CERT.br

Incident Handling and Network Monitoring Activities

Cristine Hoepers
General Manager
cristine@cert.br

Computer Emergency Response Team Brazil - CERT.br

Network Information Center Brazil - NIC.br
Brazilian Internet Steering Committee - CGI.br
Agenda

- Our Organization and Mission
  - Brazilian Internet Governance

- CERT.br Incident Handling activities
  - Reactive
  - Proactive
  - Network Monitoring
The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

Among the diverse responsibilities reinforce by the Presidential Decree 4.829, has as the main attributions:

- to propose policies and procedures related to the regulation of Internet activities
- to recommend standards for technical and operational procedures
- to establish strategic directives related to the use and development of Internet in Brazil
- to promote studies and recommend technical standards for the network and services’ security in the country
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- to collect, organize and disseminate information on Internet services, including indicators and statistics

http://www.cgi.br/english/
CGI.br and NIC.br Structure

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
Early Developments on Incident Handling in Brazil

• August/1996: CGI.br released the report: “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), as a CSIRT with national responsibility, based on the report's recommendation\(^2\)

• August/1997: the Brazilian Research Network (RNP) created it’s own CSIRT (CAIS)\(^3\), followed by the Rio Grande do Sul Academic Network (CERT-RS)\(^4\)

• 1999: other institutions, including Universities and Telecommunication Companies started forming their CSIRTs

• 2003/2004: task force to discuss the structure of a CSIRT for the Federal Government Administration

• 2004: CTIR Gov was created, with the Brazilian Federal Government Administration as their constituency\(^5\)

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

- Incident Handling
  - Coordination
  - Facilitation
  - Support
  - Statistics

- Training and Awareness
  - Courses
  - Presentations
  - Documents
  - Meetings

- Network Monitoring
  - Distributed Honeypots
  - SpamPots

Staff:
- 8 Security Analysts
  - 2 with PhD
  - 4 with MSc

Staff background:
- Computer Science or Engineering degrees
- System Administration
- Network Security

Staff shared with NIC.br/CGI.br:
- Administrative Support
- Legal department
- Public Relations
- 24/7 Data Center and Network Operations Support

Staff:
- 8 Security Analysts
  - 2 with PhD
  - 4 with MSc

Staff background:
- Computer Science or Engineering degrees
- System Administration
- Network Security

Staff shared with NIC.br/CGI.br:
- Administrative Support
- Legal department
- Public Relations
- 24/7 Data Center and Network Operations Support

http://www.cert.br/about/
CERT.br

**Incident Handling**
- Coordination
- Facilitation
- Support
- Statistics

**Training and Awareness**
- Courses
- Presentations
- Documents
- Meetings

**Network Monitoring**
- Distributed Honeypots
- SpamPots
CERT.br Incident Handling Activities

- Provides a focal point for incident notification in the country
- Provides the coordination and necessary support for organizations involved in incidents
- Supports the analysis of compromised systems and their recovery process
- Establishes collaborative relationships with other entities, such as other CSIRTs, Universities, ISPs and telecommunication companies
- Maintains public statistics of incidents handled and spam complaints received
Incidents Reported to CERT.br – 1999-2010
Incidents Reported to CERT.br in 2010

Types of Incidents

- Scan (56.54%)
- Worm (12.34%)
- Web (6.10%)
- Intrusion (0.06%)
- DoS (0.14%)
- Other (3.11%)
- Fraud (21.71%)

Types of Fraud

- Malware enabled (57.97%)
- Traditional Phishing - involving phony websites (39.18%)
- Copyright Infringement (1.12%)
- Other (1.74%)

http://www.cert.br/stats/incidentes/
Spams Reported to CERT.br – 2003-Feb/2011

Mainly botnets and open proxies at broadband networks

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

Cyber Security Best Practices Workshop, CICTE/OAS, Mexico City/MX, March 10, 2011
Establishment of new CSIRTs

- Help new Computer Security Incident Response Teams (CSIRTs) to establish their activities
  - meetings, training and presentations at conferences

- SEI/CMU Partner since 2004, delivers in Brazil the following CERT® Program courses:
  - http://www.cert.br/courses/
    - Overview of Creating and Managing CSIRTs
    - Fundamentals of Incident Handling
    - Advanced Incident Handling for Technical Staff
  - 400+ security professionals trained in Brazil
  - Overview of Creating and Managing CSIRTs workshop delivered at 2008, 2009 and 2010 LACNIC Conferences, with permission of SEI/CMU
Brazilian CSIRTs as of March/2011
32 teams with services announced to the public

<table>
<thead>
<tr>
<th>Sector</th>
<th>CSIRTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Responsibility</td>
<td>CERT.br, CTIR Gov</td>
</tr>
<tr>
<td>Government</td>
<td>CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO</td>
</tr>
<tr>
<td>Financial Sector</td>
<td>Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander</td>
</tr>
<tr>
<td>Telecom/ISP</td>
<td>CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO</td>
</tr>
<tr>
<td>Research &amp; Education</td>
<td>GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC/UNESP, TRI</td>
</tr>
<tr>
<td>Other Sectors</td>
<td>CSIRT TIVIT, GRIS Abril</td>
</tr>
</tbody>
</table>

http://www.cert.br/csirts/brazil/
“Cartilha de Segurança para Internet”
http://cartilha.cert.br/
Website and cartoons about spam and security

http://www.antispam.br/

http://www.antispam.br/videos/english/
CERT.br

Incident Handling
- Coordination
- Facilitation
- Support
- Statistics

Training and Awareness
- Courses
- Presentations
- Documents
- Meetings

Network Monitoring
- Distributed Honeypots
- SpamPots
Use of Honeypots for Network Monitoring

honeyTARG

This site contains statistics, papers and general information about CERT.br activities regarding the use of low-interaction honeypots for Abuse and Threat Analysis.

Currently we have the following projects:

- Spampots
- Distributed Honeypots for Attack Trend Analysis

SpamPots Project

The SpamPots Project uses low-interaction honeypots to gather data related to the abuse of the Internet infrastructure by spammers. The main goals are:

- measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
- help develop the spam characterization research
- measure the abuse of network infrastructure to send spam
- develop better ways to identify phishing and malware

Distributed Honeypots

CERT.br maintains the Distributed Honeypots Project, whose objective is to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet space.

The data produced by the project include:

- Daily summaries to project partners, with detailed information about the traffic observed in each honeypot;
- A system to notify CSIRTs of networks that generate attacks against the honeypots;
- The following public statistics:

Flows

Daily statistics for the network flow data directed to honeypots from the Distributed Honeypots Project

TCP/UDP Port Summary

Port summary statistics for TCP/UDP traffic data directed to honeypots from the Distributed Honeypots Project.
Brazilian Distributed Honeypots Project

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

- Sensors distributed in 22 cities
- Hosted by 46 Partners in
  - government, energy, financial, ISPs, academia
- Based on voluntary work
- Transparent configuration
  - no “black-box”
- No production data is captured
- Each partner can use its sensor as a complement to its own IDS

Data collected is used to
- Notify networks that originate attacks
- Donate data to other National CSIRTs
- Generate public statistics/trends

http://honeytarg.cert.br/honeypots/
### Public Statistics – Country Codes originating Attacks

#### Source Country Codes (CC) – 2011-03-04 GMT

<table>
<thead>
<tr>
<th>#</th>
<th>Key</th>
<th>CC</th>
<th>Name</th>
<th>Total (Bytes)</th>
<th>Max (KB/s)</th>
<th>Avg (B/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>DE</td>
<td>DE</td>
<td>Germany</td>
<td>14.37 MB</td>
<td>1.64 KB/s</td>
<td>166.30 B/s</td>
</tr>
<tr>
<td>02</td>
<td>CN</td>
<td>CN</td>
<td>China</td>
<td>6.24 MB</td>
<td>752.61 B/s</td>
<td>72.19 B/s</td>
</tr>
<tr>
<td>03</td>
<td>US</td>
<td>US</td>
<td>United States</td>
<td>5.70 MB</td>
<td>772.56 B/s</td>
<td>66.02 B/s</td>
</tr>
<tr>
<td>04</td>
<td>MX</td>
<td>MX</td>
<td>Mexico</td>
<td>3.70 MB</td>
<td>779.91 B/s</td>
<td>42.85 B/s</td>
</tr>
<tr>
<td>05</td>
<td>BR</td>
<td>BR</td>
<td>Brazil</td>
<td>3.54 MB</td>
<td>904.43 B/s</td>
<td>40.97 B/s</td>
</tr>
<tr>
<td>06</td>
<td>RU</td>
<td>RU</td>
<td>Russian Federation</td>
<td>2.89 MB</td>
<td>412.92 B/s</td>
<td>33.44 B/s</td>
</tr>
<tr>
<td>07</td>
<td>JP</td>
<td>JP</td>
<td>Japan</td>
<td>1.58 MB</td>
<td>734.93 B/s</td>
<td>18.31 B/s</td>
</tr>
<tr>
<td>08</td>
<td>PL</td>
<td>PL</td>
<td>Poland</td>
<td>820.12 KB</td>
<td>294.33 B/s</td>
<td>9.49 B/s</td>
</tr>
<tr>
<td>09</td>
<td>TW</td>
<td>TW</td>
<td>Taiwan, Province of China</td>
<td>649.69 KB</td>
<td>207.70 B/s</td>
<td>7.52 B/s</td>
</tr>
<tr>
<td>10</td>
<td>EU</td>
<td>EU</td>
<td>NA</td>
<td>379.51 KB</td>
<td>228.13 B/s</td>
<td>4.39 B/s</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>Others</td>
<td>3.49 MB</td>
<td>309.69 B/s</td>
<td>40.36 B/s</td>
</tr>
</tbody>
</table>
### Public Statistics – ASes originating Attacks

![Source AS Numbers (ASN) -- 2011-03-04 GMT](chart.png)

<table>
<thead>
<tr>
<th>#</th>
<th>Key</th>
<th>ASN</th>
<th>Name</th>
<th>CC</th>
<th>Total</th>
<th>Max</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td></td>
<td>8972</td>
<td>PLUSSERVER-AS PlusServer AG, G...</td>
<td>DE</td>
<td>14.16 MB</td>
<td>1.64 KB/s</td>
<td>163.89 B/s</td>
</tr>
<tr>
<td>02</td>
<td></td>
<td>4835</td>
<td>CHINANET-IDC-SN China Telecom ...</td>
<td>CN</td>
<td>3.55 MB</td>
<td>743.61 B/s</td>
<td>41.08 B/s</td>
</tr>
<tr>
<td>03</td>
<td></td>
<td>6503</td>
<td>Axtel, S.A.B. de C.V.</td>
<td>MX</td>
<td>3.32 MB</td>
<td>779.91 B/s</td>
<td>38.43 B/s</td>
</tr>
<tr>
<td>04</td>
<td></td>
<td>12768</td>
<td>ER-TELECOM-AS JSC ER-Telecom</td>
<td>RU</td>
<td>2.45 MB</td>
<td>408.31 B/s</td>
<td>28.32 B/s</td>
</tr>
<tr>
<td>05</td>
<td></td>
<td>8001</td>
<td>NET-ACCESS-CORP - Net Access C...</td>
<td>US</td>
<td>1.40 MB</td>
<td>758.00 B/s</td>
<td>16.25 B/s</td>
</tr>
<tr>
<td>06</td>
<td></td>
<td>46475</td>
<td>LIMESTONENETWORKS - Limestone ...</td>
<td>US</td>
<td>1.24 MB</td>
<td>669.49 B/s</td>
<td>14.32 B/s</td>
</tr>
<tr>
<td>07</td>
<td></td>
<td>4134</td>
<td>CHINANET-BACKBONE No.31,Jin-ro...</td>
<td>CN</td>
<td>1.20 MB</td>
<td>268.80 B/s</td>
<td>13.87 B/s</td>
</tr>
<tr>
<td>08</td>
<td></td>
<td>9371</td>
<td>SAKURA-C SAKURA Internet Inc.</td>
<td>JP</td>
<td>1.01 MB</td>
<td>731.37 B/s</td>
<td>11.73 B/s</td>
</tr>
<tr>
<td>09</td>
<td></td>
<td>27664</td>
<td>CTBC MultimAdia</td>
<td>BR</td>
<td>998.47 KB</td>
<td>869.11 B/s</td>
<td>11.56 B/s</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>33657</td>
<td>CMCS - Comcast Cable Communications</td>
<td>US</td>
<td>778.74 KB</td>
<td>568.75 B/s</td>
<td>9.01 B/s</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>Others</td>
<td></td>
<td>13.25 MB</td>
<td>711.43 B/s</td>
<td>153.38 B/s</td>
</tr>
</tbody>
</table>
Public Statistics – Top TCP Ports Scanned

<table>
<thead>
<tr>
<th></th>
<th>Key</th>
<th>Port</th>
<th>Name</th>
<th>Total</th>
<th>Max</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td></td>
<td>22</td>
<td>SSH (Secure Shell)</td>
<td>33.20 MB</td>
<td>1.77 KB/s</td>
<td>384.24 B/s</td>
</tr>
<tr>
<td>02</td>
<td></td>
<td>445</td>
<td>Microsoft-DS Active Directory</td>
<td>4.26 MB</td>
<td>224.78 B/s</td>
<td>49.28 B/s</td>
</tr>
<tr>
<td>03</td>
<td></td>
<td>139</td>
<td>NETBIOS Session Service</td>
<td>1.01 MB</td>
<td>87.04 B/s</td>
<td>11.70 B/s</td>
</tr>
<tr>
<td>04</td>
<td></td>
<td>9988</td>
<td>Rbot/SpyBot</td>
<td>709.86 KB</td>
<td>602.90 B/s</td>
<td>8.22 B/s</td>
</tr>
<tr>
<td>05</td>
<td></td>
<td>80</td>
<td>HTTP (Hypertext Transfer Protocol)</td>
<td>218.09 KB</td>
<td>69.23 B/s</td>
<td>2.52 B/s</td>
</tr>
<tr>
<td>06</td>
<td></td>
<td>1433</td>
<td>Microsoft SQL Server</td>
<td>142.71 KB</td>
<td>59.49 B/s</td>
<td>1.65 B/s</td>
</tr>
<tr>
<td>07</td>
<td></td>
<td>4899</td>
<td>Radmin (remote administration tool)</td>
<td>99.53 KB</td>
<td>14.83 B/s</td>
<td>1.15 B/s</td>
</tr>
<tr>
<td>08</td>
<td></td>
<td>135</td>
<td>Microsoft RCP</td>
<td>95.22 KB</td>
<td>38.12 B/s</td>
<td>1.10 B/s</td>
</tr>
<tr>
<td>09</td>
<td></td>
<td>1080</td>
<td>SOCKS</td>
<td>92.35 KB</td>
<td>19.72 B/s</td>
<td>1.07 B/s</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>5900</td>
<td>VNC (Virtual Network Computing)</td>
<td>74.83 KB</td>
<td>19.85 B/s</td>
<td>0.87 B/s</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>Others</td>
<td>1.56 MB</td>
<td>45.54 B/s</td>
<td>18.09 B/s</td>
</tr>
</tbody>
</table>
Public Statistics – Top UDP Ports Scanned

<table>
<thead>
<tr>
<th>#</th>
<th>Key</th>
<th>Port</th>
<th>Name</th>
<th>Total</th>
<th>Max</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td></td>
<td>5060</td>
<td>SIP (Session Initiation Protocol)</td>
<td>288.78 KB</td>
<td>45.68 B/s</td>
<td>3.34 B/s</td>
</tr>
<tr>
<td>02</td>
<td></td>
<td>53</td>
<td>DNS (Domain Name System)</td>
<td>175.77 KB</td>
<td>10.41 B/s</td>
<td>2.03 B/s</td>
</tr>
<tr>
<td>03</td>
<td></td>
<td>161</td>
<td>SNMP (Simple Network Management Protocol)</td>
<td>141.68 KB</td>
<td>4.22 B/s</td>
<td>1.64 B/s</td>
</tr>
<tr>
<td>04</td>
<td></td>
<td>137</td>
<td>NETBIOS Name Service</td>
<td>101.30 KB</td>
<td>29.25 B/s</td>
<td>1.17 B/s</td>
</tr>
<tr>
<td>05</td>
<td></td>
<td>1434</td>
<td>Microsoft SQL Monitor</td>
<td>76.68 KB</td>
<td>4.80 B/s</td>
<td>0.89 B/s</td>
</tr>
<tr>
<td>06</td>
<td></td>
<td>21665</td>
<td>n/a</td>
<td>38.14 KB</td>
<td>1.67 B/s</td>
<td>0.44 B/s</td>
</tr>
<tr>
<td>07</td>
<td></td>
<td>36135</td>
<td>n/a</td>
<td>9.80 KB</td>
<td>16.92 B/s</td>
<td>0.11 B/s</td>
</tr>
<tr>
<td>08</td>
<td></td>
<td>35623</td>
<td>n/a</td>
<td>7.36 KB</td>
<td>6.07 B/s</td>
<td>0.09 B/s</td>
</tr>
<tr>
<td>09</td>
<td></td>
<td>39207</td>
<td>n/a</td>
<td>5.37 KB</td>
<td>9.38 B/s</td>
<td>0.06 B/s</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>4903</td>
<td>n/a</td>
<td>4.96 KB</td>
<td>3.38 B/s</td>
<td>0.06 B/s</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Others</td>
<td>Others</td>
<td>136.49 KB</td>
<td>17.00 B/s</td>
<td>1.58 B/s</td>
</tr>
</tbody>
</table>
Public Statistics – Next Month: Heat Maps
The SpamPots Project, coordinated by CERT.br, uses low-interaction honeypots to gather data related to the abuse of the Internet infrastructure by spammers. The main goals are:

- measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
- help develop the spam characterization research
- measure the abuse of network infrastructure to send spam
- develop better ways to
  - identify phishing and malware
  - identify botnets via the abuse of open proxies and relays

**Papers in English**

- **Exploring the Spam Arms Race to Characterize Spam Evolution**
  Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS'10), 2010, Redmond, USA.
  [PDF File] (240 KB)

- **Spam Miner: A Platform for Detecting and Characterizing Spam Campaigns (demo paper)**
  International Conference on Knowledge Discovery and Data Mining (KDD'09), 2009, Paris, France.
  [PDF File] (400 KB)

- **Spamming Chains: A New Way of Understanding Spammer Behavior**
SpamPots Project – Overview of the Architecture

- Network of Honeypots emulating open proxies and SMTP servers
- Capturing 8 million spams/day, on average
- Sensors in cooperation with: CERT.at (AT), AusCERT (AU), CSIRT-USP (BR), CLCERT (CL), CSIRT UTPL (EC), SURFcert (NL), TWCERT/CC (TW), University of Washington (US), CSIRT Antel (UY)
SpamPots Project Objectives

Better understand the abuse of the Internet infrastructure by spammers

• Measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
• Help develop the spam characterization research
• Measure the abuse of end-user machines to send spam
• Use the spam collected to improve antispam filters
• Develop better ways to
  – identify phishing and malware
  – identify botnets via the abuse of open proxies and relays

We provide a grant to the e-Speed Laboratory of the Federal University of Minas Gerais (UFMG) to develop research with the data collected
Improving cooperation in spam fighting

• Provide data to trusted parties
• Help their constituency to identify infected machines
• Identify malware and scams targeting their constituency
• Currently providing data about spams coming from networks assigned to
  – JP - to JADAC / IIJ / JPCERT/CC / Min. of Communications – had a workshop in Brazil with representatives from these organizations and local ISPs and network providers to discuss how to reduce spam and network abuse
  – TW - to NCC-TW – they are using the data to shutdown spammers infrastructures
Links

- CGI.br – Brazilian Internet Steering Committee
  http://www.cgi.br/
- NIC.br – Network Information Center Brazil
  http://www.nic.br/
- CERT.br – Computer Emergency Response Team Brazil
  http://www.cert.br/
- honeyTARG – honeypots for Threats and Abuse passive
  Reconnaissance and information Gathering
  http://honeytarg.cert.br/