Outreach Initiatives

Cristine Hoepers

General Manager

cristine@cert.br

Klaus Steding-Jessen

Technical Manager

jessen@cert.br

CERT.br – Computer Emergency Response Team Brazil

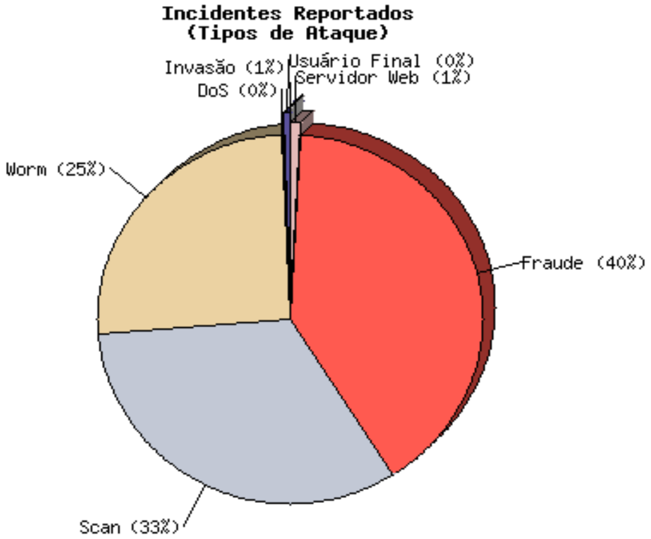
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

Agenda

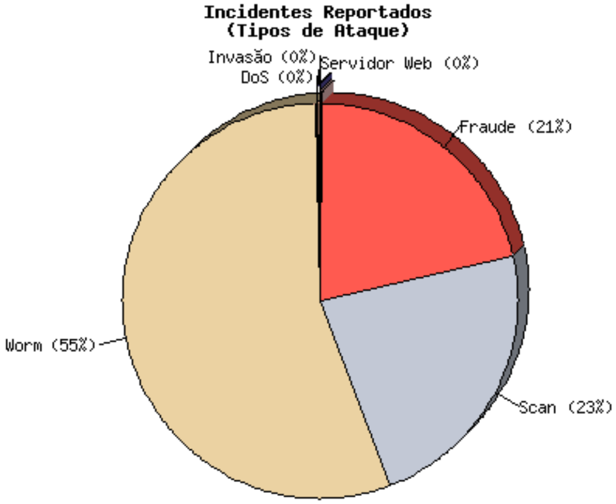
- Motivation and background
  - What is the problem?
    - Statistics and Indicators
  - What have been done so far
- New initiatives

Incident Reports

2005



2006



Fraud:

2004: 4.015 (05%)
2005: 27.292 (40%)
2006: 41.776 (21%)

Fraud attempts characteristics:

Spams

- Using different baits (news, cards, gossips about famous people, etc)
- With links to malicious code (trojans, trojan droppers, sites with malicious javascripts that download trojans, etc)

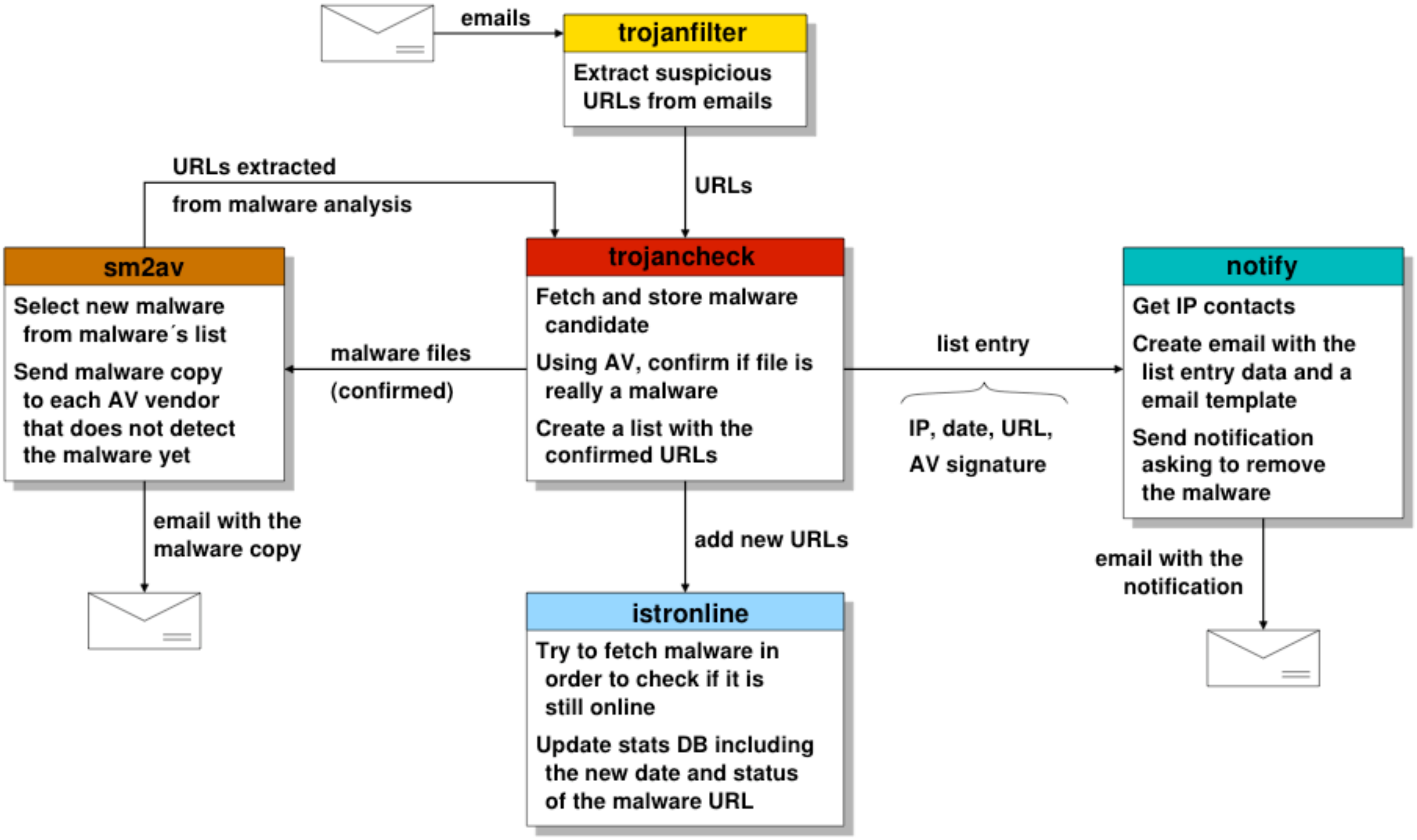
Worm (bots included):

2004: 42.267 (55%)
2005: 17.332 (25%)
2006: 109.676 (55%)

Anti-Fraud Activities

- 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 30+ antivirus vendors
    - Send new trojans to artifact analysis groups
  - Disseminate information about prevention techniques
    - Documents, best practices, training to professionals, interviews, etc
- 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

Dealing With this Information and Generating Statistics



emails

trojanfilter

Extract suspicious URLs from emails

URLs

URLs extracted from malware analysis

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

add new URLs

istronline

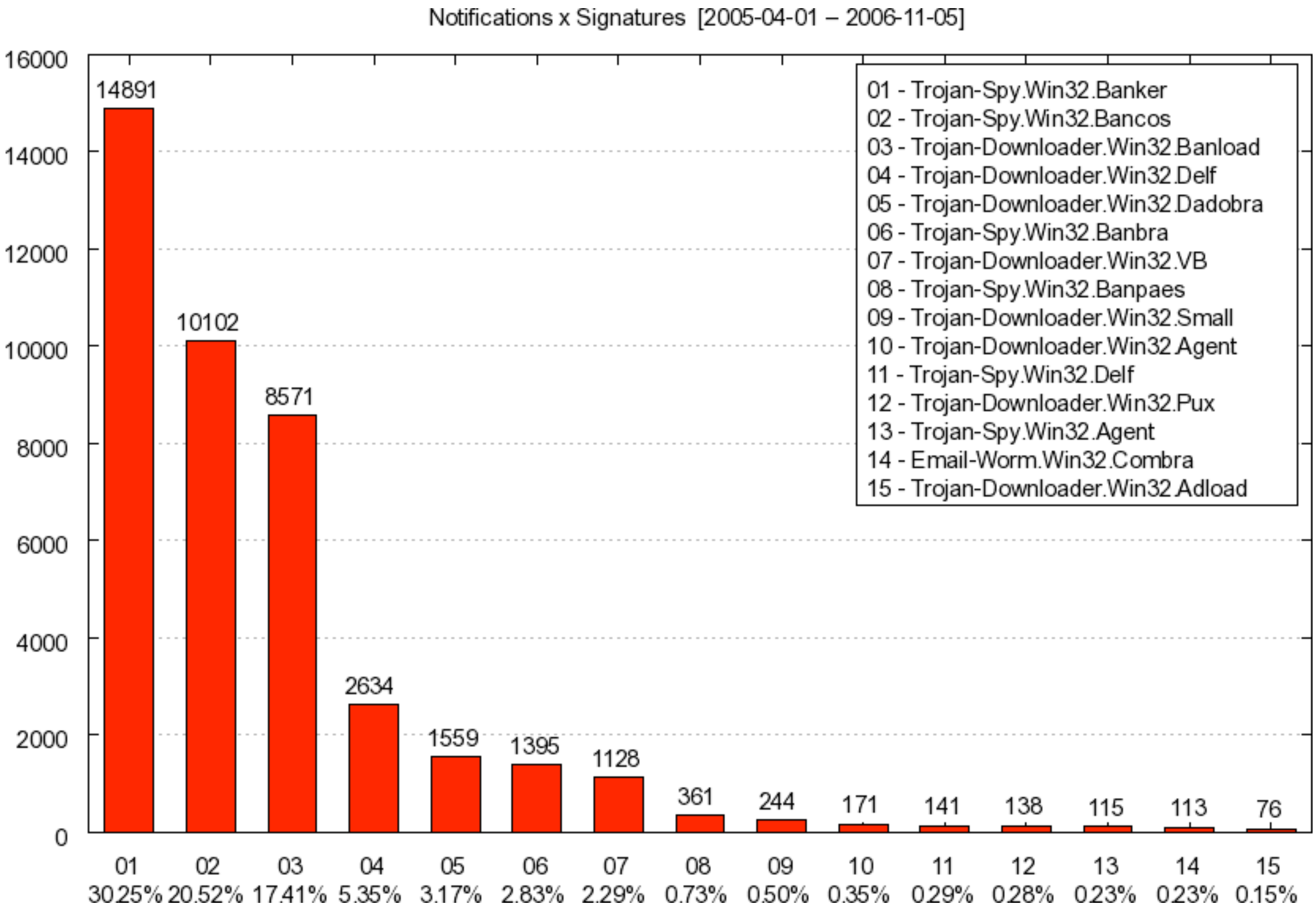
Try to fetch malware in order to check if it is still online

Update stats DB including the new date and status of the malware URL

Statistics: April 1st, 2005 - November 3rd, 2006

Category	Total
Unique URLs	36069
Hosts	11940
Domains	6886
Contacts for the domains/networks	2741
IP Addresses	5054
IP Allocation’s Country Codes	76
Unique trojan samples (unique hashes)	28350
Trojans’ file names	15157
File Extensions	78
AntiVirus signatures (unique)	2623
AntiVirus signatures (grouped by “family”)	173
Email notifications sent by CERT.br	25922

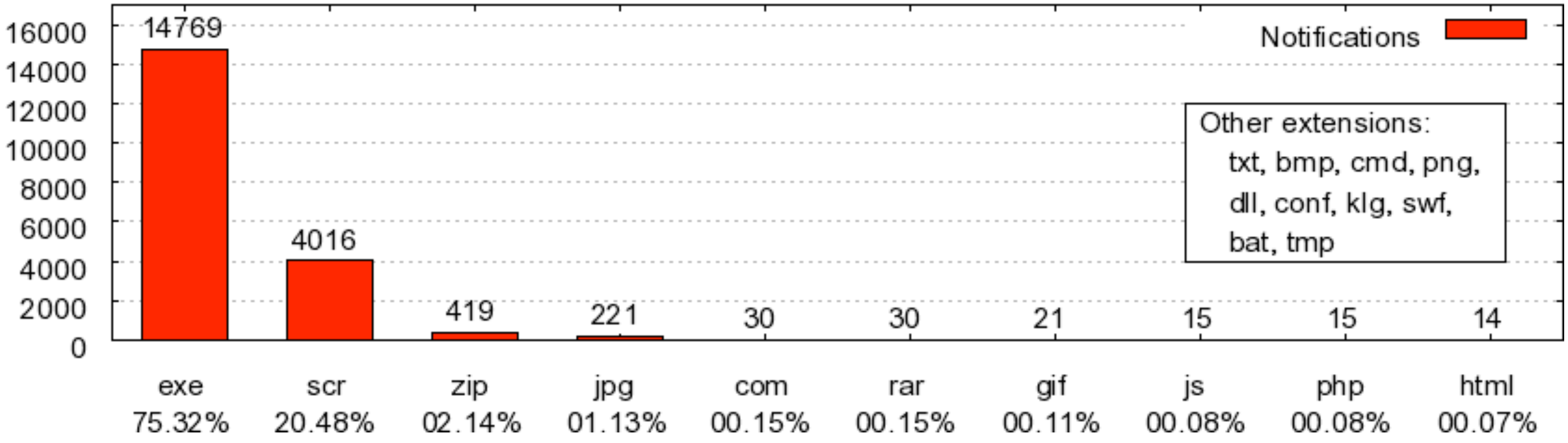
Top 15 Signature “Families”



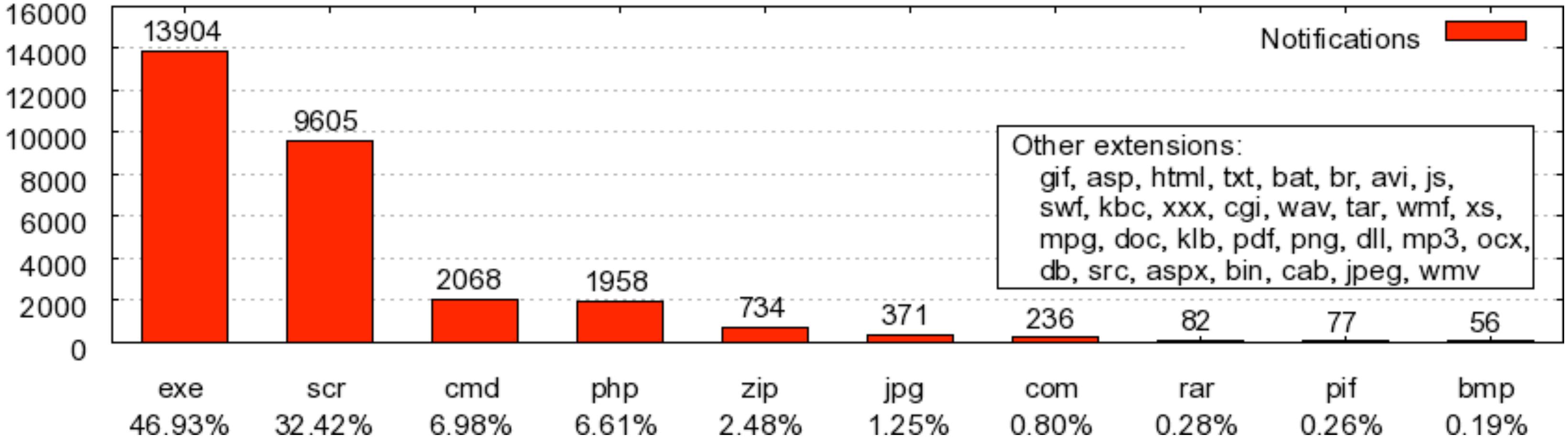
Signatures from Kaspersky Lab.

File Extensions

Notifications x Extensions [2005-04-01 -- 2005-12-31]

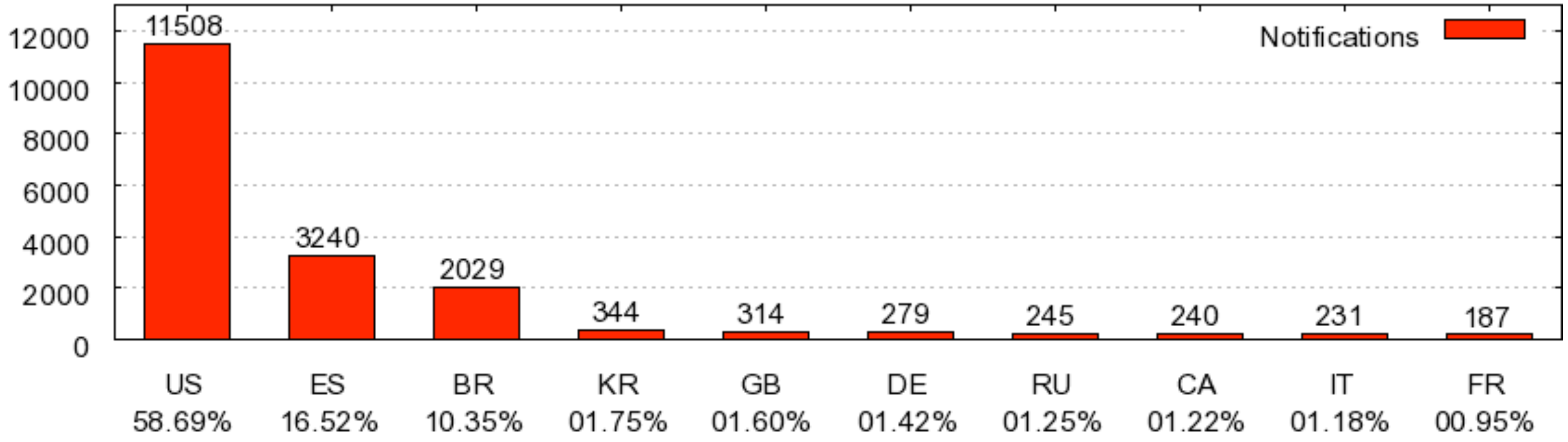


Notifications x Extensions [2006-01-01 -- 2006-11-05]

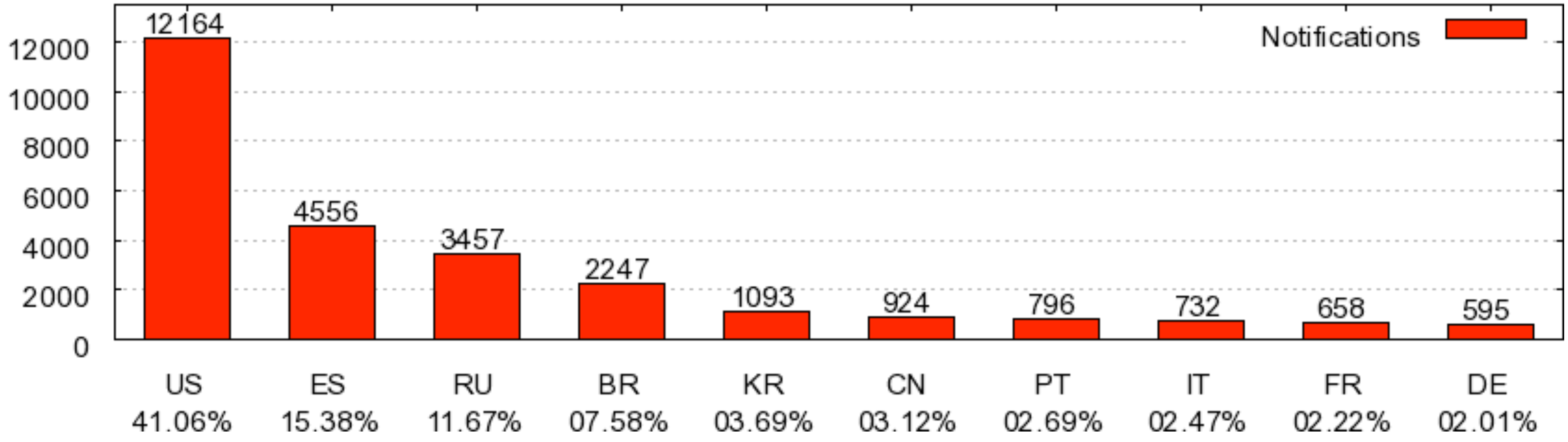


IPs Hosting Malware - RIRs Allocation Information

Notifications x Country Codes [2005-04-01 -- 2005-12-31]



Notifications x Country Codes [2006-01-01 -- 2006-11-05]



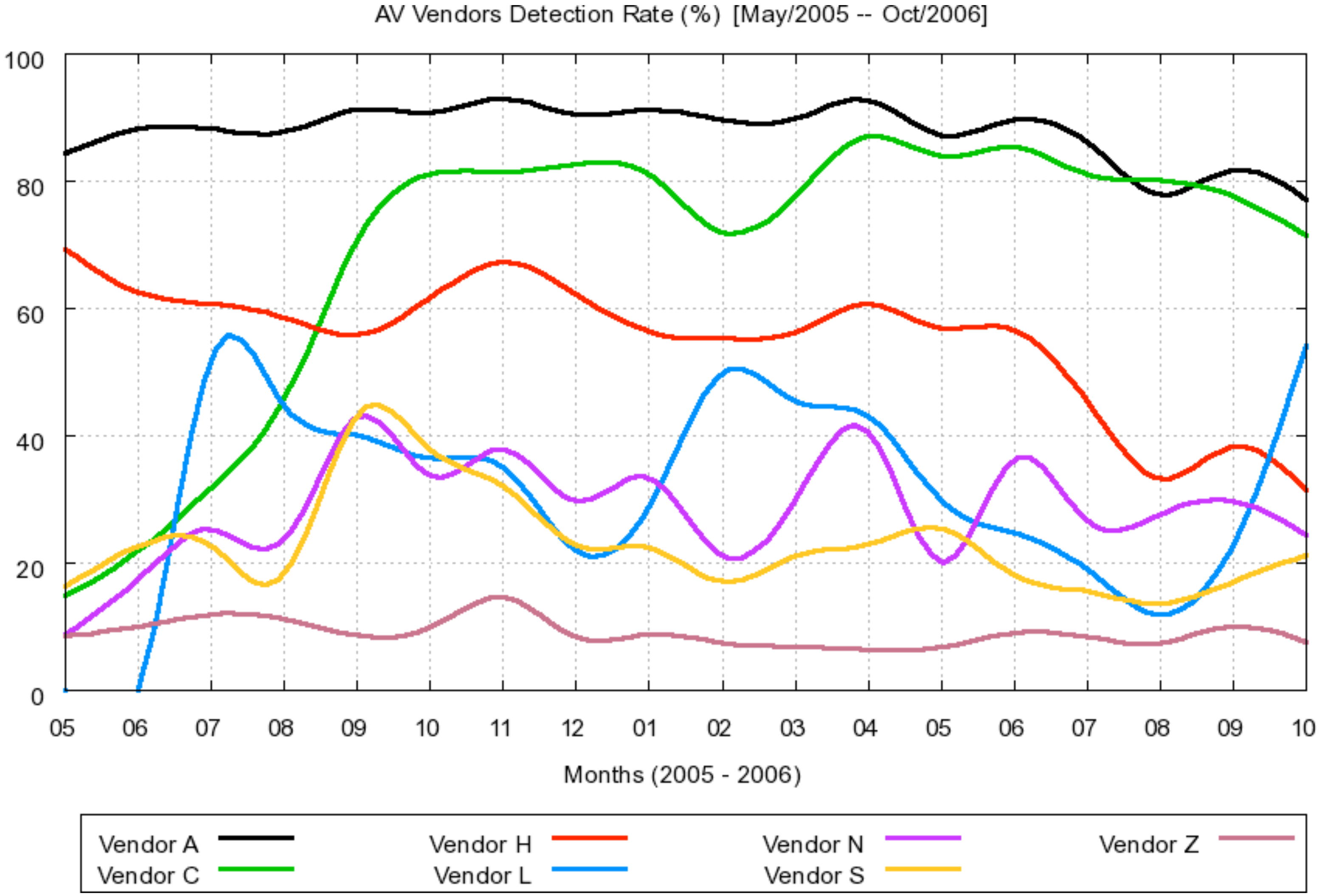
AntiVirus Detection Rate: April 1st, 2005 - November 5th, 2006

Antivirus Vendor	Samples Tested	Samples not detected	Samples Detected	Detection Rate (%)
Vendor A	28315	3505	24810	87.62
Vendor B	5651	1019	4632	81.97
Vendor C	28349	8776	19573	69.04
Vendor D	28165	9417	18748	66.56
Vendor E	28331	9473	18858	66.56
Vendor F	2611	921	1690	64.73
Vendor G	28041	11369	16672	59.46
Vendor H	28350	12745	15605	55.04
Vendor I	17160	8722	8438	49.17
Vendor K	17888	10846	7042	39.37
Vendor L	24284	15957	8327	34.29
Vendor N	28038	19891	8147	29.06
Vendor O	27983	20019	7964	28.46
Vendor P	28339	20340	7999	28.23
Vendor Q	23811	17167	6644	27.90
Vendor T	28190	21938	6252	22.18
Vendor Z	26881	24430	2451	9.12

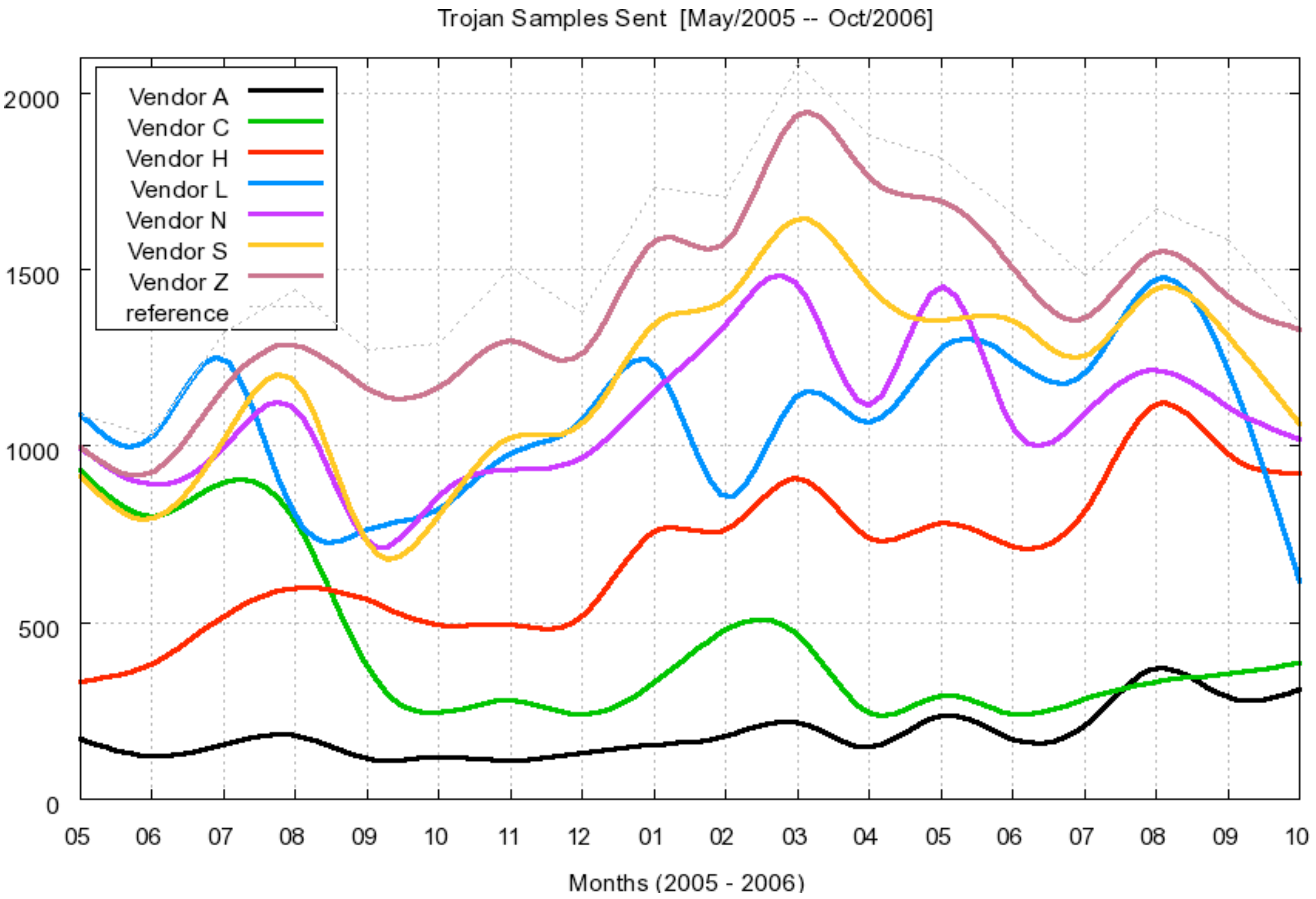
Only **2** vendors with the detection rate above **80%**

~70% of vendors with less than **40%**

Detection Rate - Monthly



Trojan Samples Sent - Monthly



National survey conducted by CETIC.br in August 2005

F1 - Security problems faced using the Internet

Percentage over the number of individuals who used the Internet in the 3 months prior to the survey

	None	Virus (un-authorized access)	Virus (software or hardware damage)	Abuse of personal information	Financial Fraud	Other	Don't Remeber
Total	40,99	19,64	7,13	1,67	0,94	1,10	0,24

F2 - Computer security measures adopted

Percentage over the number of individuals who have Internet access at home

	Anti-Virus	Personal Firewall	Anti-spyware Software
Total	69,76	19,33	22,09

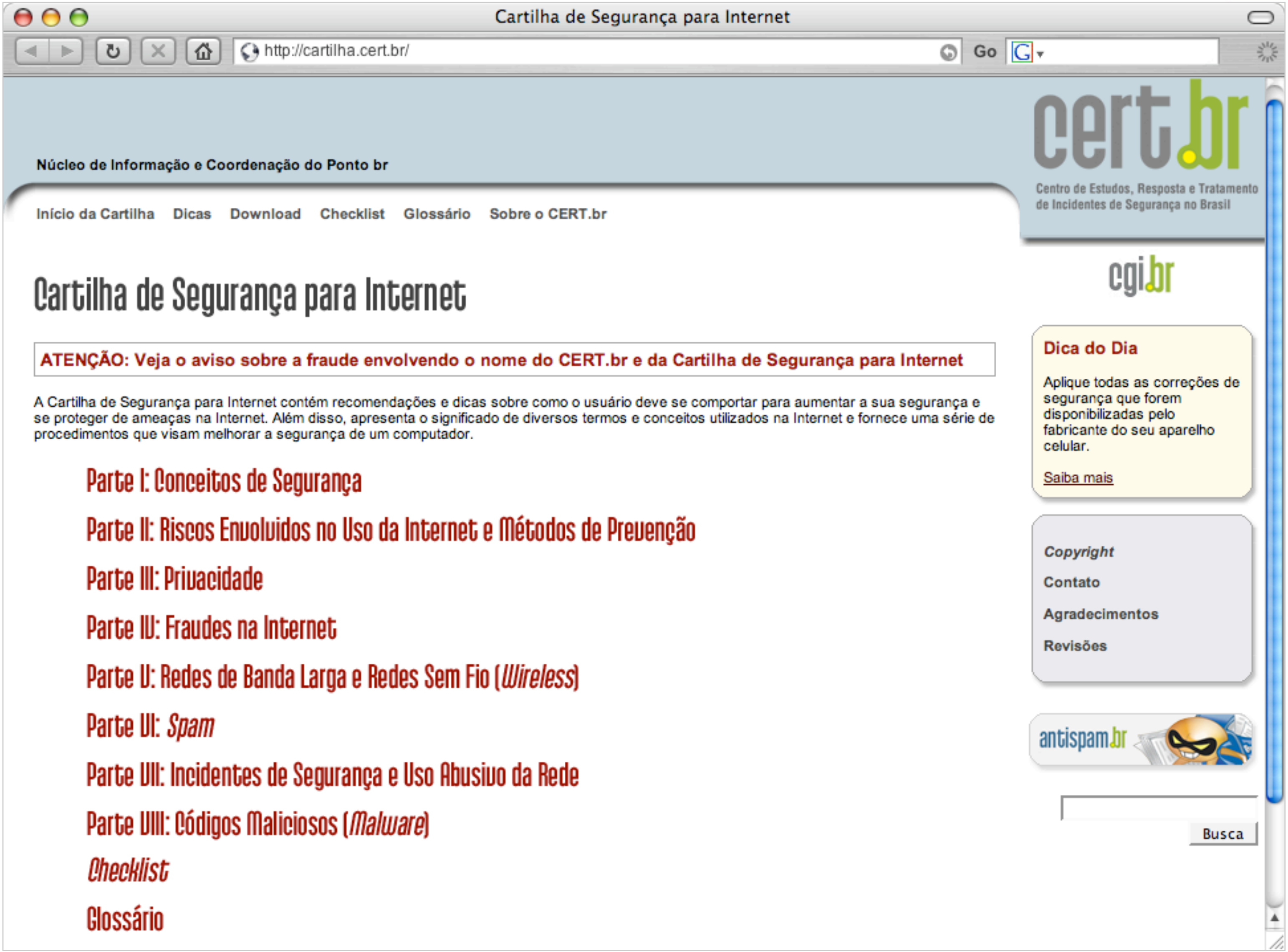
F3 - Anti-Virus updating frequency

Percentage over the number of individuals who have Internet access at home

	Daily	Weekly	Monthly	Every 3 Months	Didn't Update
Total	21,11	27,01	17,37	3,47	31,03

Notes -- *number of individuals who used the Internet in the 3 months prior to the survey: ~44 million people*
number of individuals who have internet access at home: ~17 million people

Best Practices for Internet Users


Cartilha de Segurança para Internet
http://cartilha.cert.br/
Go
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
cgi.br
antispam.br
Busca

Núcleo de Informação e Coordenação do Ponto br

Início da Cartilha | Dicas | Download | Checklist | Glossário | Sobre o CERT.br

Cartilha de Segurança para Internet

ATENÇÃO: Veja o aviso sobre a fraude envolvendo o nome do CERT.br e da Cartilha de Segurança para Internet

A Cartilha de Segurança para Internet contém recomendações e dicas sobre como o usuário deve se comportar para aumentar a sua segurança e se proteger de ameaças na Internet. Além disso, apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

- Parte I: Conceitos de Segurança
- Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
- Parte III: Privacidade
- Parte IV: Fraudes na Internet
- Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)
- Parte VI: *Spam*
- Parte VII: Incidentes de Segurança e Uso Abusivo da Rede
- Parte VIII: Códigos Maliciosos (*Malware*)
- *Checklist*
- Glossário

Dica do Dia

Aplique todas as correções de segurança que forem disponibilizadas pelo fabricante do seu aparelho celular.

Saiba mais

Copyright

Contato

Agradecimentos

Revisões

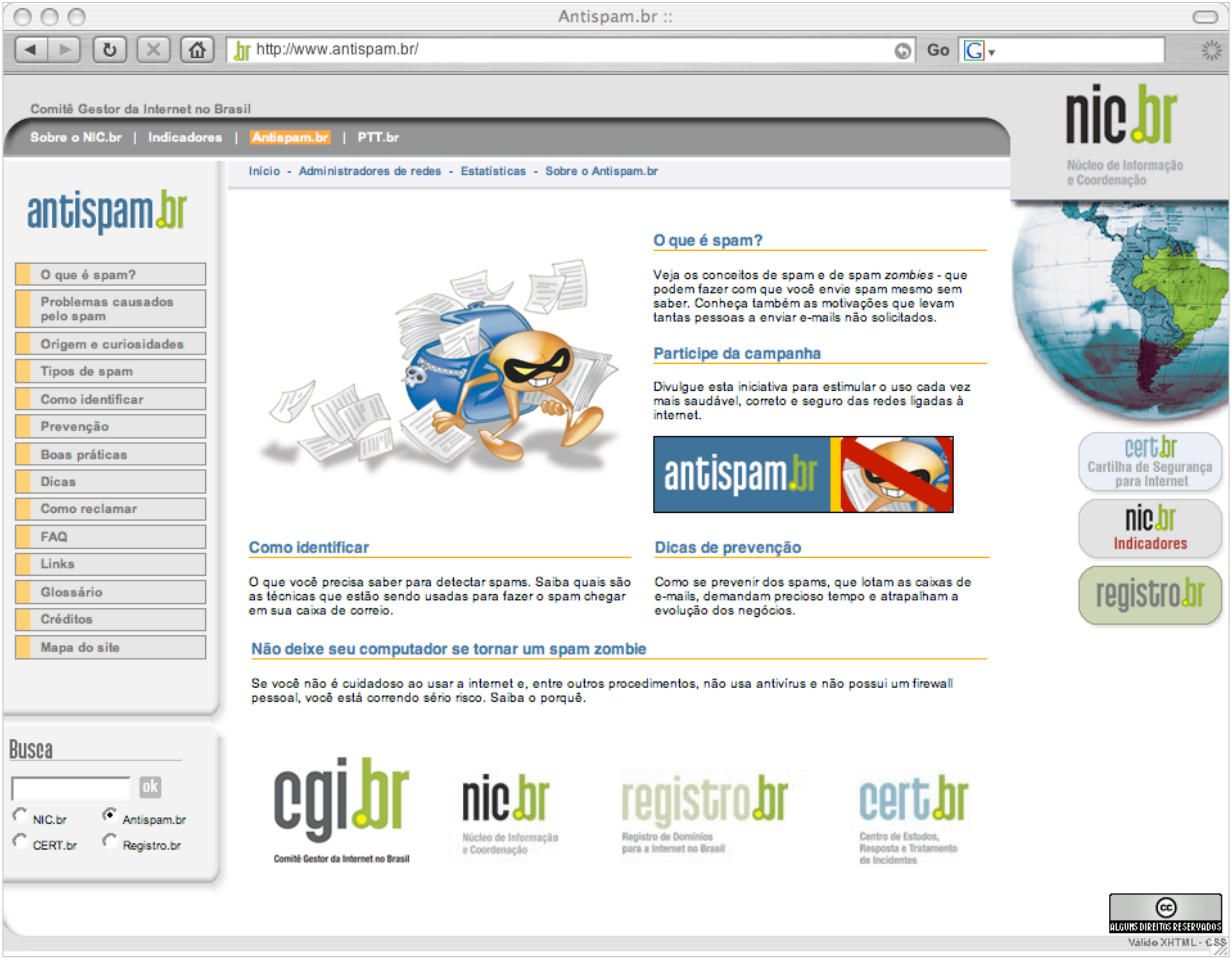
CGI.br Anti-Spam Comission

- Created by CGI.br to articulate, with all players, viable solutions to reduce the spam problem
  http://www.cgi.br/sobre-cg/antispam.htm

- Produced material that include tips for preventing from security problems coming through email
  - All material available at the www.antispam.br site

- CERT.br helped to produce 2 documents
  - Technologies and Policies to Fight Spam
  - Technical Analysis of Anti-spam Legislation

The antispam.br website


Antispam.br ::
http://www.antispam.br/
Go
Comitê Gestor da Internet no Brasil
Sobre o NIC.br | Indicadores | Antispam.br | PTT.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
Links
Glossário
Créditos
Mapa do site
Busca
ok
○ NIC.br
● Antispam.br
○ CERT.br
○ Registro.br
nic.br
Núcleo de Informação e Coordenação
cert.br
Cartilha de Segurança para Internet
nic.br
Indicadores
registro.br
cgi.br
Comitê Gestor da Internet no Brasil
nic.br
Núcleo de Informação e Coordenação
registro.br
Registro de Domínios para a Internet no Brasil
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes
ALGUNS DIREITOS RESERVADOS
Válido XHTML - CSS

O que é spam?

Veja os conceitos de spam e de spam *zombies* - que podem fazer com que você envie spam mesmo sem saber. Conheça também as motivações que levam tantas pessoas a enviar e-mails não solicitados.

Participe da campanha

Divulgue esta iniciativa para estimular o uso cada vez mais saudável, correto e seguro das redes ligadas à internet.

Como identificar

O que você precisa saber para detectar spams. Saiba quais são as técnicas que estão sendo usadas para fazer o spam chegar em sua caixa de correio.

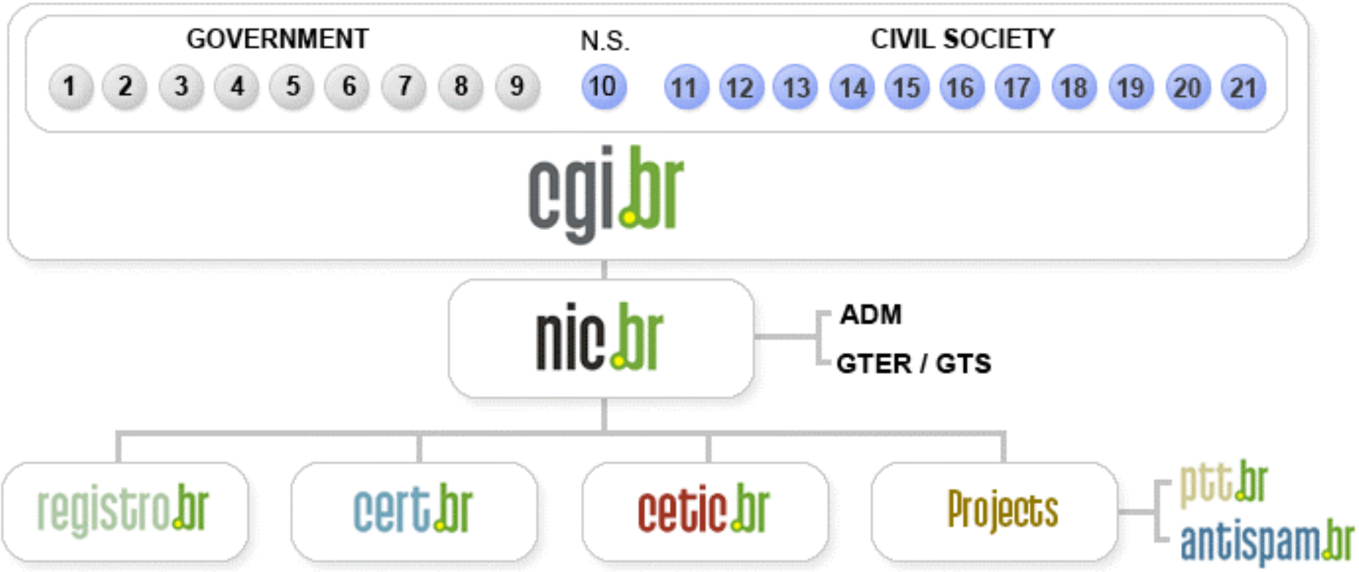
Dicas de prevenção

Como se prevenir dos spams, que lotam as caixas de e-mails, demandam precioso tempo e atrapalham a evolução dos negócios.

Não deixe seu computador se tornar um spam zombie

Se você não é cuidadoso ao usar a internet e, entre outros procedimentos, não usa antivírus e não possui um firewall pessoal, você está correndo sério risco. Saiba o porquê.

How the Initiatives are Related to Each Other



GOVERNMENT

1 2 3 4 5 6 7 8 9

N.S.

10

CIVIL SOCIETY

11 12 13 14 15 16 17 18 19 20 21

cgi.br

nic.br

ADM

GTER / GTS

registro.br

cert.br

cetic.br

Projects

ptt.br

antispam.br

1 – Ministry of Science and Technology (Coordination)

2 – Ministry of Communications

3 – Presidential Cabinet

4 – Ministry of Defense

5 – Ministry of Development, Industry and Foreign Trade

6 – Ministry of Planning, Budget and Management

7 – National Telecommunications Agency

8 – National Council of Scientific and Technological Development

9 – National Forum of Estate Science and Technology Secretaries

10 – Internet Expert

11 – Internet Service Providers

12 – Telecommunication Infrastructure Providers

13 – Hardware and Software Industries

14 – General Business Sector Users

15 – Non-governmental Entity

16 – Non-governmental Entity

17 – Non-governmental Entity

18 – Non-governmental Entity

19 – Academia

20 – Academia

21 – Academia

New Initiatives

- Cartoons
  - 4 videos - 4 minutes each
    - The Internet
    - The Intruders
    - Spam
    - The Defense
  - Freely available on the Internet
  - In several formats and resolutions
- Booklet or comics book
  - To distribute with the DVD version
    - Schools, presentations, libraries, internet cafes, etc
  - Still in discussion (funding and sponsors issues)

References

- CGI.br - Brazilian Internet Steering Committee
  http://www.cgi.br/

- NIC.br
  http://www.nic.br/

- CETIC.br - ICT Research Center
  http://www.cetic.br/

- CERT.br
  http://www.cert.br/

- Antispam.br
  http://www.antispam.br/