

## Financial Fraud Response in Brazil Challenges and Evolution

Cristine Hoepers  
cristine@cert.br

Klaus Steding-Jessen  
jessen@cert.br

Computer Emergency Response Team Brazil - CERT.br  
<http://www.cert.br/>

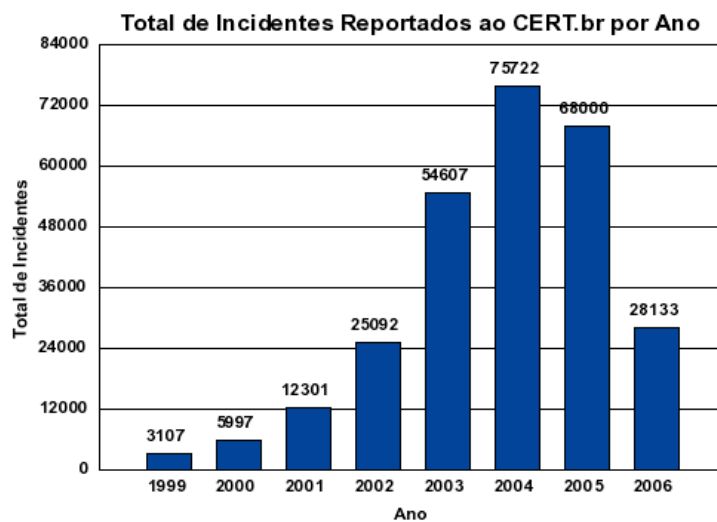
Brazilian Internet Steering Committee - CGI.br  
<http://www.cgi.br/>

## Agenda

- Some statistics
- Interaction with Law Enforcement and the Financial Sector
- CERT.br
  - Automation and coordination
- References

## Some Statistics

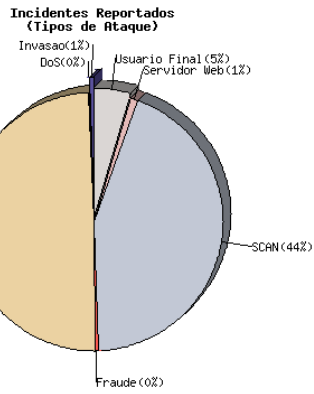
## Incidents Reported to CERT.br: 1999-2006



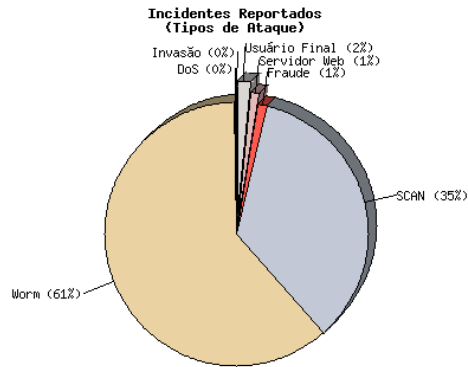
Note: 2006 has data from 1<sup>st</sup> quarter only.

# Incidents Reported to CERT.br

2002



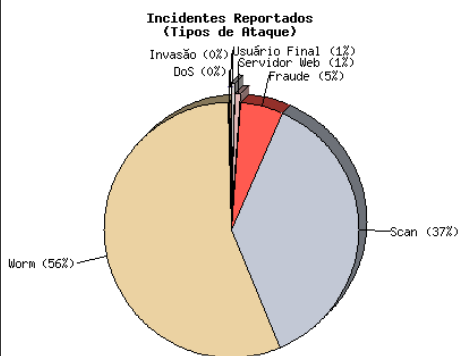
2003



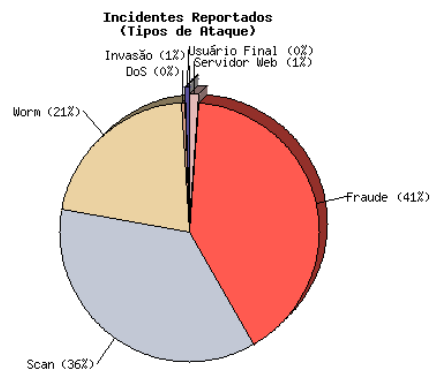
Meeting for CSIRTs with National Responsibility - July 2006

# Incidents Reported to CERT.br (cont)

2004



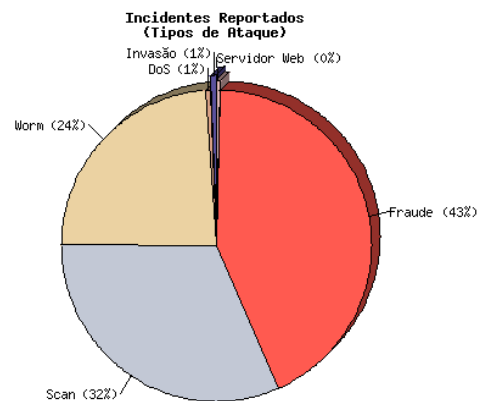
2005



Meeting for CSIRTs with National Responsibility - July 2006

## Incidents Reported to CERT.br (cont)

2006 (1<sup>st</sup> quarter)



Meeting for CSIRTs with National Responsibility - July 2006

## Characteristics of the Frauds Reported

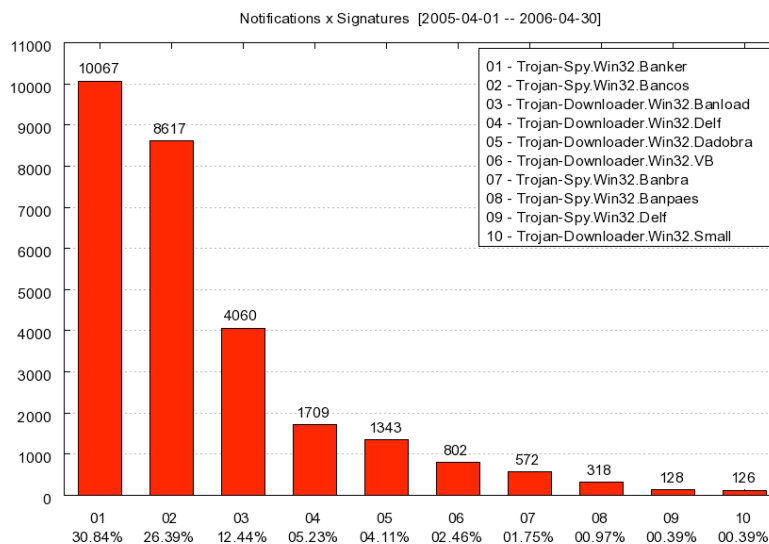
- In Brazil fraud is almost all based on malicious codes disseminated through social engineering
- Vast majority based on spam containing links to trojan horses or trojan downloaders
- Traditional phishing and DNS compromises are rarely seen (very common in 2002/2003)

Meeting for CSIRTs with National Responsibility - July 2006

## From April 1<sup>st</sup>, 2005 to April 30<sup>th</sup>, 2006

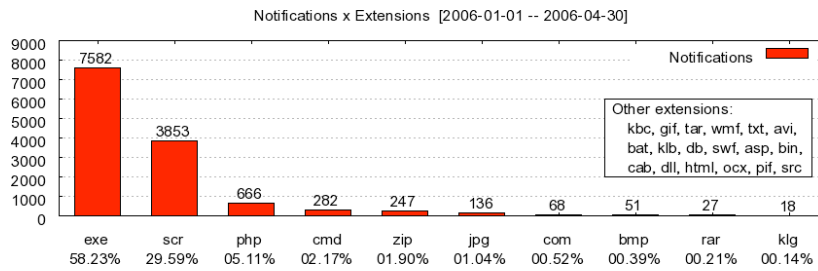
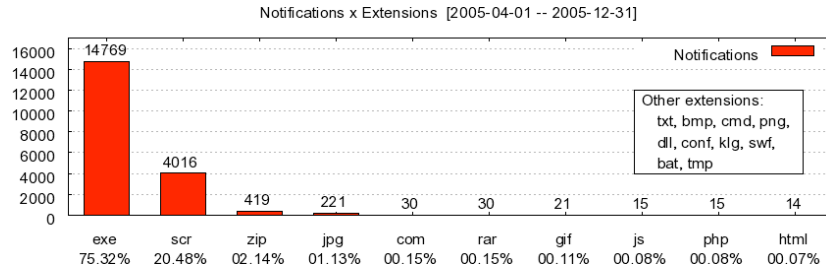
Category	Total
Unique domains hosting trojans	3807
Unique domain contact information	1782
Number of file extensions used	45
Unique filenames used by the trojans	9520
Unique hostnames	6137
Unique IP addresses	3166
Countries that the IPs were allocated to	68
Notifications sent by CERT.br	15556
Unique URLs found in the period	24005
Unique antivirus signatures found	1546

## More Common Anti-Virus Signatures



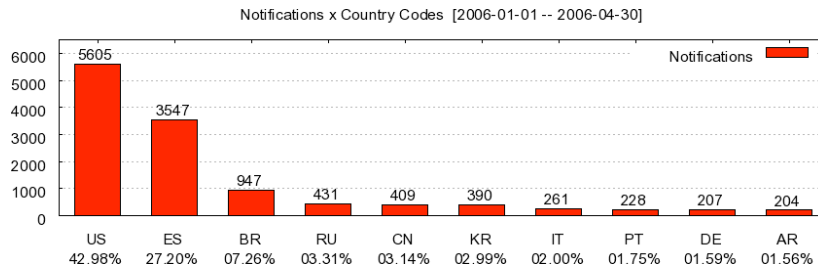
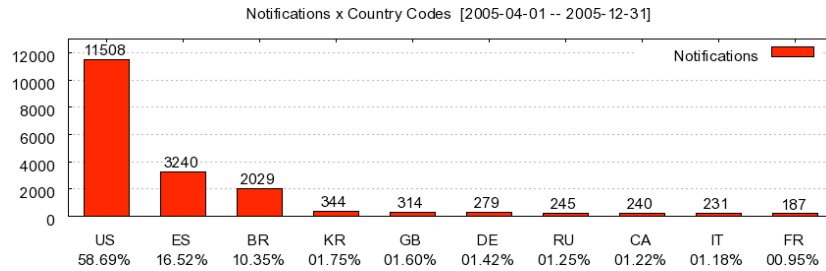
Signature's information source: Kaspersky Lab.

## Top 10 File Extensions



Meeting for CSIRTs with National Responsibility - July 2006

## Top 10 Country Codes



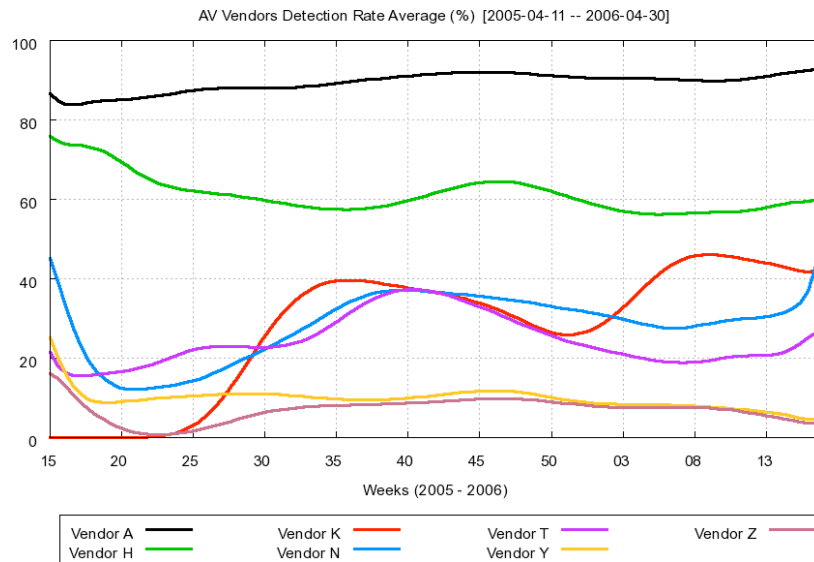
Meeting for CSIRTs with National Responsibility - July 2006

### Anti-Virus Efficiency: April/2005 to April/2006

Anti-Virus Vendor	Samples Tested	Samples not Detected	Samples Detected	Detection Rate (%)
Vendor A	18634	1913	16721	89,73
Vendor B	5653	1020	4633	81,96
Vendor D	18519	5475	13044	70,44
Vendor E	18652	6240	12412	66,55
Vendor F	18665	6857	11808	63,26
Vendor G	18348	6750	11598	63,21
Vendor H	18666	7324	11342	60,76
Vendor I	7474	3160	4314	57,72
Vendor K	14603	8873	5730	39,24
Vendor L	18658	11623	7035	37,71
Vendor N	18371	12866	5505	29,97
Vendor O	18606	13084	5522	29,68
Vendor P	14126	10162	3964	28,06
Vendor Q	18541	13395	5146	27,75
Vendor T	18652	14140	4512	24,19
Vendor Y	18469	16713	1756	9,51
Vendor Z	15784	14517	1267	8,03

Meeting for CSIRTs with National Responsibility - July 2006

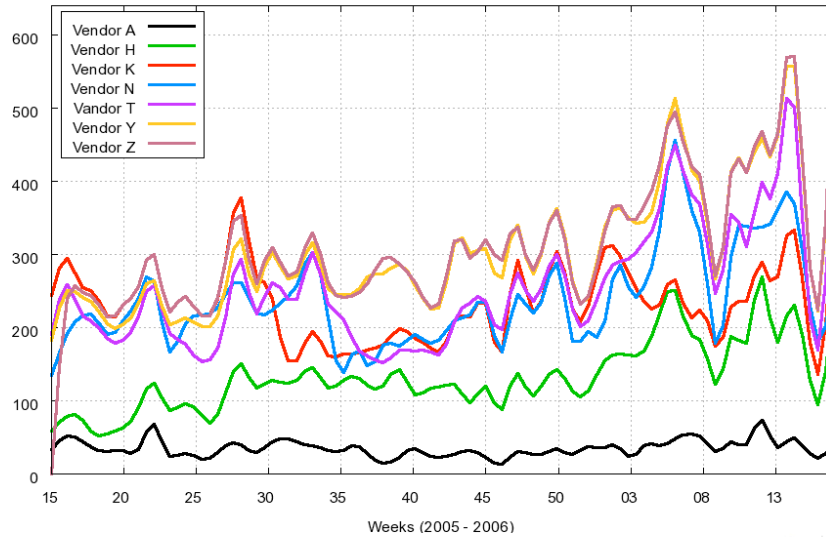
### Anti-Virus Vendors Detection Rate



Meeting for CSIRTs with National Responsibility - July 2006

## Trojan Samples Sent to the Anti-Virus Vendors

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



Meeting for CSIRTs with National Responsibility - July 2006

## Response and Interactions Between the Several Sectors

Meeting for CSIRTs with National Responsibility - July 2006

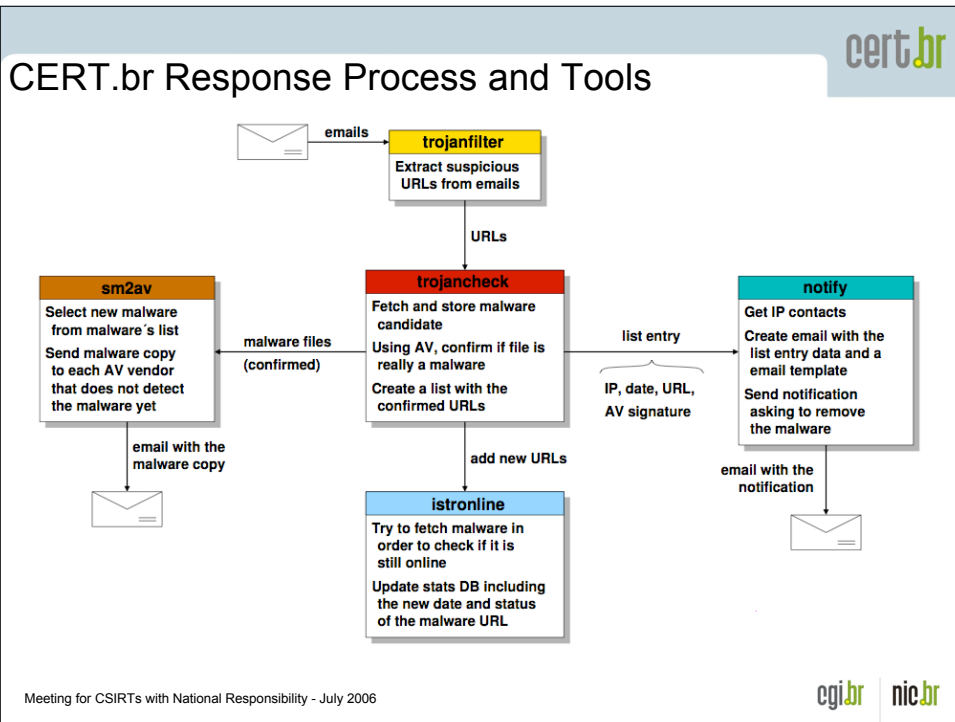


## Anti-Fraud Activities

- CERT.br and Financial Institutions' task force:
  - Share technical details about crimeware, new social engineering techniques, malicious codes, etc
  - Discuss incident management
  - Share new trends and technical information related to fraud
- Interaction with Law Enforcement
  - CERT.br
    - Provide training and technical guidance as needed/requested
    - Help victims and banks to interact with the right law enforcement authority
  - Financial Institutions
    - Coordinate efforts with the proper law enforcement agency for each case
    - Preserve clients' machines evidences

## Anti-Fraud Activities (cont)

- 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 24+ anti-virus vendors
    - Send new trojans to artifact analysis groups
  - Anti-Phishing Working Group (APWG) Research Partner  
<http://www.antiphishing.org/>



**cert.br**

# Educating the End User

Educating the End User

Meeting for CSIRTs with National Responsibility - July 2006

**cgi.br | nic.br**

## CGI.br Indicators

### National survey conducted by CGI.br in August 2005

- Is the Brazilian official survey on the use information and communication technologies in Brazil
- The survey included the following areas related to security and abuse:
  - **ICT Households:** security problems encountered, security measures adopted, antivirus updating frequency, frequency they receive spam, time spent with spam, etc.
    - F - Security
    - J - Spam
  - **ICT Enterprises:** identified IT security problems, security measures adopted, antivirus updating frequency, technologies adopted for secure communication, etc.
    - E - Security

## ICT Households

### 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

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

cgi.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.  
[Sabe mais](#)

Copyright  
Contato  
Agradecimentos  
Revisões

antisipam.br

Busca

Meeting for CSIRTs with National Responsibility - July 2006

cgi.br nic.br

# Best Practices for Internet Users - Tips

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

cgi.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)

Meeting for CSIRTs with National Responsibility - July 2006

cgi.br nic.br

## The antispam.br website

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

**O que é spam?**  
 Veja os conceitos de spam e de spam zombiões - que podem fazer com que você envie spam mesmo sem saber. Confira 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-mail, 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 comendo sério risco. Saiba o porquê.

Busca

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

cgibr.br nic.br registro.br cert.br

Meeting for CSIRTs with National Responsibility - July 2006

## Malicious codes and their relation to emails

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

**Tipos de spam**

**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 veem 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 disfarçada, 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.
- Screenshotter:** 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 o mouse e o clique.
- 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.

Busca

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

cgibr.br nic.br registro.br cert.br

Meeting for CSIRTs with National Responsibility - July 2006

## Frauds that come through emails



Antispam.br ::

http://www.antispam.br/tipos/fraudes/

Comitê Gestor da Internet no Brasil

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

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br



- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boss práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos
- Mapa do site

Busca

NIC.br Antispam.br  
CERT.br Registro

### Tipos de spam

**A Botar**

#### 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 número de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários da 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)**

Um dos fatos marcantes na história do spam tem sido sua utilização para disseminação de golpes. Os antigos, já praticados por meio de cartas ou ligações telefônicas, migraram para a Internet, propagados via spam. Um exemplo é o Golpe da Nigéria, também conhecido como golpe do 419 ou do 171, os famosos "contos do vigário".

Meeting for CSIRTs with National Responsibility - July 2006




## Tips to prevent spam and security problems



Antispam.br ::

http://www.antispam.br/dicas/

Comitê Gestor da Internet no Brasil

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

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br



- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boss práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos
- Mapa do site

Busca

NIC.br Antispam.br  
CERT.br Registro

### 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 útil: informe seus endereços de e-mail em cadastros, sites de relacionamentos etc.
- Tenha e-mails diferentes para uso pessoal, trabalho, compras online 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 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 conteúdos, 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 "cliqueador compulsivo". Não execute arquivos anexados em e-mails sem examiná-los previamente com antivírus, bem como, não clique em URLs incluídas em e-mails.
- Procure informações sobre os recursos técnicos do seu software anti-spam. Configure as listas negras e listas brancas. Monitore a quarentena, se for o caso.



Meeting for CSIRTs with National Responsibility - July 2006