Fraud and Phishing Scam Response Arrangements in Brazil

Marcelo H. P. C. Chaves

mhp@cert.br

Computer Emergency Response Team Brazil – CERT.br

http://www.cert.br/

Brazilian Internet Steering Committee

http://www.cgi.br/

Overview

- Financial Sector Statistics
- Short timeline of Internet bank fraud in Brazil
- Current trends
- Current developments
- Statistics
  - trojan notifications
  - AV vendors efficiency
- Further developments needed

Financial Sector Statistics

Financial Sector Statistics

End of 2004: 164 banks

- 88 – national and private
- 62 – foreign and private
- 14 – public → 44% of the service network

Service Evolution

indicators	2000 (%)	2004 (%)
Internet Banking	3.7	13
self–service	33.5	32.4
automatic debits	27	27
tellers	20.4	12
debit cards	1.6	4.1

indicators	number (Mi)*
checking accounts	73
savings accounts	67
I.B. end users	18.1
I.B. com. users	1.9

* end of 2004

Source: Brazilian Bankers’ Association (FEBRABAN)

Short Timeline of Internet Bank Fraud in Brazil

Timeline of Internet bank fraud in Brazil

- 2001: brute force attacks using easy passwords
- 2002–2003: increase in phishing with heavy use of compromised DNS servers
- 2003–2004: increase in sophisticated phishing
  - fraudulent homepages very similar to the real ones
  - data sent from fraudulent homepages to other homepages, that process the data and send results to email accounts

Current Trends

Current Trends

Traditional phishing and compromised DNS servers are rarely seen.

The current scheme is:

- the criminals send spams using the names of well-known entities or popular sites (government, telecom, airline companies, charity institutions, reality shows, e-commerce, etc)
- these spams have links to trojan horses hosted at various sites
- the victim usually never associates the spam with a banking fraud

Current Trends (cont.)

Once installed, the trojan has the hability to:

- monitor the victim's computer looking for accesses to Brazilian well-known banks
- capture keystrokes and mouse events, as well as snapshots of the screen
- overlap portions of the victim's screen, hiding information
- send captured information, such as account numbers and passwords, to collector sites or email accounts

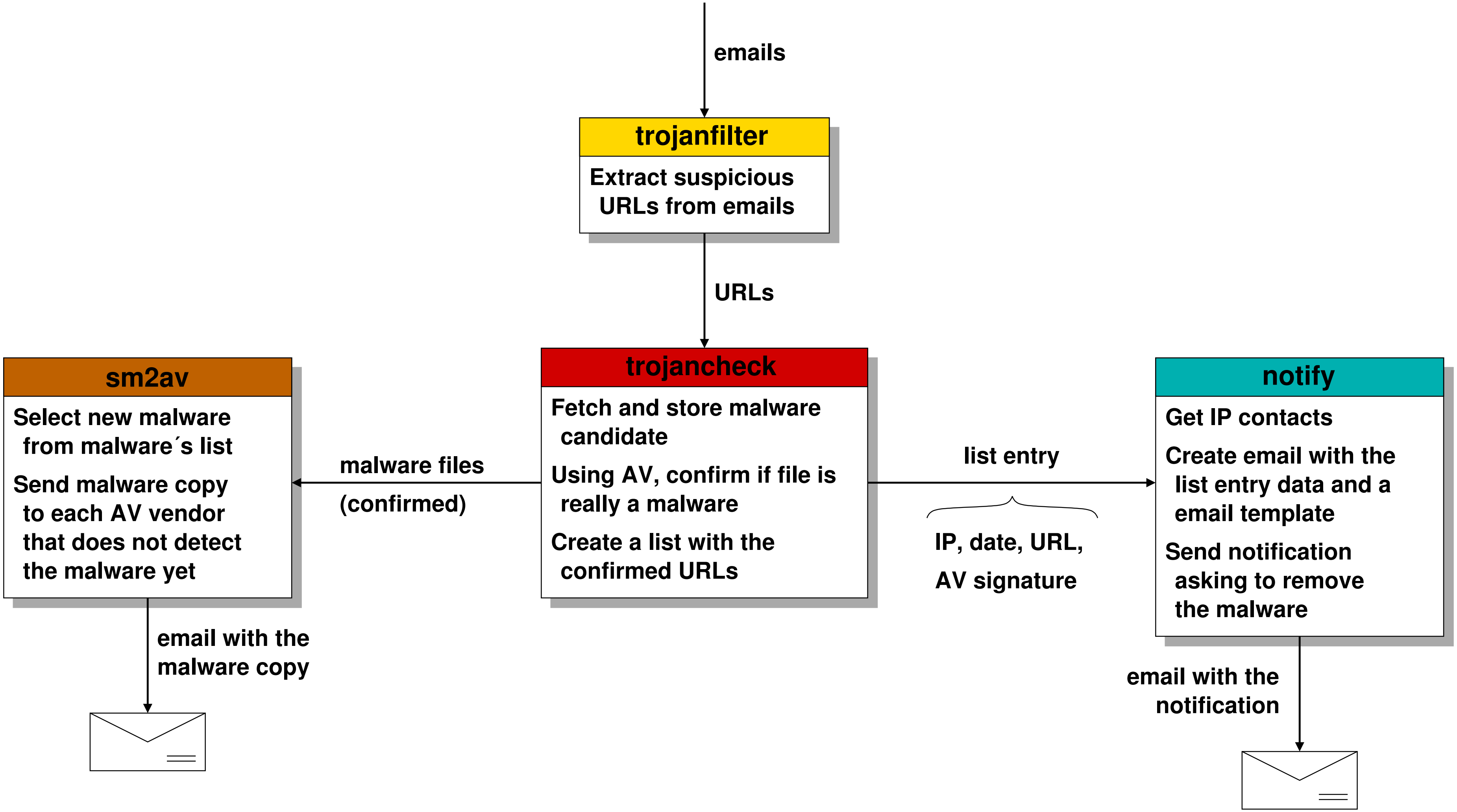
Current Trends (cont.)

- today most trojans are hosted at major ISPs
- we are seeing an increase in
  - defacers working for the criminals and uploading trojans together with their defacements
  - low profile intrusions with trojans hidden and remaining undetected by the site owners
    - usually very difficult to find the proper site contact

Current Developments

CERT.br Initiatives

Trojan notification and submission system



emails

trojanfilter

Extract suspicious URLs from emails

URLs

trojancheck

Fetch and store malware candidate

Using AV, confirm if file is really a malware

Create a list with the confirmed URLs

malware files (confirmed)

sm2av

Select new malware from malware´s list

Send malware copy to each AV vendor that does not detect the malware yet

email with the malware copy

list entry

IP, date, 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

CERT.br Initiatives (cont.)

- notifying sites hosting trojans
- sending undetected trojan samples to 25 AV vendors
  - aim is to increase AV effectiveness
- the documents aimed to home users were revised, focusing on Internet frauds and social engineering

CERT.br Initiatives (cont.)

- a task force between CERT.br and 9 biggest banks
  - PGP mailing list maintained by CERT.br
  - CERT.br facilitates exchange of technical information
  - banks coordinate efforts with the proper law enforcement agency for each case

Statistics

Top Trojan Hosting Domains

Number of times a domain was referenced in spams, and was hosting a trojan candidate

- 2005-04-01 – 2005-09-20 → 420266 emails, 541870 URLs

number	domain
140263	America Online*
26485	gratisweb.com
19655	spectrogariaclips.inf.br
14097	thefilebucket.com
9797	ripway.com
9499	noti-auto.com.ar
8608	atspace.com
7863	cartoesmagicos.com.br
6516	ncren.net
6141	terra.com.br

* `aol.{co.uk,com.br,de,com.au}, netscape.com, americaonline.com.{ar,mx,br}`

Trojan Notifications

Summary: 2005-04-01 – 2005-09-20

counter	number
domains	1409
contacts	772
extensions	16
filenames	3424
hosts	2228
IP addresses	1223
country codes	52
e-mails sent	5671
URLs	8540
AV signatures	575

Total amount of URLs notified = 11687 (with repetition)

Trojan Notifications (cont.)

Top 10 domains notified

number	(%)	domain
5245	44.88	America Online*
1154	9.88	gratisweb.com
140	1.20	terra.com.br
134	1.15	100free.com
132	1.13	galeon.com
127	1.09	webcindario.com
124	1.06	pop.com.br
102	0.87	atspace.com
99	0.85	tripod.com.br
91	0.78	yahoo.com.br

* `aol.{co.uk,com.br,de,com.au}, americaonline.com.{ar,mx,br}, netscape.com`

Trojan Notifications (cont.)

Top 12 extensions and country codes (CC)

number	(%)	extension
8860	75.84	exe
2394	20.49	scr
274	2.35	zip
76	0.65	jpg
16	0.14	com
16	0.14	rar
15	0.13	js
11	0.09	txt
10	0.09	html
3	0.03	dll
2	0.02	gif
2	0.02	swf

number	(%)	CC
1836	46.41	US
813	20.55	BR
200	5.06	ES
152	3.84	KR
108	2.73	DE
108	2.73	IT
105	2.65	UK
93	2.35	CA
93	2.35	RU
47	1.19	AR
45	1.14	FR
41	1.04	CN

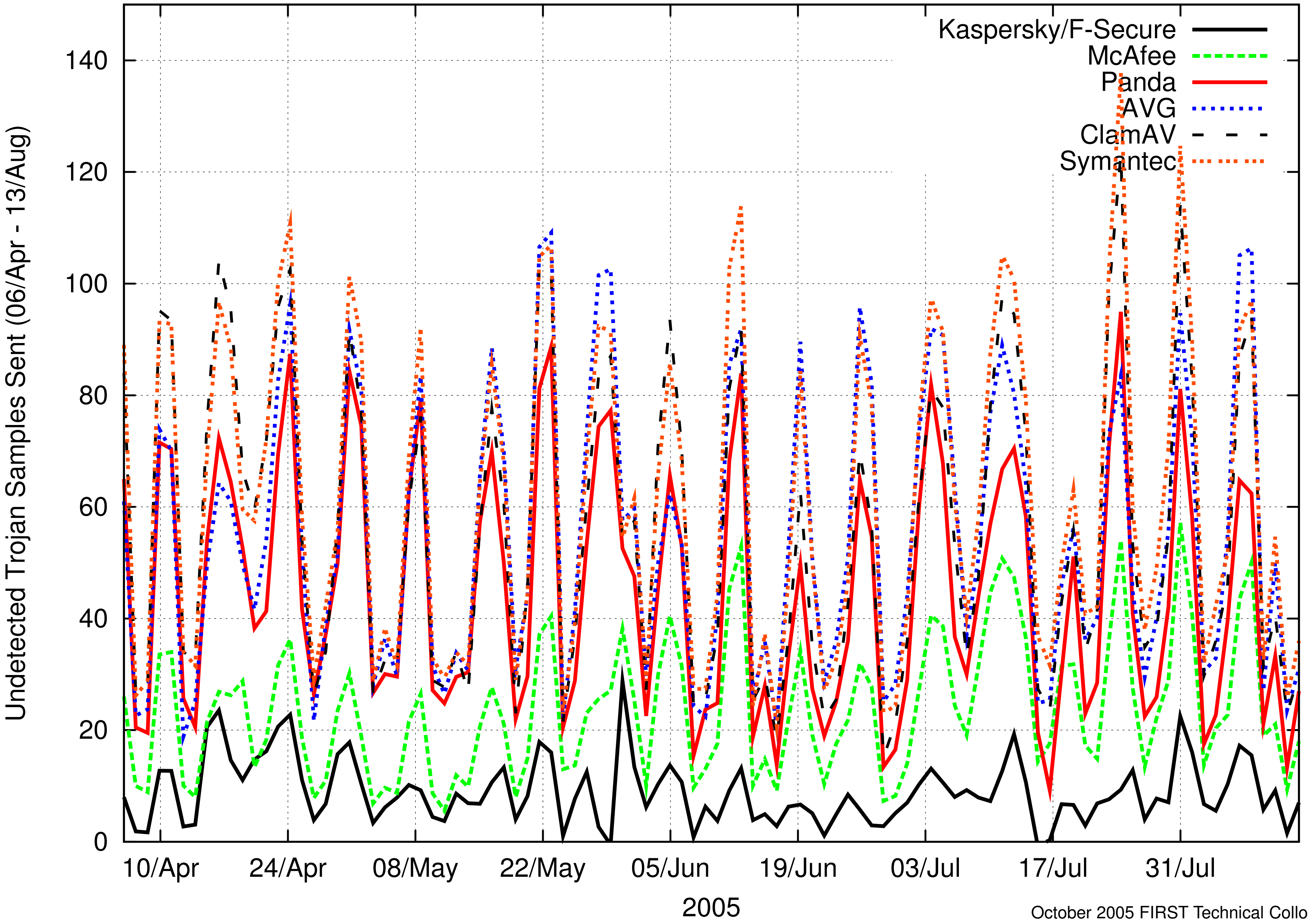
AV Vendors Efficiency

Period: 2005-04-06 – 2005-09-21

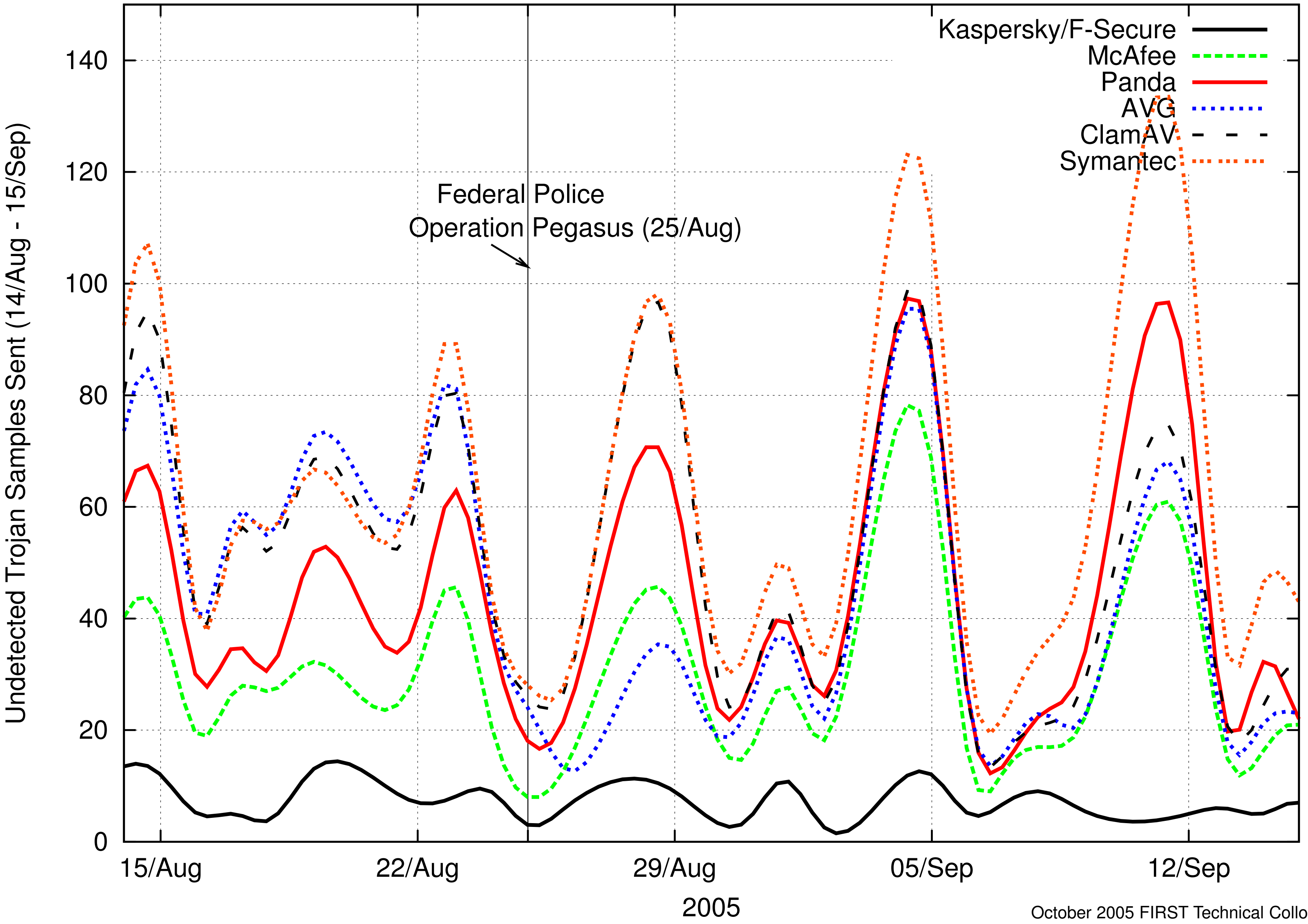
Sent a total of 6633 samples to AV vendors

Antivirus Vendor	samples	detected
Kaspersky	857	87.08 %
F-Secure	857	87.08 %
Sybari	2001	69.83 %
McAfee	2456	62.97 %
DrWeb	2706	59.20 %
Panda	4265	35.70 %
Fortinet	4408	33.54 %
eTrust-Iris	4944	25.46 %
AVG	5085	23.34 %
ClamAV	5177	21.95 %
Symantec	5916	10.81 %
eTrust-Vet	6152	7.25 %

AV Vendors Efficiency (cont.)



AV Vendors Efficiency (cont.)



Further Developments Needed

Further Developments Needed

- AV software need to better detect trojans
  - most used defense among end users
- ISPs need to be more proactive
  - check files at upload time
- more efforts to block spam at its source
  - working in some technical solutions with telcos and ISPs
- better international cooperation

Contact Information

- Computer Emergency Response Team Brazil – CERT.br

  http://www.cert.br/

- Brazilian Internet Steering Comittee – CGI.br

  http://www.cgi.br/

- Marcelo H. P. C. Chaves <mhp@cert.br>