

# CÓDIGOS MALICIOSOS

<Nome>  
<Instituição>  
<e-mail>



fonte: cartilha.cert.br

# Agenda

---

- Códigos maliciosos
- Tipos principais
- Cuidados a serem tomados
- Saiba mais
- Créditos



CC CERT.br/NIC.br

## Códigos maliciosos (1/5)

---

- Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos
- Também chamados de *malware*, pragas, etc.
- Exemplos de equipamentos que podem ser infectados:
  - computadores
  - equipamentos de rede
    - *modems, switches, roteadores*
  - dispositivos móveis
    - *tablets, celulares, smartphones*

## Códigos maliciosos (2/5)

---

- Um equipamento pode ser infectado ou comprometido:
  - pela exploração de vulnerabilidades nos programas instalados
  - pela auto-execução de mídias removíveis infectadas
  - pelo acesso a páginas web maliciosas, via navegadores vulneráveis
  - pela ação direta de atacantes
  - pela execução de arquivos previamente infectados, obtidos:
    - anexos em mensagens eletrônicas
    - via *links* recebidos por mensagens eletrônicas e redes sociais
    - via mídias removíveis
    - em páginas web
    - diretamente de outros equipamentos

## Códigos maliciosos (3/5)

---

- Porque são desenvolvidos e propagados:
  - obtenção de vantagens financeiras
  - coleta de informações confidenciais
  - desejo de autopromoção
  - vandalismo
  - extorsão
- São usados como intermediários, possibilitam:
  - prática de golpes
  - realização de ataques
  - disseminação de *spam*

## Códigos maliciosos (4/5)

---

- **Uma vez instalados:**
  - passam a ter acesso aos dados armazenados no equipamento
  - podem executar ações em nome do usuário
    - acessar informações
    - apagar arquivos
    - criptografar dados
    - conectar-se à Internet
    - enviar mensagens
    - instalar outros códigos maliciosos

## Códigos maliciosos (5/5)

---

- Melhor prevenção
  - impedir que a infecção ocorra
  - nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente os dados

# Tipos principais



fonte: [cartilha.cert.br](http://cartilha.cert.br)

# Vírus



**Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos**

- **Depende da execução do programa/arquivo hospedeiro para:**
  - **tornar-se ativo**
  - **dar continuidade ao processo de infecção**
    - para que o equipamento seja infectado é preciso que um programa já infectado seja executado
- **Principais meios de propagação: e-mail e pen drive**

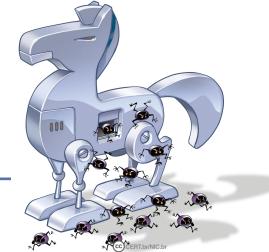
# Tipos mais comuns de vírus



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

# Cavalo de troia/*trojan*

---



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

- **Necessita ser explicitamente executado para ser instalado**
- **Pode ser instalado:**
  - pelo próprio usuário
  - por atacantes
    - após invadirem o equipamento, alteram programas já existentes para executarem ações maliciosas, além das funções originais

# Tipos de *trojans*

---



- ***Trojan Downloader***
- ***Trojan Dropper***
- ***Trojan Backdoor***
- ***Trojan DoS***
- ***Trojan Destruutivo***
- ***Trojan Clicker***
- ***Trojan Proxy***
- ***Trojan Spy***
- ***Trojan Banker (Bancos)***

## Ransomware (1/2)



Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário

- **Dois tipos principais:**
  - *Locker*: impede o acesso ao equipamento
  - *Crypto*: impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia

## Ransomware (2/2)



- Normalmente usa criptografia forte
- Costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também
- Pagamento do resgate (*ransom*) geralmente feito via *bitcoins*
- Reforça a importância de ter *backups*
  - mesmo pagando o resgate não há garantias de que o acesso será restabelecido

## **Backdoor (1/2)**

---

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



## **Backdoor (2/2)**

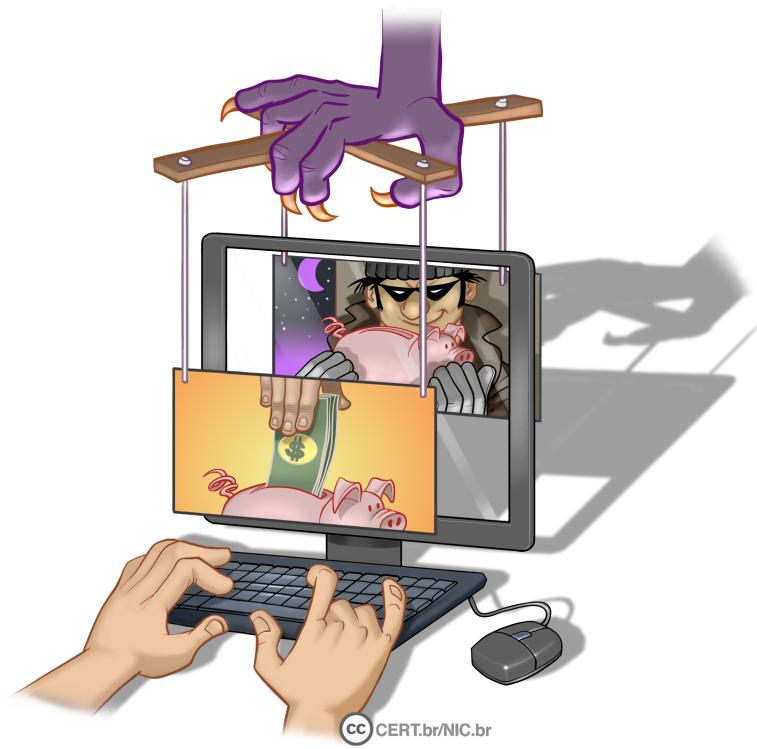


- **Pode ser incluído:**
  - **pela ação de outros códigos maliciosos**
    - que tenham previamente infectado o equipamento
  - **por atacantes**
    - que tenham invadido o equipamento
- **Após incluído:**
  - **usado para assegurar o acesso futuro ao equipamento**
  - **permitindo que seja acessado remotamente**
    - sem ter que recorrer novamente as métodos já usados

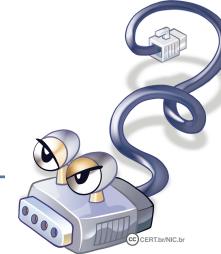
# RAT (*Remote Access Trojan*)

Programa que combina as características de *trojan* e *backdoor*

- Permite ao atacante acessar o equipamento remotamente e executar ações como se fosse o usuário



## **Worm (1/2)**



**Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de equipamento para equipamento**

- **Modo de propagação:**
  - execução direta das cópias
  - exploração automática de vulnerabilidades em programas
- **Consomem muitos recursos**
  - devido à grande quantidade de cópias geradas
  - podem afetar:
    - o desempenho de redes
    - o uso dos equipamentos

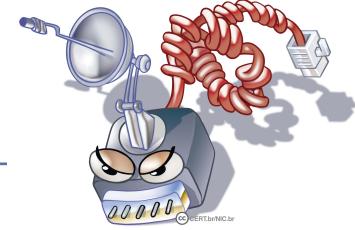
## **Worm (2/2)**



**Processo de propagação e infecção:**

- 1. Identificação dos equipamentos alvos**
- 2. Envio das cópias**
- 3. Ativação das cópias**
- 4. Reinício do processo**

# **Bot**



**Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente**

- **Modo de propagação similar ao worm:**
  - execução direta das cópias
  - exploração automática de vulnerabilidades em programas
- **Comunicação entre o invasor e o equipamento infectado pode ocorrer via:**
  - canais de IRC
  - servidores web
  - redes P2P, etc.

# Zumbi

---

Zumbi é como também é chamado um equipamento infectado por um *bot*, pois pode ser controlado remotamente, sem o conhecimento do seu dono



# **Botnet**

---

**Rede formada por centenas ou milhares de equipamentos zumbis e que permite potencializar as ações danosas dos bots**

- O controlador da **botnet** pode:
  - usá-la para seus próprios ataques
  - alugá-la para outras pessoas ou grupos que desejem executar ações maliciosas específicas



# **Spyware**

---

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



# Tipos de *spyware*

---

- **Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento
- **Screenlogger:** capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado
- **Adware:** projetado para apresentar propagandas

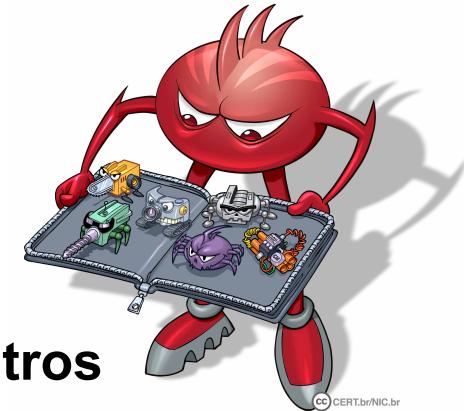


# **Rootkit**

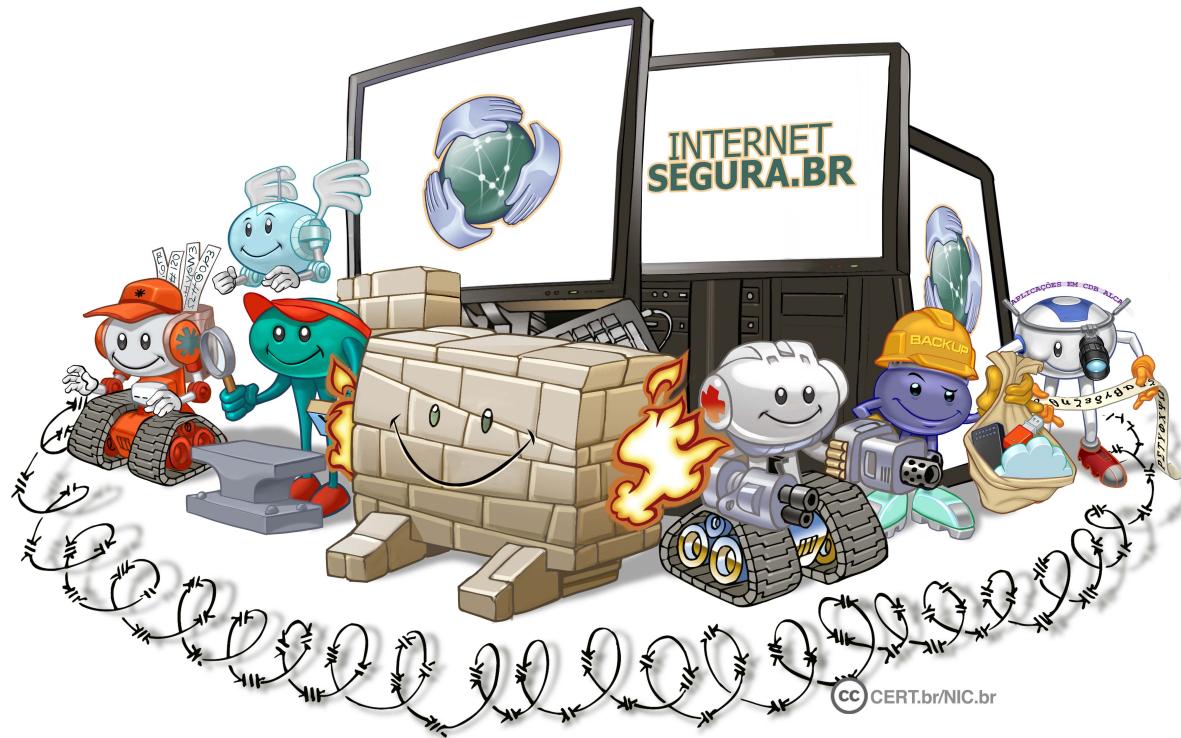
---

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

- **Pode ser usado para:**
  - remover evidências em arquivos de *logs*
  - instalar outros códigos maliciosos
  - esconder atividades e informações
  - capturar informações da rede
  - mapear potenciais vulnerabilidades em outros equipamentos



# Cuidados a serem tomados



# Mantenha os equipamentos atualizados (1/2)

---

- Use apenas programas originais
- Tenha sempre as versões mais recentes dos programas
- Configure os programas para serem atualizados automaticamente
- Remova:
  - as versões antigas
  - os programas que você não utiliza mais
    - programas não usados tendem a:
      - ser esquecidos
      - ficar com versões antigas e potencialmente vulneráveis

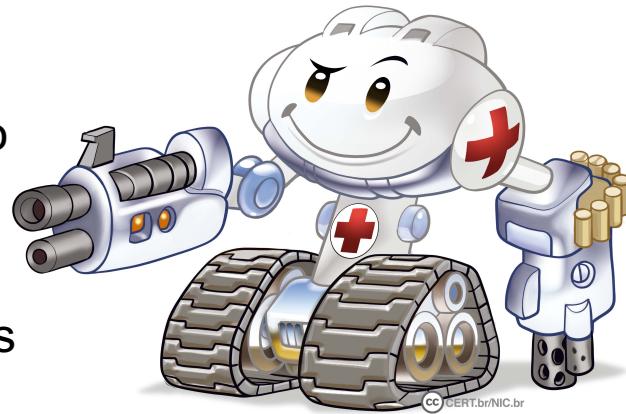
## Mantenha os equipamentos atualizados (2/2)

---

- Programe as atualizações automáticas para serem baixadas e aplicadas em um horário em que o equipamento esteja ligado e conectado à Internet
- Cheque periodicamente por novas atualizações usando as opções disponíveis nos programas
- Crie um disco de recuperação de sistema
  - certifique-se de tê-lo por perto no caso de emergências

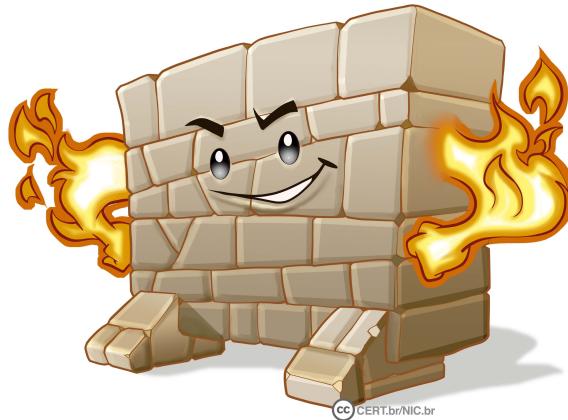
# Use mecanismos de proteção (1/2)

- Instale um antivírus (*antimalware*)
  - mantenha-o atualizado, incluindo o arquivo de assinaturas
    - atualize o arquivo de assinaturas pela rede, de preferência diariamente
  - configure-o para verificar automaticamente:
    - toda e qualquer extensão de arquivo
    - arquivos anexados aos e-mails e obtidos pela Internet
    - discos rígidos e unidades removíveis
  - verifique sempre os arquivos recebidos antes de abri-los ou executá-los



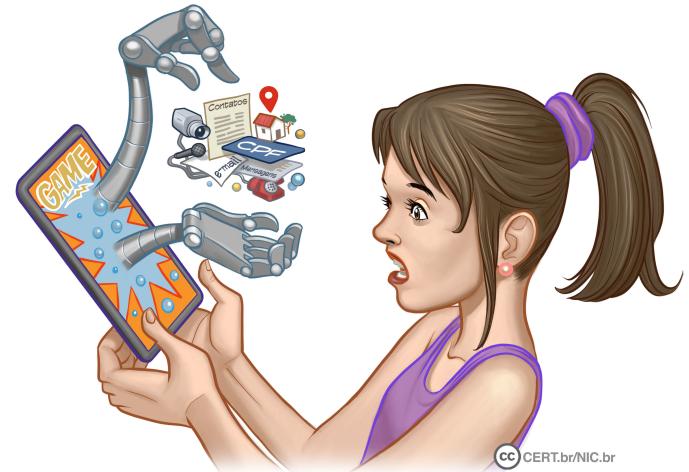
## Use mecanismos de proteção (2/2)

- Crie um disco de emergência de seu antivírus
  - use-o se desconfiar que:
    - o antivírus instalado está desabilitado ou comprometido
    - o comportamento do equipamento está estranho
      - mais lento
      - gravando ou lendo o disco rígido com muita frequência, etc.
- Assegure-se de ter um *firewall* pessoal instalado e ativo



# Ao instalar aplicativos de terceiros

- Verifique se as permissões de instalação e execução são coerentes
- Seja cuidadoso ao:
  - permitir que os aplicativos acessem seus dados pessoais
  - selecionar os aplicativos, escolhendo aqueles:
    - bem avaliados
    - com grande quantidade de usuários



CC CERT.br/NIC.br

# Faça *backups* regularmente (1/3)

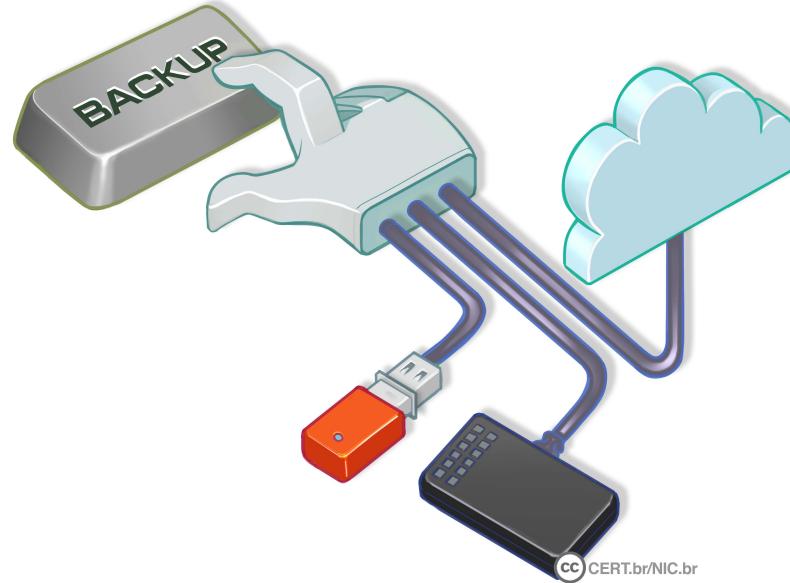
- Mantenha os *backups* atualizados
  - de acordo com a frequência de alteração dos dados
- Configure para sejam feitos automaticamente
  - certifique-se de que estejam realmente sendo feitos
- Mantenha várias cópias
  - *backups* redundantes
  - para evitar perder seus dados:
    - em incêndio, inundação, furto ou pelo uso de mídias defeituosas
    - caso uma das cópias seja infectada



CERT.br/NIC.br

## Faça *backups* regularmente (2/3)

- Assegure-se de conseguir recuperar seus *backups*
- Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis
- Mantenha os *backups* desconectados do sistema



## Faça *backups* regularmente (3/3)



*Backup é a solução  
mais efetiva contra  
ransomware*

# Seja cuidadoso ao clicar em *links*

---

- Antes de clicar em um *link* curto:
  - use complementos que permitam visualizar o *link* de destino
- Mensagens de conhecidos nem sempre são confiáveis
  - o campo de remetente do e-mail pode ter sido falsificado, ou
  - podem ter sido enviadas de contas falsas ou invadidas

## Outros

---

- **Use a conta de administrador do sistema apenas quando necessário**
  - a ação do código malicioso será limitada às permissões de acesso do usuário que estiver acessando o sistema
- **Cuidado com extensões ocultas**
  - alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos conhecidos
- **Desabilite a auto-execução de:**
  - mídias removíveis
  - arquivos anexados

## Saiba mais

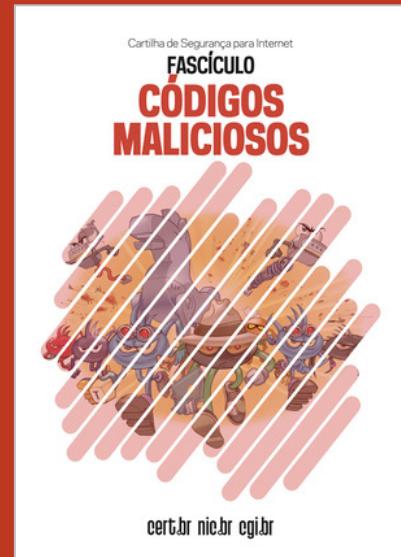
---

- Consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet: [cartilha.cert.br](http://cartilha.cert.br)
- Confira os demais materiais sobre segurança para os diferentes públicos: [internetsegura.br](http://internetsegura.br)
- Acompanhe novidades e a dica do dia no Twitter do CERT.br  
[twitter.com/certbr](http://twitter.com/certbr)



# Créditos

- Cartilha de Segurança para Internet  
Fascículo Códigos Maliciosos  
[cartilha.cert.br/fasciculos](http://cartilha.cert.br/fasciculos)
- Livro Segurança na Internet  
[cartilha.cert.br/livro](http://cartilha.cert.br/livro)



**cert.br nic.br egij.br**