The Honeynet PROJECT

Distributed Honeypot Deployment in Brazil

Klaus Steding-Jessen
<jessen@cert.br>

CERT.br - http://www.cert.br/
Honeynet.BR - http://www.honeynet.org.br/
Brazilian Honeypots Alliance - http://www.honeypots-alliance.org.br/

Speaker

Klaus Steding-Jessen
CERT.br Technical Manager

- Involved with honeypots and honeynets' research since 2001
- Ph.D. student at the Brazilian National Institute for Space Research (INPE)
- Co-author of chkrootkit tool
- CERT®-Certified Computer Security Incident Handler, and Instructor of SEI/CMU CERT®/CC Courses

About CERT.br

- Brazilian National CERT, created in 1997
- Focal point for security incident handling
- Provide statistics, best practices and training
- Maintained by the Brazilian Internet Steering Committee
  - composed of 21 members, as follows:

Sector	Representatives	Number
Federal Government	Ministries of Science and Technology, Communications, Defense, Industry, Presidential Cabinet, Telecom Regulatory Agency (ANATEL), among others.	9
Corporate Sector	Industry, Telcos, ISPs, etc.	4
NGO's	Non-profit organizations, etc	4
Sci. & Tech. Community	Academia	3
	Internet Expert	1

About Honeynet.BR

- March/2002: first honeynet deployed
- June/2002: joined the Honeynet Research Alliance
- September/2003: Started the “Brazilian Honeypots Alliance - Distributed Honeypots Project”

Agenda

- Motivation
- The Project
  - Architecture
  - Partners
  - Requirements
- Statistics
- Data usage
- Advantages and disadvantages
- Future work

Motivation

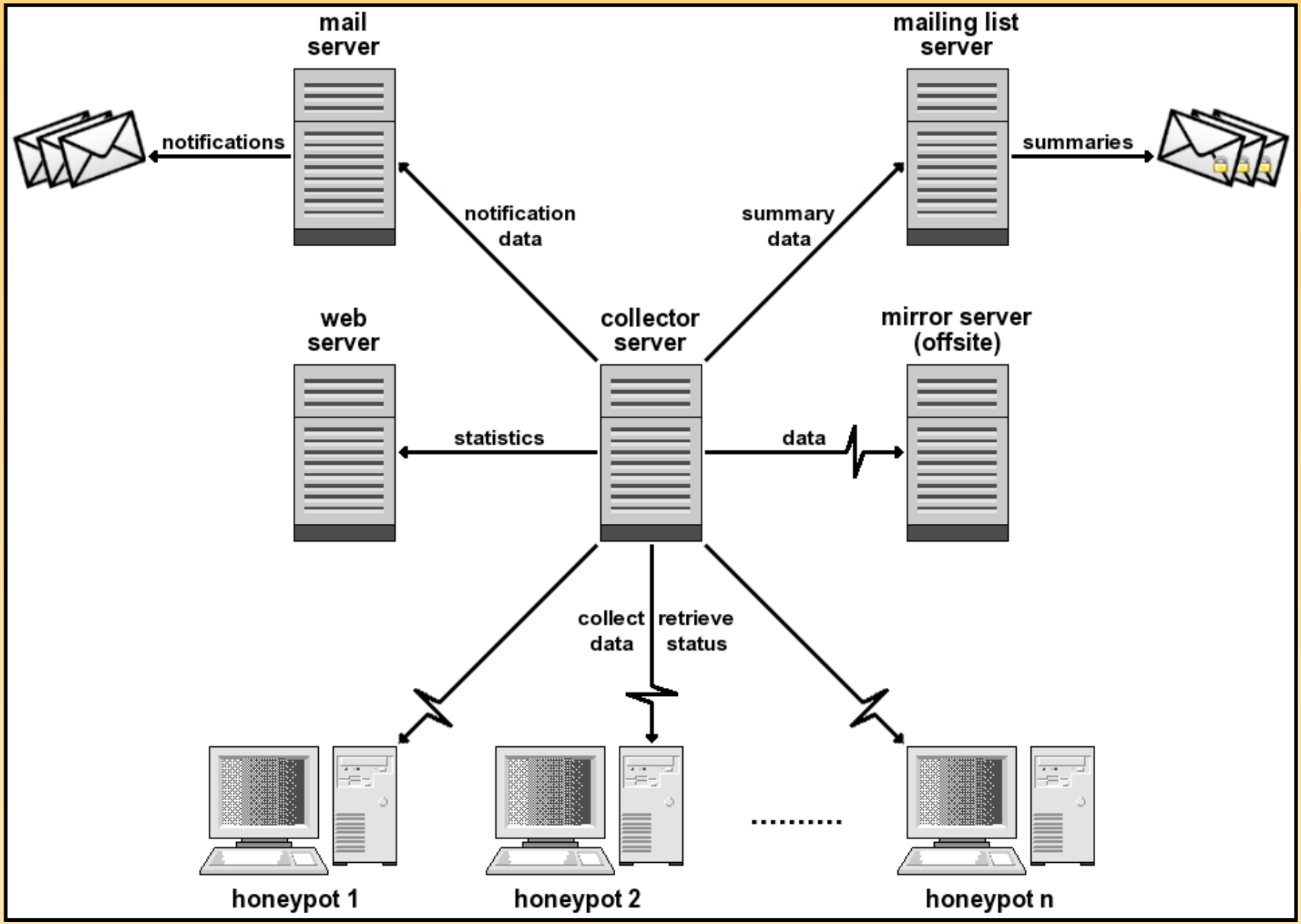
- Increase, in Brazil, the capacity of:
  - incident detection
  - event correlation
  - trend analysis
- Sensors widely distributed across the country
  - In several ASNs and locations
- Useful for Incident Response

The Project

Brazilian Honeypots Alliance
Distributed Honeypots Project

- Coordination: CERT.br and CenPRA Research Center
- Use of low interaction honeypots
- Based on voluntary work of research partners

Architecture



Low Interaction Honeypots

- OpenBSD as the base Operating System (OS)
- Honeyd
  - Emulates different OSs
  - Runs listeners to emulate services (IIS, ssh, sendmail, etc)
- Proxy arp using `arpd`
- Payload logged using `pf`
- Use a netblock range (from /28 to /24)
  - 1 management IP
  - Other IPs are used to emulate the different OSs and services

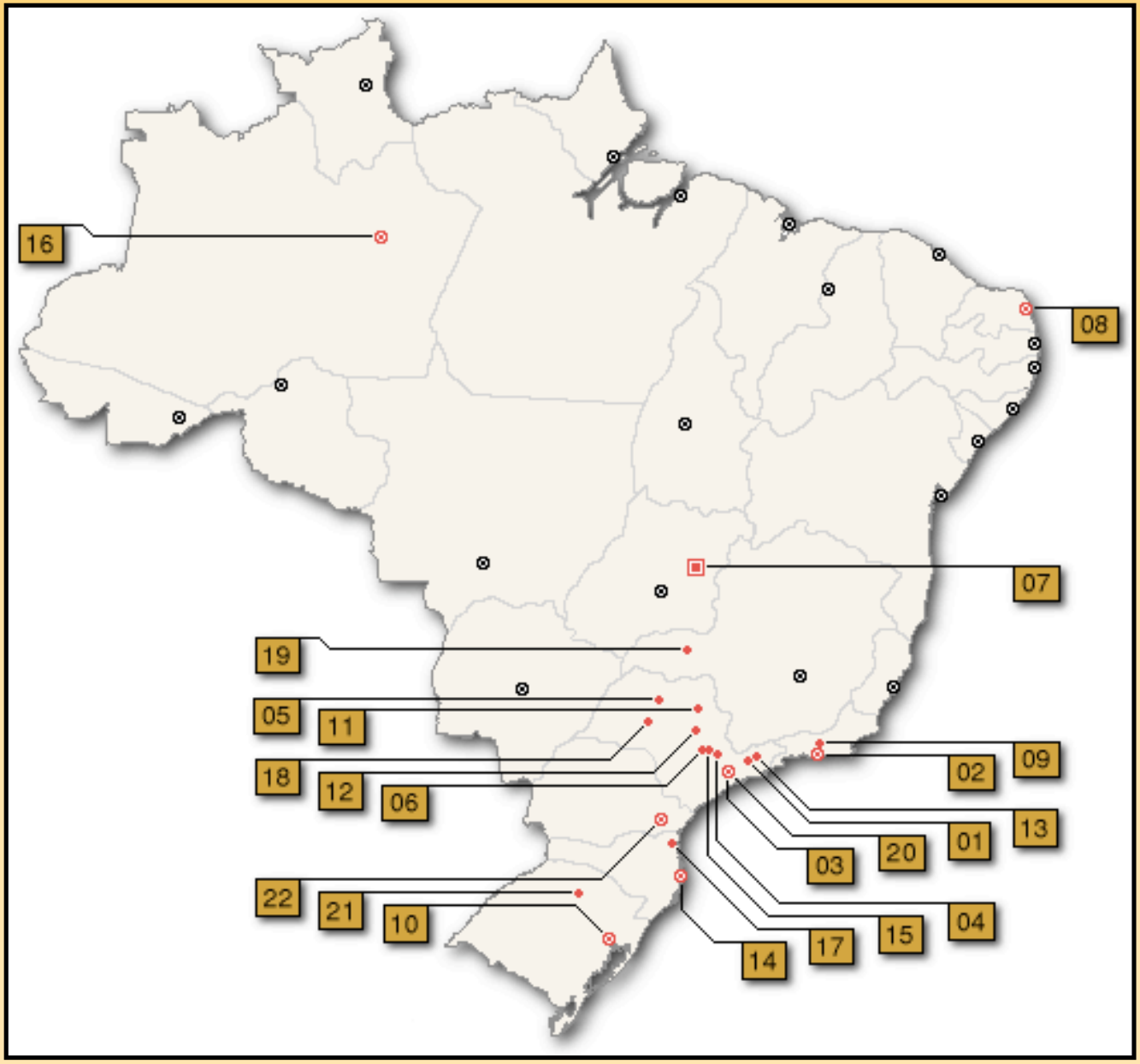
Collector Server

- Collects and stores network raw data from the honeypots
  - Initiates the transfers through ssh connections
- Performs status checks in all honeypots
  - Daemons, ntp, disk space, etc.
- Transfers the processed statistics to the web server
- Produces the notification e-mails
- All data is copied to the offsite mirror

Partners

- 34 research partner's institutions
  - Industry, telcos, academic, government and military networks
- They follow the project's policies and procedures
- Each partner provide:
  - Hardware and network
  - Honeypot(s) maintenance
- Coordination need to know and approve the institutions before they join the project

Partners (cont)



Partners (cont)

#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, USP
04	Campinas	CenPRA, HP Brazil, ITAL, 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
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	PoP-PR

Requirements

- Follow the project's standards (OS, basic secure configuration, updates, etc)
- No data pollution
- Permit all traffic to/from the honeypot
- Don't disclose IP/network
  - All network and IP information must be sanitized
- Don't collect production traffic
- Don't exchange any information in clear text

Members Only Statistics

- Summaries from each honeypot
  - Total packets
  - UDP/TCP/ICMP/Other packets
  - Size of raw captured data
  - Top countries, based on IP allocation
  - Most active OSs, IPs and ports
- A summary from all honeypots combined
- Correlated activities
  - Ports and IPs seen in more than 30% of the honeypots

Members Only Statistics (cont)

- Sample numbers from 1 day summary

Total packets	4,490,094
Raw data size	129.3MB (compressed)

Protocol	Number of Packets	Unique IPs
TCP	3,799,163 (84.61%)	14,680
UDP	584,413 (13.02%)	8,001
ICMP	72,042 (01.60%)	7,017
Other	34,476 (00.77%)	

Public Statistics

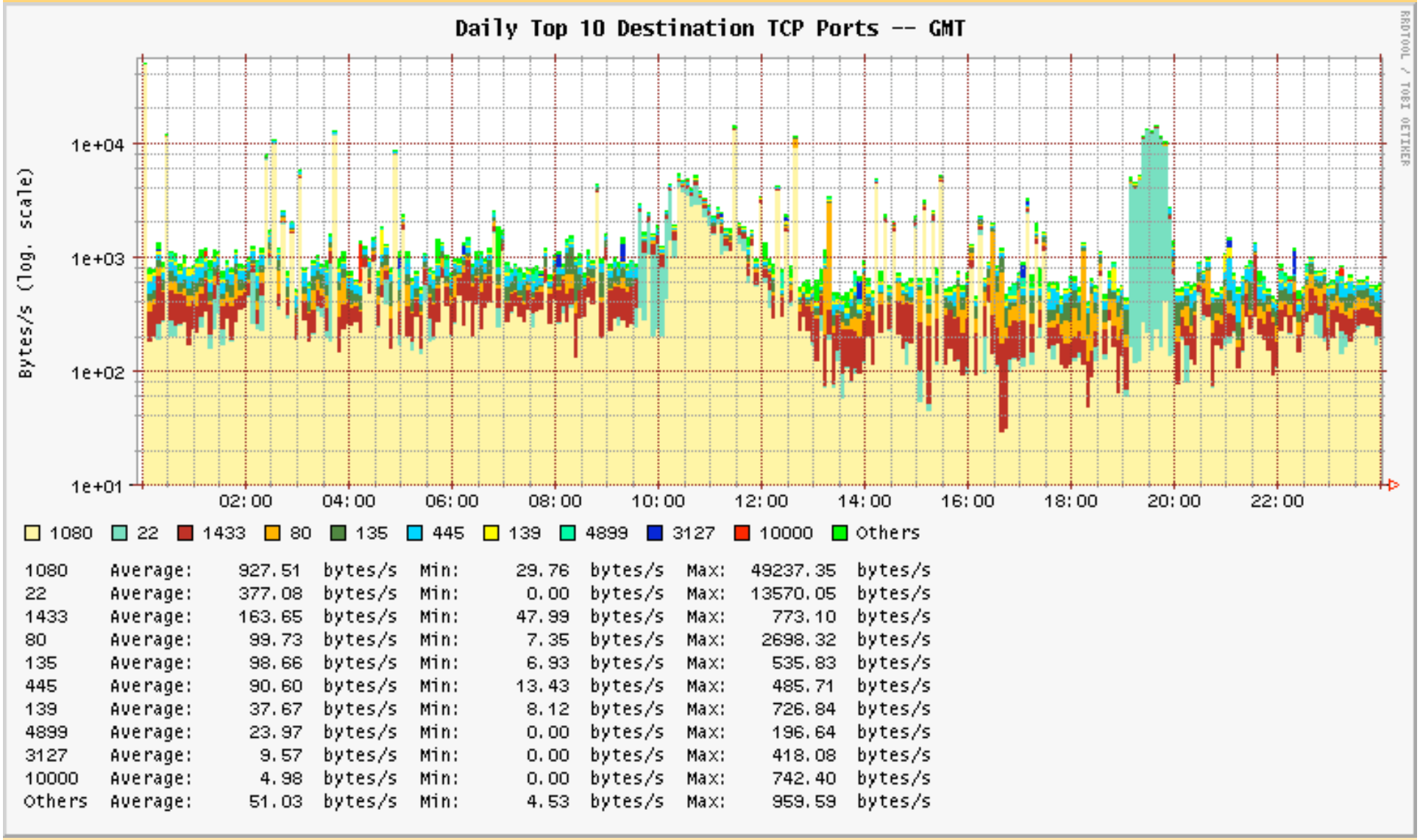
- Flows from data collected in all honeypots
- Most active OSs, TCP/UDP ports and countries
  - Packets/s and bytes/s
  - Daily and 4-hour periods
- Available at:

  http://www.honeypots-alliance.org.br/stats/

Public Statistics Generation

- Convert raw network data into flow data
- Compute the amount of bytes/packets received by each port, OS and country
- Select the top 10 to plot
- Use RRDtool and ORCA to generate the flows' graphics

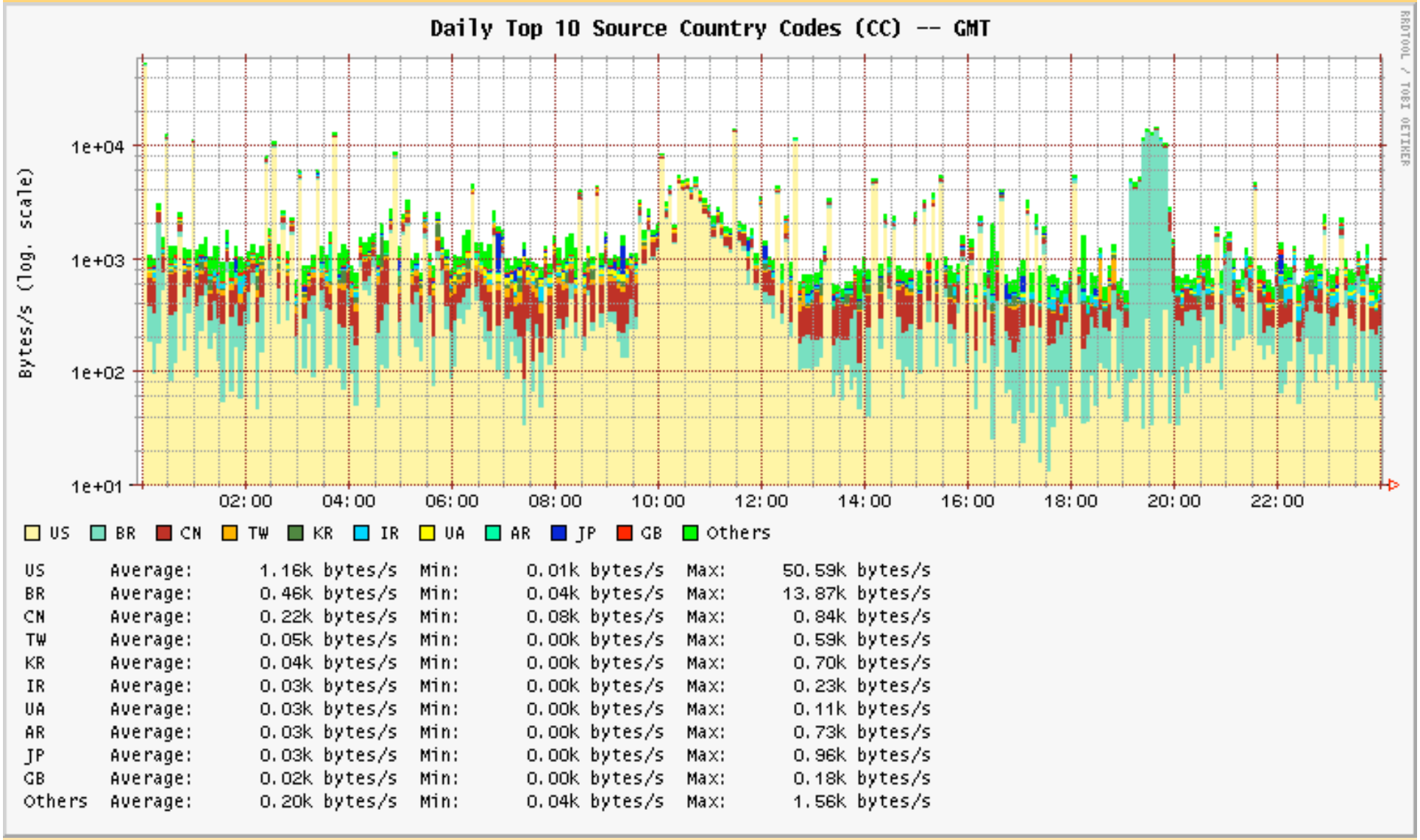
Public Statistics - Top TCP Ports



1080	Average:	927.51	bytes/s	Min:	29.76	bytes/s	Max:	49237.35	bytes/s
22	Average:	377.08	bytes/s	Min:	0.00	bytes/s	Max:	13570.05	bytes/s
1433	Average:	163.65	bytes/s	Min:	47.99	bytes/s	Max:	773.10	bytes/s
80	Average:	99.73	bytes/s	Min:	7.35	bytes/s	Max:	2698.32	bytes/s
135	Average:	98.66	bytes/s	Min:	6.93	bytes/s	Max:	535.83	bytes/s
445	Average:	90.60	bytes/s	Min:	13.43	bytes/s	Max:	485.71	bytes/s
139	Average:	37.67	bytes/s	Min:	8.12	bytes/s	Max:	726.84	bytes/s
4899	Average:	23.97	bytes/s	Min:	0.00	bytes/s	Max:	196.64	bytes/s
3127	Average:	9.57	bytes/s	Min:	0.00	bytes/s	Max:	418.08	bytes/s
10000	Average:	4.98	bytes/s	Min:	0.00	bytes/s	Max:	742.40	bytes/s
Others	Average:	51.03	bytes/s	Min:	4.53	bytes/s	Max:	959.59	bytes/s

THE HONEYNET PROJECT

Public Statistics - Top Countries

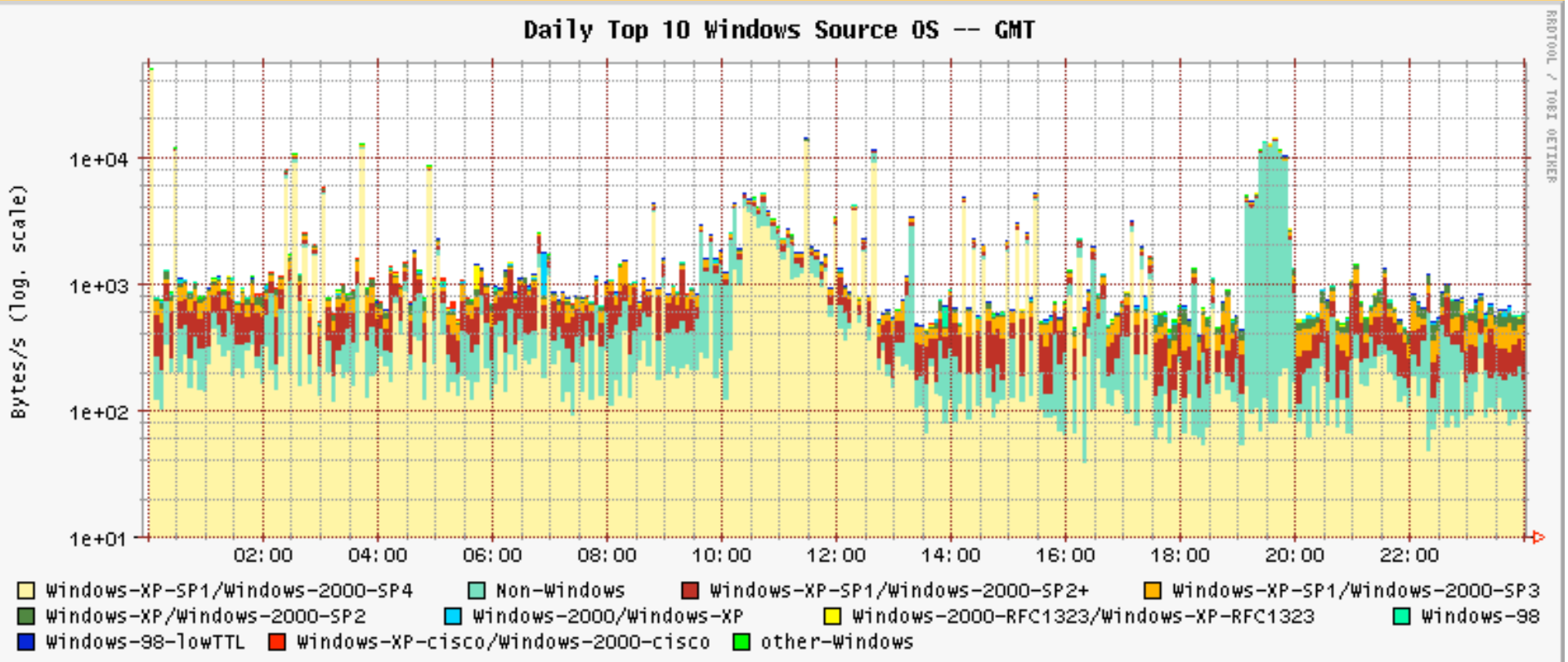


US	Average:	1.16k bytes/s	Min:	0.01k bytes/s	Max:	50.59k bytes/s
BR	Average:	0.46k bytes/s	Min:	0.04k bytes/s	Max:	13.87k bytes/s
CN	Average:	0.22k bytes/s	Min:	0.08k bytes/s	Max:	0.84k bytes/s
TW	Average:	0.05k bytes/s	Min:	0.00k bytes/s	Max:	0.59k bytes/s
KR	Average:	0.04k bytes/s	Min:	0.00k bytes/s	Max:	0.70k bytes/s
IR	Average:	0.03k bytes/s	Min:	0.00k bytes/s	Max:	0.23k bytes/s
UA	Average:	0.03k bytes/s	Min:	0.00k bytes/s	Max:	0.11k bytes/s
AR	Average:	0.03k bytes/s	Min:	0.00k bytes/s	Max:	0.73k bytes/s
JP	Average:	0.03k bytes/s	Min:	0.00k bytes/s	Max:	0.96k bytes/s
GB	Average:	0.02k bytes/s	Min:	0.00k bytes/s	Max:	0.18k bytes/s
Others	Average:	0.20k bytes/s	Min:	0.04k bytes/s	Max:	1.56k bytes/s

February 25, 2006

THE HONEYNET PROJECT

Public Statistics - Top Source OS



Windows-XP-SP1/Windows-2000-SP4	Average:	886.40	bytes/s	Min:	38.67	bytes/s	Max:	49230.33 bytes/s
Non-Windows	Average:	546.90	bytes/s	Min:	28.78	bytes/s	Max:	13634.95 bytes/s
Windows-XP-SP1/Windows-2000-SP2+	Average:	233.67	bytes/s	Min:	80.26	bytes/s	Max:	914.53 bytes/s
Windows-XP-SP1/Windows-2000-SP3	Average:	130.63	bytes/s	Min:	31.23	bytes/s	Max:	505.75 bytes/s
Windows-XP/Windows-2000-SP2	Average:	53.58	bytes/s	Min:	0.80	bytes/s	Max:	202.97 bytes/s
Windows-2000/Windows-XP	Average:	9.79	bytes/s	Min:	0.00	bytes/s	Max:	922.19 bytes/s
Windows-2000-RFC1323/Windows-XP-RFC1323	Average:	5.14	bytes/s	Min:	0.00	bytes/s	Max:	486.80 bytes/s
Windows-98	Average:	3.37	bytes/s	Min:	0.00	bytes/s	Max:	194.33 bytes/s
Windows-98-lowTTL	Average:	1.28	bytes/s	Min:	0.00	bytes/s	Max:	118.24 bytes/s
Windows-XP-cisco/Windows-2000-cisco	Average:	0.56	bytes/s	Min:	0.00	bytes/s	Max:	61.53 bytes/s
other-Windows	Average:	0.61	bytes/s	Min:	0.00	bytes/s	Max:	30.39 bytes/s

Data Usage

- Partners:
  - Observe trends and scans for new vulnerabilities
  - Detect promptly:
    - Outbreaks of new worms/bots
    - Compromised servers
    - Network configuration errors
- Incident response (CERT.br):
  - Identify well known malicious/abuse activities
    - Worms, bots, scans, spams and malware in general
  - Notify the Brazilian networks' contacts
    - including recovery tips

Advantages

- Few false positives
- Ability to collect malware samples
  - Listeners developed for: mydoom, kuang, subseven, socks, ssh, etc.
- Ability to implement spam traps
- Allow members to improve their expertise in several areas:
  - Honeypots, intrusion detection, firewalls, OS hardening, PGP, etc
- Low cost and low risk

Disadvantages

- Usually don’t catch attacks targeted to production networks
- Rely on partners’ cooperation to maintain and update the honeypots
- Information gathered is limited compared to high interaction honeypots
- The project becomes more difficult to manage as the number of honeypots grow

Future Work

- Continuously expand the network
  - 3 new partners in installation phase
  - 10 partner candidates
- Have more public statistics:
  - Monthly, weekly and hourly
- Invest more in spam traps

Related links

- Brazilian Honeypots Alliance - Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/
- Honeynet.BR
  http://www.honeynet.org.br/
- Honeynet Research Alliance
  http://www.honeynet.org/alliance/
- Honeyd
  http://www.honeyd.org/
- CERT.br
  http://www.cert.br/
- Brazilian Internet Steering Committee
  http://www.cgi.br/