Data Donation Initiatives at the Brazilian Honeypots Alliance

Klaus Steding-Jessen

jessen@cert.br

CERT.br – Computer Emergency Response Team Brazil

NIC.br – Network Information Center Brazil

CGI.br – Brazilian Internet Steering Committee

Agenda

- The Distributed Honeypots Project
  - Objective
  - Statistics
  - Incident Notification
  - Data Donation
- References

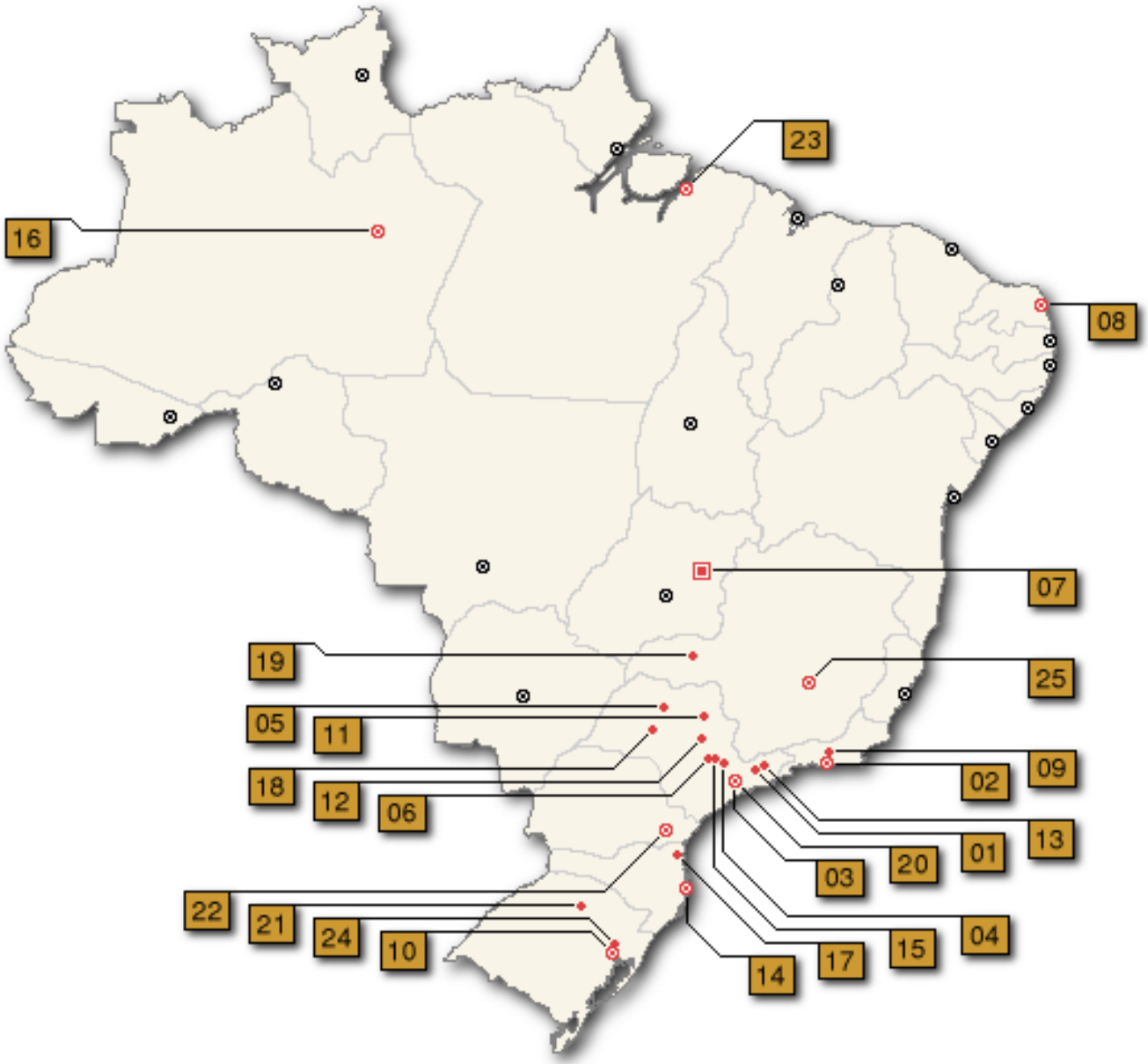
Brazilian Honeypots Alliance
Distributed Honeypots Project

Main Objective

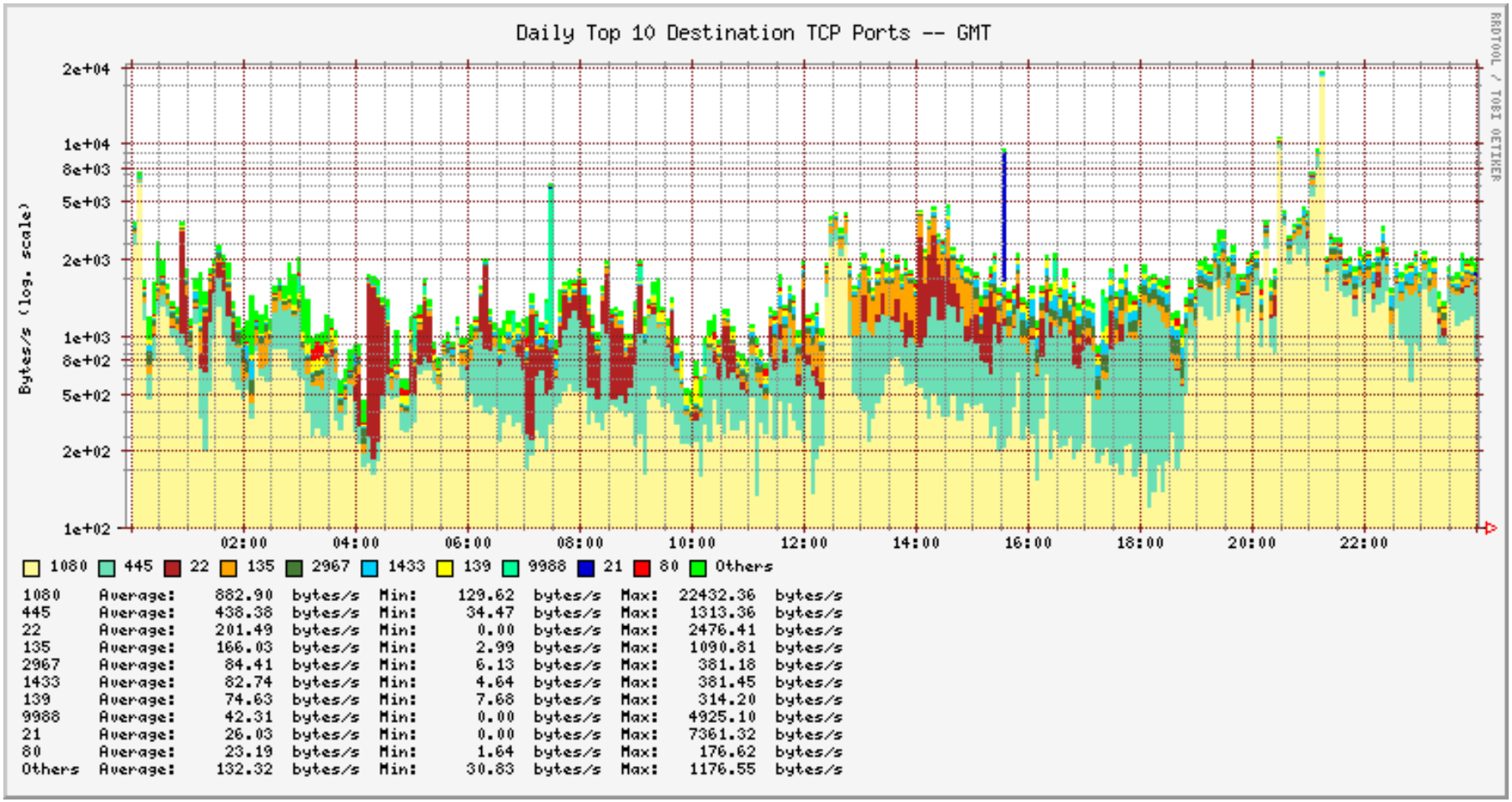
Increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 39 partner's institutions:
  - Academic, government, industry, telecom networks
- Widely distributed across the country
- Based on voluntary work
- Honeypots based on OpenBSD and Honeyd
  - Simulates machines on unused IP space (/24 to /21)
- Maintain public statistics
  http://www.honeypots-alliance.org.br/

Cities Where the Honeypots are Located



Public Statistics: Honeypots Flows

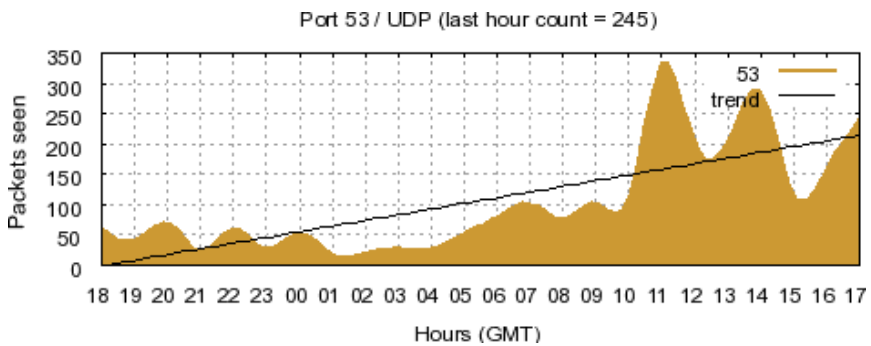


August 08, 2007 – http://www.honeypots-alliance.org.br/stats/

Public Statistics: Port summary (coming soon)

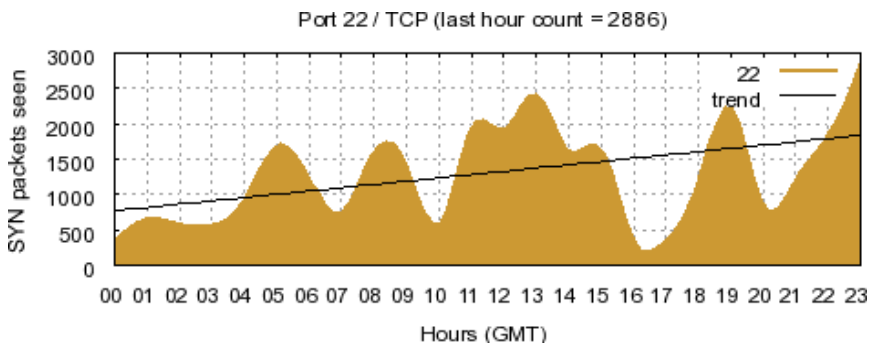
- Hourly

17: 2007-08-12 18:00 – 2007-08-13 17:59 (GMT)



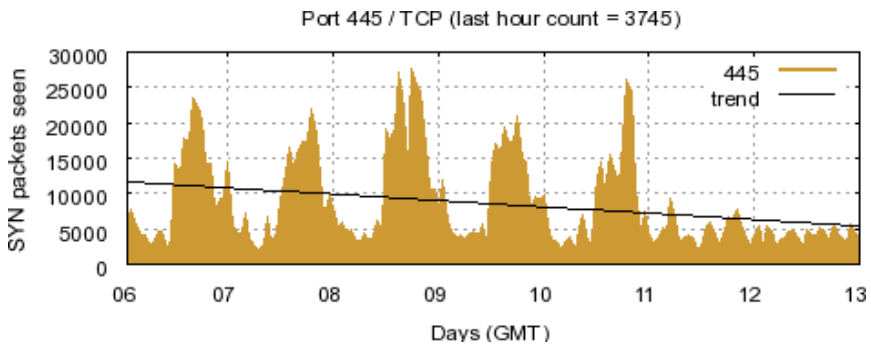
- Daily

12: 2007-08-12 00:00 – 2007-08-12 23:59 (GMT)



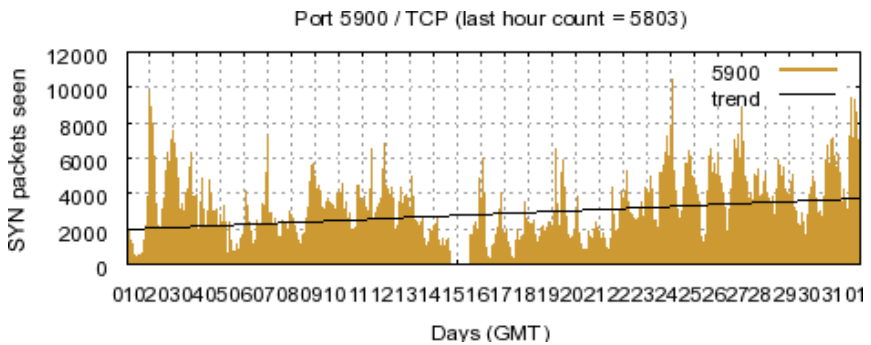
- Weekly

32: 2007-08-06 00:00 – 2007-08-12 23:59 (GMT)



- Monthly

07: 2007-07-01 00:00 – 2007-07-31 23:59 (GMT)



Incident Notification (1/2)

- Brazilian IPs only
- sent to the contacts of the offending networks
- sanitized data
- with tips explaining the problem, how to recover, etc.

Incident Notification (2/2)

Example:

```
To: contact
Subject: <a.b.c.d> - malicious activity coming from this host
---begin logs---
# all times are GMT
Sep 30 16:51:45 a.b.c.d.38840 > xxx.xxx.xxx.100.22: S
Sep 30 16:51:45 a.b.c.d.38841 > xxx.xxx.xxx.101.22: S
Sep 30 16:51:45 a.b.c.d.38842 > xxx.xxx.xxx.102.22: S
Sep 30 16:51:45 a.b.c.d.38843 > xxx.xxx.xxx.103.22: S
Sep 30 16:51:45 a.b.c.d.38844 > xxx.xxx.xxx.104.22: S
Sep 30 16:51:45 a.b.c.d.38845 > xxx.xxx.xxx.105.22: S
Sep 30 16:51:45 a.b.c.d.38846 > xxx.xxx.xxx.106.22: S
Sep 30 16:51:45 a.b.c.d.38847 > xxx.xxx.xxx.107.22: S
---end logs---
```

Data Donation (1/2)

- share some data collected
  - sanitized
- initially to teams with national responsibility
- daily logs from source IPs of given
  - Country Code
  - ASN
  - CIDR blocks
- initially `tcpdump` ASCII format

Data Donation (2/2)

Example:

```
Oct 04 04:04:50 81.12.140.218.2382 > xxx.xxx.xxx.48.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.32270 > xxx.xxx.xxx.49.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.2382 > xxx.xxx.xxx.48.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.33579 > xxx.xxx.xxx.50.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.33853 > xxx.xxx.xxx.51.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.33963 > xxx.xxx.xxx.52.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.34650 > xxx.xxx.xxx.53.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.36754 > xxx.xxx.xxx.54.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.38273 > xxx.xxx.xxx.57.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.2452 > xxx.xxx.xxx.59.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.38516 > xxx.xxx.xxx.58.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.39344 > xxx.xxx.xxx.60.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.37992 > xxx.xxx.xxx.55.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.38032 > xxx.xxx.xxx.56.6588: tcp 0 (DF)
Oct 04 04:04:51 81.12.140.218.39901 > xxx.xxx.xxx.62.6588: tcp 0 (DF)
```

References

- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/
- Brazilian Honeypots Alliance
  http://www.honeypots-alliance.org.br/