Financial Fraud Response in Brazil

Challenges and Evolution

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

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

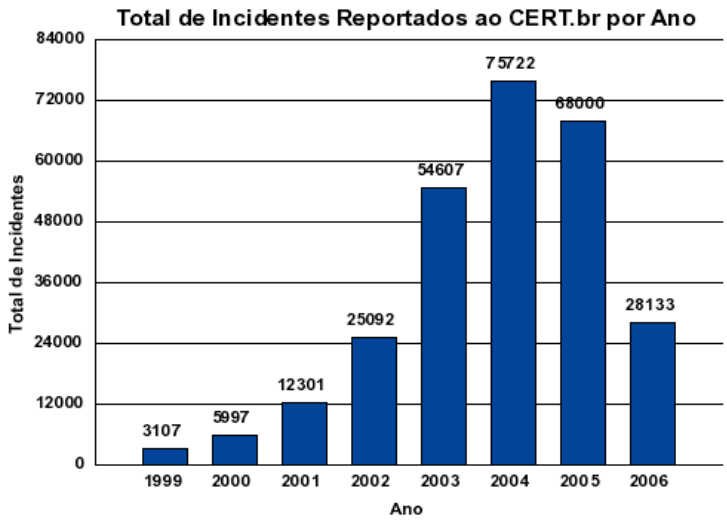
Brazilian Internet Steering Committee - CGI.br
http://www.cgi.br/

Agenda

- Some statistics
- Interaction with Law Enforcement and the Financial Sector
- CERT.br
  - Automation and coordination
- References

Some Statistics

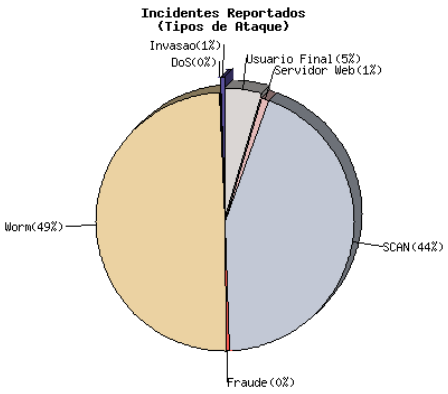
Incidents Reported to CERT.br: 1999-2006



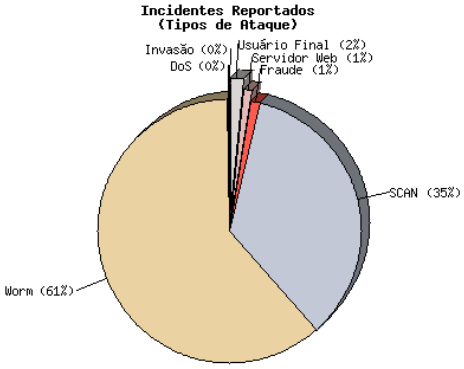
Note: 2006 has data from 1st quarter only.

Incidents Reported to CERT.br

2002

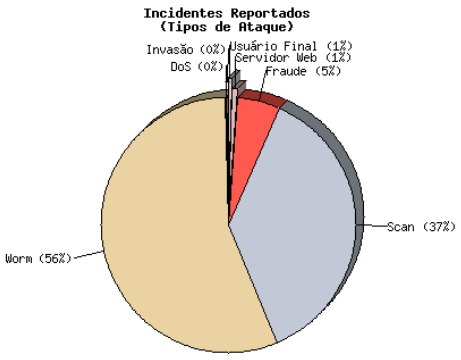


2003

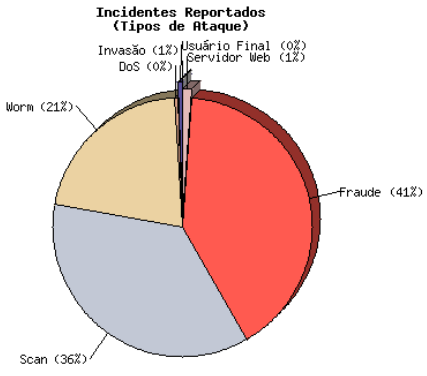


Incidents Reported to CERT.br (cont)

2004

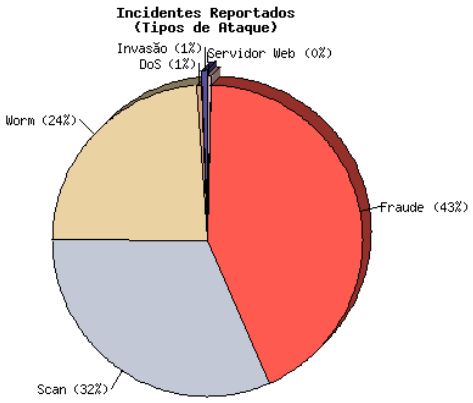


2005



Incidents Reported to CERT.br (cont)

2006 (1st quarter)



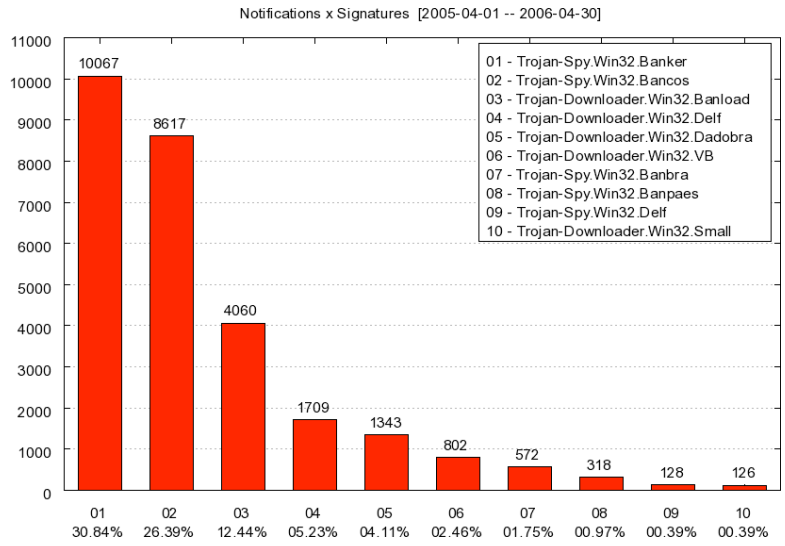
Characteristics of the Frauds Reported

- In Brazil fraud is almost all based on malicious codes disseminated through social engineering
- Vast majority based on spam containing links to trojan horses or trojan downloaders
- Traditional phishing and DNS compromises are rarely seen (very common in 2002/2003)

From April 1st, 2005 to April 30th, 2006

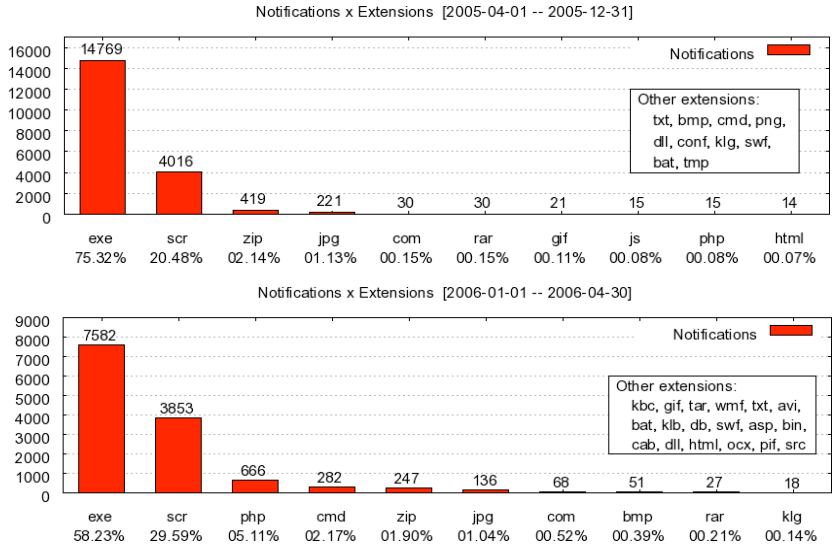
Category	Total
Unique domains hosting trojans	3807
Unique domain contact information	1782
Number of file extensions used	45
Unique filenames used by the trojans	9520
Unique hostnames	6137
Unique IP addresses	3166
Countries that the IPs were allocated to	68
Notifications sent by CERT.br	15556
Unique URLs found in the period	24005
Unique antivirus signatures found	1546

More Common Anti-Virus Signatures

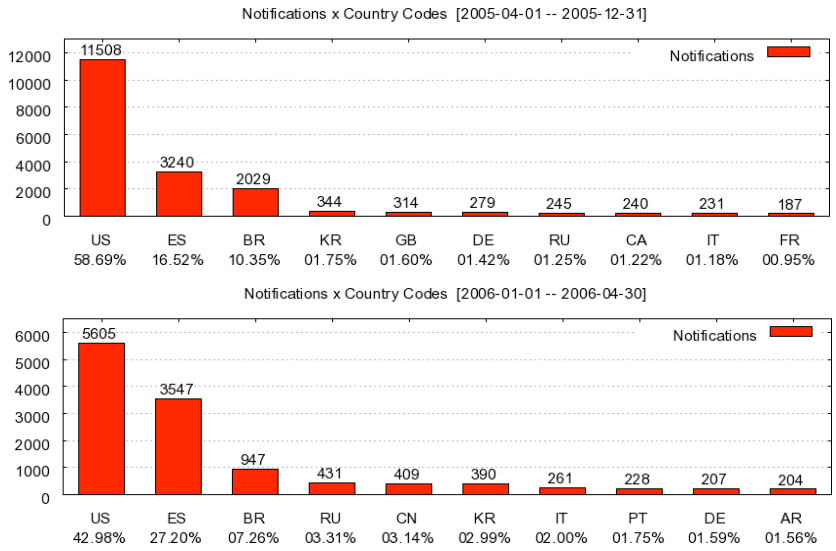


Signature's information source: Kaspersky Lab.

Top 10 File Extensions



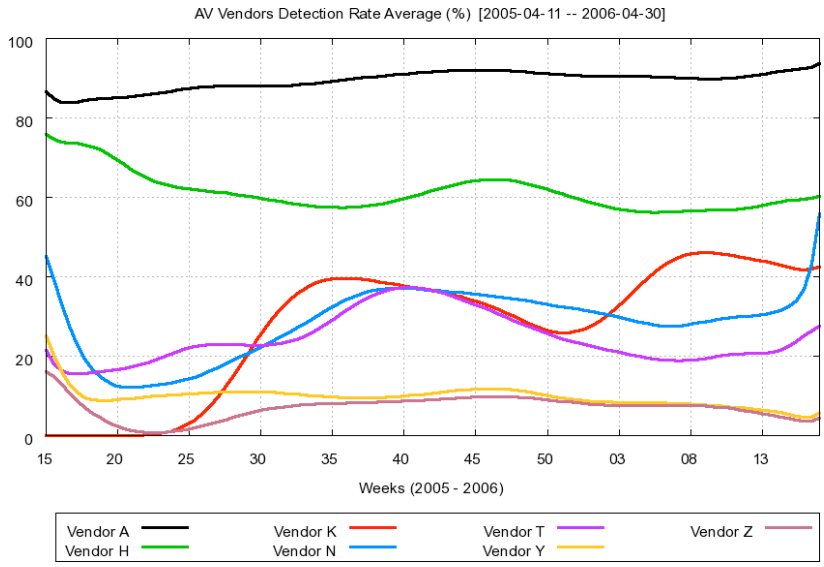
Top 10 Country Codes



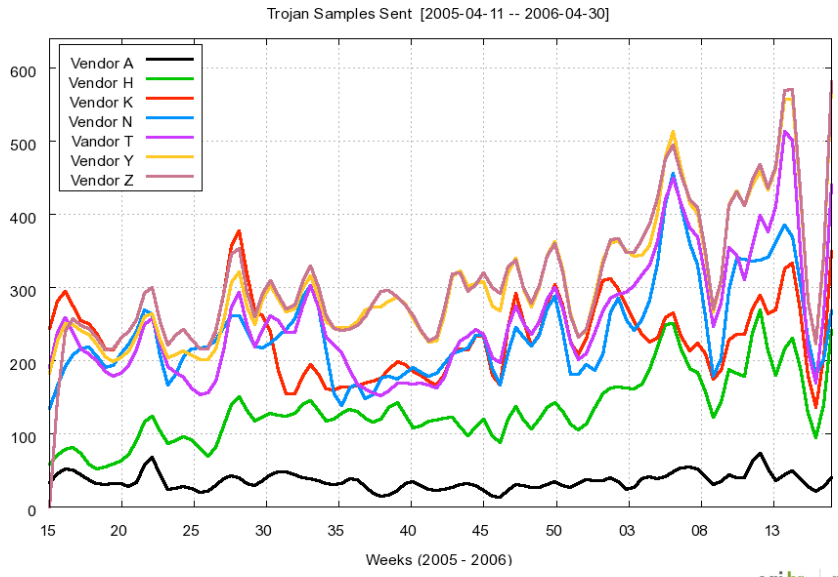
Anti-Virus Efficiency: April/2005 to April/2006

Anti-Virus Vendor	Samples Tested	Samples not Detected	Samples Detected	Detection Rate (%)
Vendor A	18634	1913	16721	89,73
Vendor B	5653	1020	4633	81,96
Vendor D	18519	5475	13044	70,44
Vendor E	18652	6240	12412	66,55
Vendor F	18665	6857	11808	63,26
Vendor G	18348	6750	11598	63,21
Vendor H	18666	7324	11342	60,76
Vendor I	7474	3160	4314	57,72
Vendor K	14603	8873	5730	39,24
Vendor L	18658	11623	7035	37,71
Vendor N	18371	12866	5505	29,97
Vendor O	18606	13084	5522	29,68
Vendor P	14126	10162	3964	28,06
Vendor Q	18541	13395	5146	27,75
Vendor T	18652	14140	4512	24,19
Vendor Y	18469	16713	1756	9,51
Vendor Z	15784	14517	1267	8,03

Anti-Virus Vendors Detection Rate



Trojan Samples Sent to the Anti-Virus Vendors



Response and Interactions Between the Several Sectors

Meeting for CSIRTs with National Responsibility - July 2006

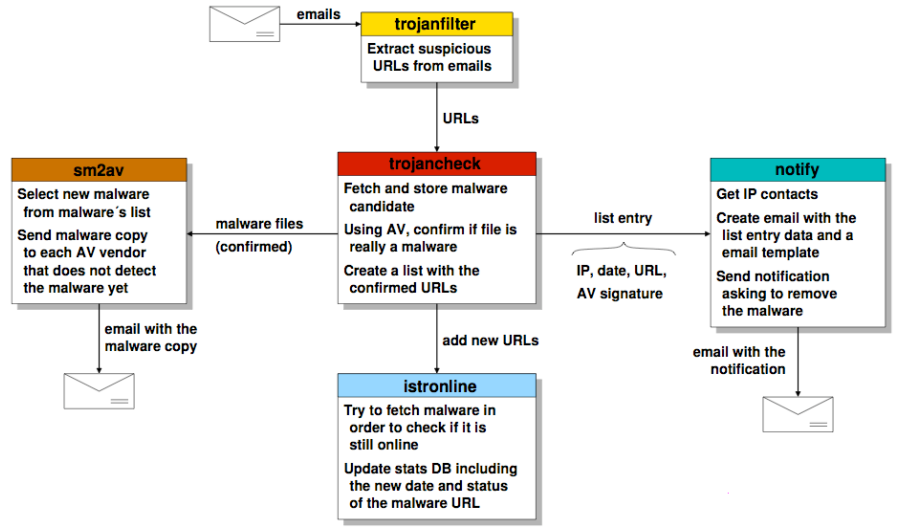
Anti-Fraud Activities

- CERT.br and Financial Institutions' task force:
  - Share technical details about crimeware, new social engineering techniques, malicious codes, etc
  - Discuss incident management
  - Share new trends and technical information related to fraud
- Interaction with Law Enforcement
  - CERT.br
    - Provide training and technical guidance as needed/requested
    - Help victims and banks to interact with the right law enforcement authority
  - Financial Institutions
    - Coordinate efforts with the proper law enforcement agency for each case
    - Preserve clients' machines evidences

Anti-Fraud Activities (cont)

- 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 24+ anti-virus vendors
    - Send new trojans to artifact analysis groups
  - Anti-Phishing Working Group (APWG) Research Partner http://www.antiphishing.org/

CERT.br Response Process and Tools



Educating the End User

CGI.br Indicators

National survey conducted by CGI.br in August 2005

- Is the Brazilian official survey on the use information and communication technologies in Brazil
- The survey included the following areas related to security and abuse:
  - **ICT Households**: security problems encountered, security measures adopted, antivirus updating frequency, frequency they receive spam, time spent with spam, etc.
    - F - Security
    - J - Spam
  - **ICT Enterprises**: identified IT security problems, security measures adopted, antivirus updating frequency, technologies adopted for secure communication, etc.
    - E - Security

ICT Households

F1 - Security problems faced using the Internet

Percentage over the number of individuals who used the Internet in the 3 months prior to the survey

	None	Virus (un-authorized access)	Virus (software or hardware damage)	Abuse of personal information	Financial Fraud	Other	Don't Remeber
Total	40,99	19,64	7,13	1,67	0,94	1,10	0,24

F2 - Computer security measures adopted

Percentage over the number of individuals who have Internet access at home

	Anti-Virus	Personal Firewall	Anti-spyware Software
Total	69,76	19,33	22,09

F3 - Anti-Virus updating frequency

Percentage over the number of individuals who have Internet access at home

	Daily	Weekly	Monthly	Every 3 Months	Didn't Update
Total	21,11	27,01	17,37	3,47	31,03

Notes -- *number of individuals who used the Internet in the 3 months prior to the survey: ~44 million people*
number of individuals who have internet access at home: ~17 million people

Best Practices for Internet Users

Best Practices for Internet Users - Tips

The antispam.br website

Malicious codes and their relation to emails

Frauds that come through emails

Tips to prevent spam and security problems