Honeynets and Honeypots: Companion Technology for Detection and Response

Cristine Hoepers
cristine@nic.br

NIC BR Security Office – NBSO
Brazilian Computer Emergency Response Team
http://www.nbso.nic.br/

Honeynet.BR & Brazilian Honeypots Alliance
http://www.honeynet.org.br/

Overview

- Some definitions
- Types of Honeypots
  - differences
  - possible uses
- Types of data gathered
  - in a Honeynet
  - in a network of distributed honeypots
- Additional Information

Honeypot Definition

“A honeypot is a security resource whose value lies in being probed, attacked or compromised.”

Lance Spitzner,
Honeypots: Tracking Hackers.

Advantages

- There is no “normal” traffic. Everything is suspicious and potentially malicious.
- Less data to analyse than in IDS systems
- Can provide valuable information about attackers
- Can capture new types of malware

Disadvantages

- There are potential risks for your network (depending on the type)
- Can be time consuming to maintain
- Narrow view – sees only what is directed to it

What honeypots aren't

- Honeypots are **not** replacements for:
  - security best practices
  - security policies
  - firewalls
  - IDS
  - patch management

Types of Honeypots

Low-interaction Honeypots

- Easy to install and maintain
- Low risk
- Limited information gathering
- Examples:
  - listeners, service emulators, honeyd, Tiny Honeypot.

Low-Interaction Honeypots (cont.)

- Emulate some parts of services and systems
- The attacker does not have access to the real operating system
- The attacker can’t compromise the honeypot (in theory)

High-interaction Honeypots

- More difficult to install and maintain
- High risk
- Need containment mechanisms
- Extensive information gathering
- Example:
  - honeynets, virtual honeynets

Honeynet Definition (1)

"A Honeynet is nothing more than one type of honeypot. Specifically, it is a high interaction honeypot designed primarily for research, to gather information on the enemy. [...] A Honeynet is different from traditional honeypots, it is what we would categorize as a research honeypot."

Lance Spitzner,

Know Your Enemy: Honeynets

Honeynet Definition (2)

"A honeynet is a research tool consisting of a network specifically designed for the purpose of being compromised, with control mechanisms that prevent this network from being used as a base for launching attacks against other networks."

Cristine Hoepers, Klaus Steding-Jessen, Antonio Montes, Honeynets Applied to the CSIRT Scenario

Honeynets Characteristics

- A network of multiple systems and applications
- Robust containment mechanism
  - may have multiple layers of control
  - sometimes called “honeywall”
- Data capture and alerting mechanisms

Honeynet Requirements

- No data pollution (i.e. no test or traffic generated by non-blackhats)
- Data control
- Data capture
- Data collection
- Alerting mechanism

Risks

Low-Interaction Honeypots Risks

- Compromise of the real operating system running the honeypot
- The honeypot software may have vulnerabilities
- Attract attackers to your network

Honeynets Risks

- A mistake in containment or configuration can
  - permit your honeynet to be used to harm other networks
  - open a port to your organization's network
- A compromise associated with your organization can affect its image
- Your honeynet being identified

Honeynets Risks (cont.)

Why they are so risky:

- Level of interaction – the attacker has full control of the machine
- Complex to deploy and maintain
  - variety of technologies working together
  - multiple points of failure
- New attacks and unexpected threats may not be contained or seen

Possible Uses

Possible Uses

- Detect automated probes and attacks
- Capture tools, new worms, etc
- Identify insider's attacks (internal honeypots, honeytokens)
- Compare with IDS and Firewall logs
- Raise awareness
- Identify infected/compromised machines
  - use the data to generate reports

When to Use

Low-Interaction Honeypots

- There is insufficient hardware to set up a honeynet
- The risk of another type of honeypot is not acceptable
- The purpose is:
  - identify scans and automated attacks
  - fool script kiddies
  - distract attackers from important systems
  - collect attack signatures and trends

When to Use (cont.)

High-Interaction Honeypots

- The purpose is to observe the intruders activities and behavior:
  - observe a real compromise
  - IRC conversations
- Need material for research and training in:
  - artifact analysis
  - forensic analysis

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

Some Results

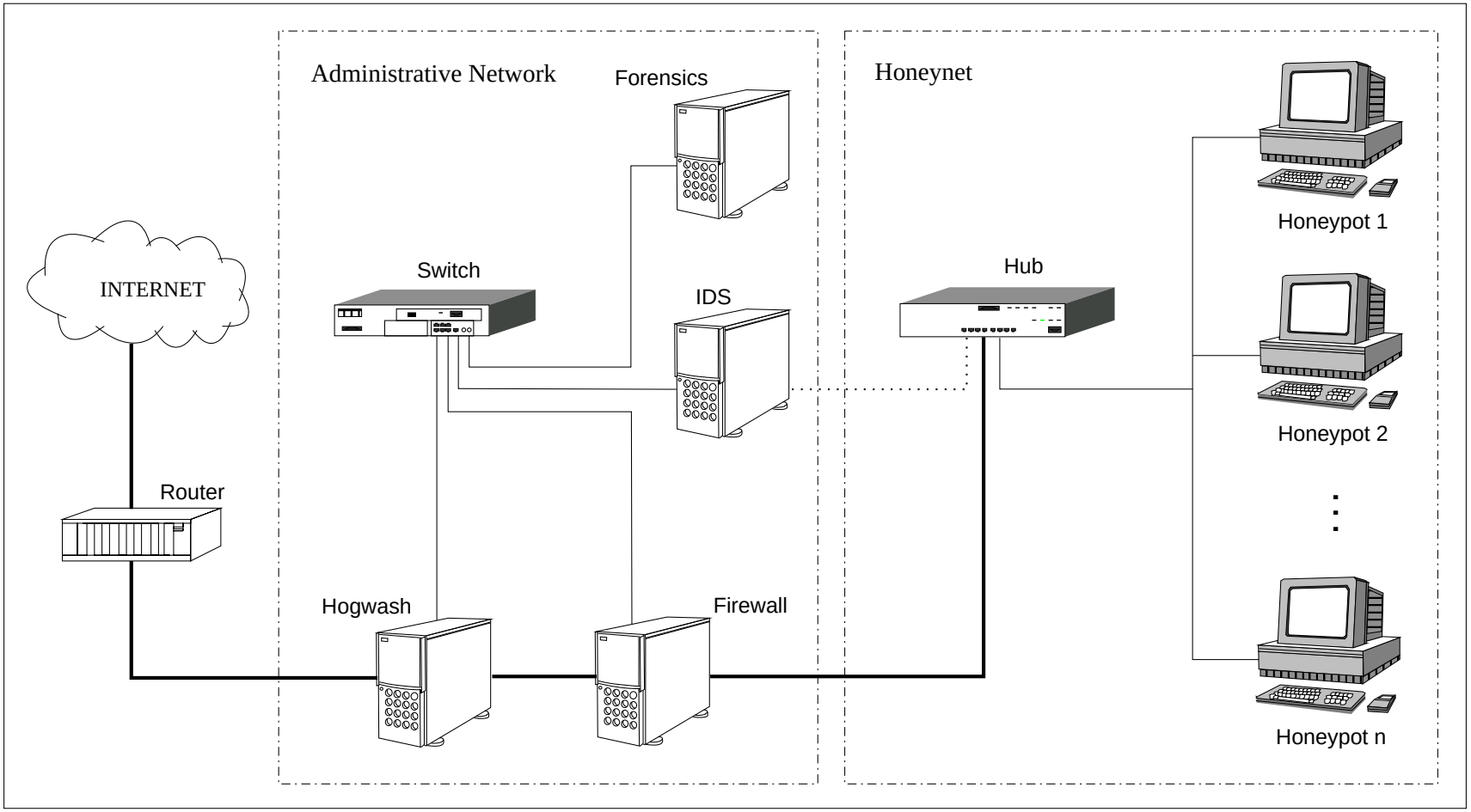
Data Gathered

Show some types of data gathered:

- In a Honeynet of the Honeynet.BR Project
  `http://www.honeynet.org.br/`
- In a Network of Distributed Honeypots
  `http://www.honeypots-alliance.org.br/`

Data Gathered by Honeynets

Honeynet.BR Topology



Data Gathered by Honeynets (cont.)

- Network traces of successful attacks
  - update IDS signatures
  - understand attacks
- Profile of intruders
  - modus operandi
  - IRC conversations, motives
  - possible origin

Data Gathered by Honeynets (cont.)

- Rootkits, exploits, etc
  - Used to update the `chkrootkit` tool

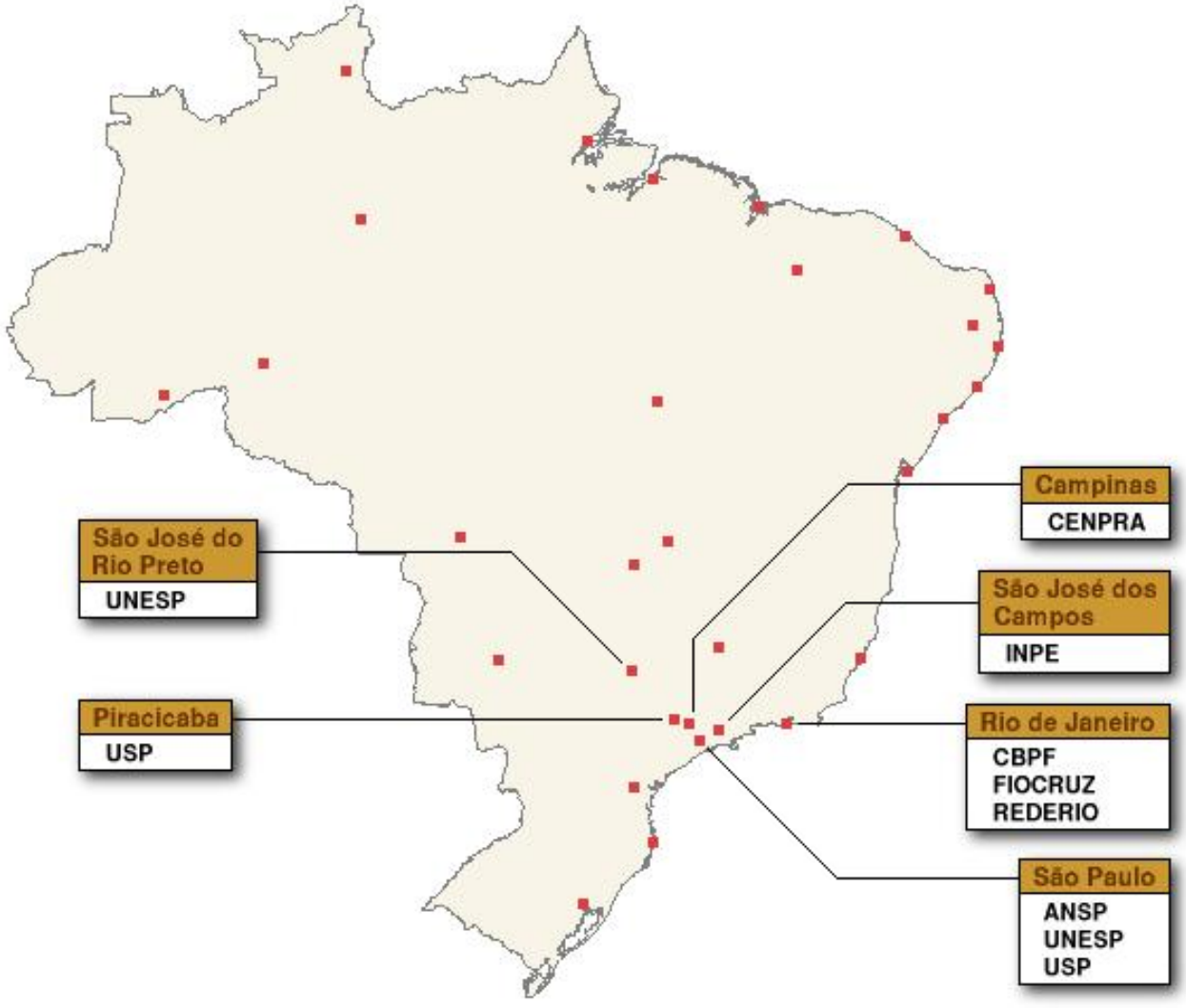
    `http://www.chkrootkit.org/`
- New worms
  - Scan of the Month Challenge 25 – Analyze a worm recovered by a Honeynet.

    `http://www.honeynet.org/scans/scan25/`
  - Propagation of "Slapper" OpenSSL/Apache Worm Variants

    `http://xforce.iss.net/xforce/alerts/id/advise134`

Data Gathered by Honeypots

Brazilian Honeypots Alliance



Data Gathered by Honeypots (cont.)

- Low-interaction honeypots distributed over mulitple networks
- Configuration of each honeypot:
  - OpenBSD
  - Honeyd
  - listeners
- Data collection in 2 central points:
  - NBSO/Brazilian CERT
  - CenPRA Research Center

Data Gathered by Honeypots (cont.)

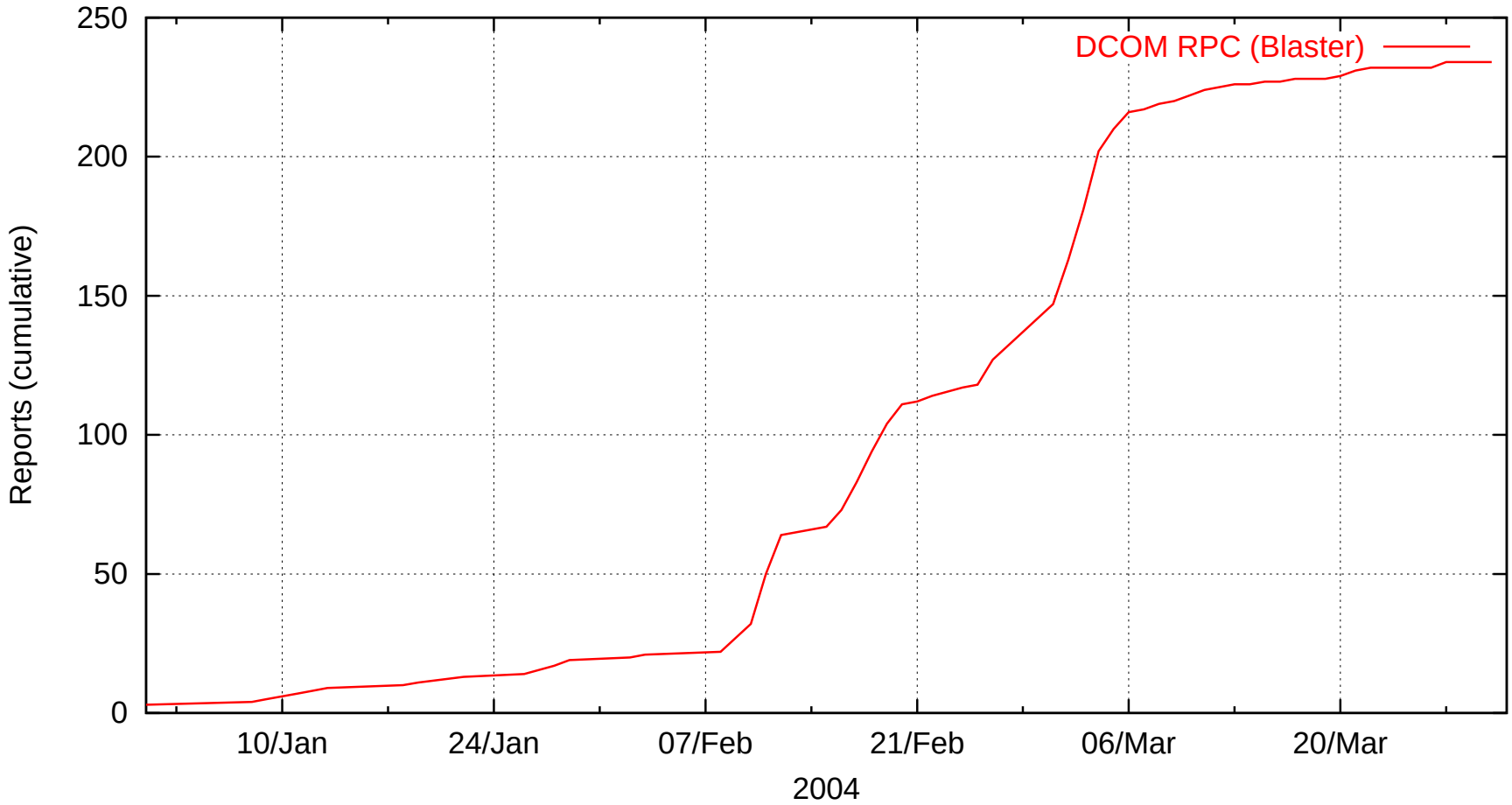
- Malware and spybot samples collected using listeners
  - mydoom
  - kuang
  - subseven
- All traffic is logged (not only “SYN” packets)
  - able to see signatures of attacks, scans and worms
  - reduce false positives
- Observe the “noise” of malware activity

Data Gathered by Honeypots (cont.)

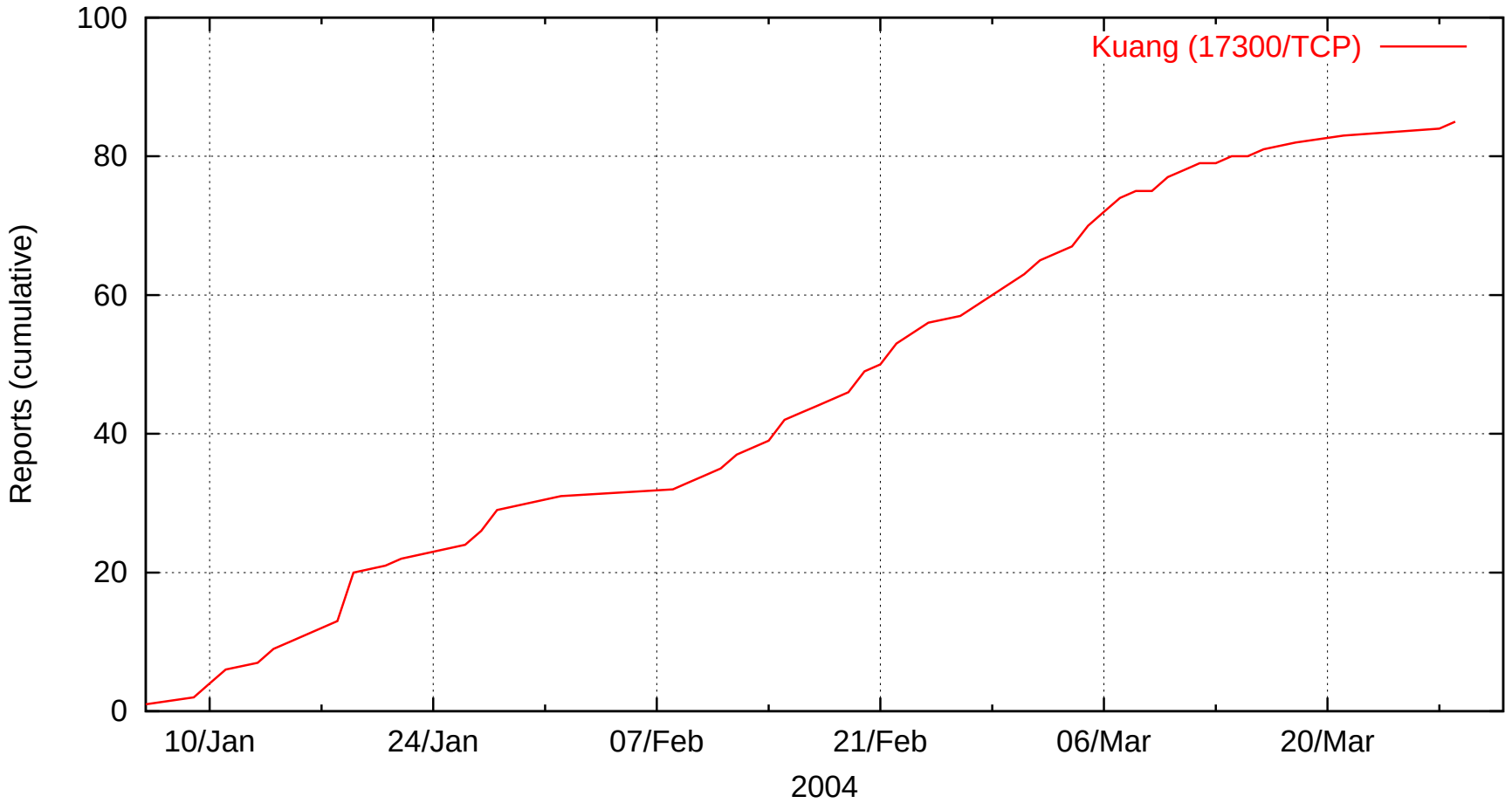
- Sanitized data is being used by NBSO to:
  - notify Brazilian networks involved in malicious activity
  - donate data to other CSIRTs interested in notifying their constituents
- Virus and malware are being sent to some AV vendors

The following graphics are based on reports sent by NBSO to Brazilian Networks, in the first quarter of 2004.

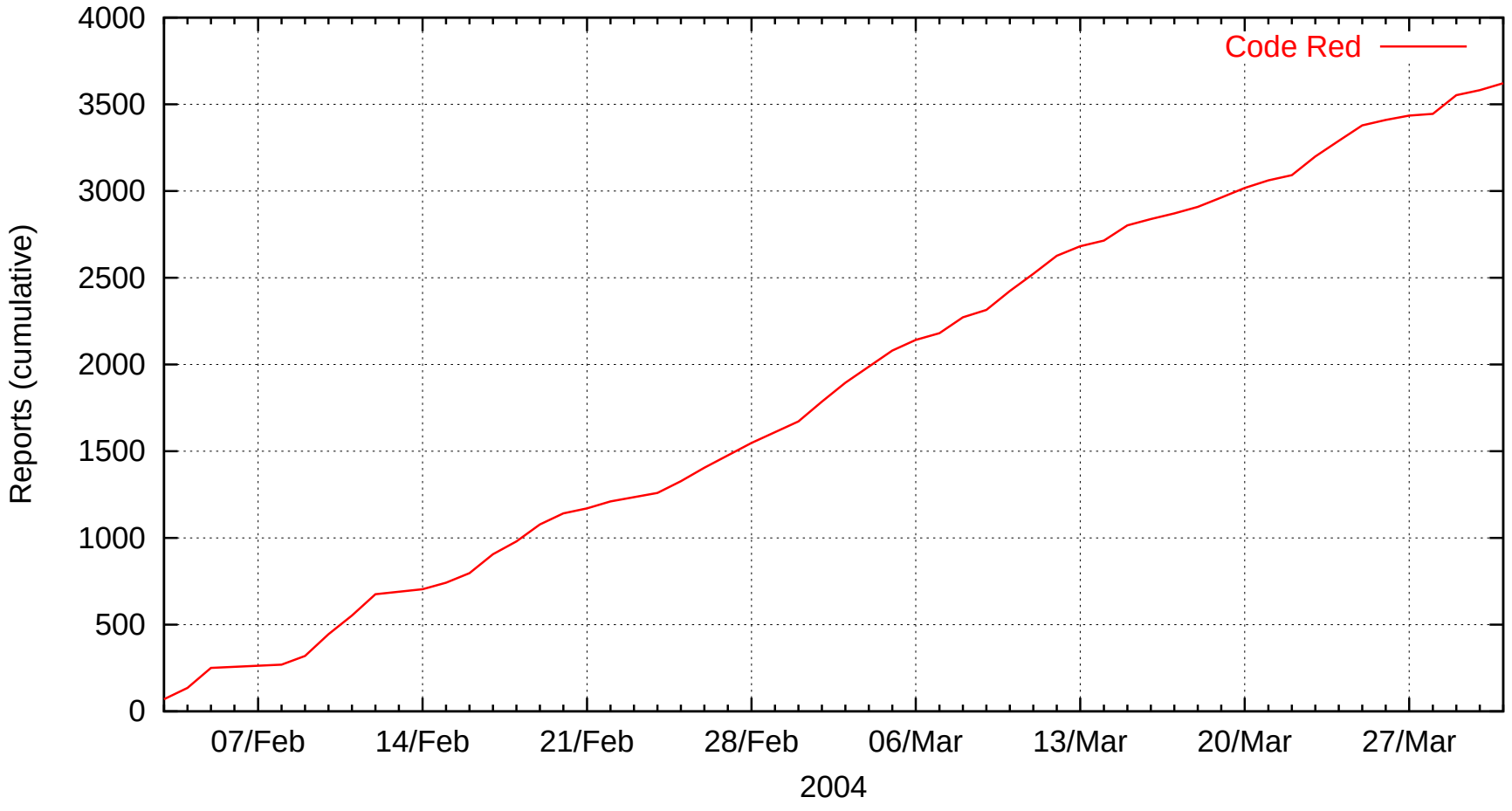
Data Gathered by Honeypots (cont.)



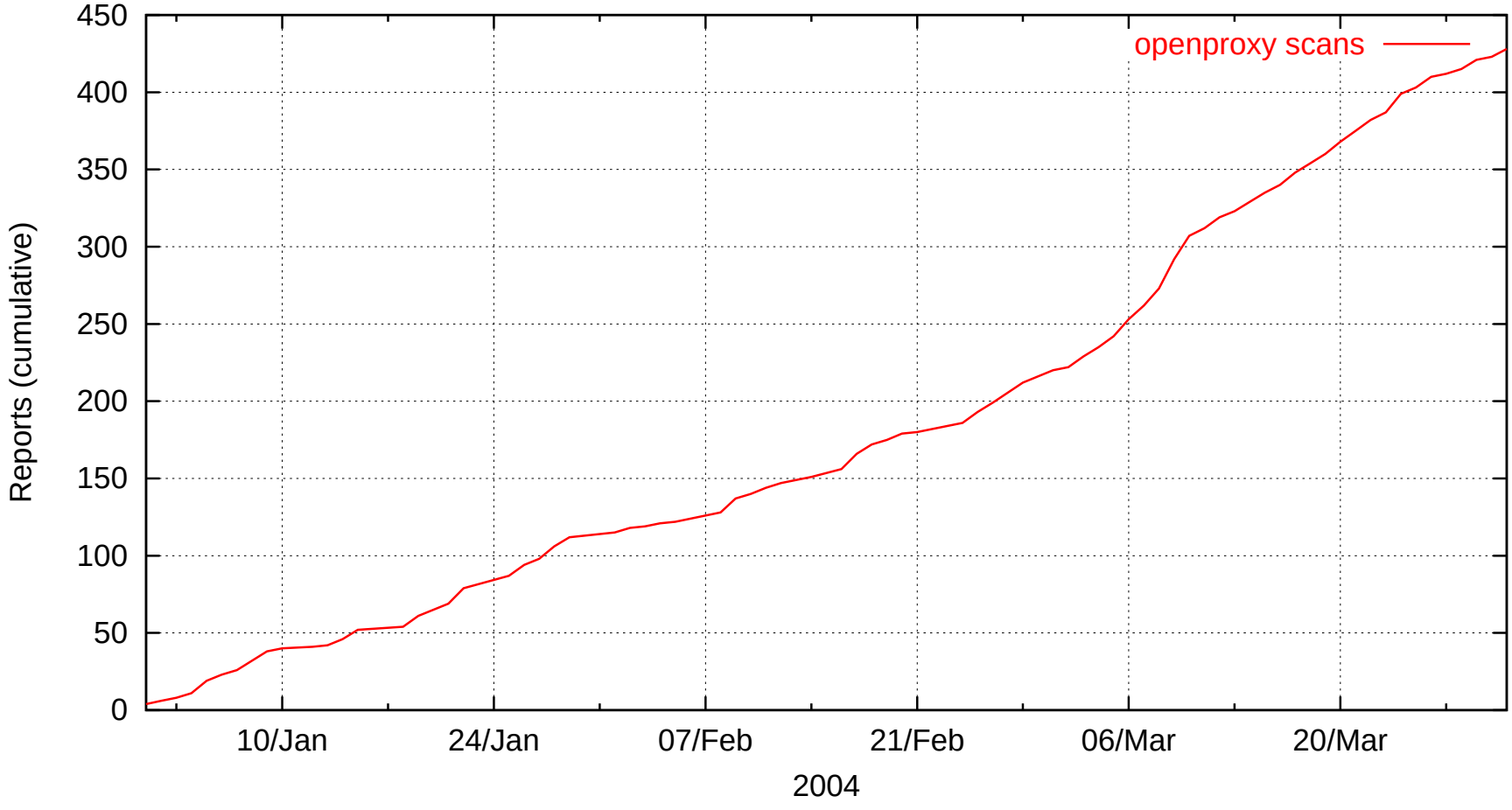
Data Gathered by Honeypots (cont.)



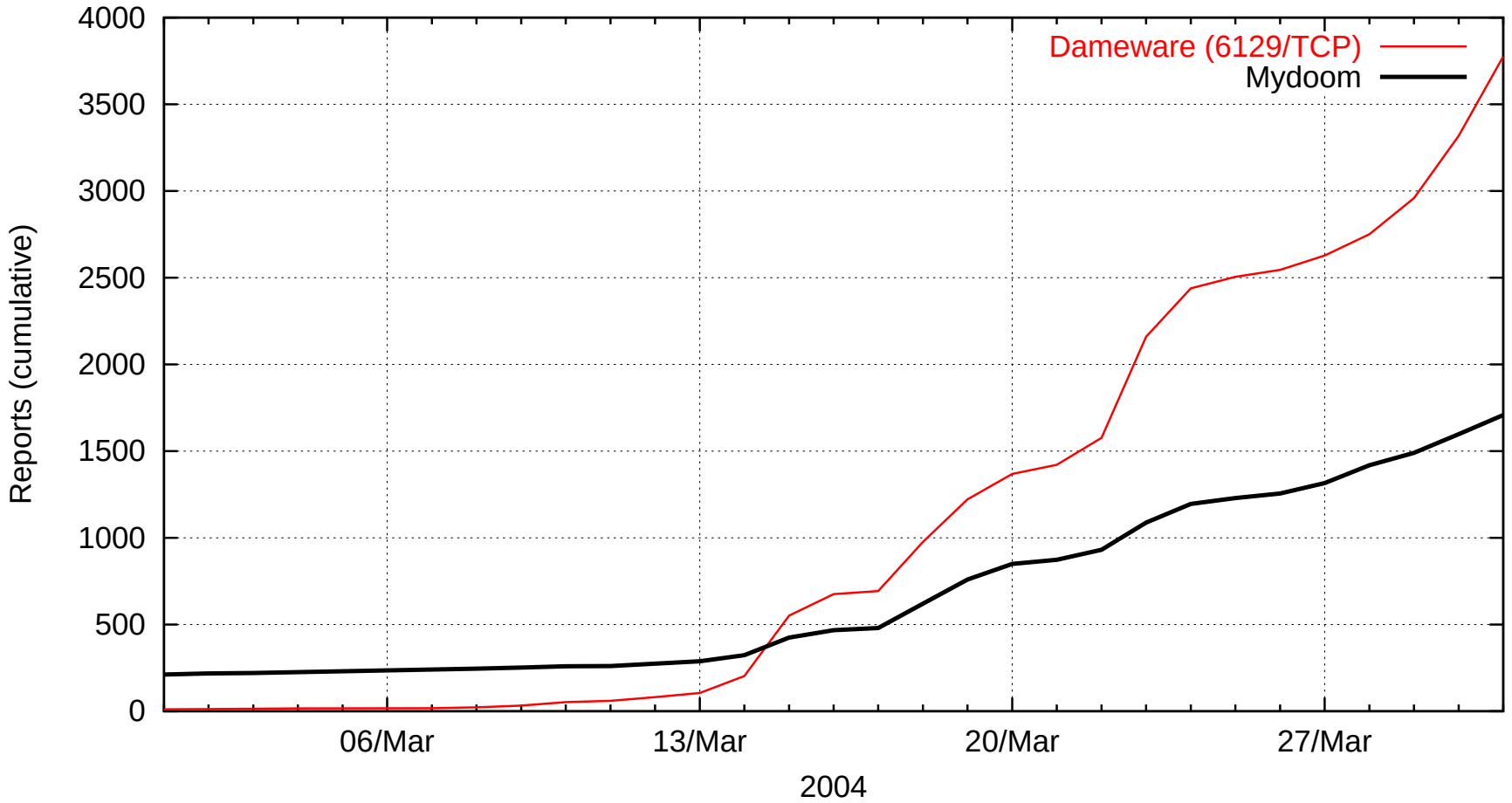
Data Gathered by Honeypots (cont.)



Data Gathered by Honeypots (cont.)

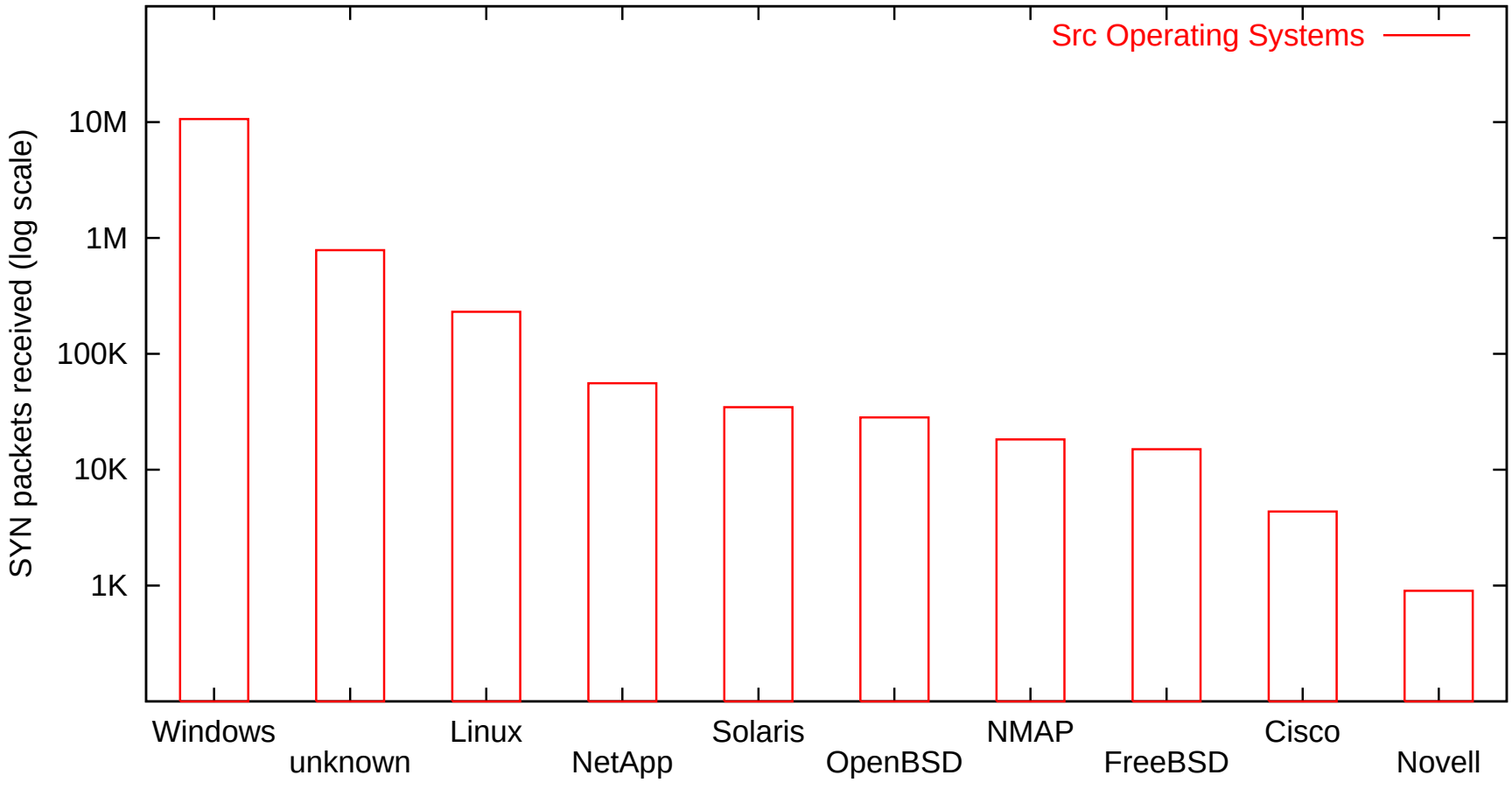


Data Gathered by Honeypots (cont.)

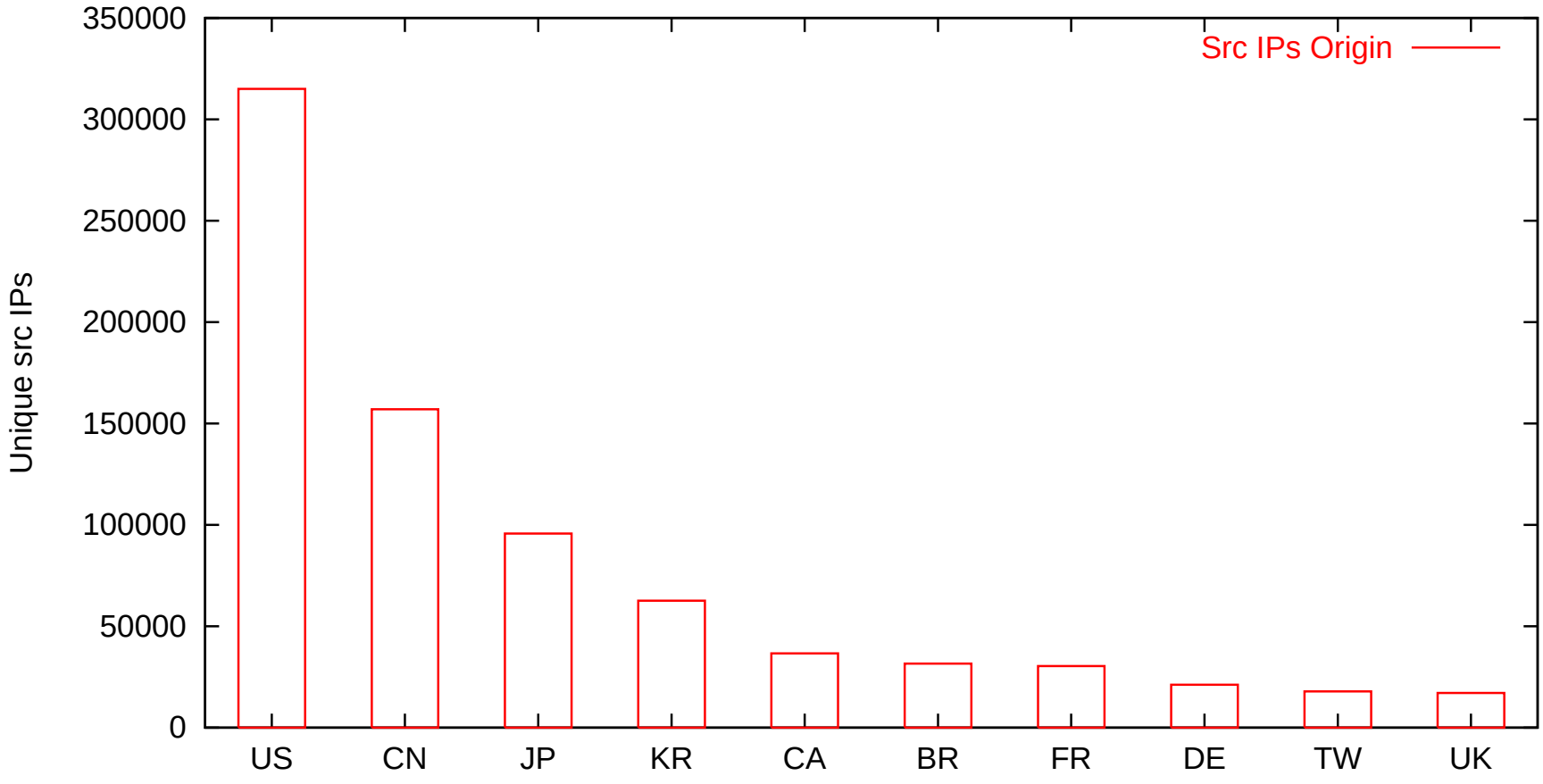


Possible Agobot/Phatbot side effect

Data Gathered by Honeypots (cont.)



Data Gathered by Honeypots (cont.)



Additional Information

- Honeynet.BR Project
  http://www.honeynet.org.br/
- Brazilian Honeypots Alliance
  http://www.honeypots-alliance.org.br/
- The Honeynet Project
  http://www.honeynet.org/
- Honeynet Research Alliance
  http://www.honeynet.org/alliance/
- Honeypots: Tracking Hackers
  http://www.tracking-hackers.com/book/
- Know Your Enemy, 2nd Edition
  http://www.honeynet.org/book/

Additional Information

- Honeyd
  http://www.honeyd.org/
- Honeyd: A Virtual Honeypot Daemon (Extended Abstract)
  http://www.citi.umich.edu/u/provos/papers/honeyd-eabstract.pdf
- Honeynets Applied to the CSIRT Scenario
  http://www.honeynet.org.br/papers/hnbr-first2003.pdf
- Honeynet Challenges
  http://www.honeynet.org/misc/chall.html
- SecurityFocus Honeypots Mailinglist
  http://www.securityfocus.com/archive/