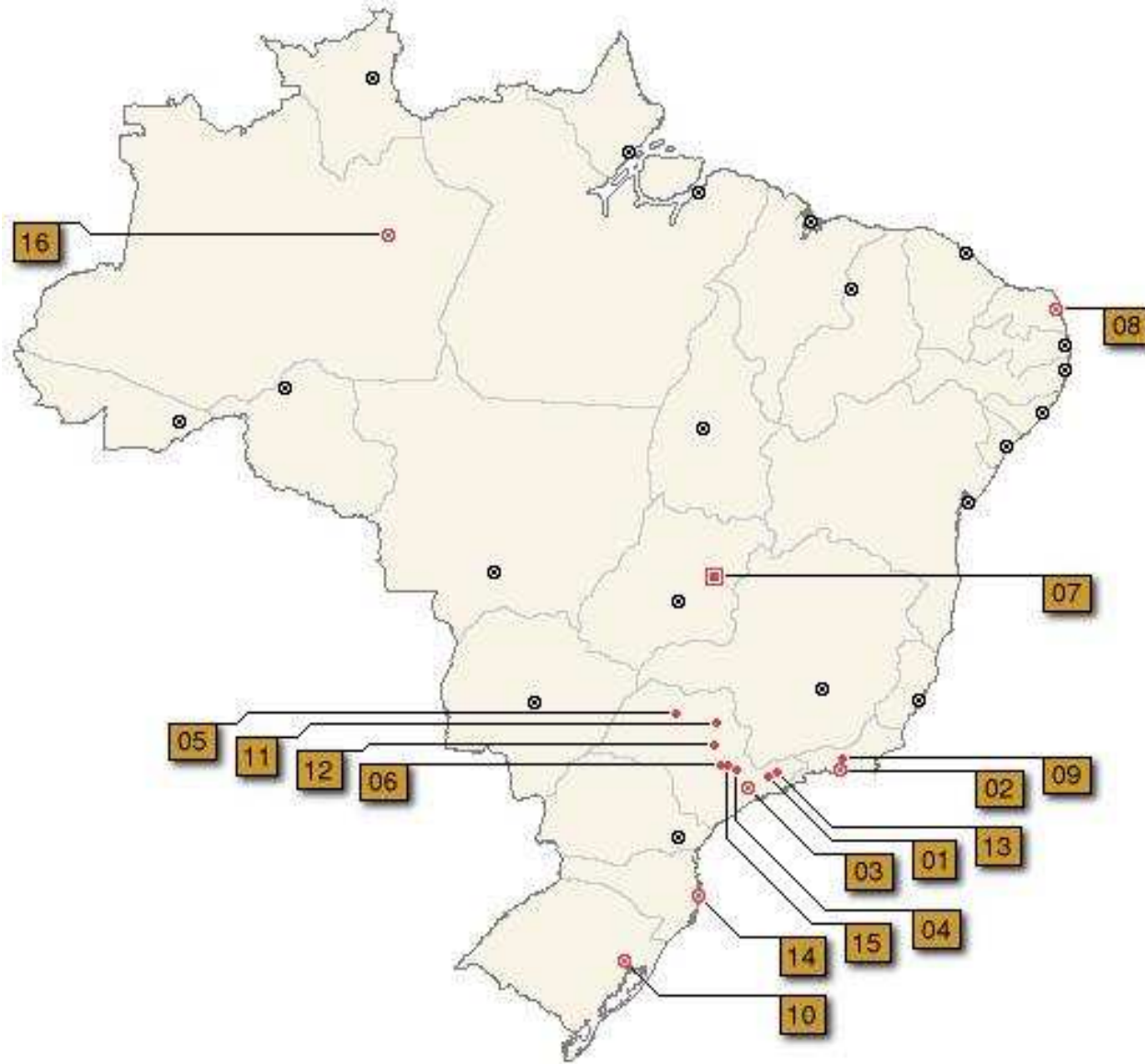
26 research partner's institutions:

- 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.)





# 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:

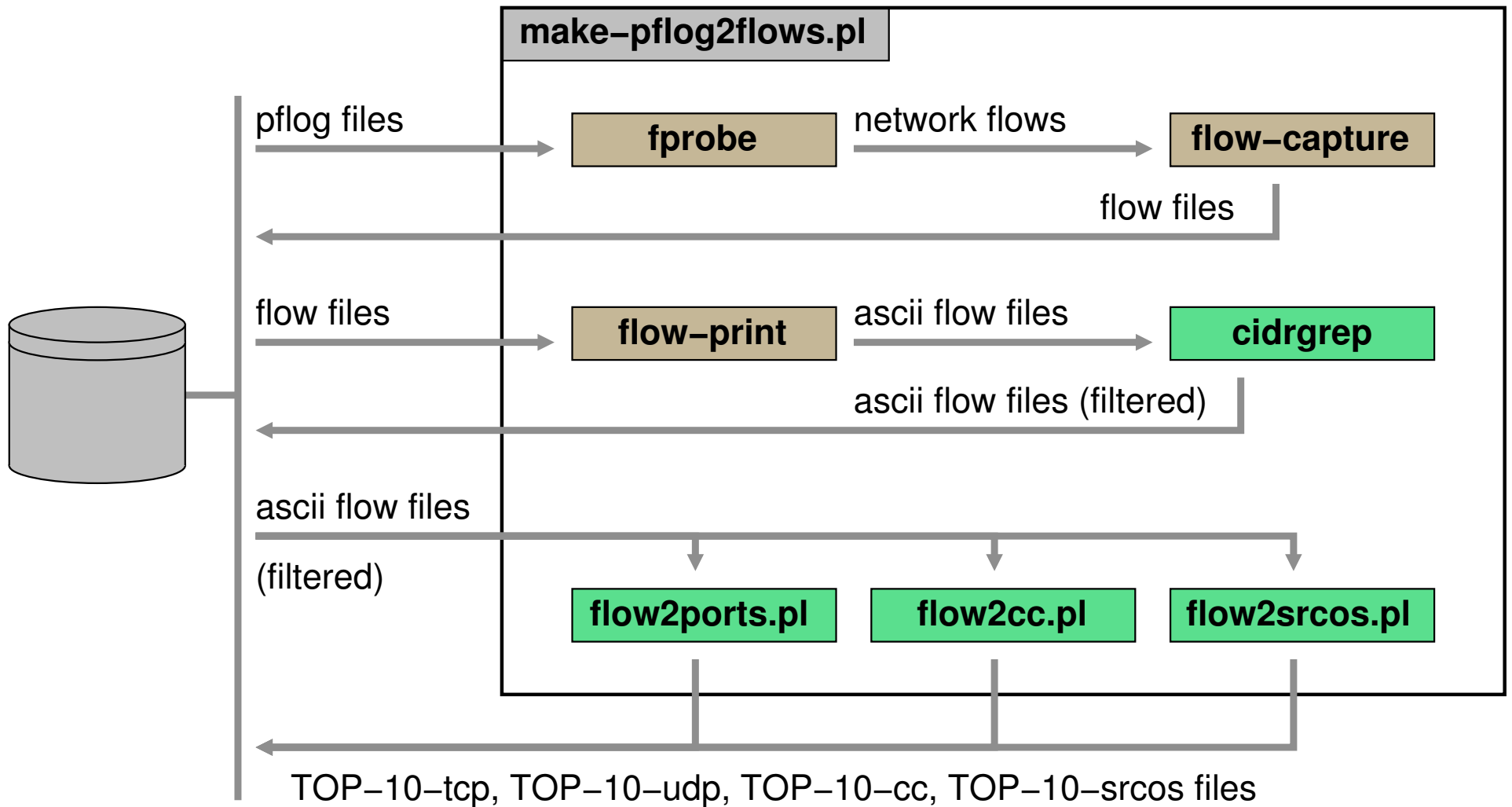
- observation of trends
  - detect scans for potential new vulnerabilities
- partner institutions are detecting promptly:
  - outbreaks of new worms/bots
  - compromised servers
  - network configuration errors
- collect new signatures and new malware

# Public Statistics Generation

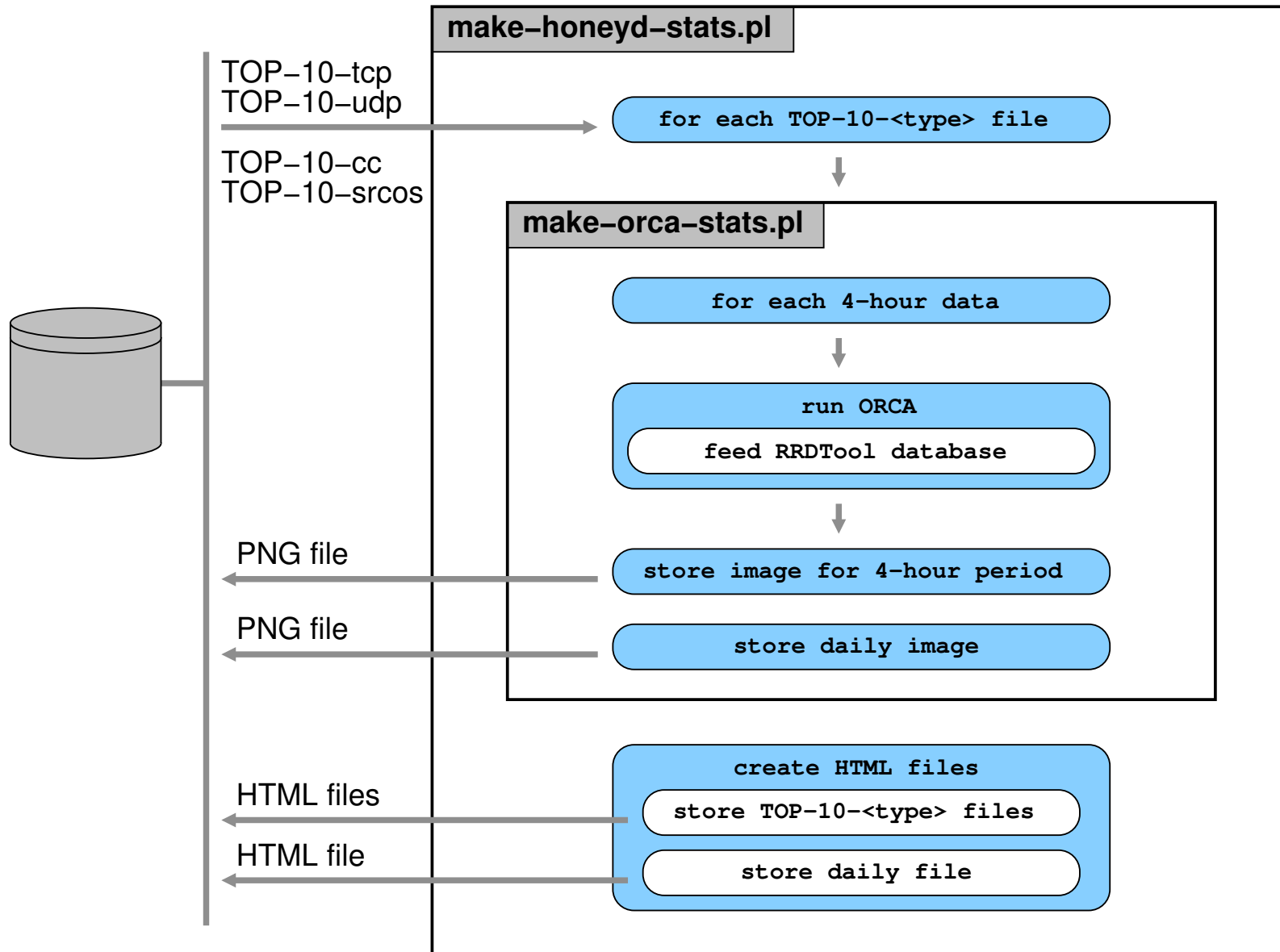
---

- 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

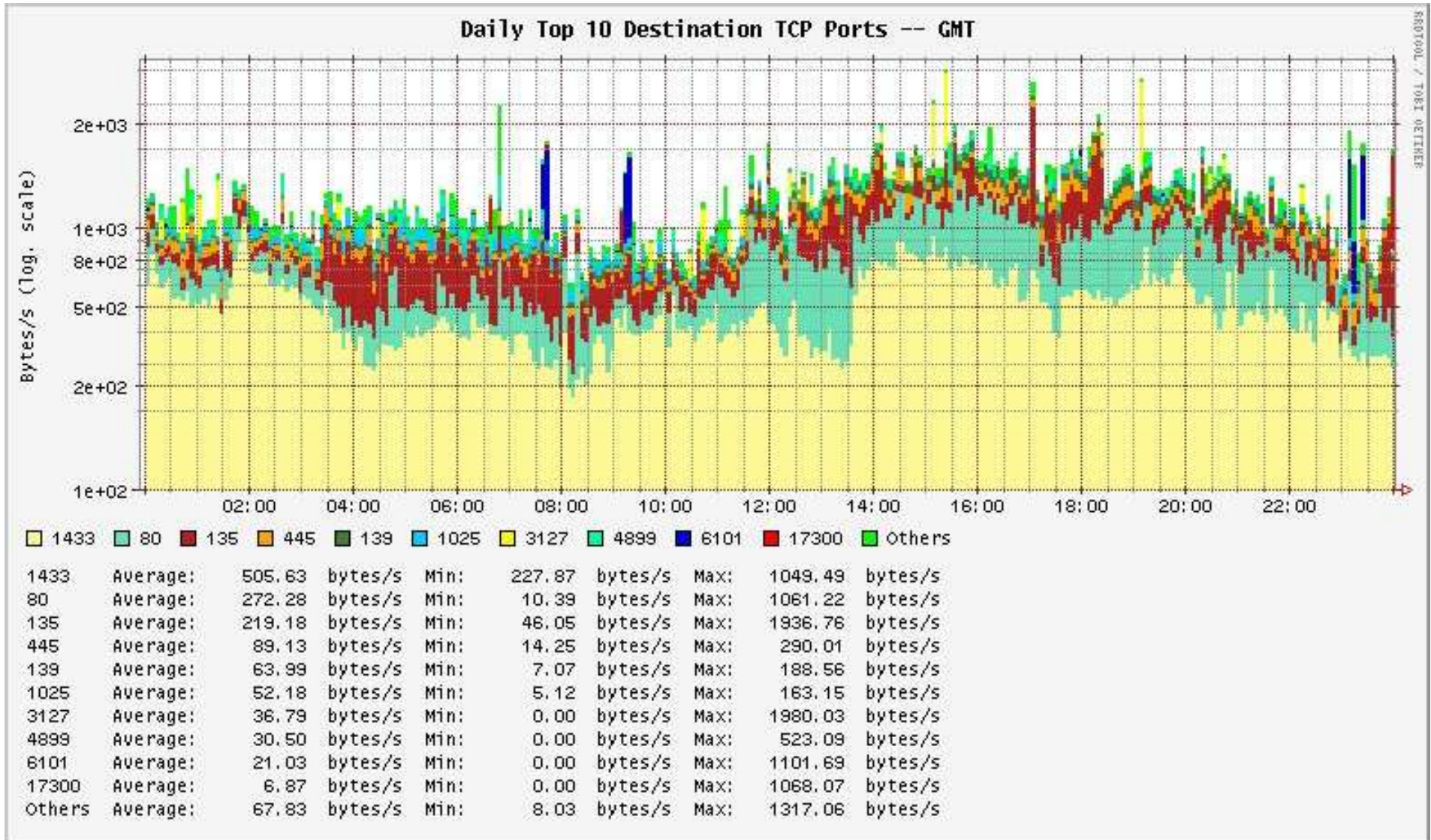
# Public Statistics Generation (cont.)



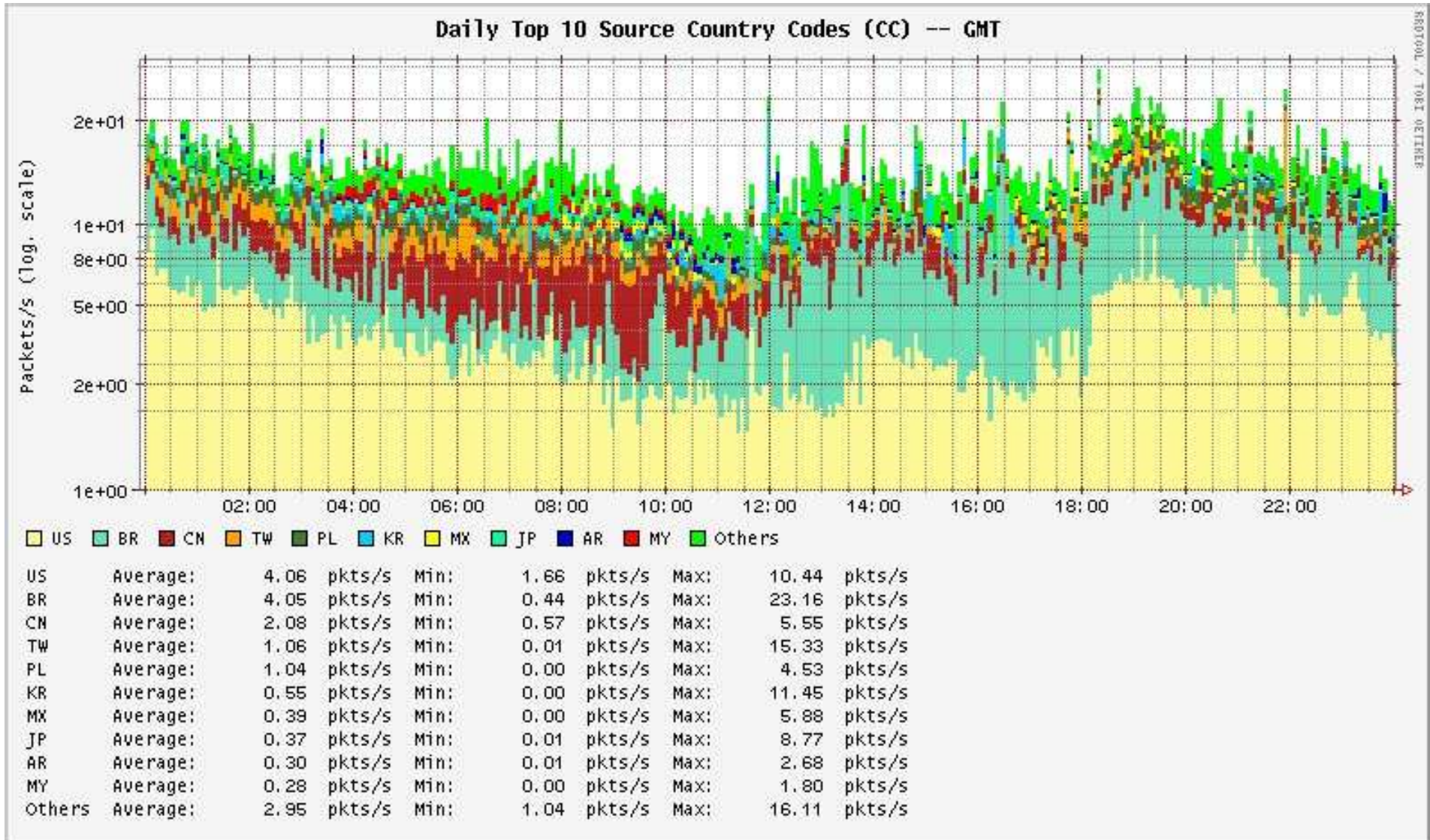
# Public Statistics Generation (cont.)



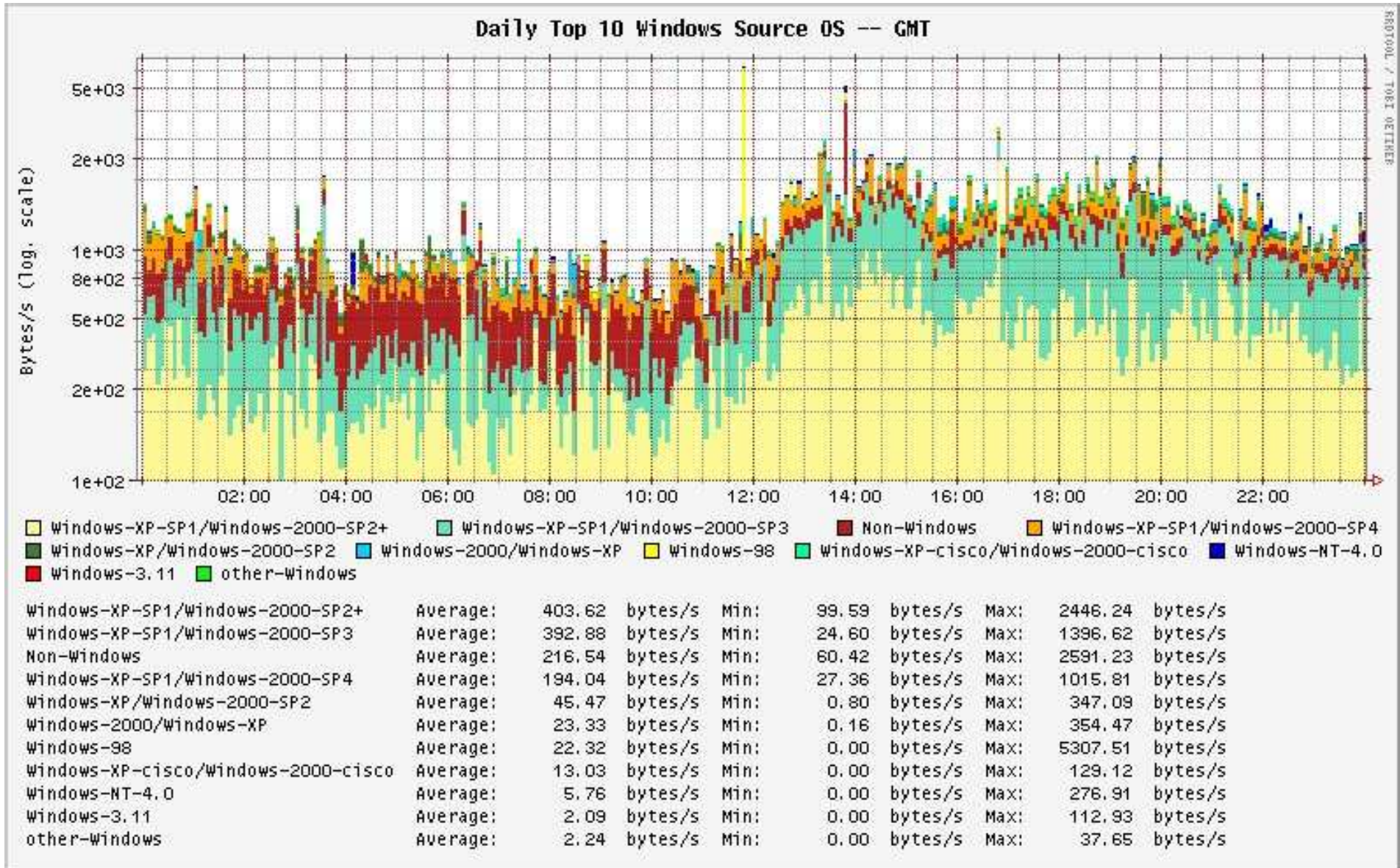
# Public Statistics – Top TCP Ports



# Public Statistics – Top Country Codes

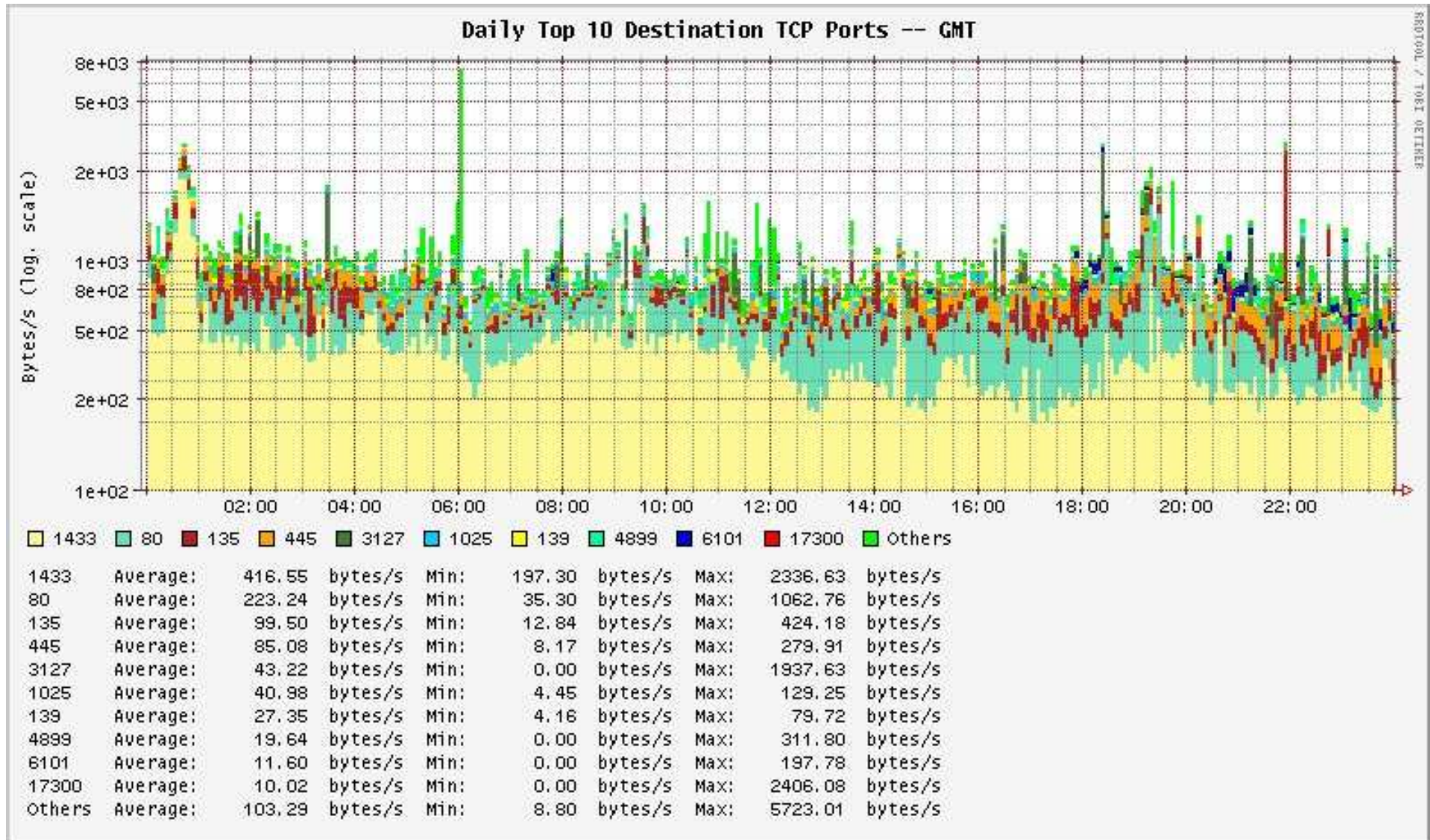


# Public Statistics – Top Source OS

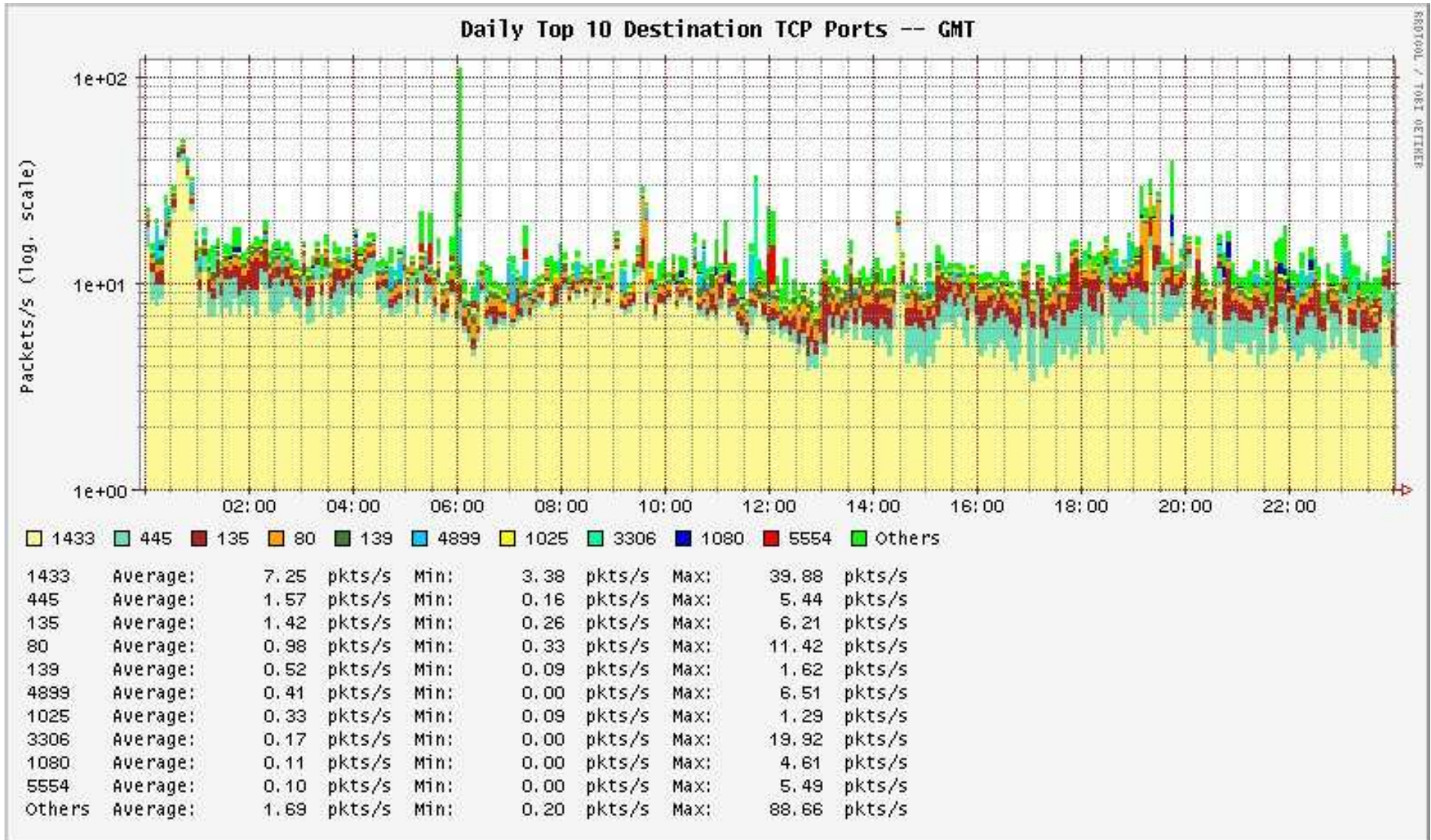




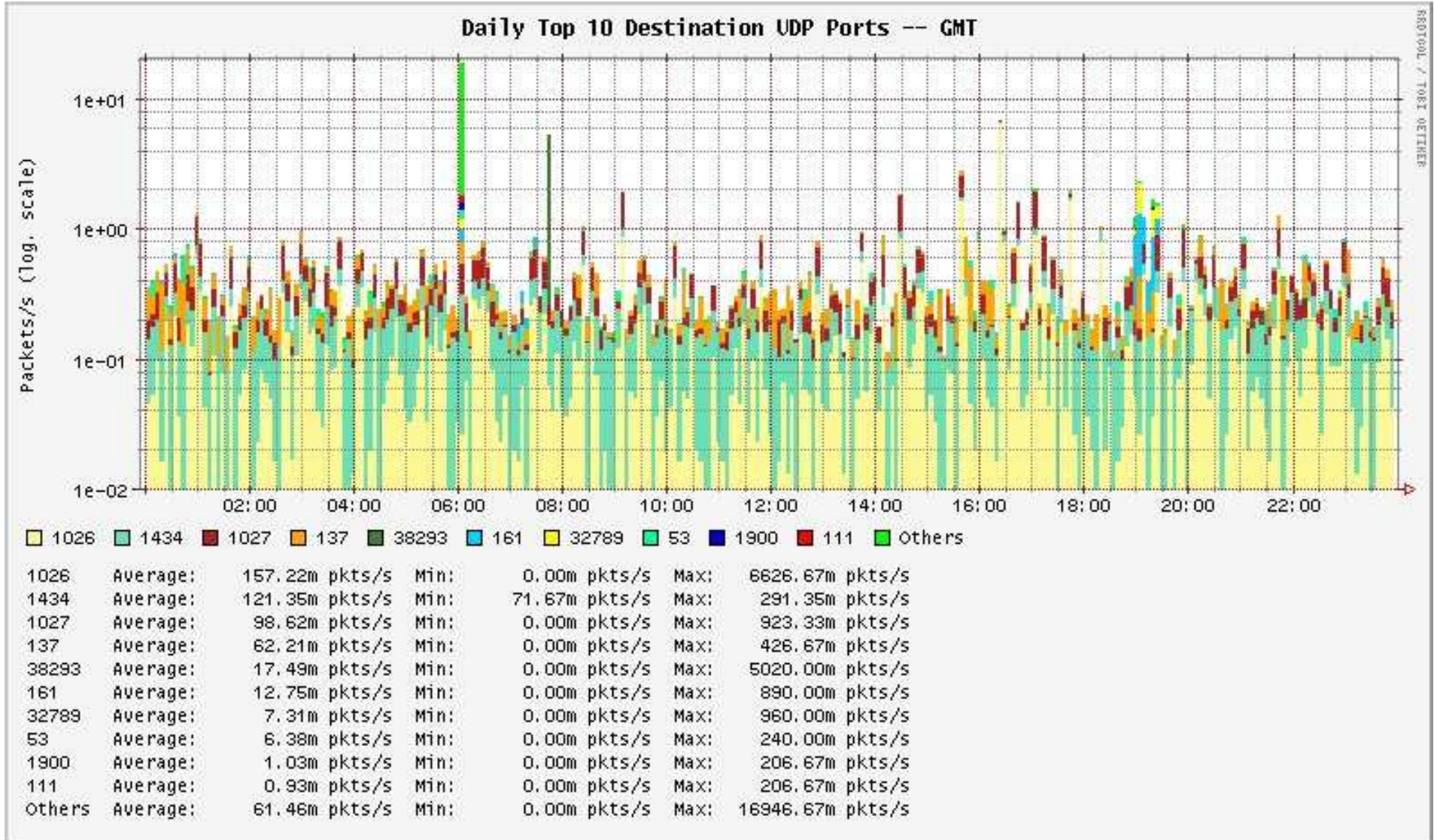
# Public Statistics – Correlation



# Public Statistics – Correlation (cont.)

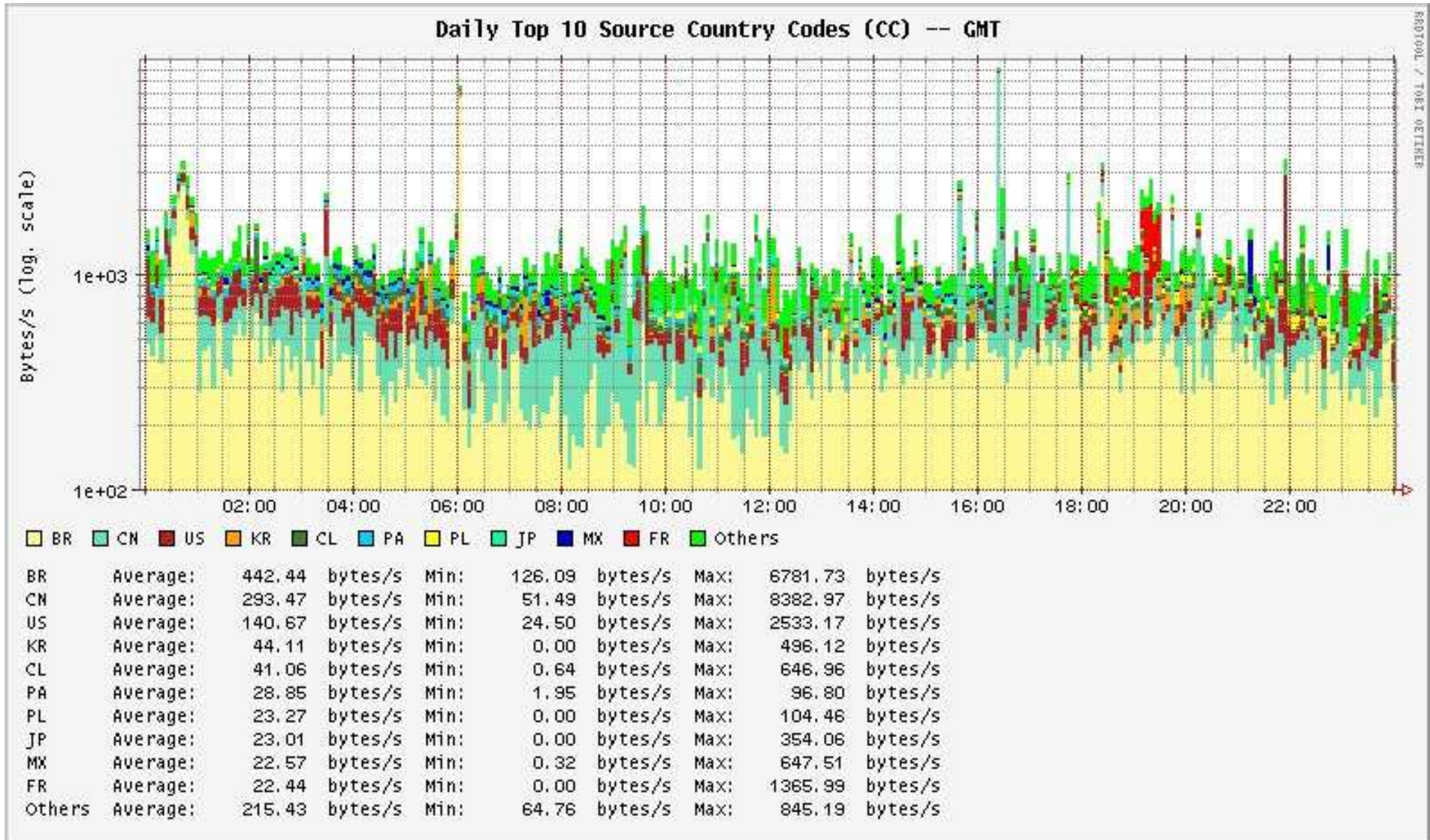


# Public Statistics – Correlation (cont.)

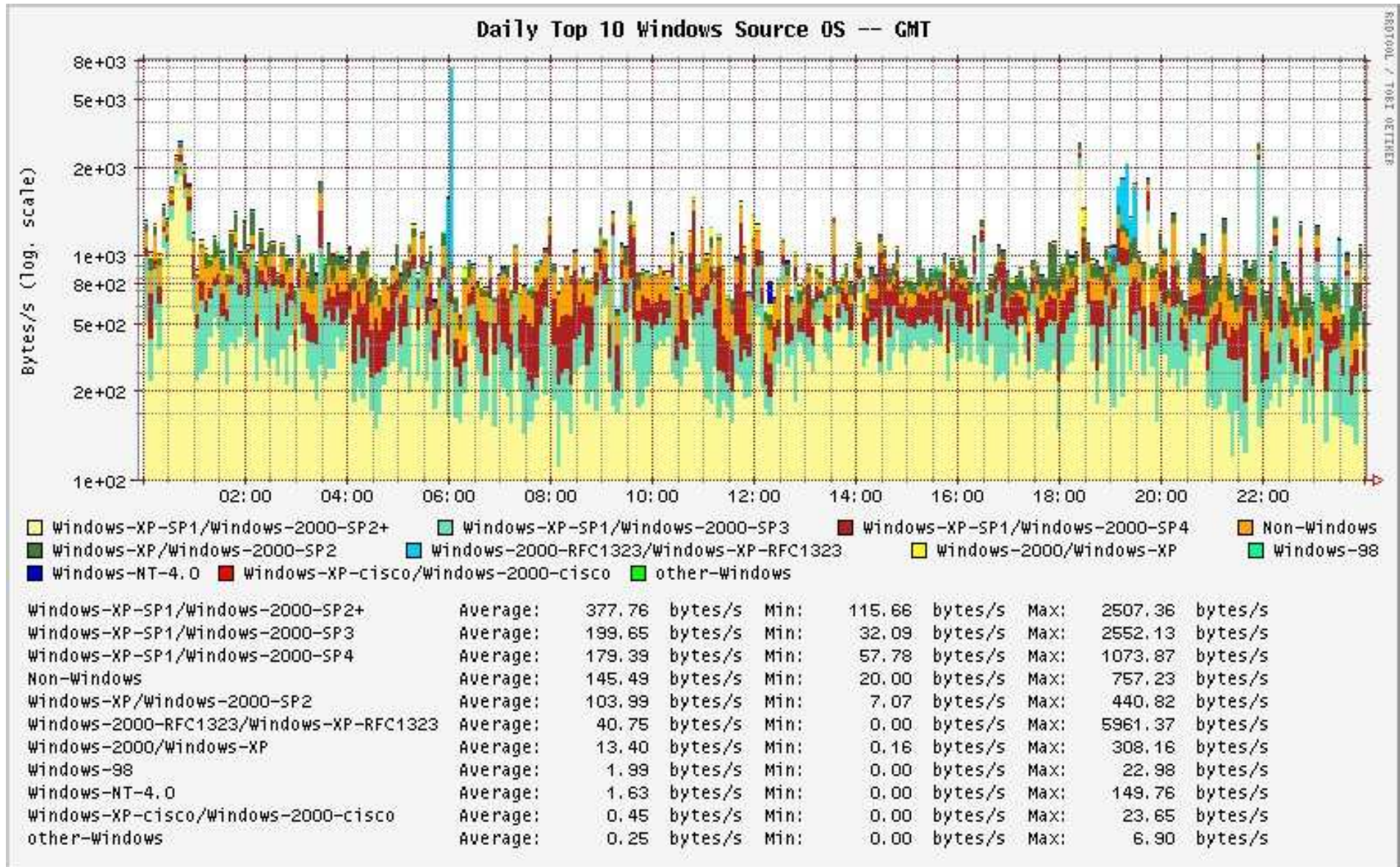


RSR0100L / T081-021101R

# Public Statistics – Correlation (cont.)



# 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 than a darknet
- Usually don't catch attacks targeted to production networks
- Need the partners cooperation to maintain and update the honeypots



# Low x High-Interaction Honeypots

|                | Low-Interaction   | High-Interaction |
|----------------|-------------------|------------------|
| Installation   | Easy              | More difficult   |
| Maintenance    | Easy              | Time consuming   |
| Risk           | Low               | High             |
| Need Control   | No                | Yes              |
| Data gathering | Limited           | Extensive        |
| Interaction    | Emulated services | Full control     |

# Future Work

---

## Honeynet.BR

- Implement a 3rd honeynet

## Distributed Honeypots Network

- 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/>
- Honeynet.BR Project  
<http://www.honeynet.org.br/>
- Brazilian Honey Pots 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/>