

## Segurança da Informação na Internet no Brasil: Últimos Estudos do Comitê Gestor da Internet no Brasil e Iniciativas para Aumentar a Segurança

Cristine Hoepers  
cristine@cert.br

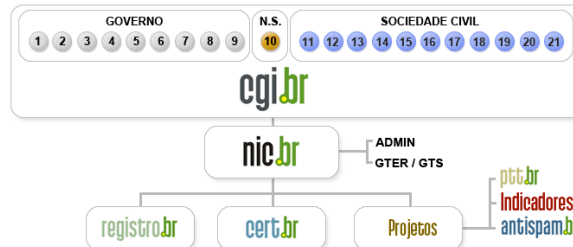
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br  
<http://www.cert.br/>

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       |  |

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## 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.**

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Atividades do CERT.br

- Articulação das ações para resposta a incidentes envolvendo redes brasileiras, por exemplo:
  - Combate a fraudes: contato com sites envolvidos para remoção de códigos maliciosos; envio de novos exemplares para fabricantes de antivírus; troca de informações técnicas com instituições financeiras
- 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®/CC
- Coordenação do “Consórcio Brasileiro de Honeypots”

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Parcerias Internacionais do CERT.br

- Forum of Incident Response and Security Teams (FIRST)  
Full member  
<http://www.first.org/membership/>
- Anti-Phishing Working Group (APWG) Research Partner  
<http://www.antiphishing.org/>
- Honeynet Research Alliance Member  
<http://honeynet.org/alliance/>

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

# Indicadores do CGI.br

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Indicadores do CGI.br

- Pesquisas em parceria com o IBGE, com o Instituto Ipsos Opinion e com o Ibope/Netratings

<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.

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Indicadores do CGI.br (cont)

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
  - J - Spam
    - J1 - Recebimento de spam na principal conta de e-mail de uso pessoal
    - J2 - Frequência de recebimento de spam na principal conta de e-mail de uso pessoal
    - J3 - Número de spams recebidos na principal conta de e-mail de uso pessoal
    - J4 - Tempo perdido com spams na principal conta de e-mail de uso pessoal
- 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

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## TIC Domicílios

### F2 - Problemas de Segurança Encontrados Usando a Internet

Percentual sobre o total de usuários Internet que possuem computador

	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

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## 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

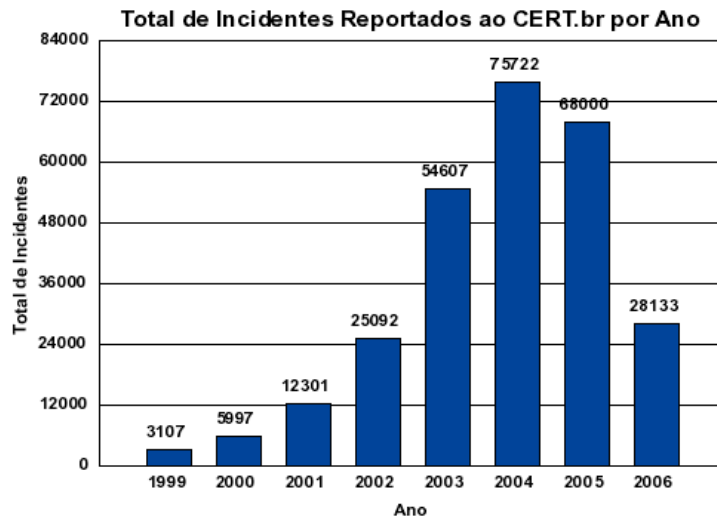
	Diária	Semanal	Mensal	Trimestral	Semestral/Anual	Não atualizou
Total	41,68	30,02	12,34	5,11	2,11	8,74

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Estatísticas do CERT.br

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Notificações de Incidentes: 1999-2006

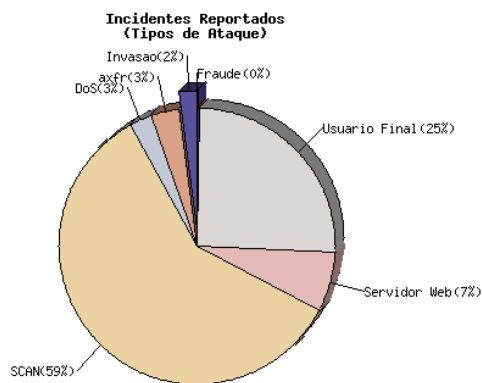


Obs.: Os dados de 2006 são referentes ao primeiro trimestre do ano.

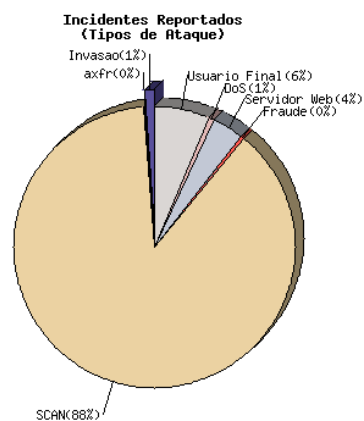
XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Evolução dos Tipos de Ataques

2000



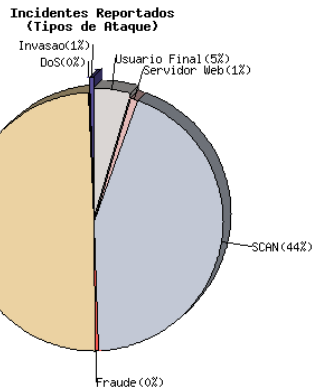
2001



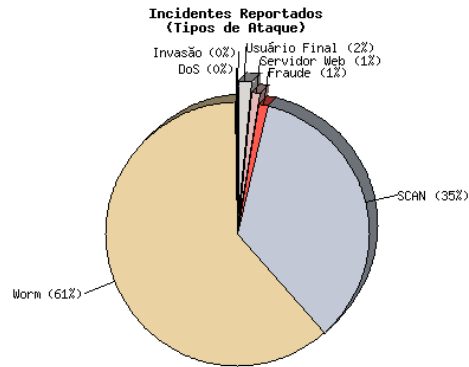
XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Evolução dos Tipos de Ataques (cont)

2002



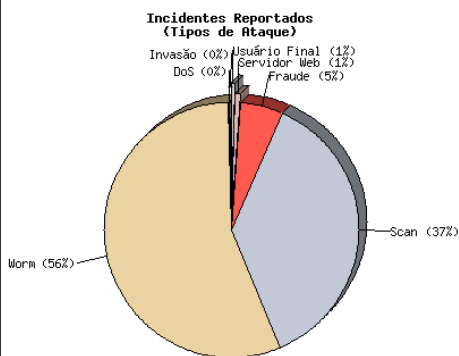
2003



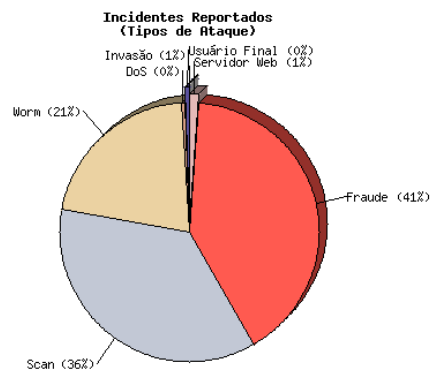
XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Evolução dos Tipos de Ataques (cont)

2004



2005

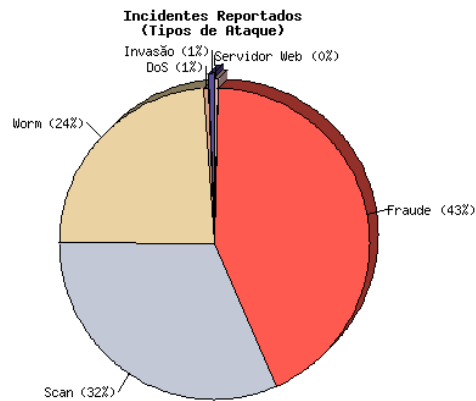


XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006



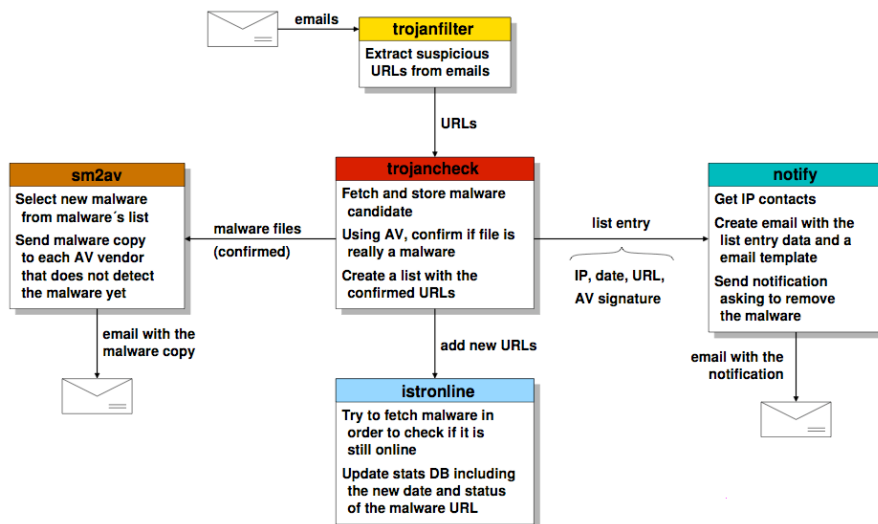
## Evolução dos Tipos de Ataques (cont)

1º Trimestre de 2006:



XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Tratamento de Incidentes Envolvendo Fraudes



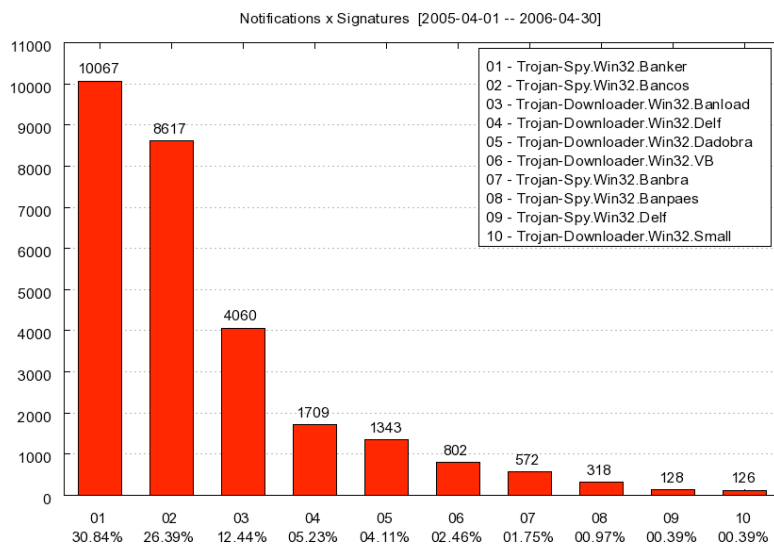
XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Estatísticas de 01/04/2005 a 30/04/2006

Categoria	Número
Domínios que estavam hospedando <i>trojans</i>	3.807
Contatos únicos para os domínios	1.782
Extensões usadas pelos arquivos de <i>trojans</i>	45
Nomes de arquivos utilizados pelos <i>trojans</i>	9.520
Nomes de máquinas ( <i>hosts</i> ) envolvidas	6.137
Endereços IP únicos	3.166
Países para os quais estavam alocados os IPs	68
<i>E-mails</i> de notificação enviados pelo CERT.br	15.556
URLs únicas encontradas no período	24.005
Diferentes assinaturas de antivírus	1.546

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

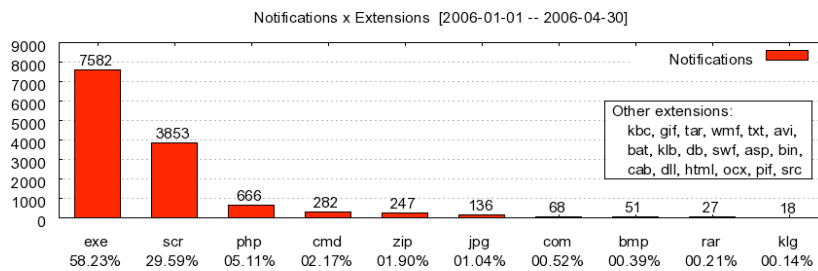
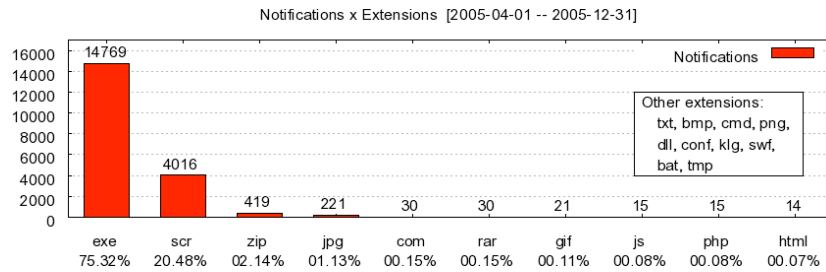
## Assinaturas Mais Comuns



Fonte das assinaturas: Kaspersky Lab.

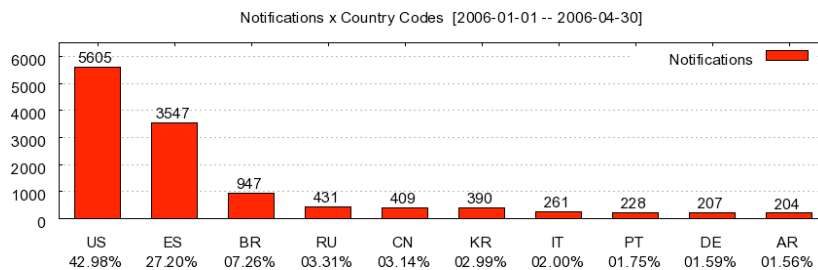
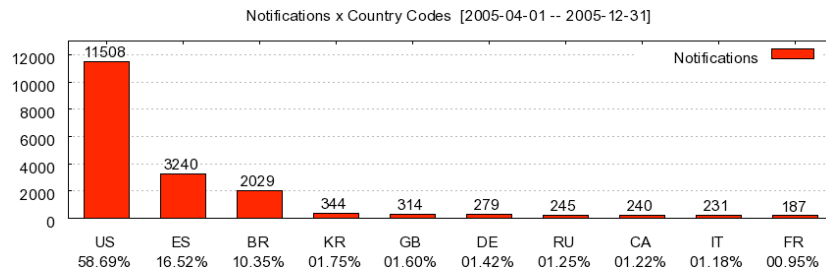
XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Extensões Mais Comuns



XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Países para os quais Estavam Alocados os IPs



XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

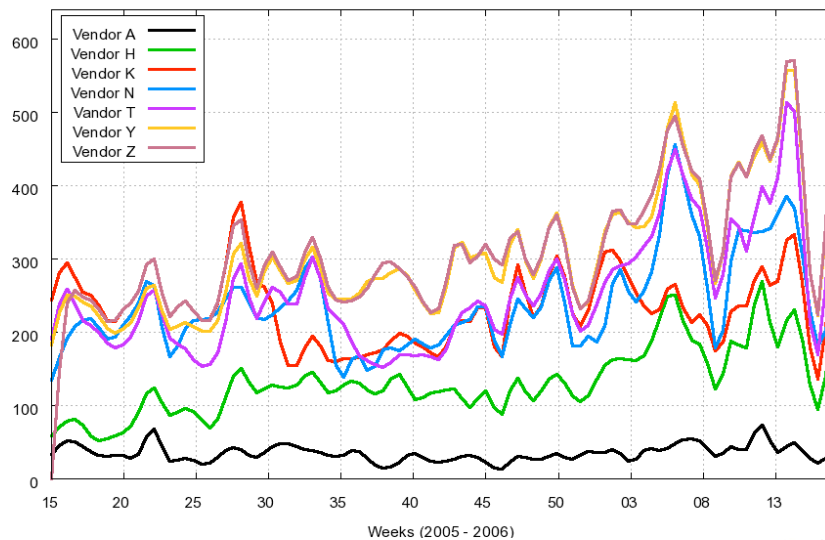
## Eficiência dos Antivírus: 06/04/2005 a 30/04/2006

Empresa de Antivírus	Exemplares testados	Exemplares não detectados	Exemplares detectados	Taxa de detecção (%)
Vendor A	18.634	1.913	16.721	89,73
Vendor B	5.653	1.020	4.633	81,96
Vendor D	18.519	5.475	13.044	70,44
Vendor E	18.652	6.240	12.412	66,55
Vendor F	18.665	6.857	11.808	63,26
Vendor G	18.348	6.750	11.598	63,21
Vendor H	18.666	7.324	11.342	60,76
Vendor I	7.474	3.160	4.314	57,72
Vendor K	14.603	8.873	5.730	39,24
Vendor L	18.658	11.623	7.035	37,71
Vendor N	18.371	12.866	5.505	29,97
Vendor O	18.606	13.084	5.522	29,68
Vendor P	14.126	10.162	3.964	28,06
Vendor Q	18.541	13.395	5.146	27,75
Vendor T	18.652	14.140	4.512	24,19
Vendor Y	18.469	16.713	1.756	9,51
Vendor Z	15.784	14.517	1.267	8,03

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

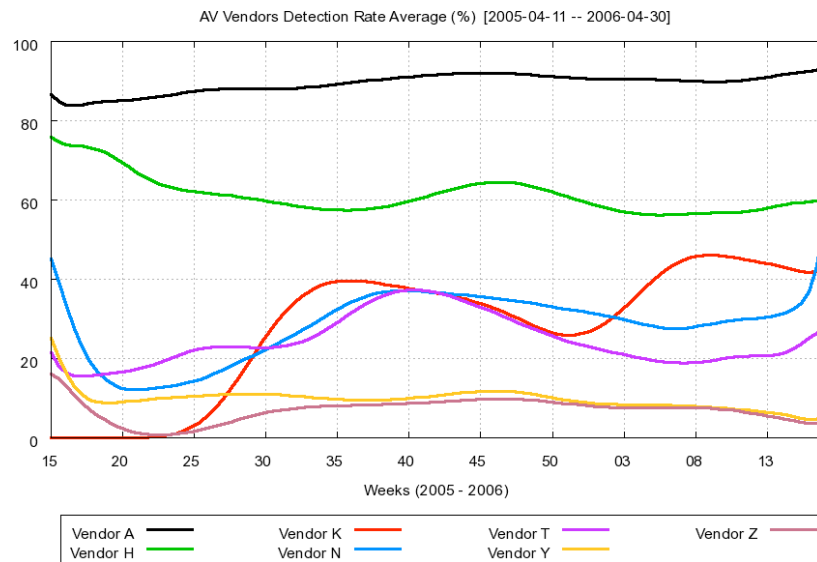
## Exemplares enviados: 06/04/2005 a 30/04/2006

Trojan Samples Sent [2005-04-11 -- 2006-04-30]



XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Taxa de Detecção: 06/04/2005 a 30/04/2006



XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

## Iniciativas para Aumentar a Segurança

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

**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/>

XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

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

Cartilha de Segurança para Internet

http://cartilha.cert.br/

**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

**cgi.br**

**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

**cert.br**  
Cartilha de Segurança para Internet

**nic.br**  
Indicadores

**registro.br**

## 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

**Tipos de spam**

[A voltar](#)

**Códigos maliciosos**

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em **spams enviados por fraudadores**.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- **Backdoor:** Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- **Spyware:** Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.
- **Keylogger:** Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
- **Screenlogger:** Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.
- **Cavalo de tróia:** Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.



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

**Tipos de spam**

[A voltar](#)

**Fraudes**

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os fraudadores têm utilizado amplamente e-mails com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os e-mails que recebem e ao utilizarem serviços de comércio eletrônico ou Internet Banking.

**Sumário**

- [Golpes \(Scams\)](#)
- [Phishing: situações em que pode ocorrer este tipo de fraude](#)
- [Mensagens que contêm links para programas maliciosos](#)
- [Como o fraudador consegue acesso ao seu computador](#)
- [Como identificar](#)
- [Recomendações](#)

**Golpes (Scams)**





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>  
 XX Dados a Salvo de Tragédias - São Paulo - 06 de junho de 2006

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

