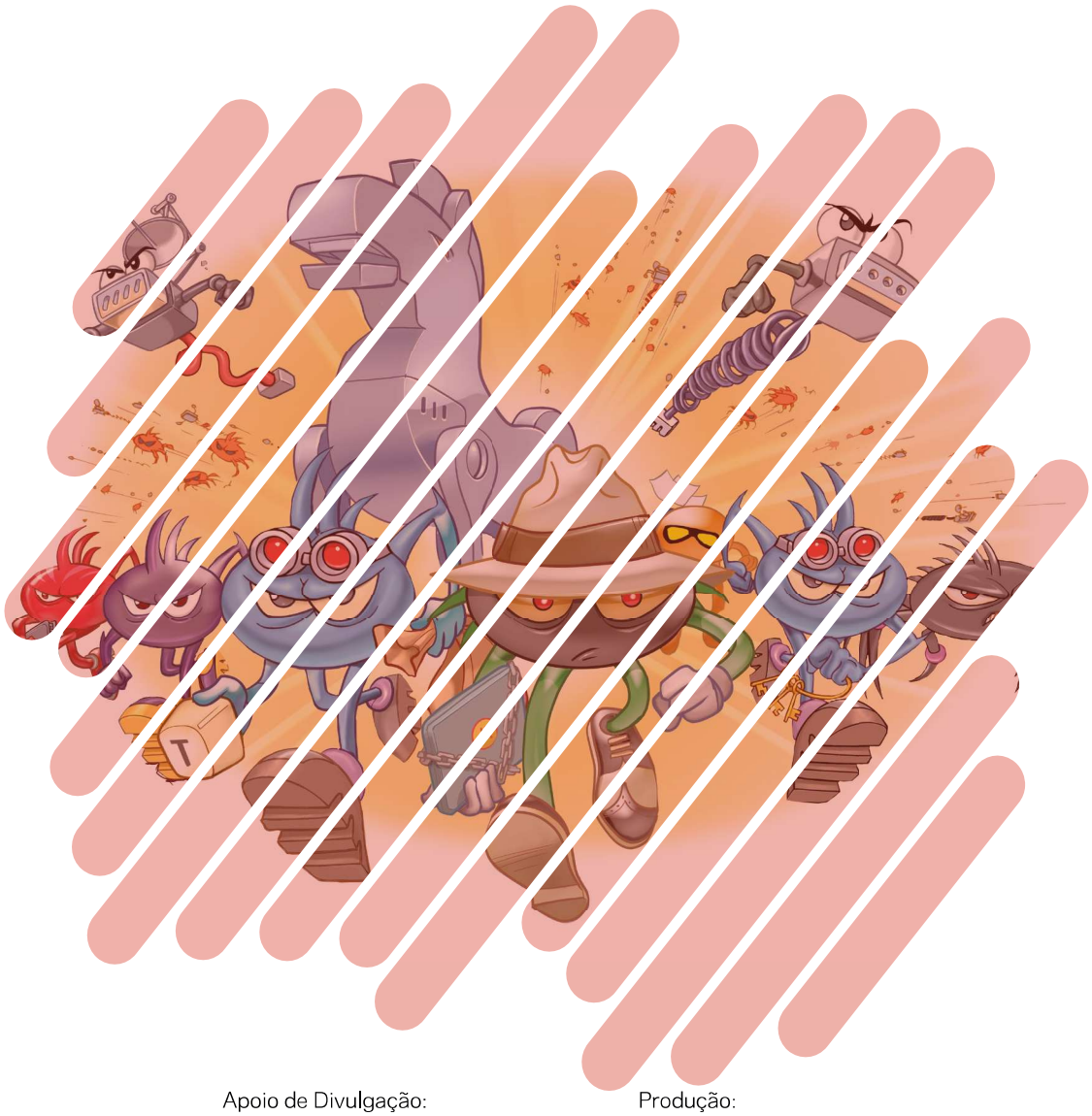
Cartilha de Segurança para Internet

# FASCÍCULO

# CÓDIGOS MALICIOSOS



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

# CÓDIGOS MALICIOSOS SÃO USADOS COMO INTERMEDIÁRIOS E POSSIBILITAM A PRÁTICA DE GOLPES, A REALIZAÇÃO DE ATAQUES E O ENVIO DE *SPAM*

Códigos maliciosos, também conhecidos como pragas e *malware*, são programas desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos, como computadores, *modems*, *switches*, roteadores e dispositivos móveis (*tablets*, celulares, *smartphones*, etc).

Um atacante pode instalar um código malicioso após invadir um equipamento ou explorando alguma vulnerabilidade existente nos programas nele instalados.

Seus equipamentos também podem ser infectados caso você:

- acesse páginas *web* maliciosas, usando navegadores vulneráveis
- acesse mídias removíveis infectadas, como *pen drives*
- execute arquivos infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *web*, redes sociais ou diretamente de outros equipamentos.

Após infectar o seu equipamento, o código malicioso pode executar ações como se fosse você, como acessar informações, apagar arquivos, criptografar dados, conectar-se à Internet, enviar mensagens e ainda instalar outros códigos maliciosos.

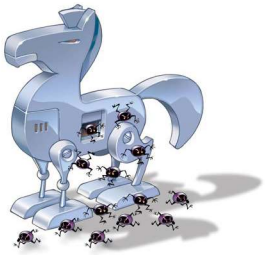
A melhor prevenção contra os códigos maliciosos é impedir que a infecção ocorra pois nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente seus dados.

## CÓDIGOS MALICIOSOS: PROTEJA-SE DESTA TURMA

# TIPOS PRINCIPAIS

## 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



## CAVALO DE TROIA (*TROJAN*)

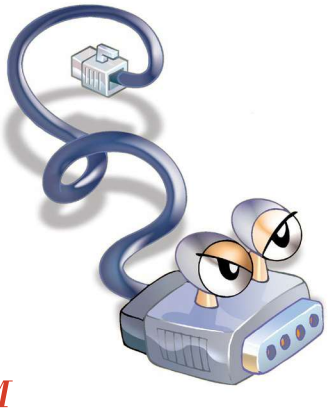
programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário

## *RANSOMWARE*

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

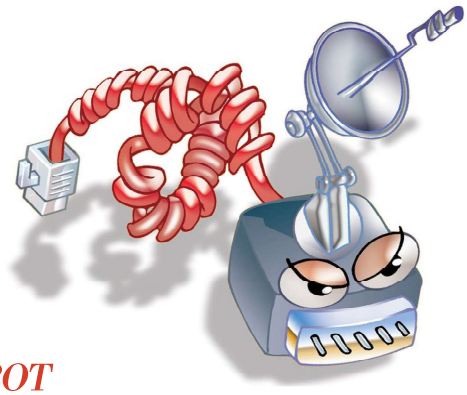
## *BACKDOOR*

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



## *WORM*

programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento



## *BOT*

programa similar ao *worm* e que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado

## RAT (*REMOTE ACCESS TROJAN*)

ou *trojan* de acesso remoto, é um programa que combina as características de *trojan* e de *backdoor*, já que permite ao atacante acessar o equipamento remotamente e executar ações como se fosse o usuário

## ZUMBI

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

## BOTNET

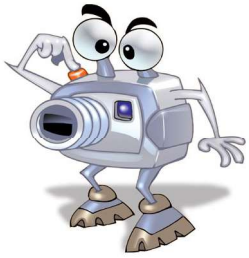
é uma rede formada por centenas ou milhares de equipamentos zumbis e que permite potencializar as ações danosas executadas pelos *bots*

## *SPYWARE*

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

## *KEYLOGGER*

é um tipo de *spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento

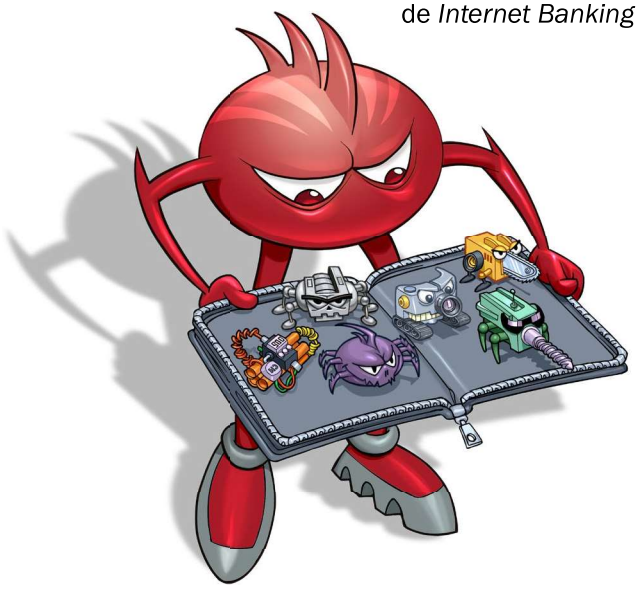


## *SCREENLOGGER*

é um tipo de *spyware*, similar ao *keylogger*, usado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*


## *ADWARE*

é um tipo de *spyware* projetado especificamente 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

# CUIDADOS A SEREM TOMADOS

## MANTENHA SEUS EQUIPAMENTOS ATUALIZADOS

» Use apenas programas originais

» Tenha sempre as versões mais recentes dos programas instalados

» Instale todas as atualizações disponíveis, principalmente as de segurança

» Crie um disco de recuperação e tenha-o por perto no caso de emergências

## INSTALE UM ANTIVÍRUS (*ANTIMALWARE*)

» Mantenha o antivírus atualizado, incluindo o arquivo de assinaturas

- atualize o arquivo de assinaturas pela rede, de preferência diariamente

» Configure o antivírus para verificar automaticamente toda e qualquer extensão de arquivo, arquivos anexados aos *e-mails*, obtidos pela Internet e os discos rígidos e as unidades removíveis

» Verifique sempre os arquivos recebidos, antes de abri-los ou executá-los

» Evite executar simultaneamente diferentes antivírus

- eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro

» Crie um disco de emergência de seu antivírus

- use-o se desconfiar que o antivírus instalado está desabilitado/comprometido ou que o comportamento do equipamento está estranho

## USE UM *FIREWALL* PESSOAL

» Assegure-se de ter um *firewall* pessoal instalado e ativo

» Verifique periodicamente os *logs* do *firewall* à procura de acessos maliciosos

## AO INSTALAR APLICATIVOS

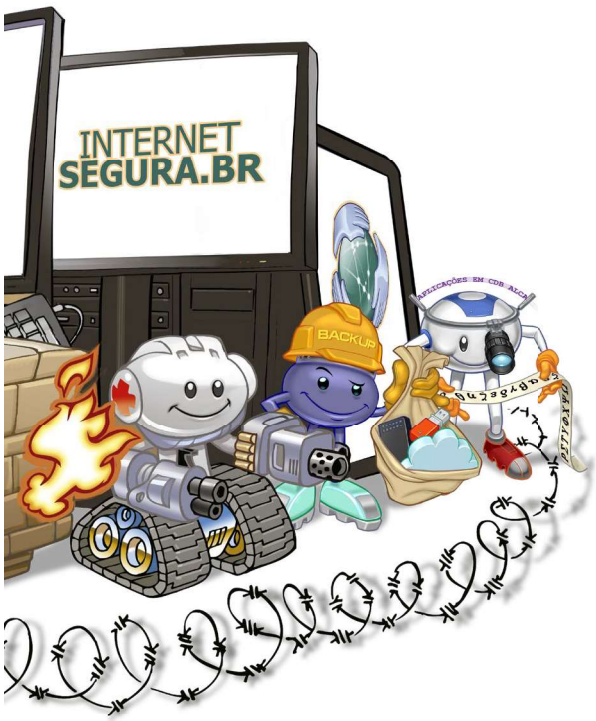
» Baixe aplicativos apenas de fontes confiáveis

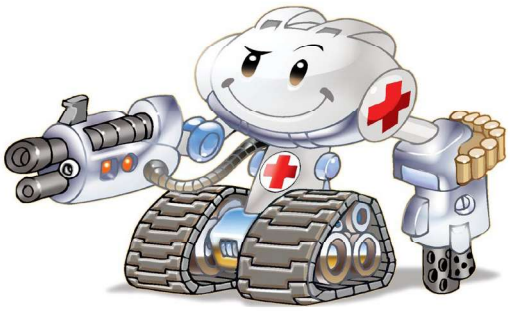
» Verifique se as permissões de instalação e execução são coerentes

» Escolha aplicativos bem avaliados e com grande quantidade de usuários

## FAÇA *BACKUPS*

» Proteja seus dados, fazendo *backups* regularmente



- Nunca recupere um *backup* se desconfiar que ele contenha dados não confiáveis
- Mantenha os *backups* desconectados do sistema

## SEJA CUIDADOSO AO CLICAR EM *LINKS*

» Não considere que mensagens vindas de conhecidos são sempre confiáveis
  - o campo de remetente do *e-mail* pode ter sido falsificado, ou
  - elas podem ter sido enviadas de contas falsas ou invadidas

» Antes de acessar um *link* curto procure usar complementos que permitam visualizar o *link* de destino

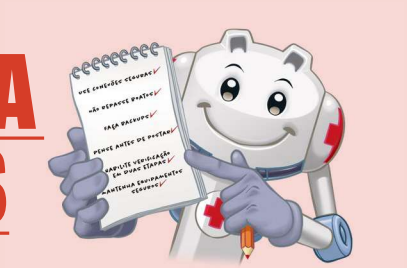
## OUTROS

» Use a conta de administrador apenas quando necessário

» 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 e de arquivos anexados

# SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

## cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

## nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

## cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.



outubro / 2020