Fraud and Phishing 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 – CGI.br

http://www.cgi.br/

About CERT.br

- Brazilian National CERT, created in 1997
- Focal point for computer security incident handling
- Provide statistics, best practices and training
- Maintained by the Brazilian Internet Steering Committee
  - composed of 21 members, as follows:

sector	representatives	number
Federal Government	Ministries of Science and Technology, Communications, Defense, Industry, etc, and Telcos Regulatory Agency (ANATEL)	9
Corporate sector	Industry, Telcos, ISPs, users	4
NGO´s	Non–profit organizations, etc	4
Sci. and Tech. Community	Academia	3
	Internet expert	1

Overview

- Short Timeline of Online Fraud in Brazil
  - Timeline of Online Fraud in Brazil
  - Current Trends
- Current Developments
  - CERT.br Initiatives
- Statistics
  - Top Trojan Hosting Domains
  - Trojan Notifications
  - AV Vendors Efficiency
- Brazilian Federal Police Operations
  - 2001 – 2006
- Further Developments Needed

Short Timeline of Online Fraud in Brazil

Timeline of Online Fraud in Brazil

2001

- initial deployment of keyloggers via e-mail
- brute force attacks on bank sites

2002 – 2003

- increase in phishing and widespread use of compromised DNS servers

2003 – 2004

- increase in sophisticated phishing
  - phony sites very similar to the real ones
  - data sent from phony sites to collector sites that processed the data and sent results to e-mail accounts

Timeline of Online Fraud in Brazil (cont.)

2005

- traditional phishing and compromised DNS servers were rarely seen
- the criminals sent spams using the names of well-known entities or popular sites (government, telecom, airline companies, charity institutions, reality shows, e-commerce, etc), as well as varied themes (elections, terrorist attacks, tsunami, fraud warnings, erotic photos, etc)
- these spams had links to trojan horses hosted at various sites
- the victim rarely associated the spam with a banking fraud

Current Trends

2006

Current Trends

Traditional phishing and compromised DNS servers continue to be rarely seen.

The current scheme is:

- spams using even more varied themes
  - usually, the moment dictates what criminals will use
- the spams have links to trojan horses hosted at various sites, but we are observing a considerable increase in the use of:
  - trojan downloaders that lead to the real trojans
  - file hosting sites that masquerade common binary extensions:
    `http://www.z05.zupload.com/dl.php?id=5314`
    `http://www10.rapidupload.com/file.php?id=20865`

Current Trends (cont.)

The victim rarely associates the spam with a banking fraud.

Once installed, the trojan has the ability to:

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

Trojan Worm: a case study

18th of April, 2006: trojan incident reported to CERT.br

- 1st infection vector is unknown
- odd netbios traffic generated by infected machines
- AV signatures: too vague or “no virus found”

20th of April, 2006: specific AV signatures

- Net-Worm.Win32.Banker.a (and others)

Artifact Analysis*

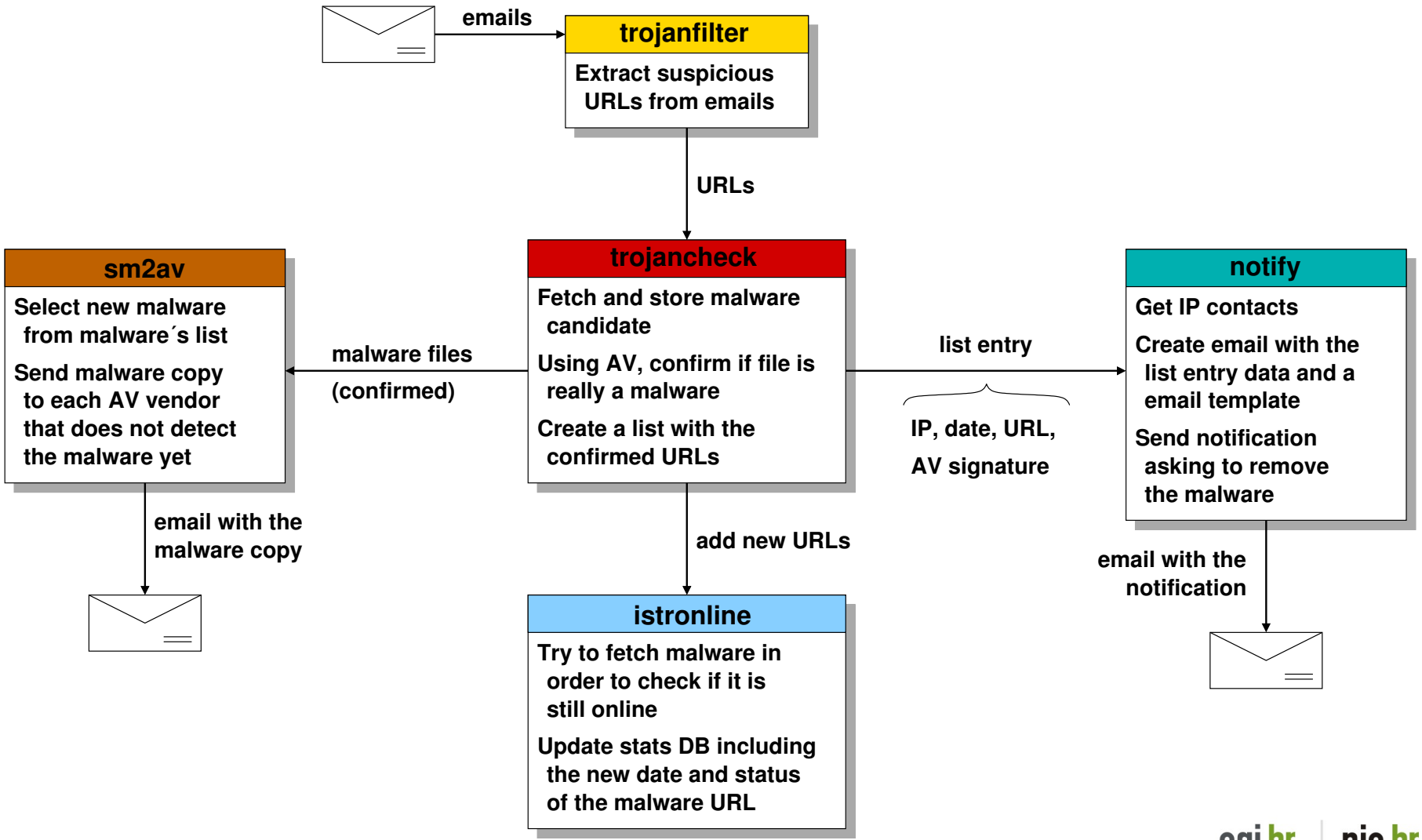
- propagation method: looks for Windows opened shares, tries to copy itself to startup directories
- path is hardcoded: works in Brazilian Windows machines
- trojan capabilities: monitors Web activities, overlaps victim’s screen, captures and sends data via e-mail

* CERT.br would like to thank Visanet CSIRT staff for the analysis

Current Developments

CERT.br Initiatives

Trojan notification and submission system



CERT.br Initiatives (cont.)

Actions:

- notifying sites hosting trojans
- sending undetected trojan samples to 28 AV vendors
  - aim is to increase AV effectiveness
- the documents aimed to home users were revised, focusing on Internet frauds and social engineering

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 – 2006-04-30 → 1063321 e-mails, 1251579 URLs

number	domain
235124	America Online *
94624	GratisWeb **
24656	webcindario.com
21420	sapo.pt
20365	symantek.us
19655	spectrogariaclips.inf.br
14097	thefilebucket.com
12607	aocusa.com
10789	ripway.com
9985	terra.com.br

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

** `gratisweb.com, wanadoo.es, telepolis.com`

Trojan Notifications

Summary: 2005-04-01 – 2006-04-30

counter	number
domains	3807
contacts	1782
extensions	45
filenames	9520
hosts	6137
IP addresses	3166
country codes	68
e-mails sent	15556
unique URLs	24005
AV signatures	1546

Total amount of URLs notified = 32648 (with repetition)

Trojan Notifications (cont.)

Top 10 domains notified: 2005-04-01 – 2006-04-30

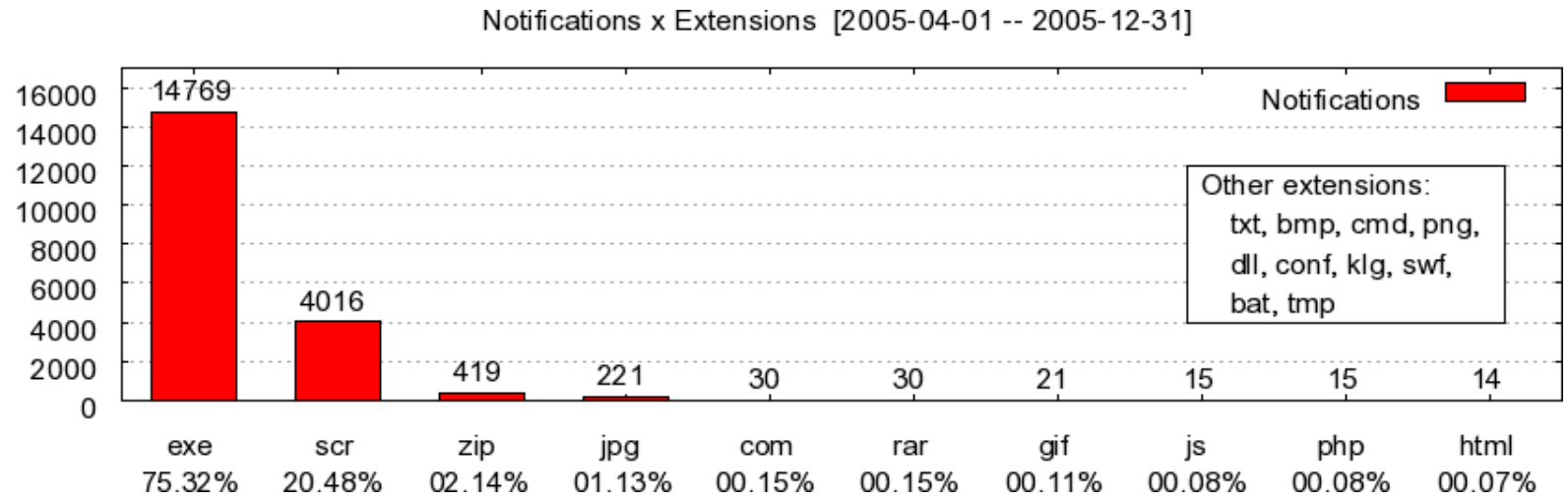
number	(%)	domain
9667	29.61	America Online*
6656	20.39	GratisWeb**
1012	03.10	webcindario.com
433	01.33	rapidupload.com
234	00.72	terra.com.br
200	00.61	uol.com.br
180	00.55	unlugar.com
168	00.51	yahoo.com.br
163	00.50	100free.com
161	00.49	beian.gov.cn

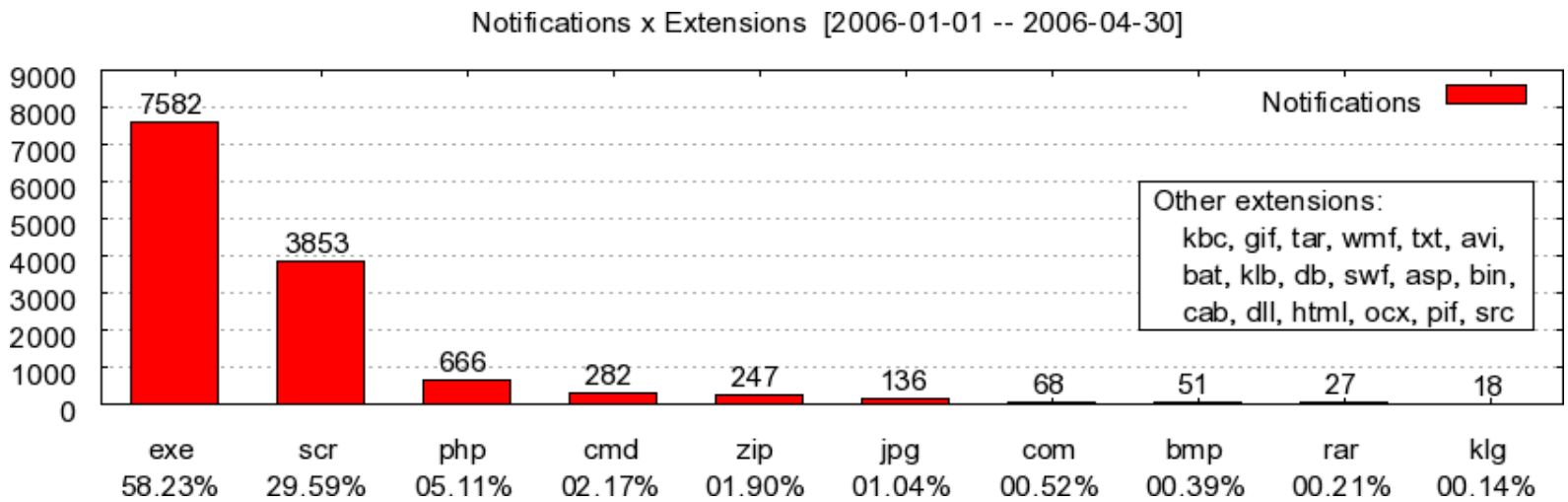
* aol.{co.uk,com.au,com,de,com.br,com.mx,ca}, netscape.com, americaonline.com.{ar,mx,br}

** gratisweb.com, wanadoo.es, telepolis.com

Trojan Notifications (cont.)

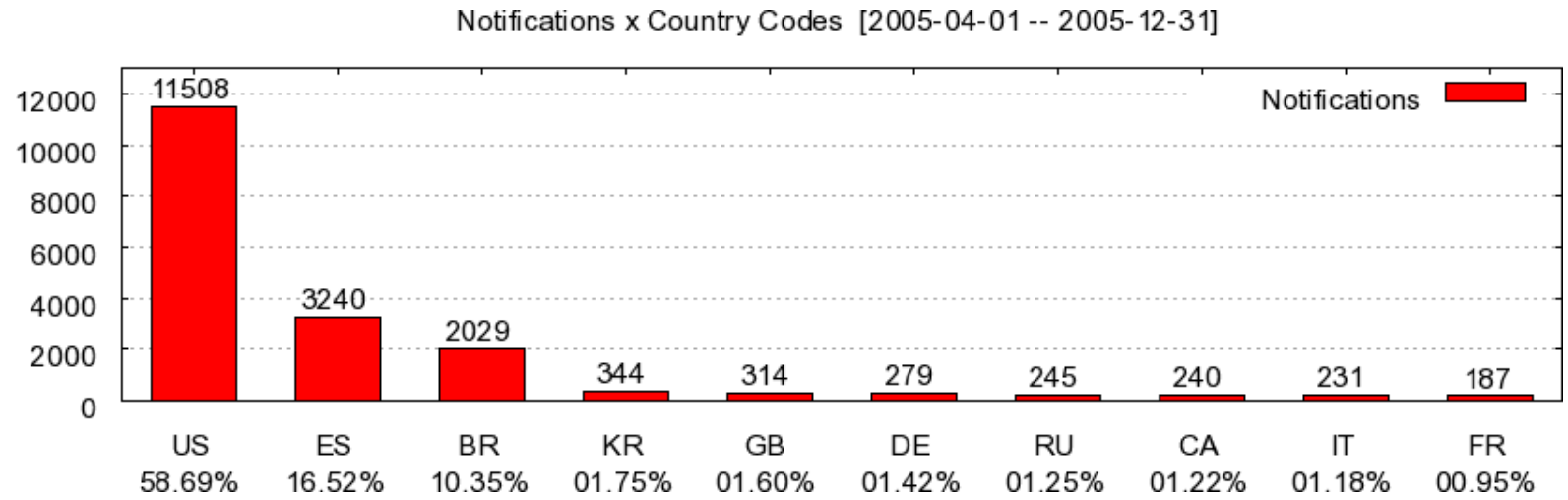
Top 10 extensions

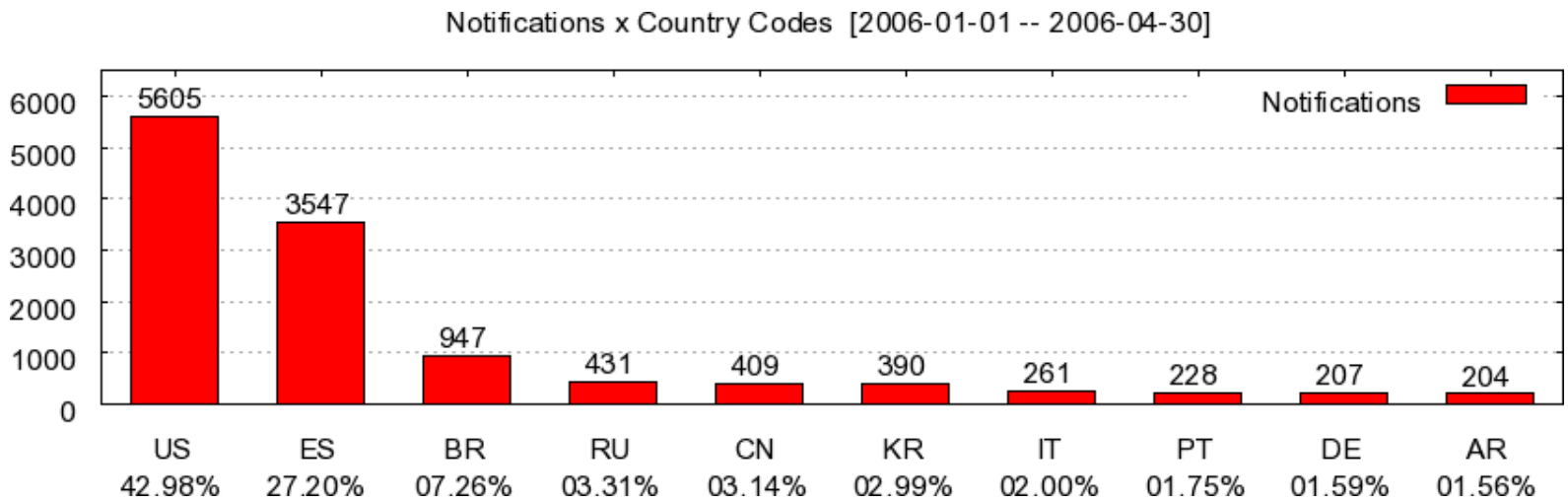




Trojan Notifications (cont.)

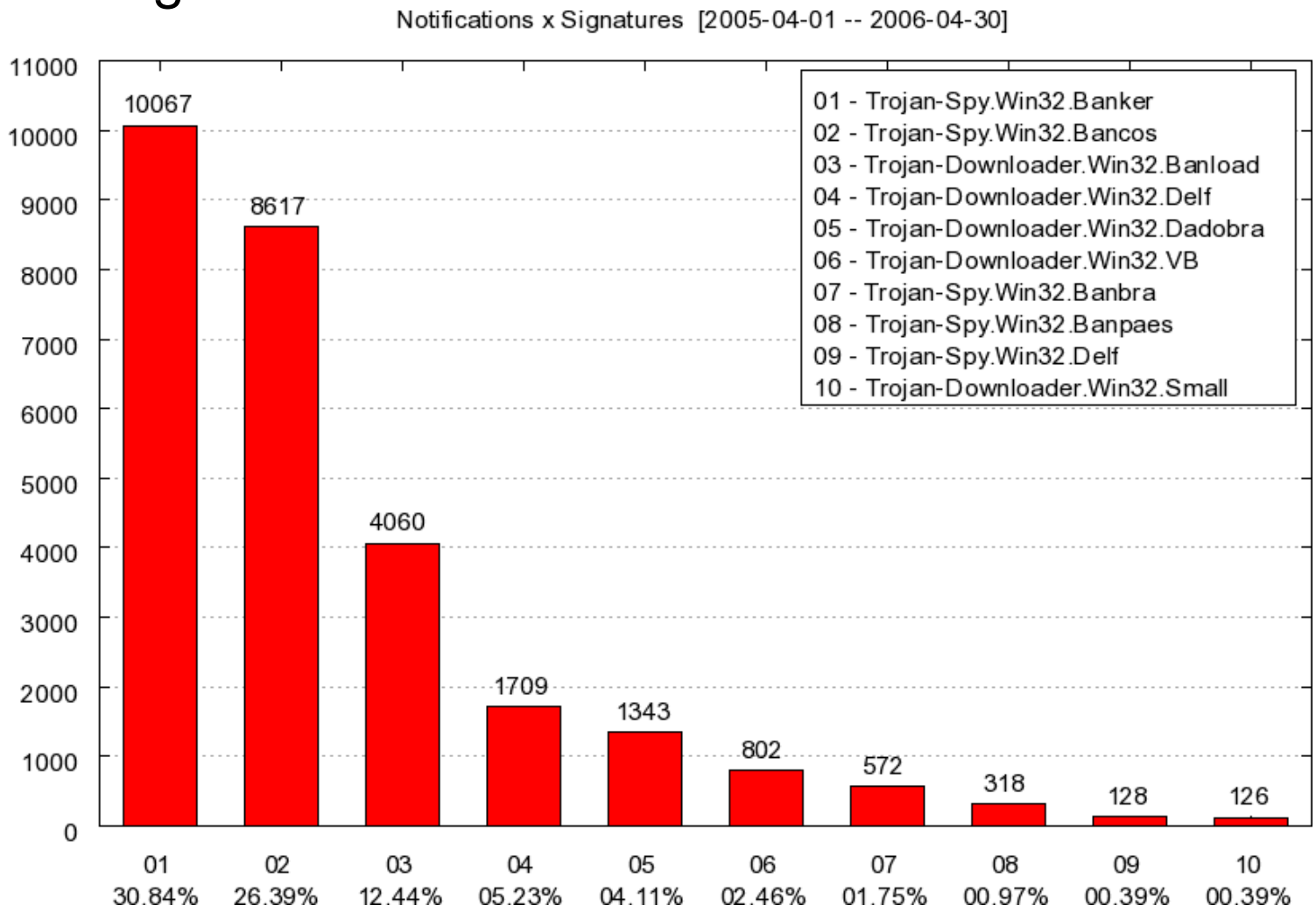
Top 10 country codes





Trojan Notifications (cont.)

Top 10 Signatures



Signatures source: Kaspersky Lab

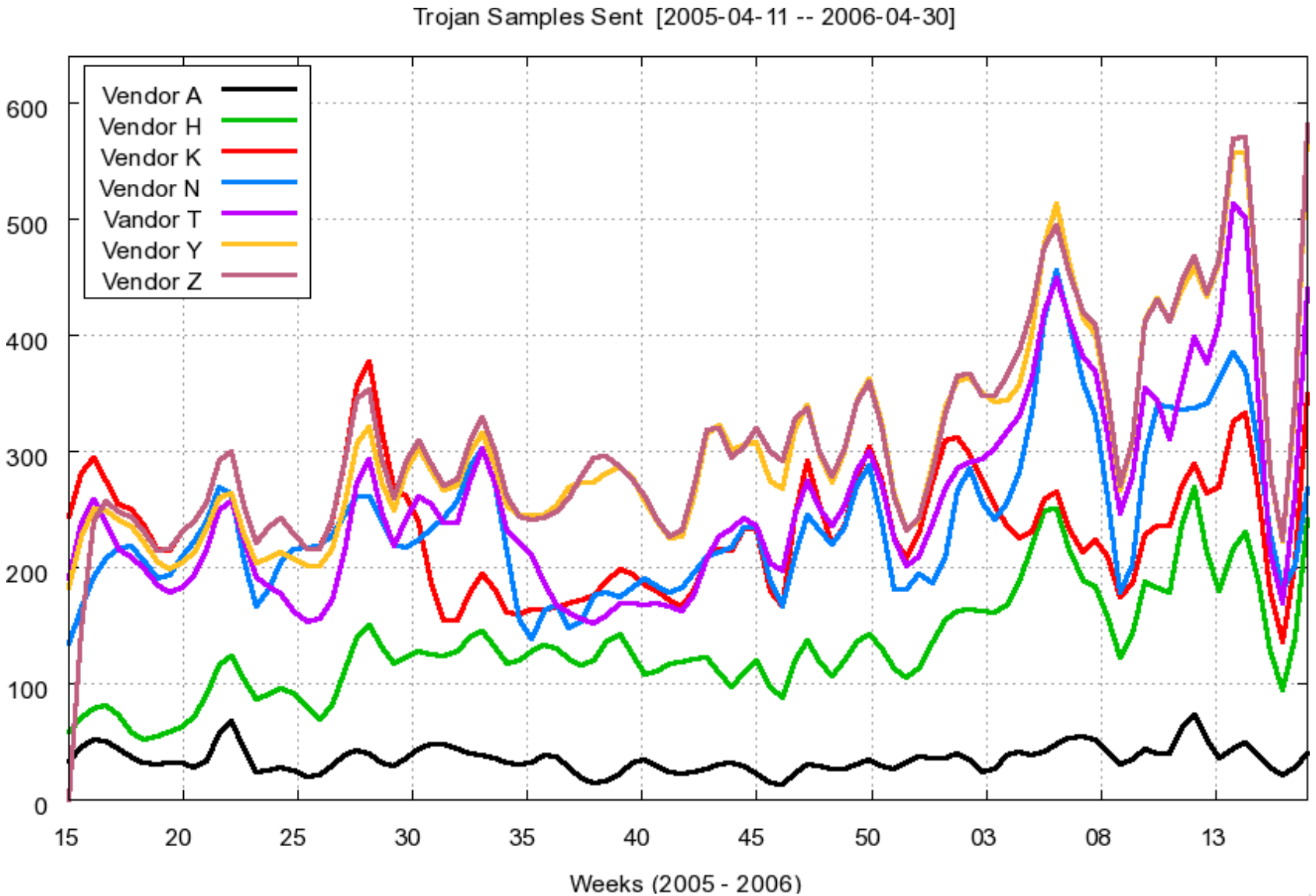
AV Vendors Efficiency

Period: 2005-04-06 – 2006-04-30

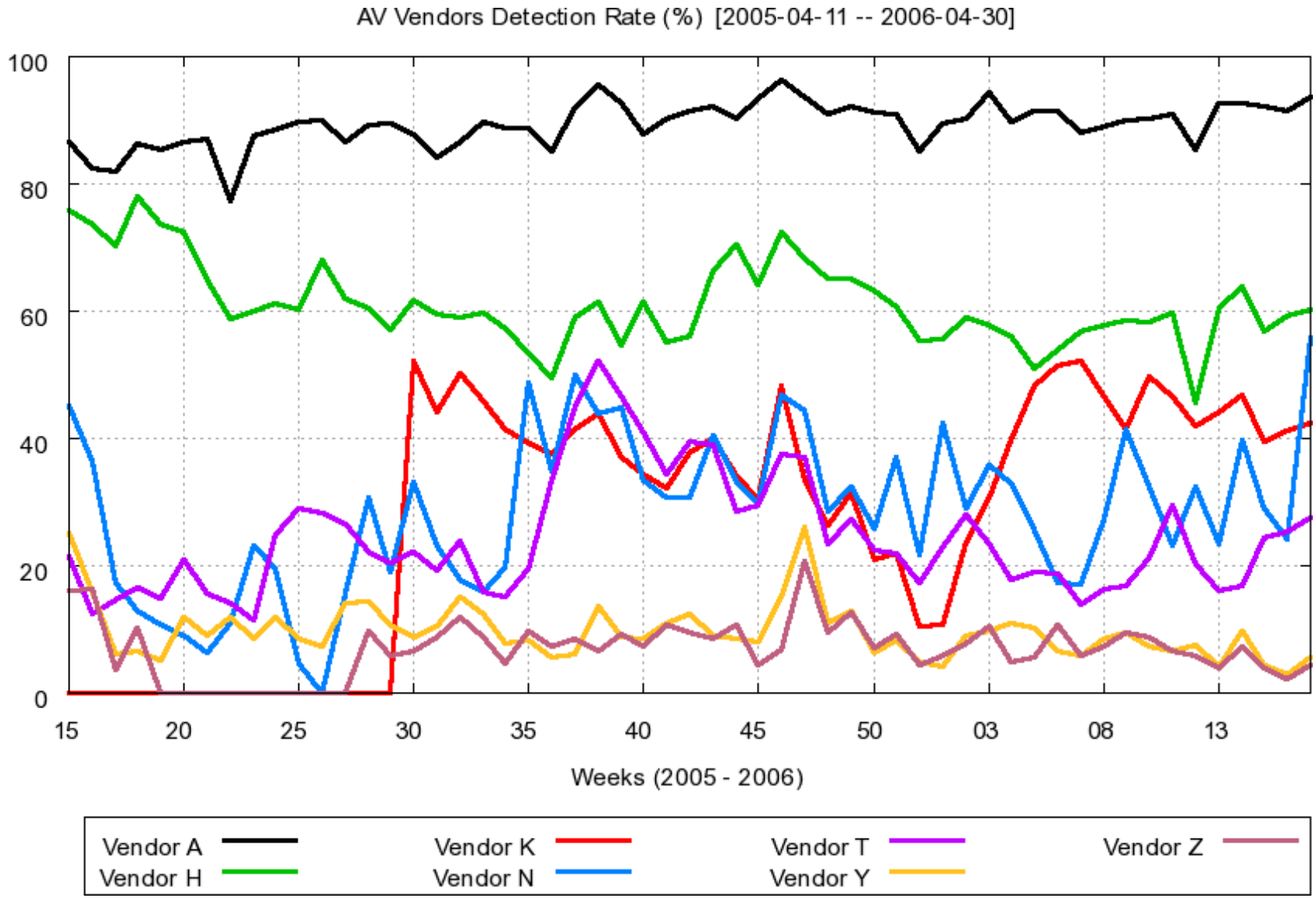
- sent a total of 18665 samples to AV vendors

Antivirus Vendor	samples	undetected	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

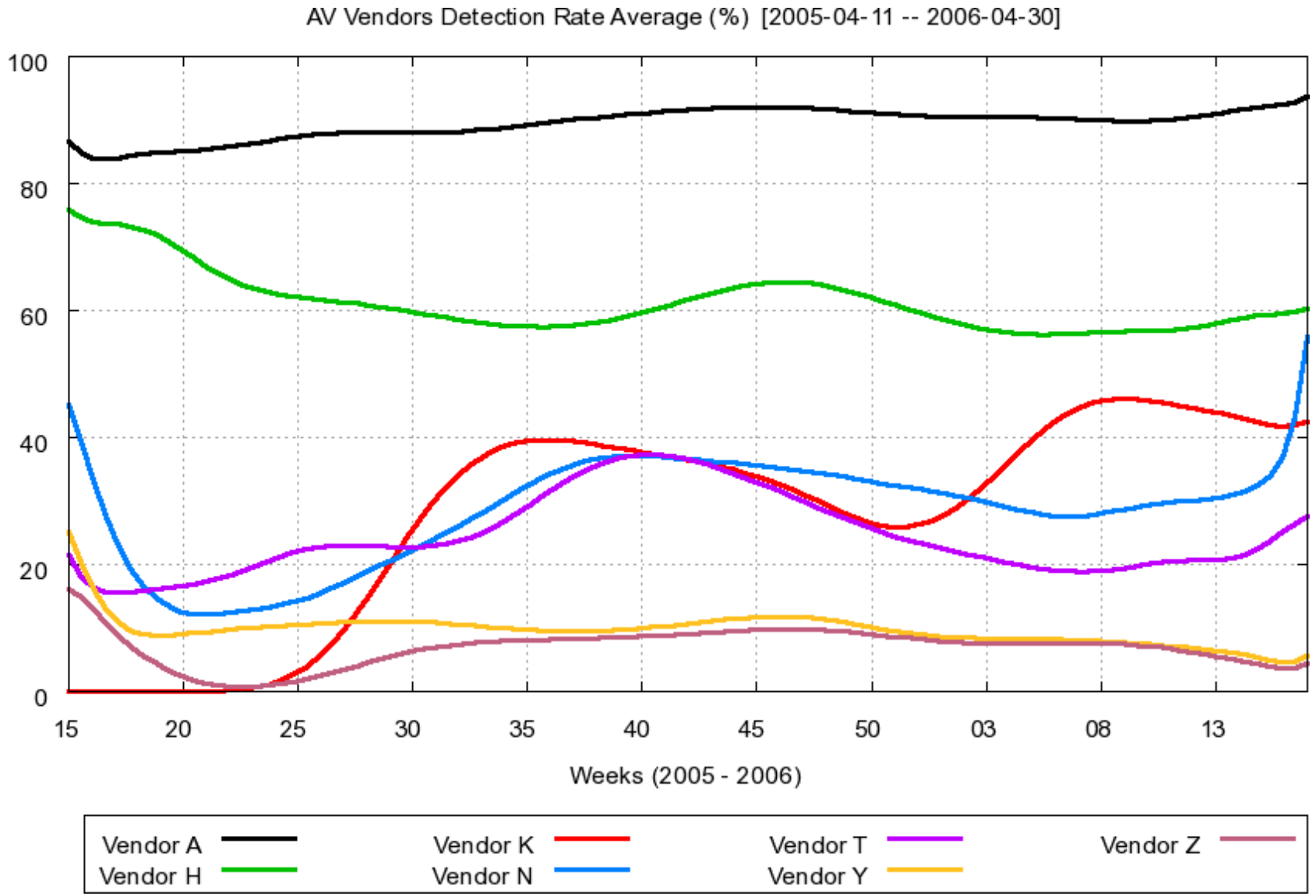
AV Vendors Efficiency (cont.)



AV Vendors Efficiency (cont.)



AV Vendors Efficiency (cont.)



Brazilian Federal Police
Operations to Fight Online Fraud

Federal Police Operations

2001: Operation Cash Net (07/Nov)

- modus operandi:
  - spams poorly written
  - 1st trojan implementations → rudimentary keyloggers
  - brute force attacks when passwords not available
- performed simultaneously in 2 states
- 70 police officers, 17 people arrested
- U$46 million stolen (estimated)

2003: Operation “Cavalo de Tróia I” (05/Nov)

- modus operandi:
  - spams / phony sites / trojans → {key,screen}loggers
  - DNS compromises widely used (“pharming”)
- performed simultaneously in 4 states
- 200 police officers, 30 arrest warrants, 27 people arrested
- U$14 million stolen (estimated)

Federal Police Operations (cont.)

2004: Operation “Cavalo de Tróia II” (20/Oct)

- criminal organization:
  - programmers
    - sophisticated trojans $\rightarrow$ {key,screen}loggers
  - mules
    - locals $\rightarrow$ drop accounts for small percentages
    - local commerce $\rightarrow$ payments
  - huge expenses with cars, motorcycles, big parties
  - fraud toolkit (including notebook, programs, howtos)
- performed simultaneously in 4 states
- over 80 police officers, and 90 arrest warrants
- 64 people arrested
- U$110 million stolen (estimated)

Federal Police Operations (cont.)

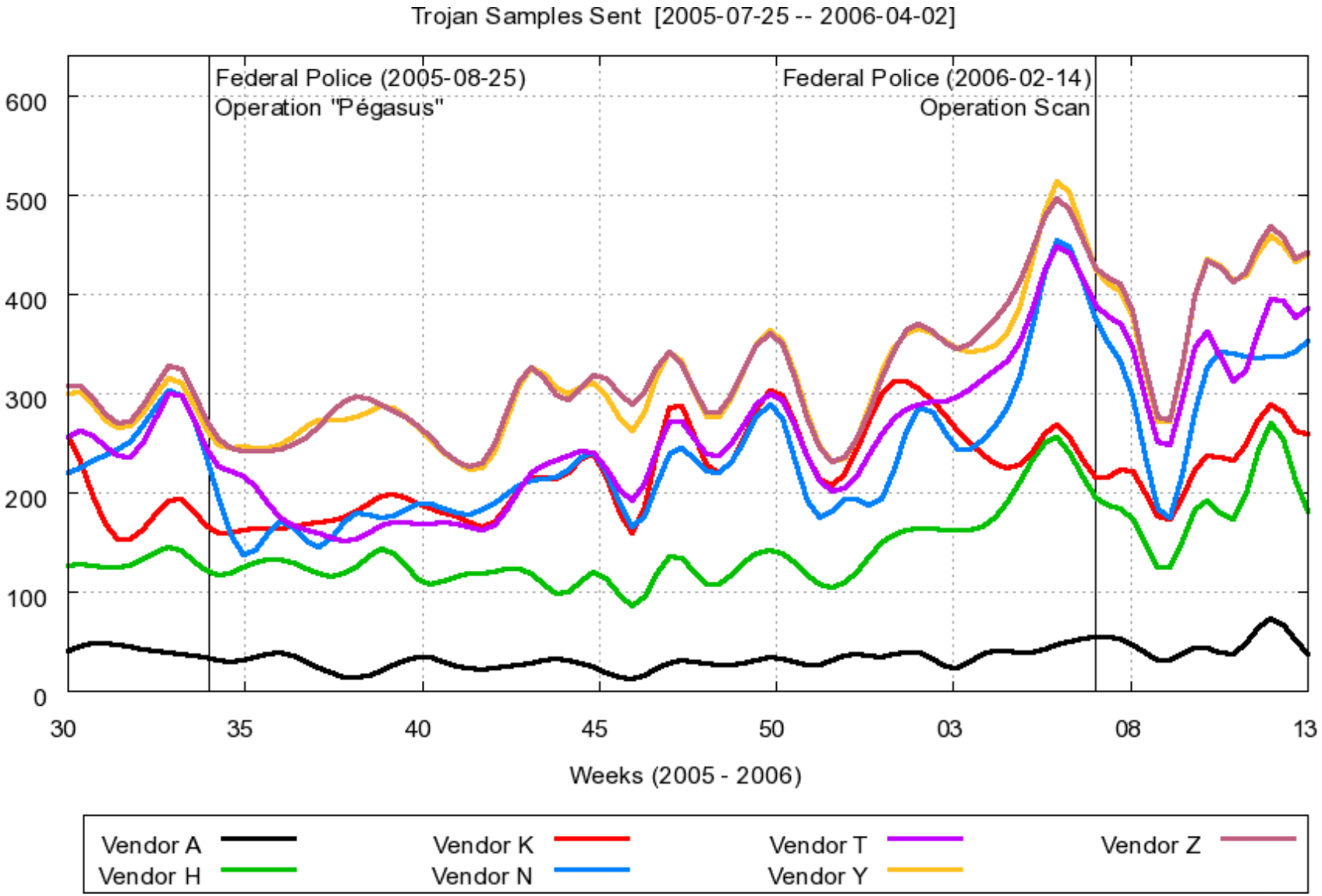
2005: Operation “Pégasus” (25/Aug)

- even more sophisticated trojans
  - keyloggers + screenloggers + screen overlapping
- performed simultaneously in 8 states
- 400 police officers, 100 arrest warrants, 85 people arrested
- U$33 million stolen (estimated)

2006: Operation Scan (14/Feb)

- performed simultaneously in 7 states
- over 300 police officers
- leader was 19 years old
- 63 people arrested (at least 9 of them minors)
- U$4.7 million stolen (estimated)

Federal Police Operations (cont.)



Further Developments Needed

Further Developments Needed

AV software need to better detect trojans

- just **1** AV with detection rate of **90%**
- **70%** of AV's with detection rates of less than **40%**
- most used defense among end users

ISPs need to be more proactive

- check files at upload time and periodically after upload

More efforts to block spam at its source

- working in some technical solutions with telcos and ISPs

Better international cooperation

Related Links

- This presentation can be found at:
  http://www.cert.br/docs/presentations/
- Computer Emergency Response Team Brazil – CERT.br
  http://www.cert.br/
- Brazilian Internet Steering Comittee – CGI.br
  http://www.cgi.br/