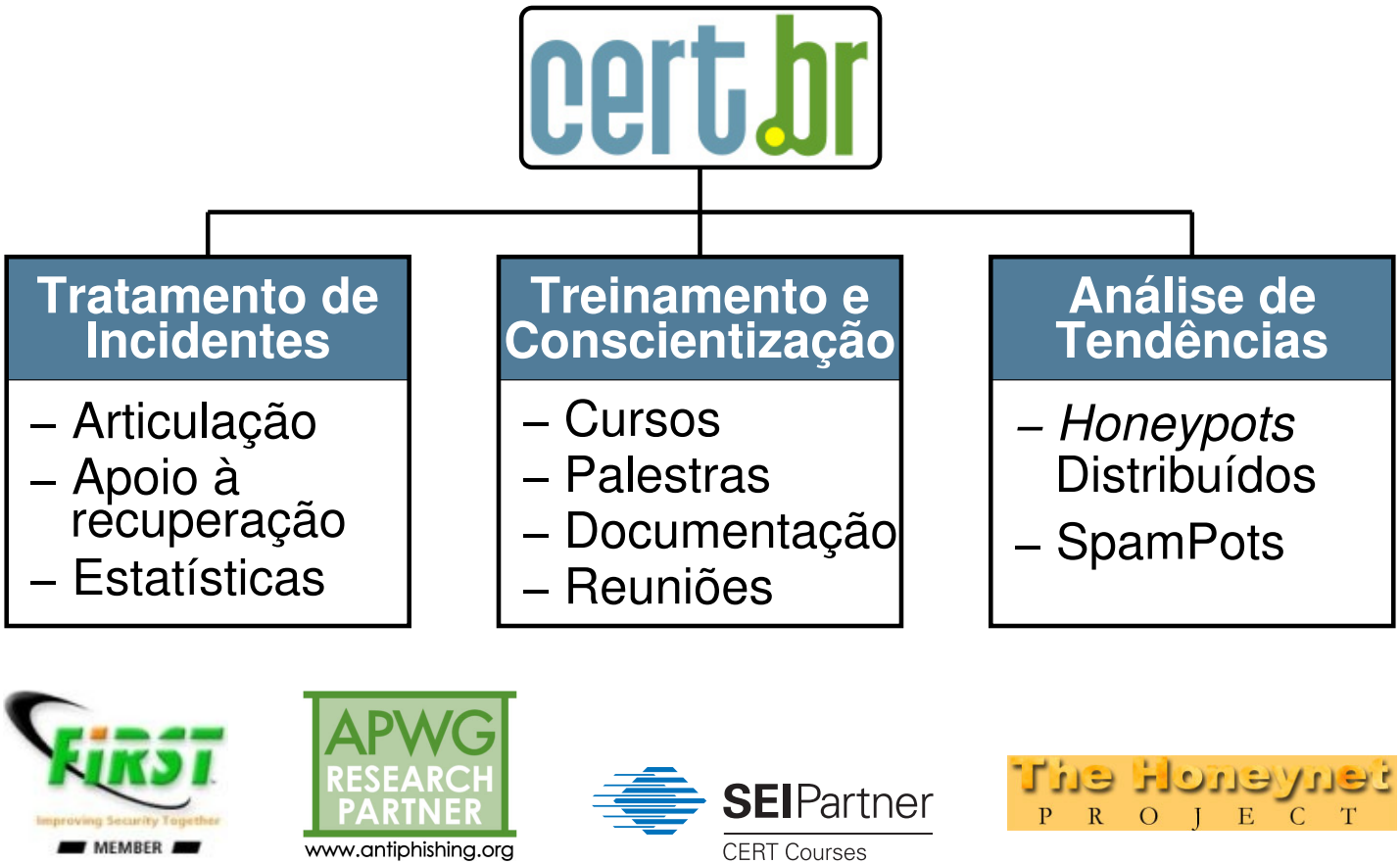
Spywares, *Worms*, *Bots*, Zumbis e outros bichos

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

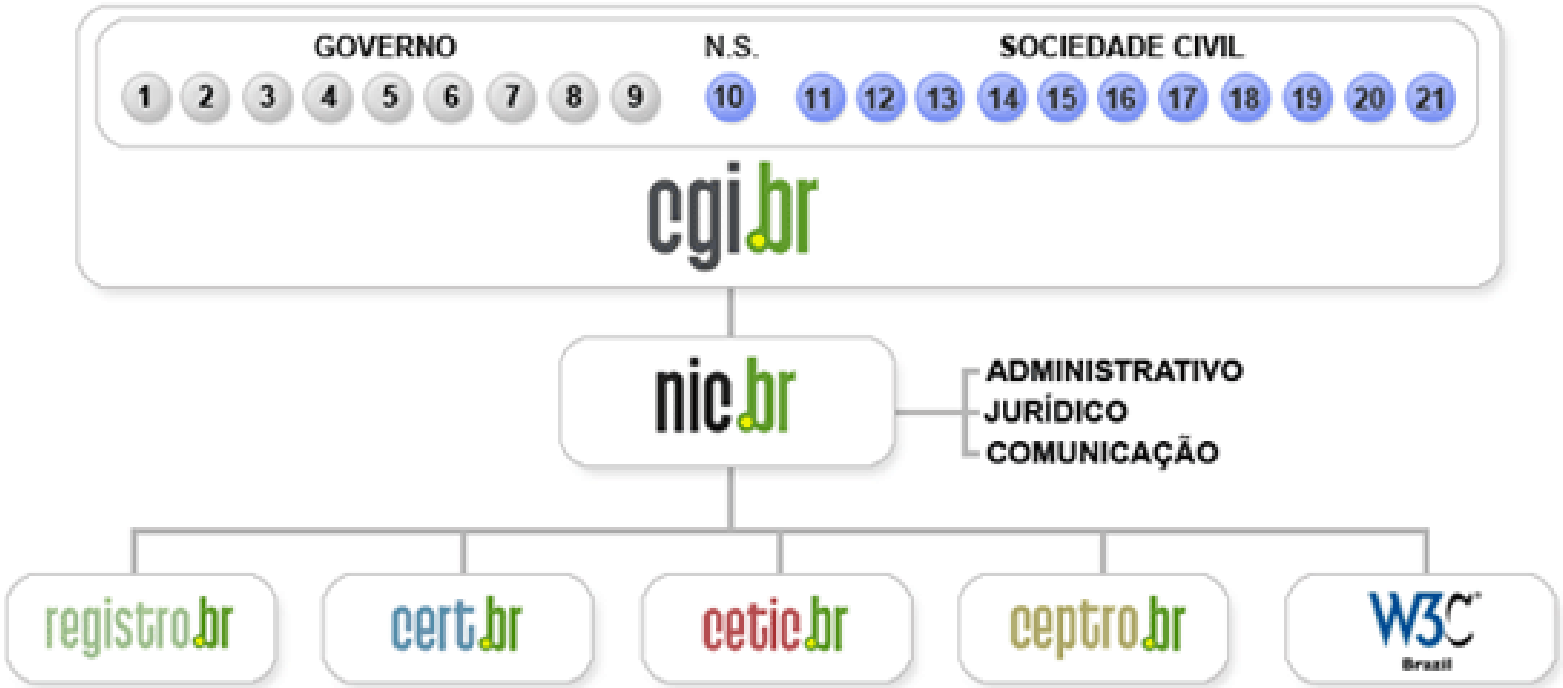
Sobre o CERT.br

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



http://www.cert.br/sobre/

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**

Agenda

- Códigos maliciosos
  - Histórico
  - Principais Tipos
  - Resumo comparativo
- Prevenção
- Referências
- Perguntas

Códigos maliciosos

Códigos maliciosos (1/3)

Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador

Principais tipos:

- Vírus
- *Worm*
- *Bot* e *Botnet*
- *Spyware*
- *Backdoor*
- *Trojan*
- *Rootkit*

Códigos maliciosos (2/3)

Podem infectar um computador, por meio de:

- auto-execução de mídias removíveis infectadas
- acesso a páginas *Web* vulneráveis
- ação direta de atacantes
- execução de arquivos previamente infectados
- exploração de vulnerabilidades existentes nos programas instalados

Podem executar ações no computador, de acordo com as permissões do usuário

Códigos maliciosos (3/3)

Por que são desenvolvidos e propagados:

- vandalismo
- prática de golpes
- realização de ataques
- disseminação de *spams*
- desejo de autopromoção
- obtenção de vantagens financeiras
- coleta de informações confidenciais
- propagação de outros códigos maliciosos

Histórico (1/6)

Década de 1970:

- Surgimento do primeiro vírus (Creeper)
- Programas experimentais
- Não possuíam comportamento destrutivo
- Surgimento do primeiro antivírus (Reaper)

Histórico (2/6)

Década de 1980:

- Surgimento dos primeiros vírus realmente maliciosos
  - Brain: considerado o primeiro
  - Sexta-feira 13 (Jerusálem)
- Surgimento do primeiro *worm* (Morris)
- Principais objetivos dos atacantes:
  - causar danos
  - demonstrar conhecimento técnico
- Surgimento dos antivírus genéricos
- Propagação: *disquetes* e *e-mails*
- Principais alvos: computadores com sistema operacional DOS

Histórico (3/6)

Década de 1990:

- Popularização da Internet
- Grande quantidade de vírus
  - Michelangelo: destaque na mídia
  - Pathogen: primeira condenação
  - Concept: vírus de macro
  - Chernobyl: deletava o acesso a unidade de disco
  - Melissa: grande velocidade propagação
  - LoveLetter: grande prejuízo
- Surgimento dos primeiros boatos sobre vírus
- Surgimento de *kits* para criação de vírus
- Principais objetivos dos atacantes:
  - vantagens financeiras: extorsão, furto de informações
  - envio de *spam*
- Meios de propagação: *e-mails*
- Principais alvos: computadores com Windows e seus aplicativos

Histórico (4/6)

Década de 2000:

- Atacantes com pouco conhecimento técnico
  - uso de ferramentas prontas
- Explosão no número de códigos maliciosos
  - múltiplas funcionalidades
- Década dos *worms*:
  - Nimda e CodeRed: vulnerabilidades do IIS
  - Slammer: vulnerabilidades do SQL Server
  - Blaster: DoS contra o *site* de *update* da Microsoft
  - Sobig: instalava servidor SMTP para se propagar
  - Mydoom: propagação através do Kazaa
  - Koobface: usuários do Facebook e MySpace, via *scraps*

Histórico (5/6)

Década de 2000 (cont.):

- Programas antivírus se tornam *antimalware*
- Popularização das redes sociais:
  - exploração da rede de confiança
  - rápida disseminação de informações
  - utilização de encurtadores de URLs
- Meios de propagação: *e-mails*, mídias removíveis, redes sociais
- Principaia alvos: usuários finais

Histórico (6/6)

Início da década de 2010 até dias atuais:

- Meios de propagação: redes sociais e *e-mails*
- Popularização dos dispositivos móveis
  - grande uso de aplicativos desenvolvidos por terceiros
  - falsa sensação de segurança
- Principais alvos:
  - usuários finais (*Worm* Ramnit)
  - sistemas industriais (*Worm* Stuxnet)
  - alvos específicos (*spear-phishing*)
  - ataques ideológicos (*botnets usadas para DoS*)

Principais Tipos de Códigos Maliciosos

Vírus

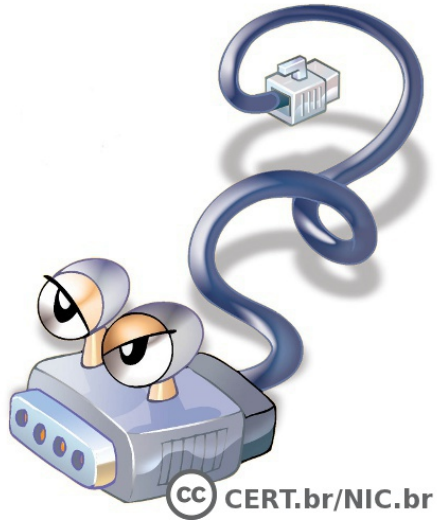
Programa que se
propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador

- depende da execução do programa ou arquivo infectado para ser tornar ativo e continuar o processo de infecção

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

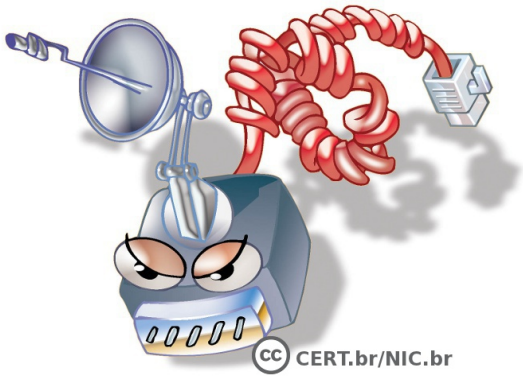
Worm

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 pela exploração de vulnerabilidades existentes em programas instalados em computadores
- consomem muitos recursos
- podem afetar o desempenho de redes e a utilização de computadores

Bot



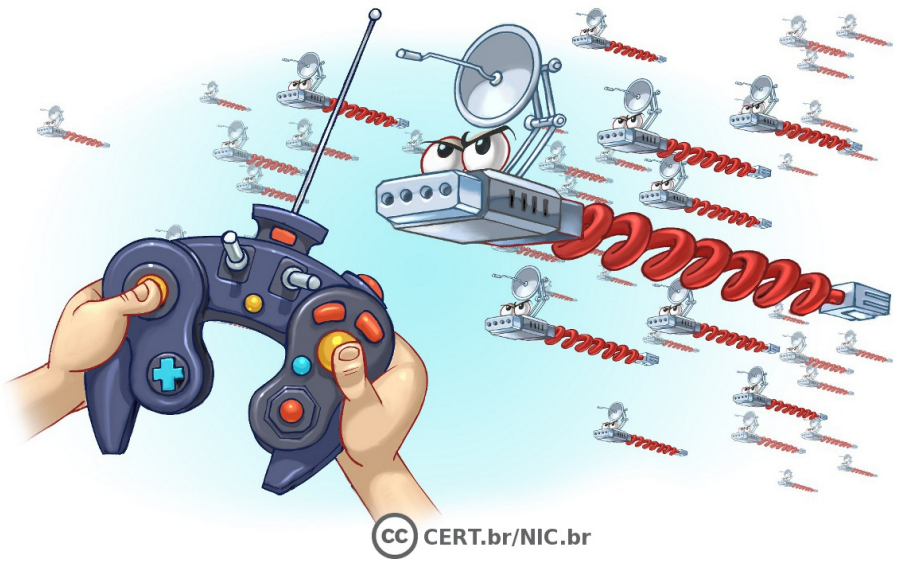
Programa que, além de incluir funcionalidades de *worms*, dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente

- modos de comunicação:
  - canais de IRC, servidores *Web*, compartilhamento de arquivos P2P
- computador zumbi pode ser orientado a:
  - desferir ataques na Internet
  - furtar dados
  - enviar *spam* e *e-mails* de *phishing*

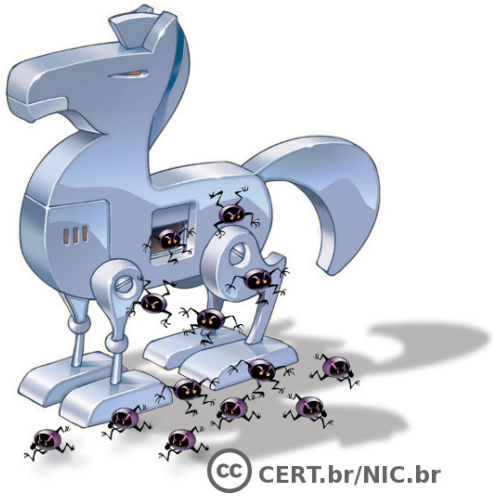
Botnet

Rede composta de centenas/milhares de computadores zumbis

- permite potencializar as ações danosas executadas pelos *bots*
- quanto mais zumbis mais potente ela será
- geralmente usada por aluguel
- associada a: ataques realizados na Internet, disseminação de *spam*, propagação de códigos maliciosos, etc.



Trojan



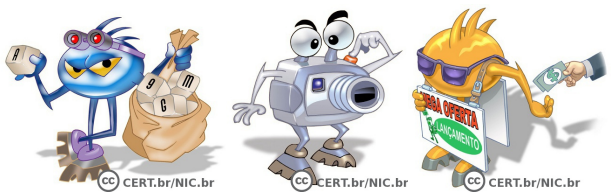
Programa que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções maliciosas sem o conhecimento do usuário

- consiste de um único arquivo
- necessita ser executado para que seja instalado
- não infecta outros arquivos
- não propaga cópias de si mesmo automaticamente
- exemplos: cartão virtual, álbum de fotos, protetor de tela
  - *Trojan Downloader*
  - *Trojan Dropper*
  - *Trojan Backdoor*
  - *Trojan DoS*
  - *Trojan* Destrutivo
  - *Trojan Proxy*
  - *Trojan Spy*
  - *Trojan Banker* ou Bancos

Spyware

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros

- pode ser usado de forma legítima ou maliciosa, dependendo de:
  - como é instalado; das ações realizadas
  - do tipo de informação monitorada
  - do uso que é feito por quem recebe as informações
- tipos:
  - *keylogger*: captura e armazena as teclas digitadas
  - *screenlogger*: armazena a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazena a região que circunda a posição onde o *mouse* é clicado
  - *adware*: projetado especificamente para apresentar propagandas

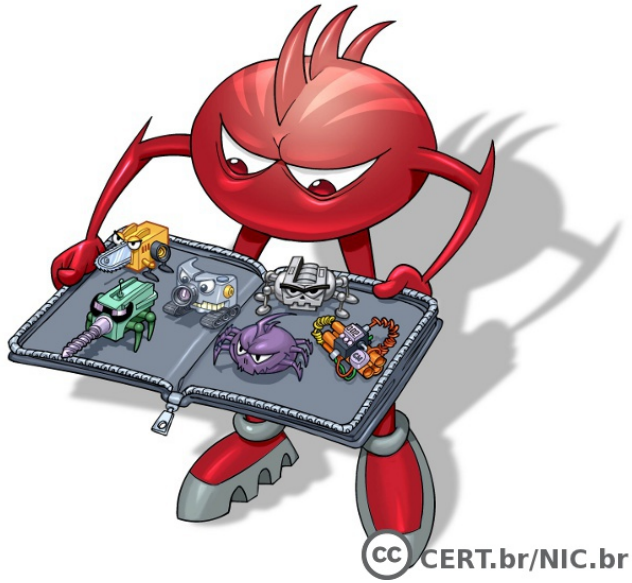


Backdoor

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim

- normalmente incluído de forma a não ser notado
- pode ser incluído:
  - por invasores
  - pela ação de outros códigos maliciosos
- usado para assegurar o acesso futuro, sem que seja necessário recorrer novamente aos métodos usados na infecção ou invasão
- forma de inclusão:
  - disponibilização de um novo serviço
  - substituição de um serviço já existente

Rootkit



Conjunto de programas
e técnicas que permite esconder e assegurar
a presença de um invasor ou de outro código
malicioso em um computador comprometido

- pode ser usado para:
  - remover evidências em arquivos de *logs*
  - instalar outros códigos maliciosos
  - esconder atividades e informações
  - mapear potenciais vulnerabilidades em outros computadores
  - capturar informações da rede
- são usados por:
  - atacantes, para manter acesso privilegiado
  - códigos maliciosos, para ficarem ocultos

Resumo comparativo

Resumo comparativo (1/3)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔

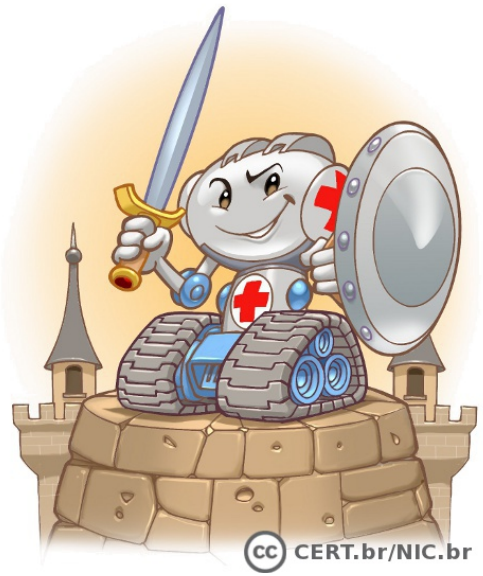
Resumo comparativo (2/3)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópias de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔

Resumo comparativo (3/3)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consume grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Prevenção



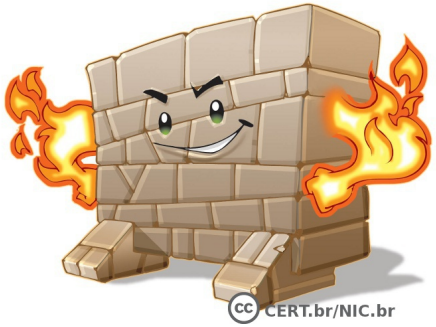
Prevenção (1/4)

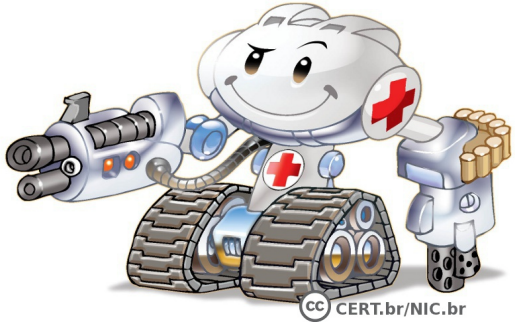
Mantenha seu computador seguro:

- todas as atualizações aplicadas
- todos os programas com as versões mais recentes

Use mecanismos de segurança:

- *firewall* pessoal
- *antiphshing*
- complementos
- *antimalware*
- *antispam*
- *plugins*





Prevenção (2/4)

Use apenas programas originais

Use as configurações de segurança já disponíveis

Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros

- verifique a opinião de outros usuários
- escolha aplicativos populares
- instale *antimalware* antes de qualquer outro programa
- denuncie aplicativos maliciosos

Prevenção (3/4)

Melhore sua postura *online*:

- não acesse *sites* ou siga *links*
  - recebidos por mensagens eletrônicas
  - em páginas sobre as quais não se saiba a procedência
- não confie apenas no remetente da mensagem
  - códigos maliciosos se propagam a partir das contas de máquinas infectadas
  - fraudadores se fazem passar por instituições confiáveis
- não forneça em páginas *Web*, *blogs* e redes sociais
  - dados pessoais ou de familiares e amigos
  - dados sobre o computador ou programas que utiliza
  - informações sobre o seu cotidiano
  - informações sensíveis (senhas e números de cartão de crédito)

Prevenção (4/4)

Proteja suas contas e senhas:

- evite 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
- use senhas longas e compostas de letras, números e símbolos
- utilize o usuário Administrador ou `root` somente quando for estritamente necessário
- crie tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador

Informe-se e Mantenha-se Atualizado (1/2)

http://cartilha.cert.br/

INTERNET SEGURA.BR http://internetsegura.br/

http://www.cert.br/rss/certbr-rss.xml

http://twitter.com/certbr

Informe-se e Mantenha-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