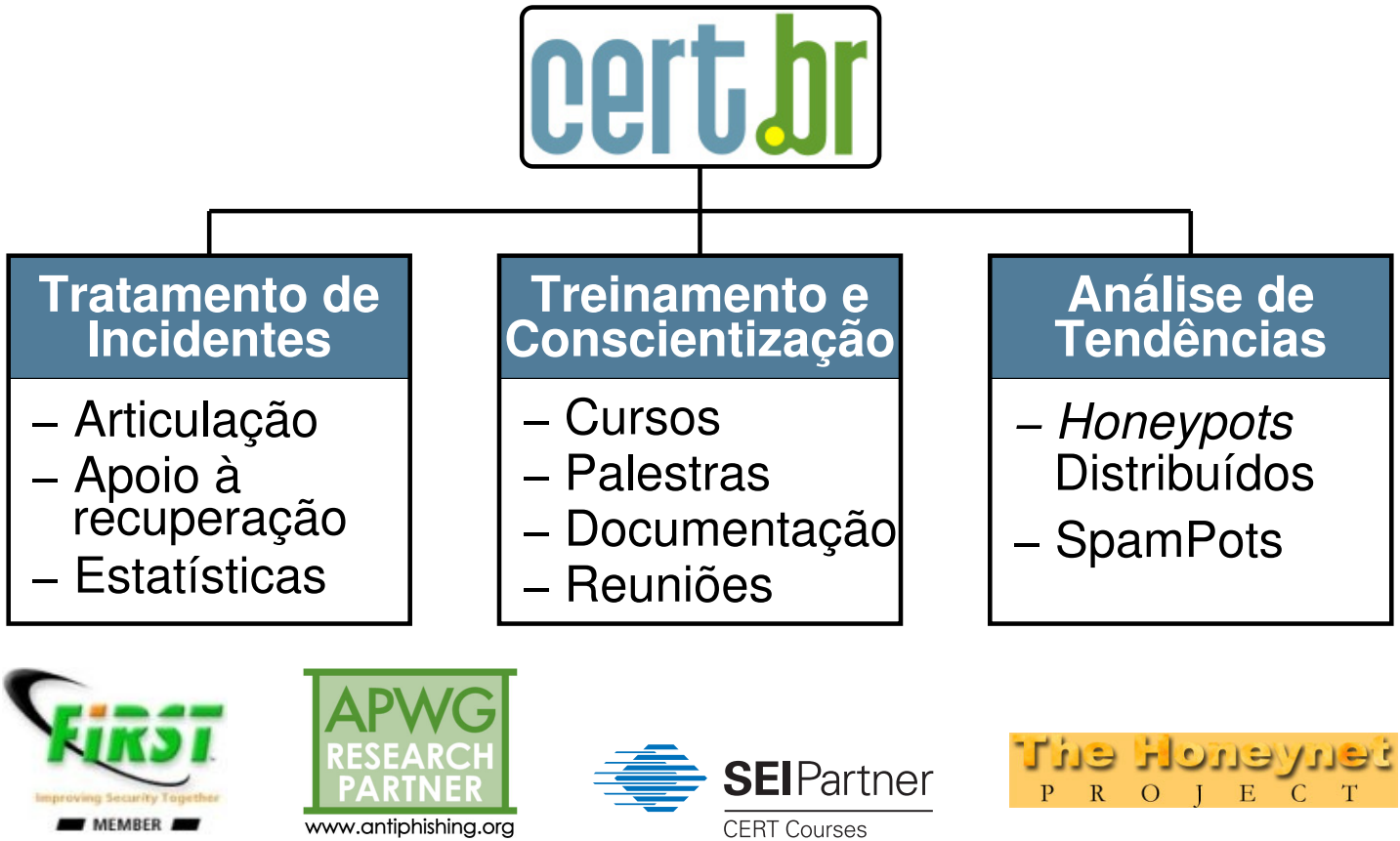
Spywares, *Worms*, *Bots*, Zumbis e outros bichos

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

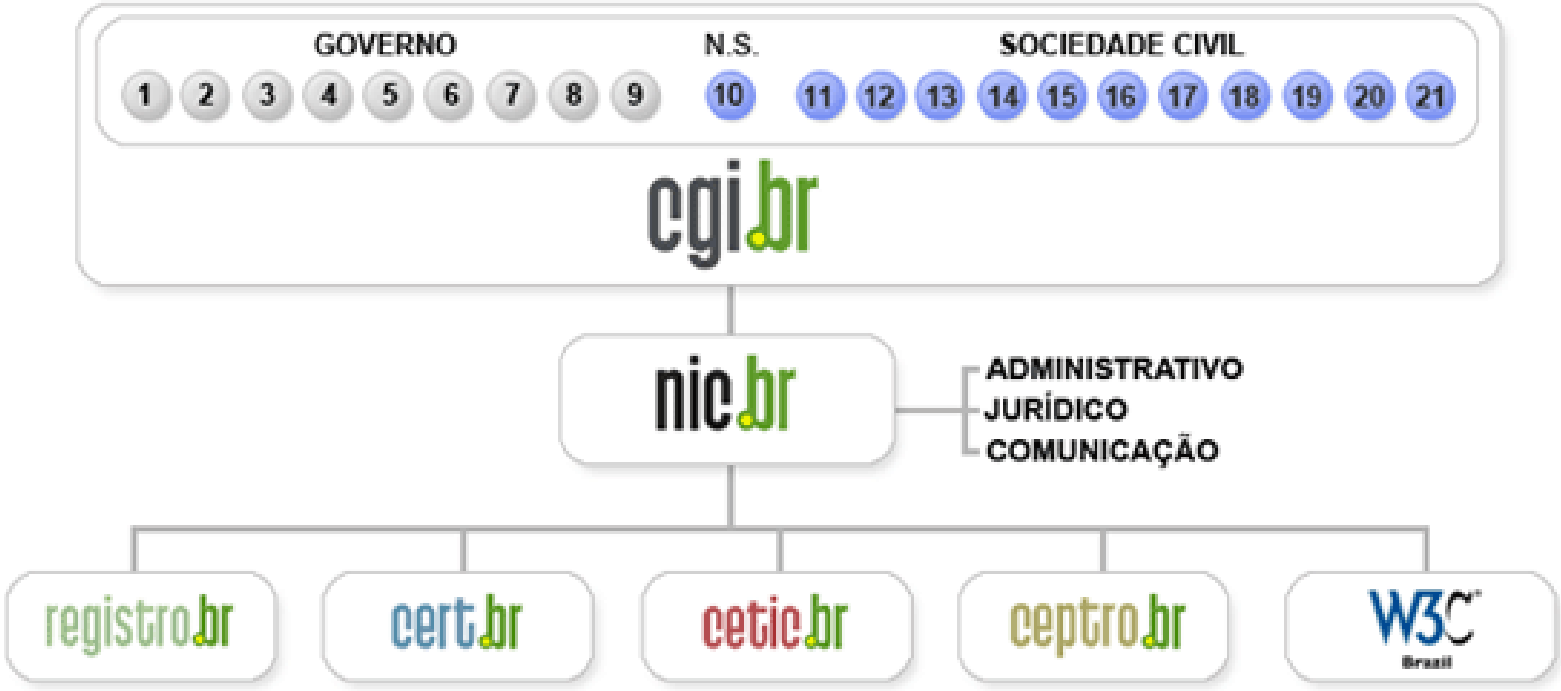
Sobre o CERT.br

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/Bichos/Pragas/*Malware*

Programas especificamente desenvolvidos para executar ações danosas em um computador

Principais tipos:

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

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*
- Principal alvo: 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 de *kits* para criação de vírus
- Principais objetivos dos atacantes:
  - vantagens financeiras: extorsão, furto de informações
  - envio de *spam*
- Propagação: *e-mails*
- Principais alvos: 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* do *update* da Microsoft
  - Sobig: instalava um 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
- Propagação: *e-mails*, mídias removíveis e redes sociais
- Principal alvo: usuários finais

Histórico (6/6)

Início da década de 2010 até dias atuais:

- 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 (1/2)

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 (2/2)

Forma de infecção:

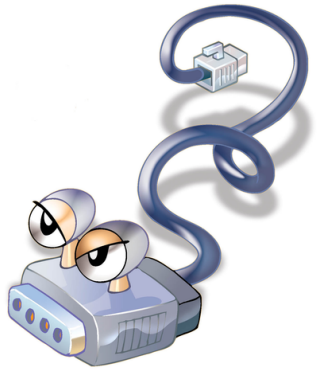
- arquivos anexados aos *e-mails*
- arquivos armazenados em outros computadores
- programas de procedência duvidosa ou desconhecida
- mídia removível (infectada) conectada ao computador, quando ligado

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

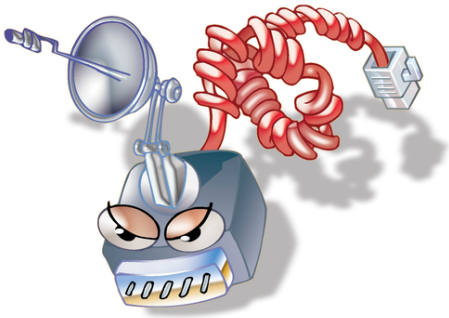
Worm

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

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*

Botnet

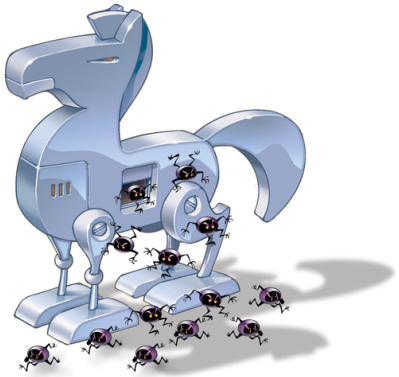
Rede composta de centenas/milhares de computadores infectados por *bots*

- 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*)

Trojan (1/2)



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
- Não propaga cópias de si mesmo automaticamente
- Exemplos: cartão virtual, álbum de fotos, protetor de tela

Trojan (2/2)

Tipos de *trojans*

- *Trojan Downloader*
- *Trojan Dropper*
- *Trojan Backdoor*
- *Trojan DoS*
- *Trojan* Destrutivo
- *Trojan Proxy*
- *Trojan Spy*
- *Trojan Banker* ou Bancos

Spyware

Programa capaz de monitorar atividades do sistema e enviar as informações coletadas para terceiros

- *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 a um invasor retornar a um computador comprometido

- Normalmente incluído de forma a não ser notado
- Pode ser incluído:
  - por invasores
  - pela ação de outros códigos maliciosos
- Forma de inclusão:
  - disponibilização de um novo serviço
  - substituição de um serviço já existente

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
- mas sim para manter o acesso privilegiado em um computador previamente comprometido

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

Mantenha seu computador atualizado

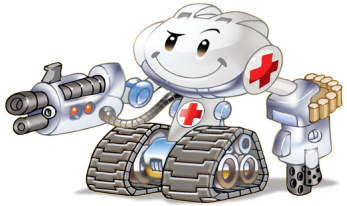
- sistema operacional, aplicativos e *hardware*

Utilize mecanismos de segurança

- *antimalware*
- *firewall* pessoal
- complementos e *plugins* em navegadores *Web*

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



Melhorar a Postura On-line (1/2)

Não acesse *sites* ou seguir *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 *sites* de 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)

Melhorar a Postura On-line (2/2)

Precauções com contas e senhas

- utilize uma senha diferente para cada serviço/*site*
- 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 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

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

http://cartilha.cert.br/

http://internetsegura.br/

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

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