Fraud and Phishing Scam in Brazil

Cristine Hoepers
cristine@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
- CERT.br initiatives
- 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 $\longrightarrow$ 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

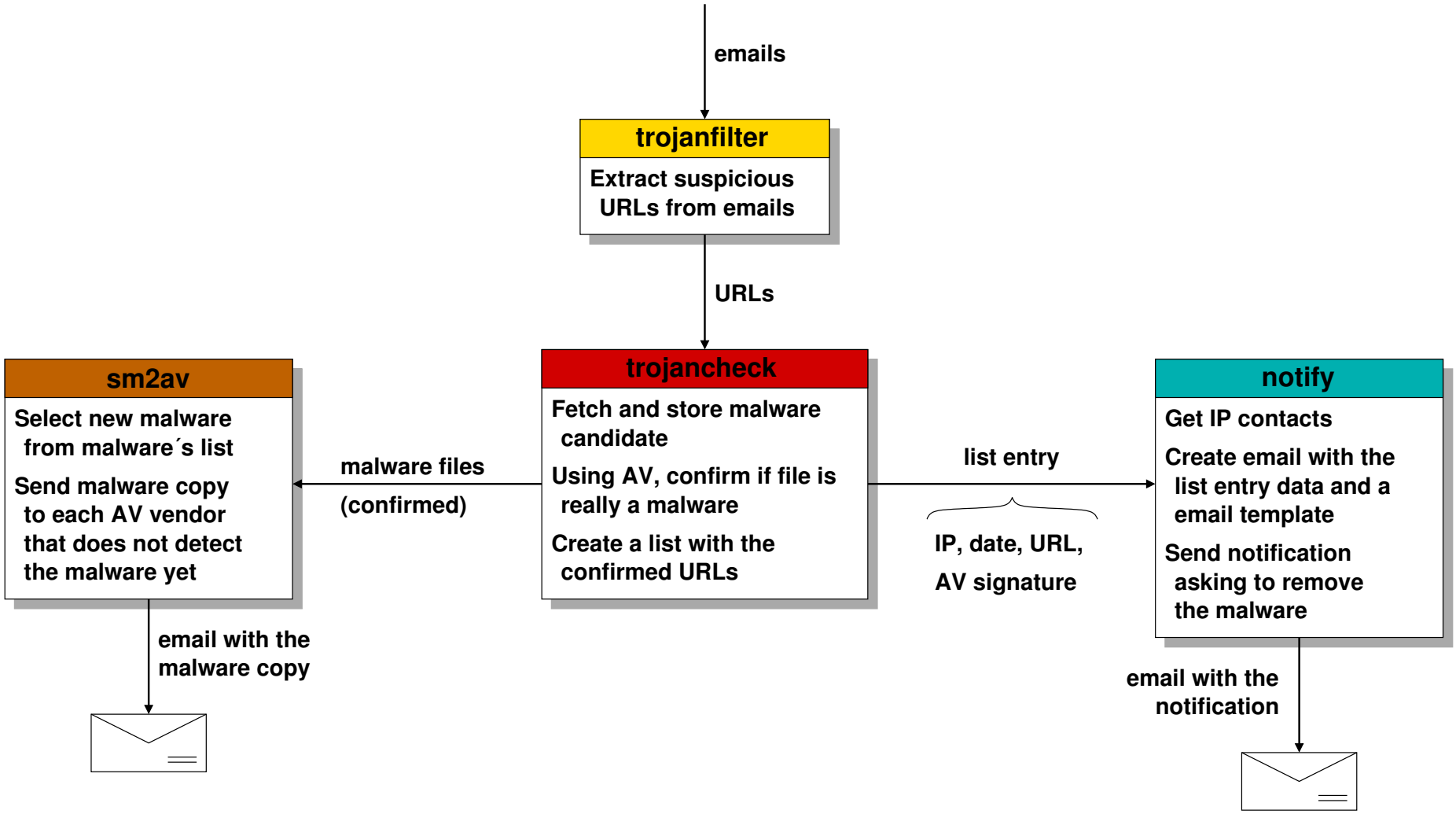
CERT.br Initiatives

CERT.br Initiatives

- 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.)

Trojan notification and submission system



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 – 2005-10-31 → 607547 emails, 701281 URLs

number	domain
153151	America Online*
38568	gratisweb.com
19655	spectrogariaclips.inf.br
14097	thefilebucket.com
9800	ripway.com
9498	noti-auto.com.ar
8564	atspace.com
7863	cartoesmagicos.com.br
6633	aocusa.com
6059	ronaldg.com

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

Trojan Notifications

Summary: 2005-04-01 – 2005-10-31

counter	number
domains	1829
contacts	952
extensions	19
filenames	4185
hostnames	2830
IP addresses	1550
country codes	55
e-mails sent	7303
URLs	10730
AV signatures	725

Total amount of URLs notified = 14727 (with repetition)

Trojan Notifications (cont.)

Top 12 domains notified

number	(%)	domain
5754	39.18	America Online*
1821	12.37	gratisweb.com
194	1.32	webcindario.com
190	1.29	terra.com.br
149	1.01	100free.com
139	0.94	telepolis.com
133	0.90	galeon.com
124	0.84	pop.com.br
109	0.74	wanadoo.es
104	0.71	cjb.net
103	0.70	atspace.com
101	0.69	yahoo.com.br

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

Trojan Notifications (cont.)

Top 16 extensions and top 11 country codes (CC)

number	(%)	extension
11185	75.95	exe
3033	20.59	scr
334	2.27	zip
80	0.54	jpg
42	0.28	com & rar
15	0.10	js
12	0.08	txt
10	0.07	html
6	0.04	dll & gif
6	0.04	cmd & php & swf
2	0.02	bat & bmp

number	(%)	CC
2395	46.46	US
966	18.74	BR
248	4.81	ES
214	4.15	KR
161	3.12	DE
145	2.81	IT
139	2.70	CA
139	2.70	RU
124	2.41	UK
82	1.59	FR
81	1.57	CN

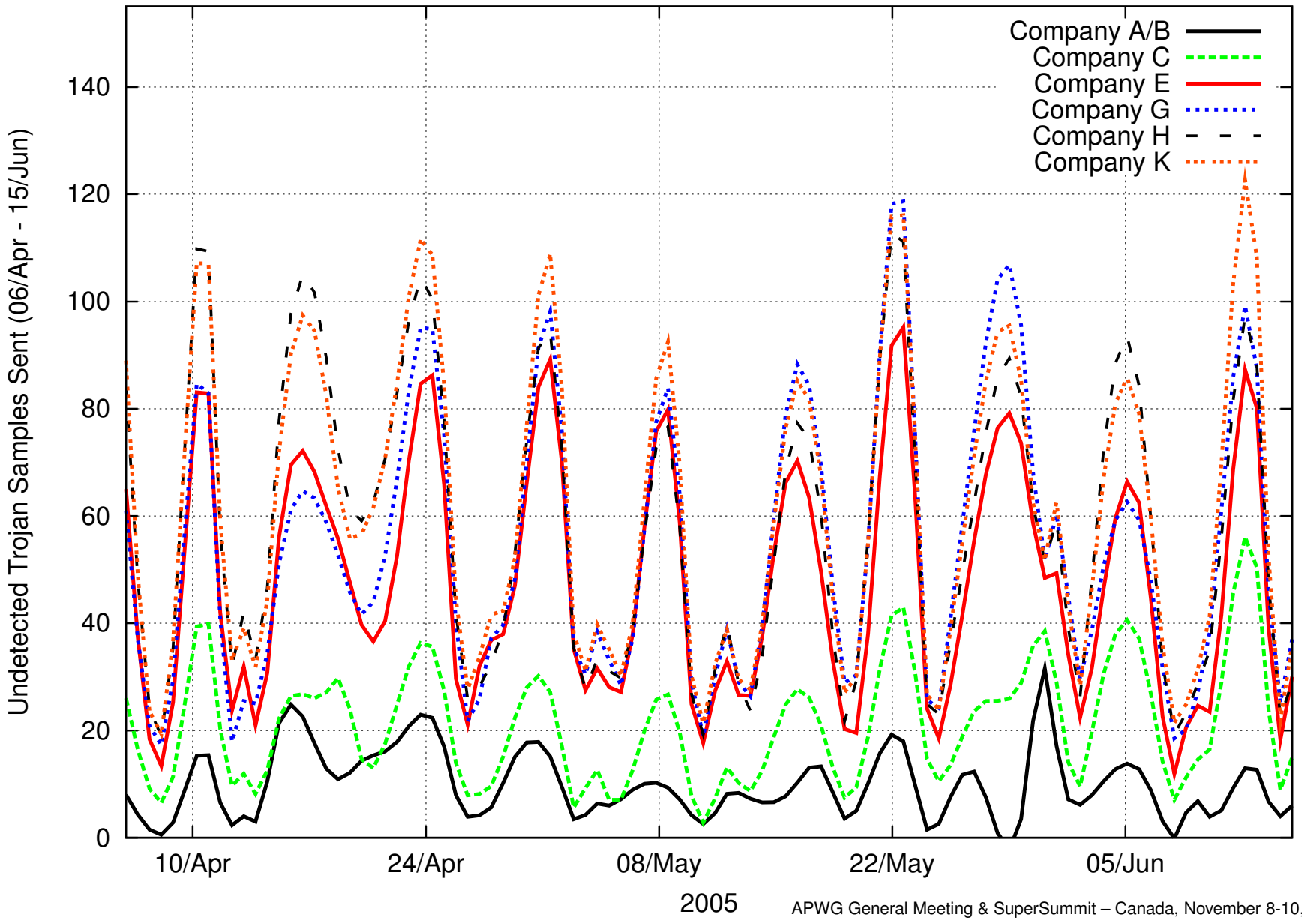
AV Vendors Efficiency

Period: 2005-04-06 – 2005-10-31

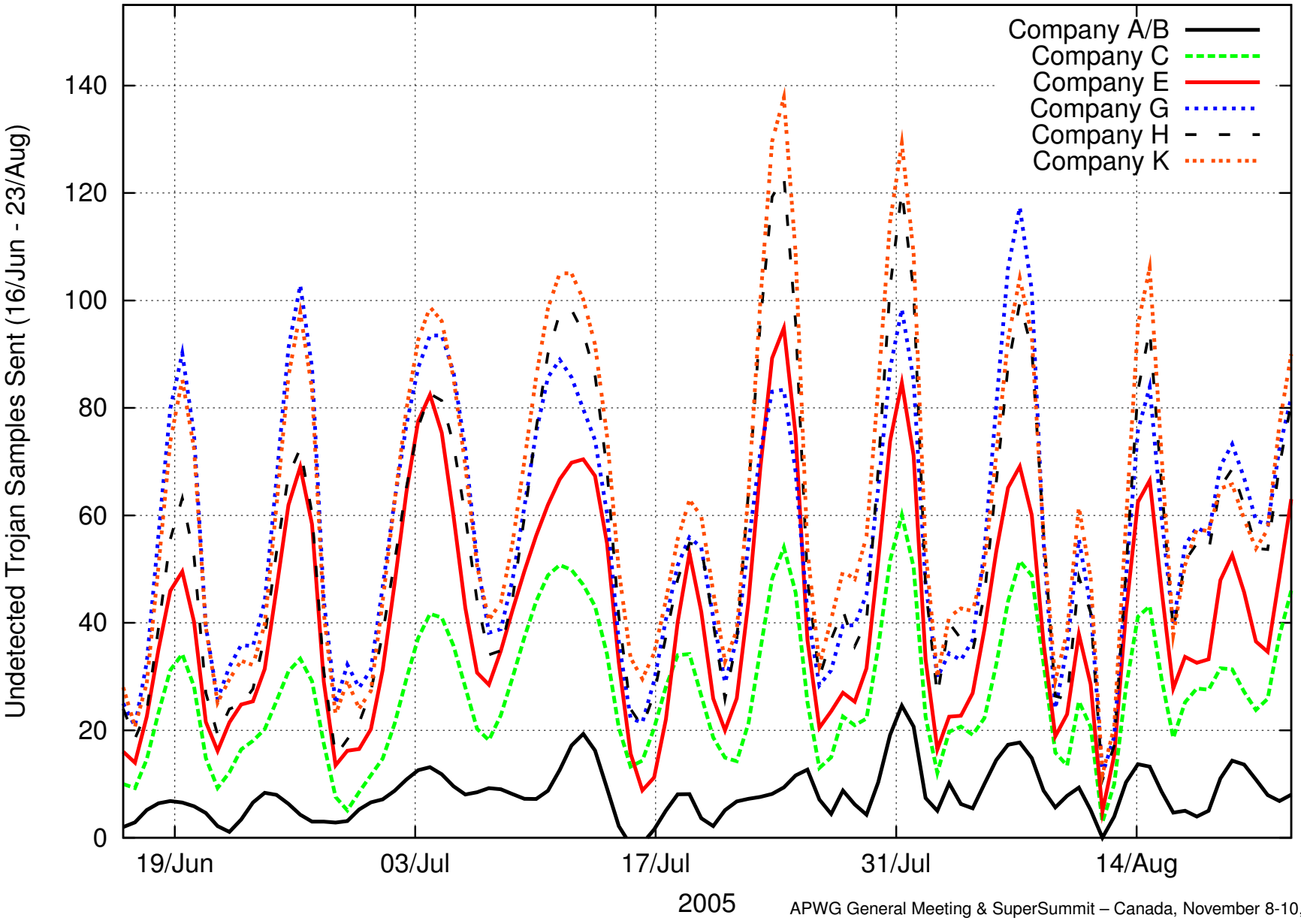
Sent a total of 8380 samples to AV vendors

AV Vendor	samples	detected
Company A	1006	88.00 %
Company B	1006	88.00 %
Company C	3143	62.49 %
Company D	3466	58.64 %
Company E	5210	37.83 %
Company F	5572	33.51 %
Company G	6186	26.18 %
Company H	6211	25.88 %
Company I	6411	23.50 %
Company J	6960	16.95 %
Company K	7491	10.61 %
Company L	7829	6.58 %

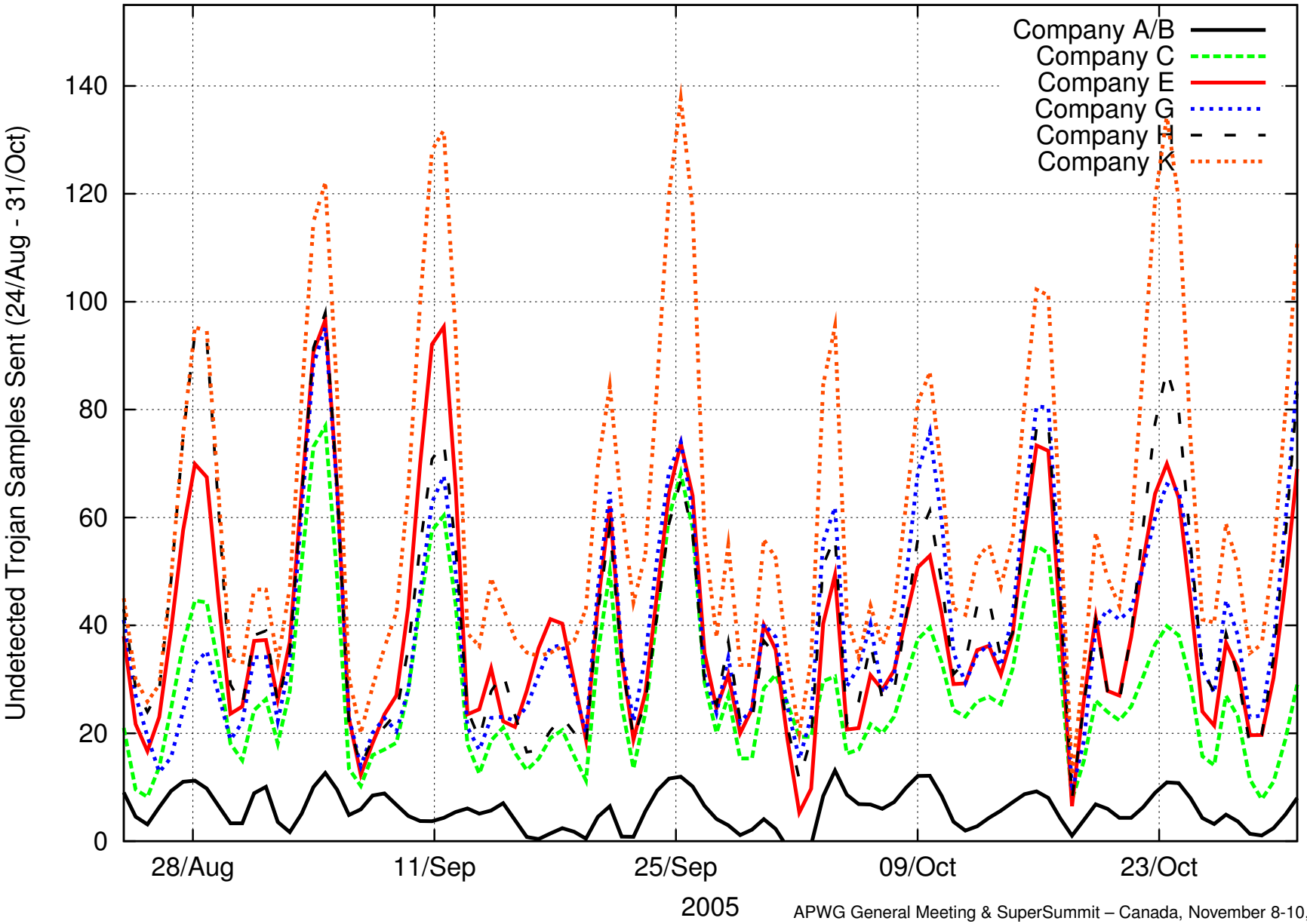
AV Vendors Efficiency (part 1/3)



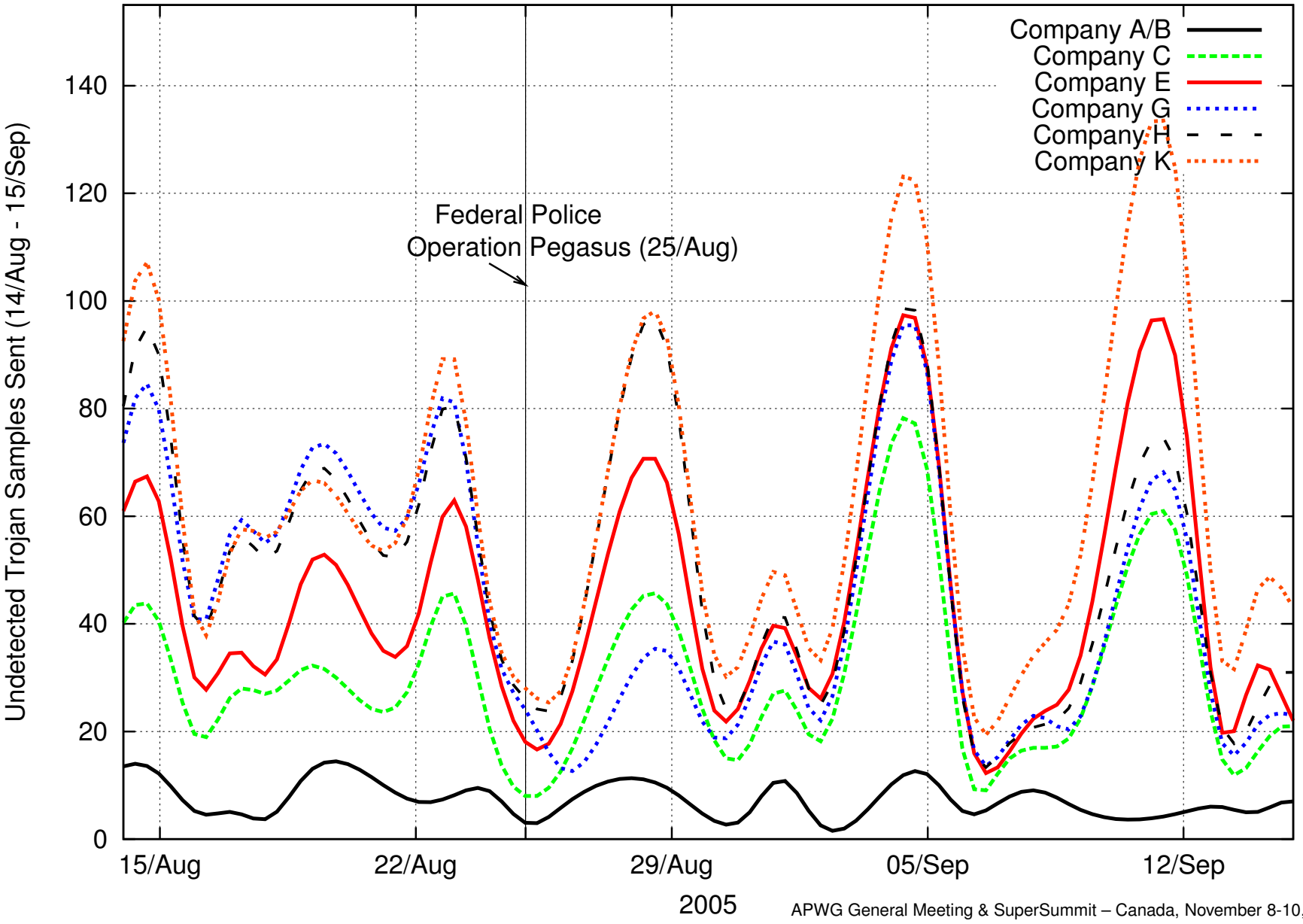
AV Vendors Efficiency (part 2/3)



AV Vendors Efficiency (part 3/3)



AV Vendors Efficiency (Pegasus)



Further Developments Needed

Further Developments Needed

- AV software need to increase trojan detection
  - 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 Brazilian telcos and ISPs
- increase 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/

- Cristine Hoepers <cristine@cert.br>