Global 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
  - **Help raise the security awareness in the country**
  - **Maintain public statistics about incidents and abuse**
  - Produce best practices' documents
  - Develop collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling

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

Agenda

- Updates
  - Malware statistics
  - Trends
  - Awareness initiatives

Anti-Fraud Activities in Brazil

- CERT.br focus:
  - Notifies sites hosting malware related to frauds
  - Coordinates with international sites and CSIRTs to take down the malware and phishing pages
  - Perform surface analysis
    - Send undetected malware (trojans, keyloggers, etc) to 35+ antivirus vendors
    - Send new trojans to artifact analysis groups
- Finantial sector focus:
  - Perform run-time analysis
    - Aim to identify drop boxes, affected banks, see if the countermeasures still work, etc
  - Send all new sites, URLs, malware to CERT.br

2008 Malware Statistics: Q1—Q3

Category	Q1	Q2	Q3
AntiVirus signatures (unique)	1344	2197	1737
AntiVirus signatures (grouped by “family”)	47	80	80
Unique trojan samples (unique hashes)	3823	4450	3156
File Extensions	64	61	63
Unique URLs	4718	5550	3885
Domains	1803	2215	1410
Unique IP Addresses	1298	1461	1034
IP Allocation’s Country Codes	58	63	57
Email notifications sent by CERT.br	4121	4983	3305

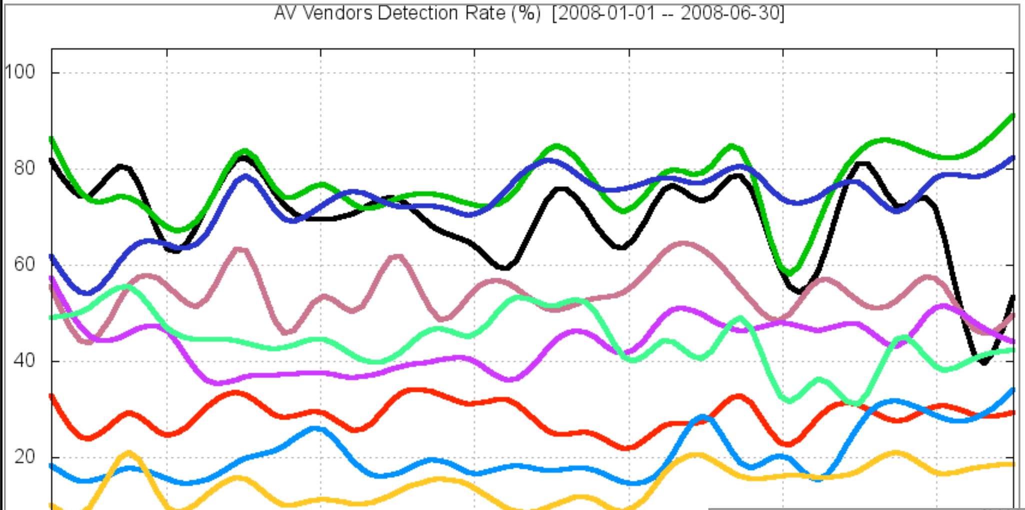
Includes:

- Keyloggers
- Screen loggers
- Trojan Downloaders

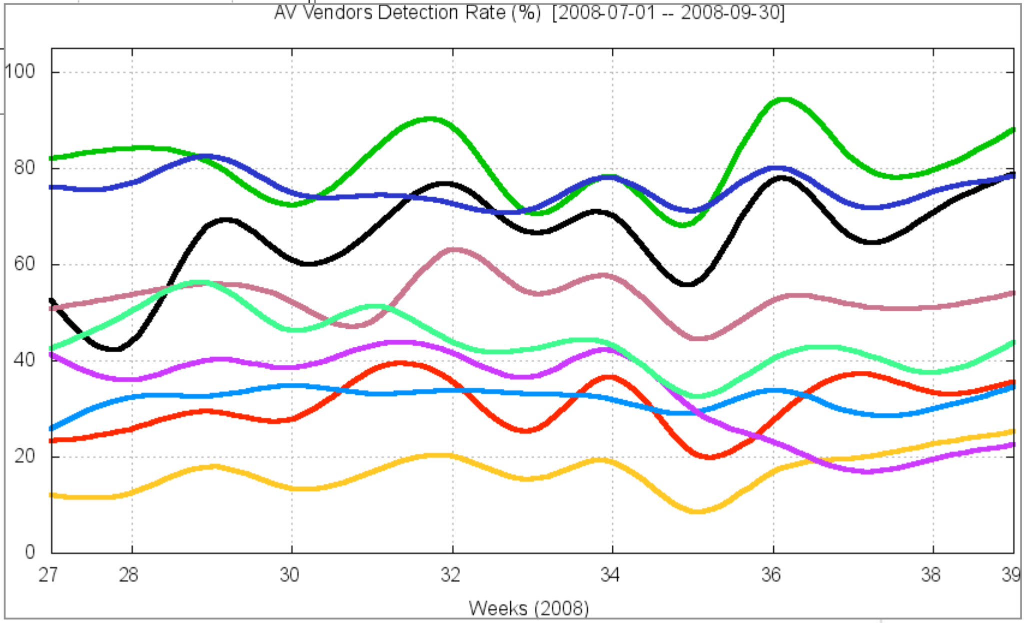
Does NOT include:

- Bots/Botnets
- Worms

2008 Detection Rate – 1st Semester and 3rd Quarter

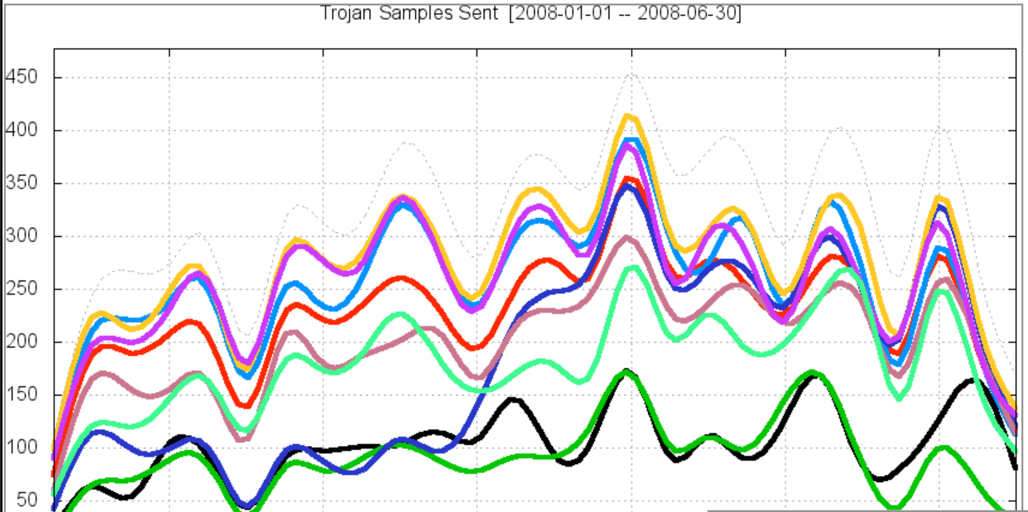


Only **6** vendors with the detection rate above **70%**

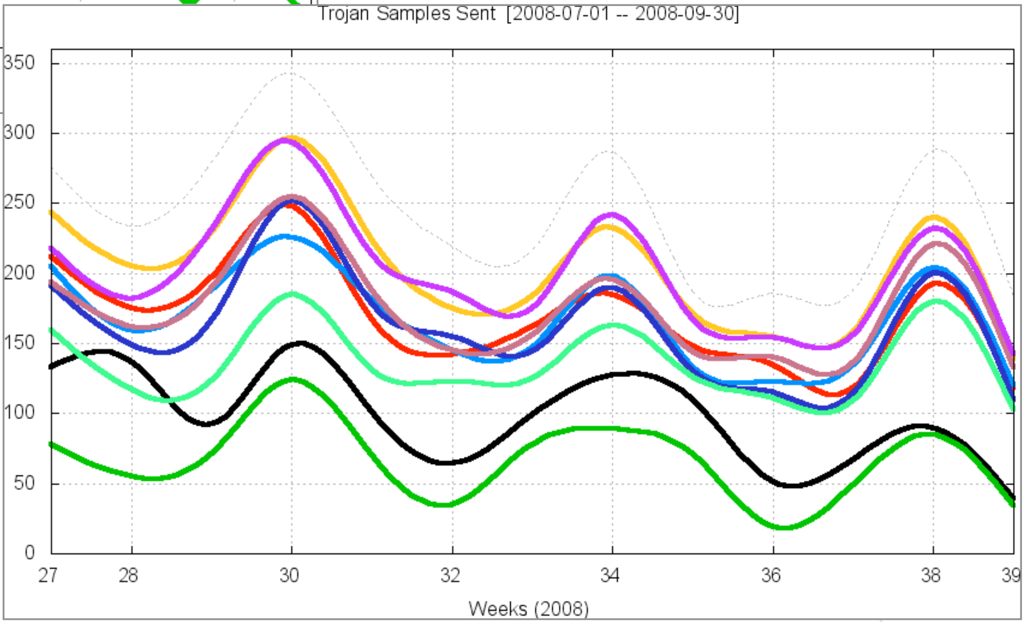


~70% of vendors with less than **50%**

2008 Samples Sent – 1st Semester and 3rd Quarter



The number of **malware** related frauds **droped 30%** on the 3rd quarter



The number of **phishing sites** increased **100%** in the 3rd quarter

Other Trends (1/2)

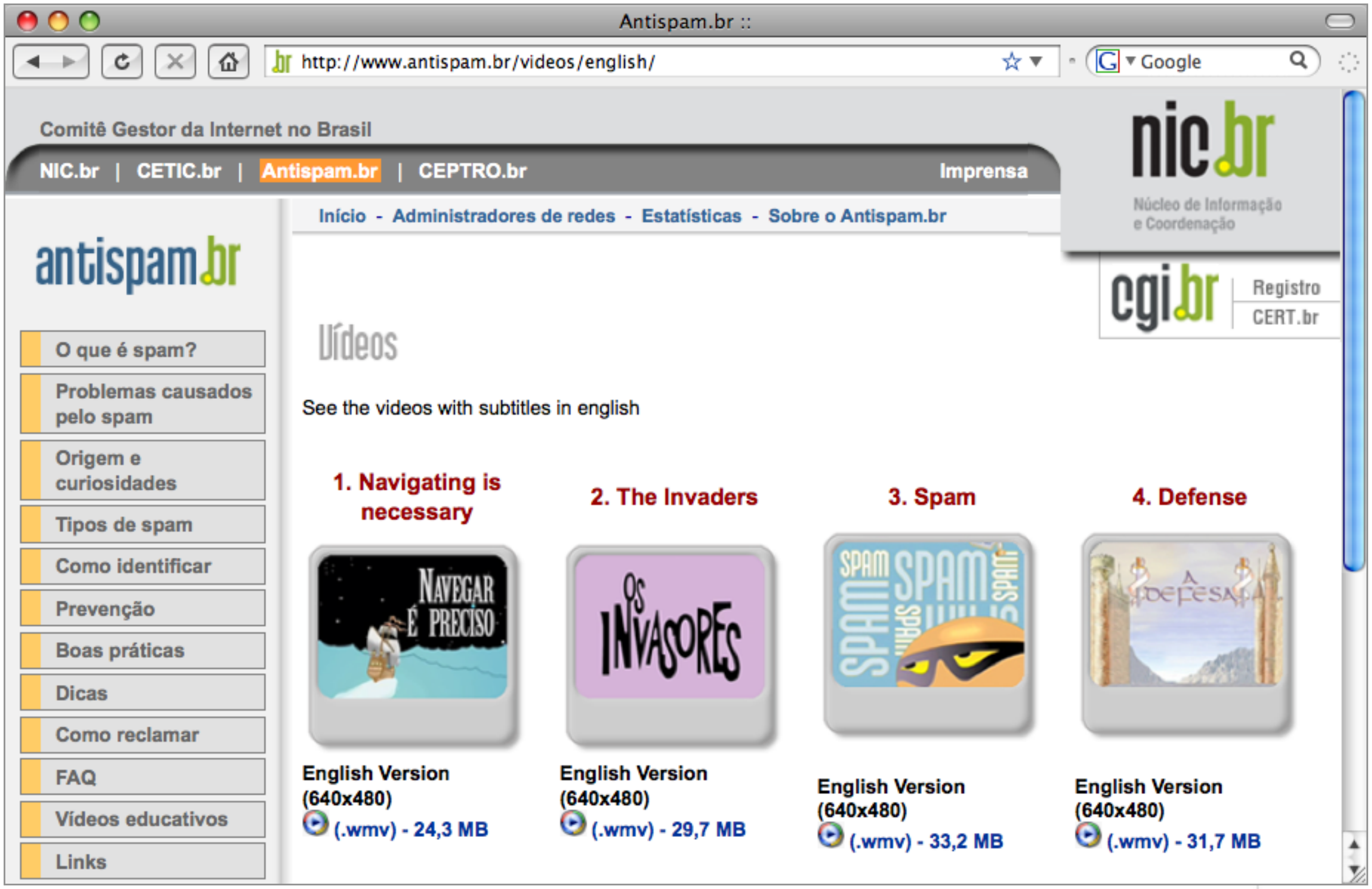
- Google sponsored links
  - Use the word "bank" and some brands as the AdWords
    - direct the users to pages with malware
  - Are allways prepaid
  - There is no clear channel on how to complain to Google
- Drive-by downloads
  - not really common, but we have seen some
- Client's hosts file modified by malware
  - really old, but still works

Other Attacks Seen in Brasil (2/2)

- DNS cache poisoning
  - One of the major cable providers had one of their recursive servers poisoned
    - google.com.br was directed to a different IP
    - the phony page had links pointing to malware affecting brazilian banks
  - Using data from queries to the brazilian ccTLD (NIC.br) server we identified 11470 vulnerable recursive servers
- **Not** being widely used
  - botnets
  - fast-flux networks

Videos in English

- Version with subtitles already available: http://antispam.br/videos/english/
- Voice-over will be available soon


Antispam.br ::
http://www.antispam.br/videos/english/
Google
Comitê Gestor da Internet no Brasil
NIC.br | CETIC.br | Antispam.br | CEPTRO.br
Imprensa
nic.br
Núcleo de Informação e Coordenação
cgi.br
Registro
CERT.br
Início - Administradores de redes - Estatísticas - Sobre o Antispam.br
antispam.br
O que é spam?
Problemas causados pelo spam
Origem e curiosidades
Tipos de spam
Como identificar
Prevenção
Boas práticas
Dicas
Como reclamar
FAQ
Vídeos educativos
Links
Navegar é preciso
Os Invasores
Spam
A Defesa

Vídeos

See the videos with subtitles in english

1. Navigating is necessary
English Version (640x480)
(.wmv) - 24,3 MB

2. The Invaders
English Version (640x480)
(.wmv) - 29,7 MB

3. Spam
English Version (640x480)
(.wmv) - 33,2 MB

4. Defense
English Version (640x480)
(.wmv) - 31,7 MB

Additional References

- This presentation (by the end of the month)
  http://www.cert.br/docs/presentations/
- Awareness videos

  http://www.antispam.br/videos/english/
- CERT.br
  Computer Emergency Response Team Brazil
  http://www.cert.br/