Segurança de Redes
Aula-1

Prof.: Fred Sauer

fsauer@gmail.com

Material Produzido por:

Prof. Túlio Alvarez – tulioalvarez@gmail.com

Programa de aulas

Aula 1

- Introdução
- Conceitos Básicos:
  - Confidencialidade, integridade e disponibilidade
  - Ameacas, vulnerabilidades, risco, impacto
  - Hackers/Crackers
  - Engenharia social
  - Códigos maliciosos
    - vírus
    - worms adware / spyware
    - keylogger/ screenlogger
    - cavalo de tróia (trojan horse)
    - backdoors
    - bots
    - Rootkits
    - hoax

Aula 2

- Tipos de Ataques
  - Sniffers
  - DOS/DDOS
  - Buffer overflow
  - Varredura de portas
  - Varredura de vulnerabilidades
  - Spoofing
  - Poisoning
  - Phishing
  - Man-in-the-middle
  - *defacement* (pichação)
  - SQL *injection* e *cross-site scripting*
  - exploits
  - *honeynets* e *honeypots*

Aula 3

- Hardening
- Controle de acesso
  - RADIUS / TACACS
- Firewall/Proxy
  - Tipos
  - DMZ
  - Bastian host
- NAT
- VPN
- IDS
- IPS

Sumário – Fundamentos de Seg Redes

- Introdução
- Conceitos Básicos de Segurança

Introdução: Segurança da Informação

- Normas ABNT

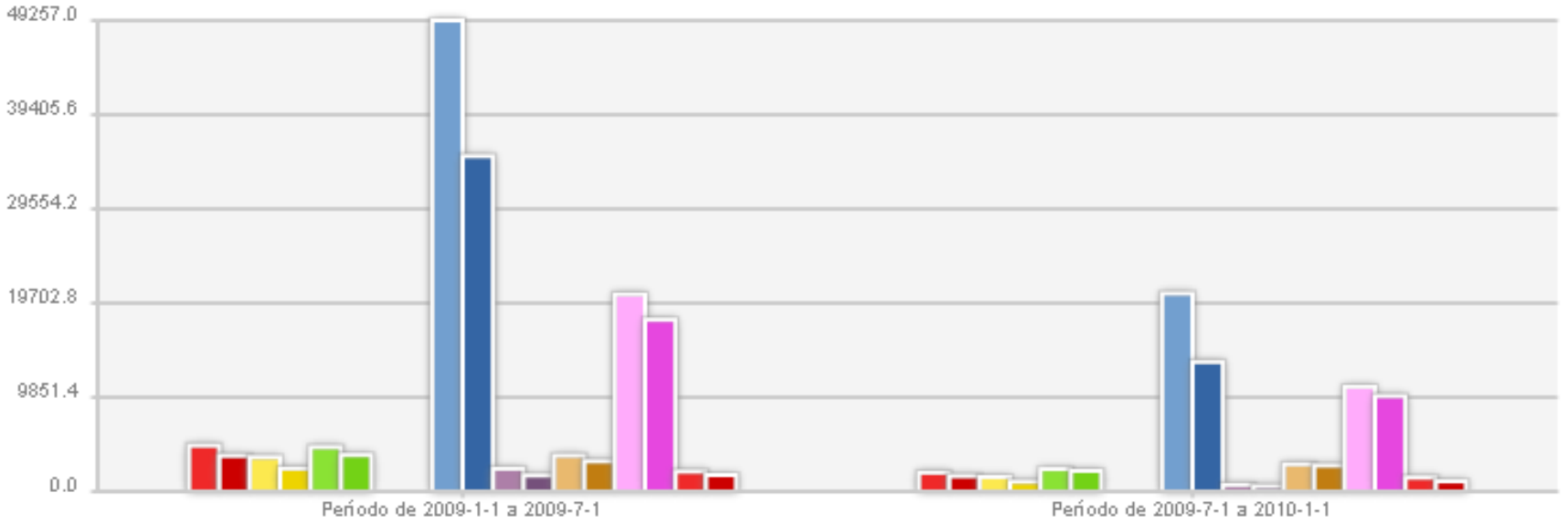
  - NBR ISO/IEC 27001/2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos

  - NBR ISO/IEC 27002/2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação (CONTEÚDO TÉCNICO IDÊNTICO AO DA ABNT NBR ISO/IEC 17799)

  - NBR ISO/IEC 27005/2008 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação

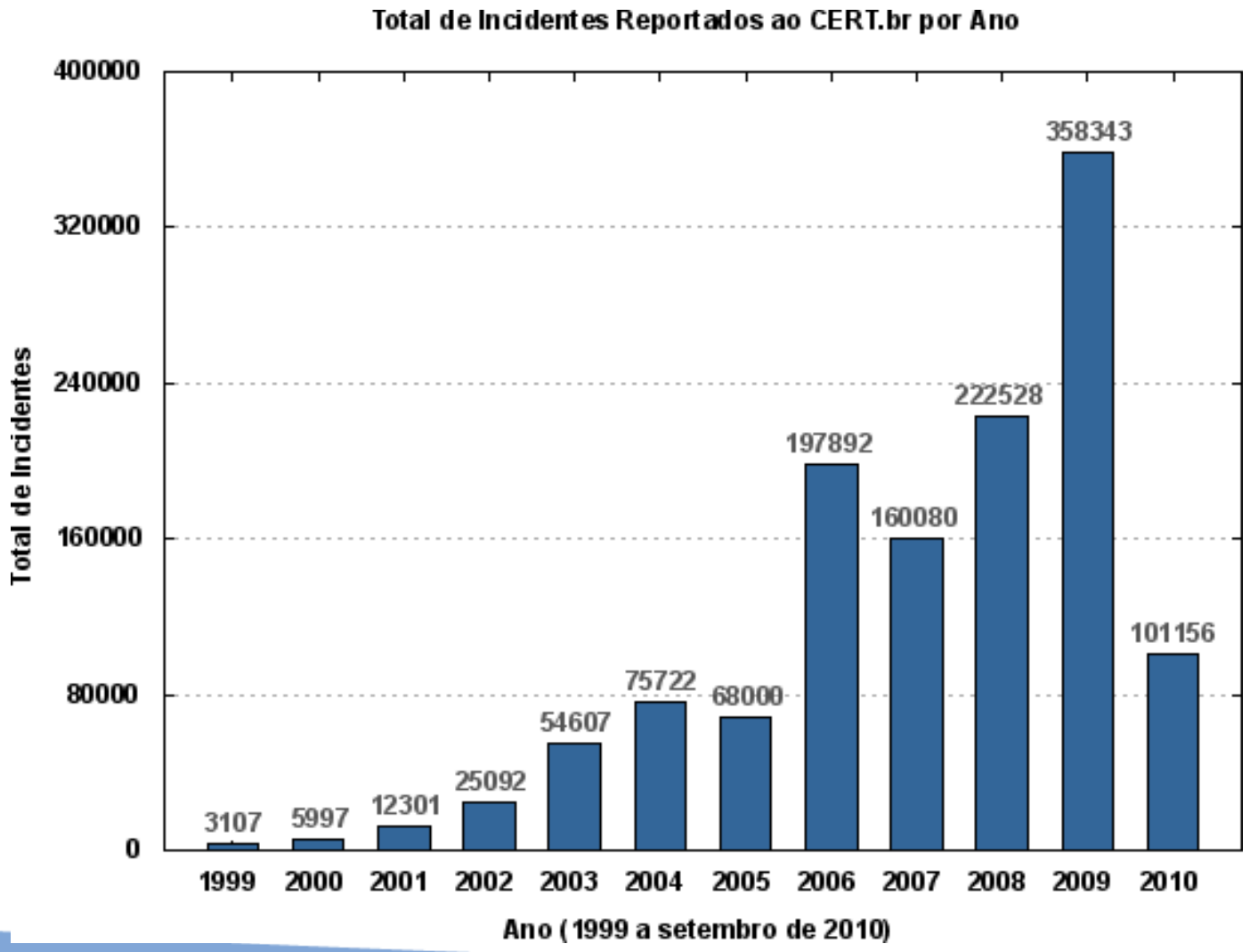
Índices

Tipo de conteúdo	Período de 2009-1-1 a 2009-7-1		Período de 2009-7-1 a 2010-1-1		Variação Únicas
	Únicas	Domínio Orkut	Únicas	Domínio Orkut	
Intolerância Religiosa	4810	3748	1965	1607	-59.1%
Racismo	3583	2399	1519	1009	-57.6%
Neo Nazismo	4645	3812	2348	2159	-49.5%
Tráfico de Pessoas	0	0	0	0	NaN%
Pornografia Infantil	49257	35067	20706	13553	-58.0%
Maus Tratos Contra Animais	2378	1673	687	549	-71.1%
Xenofobia	3761	3161	2838	2717	-24.5%
Apologia e Incitação a crimes contra a Vida	20620	17967	10946	9983	-46.9%
Homofobia	2086	1712	1457	1052	-30.2%
Todos	**91140**	**69539**	**42466**	**32629**	**-53.4%**



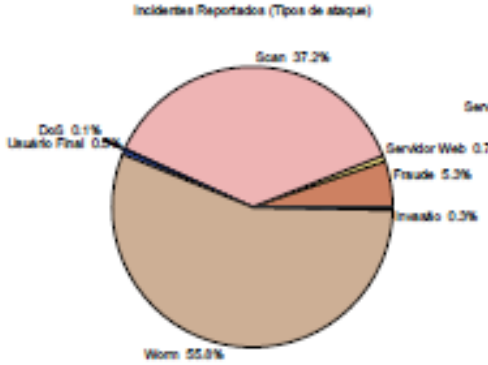
- http://www.safernet.org.br/site/indicadores

Incidentes de segurança por ano

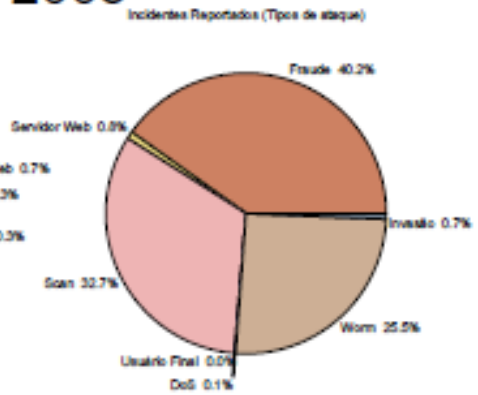


Incidentes de Segurança: Categorias

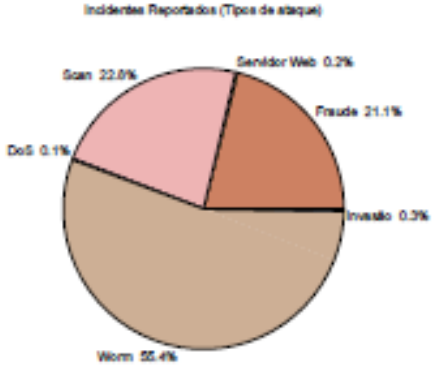
2004



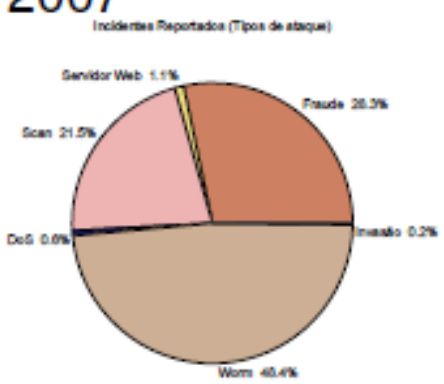
2005



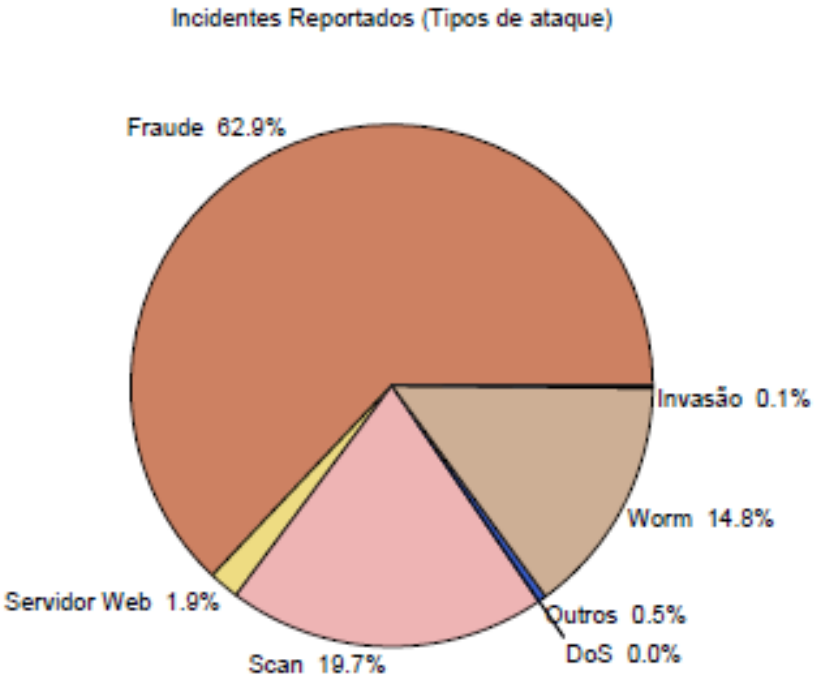
2006



2007



2008



Totais da categoria fraude:

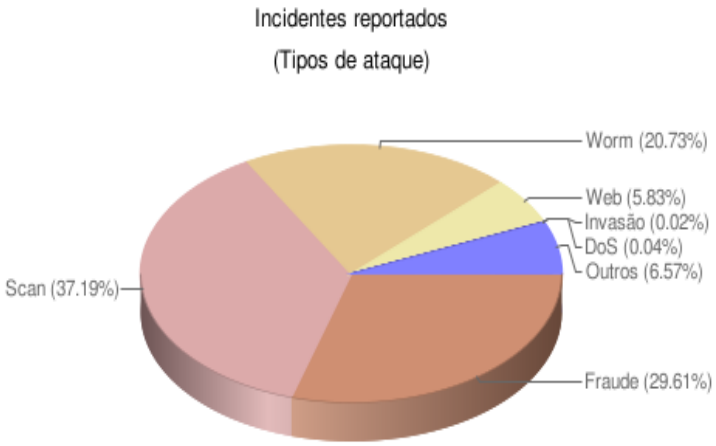
2004	4.015 (05%)
2005	27.292 (40%)
2006	41.776 (21%)
2007	45.298 (28%)
2008	140.067 (65%)

Totais da categoria *worm* (engloba *bots*):

2004	42.267 (55%)
2005	17.332 (25%)
2006	109.676 (55%)
2007	77.473 (48%)
2008	32.960 (14%)

Jan – Dez 2009

Jan – Mar 2010



Abr– Jun 2010

Evolução dos problemas de segurança

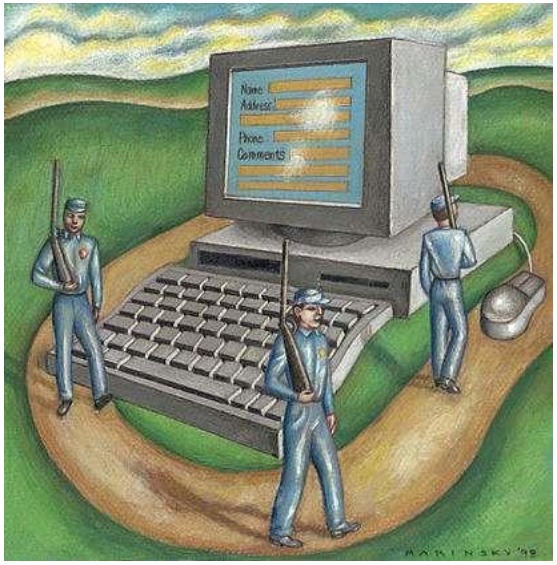
- Anos 1991–2001
  - Uso da “engenharia social” em grande escala
  - Ataques remotos aos sistemas
  - popularização de cavalos de tróia, furto de senhas,
  - varreduras, sniffers, DoS, etc
  - ferramentas automatizadas para realizar invasões
  - ocultar a presença dos invasores (rootkits)
- Anos 2002–2007
  - explosão no número de códigos maliciosos:
    - worms, bots, cavalos de tróia, vírus, spyware
  - múltiplas funcionalidades e vetores de ataque, eficiente, aberto, adaptável, controle remoto
  - praticamente não exige interação com o invasor

Evolução dos problemas de segurança

- Dias atuais - Características dos Ataques
  - Amplo uso de ferramentas automatizadas de ataque
  - Botnets – Usadas para envio de scams, phishing, invasões, esquemas de extorsão
  - Redes mal configuradas sendo abusadas para realizacão de todas estas atividades sem o conhecimento dos donos
  - **Usuários finais passaram a ser alvo**
  - **OBS: ataques web em crescimento**
  - **Ataques em redes sociais**
  - **Cloud Computing – novo emprego da web**

Objetivos da Segurança da Informação

- Proteger os Ativos (informação, computadores, equipamentos de conectividade, etc) , garantindo a integridade, confidencialidade e disponibilidade das informações.

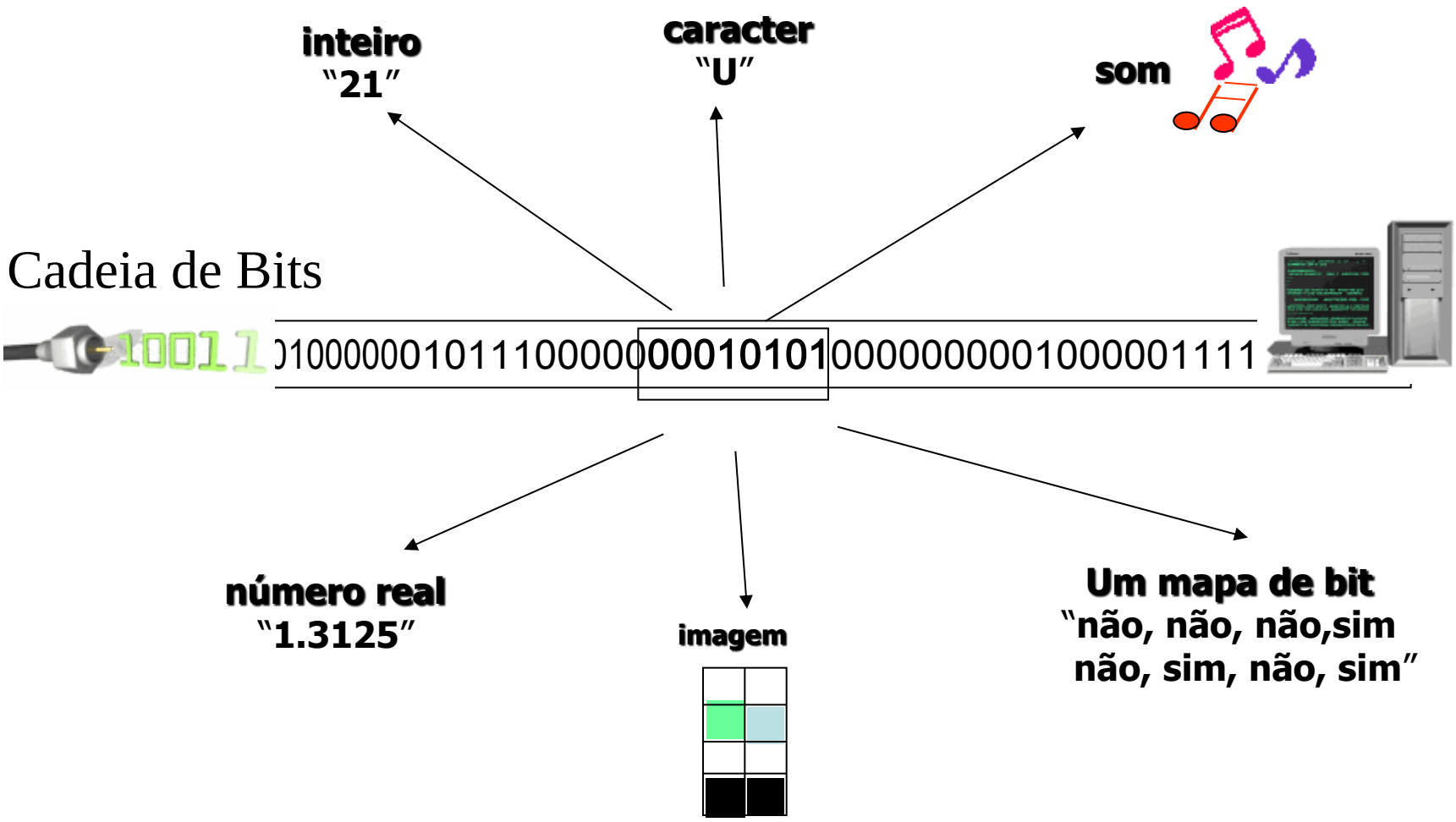


Objetivos da Segurança da Informação (cont.)

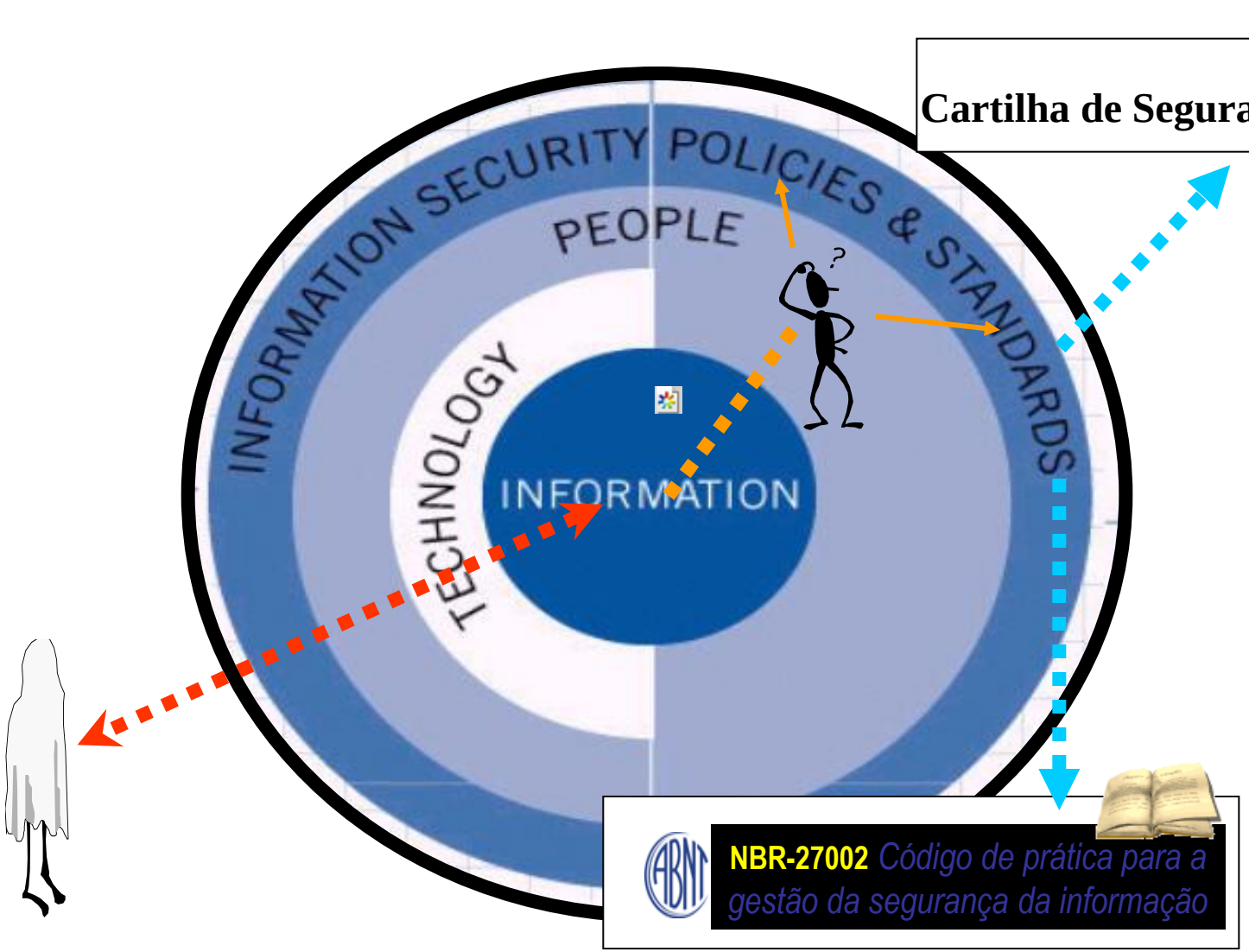
- Garantir:
  - continuidade dos negócios
  - minimização do risco
  - maximização do Retorno do Investimento (ROI)
  - oportunidades de negócio
  - privacidade

Valor da informação

- Era da informação - valor como ativo/patrimônio.
- Fundamenta tomada de decisões (Importância Estratégica).
- Pode ser roubada, furtada, alterada, apagada, etc.


inteiro
"21"
caracter
"U"
som
Cadeia de Bits
0100000010111000000010101000000000010000011111
número real
"1.3125"
imagem
Um mapa de bit
"não, não, não,sim
não, sim, não, sim"

Informação


Cartilha de Segurança CERT
INFORMATION SECURITY
POLICIES & STANDARDS
PEOPLE
TECHNOLOGY
INFORMATION
NBR-27002 Código de prática para a gestão da segurança da informação

A INFORMAÇÃO ESTÁ VULNERÁVEL

DEVE SER PROTEGIDA!

MEDIDAS DE SEGURANÇA DEVEM SER PROPORCIONAIS AO VALOR DA INFORMAÇÃO

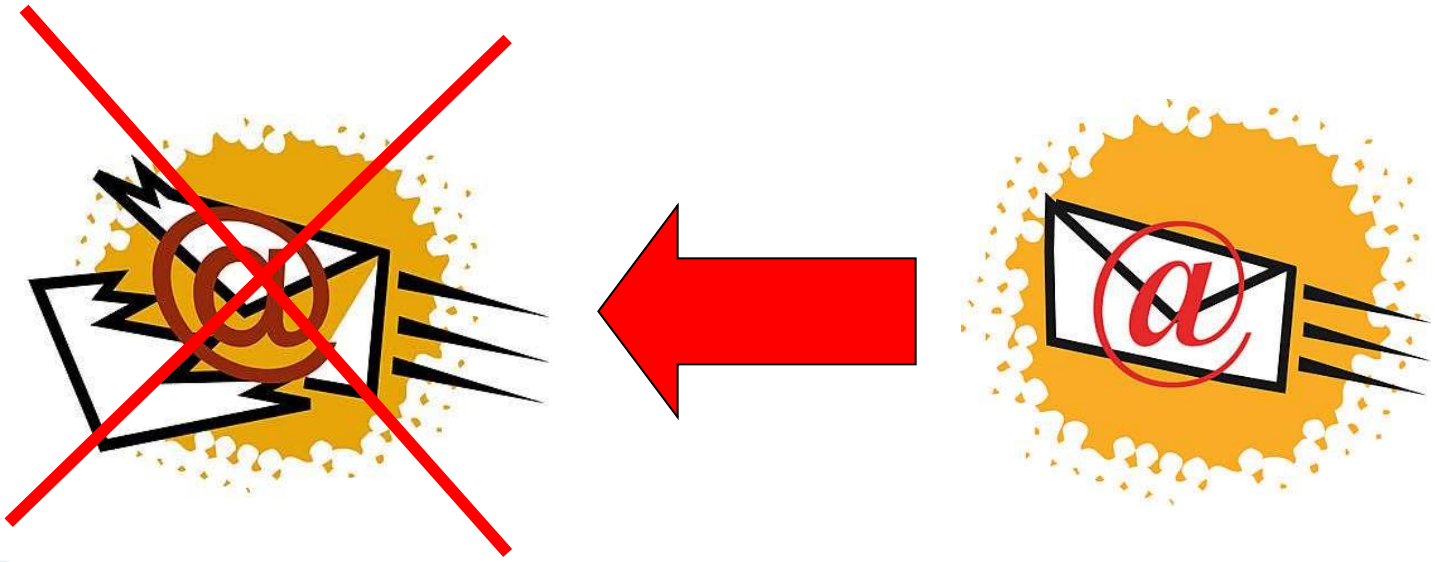
Introdução

Requisitos da Segurança da Informação

- Principais
  - Integridade
  - Confidencialidade
  - Disponibilidade
- Outros:
  - Autenticidade
  - Responsabilidade
  - Não repúdio
  - Confiabilidade

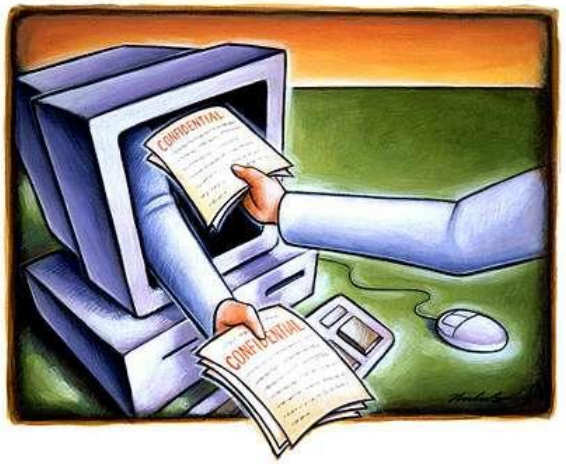
Introdução

- Integridade
  - garantir que a informação **não tenha sido alterada** em seu conteúdo, seja intencionalmente ou não.
  - ter a certeza que a informação disponibilizada pelo emissor é a mesma que chegou ao receptor



Introdução

- Confidencialidade
  - Garantir que **somente as pessoas autorizadas tenham acesso** às informações que queremos distribuir
  - Graus de confidencialidade
    - Ex. Confidencial, Secreto, Ultra-Secreto



Introdução

- Confidencialidade
  - Exige mecanismos de proteção compatíveis - acesso restrito baseado na necessidade de conhecer
  - Envolve todo o processo de comunicação
  - Perda da confidencialidade = perda do segredo, quebra do sigilo.
    - Ex.:
      - Furto do nº do cartão e senha
      - Acesso não autorizado ao sistema

Introdução

- **Disponibilidade**
  - a informação deve estar disponível no momento que se precise dela
    - possa ser acessada no momento desejado
    - deve estar ao alcance dos usuários e destinatários
  - Ex.: Banco de dados on-line para devido a problemas técnicos
  - Ex.: Vírus corrompe os dados de seu computador

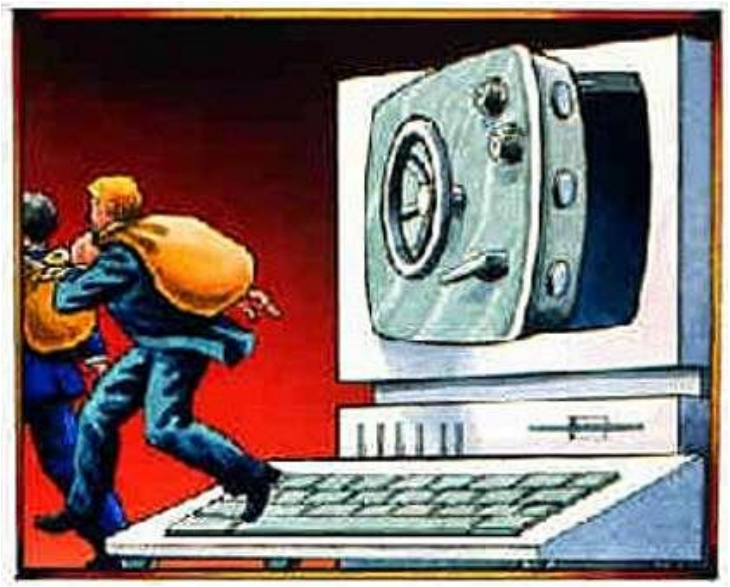
Ativos

- Todo elemento que compõe o processo de comunicação (emissor, receptor, meio,etc)
- Possuem valor
- Devem receber proteção adequada para não causar danos
- Tipos:
  - informação
  - equipamentos
  - pessoa

Ameaças

- **<u>Agentes</u>** capazes de explorar falhas de segurança - pontos fracos

- Podem provocar perdas ou danos aos ativos da empresa afetando os negócios



Ameaças

- Constantes e podem ocorrer a qualquer momento
- Grupos de ameaças:
  - naturais: condições da natureza, intempéries, etc.
  - intencionais: fraudes, vandalismo, sabotagem, espionagem, invasões e furtos e informações, etc.
  - involuntárias: resultante de ação inconsciente, vírus, falta de conhecimento, etc.

Introdução - Ameaças

- Agentes capazes de explorar falhas
- Sempre existiram(rão)
- Conforme a tecnologia avança, novas ameaças aparecem

- Ex.:
  - Tecnologia : Internet
    - Ameaças: Hackers, Vírus, Trojan, etc.

Vulnerabilidades

- São os Pontos Fracos que, ao serem explorados pelas ameaças, afetam os requisitos da segurança (integridade, confidencialidade e disponibilidade).

- Segurança visa rastrear, identificar e eliminar os pontos fracos para minimizar os danos.

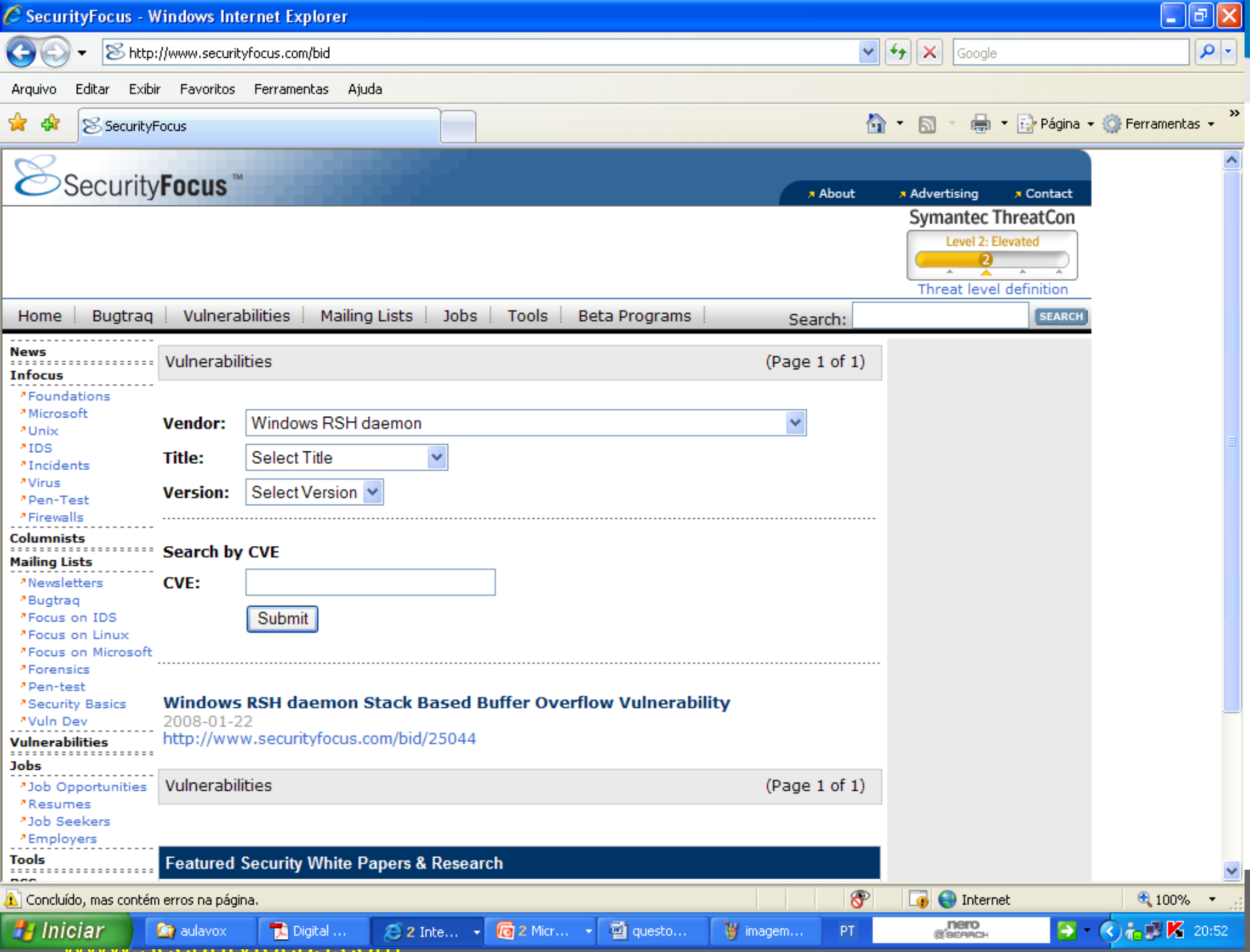
Vulnerabilidades

- Podem ser:
  - Físicas
  - Naturais
  - de Hardware
  - de Software
  - de meios de armazenagem
  - de comunicação
  - Humanas

Vulnerabilidades

- De Software
  - pontos fracos que permitem que ocorram acessos indevidos aos sistemas, mesmo sem o conhecimento do usuário.
  - Ex.:
    - configurações de computadores
    - instalação indevida de programas
    - aplicativos e sistemas operacionais desatualizados e sem os patches de segurança
      - Ex.: Antivírus mal configurado

- http://www.sans.org/top-cyber-security-risks/


SecurityFocus - Windows Internet Explorer
http://www.securityfocus.com/bid
Google
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
SecurityFocus
Página Ferramentas
SecurityFocus
About Advertising Contact
Symantec ThreatCon
Level 2: Elevated
2
Threat level definition
Home Bugtraq Vulnerabilities Mailing Lists Jobs Tools Beta Programs
Search:
SEARCH
News
Infocus
Foundations
Microsoft
Unix
IDS
Incidents
Virus
Pen-Test
Firewalls
Columnists
Mailing Lists
Newsletters
Bugtraq
Focus on IDS
Focus on Linux
Focus on Microsoft
Forensics
Pen-test
Security Basics
Vuln Dev
Vulnerabilities
Jobs
Job Opportunities
Resumes
Job Seekers
Employers
Tools
Vulnerabilities
(Page 1 of 1)
Vendor:
Windows RSH daemon
Title:
Select Title
Version:
Select Version
Search by CVE
CVE:
Submit
Windows RSH daemon Stack Based Buffer Overflow Vulnerability
2008-01-22
http://www.securityfocus.com/bid/25044
Vulnerabilities
(Page 1 of 1)
Featured Security White Papers & Research
Concluído, mas contém erros na página.
Internet
100%
Iniciar
aulavox
Digital ...
2 Inte...
2 Micr...
questo...
imagem...
PT
20:52

Vulnerabilidades

- Humanas
  - danos que as pessoas podem causar às informações e ao ambiente tecnológico que oferece o suporte.
  - Podem ser intencionais ou não
  - Ex.:
    - desconhecimento das medidas de segurança; senhas fracas, compartilhamentos, etc;
    - falta de capacitação específica
    - vandalismo, fraudes, etc.

RISCOS

- Probabilidade que as ameaças explorem os pontos fracos (vulnerabilidades)

RISCOS

- Análise dos Riscos
  - medida que busca rastrear as vulnerabilidades nos ativos que possam ser explorados por ameaças.
  - Resultado:
    - Grupo de recomendações que tem como objetivo corrigir os ativos a fim de que possam ser protegidos.

RISCOS

- Análise dos Riscos
  - Identificar
  - Avaliar
  - Analisar
  - Tratar

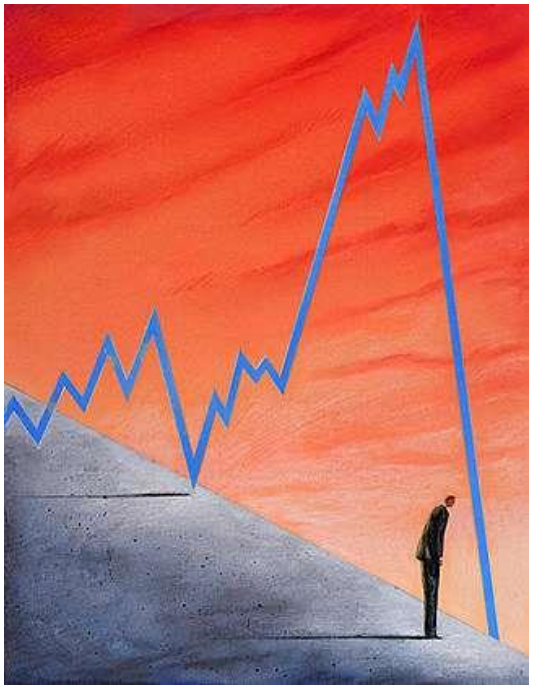
  - Após análise são escolhidos os controles e medidas de segurança (base na ISO27001)

Impacto

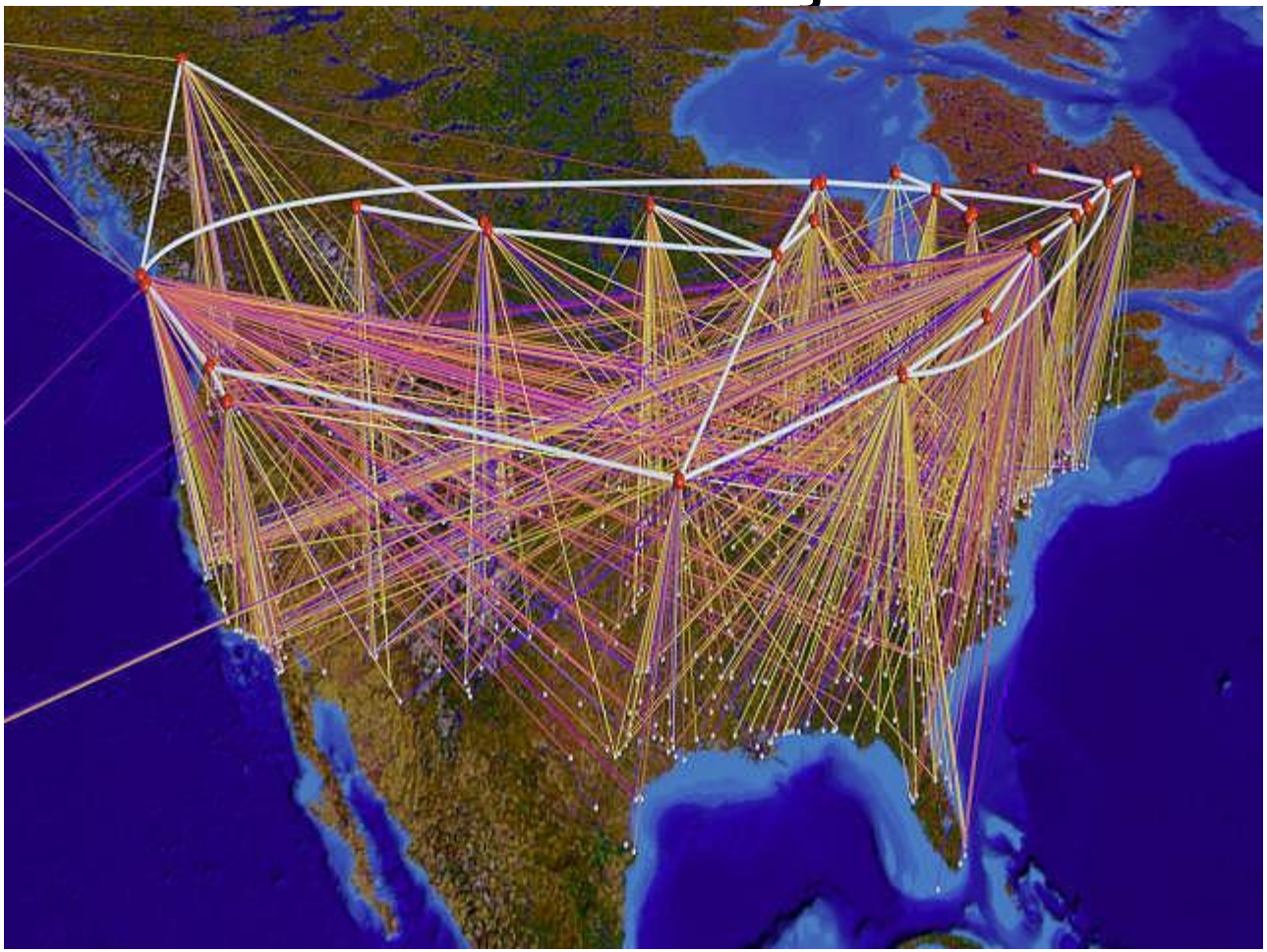
- dano ou prejuízo que pode ser causado quando uma vulnerabilidade é explorada pelas ameaças

Ex.:

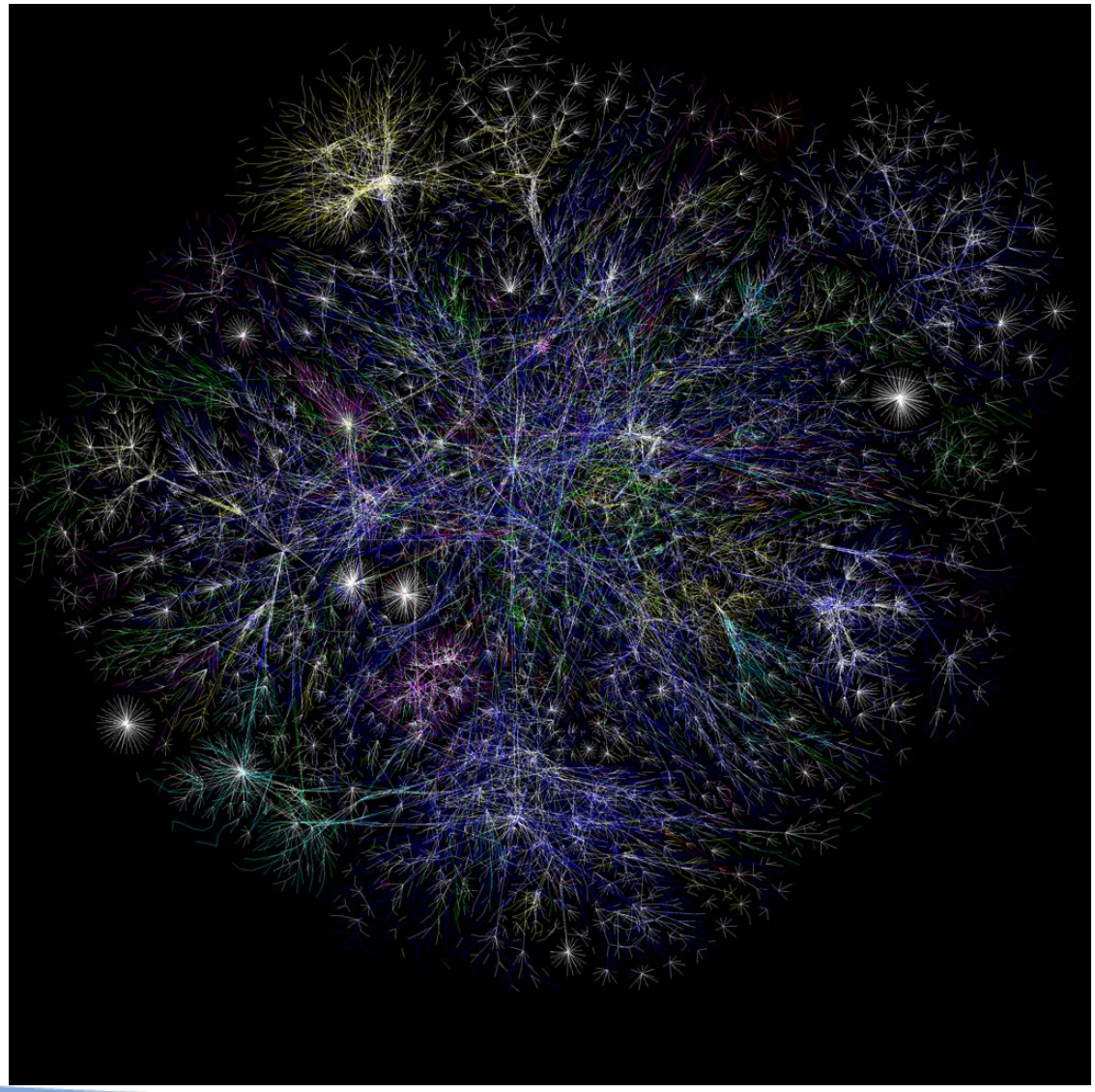
- roubo de arquivo com número dos cartões de créditos de uma empresa
- servidor fora do ar por 2 dias numa empresa de vendas on-line.



A Internet e principais ameaças



Internet – conexões no ano 2005 – www.opte.org



Tipos de Hackers

- White Hats – usa os conhecimentos para implementar segurança
- Black Hats (crackers) – usa os conhecimentos para atividades ilegais e propósitos maliciosos
- Grey hats – podem ser “bons” ou “maus” , dependendo da situação.
- Script Kiddies – novatos que usam programas prontos

Hackers / Crackers

- Usa conhecimento técnico para ataques
- Fases do ataque (normalmente):

1. Reconhecimento (ativo e passivo)
    1. Footprint : levantamento de informações
    2. Pesquisas na net (ex. Google).
    3. Engenharia Social
    4. Sniffig da rede
2. Scanning –
    1. Port Scan : varredura de portas pela rede
    2. Vulnerability Scan: varredura de vulnerabilidades

Hackers / Crackers

3. Gaining Access
   - Exploit: explora as vulnerabilidades e ganha acesso (owning)
   - Pode ser dentro ou fora da rede
4. Maintaining Access
   - implanta programas de acesso remoto (backdoors, rootkits e trojans)
5. Covering Tracks
   - Apaga rastros para evitar detecção

Conceitos Básicos (cont.)

- Engenharia social
- Códigos maliciosos
  - vírus
  - worms adware / spyware
  - keylogger/ screenlogger
  - cavalo de tróia (trojan horse)
  - backdoors
  - bots
  - rootkits

Engenharia Social

- É uma técnica de ataque:
  - usa persuasão
  - confiança
  - ingenuidade
  - “171”

  - consegue informações ou acesso a elas
  - Ex.:
    - Filme: Prenda-me se for capaz
    - O Impostor (programa Pânico na TV)

Engenharia Social

- por telefone
- por e-mail
- por contato pessoal
- por funcionários externos

Engenharia Social

- tentativa de indução ao erro

- o **sucesso** do golpe **depende do usuário** (de você!!!)

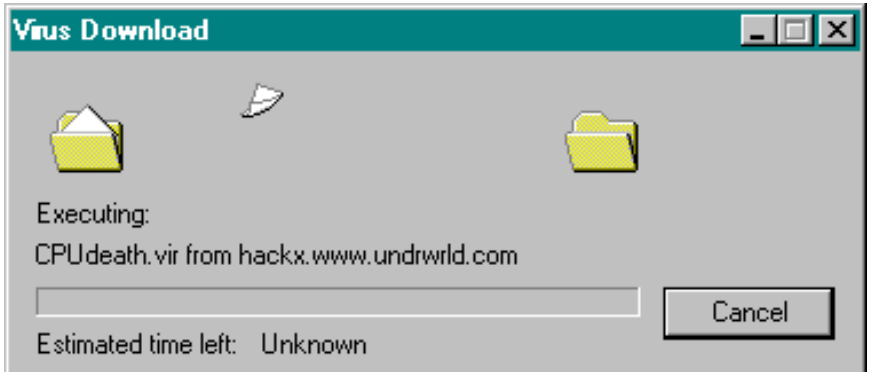
Engenharia Social

- Como se proteger
  - uso do bom senso
  - não seja ingênuo

- Não forneça senhas e dados sigilosos (principalmente por e-mail ou sites suspeitos)
- Técnica mais usada: e-mail

Códigos maliciosos

- **<u>Vírus</u>:**
  - programa malicioso que se propaga infectando
  - <u>depende da execução de arquivo</u> hospedeiro para ser ativado
  - Pode deletar e corromper arquivos, causando indisponibilidade da informação ou do computador



Códigos maliciosos

- **Vírus:**
  - Seu computador, celular ou tablet pode ser contaminado por diversas maneiras:
    - abrindo
      - anexos de emails
      - WORD, EXCEL, PPT
      - fotos, vídeos, etc
      - arquivos de outros computadores (pastas compartilhadas)
    - instalando programas de procedência duvidosa
    - através mídia removível infectada (PenDrive, Disquetes,etc)

Tipos de Vírus (algumas definições)

- Stealth / invisíveis/ encriptados
  - escondem a presença tanto do Sist. Operacional quanto dos programas anti-vírus
    - Auto-criptografados
    - Escondem os timestamp
- Vírus Polimórficos
  - Muda o estilo de criptografia a cada infecção(cópia)
  - Milhares de versões diferentes do mesmo vírus
  - Pedaço de código comum a todas as variações
- Vírus metamórfico
  - código cria novas instâncias com o mesmo funcionamento, porém com código diferente
  - faz mutação a cada infecção, podendo tanto mudar de comportamento quanto de aparência

Tipos de Vírus (algumas definições)

- Vírus de Macro
  - pode facilmente infectar diversos tipos de aplicações (word, excel, ppt, etc)
  - quando se executa a aplicação, o vírus de macro entra em ação
  - Ex.: Melissa, I Love You
- Vírus de boot
  - Modifica setores de boot dos discos

Códigos maliciosos

- **<u>Vírus:</u>**
  - pode ser invisível ao usuário
  - É descoberto com o uso do <u>ANTIVÍRUS</u>
    - “Assinaturas”
    - Cuidado com falso positivos!!!
      - *Falso positivo: Ocorre quando alerta é enviado de um arquivo não infectado, a informação é incorretamente processada identificando uma suposta contaminação por vírus.*

Códigos maliciosos

- **Proteja-se dos Vírus:**
  - instale e mantenha atualizado um bom ANTIVÍRUS
  - não execute arquivos antes de verificar com antivírus
  - tenha atenção a arquivos:
    - **.EXE, .SCR, .DLL, .COM, .ZIP.**
  - desabilite no seu leitor de e-mail a auto-execução de arquivos anexados

VIRUSTOTAL - Free Online Virus and Malware Scan - Microsoft Internet Explorer

www.virustotal.com

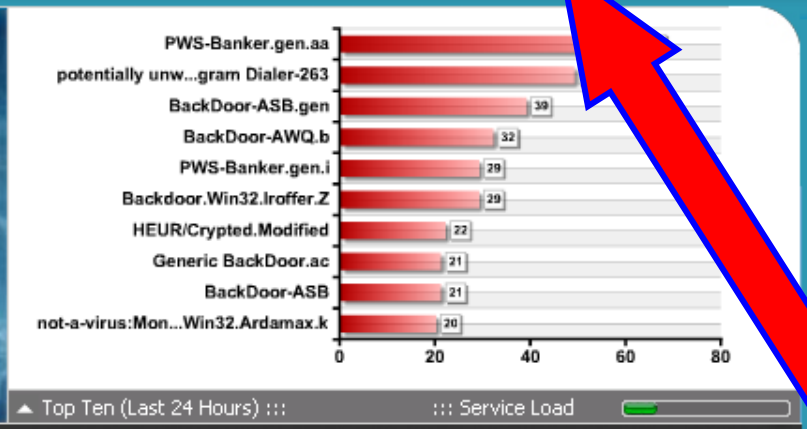
Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço http://www.virustotal.com/en/indexf.html Ir Links Norton Internet Security Norton AntiVirus

VIRUSTOTAL Distribute SSL Select file Procurar... Send

News Statistics VirusTotal

analizar



Top Ten (Last 24 Hours) ::: ::: Service Load

Latest News:

06.13.2006 VirusTotal += VirusBuster

05.23.2006 VirusTotal += Authentium

05.09.2006 VirusTotal -= Avira Desktop

04.27.2006 VirusTotal += Microsoft

04.19.2006 New response system

04.04.2006 Presentation

Virustotal offers a free service for scanning suspicious files using several antivirus engines.
Use the upper textbox to select and send any suspicious file to Virustotal for a scan. If you wish, you can also send files using your email client. In that case, please follow these steps:

- Create a new message with scan@virustotal.com as destination address of your email.
- Write **SCAN** in the Subject field (write **SCAN-** if you do not want to distribute your sample to any AV company).
- Attach the file to be scanned. Such file must not exceed 10 MB in size. If the attached file is larger, the system will reject it automatically.
- You will receive an email with a report of the file analysis. Response time will vary depending on the load of the system at the time of placing your request.

Home Contactar En Español

www.virustotal.com :: ©Hispasec Sistemas 2004-06:: e-mail info@virustotal.com

Concluído Internet

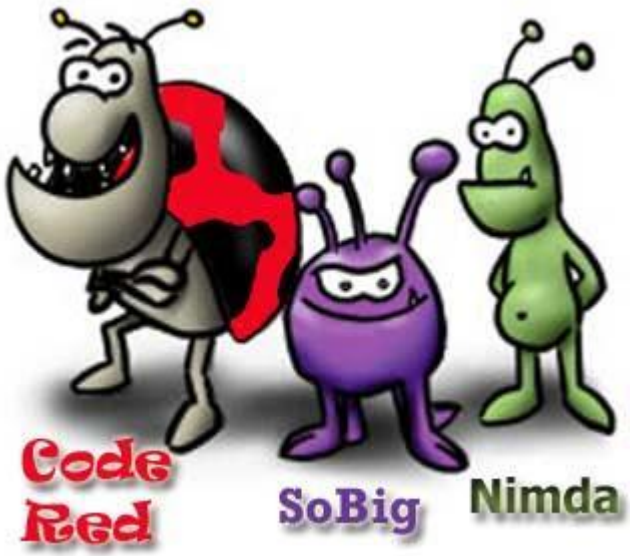
Iniciar F:\TULIO\Curso de S... aula 1 - conceitos bás... aula 2 - Segurança n... VIRUSTOTAL - Free ... PT 00:18

Códigos maliciosos

- **Worm**
  - programa que se propaga automaticamente na rede enviando cópias de si mesmo de computador para computador
  - diferente dos vírus
    - não necessita ser executado
    - não embute cópia de si em outros programas
  - explora falhas e vulnerabilidades!
    - Se o seu SO (Windows, LINUX, etc) estiver desatualizado , você corre sérios riscos de ser atacado por esta ameaça

Códigos maliciosos

- **Worm**
  - consome recursos
  - degradam desempenho rede
  - pode lotar disco rígido (cópias de si mesmo)



Códigos maliciosos

- **Proteja-se dos Worm**
  - antivírus
  - firewall
  - atualização de software

Códigos maliciosos

- **Adware e Spyware**

  - **adware** = advertising software
    - apresentam propagandas
    - incorporados a softwares e serviços
  - **spyware** = software que monitora informações e as envia para terceiros
  - ambos podem ser de uso legítimo e/ou malicioso

Códigos maliciosos

- **<u>Spyware</u> podem:**
  - monitorar acesso Internet, teclas ou cliques
  - alterar página inicial
  - varrer arquivos do HD
  - instalar outros programas
  - capturar informações capturar senhas bancárias/nº cartões crédito
  - capturar senhas de acesso a sites

Adware e Spyware

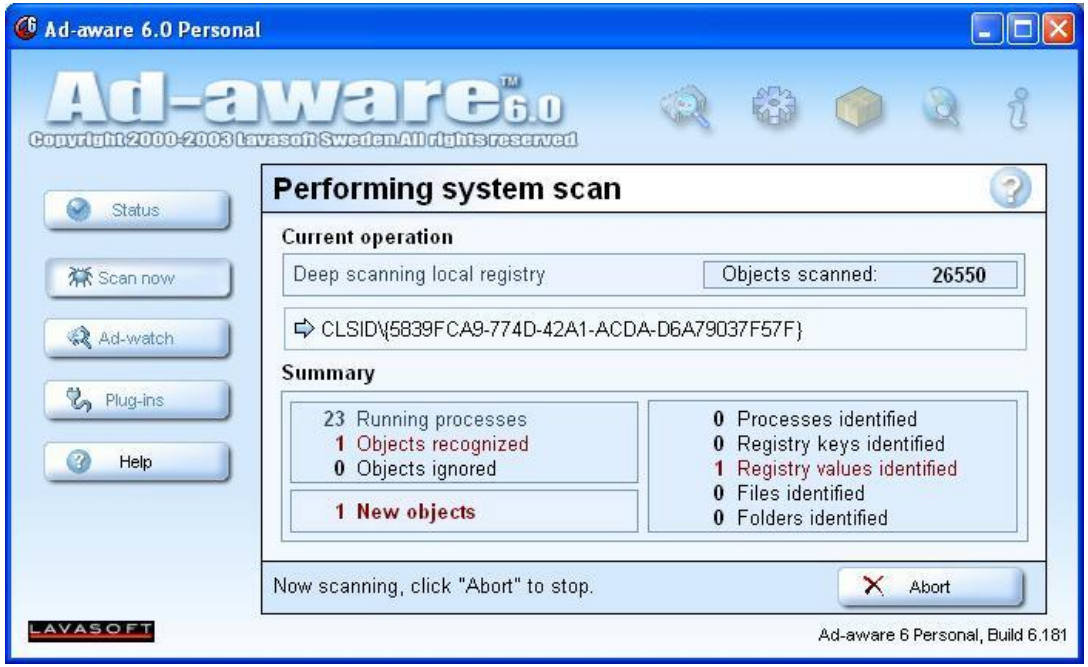
– Anti-Spyware

Ex.:

- ADWARE
- SPYBOT

– Antivírus

– Firewall



Antispyware FREE

- AD-AWARE - http://www.lavasoftusa.com/software/adaware/
- SPYBOT Search and Destroy - http://www.safer-networking.org/pt/download/index.html
- Sites de download:

  www.superdownloads.com.br

  www.baixaki.com.br

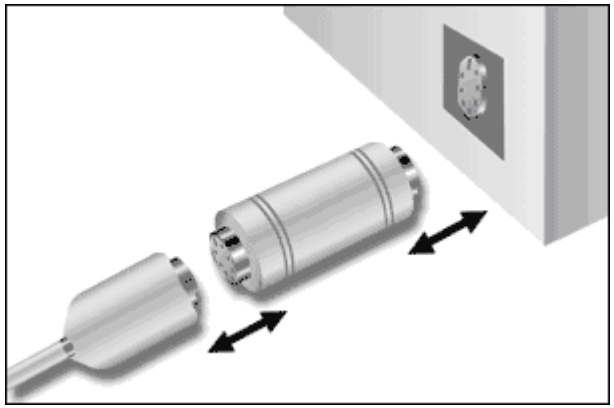
  (baixar do site do fabricante)

Códigos maliciosos

- **Keylogger**
  - captura e armazena teclas digitadas no teclado
  - textos, dados de Imposto de Renda, Dados pessoais, nº cartão de crédito, etc.
  - envio das informações capturadas por e-mail

Códigos maliciosos

- **Keylogger**
  - Internet Banking - usa teclado virtual
  - o keylogger não captura a imagem, mas existem os screenloggers!

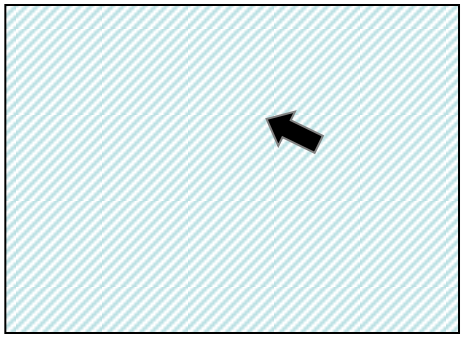


Keylogger Hardware

Cuidado em Lan -houses

Códigos maliciosos

- **Screenlogger**
  - armazena região próxima do clique do mouse ou a tela toda a cada clique



  - desenvolvidos para Internet Banking e outros sites que necessitam de senha com cliques

Não abra e-mail de origem desconhecida - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço https://www2.bancobrasil.com.br/aapf/aai/login.pbk?loginSCD=true

Ir Links Norton Internet Security Norton AntiVirus

Procure aqui... Buscar Sites do Banco do Brasil Ouvidoria BB . Rede de Atendimento Escolha sua conta

Sua Conta

Perguntas Freqüentes

Serviços Investimentos Empréstimos Cartões Consórcios Seguros Previdência Capitalização

Problemas com o campo senha ou no acesso à sua conta?
O BB disponibiliza atendimento 24 horas para soluções de problemas de acesso. Caso necessite ligue para 0800-729-0500.
Saiba mais »

BB Crédito Parcelado Cartão
Sua fatura Ourocard já vem com a solução para você levar a vida leve.
Saiba mais »

Solução de Segurança
Cadastramento de Computadores
Saiba mais »

Informe o prefixo da agência.

Titular
1º Titular

Agência

Conta

Teclado virtual

6 7 8 9 0
1 2 3 4 5

Senha de Auto-Atendimento

... contraste ...

Problemas com o campo senha, clique aqui

entrar limpar

Atenção! Mais segurança para suas transações eletrônicas. Instale sempre o teclado virtual e a ferramenta de segurança. Saiba mais »

Navegue com segurança

Mantenha atualizado o seu navegador (browser). »

Mantenha em segredo a sua senha. »

Instale e mantenha sempre atualizado um programa antivírus. »

Central de Atendimento BB
Informações e solicitações sobre produtos e serviços. »
4004 0001 ou **0800 729 0001** (conforme a localidade)

Suporte Técnico
Atendimento 24 horas para soluções de problemas de acesso. »
0800 729 0500

acesso e segurança · política de privacidade · patrocínios · relações com investidores · central de atendimento BB · English · mapa do site

Applet br.com.bb.aapf.bbteclado.CampoTeclado started

Internet

Iniciar F:\TULIO\Curso de S... aula 1 - conceitos bás... aula 2 - Segurança n... Não abra e-mail de or... PT 00:24

Códigos maliciosos

- **Keylogger e Screenlogger**
  - Evita-se com:
    - Antivírus
    - Anti-spyware
    - Firewall
    - Atualização softwares
- Vídeologger
  - Grava em vídeo

Códigos maliciosos

- **<u>Cavalos de Tróia</u> (Trojan horse)**
  - programa que executa funções projetadas
  - pode vir através de e-mail
    - cartão virtual
    - álbum de fotos
    - protetor de telas
    - jogos
    - Sites pornográficos
    - Etc.

Códigos maliciosos

- **Cavalos de Tróia (Trojan horse)** podem:
  - instalar Keylogger e/ou ScreenLogger
  - furtar senhas e informações sensíveis
  - incluir Backdoors: que permitem acesso remoto ao seu computador
  - alterar ou destruir arquivos

Códigos maliciosos

- **<u>Cavalos de Tróia</u> (Trojan horse):**
  - não propaga cópia de si mesmo (diferente de vírus/worm)
  - age sem o conhecimento do usuário

Lixo eletrônico - Outlook Express

Arquivo Editar Exibir Ferramentas Mensagem Ajuda

Criar email | Responder | Responder a todos | Encaminhar | Imprimir | Excluir | Enviar/receber | Endereços | Localizar | Norton AntiSpam

Lixo eletrônico

De: correio.eletronico **Para:** ttthhyago
Assunto: Você é uma pessoa Maravilhosa, mim ligue ok.

s e importantes... Simples como eu e importantes como você... , "" T

Mensagem:
Penso muito em você...

"As coisas que realizamos, nunca são tão belas quanto às que sonhamos. Mas às vezes, nos acontecem coisas tão belas, que nunca pensamos em sonhá-las. Para mim aconteceu... VOCÊ !!!"

Clique aqui para visualizar o cartão por inteiro

Existe um presente especial esperando por você no site de cartões do terra.

Para recebê-lo, vá até o endereço abaixo no seu navegador e faça o download:

http://www.terra.com.br/cartoes.pl?ecartao=8111066162813012

Este cartão ficará disponível por 15 dias.

http://saudades-1.at.vwdhosting.net/visualizar.html

Exemplo de trojan

Códigos maliciosos

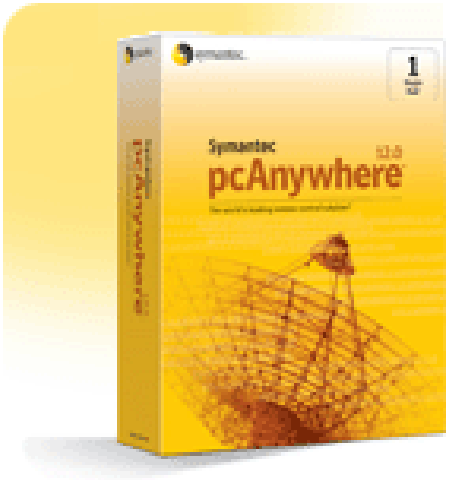
- **Evitam-se os Cavalos de Tróia** com o:
  - uso de antivírus atualizado
  - uso de firewall
  - atenção aos arquivos recebidos por e-mail

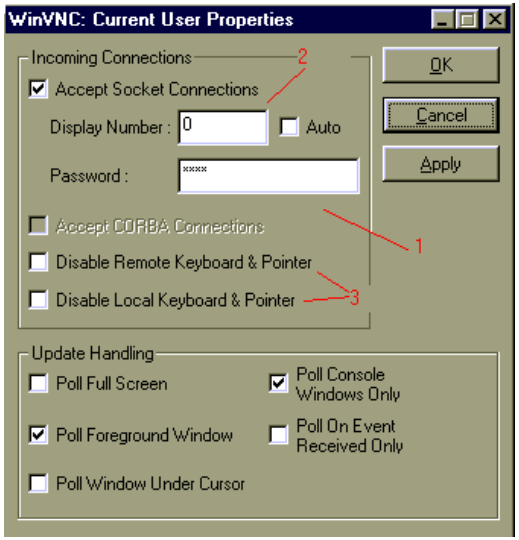
Códigos maliciosos

- **BackDoors**
  - programa servidor que abre portas lógicas de acesso pela Internet
  - instalado por um trojan

Códigos maliciosos

- **BackDoors**
  - instalação e má configuração de programa de acesso remoto comercial.
    - Ex.: PCAnywhere, VNC





Códigos maliciosos

- Proteja-se de BackDoors
  - não execute programas de origem duvidosa
  - caso precise, configure o programa de acesso remoto corretamente

Códigos maliciosos

- Proteja-se de BackDoors

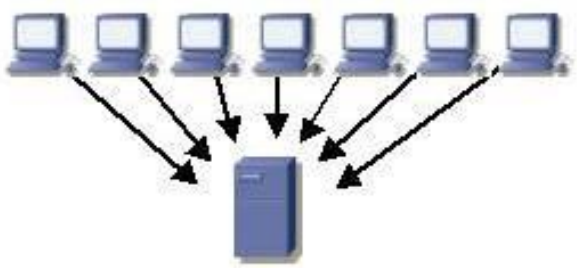
  – firewall pessoal (negar conexões de fora para backdoor instalados na máquina)
  – Antivírus
  – atualizar o sistema operacional e sistemas de uso

Códigos maliciosos

- **BOTs**
  - programa que explora vulnerabilidades
  - similar ao worm
  - propaga-se sozinho
  - pode dispor de mecanismo de comunicação com o invasor

Códigos maliciosos

- **BOTs** - o invasor pode:
  - realizar ataques em massa
  - realizar ataque de negação de serviço - DOS
  - furtar dados dos computadores com bots
  - enviar e-mail phishing
  - enviar spam



Códigos maliciosos

- **BOTs - proteja-se:**
  - atualizando os sistemas existentes
  - antivírus
  - firewall

Códigos maliciosos

- **Rootkit**
  - programa que garantem e mantém acesso privilegiado ao computador
  - Invisível ao usuário

Códigos maliciosos

- **Rootkit**
  - podem:
    - remover arquivos de log
    - capturar informações (sniffers)
    - varrer as vulnerabilidades (scanners)
    - servir como backdoors
    - etc.

Códigos maliciosos

- **Proteja-se do Rootkit**
  - antivírus
  - Firewall
  - Programas de identificacao de rootkits
  - atualização de sistema operacional

Hoax

- Boatos da Internet
- Geram tráfego desnecessário
- Criam pânico nos usuários