Honeynets Applied to the CSIRT Scenario

Cristine Hoepers*
Klaus Steding-Jessen*
Antonio Montes, Ph.D.†

*NIC BR Security Office – NBSO
http://www.nbso.nic.br/

†National Institute for Space Research – INPE
http://www.lac.inpe.br/

Overview

- Honeynet.BR objectives
- Timeline
- Topology
- Activities observed
- Usefulness to CSIRTs

Honeynet.BR Objectives

- Monitor current attacks and intrusions
- Collect data
- Develop new tools
- Evaluate the usefulness to CSIRTs

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`)

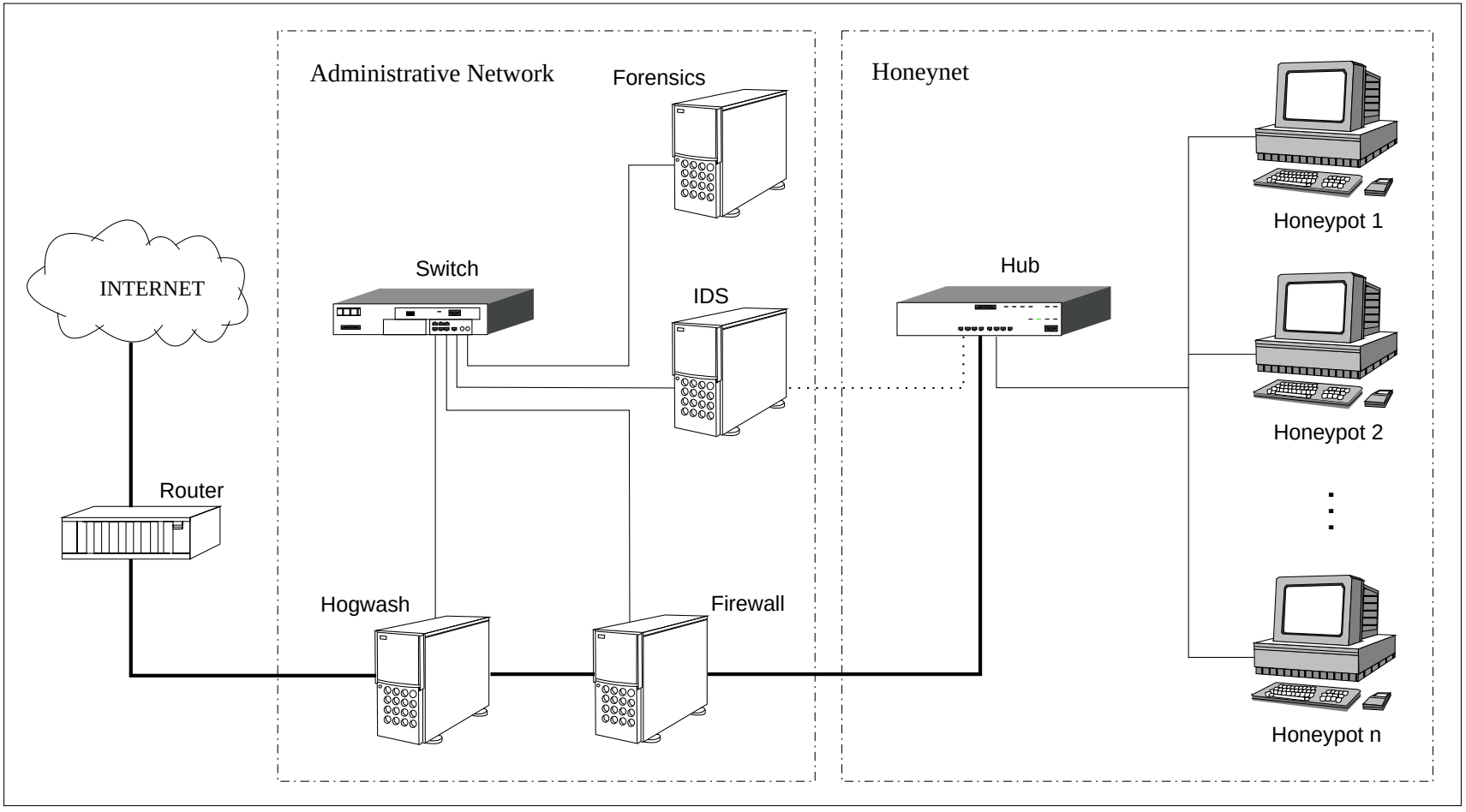
Timeline

- Late 2001: first honeypot experiment
- January-March 2002: topology definition and test phase
- Late March 2002: beginning of operation
- June 2002: joined the Honeynet Research Alliance

Topology

- Administrative Network
  - Firewall
  - Hogwash
  - IDS
  - Forensics
- Honeynet
  - Honeypots

Topology (Cont.)



Data Control

- Firewall rules
- Outgoing Traffic normalization
- `sessionlimit`
  - developed within the project
  - interacts with OpenBSD `pf` blocking outgoing traffic
- Bandwidth limitation
- Outgoing content filter (`hogwash`)

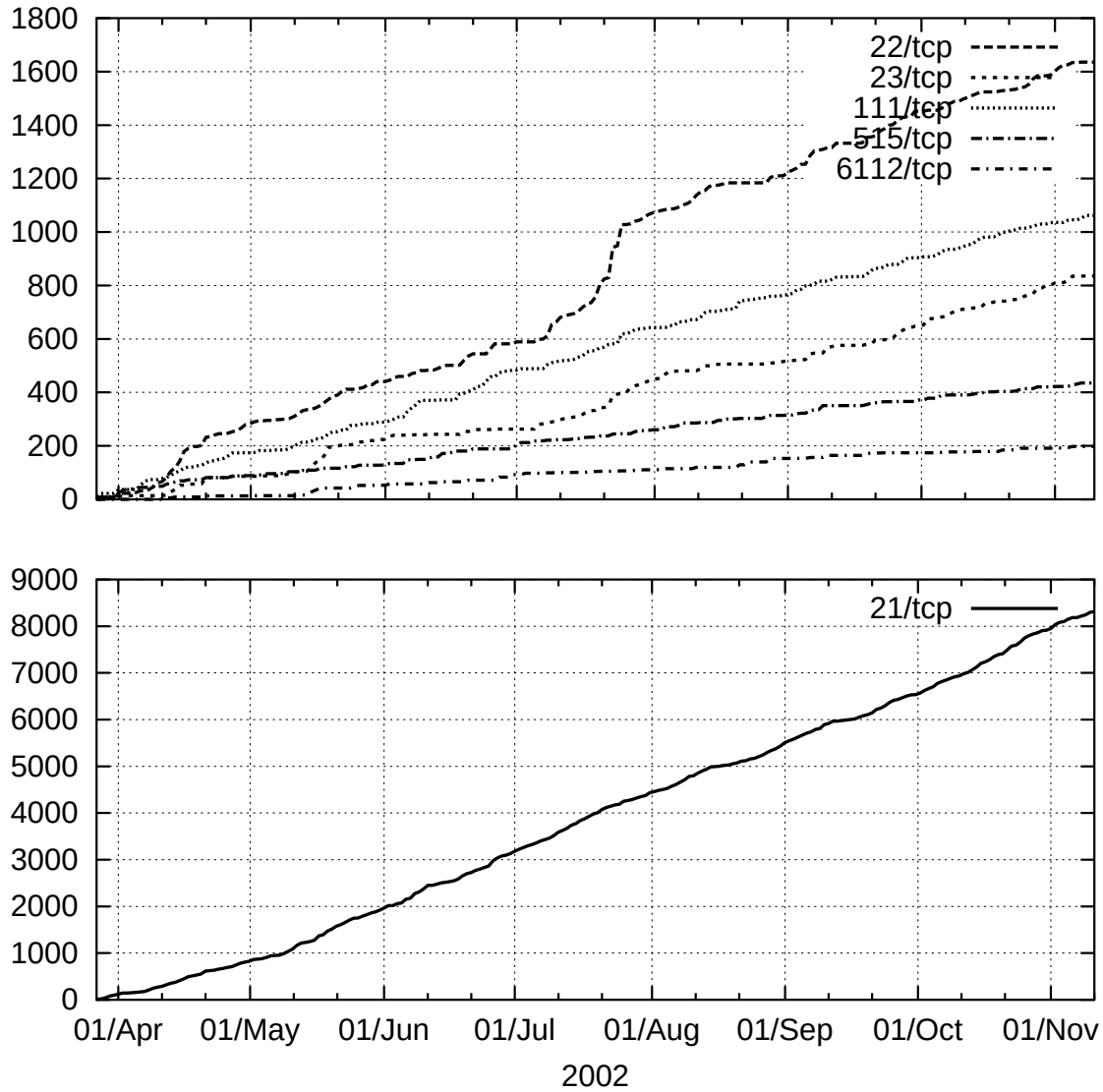
Alerts and Summaries

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

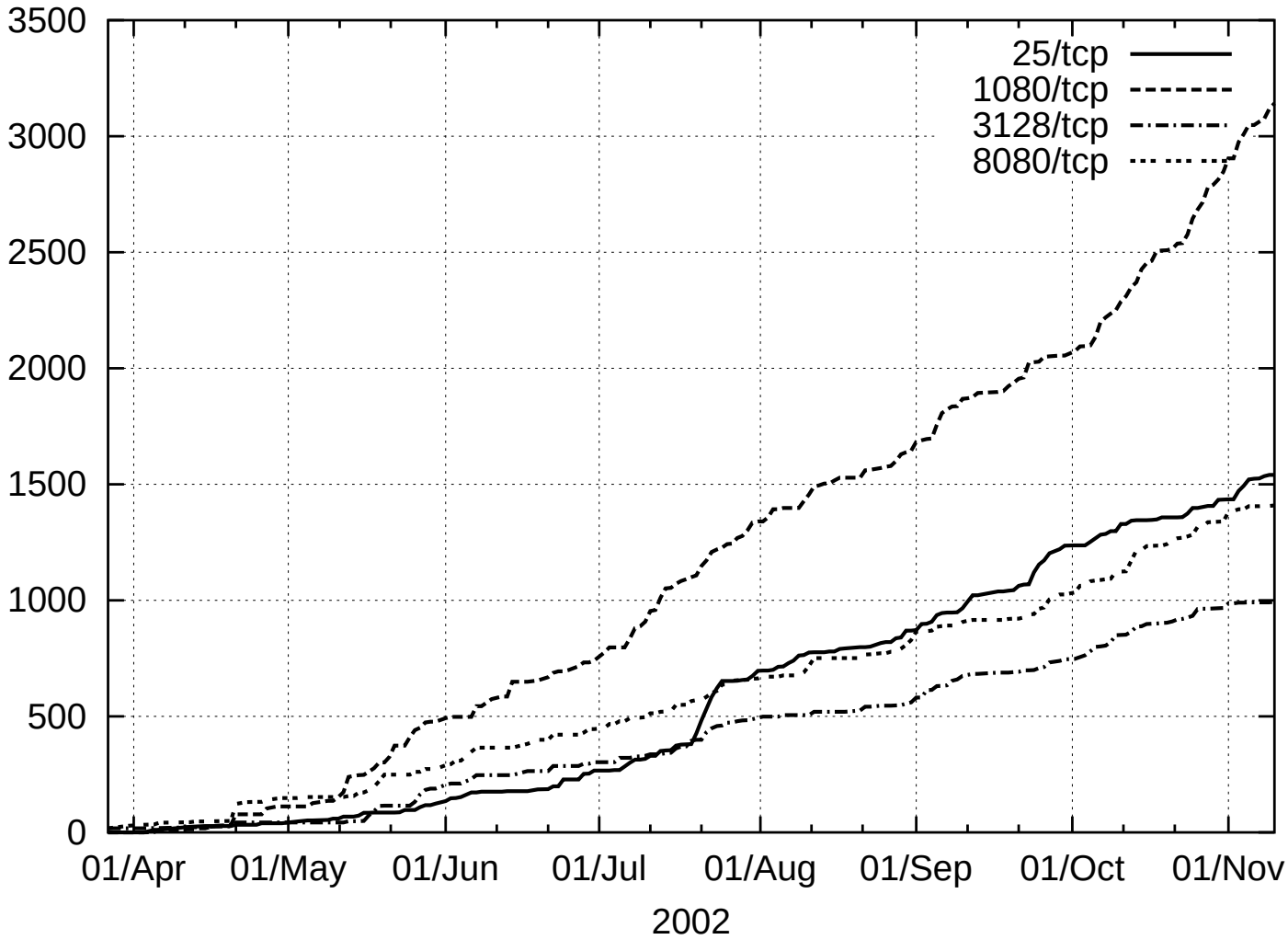
Activities Observed

- IRC sessions
- Worms
- DoS
- Tools
  - IRC related
  - rootkits and massrooters
  - exploits, etc

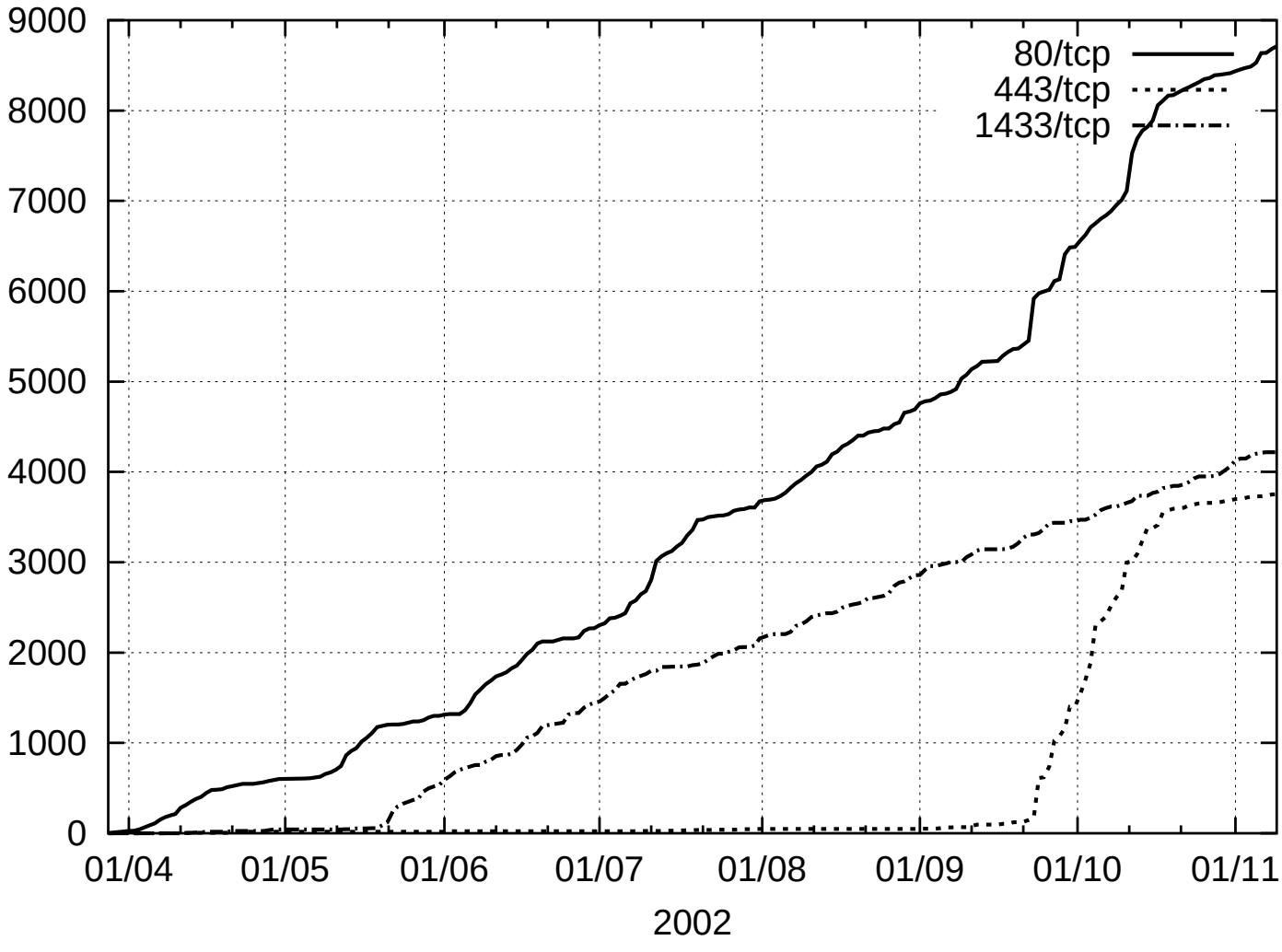
Top Scanned Services



Scans for Open Proxies and Relays



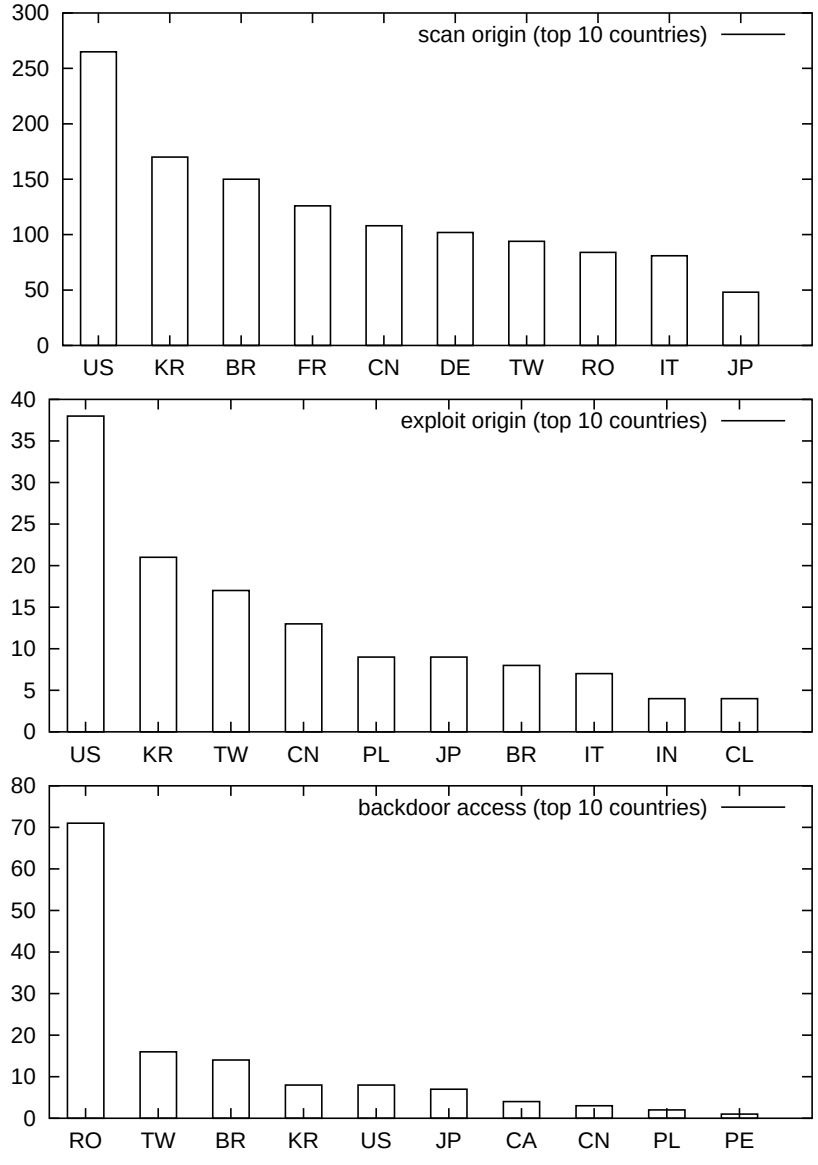
Worm Related Activity



Sources of Scans, Exploits and Backdoor Access

Country info obtained via:

- APNIC
- ARIN
- LACNIC
- RIPE



Usefulness to CSIRTs

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

Usefulness to CSIRTs (cont.)

Source of training material:

- Log analysis
- Artifact analysis
- Forensic methods
- Help to train new incident handlers

Lessons Learned

- Needs good contention 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

Contact Information

- Honeynet Research Alliance

  http://www.honeynet.org/alliance/

- Honeynet.BR Project

  http://www.honeynet.org.br/

- Authors:
  - Cristine Hoepers <cristine@nic.br>
  - Klaus Steding-Jessen <jessen@nic.br>
  - Antonio Montes, Ph.D. <montes@lac.inpe.br>