Global Field Reports
Brazil

Cristine Hoepers
cristine@cert.br

CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee
CERT.br - Brazilian National CERT

- Created in 1997 to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.
  - National focal point for reporting security incidents
  - Help raise the security awareness in the country
  - Maintain public statistics about incidents and abuse
  - Produce best practices’ documents
  - Develop collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling

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

• Updates
  – Malware statistics
  – Trends
  – Awareness initiatives
Anti-Fraud Activities in Brazil

• CERT.br focus:
  – Notifies sites hosting malware related to frauds
  – Coordinates with international sites and CSIRTs to take down the malware and phishing pages
  – Perform surface analysis
    • Send undetected malware (trojans, keyloggers, etc) to 35+ antivirus vendors
    • Send new trojans to artifact analysis groups

• Financial sector focus:
  – Perform run-time analysis
    • Aim to identify drop boxes, affected banks, see if the countermeasures still work, etc
  – Send all new sites, URLs, malware to CERT.br
# 2008 Malware Statistics: Q1—Q3

<table>
<thead>
<tr>
<th>Category</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntiVirus signatures (unique)</td>
<td>1344</td>
<td>2197</td>
<td>1737</td>
</tr>
<tr>
<td>AntiVirus signatures (grouped by “family”)</td>
<td>47</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>Unique trojan samples (unique hashes)</td>
<td>3823</td>
<td>4450</td>
<td>3156</td>
</tr>
<tr>
<td>File Extensions</td>
<td>64</td>
<td>61</td>
<td>63</td>
</tr>
<tr>
<td>Unique URLs</td>
<td>4718</td>
<td>5550</td>
<td>3885</td>
</tr>
<tr>
<td>Domains</td>
<td>1803</td>
<td>2215</td>
<td>1410</td>
</tr>
<tr>
<td>Unique IP Addresses</td>
<td>1298</td>
<td>1461</td>
<td>1034</td>
</tr>
<tr>
<td>IP Allocation’s Country Codes</td>
<td>58</td>
<td>63</td>
<td>57</td>
</tr>
<tr>
<td>Email notifications sent by CERT.br</td>
<td>4121</td>
<td>4983</td>
<td>3305</td>
</tr>
</tbody>
</table>

Includes:
- Keyloggers
- Screen loggers
- Trojan Downloaders

Does NOT include:
- Bots/Botnets
- Worms
2008 Detection Rate – 1st Semester and 3rd Quarter

~70% of vendors with less than 50%

Only 6 vendors with the detection rate above 70%
The number of malware related frauds dropped 30% on the 3rd quarter.

The number of phishing sites increased 100% in the 3rd quarter.
Other Trends (1/2)

• Google sponsored links
  – Use the word "bank" and some brands as the AdWords
    • direct the users to pages with malware
  – Are always prepaid
  – There is no clear channel on how to complain to Google

• Drive-by downloads
  – not really common, but we have seen some

• Client's hosts file modified by malware
  – really old, but still works
Other Attacks Seen in Brasil (2/2)

• **DNS cache poisoning**
  – One of the major cable providers had one of their recursive servers poisoned
    • google.com.br was directed to a different IP
    • the phony page had links pointing to malware affecting brazilian banks
      – Using data from queries to the brazilian ccTLD (NIC.br) server we identified 11470 vulnerable recursive servers

• **Not** being widely used
  – botnets
  – fast-flux networks
Videos in English

• Version with subtitles already available: http://antispam.br/videos/english/

• Voice-over will be available soon
Additional References

- This presentation (by the end of the month)
  [http://www.cert.br/docs/presentations/](http://www.cert.br/docs/presentations/)

- Awareness videos

- CERT.br
  Computer Emergency Response Team Brazil
  [http://www.cert.br/](http://www.cert.br/)