Incident Response and Early Warning Initiatives in Brazil

Marcelo H. P. C. Chaves
mhp@cert.br

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

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

• CERT.br
  – The CERT.br Sponsor
  – Mission, constituency and services
  – Initiatives

• Early Warning
  – Motivation
  – The honeypots network
  – public and private statistics and use in incident response
  – Advantages, disadvantages and future work
CGI.br / CERT.br
The Brazilian Internet Steering Committee (CGI.br)

- created by the Interministerial Ordinance Nº 147, of May 31st 1995
- altered by the Presidential Decree Nº 4,829, of September 3rd 2003

It is a multistakeholder organization composed of:

<table>
<thead>
<tr>
<th>sector</th>
<th>representatives</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government</td>
<td>Ministries of Science and Technology, Communications, Defense, Industry, etc, and Telcos Regulatory Agency (ANATEL)</td>
<td>9</td>
</tr>
<tr>
<td>Corporate sector</td>
<td>Industry, Telcos, ISPs, users</td>
<td>4</td>
</tr>
<tr>
<td>NGO’s</td>
<td>Non-profit organizations, etc</td>
<td>4</td>
</tr>
<tr>
<td>Sci. and Tech. Community</td>
<td>Academia</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Internet expert</td>
<td>1</td>
</tr>
</tbody>
</table>
Brazilian Internet Steering Committe’s main attributions:

• to propose policies and procedures related to the regulation of Internet activities;
• to recommend standards for technical and operational procedures for the Internet in Brazil;
• 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 – The CERT.br Sponsor (cont.)

Diagram:
- CGI.br – Brazilian Internet Steering Committee
- NIC.br – Network Information Center
  - CERT.br – Computer Emergency Response Team Brazil
  - Registro.br – Domain Registration
  - PTT.br – Internet Exchange Points
CERT.br

Mission:

• An 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.
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/)
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:

• Training:
  – SEI Partner for 4 CERT®/CC courses
    * Creating a Computer Security Incident Response Team
    * Managing Computer Security Incident Response Teams
    * Fundamentals of Incident Handling
    * Advanced Incident Handling for Technical Staff
  – 140+ people trained

• Help new teams’ creation
• Maintain a list of Brazilian CSIRTs
Brazilian CSIRTs

http://www.cert.br/contact-br.html
CGI.br Initiatives

• sponsors 2 meetings/conferences free of charge per year, to the security and network communities (GTS/GTER)

• iNOC-DBA BR – project to stimulate Brazilian networks to join the iNOC-DBA global network
  – 100 IP phones were provided to ASNs
  – 20 IP phones were provided to CSIRTs recognized by CERT.br

iNOC-DBA – global hotline phone system which directly interconnects the Network Operations Centers and Security Incident Response Teams
Task Force on Spam (CT-Spam)

• to propose a national strategy to fight spam
• to articulate the actions among the different actors
• documents created
  – “Technologies and Policies to Fight Spam”
  – technical analysis of international antispam laws and brazilian proposals of new laws
Early Warning Initiative
Motivation

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
The Honeypots Network

Brazilian Honeypots Alliance – Distributed Honeypots Project

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

- Technical requirements:
  - secure configuration
  - follow the project’s standards (OS, configurations, updates, etc)
  - no data pollution

- Privacy concerns (in a NDA):
  - don’t disclose IP/network information
  - don’t collect production network traffic
  - don’t exchange any information in clear text
The Honeypots Network (cont.)

The architecture:

• low interaction honeypots
  – OpenBSD + Honeyd
  – using a netblock range
  – emulating services (HTTP, SMTP, malwares backdoors, etc)

• a central server
  – collects logs and uploaded malware
  – performs a status check in all honeypots
The Honeypots Network (cont.)

31 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, IME, 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, ITAL, HP Brazil, UNICAMP, UNICAMP FEEC</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>
<tr>
<td>17</td>
<td>Joinville</td>
<td>UDESC</td>
</tr>
<tr>
<td>18</td>
<td>Lins</td>
<td>FPTE</td>
</tr>
<tr>
<td>19</td>
<td>Uberlândia</td>
<td>CTBC Telecom</td>
</tr>
</tbody>
</table>
The Honeypots Network (cont.)

As of October, 2005
Early Warning

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

• Public Statistics:
  – combined daily flows seen in the honeypots
  – most active OSs, TCP/UDP ports and Country Codes (CC)
  * the top ports, OSs and CCs are calculated every day
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 Generation

• convert the raw network data into flow data
• compute the amount of bytes/packets received by each port (or OS or CC)
• select the top 10 to plot
  – the remaining will be displayed as “others”
• use RRDtool and ORCA to generate the flows’ graphics
  – stack area graphics
  – logarithmic scale
Public Statistics Generation (cont.)

pflog files

flow files

ascii flow files

ascii flow files (filtered)

TOP−10−tcp, TOP−10−udp, TOP−10−cc, TOP−10−s cosmos files

make−pflog2flows.pl

fprobe

flow−capture

flow−print

asci i flow files

asci i flow files (filtered)

flow2ports.pl

flow2cc.pl

flow2s cosmos.pl

cidrgrep
Public Statistics Generation (cont.)

- TOP−10−tcp
- TOP−10−udp
- TOP−10−cc
- TOP−10−srcos

**make-honeyd-stats.pl**
- for each TOP-10-<type> file

**make-orca-stats.pl**
- for each 4-hour data
- run ORCA
- feed RRDTool database
- store image for 4-hour period
- store daily image

**create HTML files**
- store TOP-10-<type> files
- store daily file

Public Statistics – Top UDP Ports

---

Daily Top 10 Destination UDP Ports -- GMT

<table>
<thead>
<tr>
<th>Port</th>
<th>Average:</th>
<th>Min:</th>
<th>Max:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1434</td>
<td>151.79m</td>
<td>88.33m</td>
<td>238.75m</td>
</tr>
<tr>
<td>53</td>
<td>34.96m</td>
<td>0.00m</td>
<td>3526.67m</td>
</tr>
<tr>
<td>1026</td>
<td>94.05m</td>
<td>6.67m</td>
<td>510.00m</td>
</tr>
<tr>
<td>1027</td>
<td>76.90m</td>
<td>0.00m</td>
<td>560.00m</td>
</tr>
<tr>
<td>137</td>
<td>51.30m</td>
<td>0.00m</td>
<td>900.00m</td>
</tr>
<tr>
<td>161</td>
<td>18.81m</td>
<td>0.00m</td>
<td>2853.33m</td>
</tr>
<tr>
<td>135</td>
<td>1.43m</td>
<td>0.00m</td>
<td>13.33m</td>
</tr>
<tr>
<td>1</td>
<td>0.84m</td>
<td>0.00m</td>
<td>26.67m</td>
</tr>
<tr>
<td>33438</td>
<td>0.19m</td>
<td>0.00m</td>
<td>23.33m</td>
</tr>
<tr>
<td>33436</td>
<td>0.15m</td>
<td>0.00m</td>
<td>30.00m</td>
</tr>
<tr>
<td>Others</td>
<td>2.24m</td>
<td>0.00m</td>
<td>46.67m</td>
</tr>
</tbody>
</table>

September 17, 2005
Public Statistics – Top TCP Ports

**Daily Top 10 Destination TCP Ports -- GMT**

<table>
<thead>
<tr>
<th>Port</th>
<th>Average (bytes/s)</th>
<th>Min (bytes/s)</th>
<th>Max (bytes/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>730.92</td>
<td>263.89</td>
<td>1968.32</td>
</tr>
<tr>
<td>445</td>
<td>451.76</td>
<td>18.94</td>
<td>2853.51</td>
</tr>
<tr>
<td>3127</td>
<td>259.07</td>
<td>0.00</td>
<td>7684.20</td>
</tr>
<tr>
<td>135</td>
<td>124.78</td>
<td>5.99</td>
<td>871.34</td>
</tr>
<tr>
<td>80</td>
<td>55.77</td>
<td>4.01</td>
<td>389.67</td>
</tr>
<tr>
<td>139</td>
<td>50.66</td>
<td>5.28</td>
<td>249.49</td>
</tr>
<tr>
<td>4899</td>
<td>19.99</td>
<td>0.00</td>
<td>232.58</td>
</tr>
<tr>
<td>1025</td>
<td>10.42</td>
<td>0.48</td>
<td>44.41</td>
</tr>
<tr>
<td>22</td>
<td>8.75</td>
<td>0.00</td>
<td>520.95</td>
</tr>
<tr>
<td>5000</td>
<td>8.11</td>
<td>0.00</td>
<td>42.60</td>
</tr>
<tr>
<td>Others</td>
<td>58.04</td>
<td>6.91</td>
<td>970.72</td>
</tr>
</tbody>
</table>

September 21, 2005
Public Statistics – Top Country Codes

September 21, 2005
Public Statistics – Top Source OS

Daily Top 10 Windows Source OS -- GMT

<table>
<thead>
<tr>
<th>Source OS</th>
<th>Average</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows-XP-SP1/Windows-2000-SP2+</td>
<td>7.11</td>
<td>1.03</td>
<td>76.24</td>
</tr>
<tr>
<td>Windows-XP-SP1/Windows-2000-SP4</td>
<td>4.89</td>
<td>0.65</td>
<td>21.38</td>
</tr>
<tr>
<td>Windows-XP/Windows-2000-SP3</td>
<td>3.88</td>
<td>0.57</td>
<td>10.14</td>
</tr>
<tr>
<td>Windows-XP/Windows-2000-SP2</td>
<td>3.42</td>
<td>0.04</td>
<td>14.96</td>
</tr>
<tr>
<td>Non-Windows</td>
<td>0.60</td>
<td>0.00</td>
<td>4.11</td>
</tr>
<tr>
<td>Windows-2000/Windows-XP</td>
<td>0.11</td>
<td>0.00</td>
<td>5.87</td>
</tr>
<tr>
<td>Windows-2000-RFC1323/Windows-XP-RFC1323</td>
<td>0.05</td>
<td>0.00</td>
<td>1.75</td>
</tr>
<tr>
<td>Windows-NT-4.0</td>
<td>0.03</td>
<td>0.00</td>
<td>0.81</td>
</tr>
<tr>
<td>Windows-98</td>
<td>0.03</td>
<td>0.00</td>
<td>2.30</td>
</tr>
<tr>
<td>Windows-XP-SP3/Windows-2000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.05</td>
</tr>
<tr>
<td>other-Windows</td>
<td>0.00</td>
<td>0.00</td>
<td>0.07</td>
</tr>
</tbody>
</table>

September 13, 2005
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 (e.g. Team Cymru)
Architecture advantages

- Few false positives
- Ability to collect malware samples
  - specific listeners: mydoom, kuang, subseven, etc.
- Ability to implement spam traps
- Permits the members expertise’s improvement in several areas:
  - honeypots, intrusion detection, PGP, firewalls, OS hardening
Architecture disadvantages

• It’s more difficult to maintain
• Usually don’t catch attacks targeted to production networks
• Need the partners cooperation to maintain and update the honeypots
Future Work

• Continuously expand the network
  – 4 new partners in installation phase
  – 17 partner candidates

• Have more frequent private summaries

• Provide monthly, weekly, and hourly public statistics

• Increase data donation to trusted parties
Related Links

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

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

- Brazilian Internet Steering Committee – CGI.br
  http://www.cgi.br/

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

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

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