

## Segurança da Internet no Brasil: Estudos e Iniciativas

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

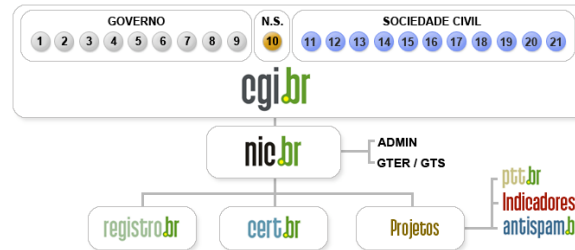
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br  
<http://www.cert.br/>

Comitê Gestor da Internet no Brasil - CGI.br  
<http://www.cgi.br/>

## Agenda

- Sobre o CGI.br e o CERT.br
- Indicadores do CGI.br
- Estatísticas do CERT.br
- Iniciativas de Segurança
- Referências

## Comitê Gestor da Internet no Brasil



- |   |  |
|---|--|
| 1 – Ministério da Ciência e Tecnologia (Coordenação)              | 11 – provedores de acesso e conteúdo                               |
| 2 – Ministério das Comunicações                                   | 12 – provedores de infra-estrutura de telecomunicações             |
| 3 – Casa Civil da Presidência da República                        | 13 – indústria de bens de informática, telecomunicações e software |
| 4 – Ministério da Defesa  | 14 – segmento das empresas usuárias de Internet                    |
| 5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior  | 15-18 – representantes do terceiro setor                           |
| 6 – Ministério do Planejamento, Orçamento e Gestão                | 19-21 – representantes da comunidade científica e tecnológica      |
| 7 – Agência Nacional de Telecomunicações (Anatel)                 |  |
| 8 – Conselho Nacional de Desenvolvimento Científico e Tecnológico |  |
| 9 – Fórum Nacional de Secretários Estaduais para Assuntos de C&T  |  |
| 10 – Representante de Notório Saber em assuntos de Internet       |  |

<http://www.cgi.br/sobre-cg/>

2ª Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 3/34

## Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na Internet;
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**

2ª Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 4/34

## Atividades do CERT.br

- Articulação das ações para resposta a incidentes envolvendo redes brasileiras
- Manutenção de estatísticas sobre incidentes de segurança
- Desenvolvimento de documentos de Boas Práticas para usuários e administradores de redes
- Fomento à criação de novos Grupos de Segurança e Resposta a Incidentes (CSIRTs) no Brasil
- Oferecimento de cursos oficiais do CERT® Program
- Coordenação do “Consórcio Brasileiro de Honeypots”
- Membro do FIRST e da HoneyNet Research Alliance
- Anti-Phishing Working Group (APWG) Research Partner

## Indicadores do CGI.br

## Indicadores do CGI.br

- Parceria com o IBGE e IBOPE/NetRatings
- Pesquisas TIC Domicílios e TIC Empresas 2005, realizadas para o CGI.br, pelo Instituto Ipsos Opinion  
<http://www.nic.br/indicadores/>

### Objetivos:

- Produzir e divulgar com periodicidade indicadores oficiais sobre penetração e uso da Internet;
- Fornecer subsídios para a elaboração de políticas públicas que garantam o acesso às TICs no Brasil;
- Acompanhar, monitorar e avaliar o impacto sócio econômico das TICs;
- Permitir a comparabilidade da realidade brasileira com outros países.

## Indicadores do CGI.br (2)

### TIC Domicílios

Tabela 10 - População segundo PNAD 2003 = 173.966.052

C1 - Proporção de Domicílios com Internet = 21,43%  
*Percentual sobre o total de domicílios (8540 domicílios entrevistados)*

C2 - Proporção de Indivíduos com Acesso à Internet no Domicílio = 9,39%  
*Percentual sobre o total da população (8540 domicílios entrevistados)*

C5 - Proporção de Indivíduos que Acessaram à Internet, de qualquer Local  
*Percentual sobre o total da população (8540 domicílios entrevistados)*

	< 3 meses	Entre 3 e 6 meses	Entre 6 e 12 meses	+ 12 meses	Nunca usou
Percentual	24,41	2,65	2,26	2,93	67,76

## Indicadores do CGI.br (3)

Números relacionados com segurança:

- TIC Domicílios
  - F - Segurança
    - F1 - Problemas de segurança encontrados usando a Internet
    - F2 - Medidas de segurança tomadas com relação ao computador
    - F3 - Frequência de atualização do antivírus
- TIC Empresas
  - E - Segurança
    - E1 - Problemas de segurança encontrados
    - E2 - Medidas de segurança adotadas
    - E3 - Frequência de atualização do antivírus
    - E4 - Uso de recursos de segurança para comunicação

## TIC Domicílios

### F1 - Problemas de Segurança Encontrados Usando a Internet

Percentual sobre o total de usuários Internet

	Nenhum	Vírus (com acesso não autorizado)	Vírus (com danos em SW ou HW)	Abuso de Informação pessoal	Fraude	Outro	Não lembra
Total	40,99	19,64	7,13	1,67	0,94	1,10	0,24

### F2 - Medidas de Segurança Tomadas com Relação ao Computador

Percentual sobre o total de usuários Internet que possuem computador

	Antivírus	Firewall Pessoal	Software Anti-spyware
Total	69,76	19,33	22,09

### F3 - Frequência de Atualização do Antivírus

Percentual sobre o total de usuários Internet que possuem computador

	Diária	Semanal	Mensal	Trimestral	Não atualizou
Total	21,11	27,01	17,37	3,47	31,03

## TIC Empresas

### E1 - Problemas de Segurança Encontrados

Percentual sobre o total de empresas com acesso à Internet

	Vírus	Worms ou Bots	Trojans	Acesso externo não autorizado	Acesso interno não autorizado	DoS	Desfiguração de Servidor Web
Total	50,34	17,44	31,13	10,89	7,61	6,25	11,20

### E2 - Medidas de Segurança Adotadas

Percentual sobre o total de empresas com acesso à Internet

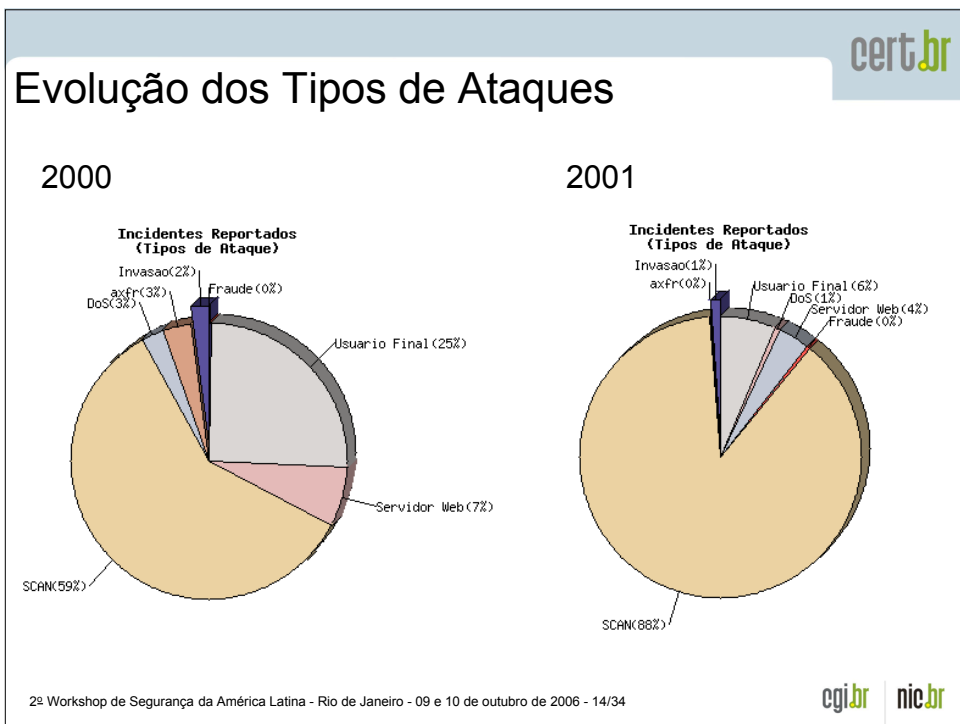
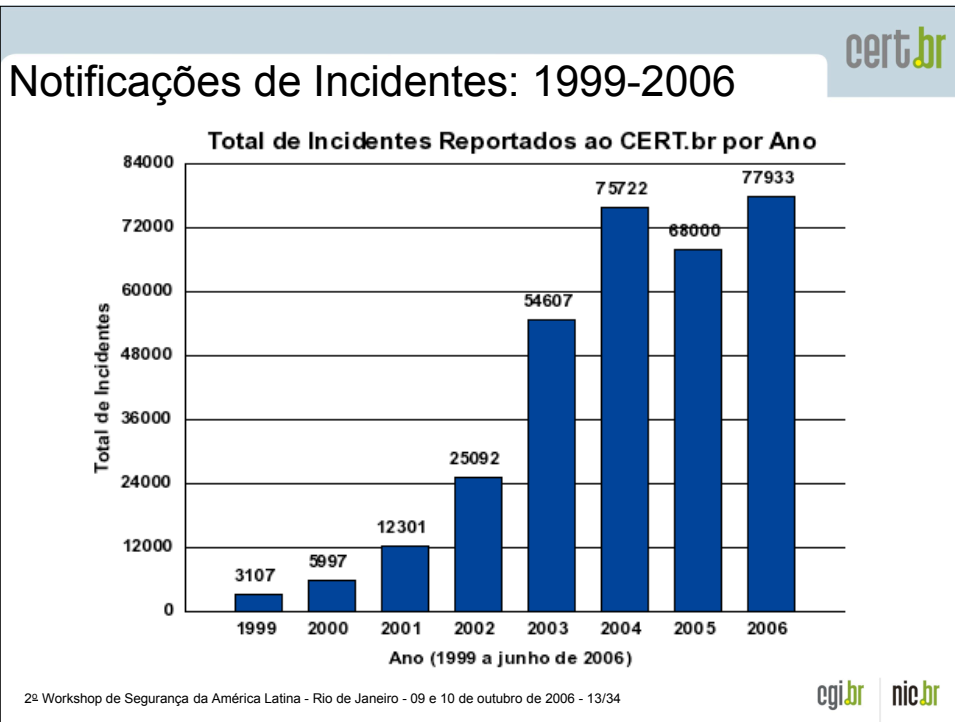
	Antivírus	Software Anti-spyware	Firewall	SSL, HTTPs	Autenticação para usuários internos	Autenticação para usuários externos	IDS	Backup	Backup offsite	Programa de Treinamento para Funcionários
Total	95,72	59,46	54,11	49,48	42,33	21,12	29,21	69,62	38,33	19,69

### E3 - Frequência de Atualização do Antivírus

Percentual sobre o total de empresas com acesso à Internet

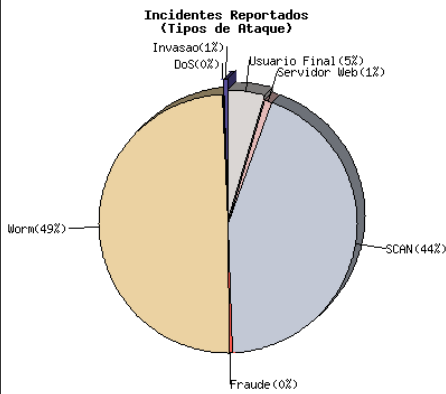
	Diária	Semanal	Mensal	Trimestral	Semestral/Anual	Não atualizou
Total	41,68	30,02	12,34	5,11	2,11	8,74

## Estatísticas do CERT.br

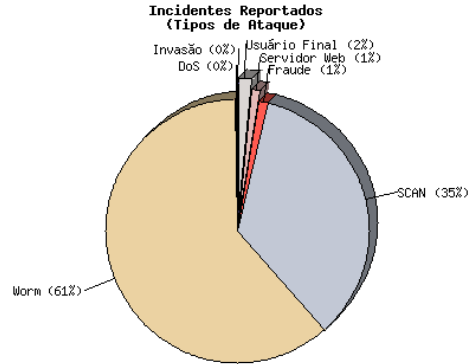


## Evolução dos Tipos de Ataques (cont)

2002



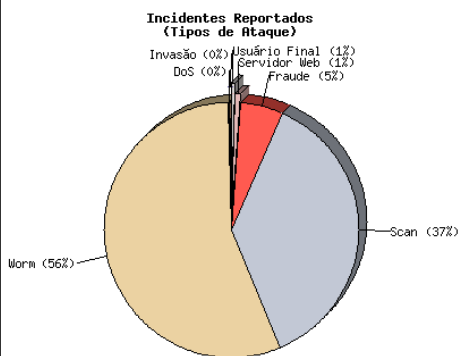
2003



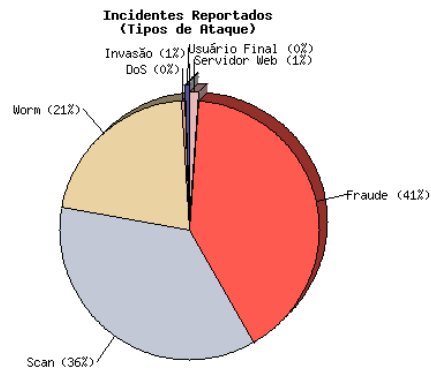
2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 15/34

## Evolução dos Tipos de Ataques (cont)

2004



2005



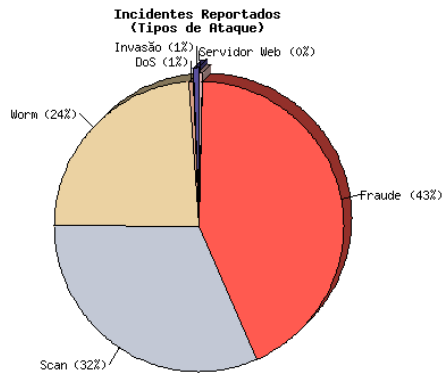
2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 16/34



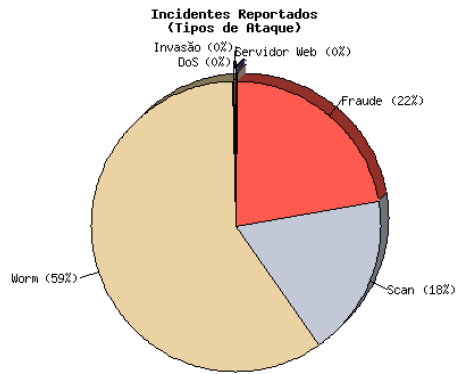
## Evolução dos Tipos de Ataques (cont)

2006

1º Trimestre:

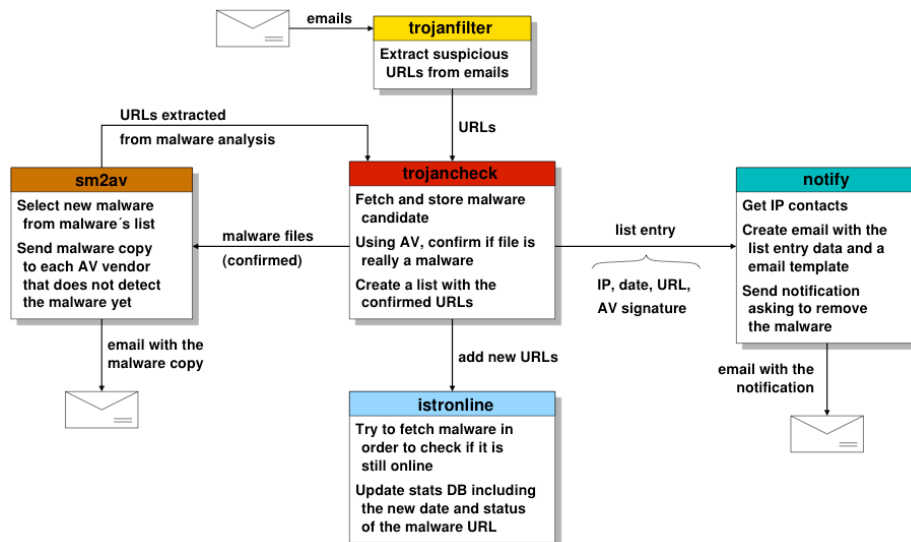


2º Trimestre:



2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 17/34

## Tratamento de Incidentes Envolvendo Fraudes



2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 18/34

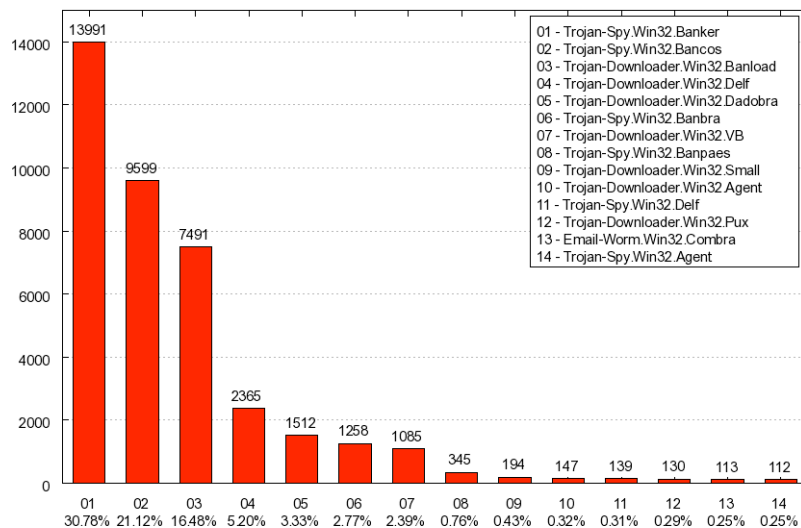
## Estatísticas de 01/04/2005 a 26/09/2006

Categoria	Número
Domínios que estavam hospedando <i>trojans</i>	6.284
Contatos únicos para os domínios	2.552
Extensões usadas pelos arquivos de <i>trojans</i>	68
Nomes de arquivos utilizados pelos <i>trojans</i>	14.237
Nomes de máquinas ( <i>hosts</i> ) envolvidas	10.818
Endereços IP únicos	4.686
Países para os quais estavam alocados os IPs	75
<i>E-mails</i> de notificação enviados pelo CERT.br	23.709
URLs únicas encontradas no período	33.946
Assinaturas de antivírus (agrupadas)	161
Assinaturas de antivírus (com variantes)	2.418

2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 19/34

## Assinaturas Mais Comuns

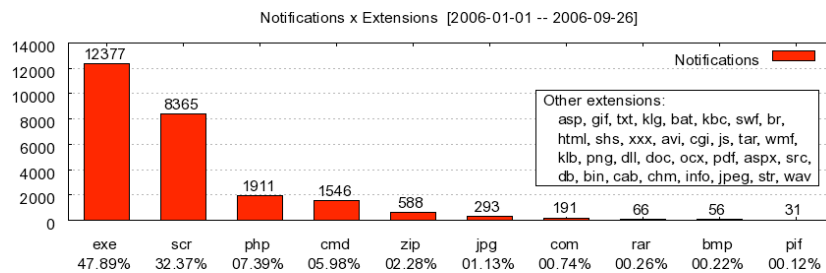
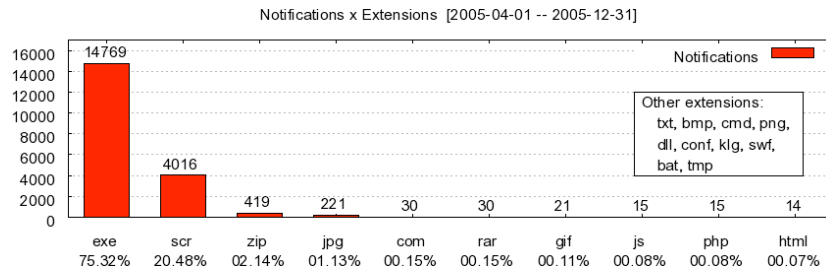
Notifications x Signatures [2005-04-01 - 2006-09-26]



Fonte das assinaturas: Kaspersky Lab.

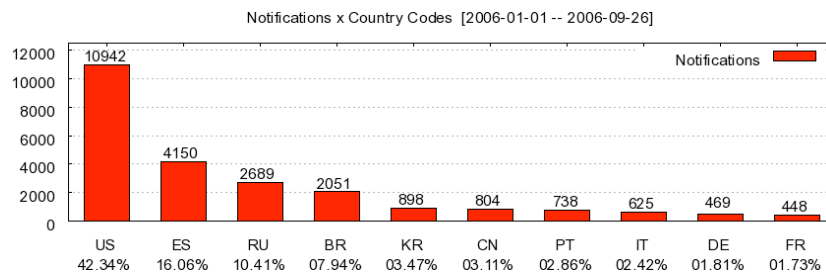
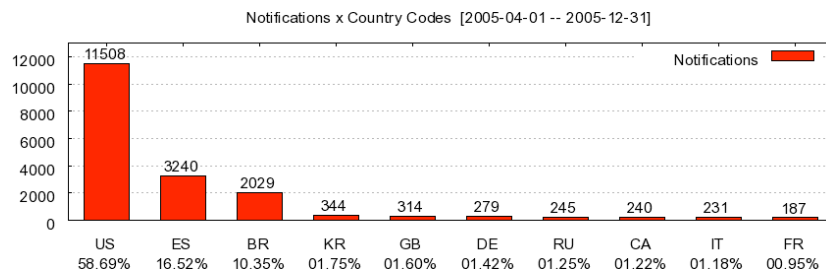
2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 20/34

## Extensões Mais Comuns



2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 21/34

## Países para os quais Estavam Alocados os IPs



2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 22/34

### Eficiência dos Antivírus: 06/04/2005 a 26/09/2006

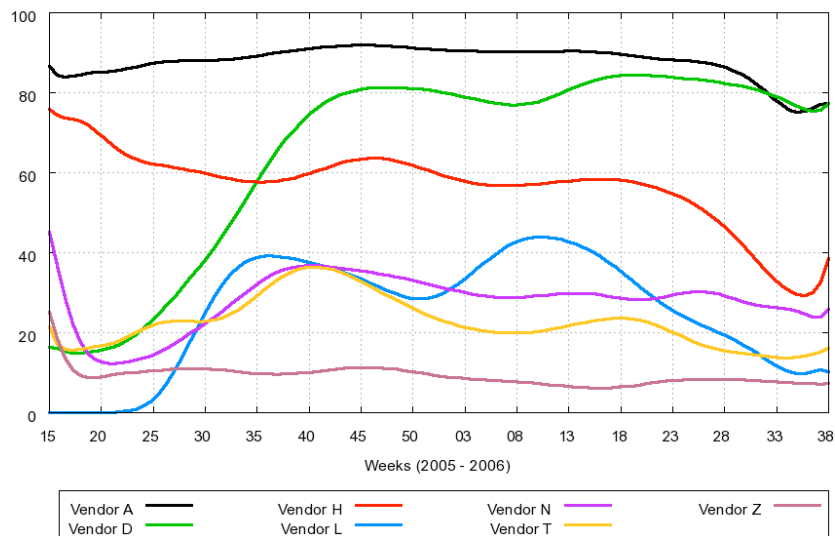
Empresa de Antivírus	Exemplares testados	Exemplares não detectados	Exemplares detectados	Taxa de detecção (%)
Vendor A	26.492	3.164	23.328	88,06
Vendor B	5.651	1.019	4.632	81,97
Vendor C	790	240	550	69,62
Vendor D	26.526	8.300	18.226	68,71
Vendor E	26.342	8.787	17.555	66,64
Vendor F	26.513	8.856	17.657	66,60
Vendor G	26.219	10.512	15.707	59,91
Vendor H	26.527	11.576	14.951	56,36
Vendor I	15.337	7.559	7.778	50,71
Vendor K	17.888	10.846	7.042	39,37
Vendor L	22.462	15.142	7.320	32,59
Vendor N	26.215	18.592	7.623	29,08
Vendor O	26.160	18.653	7.507	28,70
Vendor P	21.988	15.836	6.152	27,98
Vendor Q	26.524	19.168	7.356	27,73
Vendor T	26.509	20.595	5.914	22,31
Vendor Z	26.281	23.906	2.375	9,04

Apenas 2 fabricantes com taxa de detecção acima de 80%

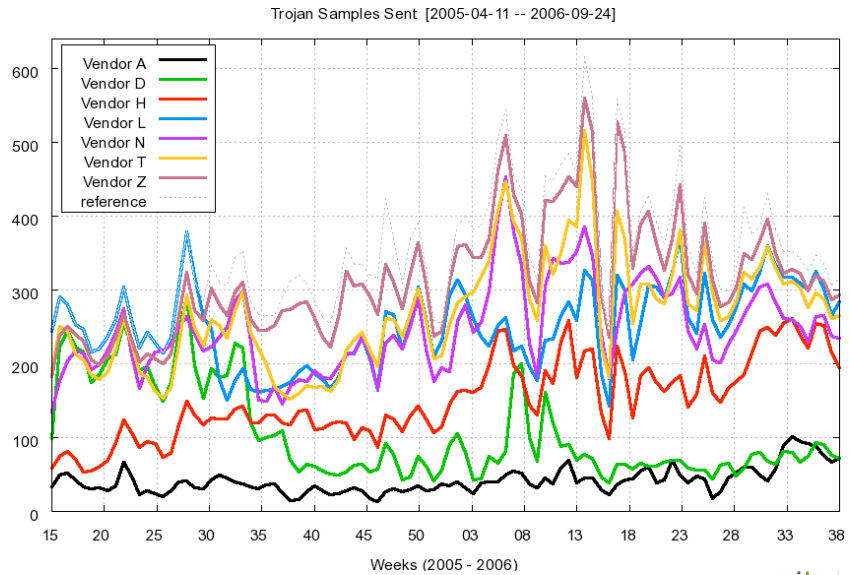
~70% dos fabricantes com menos de 40% de taxa de detecção

### Taxa de Detecção: 11/04/2005 a 24/09/2006

AV Vendors Detection Rate Average (%) [2005-04-11 -- 2006-09-24]



Exemplares enviados: 11/04/2005 a 24/09/2006



2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 25/34

## Iniciativas para Aumentar a Segurança

2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 26/34

**cert.br**

## Ações em Diversas Frentes

- Não há solução única
  - Combinar soluções e tecnologias
  - Investir em treinamento e atualização dos profissionais
- Educação de usuários é fundamental
  - vetores disseminação de worms/vírus
  - alvos de engenharia social (trojans, fraudes, etc)
- Materiais gratuitos disponíveis
  - Práticas de Segurança para Administradores de Redes Internet  
<http://www.cert.br/seg-adm-redes/>
  - Cartilha de Segurança para Internet  
<http://cartilha.cert.br/>
  - Site Antispam.br  
<http://www.antispam.br/>

2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 27/34

**cgi.br** | **nic.br**

Cartilha de Segurança para Internet

**cert.br**  
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

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

---

**antispam.br**

Busca

Cartilha de Segurança para Internet

http://cartilha.cert.br/dicas/

**cert.br**  
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

**egi.br**

Núcleo de Informação e Coordenação do Ponto br

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

## Cartilha de Segurança para Internet

Nesta página está disponível uma compilação de dicas básicas de segurança.

Estas dicas também estão em 2 folhetos disponíveis para *download*. Para visualizá-los você precisa ter instalado em seu computador o software *Acrobat Reader*.

**Proteja-se de fraudes**

- Atualize seu antivírus diariamente.
- Não clique em *links* recebidos por *e-mail*.
- Não execute arquivos recebidos por *e-mail* ou via serviços de mensagem instantânea.

**Proteja-se de vírus, cavalos de tróia, spywares, worms e bots**

- Mantenha todos os programas que você usa sempre atualizados.
- Instale todas as correções de segurança.
- Use antivírus, *firewall* pessoal e anti-*spyware*.

**Navegue com segurança**

- Mantenha seu navegador sempre atualizado.
- Desative *Java* e *ActiveX*. Use-os apenas se for estritamente necessário.
- Só habilite *JavaScript*, *cookies* e *pop-up windows* ao acessar sites confiáveis.

**Cuide-se ao ler e-mails**

**Folheto com dicas de segurança, formato A4. (102 KB)**

**Folder com dicas de segurança, formato A4. (1.1 MB)**

Antispam.br ::

http://www.antispam.br/

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

NIC.br Antispam.br  
CERT.br Registro.br

**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

### O que é spam?

Veja os conceitos de spam e de spam zombiês - 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.

Antispam.br ::

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | **Antispam.br** | PTT.br

Inicio - 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

NIC.br Antispam.br  
 CERT.br Registro CERT.br

**Dicas**

Principais dicas para ajudar o usuário a receber menos spam, preservar sua privacidade e evitar que códigos maliciosos sejam instalados em seu computador:

**Preserve sua privacidade**

- Seja criterioso ao informar seus endereços de e-mail em cadastros, sites de relacionamentos etc.
- Tenha e-mails diferentes para uso pessoal, trabalho, compras on-line e cadastros em sites em geral
- Evite utilizar e-mails simples, como aqueles formados apenas pelo primeiro nome.
- Leia com atenção os formulários e cadastros on-line, evitando preencher ou concordar, inadvertidamente, com as opções para recebimento de e-mails de divulgação do site e de seus parceiros.
- Não forneça dados pessoais, documentos e senhas por e-mail ou via formulários on-line.
- Verifique a política de privacidade dos sites, onde pretende registrar seus dados.

**Mantenha-se informado**

- Conhecer os tipos de spam ajuda a reconhecer e-mails suspeitos e, eventualmente, não detectados pelos softwares anti-spam.
- Acompanhar as notícias e alertas sobre os golpes e fraudes, reduz o risco de ser enganado e/ou prejudicado financeiramente por e-mails desse gênero.
- Procurar informações sobre fatos recebidos por e-mail, antes de repassá-los, contribui para a redução do volume de mensagens de correntes, boatos e lendas urbanas, enviadas repetidas vezes na rede.
- Procurar informações no site das empresas, ao receber e-mails sobre prêmios e promoções, reduz o risco de ser enganado em golpes propagados por e-mail.

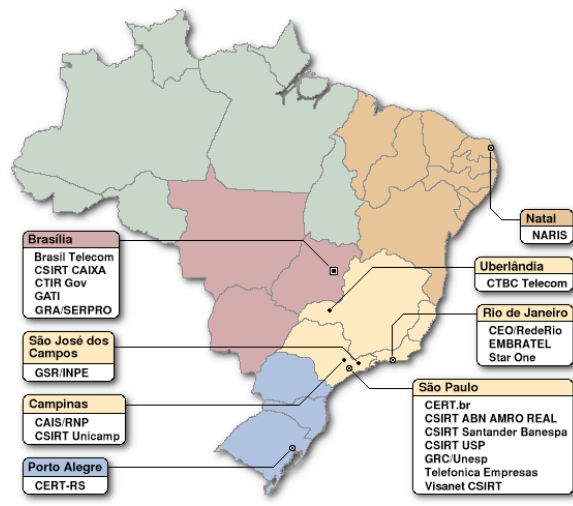
**Proteja-se**

- Utilize softwares de proteção (antivírus, anti-spam, anti-spyware e firewall pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas.
- Não seja um "cliquador compulsivo". Não execute arquivos anexados em e-mails sem examiná-los previamente com antivírus, bem como,



Compartilhar Informações e Experiências é Fundamental

**cert.br**



**Brasília**  
 Brasil Telecom  
 CSIRT CAIXA  
 CTIR Gov  
 GATI  
 GRASERPRO

**São José dos Campos**  
 GSRINPE

**Campinas**  
 CAIS/RNP  
 CSIRT Unicamp

**Porto Alegre**  
 CERT-RS

**Natal**  
 NARIS

**Uberlândia**  
 CTBC Telecom

**Rio de Janeiro**  
 CEO/RedeRio  
 EMBRATEL  
 Star One

**São Paulo**  
 CERT.br  
 CSIRT ABN AMRO REAL  
 CSIRT Santander Banespa  
 CSIRT USP  
 GRC/Unesp  
 Telefonica Empresas  
 Visanet CSIRT

CSIRTs Brasileiros  
<http://www.cert.br/contato-br.html>

2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 32/34

**cgi.br** | **nic.br**



## Também com Grupos de Outros Países

Incident Response Teams Around the World International cooperation speeds response to Internet security breaches.



CSIRTs no Mundo

<http://www.cert.org/csirts/>

2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 33/34

## Referências

- Esta palestra  
<http://www.cert.br/docs/palestras/>
- Indicadores do CGI.br  
<http://www.nic.br/indicadores/>
- Antispam.br  
<http://www.antispam.br/>
- Material de Apoio para CSIRTs  
<http://www.cert.br/csirts/>
- Cartilha de Segurança para Internet  
<http://cartilha.cert.br/>
- Cursos Oficiais do CERT® Program ministrados pelo CERT.br  
<http://www.cert.br/cursos/>



2º Workshop de Segurança da América Latina - Rio de Janeiro - 09 e 10 de outubro de 2006 - 34/34