Distributed Honeypots Network Implementation based on OpenBSD and Free Software Tools

Marcelo H. P. C. Chaves

mhp@cert.br

CERT.br – Computer Emergency Response Team Brazil

NIC.br – Network Information Center Brazil

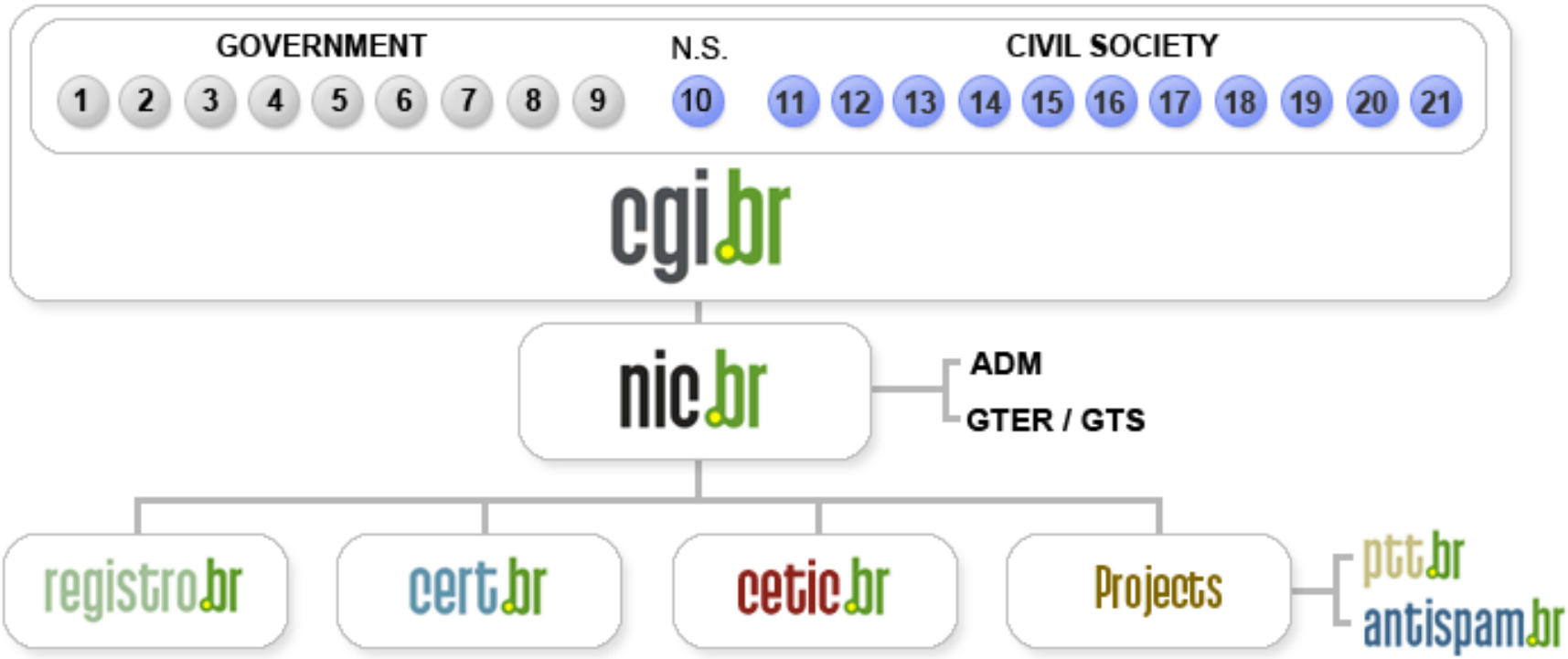
CGI.br – Brazilian Internet Steering Committee

Our Parent Organization: CGI.br

Among the diverse responsibilities of The Brazilian Internet Steering Committee – CGI.br, the main attributions are:

- to propose policies and procedures related to the regulation of the Internet activities
- to recommend standards for technical and operational procedures
- 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 Structure



01- Ministry of Science and Technology
02- Ministry of Communications
03- Presidential Cabinet
04- Ministry of Defense
05- Ministry of Development, Industry and Foreign Trade
06- Ministry of Planning, Budget and Management
07- National Telecommunications Agency
08- National Council of Scientific and Technological Development
09- National Forum of Estate Science and Technology Secretaries
10- Internet Expert

11- Internet Service Providers
12- Telecommunication Infrastructure Providers
13- Hardware and Software Industries
14- General Business Sector Users
15- Non-governamental Entity
16- Non-governamental Entity
17- Non-governamental Entity
18- Non-governamental Entity
19- Academia
20- Academia
21- Academia

About CERT.br

Created in 1997 to receive, review and respond to computer security incident reports and activities related to networks connected to the Internet in Brazil.

- National focal point for reporting security incidents
- Establishes collaborative relationships with other entities
- Helps new CSIRTs to establish their activities
- Provides training in incident handling
- Provides statistics and best practices' documents
- Helps raise the security awareness in the country

http://www.cert.br/mission.html

Agenda

- Timeline
- Motivation
- The Project
  - Architecture
  - Partners
  - Requirements
- Statistics and Data Usage
- Challenges to Build and Maintain the Network
- Benefits and Disavantages
- Future Work
- References

Timeline

- March/2002
  - Honeynet.BR project first honeynet deployed
- June/2002
  - Joined the Honeynet Research Alliance
- September/2003
  - The “Brazilian Honeypots Alliance – Distributed Honeypots Project” was started

Motivation

- Increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet
- Sensors widely distributed across the country
  - in several ASNs and locations
- Useful for incident response

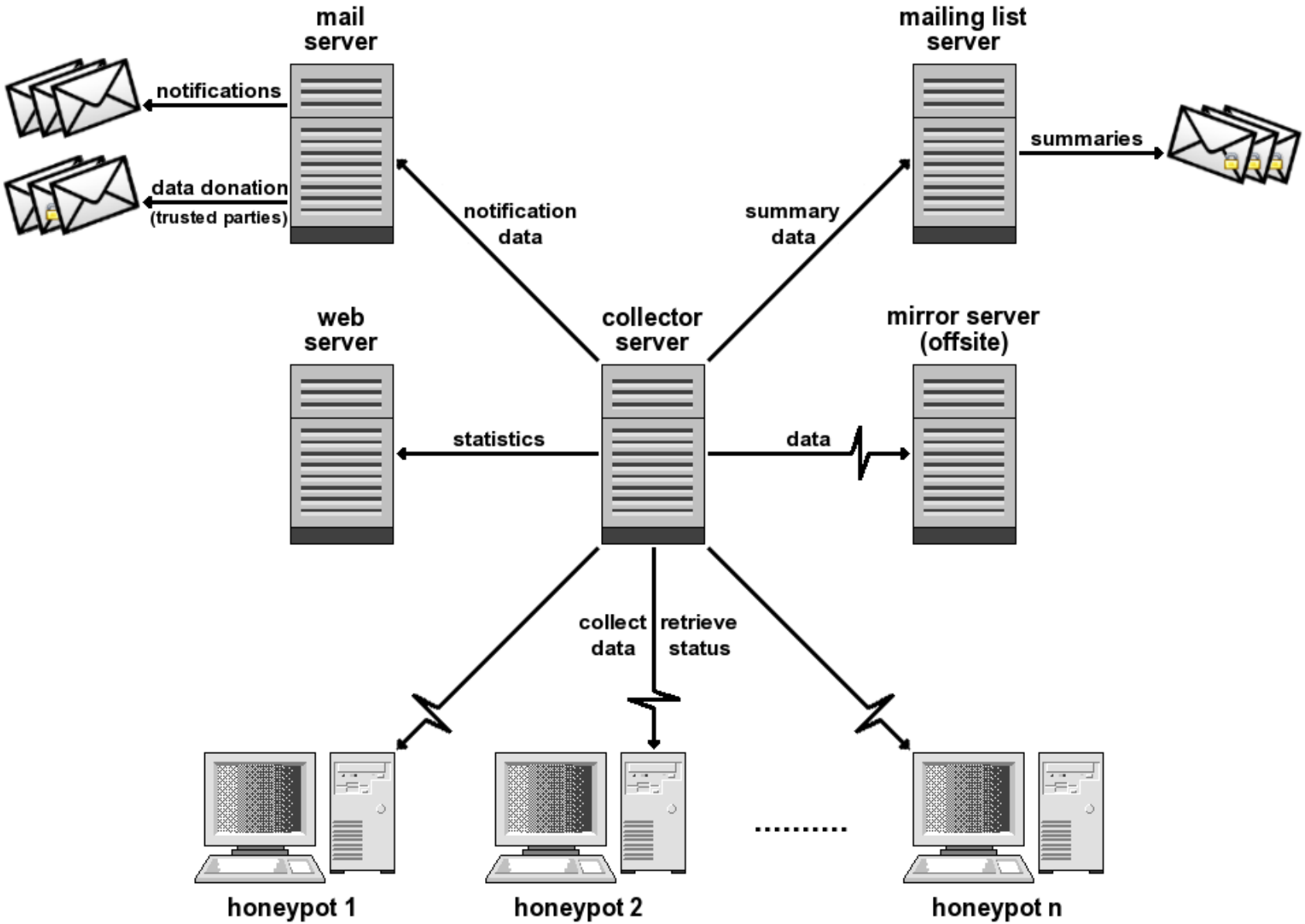
The Project

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)
  - familiarity
  - number of security holes is extremely low, if compared with other operating systems
  - good proactive security features
    - W^X, ProPolice, systrace, random lib loading order
  - well-defined upgrade cicle (twice a year)
  - runs in multiple architectures
    - i386, sparc, sparc64, amd64, etc
  - one of the best available free packet filters
    - stateful, redundancy, integrated queueing (ALTQ), etc
  - firewall logs in `libpcap` format

http://www.openbsd.org/

Low Interaction Honeypots (2)

- **Honeyd** - http://www.honeyd.org/
  - Emulates different OSs
  - Runs listeners to emulate services (`IIS`, `ssh`, `sendmail`, etc)
- **Arpd** - http://www.honeyd.org/tools.php
  - Proxy arp using a netblock range (from /28 to /21)
  - 1 management IP
  - Other IPs are used to emulate different OSs and services
- OpenBSD **pf** - http://www.openbsd.org/faq/pf/
  - Network traffic logging (including payload)
  - libpcap format

Collector Server

- Collects and stores network raw data from honeypots
  - initiates transfers through ssh connections
    openssh - `http://www.openssh.org/`
- Performs status checks in all honeypots
  - daemons, ntp, disk space, etc
- Transfers the processed statistics to the web server
- Produces the notification e-mails
  - tools used: `make`, `sh`, `perl`, `tcpdump`, `ngrep (modified)`, `jwhois`
- All data is copied to the offsite mirror

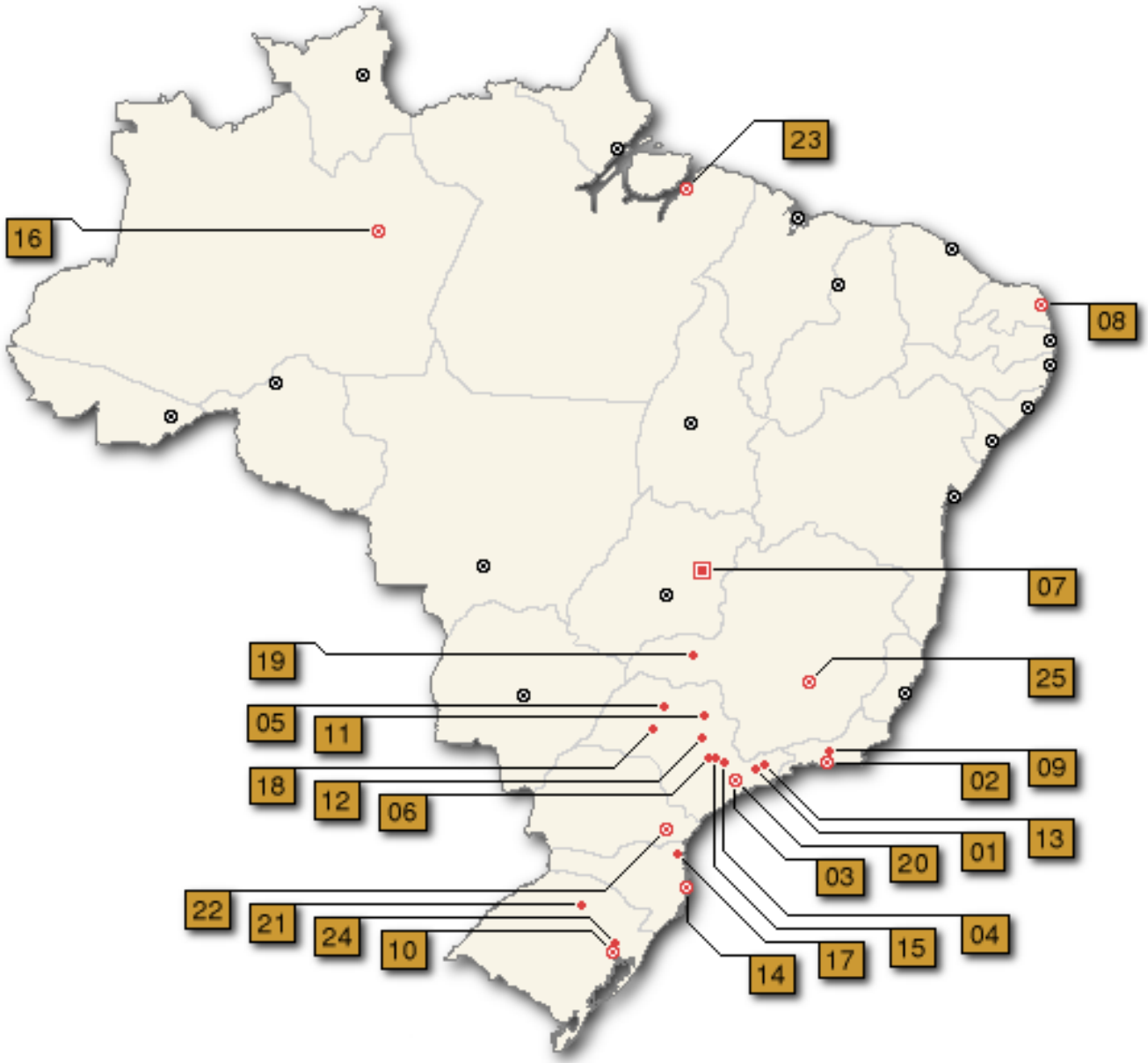
Partners

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

Partner Requirements

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

Cities Where the Honeypots are Located



37 Partners of the Brazilian Honeypots Alliance

#	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, UOL, USP
04	Campinas	CenPRA, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministério da Justiça, 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, PUCPR
23	Belém	UFPA
24	São Leopoldo	Unisinos
25	Belo Horizonte	Diveo

Statistics and Data Usage

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/IPs seen in more than 30% of the honeypots
- Tools used:
  - `sh`, `perl`, `tcpdump (OS fingerprinting)`, `gpg`

Members Only Statistics (2)

- Sample numbers from 1 day summary

Total packets	21,455,939
Raw data size	573.9MB (compressed)

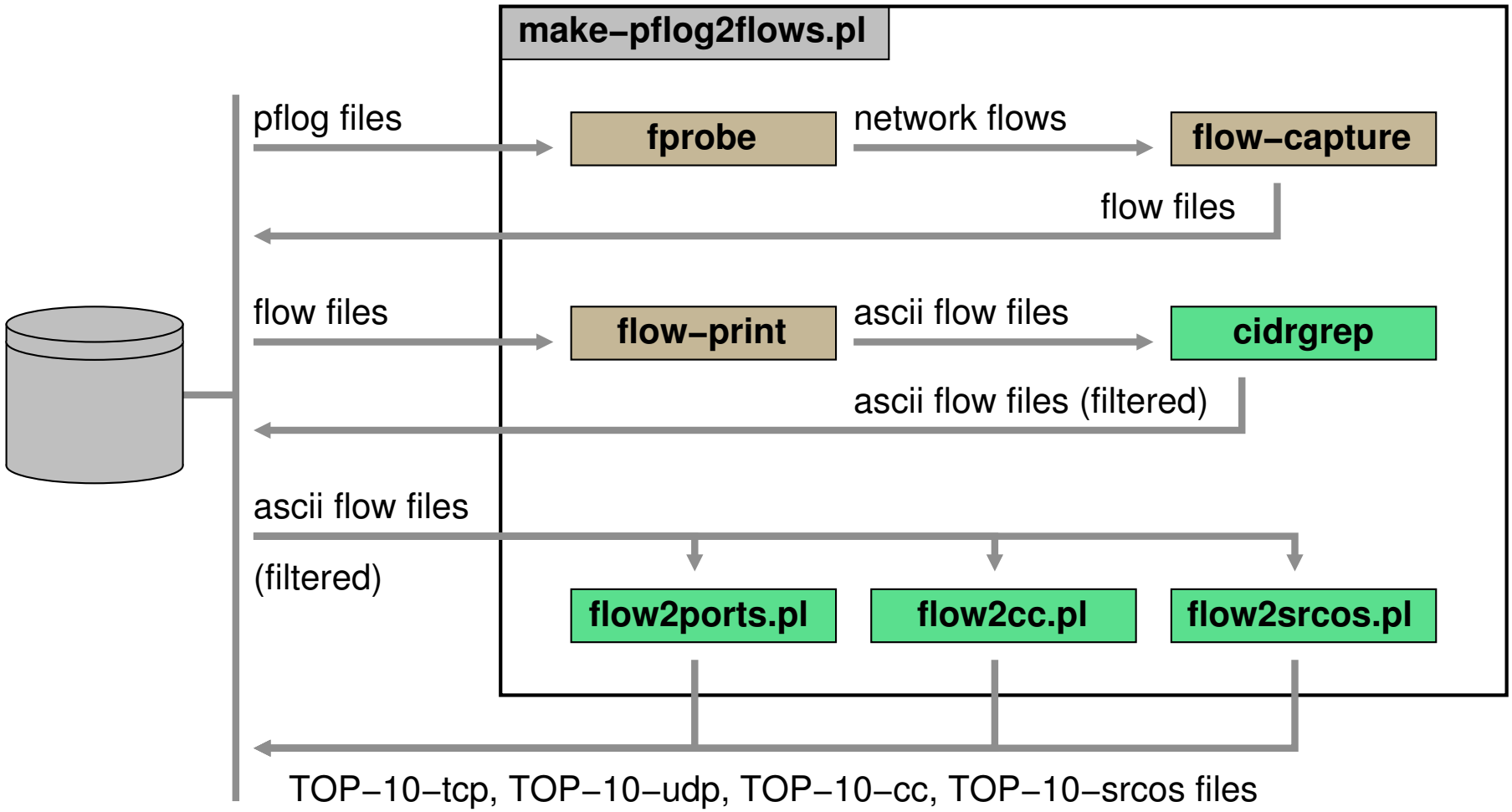
Protocol	Number of Packets	Unique IPs
TCP	20,420,621 (95.17%)	30,802
UDP	240,530 (01.12%)	7,488
ICMP	785,734 (03.66%)	14,712
Others	9,054 (00.04%)	—

Public Statistics

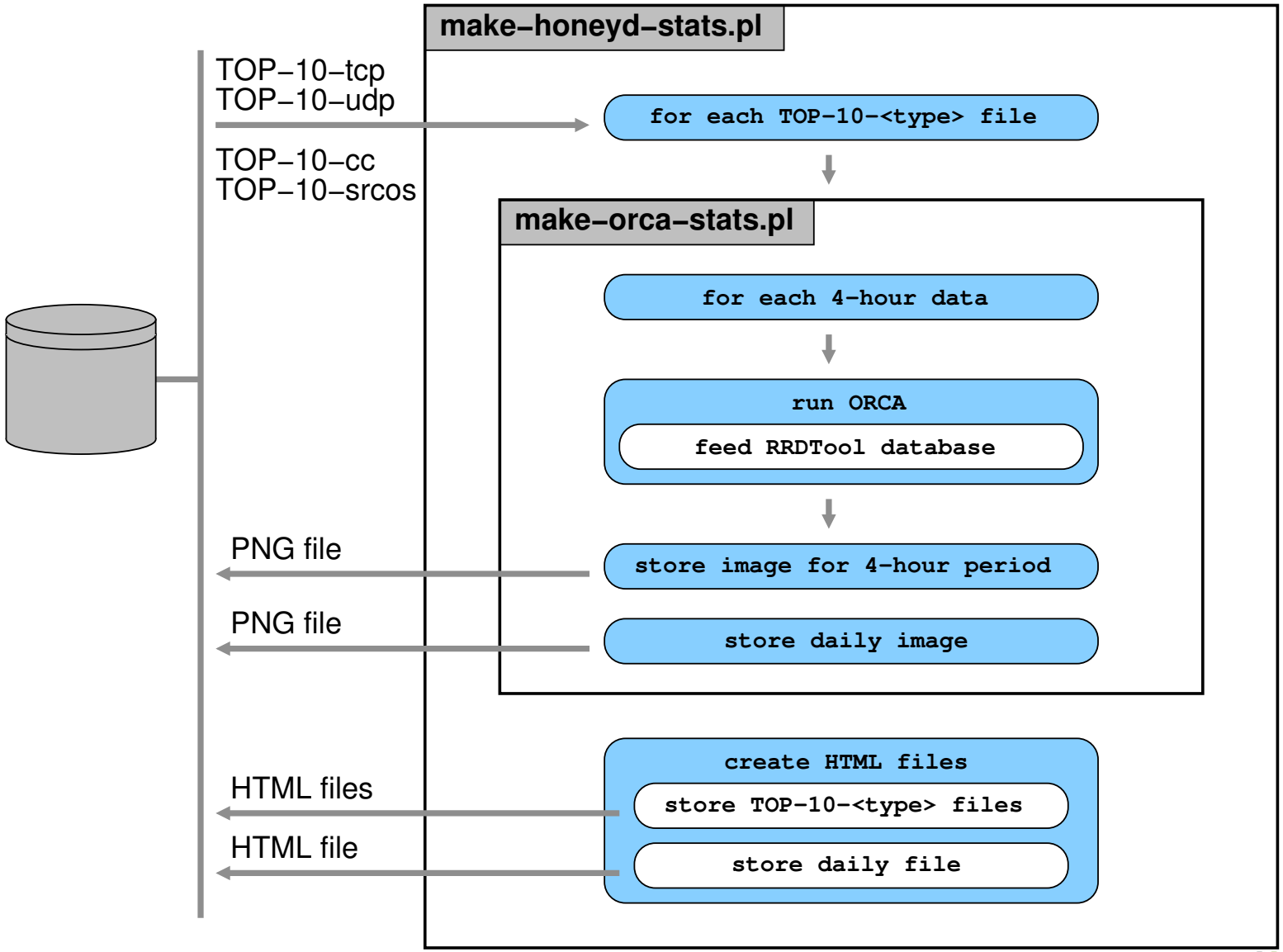
- Flows from data collected in all honeypots
  - Most active OSs, TCP/UDP ports and countries
  - packets/s and bytes/s
  - daily and 4-hour periods
- Tools used:
  - `perl`, `tcpdump (OS fingerprinting)`, `fprobe`, `flow-tools`, `RRDtool`, `Orca`
- Available at:

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

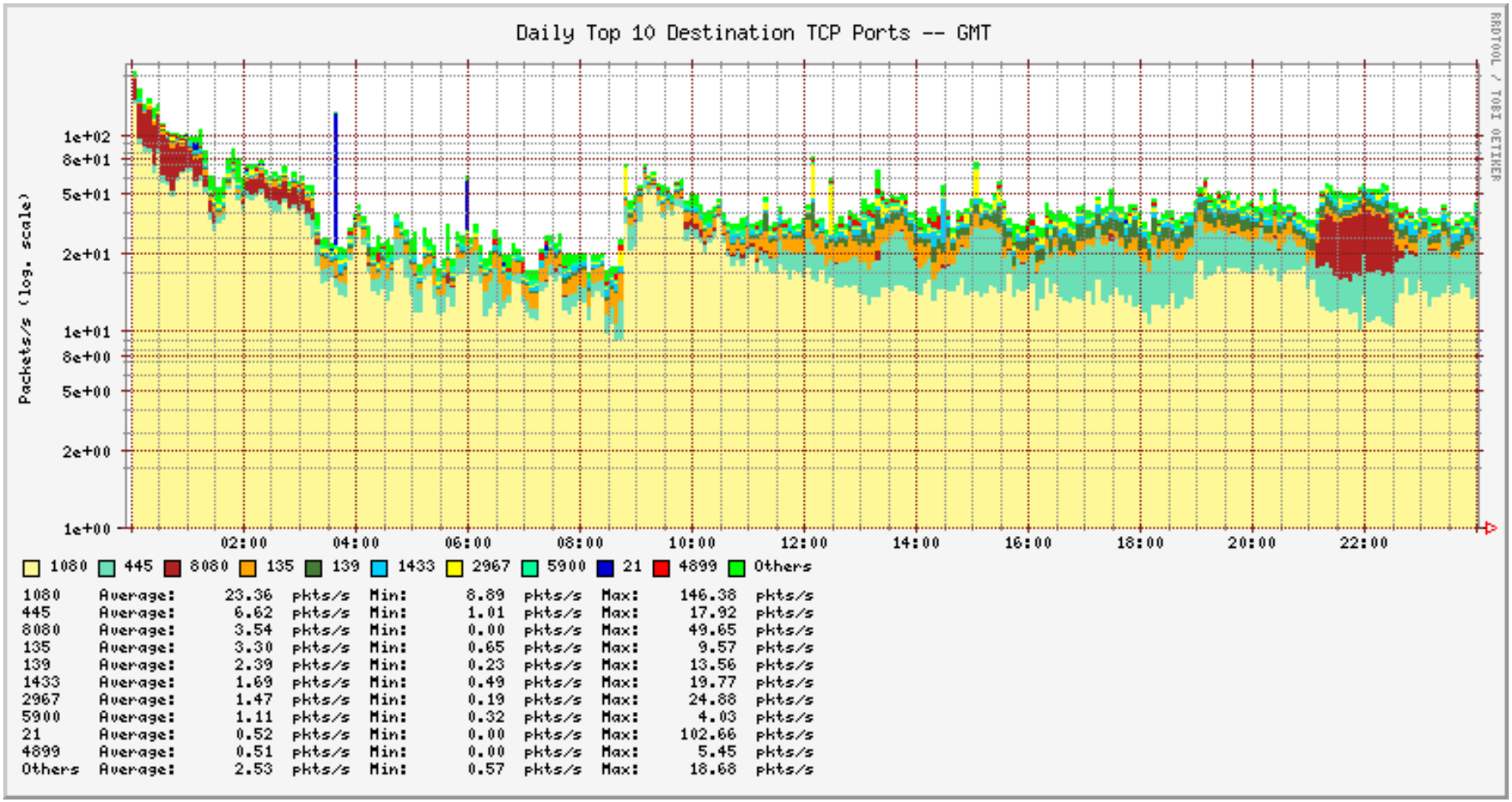
Public Statistics Generation



Public Statistics Generation (2)

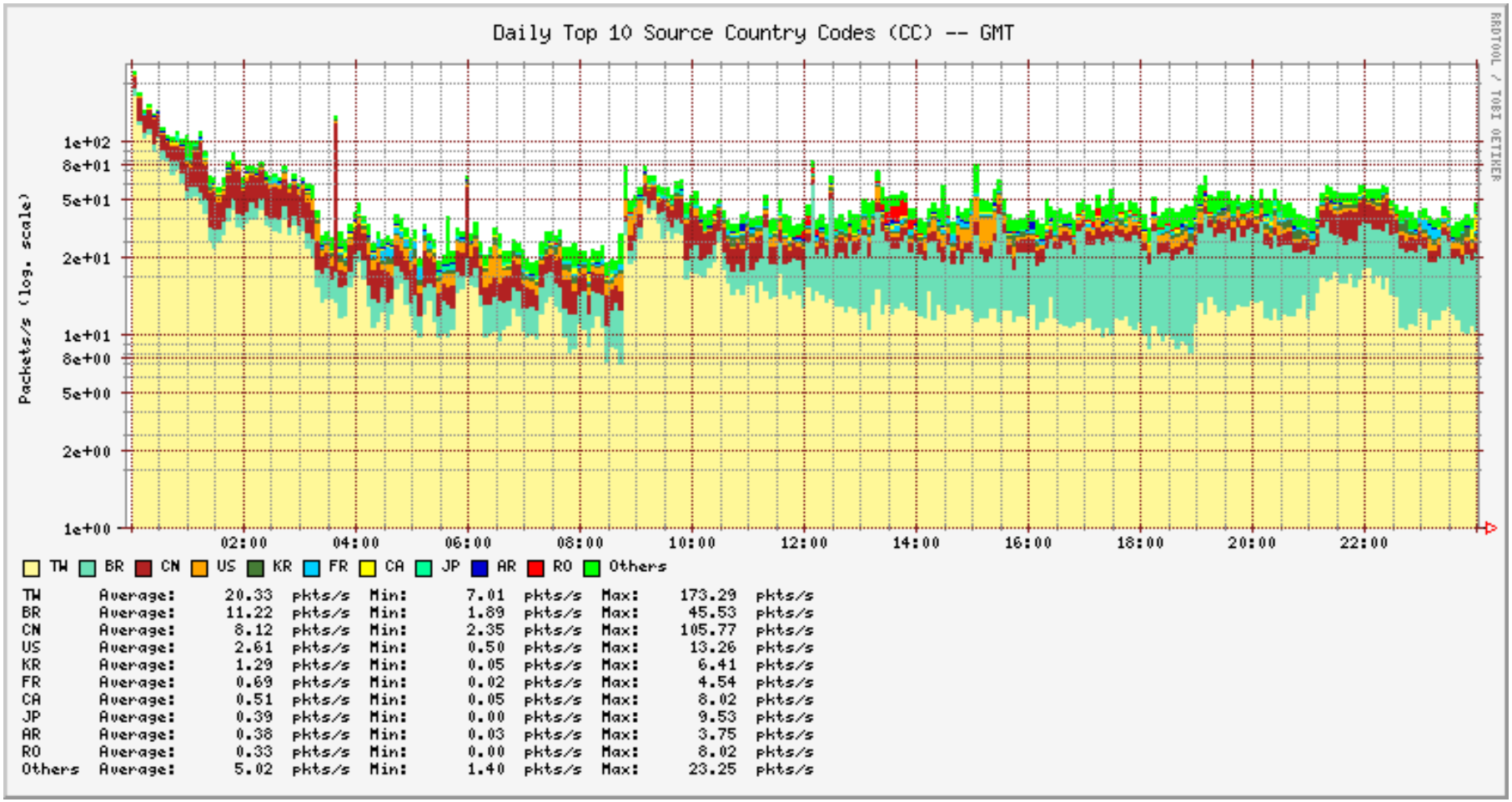


Public Stats (flows): Top TCP Ports



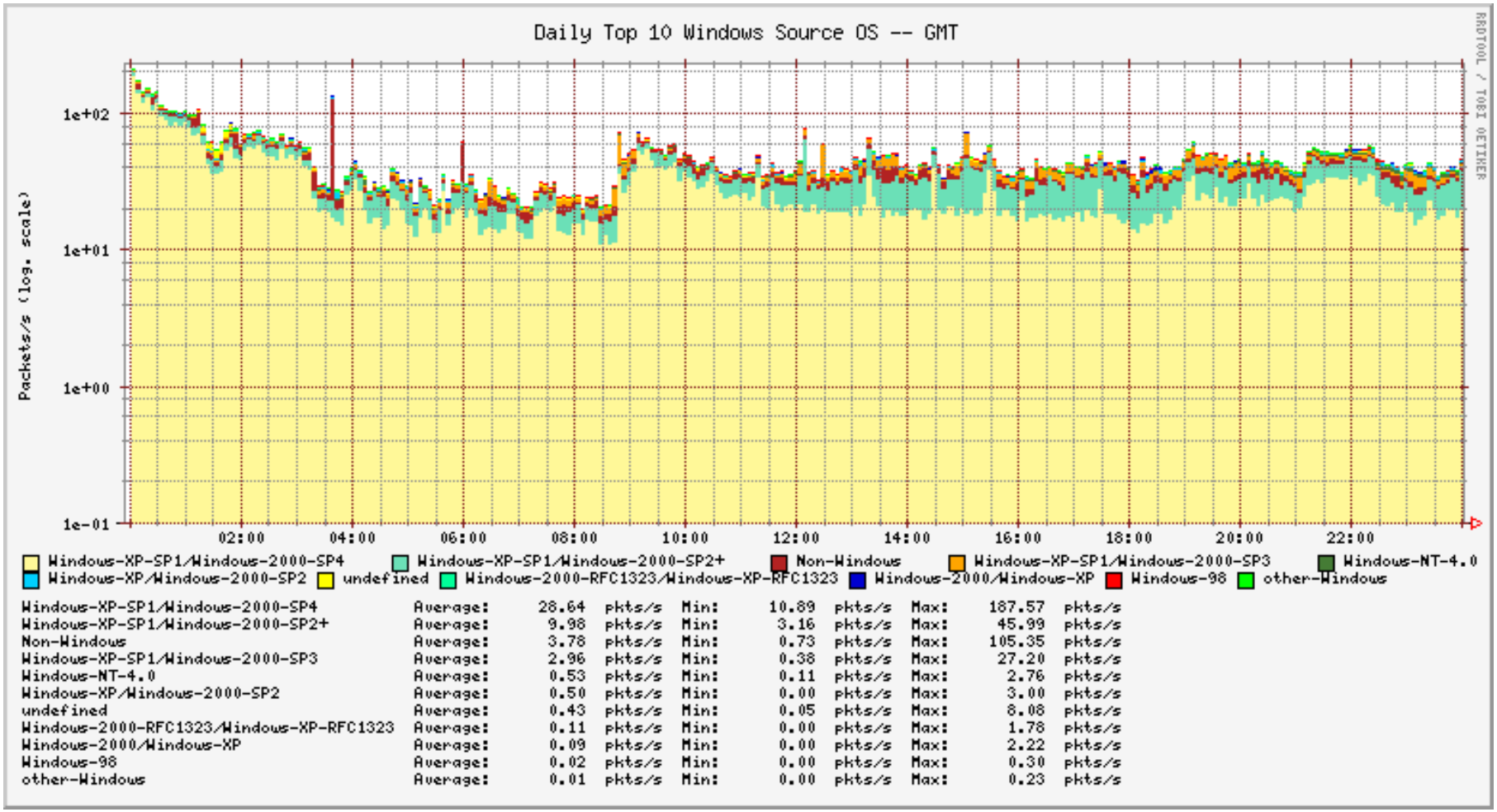
March 29, 2007 – http://www.honeypots-alliance.org.br/stats/

Public Stats (flows): Top CC



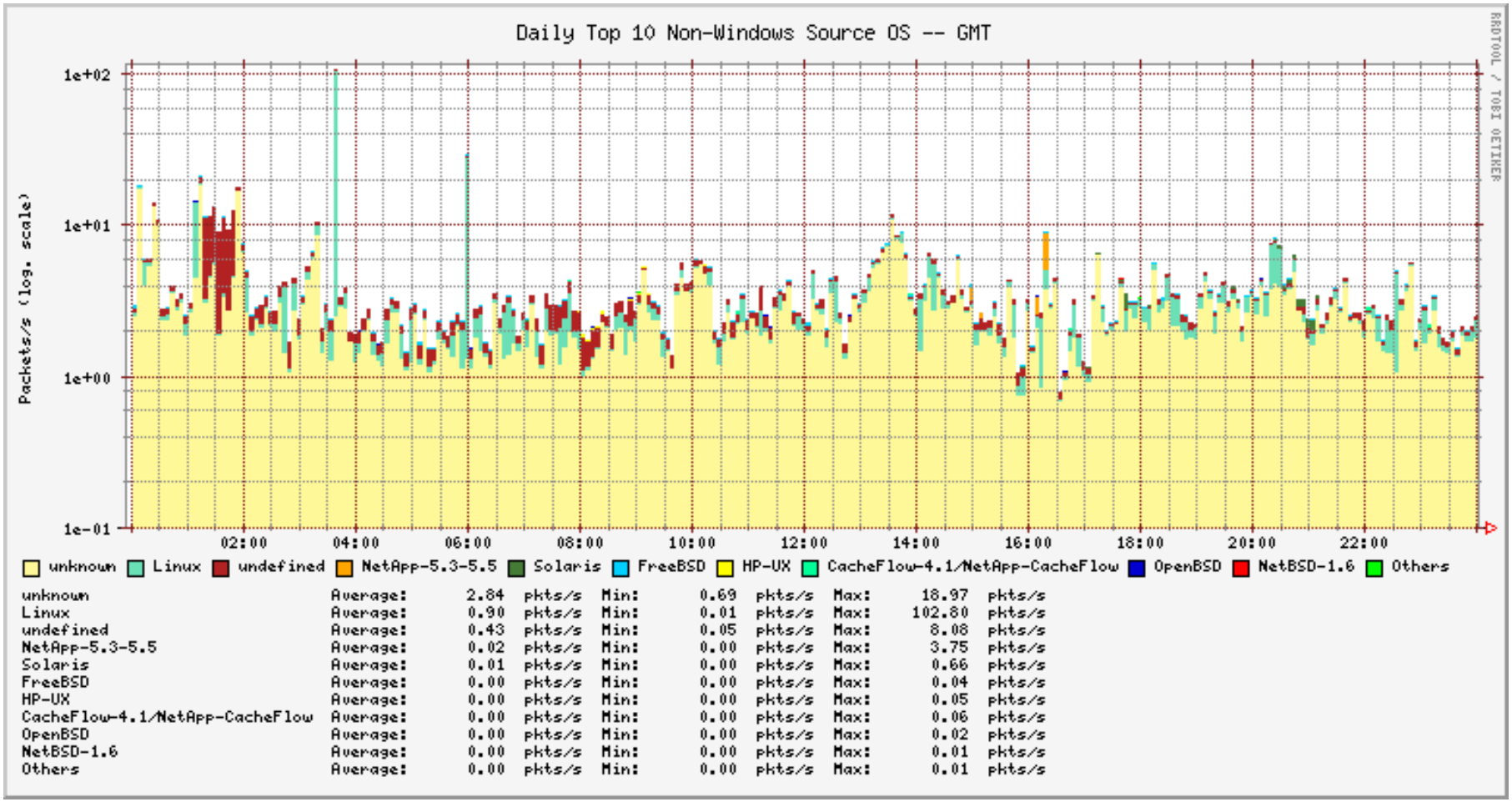
March 29, 2007 – http://www.honeypots-alliance.org.br/stats/

Public Stats (flows): Top Win Src.OS



March 29, 2007 – http://www.honeypots-alliance.org.br/stats/

Public Stats (flows): Top Non-Win Src.OS

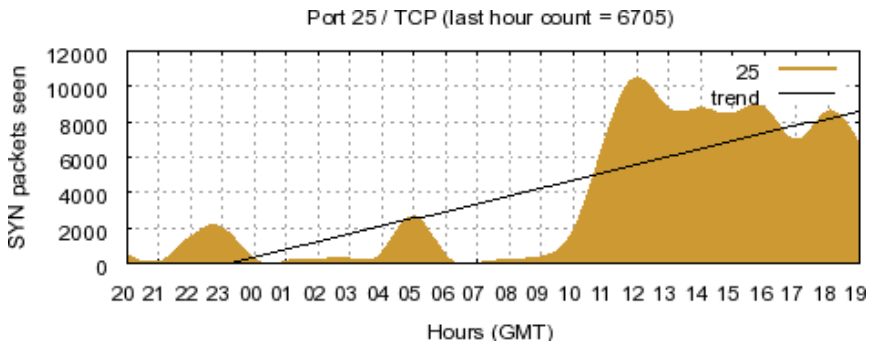


March 29, 2007 – http://www.honeypots-alliance.org.br/stats/

Public Stats: Port summary (future work)

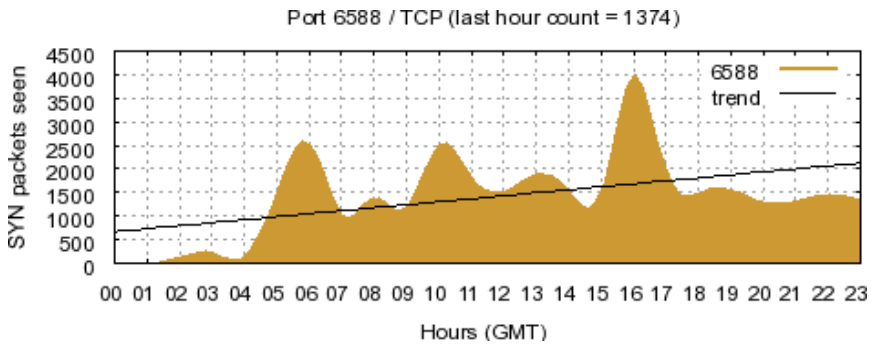
- Hourly

19: 2007-04-08 20:00 – 2007-04-09 19:59 (GMT)



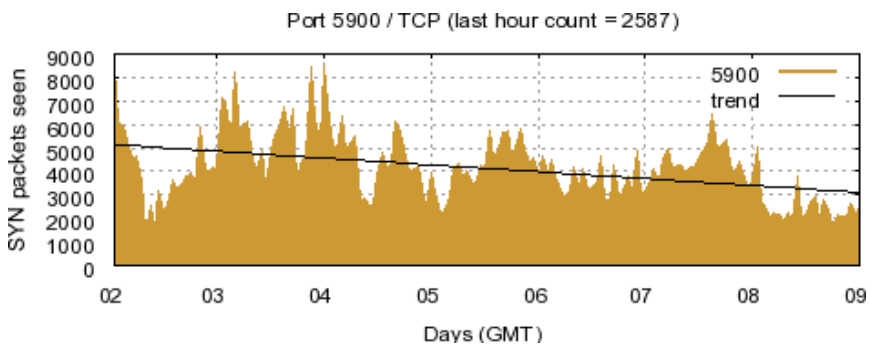
- Daily

08: 2007-04-08 00:00 – 2007-04-08 23:59 (GMT)



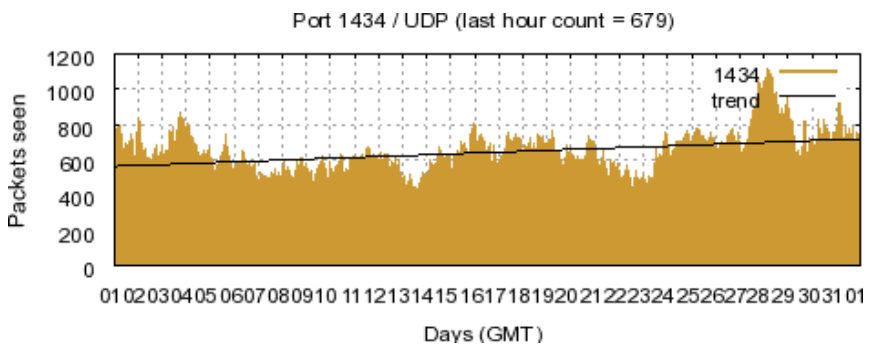
- Weekly

14: 2007-04-02 00:00 – 2007-04-08 23:59 (GMT)



- Monthly

03: 2007-03-01 00:00 – 2007-03-31 23:59 (GMT)



Tools used: `sh`, `perl`, `gnuplot`

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/abusive activities
    - worms, bots, scans, spam and malware in general
  - notify the Brazilian networks' contacts
    - including recovery tips
  - donate colleted data related to other countries to trusted parties

Challenges to Build and Maintain the Network

Challenges to Find Partners

How to find partners

- Other CSIRTs
- Known incident reporters
- Attendees of our courses
- People indicated by trusted partners

After finding them, we have to convince them

- Why they should place a honeypot in their networks
- What are the advantages that they have in sharing the information with us

Key Points to Reach & Keep a Partner

We are not offering a “black box”

- They have access to their honeypots
- They can extend the honeypot configuration

The honeypot does not capture production data

- Only data directed to the honeypot is collected

They can use their data freely

- For example, as a complement to their IDS infrastructures

We provide specific information to partners

- Daily summaries (sanitized) – each, combined, correlated

Info exchanged with an encrypted mailing list

Challenges to Maintain the Project

Depend on partners' cooperation to maintain and update the honeypots

- Harder to maintain than a "plug and play" honeypot

The project becomes more difficult to manage as the number of honeypots grow

- More people to coordinate with
- PGP keys' management issues
- More resources needed (disk space, bandwidth, etc)
- Some honeypots start to present hardware problems

Benefits of the Project and Disavantages of the Architecture

Benefits

Short Term

- Few false positives, low cost and low risk
- Notification of networks that are originating malicious activities, and production of statistics
- Ability to collect malware samples
  - listeners developed for: `mydoom`, `subseven`, `socks`, `ssh`, `etc`.

Long Term

- Allow members to improve their expertise in several areas:
  - honeypots, firewall, OS hardening, PGP, intrusion detection, etc
- Improve CERT.br's relationship with the partners

Disavantages of the Architecture

- Honeypots usually don't catch attacks targeted to production networks
- Information gathered is limited compared to high interaction honeypots

Future Work and References

Future Work

- Continuously expand the network
  - 2 new partners in installation phase
  - 5 partner candidates
- Have more public statistics:
  - monthly, weekly, daily and hourly
- Invest more in spam traps

References

- This presentation can be found at:
  http://www.cert.br/docs/presentations/
- Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/
- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/
- Brazilian Honeypots Alliance – Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/
- Honeynet.BR
  http://www.honeynet.org.br/
- Previous Presentations about the Project
  http://www.honeynet.org.br/presentations/
- Honeypots and Honeynets white paper (in Portuguese)
  http://www.cert.br/docs/whitepapers/honeypots-honeynets/