Incident Response
Initiatives in Brazil

Klaus Steding-Jessen
jessen@cert.br

Computer Emergency Response Team Brazil – CERT.br
http://www.cert.br/

Brazilian Internet Steering Committee
http://www.cgi.br/
Overview

- Incident Response
  - CERT.br
  - History
  - Initiatives
  - Brazilian CSIRTs
  - Early Warning
CERT.br

Mission:
• A organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet.

Constituency:
• Brazil - Internet .br domain and IP addresses assigned to Brazil.
CERT.br Services

- provide a focal point for reporting incidents related to Brazilian networks;
- provide coordinated support in incident response;
- establish collaborative relationships (law enforcement, service providers, telephone companies, financial sector, etc);
- increase security awareness and help new CSIRTs to establish their activities;

CERT.br is a member of FIRST [http://www.first.org/](http://www.first.org/)
The Brazilian Internet Steering Committee (CGI.br)

- Multilateral Committee created in 1995
  - 10 members from the government, including: Ministries of Science and Technology, Communications, Defense, Industry, and the Telecommunications Regulatory Agency (Anatel)
  - 11 members from the civil society and private sector, including: industry, telcos, ISPs, academia and third sector
Brazilian Internet Steering Committee’s main attributions are:

- to foment the development of Internet services;
- to recommend technical standards and procedures for the Brazilian Internet;
- to coordinate the attribution of IP addresses and the registration of domain names;
- to collect, organize and disseminate information to the Brazilian Internet community.
How CERT.br was created

- August/1996: CGI.br released the document: "Towards the Creation of a Security Coordination Center in the Brazilian Internet."
  - to be a neutral organization
  - to act as a focal point for security incidents in Brazil
  - to facilitate information sharing and incident handling
- June/1997: They created NBSO/Brazilian CERT
- May/2005: NBSO changed its name to:
  - CERT.br
    Computer Emergency Response Team Brazil
CERT.br Initiatives

- Produce technical documents in Portuguese
- Maintain statistics (incidents and spam)
- Anti-Phishing Working Group Research Partner
  - detect malware enabled fraud
  - notify hosting sites
  - send samples to 20+ AV vendors
- Honeypots and Honeynets research
  - Honeynet Research Alliance Member
  - Brazilian Honeypots Alliance – Distributed Honeypots Project
CERT.br Initiatives (cont.)

CSIRT Development

• iNOC-DBA – IP phones distributed to all CSIRTs

• Training
  – SEI Partner for 4 CERT®/CC courses
  – 100+ people trained

• Help new teams’ creation

• Maintain a list of Brazilian CSIRTs
Brazilian CSIRTs

http://www.cert.br/contact-br.html
Early Warning

Have a national early warning capability with the following characteristics:

- Widely distributed across the country – in several ASNs and geographical locations
- Based on voluntary work of research partners
- High level of privacy for the members
- Useful for Incident Response

A distributed networks of honeypots was chosen
The Honeypots Network

Brazilian Honeypots Alliance – Distributed Honeypots Project

• Coordination:
  – CERT.br – Computer Emergency Response Team Brazil (formerly NBSO)
    Brazilian Internet Steering Committee
  – CenPRA Research Center
    Ministry of Science and Technology
The Honeypots Network (cont.)

26 research partner’s institutions:

- Academia, Government, Industry, Military and Telcos networks
- They provide:
  - hardware and network blocks (usually a /24)
  - maintenance of their own honeypots
- Use the data for intrusion detection purposes
  - less false positives than traditional IDSs
- Several have more than one honeypot
### The Honeypots Network (cont.)

<table>
<thead>
<tr>
<th>#</th>
<th>City</th>
<th>Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>São José dos Campos</td>
<td>INPE, ITA</td>
</tr>
<tr>
<td>02</td>
<td>Rio de Janeiro</td>
<td>CBPF, Fiocruz, PUC-RIO, RedeRio, UFRJ</td>
</tr>
<tr>
<td>03</td>
<td>São Paulo</td>
<td>ANSP, CERT.br, Diveo, Durand, UNESP, USP</td>
</tr>
<tr>
<td>04</td>
<td>Campinas</td>
<td>CenPRA, HP Brazil, UNICAMP</td>
</tr>
<tr>
<td>05</td>
<td>São José do Rio Preto</td>
<td>UNESP</td>
</tr>
<tr>
<td>06</td>
<td>Piracicaba</td>
<td>USP</td>
</tr>
<tr>
<td>07</td>
<td>Brasília</td>
<td>Brasil Telecom, Ministry of Justice, TCU, UNB LabRedes</td>
</tr>
<tr>
<td>08</td>
<td>Natal</td>
<td>UFRN</td>
</tr>
<tr>
<td>09</td>
<td>Petrópolis</td>
<td>LNCC</td>
</tr>
<tr>
<td>10</td>
<td>Porto Alegre</td>
<td>CERT-RS</td>
</tr>
<tr>
<td>11</td>
<td>Ribeirão Preto</td>
<td>USP</td>
</tr>
<tr>
<td>12</td>
<td>São Carlos</td>
<td>USP</td>
</tr>
<tr>
<td>13</td>
<td>Taubaté</td>
<td>UNITAU</td>
</tr>
<tr>
<td>14</td>
<td>Florianópolis</td>
<td>UFSC DAS</td>
</tr>
<tr>
<td>15</td>
<td>Americana</td>
<td>VIVAX</td>
</tr>
<tr>
<td>16</td>
<td>Manaus</td>
<td>VIVAX</td>
</tr>
</tbody>
</table>
The Honeypots Network (cont.)

As of June, 2005
Early Warning

• Private Statistics – summaries including:
  – specific information for each honeypot
  – most active IPs, Operating Systems, ports, protocols and Country Codes
  – correlated activities (ports and IPs)

• Public Statistics
  – combined daily flows seen in the honeypots
  – most active Operating Systems, TCP/UDP ports and Country Codes (CC)
Usefulness:

• observation of trends
  – detect scans for potential new vulnerabilities

• partner institutions are detecting promptly:
  – outbreaks of new worms/bots
  – compromised servers
  – network configuration errors

• collect new signatures and new malware
Public Statistics – Top TCP Ports

---

Daily Top 10 Destination TCP Ports -- GMT

- **1433**: Average: 505.63 bytes/s, Min: 227.87 bytes/s, Max: 1049.49 bytes/s
- **80**: Average: 272.28 bytes/s, Min: 10.39 bytes/s, Max: 1061.22 bytes/s
- **135**: Average: 219.18 bytes/s, Min: 46.05 bytes/s, Max: 1936.76 bytes/s
- **445**: Average: 89.13 bytes/s, Min: 14.25 bytes/s, Max: 290.01 bytes/s
- **139**: Average: 63.99 bytes/s, Min: 7.07 bytes/s, Max: 198.56 bytes/s
- **1025**: Average: 52.18 bytes/s, Min: 5.12 bytes/s, Max: 163.15 bytes/s
- **3127**: Average: 36.79 bytes/s, Min: 0.00 bytes/s, Max: 1980.03 bytes/s
- **4899**: Average: 30.50 bytes/s, Min: 0.00 bytes/s, Max: 523.09 bytes/s
- **6101**: Average: 21.03 bytes/s, Min: 0.00 bytes/s, Max: 1101.69 bytes/s
- **17300**: Average: 6.87 bytes/s, Min: 0.00 bytes/s, Max: 1068.07 bytes/s
- **Others**: Average: 67.83 bytes/s, Min: 8.03 bytes/s, Max: 1317.06 bytes/s

June 15, 2005
Public Statistics – Top Country Codes

Daily Top 10 Source Country Codes (CC) -- GMT

<table>
<thead>
<tr>
<th>Country</th>
<th>Average</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>4.06</td>
<td>1.66</td>
<td>10.44</td>
</tr>
<tr>
<td>BR</td>
<td>4.05</td>
<td>0.44</td>
<td>23.16</td>
</tr>
<tr>
<td>CN</td>
<td>2.08</td>
<td>0.57</td>
<td>5.55</td>
</tr>
<tr>
<td>TW</td>
<td>1.06</td>
<td>0.01</td>
<td>15.33</td>
</tr>
<tr>
<td>PL</td>
<td>1.04</td>
<td>0.00</td>
<td>4.53</td>
</tr>
<tr>
<td>KR</td>
<td>0.55</td>
<td>0.00</td>
<td>11.45</td>
</tr>
<tr>
<td>MX</td>
<td>0.39</td>
<td>0.00</td>
<td>5.88</td>
</tr>
<tr>
<td>JP</td>
<td>0.37</td>
<td>0.01</td>
<td>8.77</td>
</tr>
<tr>
<td>AR</td>
<td>0.30</td>
<td>0.01</td>
<td>2.68</td>
</tr>
<tr>
<td>MY</td>
<td>0.28</td>
<td>0.00</td>
<td>1.80</td>
</tr>
<tr>
<td>Others</td>
<td>2.95</td>
<td>1.04</td>
<td>16.11</td>
</tr>
</tbody>
</table>

June 17, 2005
Public Statistics – Top Source OS

Daily Top 10 Windows Source OS -- GMT

<table>
<thead>
<tr>
<th>Source OS</th>
<th>Average Bytes/s</th>
<th>Min Bytes/s</th>
<th>Max Bytes/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows-XP-SP1/Windows-2000-SP3</td>
<td>392.88</td>
<td>24.60</td>
<td>1396.62</td>
</tr>
<tr>
<td>Non-Windows</td>
<td>216.54</td>
<td>60.42</td>
<td>2591.23</td>
</tr>
<tr>
<td>Windows-XP-SP1/Windows-2000-SP4</td>
<td>194.04</td>
<td>27.36</td>
<td>1015.81</td>
</tr>
<tr>
<td>Windows-XP/Windows-2000-SP2</td>
<td>45.47</td>
<td>0.80</td>
<td>347.09</td>
</tr>
<tr>
<td>Windows-2000/Windows-XP</td>
<td>23.33</td>
<td>0.16</td>
<td>354.47</td>
</tr>
<tr>
<td>Windows-98</td>
<td>22.32</td>
<td>0.00</td>
<td>5307.51</td>
</tr>
<tr>
<td>Windows-XP-cisco/Windows-2000-cisco</td>
<td>13.03</td>
<td>0.00</td>
<td>129.12</td>
</tr>
<tr>
<td>Windows-NT-4.0</td>
<td>5.76</td>
<td>0.00</td>
<td>276.91</td>
</tr>
<tr>
<td>Windows-3.11</td>
<td>2.09</td>
<td>0.00</td>
<td>112.93</td>
</tr>
<tr>
<td>Other-Windows</td>
<td>2.24</td>
<td>0.00</td>
<td>37.65</td>
</tr>
</tbody>
</table>
Incident Response

- Identify signatures of well known malicious/abusive activities
  - worms, bots, scans, spam and other malware
- Notify the responsible networks of the Brazilian IPs
  - with recovery tips
- Donate sanitized data of non-Brazilian IPs to other CSIRTs
Related Links

• This presentation
  http://www.cert.br/docs/palestras/

• Brazilian Honeypots Alliance
  Distributed Honeypots Project
  http://www.honeypots-alliance.org.br/

• Brazilian Honeypots Alliance Statistics
  http://www.honeypots-alliance.org.br/stats/

• Computer Emergency Response Team Brazil –
  CERT.br
  http://www.cert.br/

• The Honeynet Research Alliance
  http://project.honeynet.org/alliance/