



Sistemas Operacionais

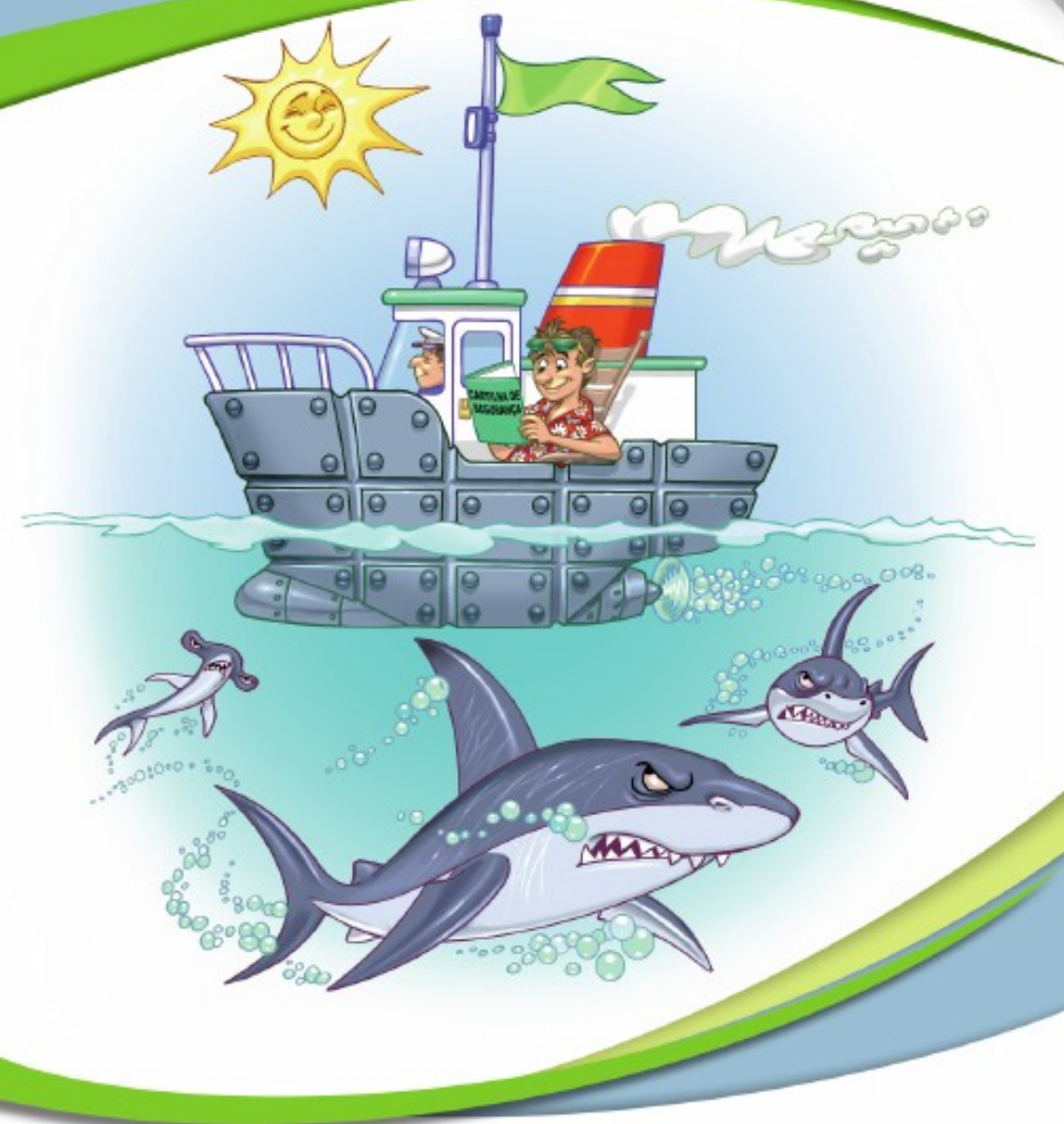
Prof. Wandelson Ferreira

Das aulas anteriores..

- Golpes na Internet
- Ataques na Internet

Cartilha de Segurança para Internet

Publicação
cert.br



<http://cartilha.cert.br/>

nie.br

cgi.br

Malwares

- Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:
 - pela exploração de vulnerabilidades existentes nos programas instalados;
 - pela auto-execução de mídias removíveis infectadas, como pen-drives;
 - pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;

Malwares

- Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:
 - pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
 - pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Malwares

- Principais motivos que levam um atacante a propagar códigos maliciosos:
 - Obtenção de vantagens financeiras
 - A coleta de informações confidenciais
 - O desejo de autopromoção
 - Vandalismo.

Malwares

- Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:
 - pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
 - pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Malwares

- **Malicious Software**
 - Vírus
 - Worms
 - Bot e BotNet
 - Spywares
 - Adware
 - Cavalos-de-Tróia
 - Bombas Lógicas
 - Backdoor
 - Rootkit

Vírus

- Programa malicioso
- O vírus se replica em arquivos do PC
- Precisa de um hospedeiro para reprodução
- Se reproduz geralmente no mesmo PC
- Pode realizar diversas atividades
 - Desativar portas USB
 - Aumentar processamento
 - Usar memória RAM
 - Desabilitar firewall



Vírus

Tipos:

- Vírus propagado por e-mail
- Vírus de script
- Vírus de macro
- Vírus de telefone celular



Worm

- Capaz de se propagar automaticamente através da rede
- Não precisa de outros programas para se replicar e propagar – se
- Sua replicação explora as vulnerabilidades
- Consume recursos e degrada o desempenho
- Capaz de gerar negação de serviço (DoS)



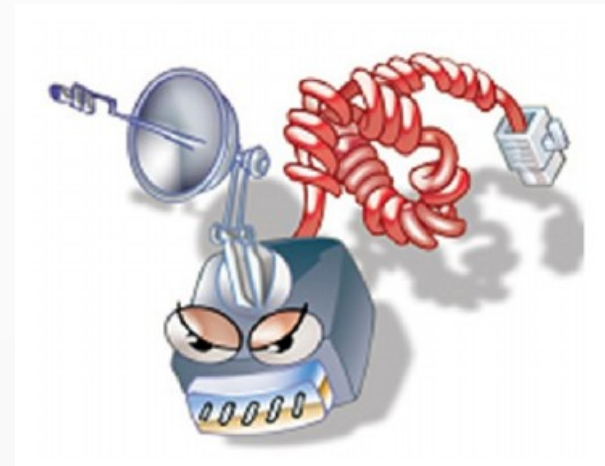
Worm

- Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.



Bot e botnet

- É capaz de se propagar automaticamente
- É um WORM controlado remotamente
- Uma rede infectada com bots é uma BotNet
- Promove DoS ou então facilita roubo de informações, envio de SPAM e outras atividades maliciosas



Trojan Horses

- Executa ações clandestinas
- Deve ser executado para entrar em ação
- Pode conter:
 - Vírus
 - Worm
 - Keylogger
 - Outros
- Não se propagam automaticamente



Spywares

- Violam a confidencialidade
- Monitoram atividades do sistema
- São capazes de enviar dados pela rede
- Há diversas utilidades, desde vigiar um companheiro até roubar dados de uma conta bancária e o dinheiro



Keyloggers

- Lêem os dados do teclado
- Podem ser em SW ou HW
- Os dados do teclado são salvos e enviados pela internet para o endereço da pessoa que o instalou e configurou.



Screenloggers

- Leem os dados da tela
- Capturam as telas quando o usuário do computador clica usando o mouse.
- São úteis para ver a senha no caso de um teclado virtual do internet banking
- Também podem enviar os dados por e-mail

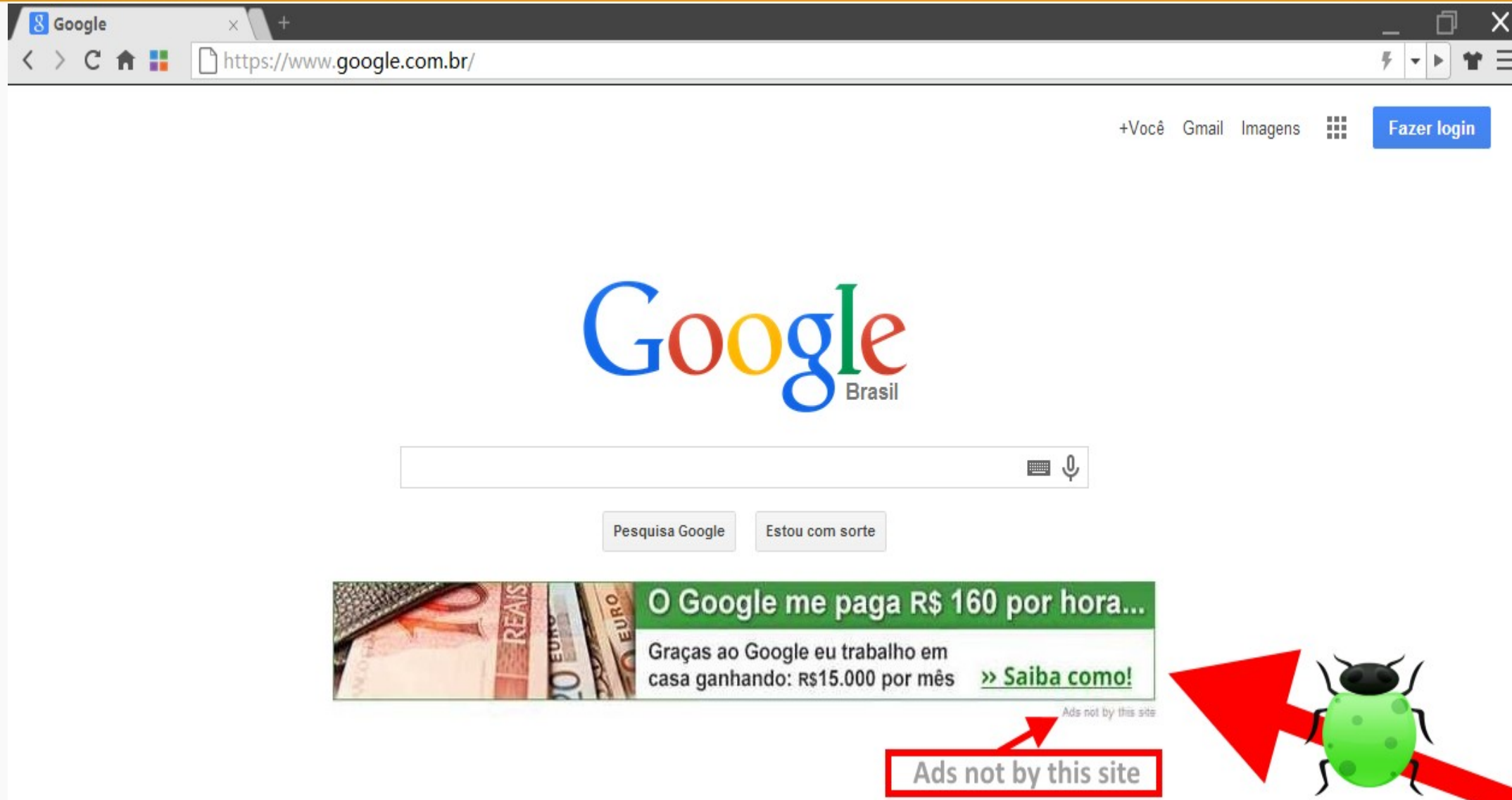


Adware

- Advertisement
- Tem a intenção de forçar a compra de um produto
- Se incorporam a softwares legítimos para parecerem corretos
- Podem executar programas maliciosos por trás



Adware



The image shows a screenshot of the Google Brazil homepage in a web browser. The browser's address bar displays `https://www.google.com.br/`. In the top right corner, there are links for '+Você', 'Gmail', 'Imagens', and a 'Fazer login' button. The Google logo with 'Brasil' underneath is centered on the page. Below the logo is a search bar with a keyboard and microphone icon to its right. Under the search bar are two buttons: 'Pesquisa Google' and 'Estou com sorte'.

An advertisement is displayed below the search area. It features a background image of Brazilian and European banknotes. The headline reads 'O Google me paga R\$ 160 por hora...'. The body text says 'Graças ao Google eu trabalho em casa ganhando: R\$15.000 por mês' followed by a link '>> Saiba como!'. Below the ad, the text 'Ads not by this site' is visible in small font.

Two red annotations are present: a red arrow points from a red-bordered box containing the text 'Ads not by this site' to the small text below the ad; another red arrow points from a green ladybug icon to the same text.

Backdoor

- É uma brecha deixada propositalmente para que se possa voltar
ao computador previamente invadido
- Pode estar contida em um programa modificado
- Netbus e BackOrifice
- O computador não precisa ter sido invadido para ter
Um backdoor



Rootkit

- Programas para apagar os rastros de uma invasão
- É utilizado para manter o acesso privilegiado a uma máquina
- Ajuda o invasor a permanecer conectado à máquina invadida de maneira não- detectável



Spam

- Spam é um e-mail não solicitado
- Problemas causados por ele:
 - Perda de mensagens
 - Conteúdo ofensivo/pornográfico
 - Gasto de tempo
 - Impacto na banda
 - Investimento extra em recursos



Outros Riscos

- Cookies
- Janelas de Pop-up
- Plugins e extensões
- Links Patrocinados
- Banners de Propaganda
- P2P
- Compartilhamento de recursos



Prevenção

- Manter os programas nas versões mais recentes
- Mantenha os programas instalados com todas as atualizações aplicadas
- Use apenas programas originais
- Use mecanismos de proteção
- Use as configurações de segurança já disponíveis
- Seja cuidadoso ao manipular arquivos
- Crie um disco de recuperação de sistema