Malware e Spam

Isledna Rodrigues

Roteiro

- Malware
- Spam

O QUE É UM MALWARE?

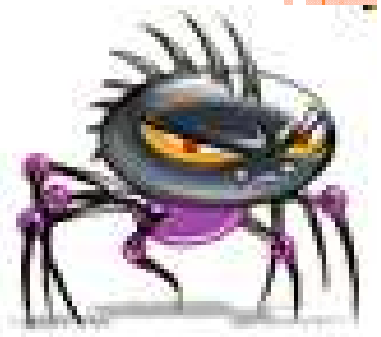
Malware (código malicioso) são programas desenvolvidos para executar ações danosas em computador.

Tipos de Malware

- Vírus
- Cavalos de Tróia
- Adware e Spywares
- Backdoors
- Keyloggers e Screenlogers
- Worms
- Bots
- Rootkits

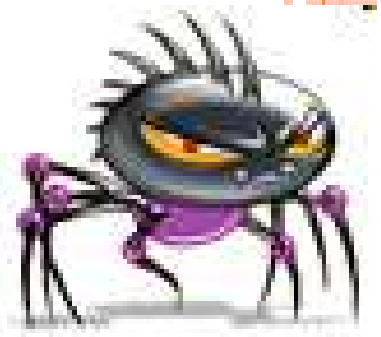
Vírus

- Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.
- Depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.



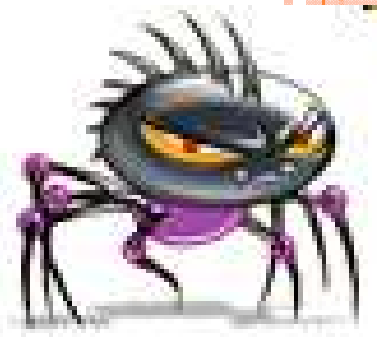
Como acontece a infecção por vírus?

- Abrindo arquivos anexados aos e-mails.
- Abrir arquivos do Word, Excel, etc.
- Abrir arquivos em outros computadores através de compartilhamento.
- Instalando programas de procedência duvidosa.
- Executando uma mídia removível infectada.



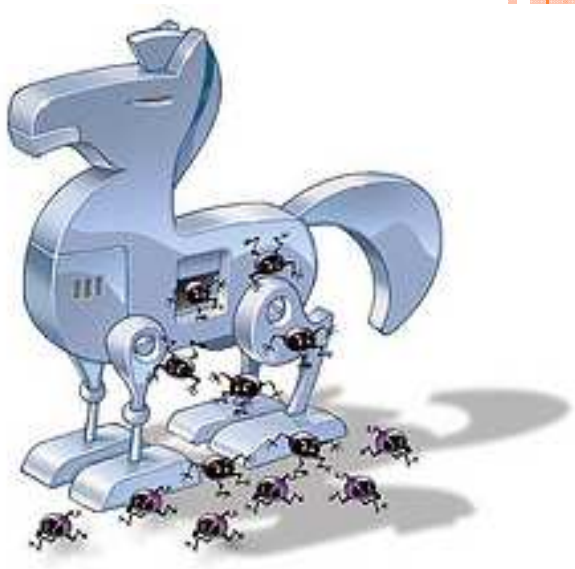
Ainda sobre vírus...

- Pode ficar inativo na máquina e só ser executado, por exemplo, quando uma data for alcançada.
- *E-mail borne vírus* são vírus propagados por e-mail mas que só infectam ou se propagam se o arquivo for executado.
- Vírus de macro (automatizam tarefas repetitivas) pode ser executados se o arquivo que possui essas macros for executado.
- *Vírus de celular* que podem se propagar pela tecnologia bluetooth ou MMS.



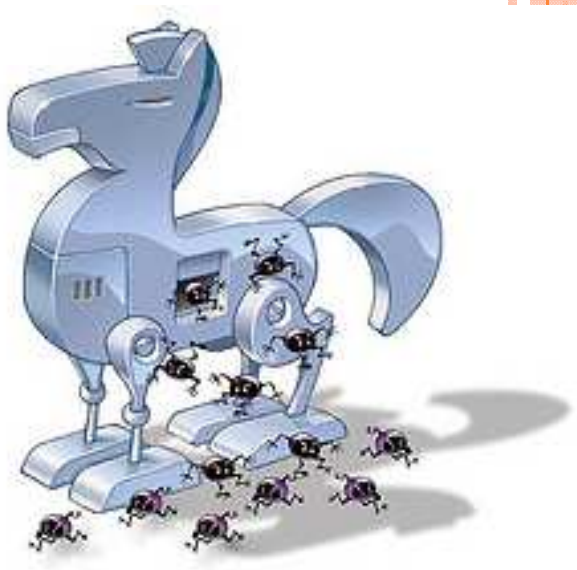
Cavalos de Tróia

- Trojan Horse
- programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc).
- Além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.



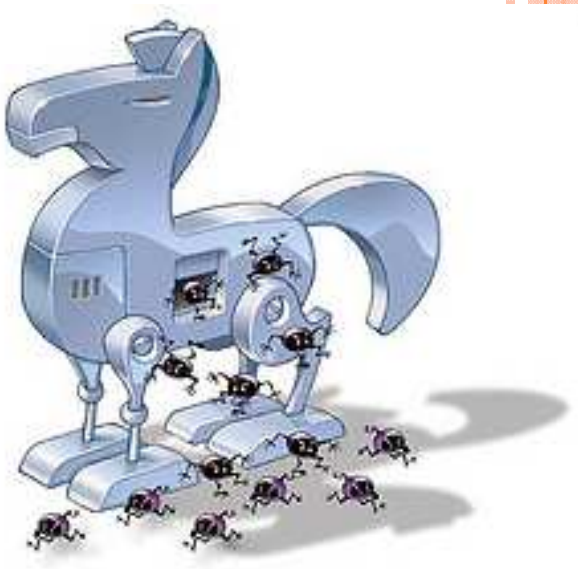
Cavalos de Tróia

- Instalação de *keyloggers* ou *screenloggers*.
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de *backdoors*.
- Alteração ou destruição de arquivos.



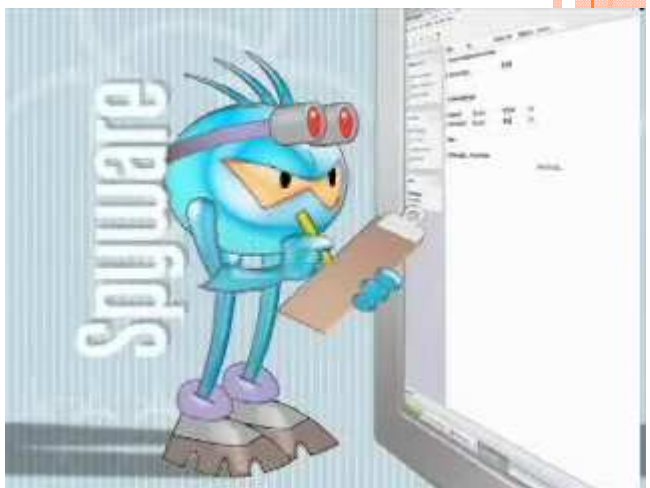
Cavalos de Tróia x Vírus

- Não infecta outros arquivos.
- Não propaga cópias de si mesmo automaticamente.
- Precisa ser explicitamente executado.
- Um cavalo de tróia pode conter um vírus ou *worm*.



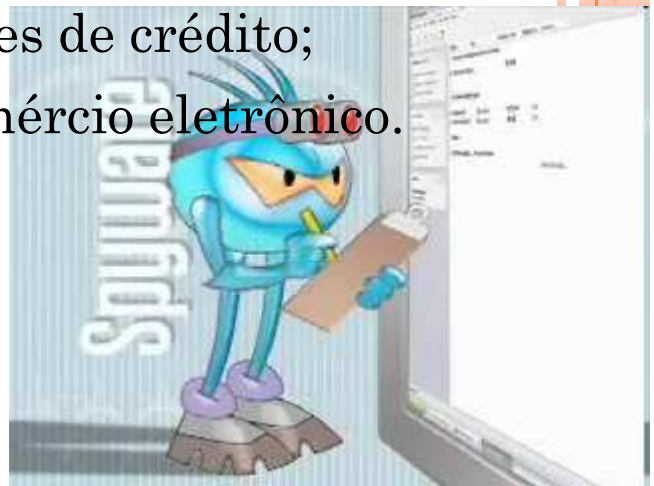
Adware e Spyware

- Adware (Advertising software) software projetado para apresentar propagandas, seja através de um browser, seja através de algum outro programa instalado em um computador.
  - Ex: MSN usa de forma legítima adwares.
- Spyware tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros



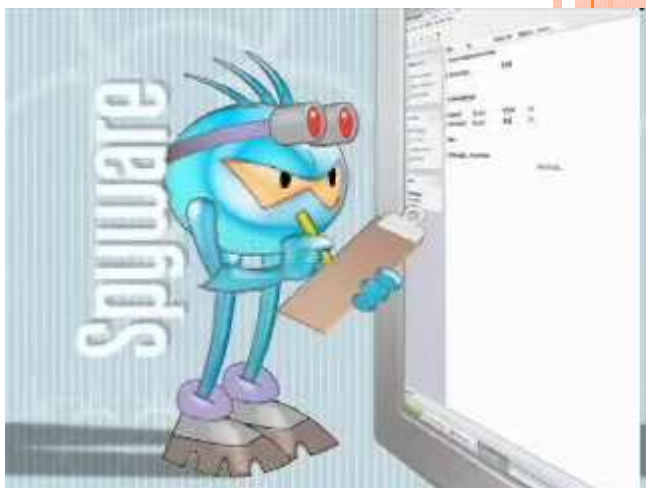
Adware e Spyware

- O que podem fazer?
  - monitoramento de URLs acessadas enquanto o usuário navega na Internet;
  - alteração da página inicial apresentada no browser do usuário;
  - varredura dos arquivos armazenados no disco rígido do computador;
  - monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;
  - instalação de outros programas spyware;
  - monitoramento de teclas digitadas pelo usuário ou regiões da tela.
  - captura de senhas bancárias e números de cartões de crédito;
  - captura de outras senhas usadas em sites de comércio eletrônico.



Adware e Spyware

- Podem ser usados de forma legítima mas na maioria das vezes são utilizados de forma dissimulada, não autorizada e maliciosa.

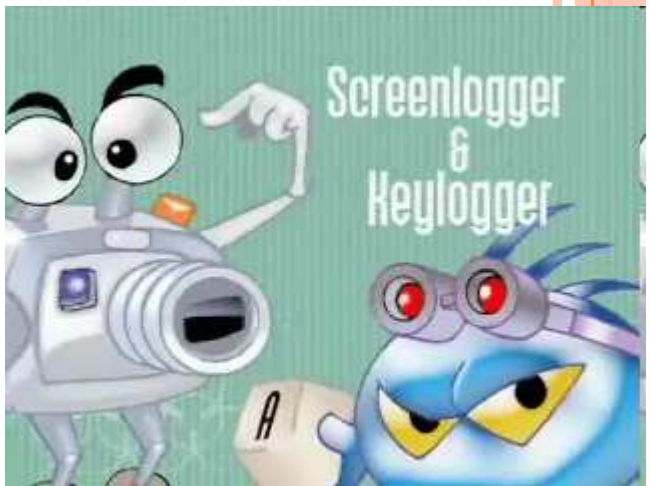


Backdoors

- São programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim.
- O BackOrifice e NetBus são exemplos de programas que podem ser usados na administração remota.

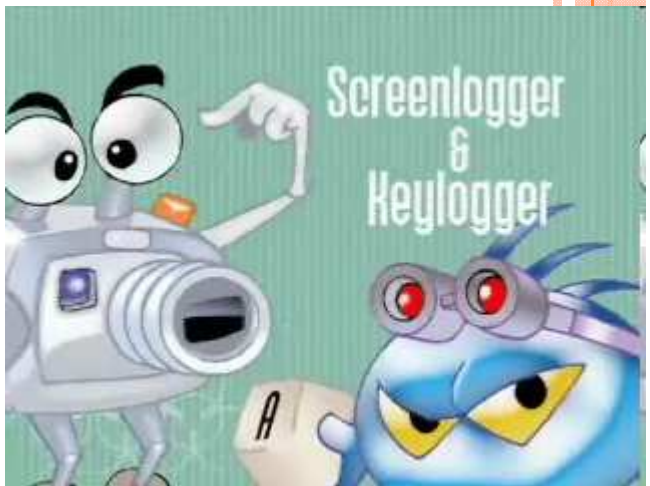
KEYLOGGERS

- É um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.
- Emails, senhas, endereços, telefones, etc.
- Instituições financeiras desenvolveram os teclados virtuais.
- Normalmente vem com um programa spyware ou cavalo de tróia.



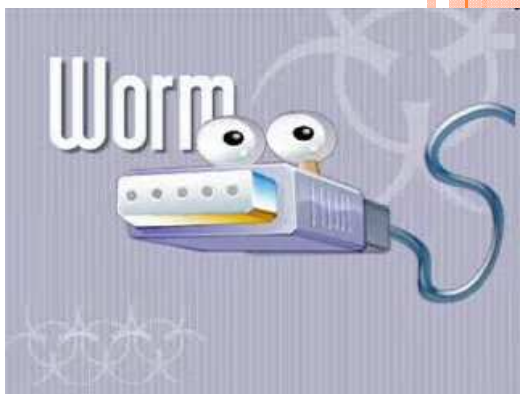
Screenlogger

- Forma mais avançadas de keyloggers, capazes:
  - 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.



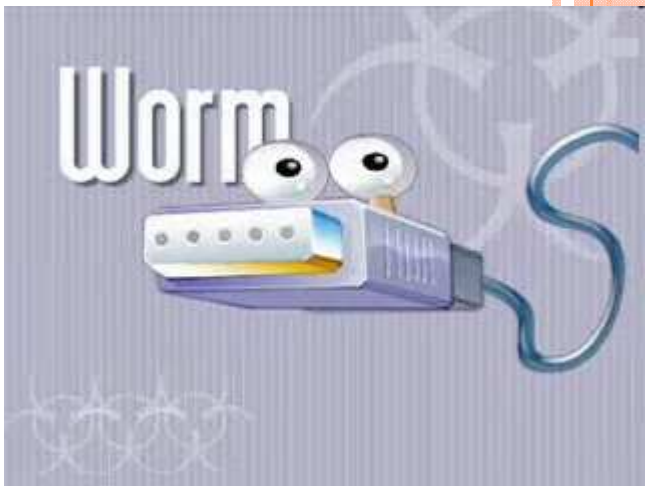
Worms

- Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.
- Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos.
- Não necessita ser explicitamente executado para se propagar.
- Propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de software instalados em computadores.



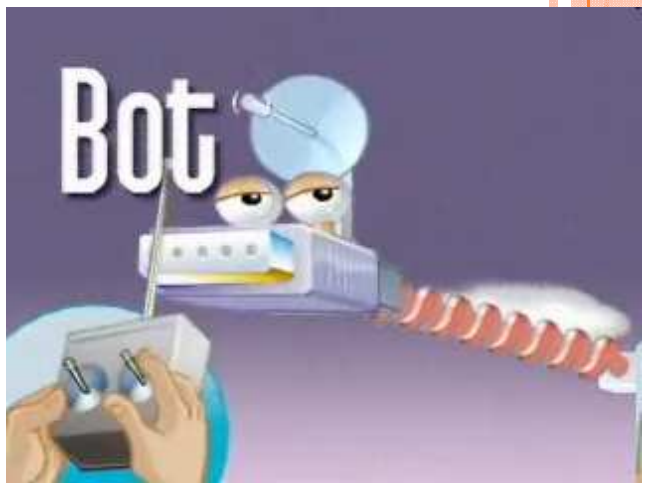
Como um worm pode afetar o computador?

- Mesmos danos gerados pelo vírus.
- Consumindo muitos recursos do computador por ficar propagando cópias.
- Anti-vírus + programas atualizados + firewall



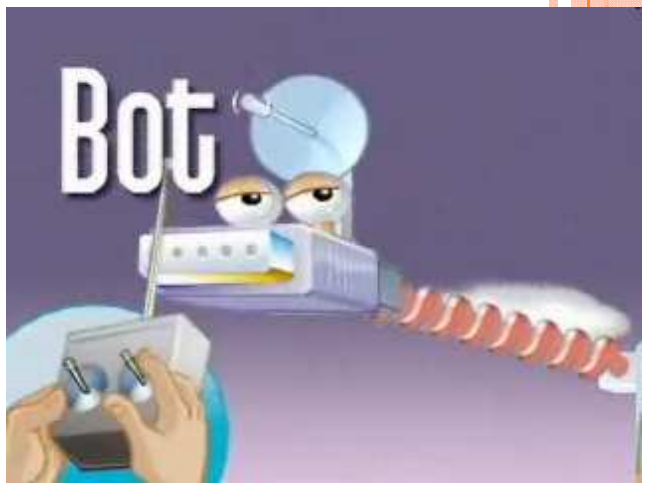
Bots

- É um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.
- Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente.



O que o invasor pode fazer através do Bot?

- desferir ataques na Internet;
- executar um ataque de negação de serviço;
- furtar dados do computador onde está sendo executado, como por exemplo números de cartões de crédito;
- enviar e-mails de phishing;
- enviar spam.



Botnets

- São redes formadas por computadores infectados com bots.
- O invasor utiliza essas redes para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de e-mails de phishing ou spam, desferir ataques de negação de serviço, etc.
- Proteção através de manutenção constante dos programas utilizados.

Rootkits

- Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido através de um conjunto de programas.

Vídeo

- 1. Os Invasores

Spams

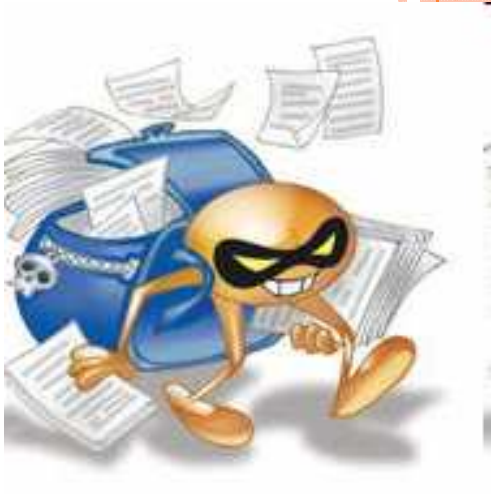
- É o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.
- Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês Unsolicited Commercial E-mail).

Problemas para os usuários...

- Não recebimento de e-mails.
- Gasto desnecessário de tempo
- Aumento dos custos.
- Perda de produtividade.
- Conteúdo impróprio ou ofensivo.
- Prejuízos financeiros causados por fraudes.

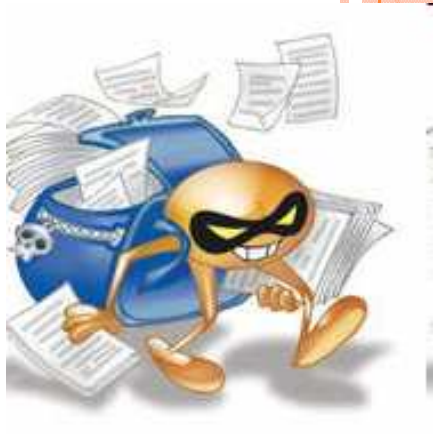
Problemas para os provedores...

- Impacto na banda
- Má utilização dos servidores
- Inclusão em listas de bloqueio
- Investimento em pessoal e equipamento.



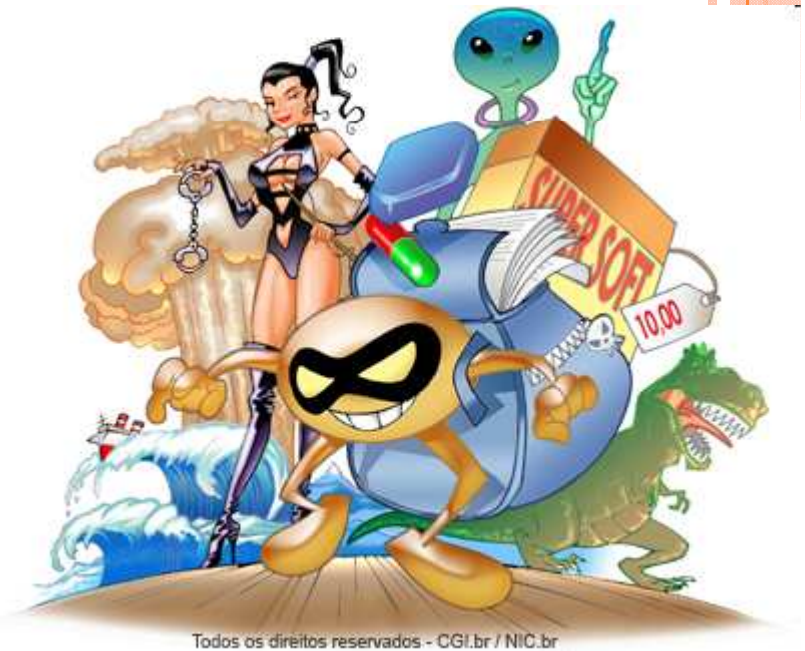
Como spammers conseguem e-mails?

- Compra de banco de dados com e-mails variados.
- Produção de sua própria lista via programas maliciosos.
- *Harvesting*:varrer páginas Web e arquivos de listas de discussão em busca de e-mails.



Tipos de Spam

- Correntes (chain letters)
- Boatos (hoaxes) e lendas urbanas
- Propagandas
- Ameaças, brincadeiras e difamação
- Pornografia
- Códigos maliciosos
- Fraudes
- Spit e spim (Spam via telefonia IP)
- Spam via redes de relacionamentos



Como se prevenir?

- Preservar as informações pessoais.
- Ter, sempre que possível, e-mails separados para assuntos pessoais, profissionais, para as compras e cadastros on-line.
- Não ser um "clicador compulsivo", ou seja, o usuário deve procurar controlar a curiosidade de verificar sempre a indicação de um site em um e-mail suspeito de spam.

Como se prevenir?

- Não ser um "caça-brindes", "papa-liquidações" ou "destruidor-de-promoções".
- Ter um filtro anti-spam instalado, ou ainda, usar os recursos anti-spam oferecidos pelo seu provedor de acesso.
- Além do anti-spam, existem outras ferramentas bastante importantes para o usuário da rede: anti-spyware, firewall pessoal e antivírus.

Em resumo a solução é...

- Anti-Vírus Atualizado
- Anti-Spyware Atualizado
- Firewall bem configurado
- Atualização contínua de patches dos programas utilizados.

Vídeo

- 2. Spam
- 3. A Defesa

Atividade

Escolha um aparato de software e rotinas que vocês selecionariam para resolver problemas com Spams e Malwares em uma organização. Justifique a adoção de cada ferramenta escolhida e se preparem para defender suas escolhas na próxima aula.

Referências

- Cartilha de segurança para Internet. Versão 3.1. Comitê Gestor da Internet no Brasil.
- http://www.antispam.br/
- http://www.cert.br/