Incident Handling and Internet Security in Brazil

Cristine Hoepers
<cristine@cert.br>

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Computer Emergency Response Team Brazil
http://www.cert.br/

Comitê Gestor da Internet no Brasil
Brazilian Internet Steering Committee
http://www.cgi.br/

Agenda

• CERT.br
  – Mission
  – CGI.br Structure
• History of Incident Response in Brazil
• CERT.br Activities
  – Training, Early Warning, Awareness, Partnerships, etc
• Other Initiatives Related to Security
• References
CERT.br

- Created in 1997 to receive, review and respond to computer security incident reports and activities related to networks connected to the Internet in Brazil.
  - National focal point for reporting security incidents
  - Establish collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling
  - Produce best practices’ documents
  - Help raise the security awareness in the country
  - Forum of Incident Response and Security Teams (FIRST)
  - Full member (http://www.first.org/membership/)

http://www.cert.br/mission.html

The Brazilian Internet Steering Committee (CGI.br)

1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – National Forum of Estate Science and Technology Secretaries
10 – Internet Expert
11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

http://www.cgi.br/internacional/
History of CSIRTs in Brazil

- **August/1996**: CGI.br released the document: “Towards the Creation of a Security Coordination Center for the Brazilian Internet.”¹
- **June/1997**: CGI.br created CERT.br (at that time called NBSO - NIC BR Security Office), based on the report’s recommendation²
- **August/1997**: the Brazilian Research Network (RNP) created its own CSIRT (CAIS)³, followed by the Rio Grande do Sul State, that created CERT-RS⁴
- **1999**: other institutions, including Universities and Telecommunication Companies announced their CSIRTs
- **2003**: more than 20 CSIRTs formed
- **2004**: CTIR Gov was created, with the Brazilian Federal Government Administration as their constituency⁵

¹[http://www.nic.br/grupo/historico-gts.htm](http://www.nic.br/grupo/historico-gts.htm)  
²[http://www.nic.br/grupo/gts.htm](http://www.nic.br/grupo/gts.htm)  
³[http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf](http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf)  
⁴[http://www.cert-rs.tche.br/cert-rs.html](http://www.cert-rs.tche.br/cert-rs.html)  
⁵[http://www.ctir.gov.br](http://www.ctir.gov.br)
CERT.br Activities

Incident Handling and Statistics

http://www.cert.br/stats/incidentes/
http://www.cert.br/stats/spam/

Anti-Fraud Activities

- In Brazil fraud is almost all based on malicious codes disseminated through social engineering

- CERT.br and Financial Institutions:
  - Share technical details about crimeware, new social engineering techniques, malicious codes, etc
  - CERT.br:
    - Notifies sites hosting crimeware related to frauds
    - Coordinates with international sites and CSIRTs to take down the crimeware sites
    - Send new crimeware (trojans, keyloggers, etc) to 24 anti-virus vendors
    - Anti-Phishing Working Group (APWG) Research Partner
      - http://www.antiphishing.org/

Trojan Notification System

- emails
- trojanfilter
  - Extract suspicious URLs from emails
  - URLs
- sm2av
  - Select new malware from malware list
  - Send malware copy to each AV vendor that does not detect the malware yet
- email with the malware copy
- malware files (confirmed)
- trojanchec
  - Fetch and store malware candidate
  - Using AV, confirm if file is really a malware
  - Create a list with the confirmed URLs
- list entry
- IP, data, URL, AV signature
- notify
  - Get IP contacts
  - Create email with the list entry data and a email template
  - Send notification asking to remove the malware
- email with the notification
- lonline
  - Try to fetch malware in order to check if it is still online
  - Update stats DB including the new data and status of the malware URL
Best Practices for Internet Users

- Protecting your identity
  - Monitor your credit report
  - Use strong passwords
  - Keep your personal information secure

- Protecting your devices
  - Install security software
  - Keep your software updated
  - Use firewalls

- Protecting your sensitive information
  - Use secure websites
  - Be cautious with emails
  - Use strong encryption

- Protecting your network
  - Use a strong Wi-Fi password
  - Keep your network offline
  - Use a virtual private network (VPN)

Best Practices for Internet Users - Tips

- Protect against fraud
  - Be cautious with online transactions
  - Avoid giving out personal information
  - Use a secure payment method

- Protect against malware
  - Install and update antivirus software
  - Be cautious with email attachments
  - Use a firewall

- Protect against hacking
  - Use strong passwords
  - Update your software regularly
  - Be cautious with suspicious websites

- Protect against phishing
  - Avoid clicking on suspicious links
  - Use a phishing filter
  - Be cautious with emails from unknown senders

Trend Analysis and Early Warning

Brazilian Honeypots Alliance - Distributed Honeypots Project

Objective: to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 35 partner’s institutions:
  - Academic, government, industry, telecom and military networks
  - Widely distributed across the country
  - Based on voluntary work
  - Maintain public statistics
  - http://www.honeypots-alliance.org.br/

- Honeynet Research Alliance Member since June 2002
  http://honeynet.org/alliance/

Cities Where the Honeypots are Located
Partners of the Brazilian Honeypots Alliance

<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, Embratel, Flócruz, IME, PUC-RIO, RedeRio, UFRJ</td>
</tr>
<tr>
<td>03</td>
<td>São Paulo</td>
<td>ANSP, CERT.br, Dimeo, Durand, UNESP, USP</td>
</tr>
<tr>
<td>04</td>
<td>Campinas</td>
<td>CenPRA, HP Brazil, ITAL, UNICAMP, UNICAMP FECC</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>Linha</td>
<td>FPTE</td>
</tr>
<tr>
<td>19</td>
<td>Uberlândia</td>
<td>CTBC Telecom</td>
</tr>
<tr>
<td>20</td>
<td>Santo André</td>
<td>VIVAX</td>
</tr>
<tr>
<td>21</td>
<td>Passo Fundo</td>
<td>PF-FPR</td>
</tr>
<tr>
<td>22</td>
<td>Curitiba</td>
<td>PoP-PR</td>
</tr>
<tr>
<td>23</td>
<td>Belém</td>
<td>UFPA</td>
</tr>
</tbody>
</table>


Honeypots Flows - Top Destination TCP Ports


Honeypots Flows - Top Source Country Codes

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


Daily Top 10 Source OS -- GMT
Support for new CSIRTs

• Help new CSIRTs to establish their activities
  – Meetings, presentations to C-level managers, training, etc

• SEI^{SM}/CMU Partner, licensed to deliver CERT® Program courses in Brazil:
  • Creating a Computer Security Incident Response Team
  • Managing Computer Security Incident Response Teams
  • Fundamentals of Incident Handling
  • Advanced Incident Handling for Technical Staff
  – 160+ incident handlers trained

http://www.cert.br/cursos/

Other CGI.br Initiatives Related to Security
CGI.br Anti-Spam Commission

- Created by CGI.br to articulate, with all players, viable solutions to reduce the spam problem
  [http://www.cgi.br/sobre-cg/antispam.htm](http://www.cgi.br/sobre-cg/antispam.htm)

- Produced material that include tips for preventing from security problems coming through email
  - All material available at the [www.antispam.br](http://www.antispam.br) site

- CERT.br helped to produce 2 documents
  - Technologies and Policies to Fight Spam
  - Technical Analysis of Anti-spam Legislation

The antispam.br website
Malicious codes and their relation to emails

Frauds that come through emails
Tips to prevent spam and security problems

CGI.br Indicators

- Survey on the Use of Information and Communication Technologies In Brazil 2005
- Includes indicators about security and spam
  - **Households**: security problems encountered, security measures adopted, antivirus updating frequency, frequency they receive spam, time spent with spam, etc.
  - **Enterprises**: identified IT security problems, security measures adopted, antivirus updating frequency, technologies adopted for secure communication, etc.

http://www.nic.br/indicadores/
http://www.nic.br/indicadores/indicadores.pdf
References

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

- CSIRT development references (English and Portuguese)
  http://www.cert.br/csirts/

- Best Practices in Portuguese:
  • Tips for home users (Cartilha de Segurança para Internet)
    http://cartilha.cert.br/
  • Security Best Practices for System and Network Administrators
    (Práticas de Segurança para Administradores de Redes Internet)
    http://www.cert.br/seg-adm-redes/

- SEI®/CMU CERT® Program Courses delivered by CERT.br
  http://www.cert.br/cursos/

- CERT.br Statistics
  http://www.cert.br/stats/

- Comitê Gestor da Internet - CGI.br: http://www.cgi.br/

- CGI.br Indicators: http://www.nic.br/indicadores/

References (cont)

CSIRTs around the world:

- FIRST Member Teams
  http://www.first.org/about/organization/teams/

- National Computer Emergency Response Teams
  http://www.cert.org/csirts/national/contact.html

- TI Directory of European CSIRTs
  http://www.ti.terena.nl/teams/

- APCERT Member Teams
  http://www.apcert.org/about/structure/members.html

- Brazilian CSIRTs Contact Information
  http://www.cert.br/contact-br.html