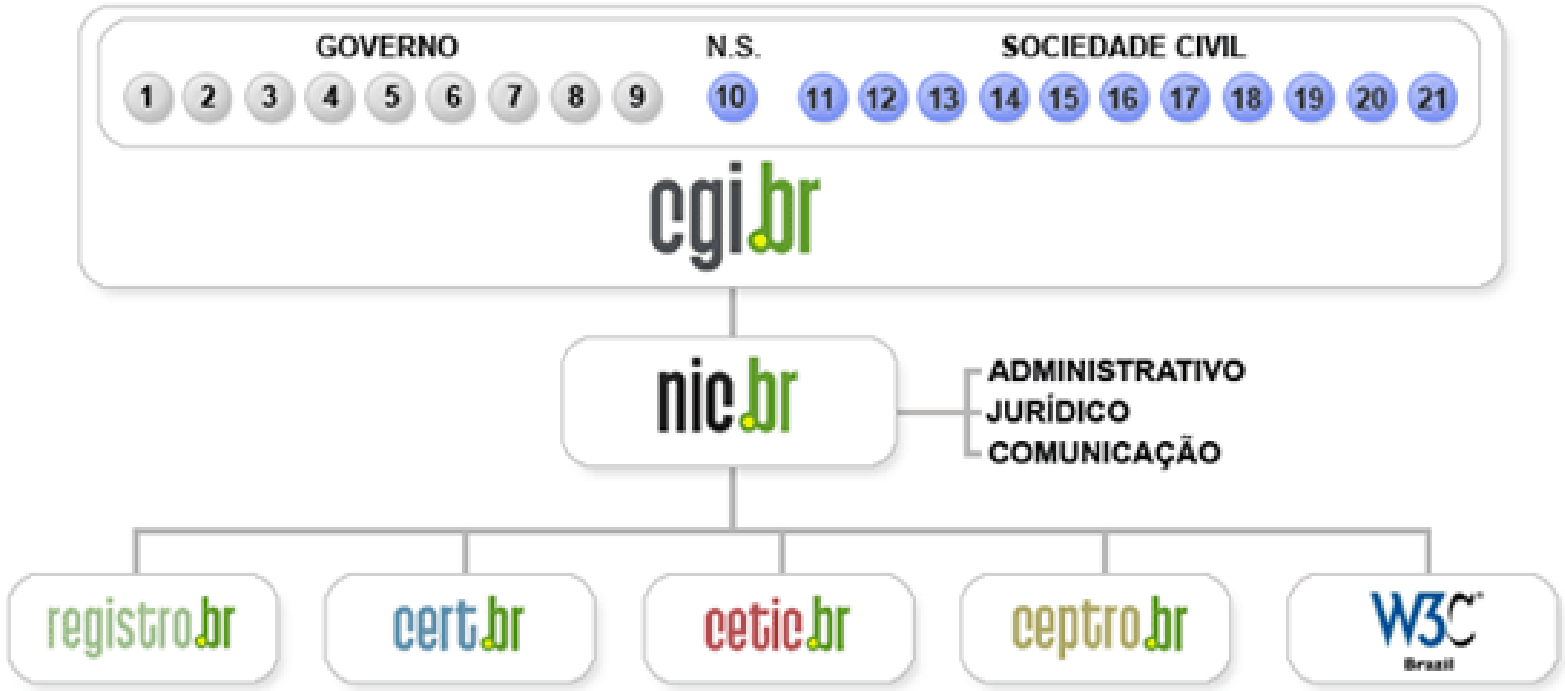
Internet, pragas e segurança

Miriam von Zuben
miriam@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

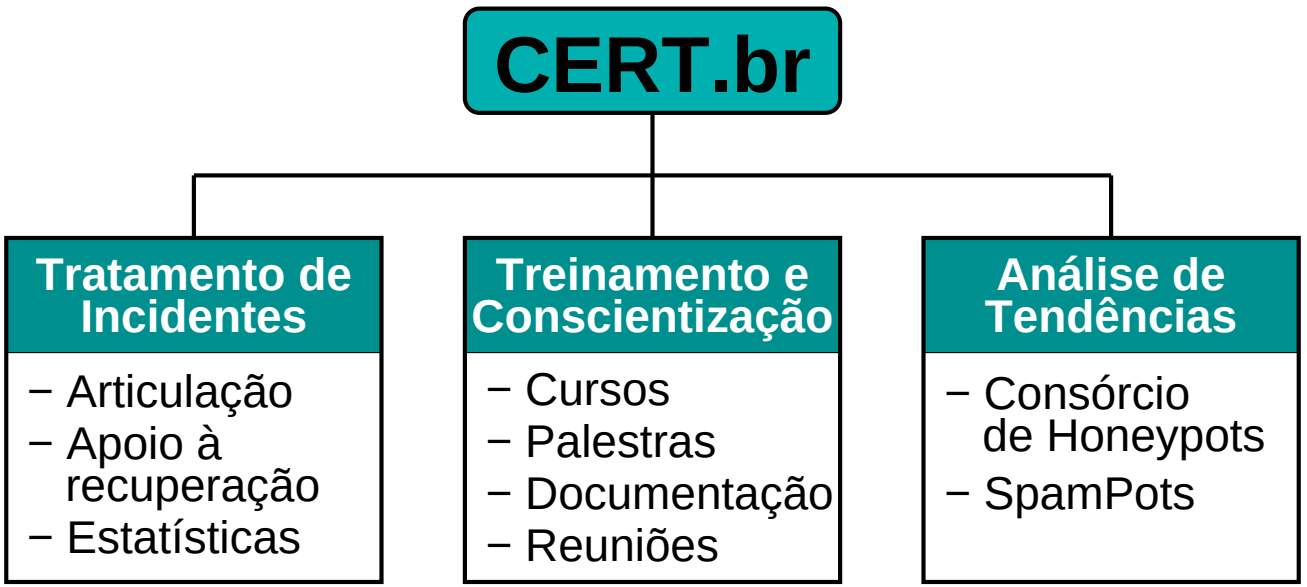
Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas**

Sobre o CERT.br

Criado em 1997 como ponto focal para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Agenda

Códigos maliciosos
- Histórico
- Principais Tipos
- Resumo comparativo

Prevenção
- Estamos nos prevenindo?
- O que fazer para se prevenir

Referências

Perguntas

Códigos maliciosos

Códigos maliciosos/Pragas/*Malware*

Programas especificamente desenvolvidos para executar ações danosas em um computador

Principais tipos:

- Vírus
- *Worm*
- *Adware* e *Spyware*
- *Keylogger* e *Screenlogger*
- *Trojan*
- *Bot* e *Botnet*
- *Backdoor*
- *Rootkit*

Histórico

Década de 1970:

- Surgimento dos primeros códigos maliciosos (Creeper)
- Detectado na ARPANET
- Programas experimentais
- Não possuíam comportamento destrutivo
- Surgimento do primeiro antivírus (Reaper)

Década de 1980:

- Principais objetivos dos atacantes:
  - demonstrar conhecimento técnico
  - causar danos como perda de dados
- Propagação via *disquetes* e *e-mails*
- Surgimento dos antivírus genéricos
- Principal alvo: sistema operacional DOS

Histórico

Década de 1990:

- Popularização da Internet
- Surgimento do *spam*
- Principais objetivos dos atacantes:
  - obter vantagens financeiras: extorsão, furto de informações
  - envio de *spam*
  - ataques ideológicos
- Propagação: *e-mail* e compartilhamento de recursos
- Principais alvos: Windows e seus aplicativos

Histórico

Década de 2000 até os dias atuais:

- Atacantes com pouco conhecimento técnico: uso de ferramentas
- Programas com grande quantidade de vulnerabilidades
  - exploradas em curto espaço de tempo
  - sistemas operacionais e programas desatualizados
- Explosão no número de códigos maliciosos: múltiplas funcionalidades
- Principais alvos: usuários finais (uso de engenharia social)
- Popularização das redes sociais
  - utilização de senhas fracas
  - reutilização de senhas
  - roubo de identidade (exploração da rede de confiança)
  - grande disponibilização de informações
  - utilização de encurtadores de URLs

Principais Tipos de Códigos Maliciosos

Vírus (1/3)

Programa que se
propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador

- depende da execução do programa ou arquivo infectado para ser tornar ativo e continuar o processo de infecção
- possui controle total sobre o computador

Vírus (2/3)

Forma de infecção:

- abrir arquivos anexados aos *e-mails*
- abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos
- instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de *pen drives*, CDs, DVDs, etc
- ter alguma mídia removível (infectada) conectada ou inserida no computador, quando ele é ligado

Principais tipos:

- Boot: infectam o setor de inicialização do disco rígido/disquete
- Programas: infectam arquivos executáveis
- Macro: infectam arquivos lidos por programas que utilizam macros

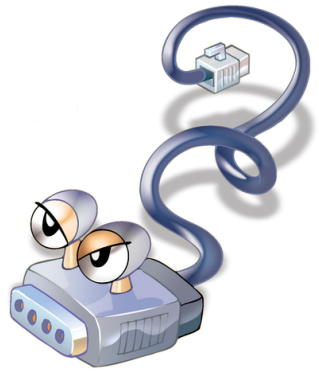
Vírus (3/3)

Cronologia:

- 1984: Termo Vírus foi cunhado por Fred Cohen
- 1986: Brain - primeiro vírus malicioso (boot)
- 1988: Jerusálem (programa) - primeiro vírus residente em memória. Surgimento do primeiro antivírus, escrito por Denny Yanuar Ramdhani
- 1989: Primeiro antivírus comercial (IBM)
- 1991: Surgimento dos primeiros kits para criação de vírus
- 1992: Michelangelo (boot) - primeiro vírus a aparecer na mídia
- 1995: Concept - primeiro vírus de macro
- 1999: Melissa (macro) - grande velocidade de propagação. Envia *e-mail* pelo Outlook com os últimos arquivos .doc acessados
- 2000: LoveLetter (macro) - grande prejuízo

Worm (1/2)

Programa capaz de se propagar automaticamente pela rede, enviando cópias de si mesmo de computador para computador



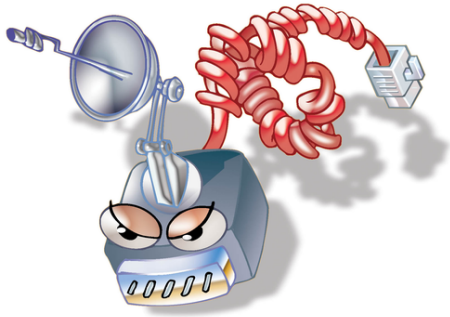
- não embute cópias em outros programas ou arquivos
- não necessita ser explicitamente executado para se propagar
- propaga-se através da exploração de:
  - vulnerabilidades existentes ou
  - falhas na configuração de programas instalados em computadores

Worm (2/2)

Cronologia:

- 1988: Morris - escrito por Robert Morris, explorava vulnerabilidades do sendmail e finger, entre outras
- 2001: Nimda e CodeRed - rápida propagação, exploravam vulnerabilidades do IIS
- 2003: Slammer - explorava vulnerabilidades do SQL Server
  Blaster - programava um DOS contra o site do update da Microsoft
  Sobig - instalava um servidor SMTP para se propagar
- 2005: Mydoom - propaga-se através da rede do P2P Kazaa
- 2008: Koobface: atacava usuários do Facebook e MySpace, via scraps. Direcionava para uma atualização falsa do Abobe Flash Player
- 2010: Stuxnet: primeiro Worm a atacar sistemas SCADA, possivelmente instalações iranianas

Bot



Programa que, além de incluir funcionalidades de *worms*, dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente

- Modos de comunicação:
  - canais de IRC
  - servidores Web
  - compartilhamento de arquivos P2P
- Computador pode ser orientado a:
  - desferir ataques na Internet
  - furtar dados
  - enviar *spam* e *e-mails* de *phishing*
- Exemplo: Agobot

Botnet

Rede composta de centenas/milhares de computadores infectados por *bots*

- usadas para aumentar a potência dos ataques
- geralmente usadas por aluguel

Spam zombie: computador infectado por código malicioso e transformado em servidor de *e-mail* para envio de *spam*

- Spit (**Sp**am via **I**nternet ***T****elephone*)
- Spim (**Sp**am via ***I****nstant* ***M****essaging*)

Adware, *Spyware* e *Backdoor*

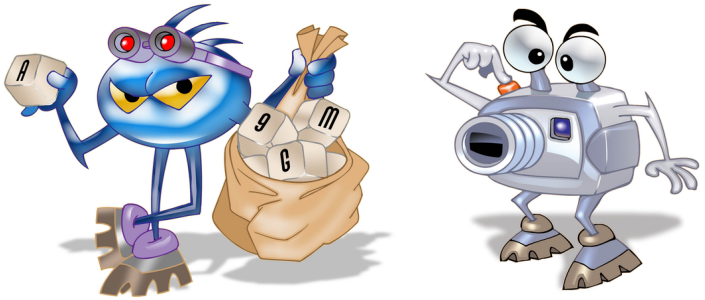
Adware: programa projetado especificamente para apresentar propagandas

Spyware: programa capaz de monitorar atividades do sistema e enviar as informações coletadas para terceiros

Backdoor: programa que permite a um invasor retornar a um computador comprometido. Normalmente colocado de forma a não ser notado

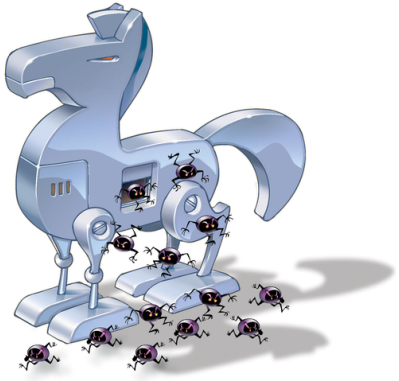
Keylogger e *Screenlogger*

Keylogger:
programa capaz de capturar
e armazenar as teclas digitadas



Screenlogger: *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

Trojan



Programa que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções maliciosas sem o conhecimento do usuário

- Consiste de um único arquivo que necessita ser executado para que seja instalado
- Não infecta outros arquivos e não propaga cópias de si mesmo automaticamente
- Exemplos: cartão virtual, álbum de fotos, protetor de tela
- Pode instalar outros códigos maliciosos: keylogger, *screenlogger*, *spyware* e *backdoor*
- Estes códigos maliciosos podem ser: baixados da Internet (*Downloader*) ou já fazem parte do seu próprio código (*Dropper*)

Rootkit

Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido

Estes programas:

- não são usados para obter acesso privilegiado a um computador
- permitem manter o acesso privilegiado em um computador previamente comprometido

Resumo comparativo

Como ocorre a instalação e a propagação

Códigos Maliciosos								
	Vírus	*Trojan*	*Worm*	*Bot*	*Spyware*	*Backdoor*	*Keylogger*	*Rootkit*
Como ocorre a instalação:								
Ação de outro código malicioso	X		X	X	X	X	X	
Ação do invasor						X	X	X
Execução de um arquivo/programa infectado	X							
Execução explícita do código malicioso		X	X	X				
Exploração de vulnerabilidades			X	X				
Exploração de falhas de configuração			X	X		X		
Como se propaga:								
Insere cópias de si em arquivos/programas	X							
Envia cópia de si automaticamente pela rede			X	X				

Resumo comparativo

Ações maliciosas mais comuns:

Códigos Maliciosos								
	Vírus	*Trojan*	*Worm*	*Bot*	*Spyware*	*Backdoor*	*Keylogger*	*Rootkit*
Ações maliciosas mais comuns:								
Alteração e/ou remoção de arquivos	X	X						X
Consumo de grande quantidade de recursos			X	X				
Possibilita a comunicação com o invasor				X	X			
Furto de informações sensíveis		X			X		X	X
Inclusão de *backdoor*		X	X					X
Instalação de *keylogger*		X			X			X
Instalação de *spyware*		X						
Possibilita o retorno do invasor						X		X
Envio de *spam* e *phishing*				X				
Desferir ataques na Internet			X	X				

Prevenção

Estamos nos Prevenindo?

Problemas de Segurança Encontrados:

	Nenhum	Vírus ou outro programa malicioso	Uso indevido de informações	Fraude financeira	Outro	Não sabe
2007	69	27	2	1	2	2
2008	68	28	1	1	ND	3
2009	63	35	1	1	ND	1

Medidas de Segurança Adotadas:

	Antivírus	*Firewall* pessoal	Outro programa	Nenhuma medida
2007	75	11	6	22
2008	70	10	4	28
2009	75	9	4	22

Freqüência de Atualização do Antivírus:

	Diária	Semanal	Mensal	Trimestral	Automática	Não atualizou	Não sabe
2007	38	26	17	3	ND	8	7
2008	28	23	15	3	22	3	5
2009	22	17	13	5	34	3	5

Fonte: Pesquisa TIC Domícilios – CETIC.br (http://www.cetic.br/)

O que fazer para se prevenir (1/3)

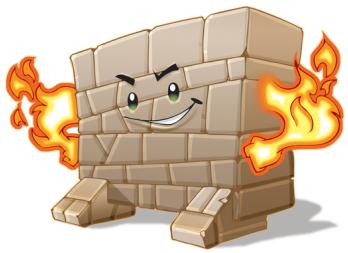
Manter o computador atualizado

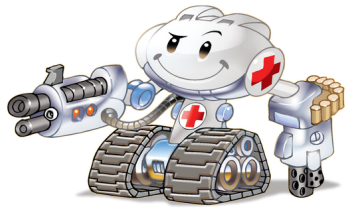
- Instalar a última versão e aplicar todas as correções de segurança (*patches*)
  - sistema operacional (checar horário da atualização automática)
  - aplicativos (navegador, proc. de textos, leitor de *e-mails*, visualizador de imagens, PDFs e vídeos, etc)
  - *Hardware* (*firmware* de *switches*, bases *wireless*, etc)

O que fazer para se prevenir (2/3)

Utilizar Programas de Segurança

- *firewall* pessoal
- antivírus
- anti-*spyware*
- anti-*spam*
- anti-*rootkit*
- complementos e *plugins* em navegadores





O que fazer para se prevenir (3/3)

Principais medidas preventivas:

Códigos Maliciosos								
	Vírus	*Trojan*	*Worm*	*Bot*	*Spyware*	*Backdoor*	*Keylogger*	*Rootkit*
Principais medidas preventivas a ser tomadas:								
Desabilitar a auto-execução de arquivos	X	X	X	X	X	X	X	
Manter os programas instalados atualizados			X	X		X	X	X
Ser cuidadoso ao manipular arquivos	X	X	X	X	X	X	X	
Utilizar anti-*rootkit* atualizado						X		X
Utilizar anti-*spyware* atualizado					X		X	
Utilizar antivírus atualizado	X	X	X	X	X	X	X	X
Utilizar firewall pessoal atualizado		X	X	X	X	X	X	X

Melhorar a Postura On-line (1/2)

Não acessar *sites* ou seguir *links*

- recebidos por *e-mail* ou por serviços de mensagem instantânea
- em páginas sobre as quais não se saiba a procedência

Receber um *link* ou arquivo de pessoa ou instituição conhecida não é garantia de confiabilidade

- códigos maliciosos se propagam a partir das contas de máquinas infectadas
- fraudadores se fazem passar por instituições confiáveis

Não fornecer em páginas *Web*, *blogs* e *sites* de redes sociais:

- seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc)
- dados sobre o computador ou sobre *softwares* que utiliza
- informações sobre o seu cotidiano
- informações sensíveis (senhas e números de cartão de crédito)

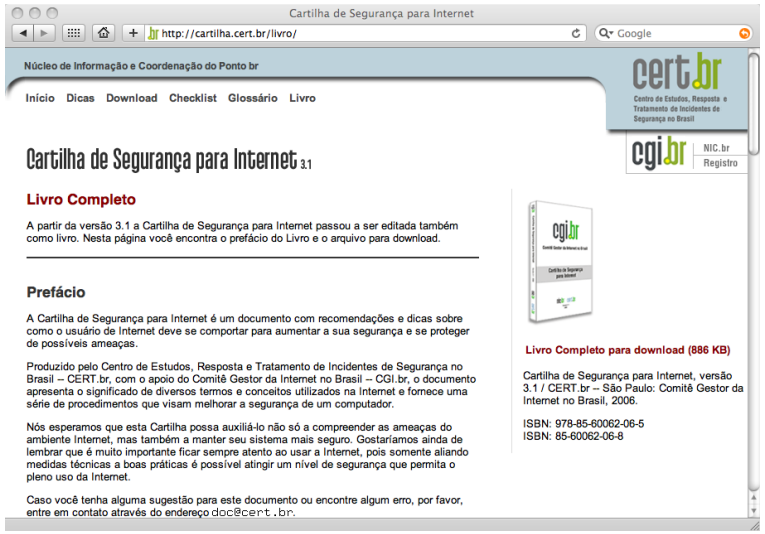
Melhorar a Postura On-line (2/2)

Precauções com contas e senhas

- utilizar uma senha diferente para cada serviço/*site*
- evitar senhas fáceis de adivinhar
  - nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários
- usar uma senha composta de letras, números e símbolos
- utilizar o usuário Administrador ou `root` somente quando for estritamente necessário
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador

Informar-se e Manter-se Atualizado (1/2)

http://cartilha.cert.br/



http://twitter.com/certbr

Informar-se e Manter-se Atualizado (2/2)

- **Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br**
  http://www.antispam.br/

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/

Perguntas