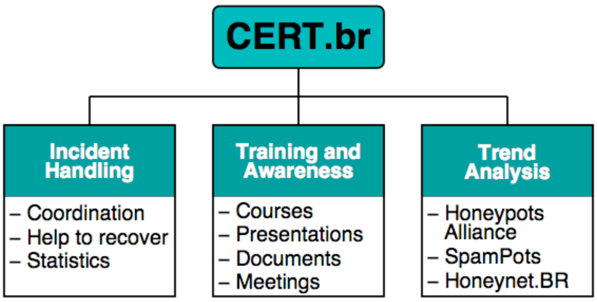
Challenges and Best Practices in Fighting Financial Fraud in Brazil

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 as a national focal point to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.



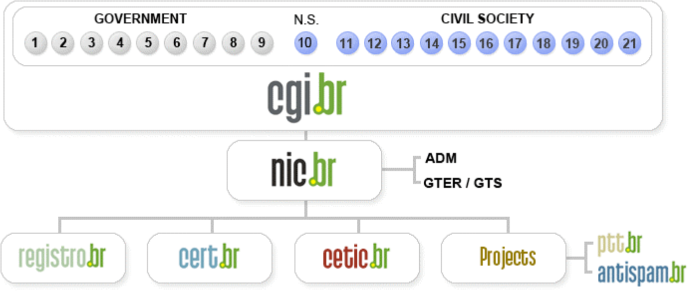
CERT.br

Incident Handling
- Coordination
- Help to recover
- Statistics

Training and Awareness
- Courses
- Presentations
- Documents
- Meetings

Trend Analysis
- Honeypots Alliance
- SpamPots
- Honeynet.BR

Brazilian Internet Steering Committee (CGI.br) Structure



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

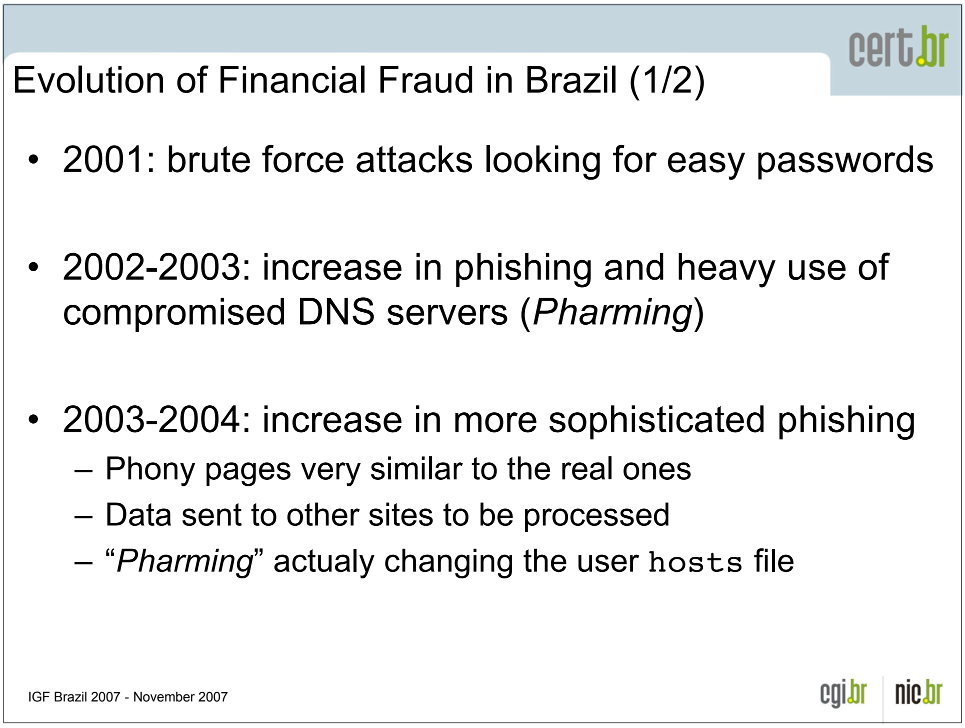
antispam.br

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

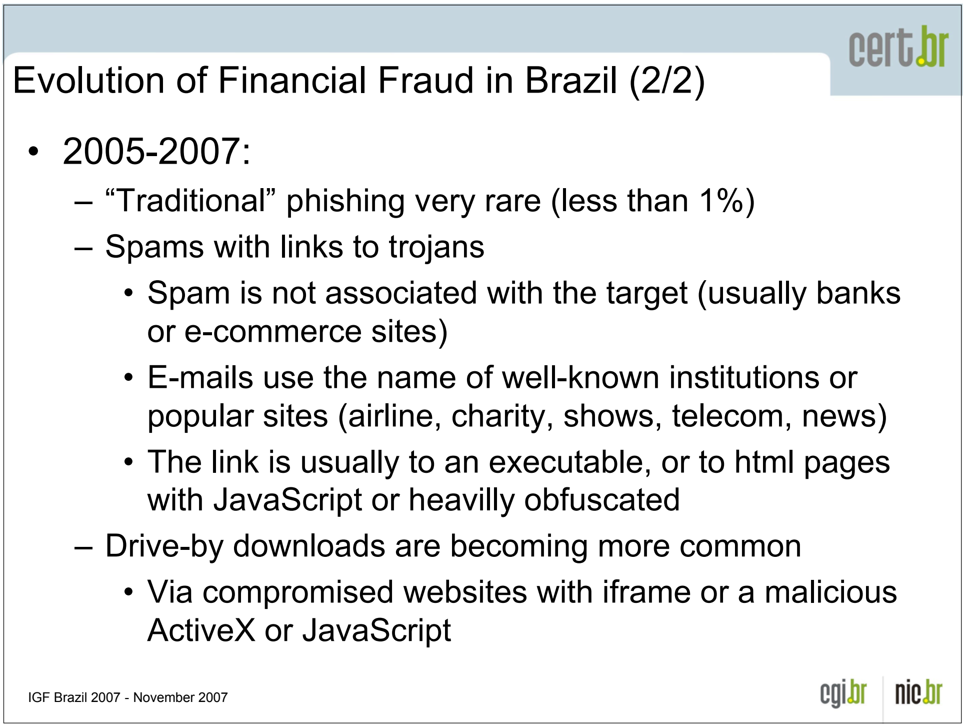
Agenda

- Evolution of financial fraud in Brazil
- Cooperation
- User awareness initiatives



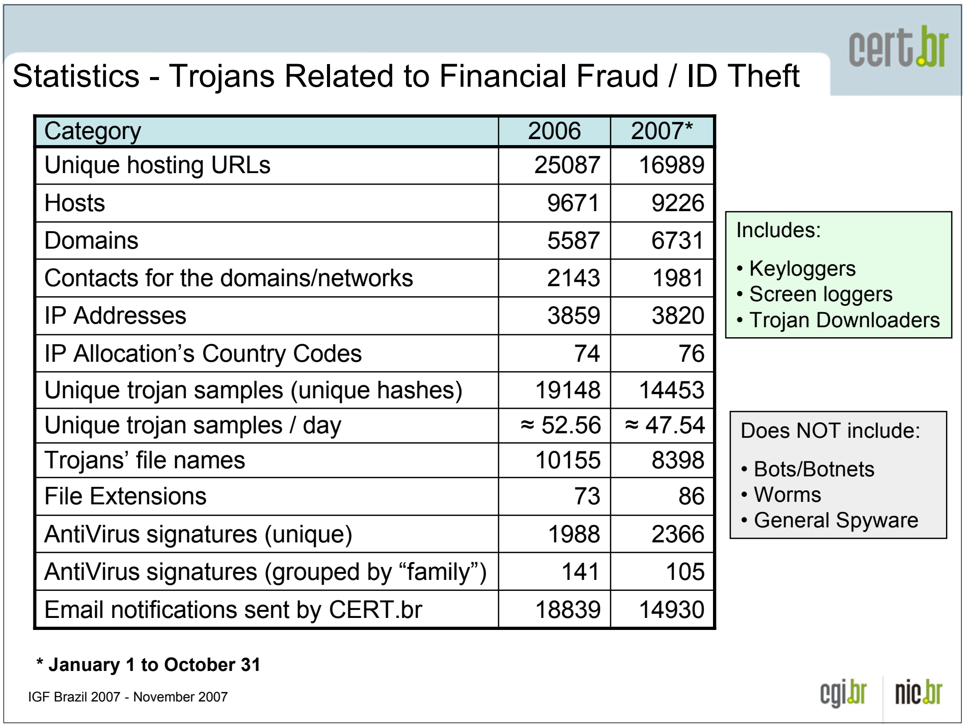
Evolution of Financial Fraud in Brazil (1/2)

- 2001: brute force attacks looking for easy passwords
- 2002-2003: increase in phishing and heavy use of compromised DNS servers (*Pharming*)
- 2003-2004: increase in more sophisticated phishing
  - Phony pages very similar to the real ones
  - Data sent to other sites to be processed
  - "*Pharming*" actualy changing the user `hosts` file



Evolution of Financial Fraud in Brazil (2/2)

- 2005-2007:
  - "Traditional" phishing very rare (less than 1%)
  - Spams with links to trojans
    - Spam is not associated with the target (usually banks or e-commerce sites)
    - E-mails use the name of well-known institutions or popular sites (airline, charity, shows, telecom, news)
    - The link is usually to an executable, or to html pages with JavaScript or heavilly obfuscated
  - Drive-by downloads are becoming more common
    - Via compromised websites with iframe or a malicious ActiveX or JavaScript



Statistics - Trojans Related to Financial Fraud / ID Theft

Category	2006	2007*
Unique hosting URLs	25087	16989
Hosts	9671	9226
Domains	5587	6731
Contacts for the domains/networks	2143	1981
IP Addresses	3859	3820
IP Allocation’s Country Codes	74	76
Unique trojan samples (unique hashes)	19148	14453
Unique trojan samples / day	≈ 52.56	≈ 47.54
Trojans’ file names	10155	8398
File Extensions	73	86
AntiVirus signatures (unique)	1988	2366
AntiVirus signatures (grouped by “family”)	141	105
Email notifications sent by CERT.br	18839	14930

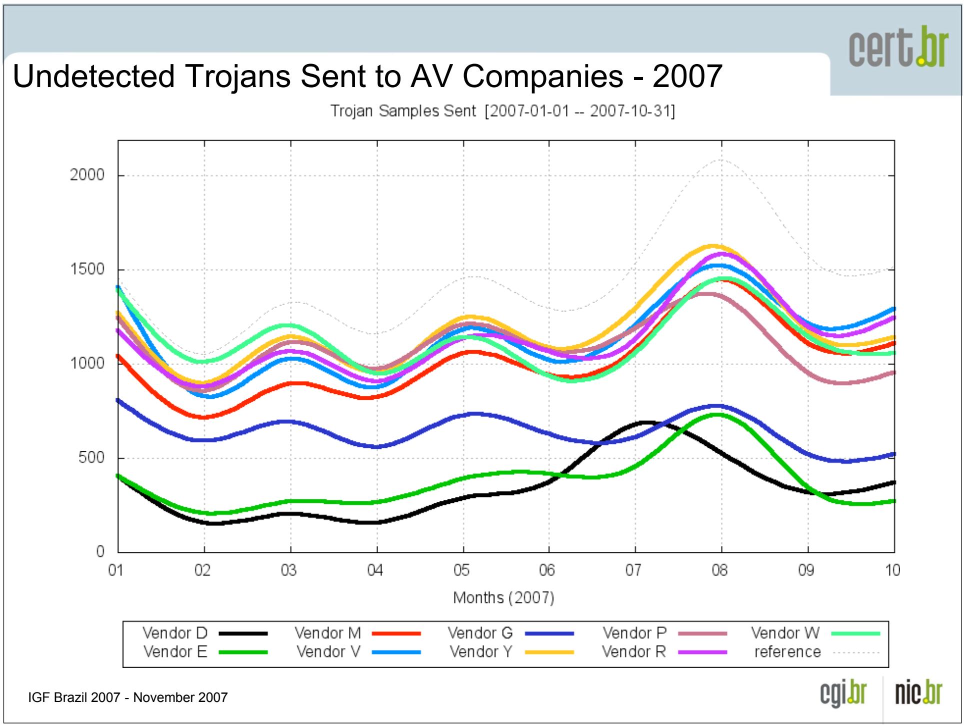
Includes:

- Keyloggers
- Screen loggers
- Trojan Downloaders

Does NOT include:

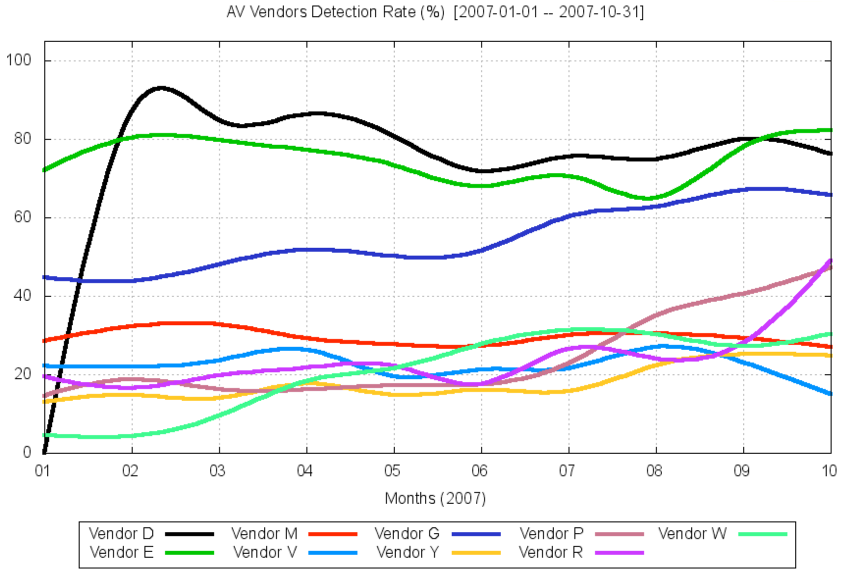
- Bots/Botnets
- Worms
- General Spyware

*** January 1 to October 31**



Undetected Trojans Sent to AV Companies - 2007

AV Detection Rate - 2007



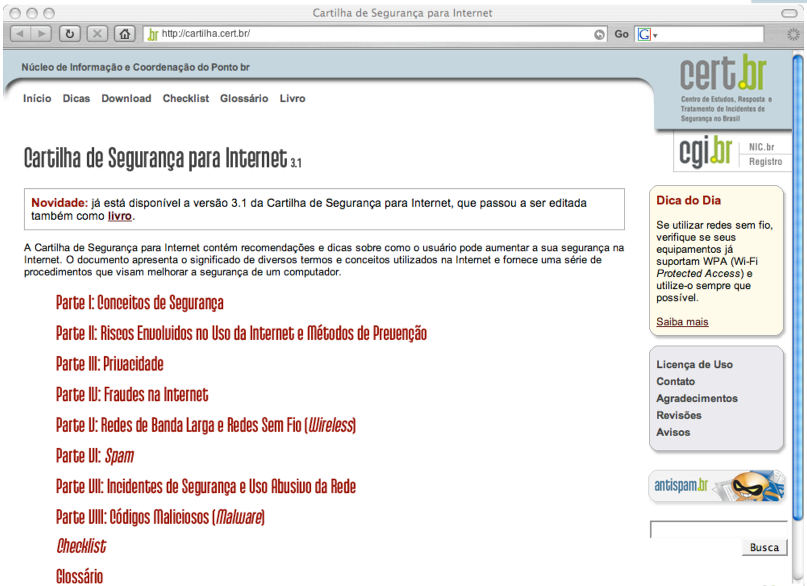
Cooperating to Fight the Problems (1/2)

- CERT.br focus:
  - Notify sites hosting malware related to frauds and phishing pages
    - Mostly in other countries
    - Other CSIRTs with National Resposibility are being of big help
  - Send undetected malware/trojans to 35+ antivirus vendors
  - Send new trojans to artifact analysis groups
  - Develop user awareness materials
    - Risks, threats, early signs of problems, basic tips, etc
    - Now in use by some banks in awareness campaigns
    - Used by major ISPs to inform their users

Cooperating to Fight the Problems (2/2)

- Regular meetings between CERT.br, financial sector and ISPs
  - Share new trends
  - Discuss best practices
    - CERT.br takes the discussions as input for the CGI.br task forces
  - Define strategies for
    - user awareness
    - spam/phishing detection and prevention

Site with Security Information for End Users


Cartilha de Segurança para Internet
http://cartilha.cert.br/
Go
Núcleo de Informação e Coordenação do Ponto br
Início Dicas Download Checklist Glossário Livro
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
NIC.br
Registro

Cartilha de Segurança para Internet 3.1

Novidade: já está disponível a versão 3.1 da Cartilha de Segurança para Internet, que passou a ser editada também como livro.

A Cartilha de Segurança para Internet contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet. O documento 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.

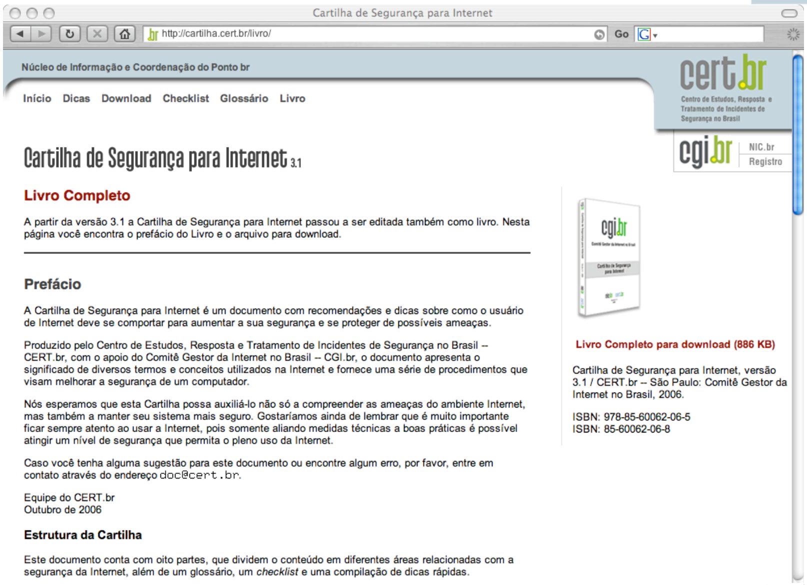
Parte I: Conceitos de Segurança
Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
Parte III: Privacidade
Parte IV: Fraudes na Internet
Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)
Parte VI: *Spam*
Parte VII: Incidentes de Segurança e Uso Abusivo da Rede
Parte VIII: Códigos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

Dica do Dia

Se utilizar redes sem fio, verifique se seus equipamentos já suportam WPA (Wi-Fi *Protected Access*) e utilize-o sempre que possível.

Saiba mais

Site with Security Information for End Users - Book


Cartilha de Segurança para Internet
http://cartilha.cert.br/livro/
Go
Núcleo de Informação e Coordenação do Ponto br
Início Dicas Download Checklist Glossário Livro
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
cgi.br
NIC.br
Registro

Cartilha de Segurança para Internet 3.1

Livro Completo

A partir da versão 3.1 a Cartilha de Segurança para Internet passou a ser editada também como livro. Nesta página você encontra o prefácio do Livro e o arquivo para download.

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.

Produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil -- CERT.br, com o apoio do Comitê Gestor da Internet no Brasil -- CGI.br, o documento 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.

Nós esperamos que esta Cartilha possa auxiliá-lo não só a compreender as ameaças do ambiente Internet, mas também a manter seu sistema mais seguro. Gostaríamos ainda de lembrar que é muito importante ficar sempre atento ao usar a Internet, pois somente aliando medidas técnicas a boas práticas é possível atingir um nível de segurança que permita o pleno uso da Internet.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, por favor, entre em contato através do endereço doc@cert.br.

Equipe do CERT.br
Outubro de 2006

Estrutura da Cartilha

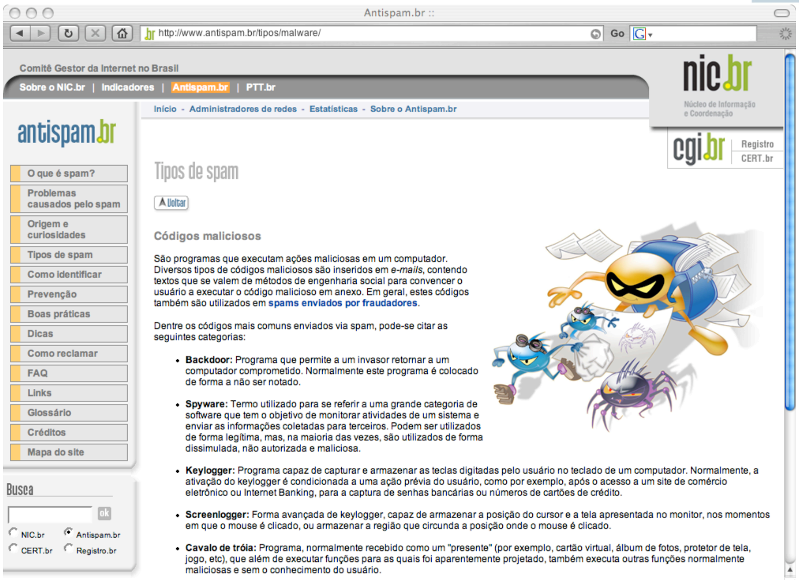
Este documento conta com oito partes, que dividem o conteúdo em diferentes áreas relacionadas com a segurança da Internet, além de um glossário, um *checklist* e uma compilação de dicas rápidas.

Livro Completo para download (886 KB)

Cartilha de Segurança para Internet, versão 3.1 / CERT.br -- São Paulo: Comitê Gestor da Internet no Brasil, 2006.

ISBN: 978-85-60062-06-5
ISBN: 85-60062-06-8

Antispam.br Website - Malicious Code Through E-mail


Antispam.br ::
http://www.antispam.br/tipos/malware/
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
nic.br
Núcleo de Informação e Coordenação
cgi.br
Registro
CERT.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
Voltar

Tipos de spam

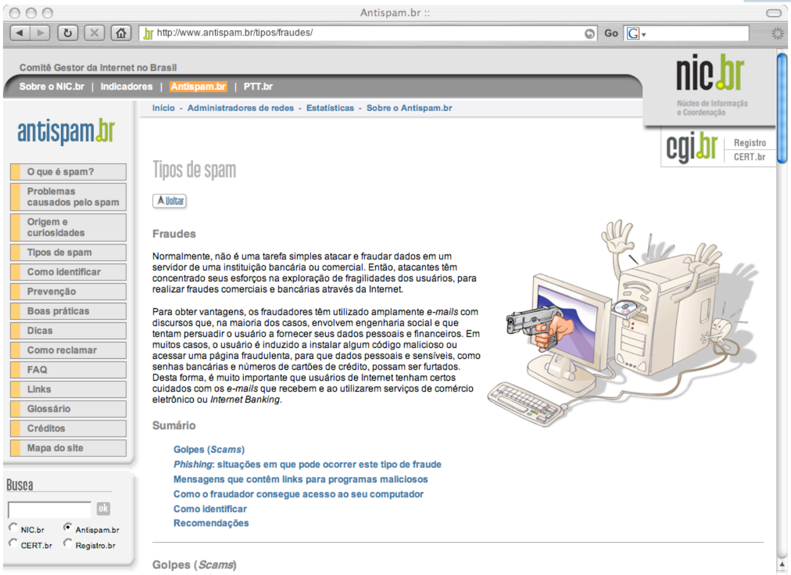
Códigos maliciosos

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em *e-mails*, contendo textos que se 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 Website - Fraud, Phishing, Scam, etc


Antispam.br ::
http://www.antispam.br/tipos/fraudes/
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
nic.br
Núcleo de Informação e Coordenação
cgi.br
Registro
CERT.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
Voltar

Tipos de spam

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

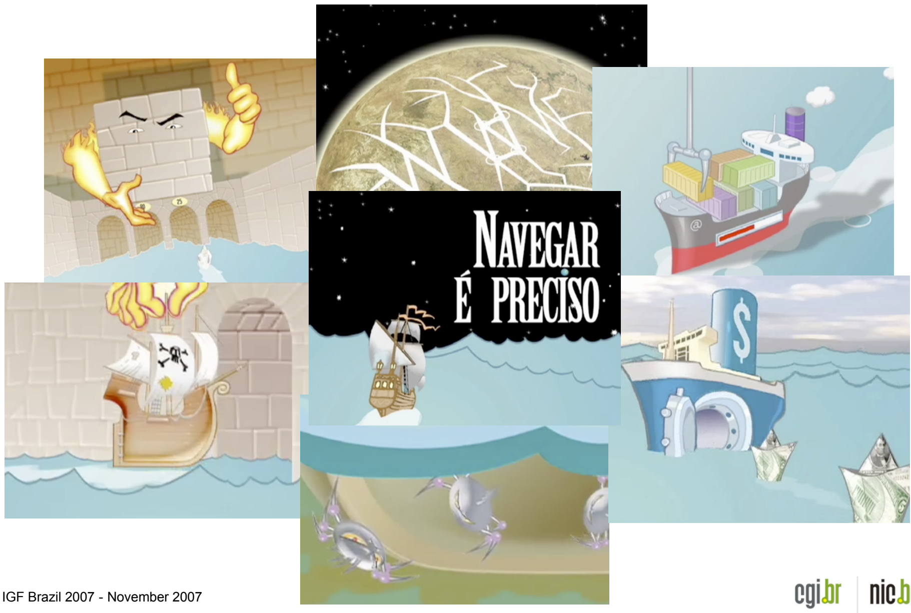
- Golpes (*Scams*)
- *Phishing*: situações em que pode ocorrer este tipo de fraude
- Mensagens que contêm links para programas maliciosos
- Como o fraudador consegue acesso ao seu computador
- Como identificar
- Recomendações

Golpes (*Scams*)

Other Initiatives

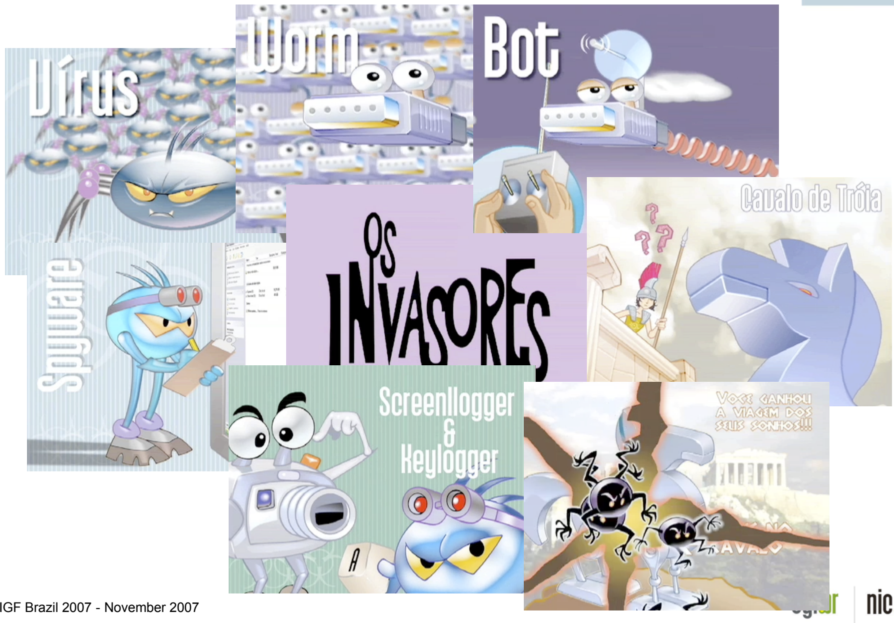
- Best practices are being translated to Spanish by ANTEL Uruguay Incident Response Team
- 4 videos
  - Navigating is Necessary
  - Invaders
  - Spam
  - Defense
- http://www.antispam.br/videos/

Video 1: Navigating is Necessary



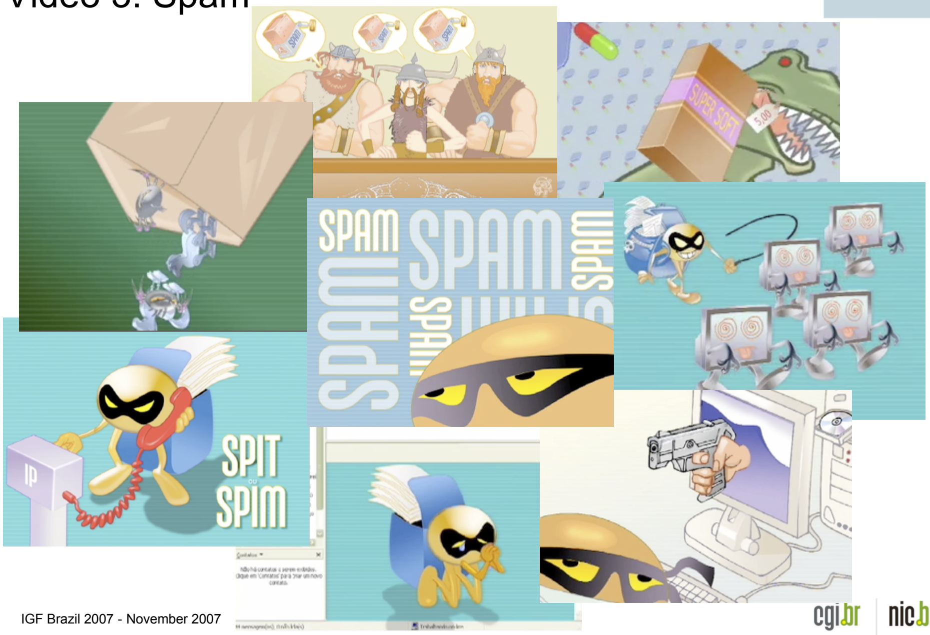
IGF Brazil 2007 - November 2007

Video 2: Invaders

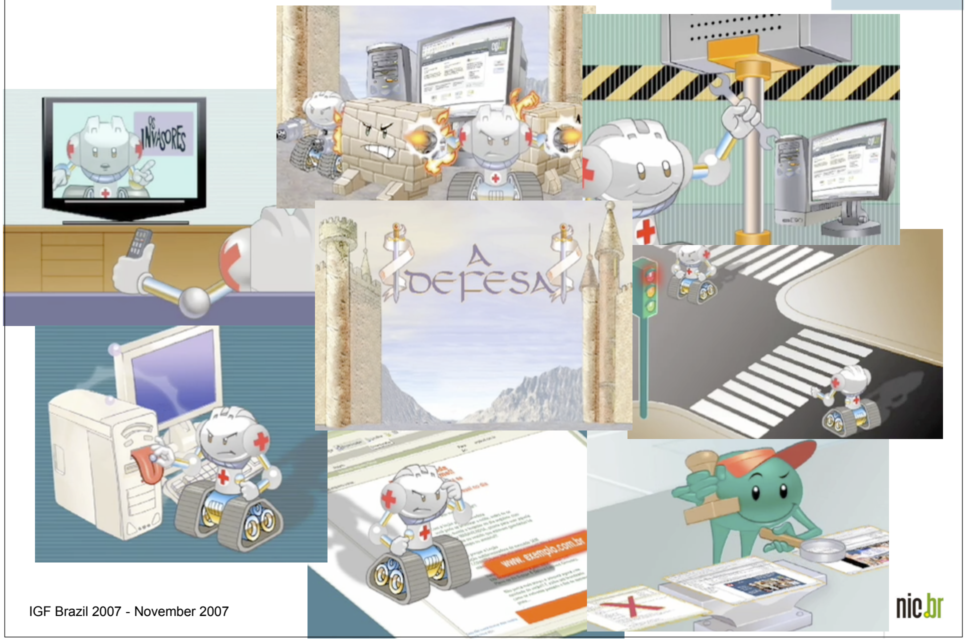


IGF Brazil 2007 - November 2007

Video 3: Spam



Video 4: Defense



Stickers

www.antispam.br
antispam.br

Additional References

- This presentation (next week)
  http://www.cert.br/docs/presentations/
- Awareness videos
  http://www.antispam.br/videos/
- CERT.br - Computer Emergency Response Team Brazil
  http://www.cert.br/
- NIC.br - Network Information Center Brazil
  http://www.nic.br/
- CGI.br - Brazilian Internet Steering Committee
  http://www.cgi.br/