Códigos Maliciosos

Apoio de Divulgação:

GUARDIÃO CIBERNÉTICO

Produção:

cert.br nic.br cgi.br

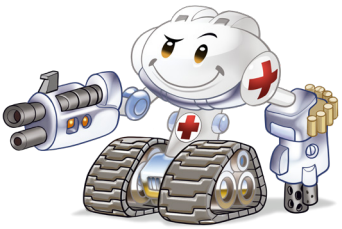
PROTEJA-SE DESTA TURMA!

Códigos maliciosos (*malware*) são usados como intermediários para prática de golpes, realização de ataques e envio de *spam*. A melhor prevenção é impedir a infecção inicial, pois nem sempre é possível reverter ações já feitas ou recuperar dados vazados ou perdidos.

Veja aqui dicas de como se proteger de códigos maliciosos.

COMO SE PROTEGER

UTILIZE MECANISMOS DE PROTEÇÃO



Antivírus (*antimalware*) podem ajudar a detectar, prevenir a infecção e/ou remover *malware*. Mas para serem efetivos contra a infinidade de variantes e novos *malware* que surgem todos os dias, precisam de atualização contínua.

- Escolha um antivírus que melhor se adapte à sua necessidade
- Mantenha o antivírus atualizado
- Configure o antivírus para verificar automaticamente seus arquivos
- Certifique-se de ter um *firewall* pessoal instalado e ativo

Antivírus é nome popular para ferramentas *antimalware*, que atuam sobre diversos tipos de códigos maliciosos (não exclusivamente sobre vírus). Podem incluir funcionalidades extras, como *firewall* pessoal.

MANTENHA OS SISTEMAS E APLICATIVOS ATUALIZADOS

Códigos maliciosos costumam explorar vulnerabilidades em sistemas e aplicativos para infectar dispositivos e se propagar. Aplicar correções de segurança pode evitar que seus dispositivos sejam infectados e usados por atacantes.

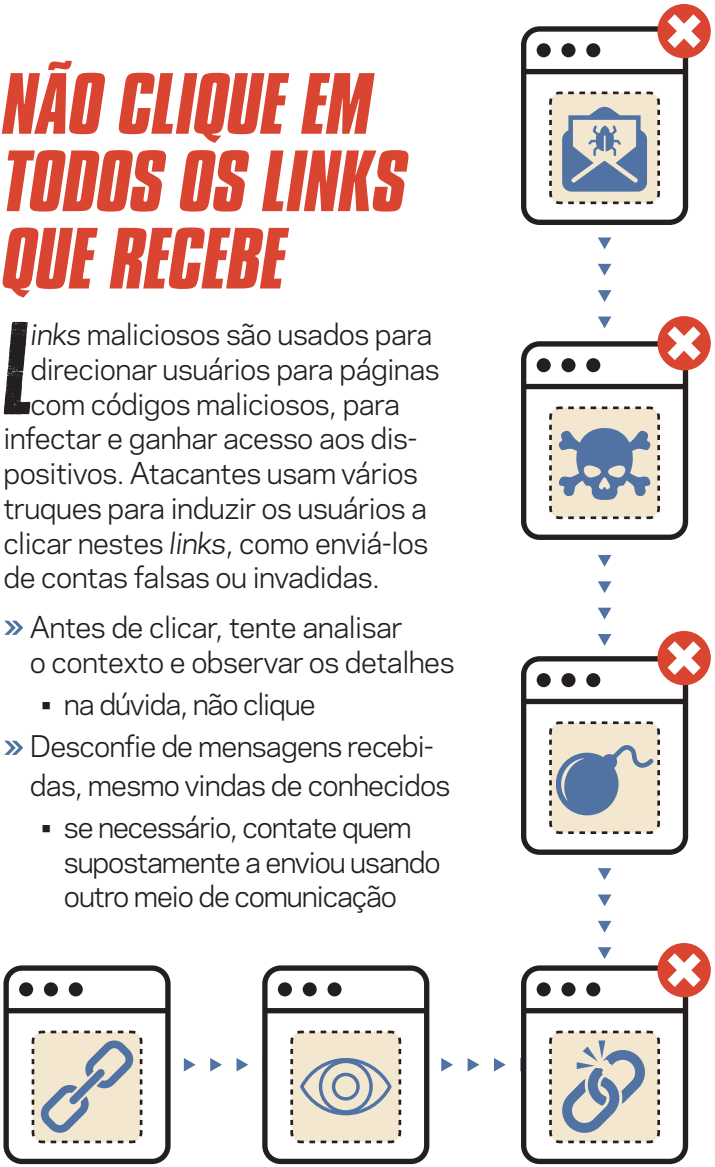
» Instale atualizações regularmente
  - ative a atualização automática, sempre que possível

» Reforce os cuidados caso seu dispositivo já tenha sido infectado, para que não ocorra novamente

NÃO CLIQUE EM TODOS OS LINKS QUE RECEBE

Links maliciosos são usados para direcionar usuários para páginas com códigos maliciosos, para infectar e ganhar acesso aos dispositivos. Atacantes usam vários truques para induzir os usuários a clicar nestes *links*, como enviá-los de contas falsas ou invadidas.

- Antes de clicar, tente analisar o contexto e observar os detalhes
  - na dúvida, não clique
- Desconfie de mensagens recebidas, mesmo vindas de conhecidos
  - se necessário, contate quem supostamente a enviou usando outro meio de comunicação



DESCONFIE SEMPRE DE ARQUIVOS ANEXOS

E-mails com anexos maliciosos são usados por atacantes para instalar *malware*. Podem usar temas que despertam a curiosidade ou serem direcionados para convencer os usuários.

» Cheque o arquivo com antivírus antes de abri-lo

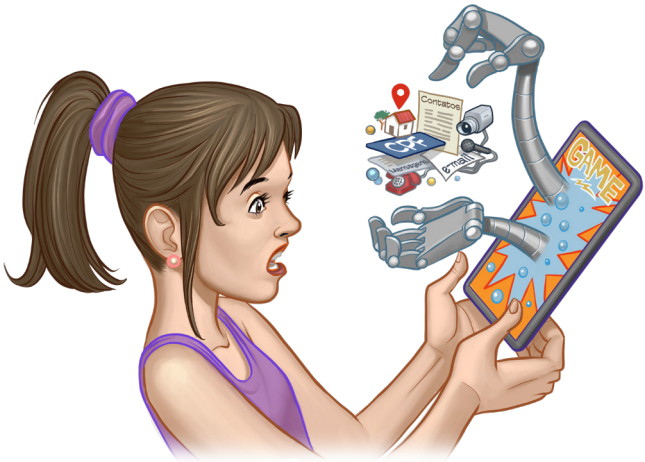
- na dúvida, não abra

BAIXE APLICATIVOS SOMENTE DE LOJAS OFICIAIS

Existem aplicativos para celulares e *tablets* que se passam por legítimos, mas que na verdade possuem códigos maliciosos. As lojas oficiais costumam ter políticas mais rígidas e mecanismos mais rápidos de exclusão destes aplicativos, quando detectados.

» Use apenas a loja oficial do sistema ou do fabricante do dispositivo
  - nunca instale aplicativos recebidos via mensagens ou *links*

» Mesmo assim, cuidado com aplicativos falsos
  - antes de instalar, confirme o nome do aplicativo e se o desenvolvedor é mesmo quem deveria ser

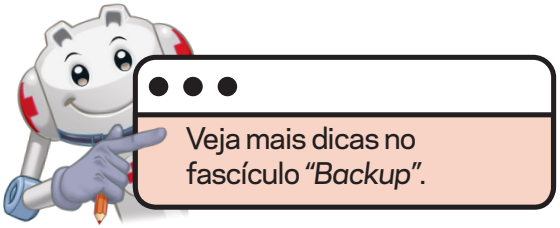


FAÇA BACKUPS

Os dados armazenados em seus dispositivos podem ser perdidos pela ação de códigos maliciosos, como *ransomware*. Ter cópias permite recuperá-los, reduzindo os transtornos.

» Faça cópias periódicas de seus dados

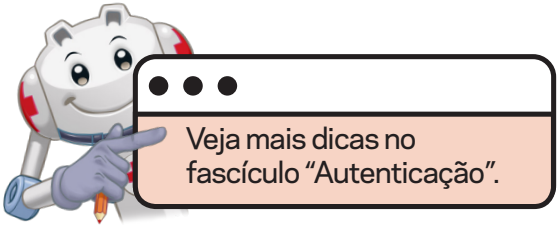
- programe seus *backups* para serem feitos automaticamente, sempre que possível



USE AUTENTICAÇÃO FORTE

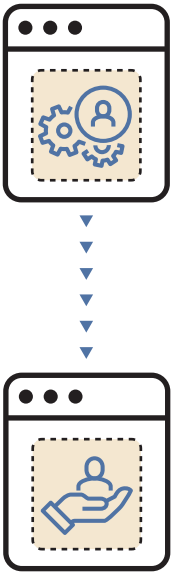
Códigos maliciosos podem capturar e expor suas senhas. Para se prevenir contra vazamentos e acessos indevidos, é importante proteger suas contas com formas adicionais de autenticação.

- Use verificação em duas etapas, sempre que possível
- Não repita senhas
  - uma senha vazada pode levar à invasão de outras contas
- Armazene suas senhas de forma segura
  - não salve no navegador
- Troque imediatamente suas senhas se desconfiar que elas vazaram ou foram usadas em um dispositivo infectado



USE A CONTA DE ADMINISTRADOR APENAS QUANDO NECESSÁRIO

Um *malware* consegue fazer no dispositivo o mesmo que o usuário que o ativou e terá acesso irrestrito se a conta usada for de administrador. Criar contas padrão e usá-las no cotidiano, ajuda a limitar as ações dos códigos maliciosos.



- » Evite usar conta de administrador para atividades cotidianas, como acessar *sites*
- » Use a conta de administrador apenas em situações que exijam tais privilégios
  - volte a usar a conta padrão assim que não precisar mais de acessos privilegiados

Essa recomendação baseia-se em um princípio de segurança conhecido como "privilégio mínimo" e visa evitar danos por uso não autorizado ou erros.

AJA RAPIDAMENTE EM CASO DE SUSPEITAS DE PROBLEMAS

Abriu um arquivo ou clicou no *link* de um *e-mail* e depois descobriu que era *malware*? Seu dispositivo está estranho? Nessas situações é melhor agir rapidamente para evitar problemas maiores.

- Use um antivírus instalado em seu dispositivo ou opções *online*
- Reinicie o dispositivo
  - isso pode ser suficiente para remover o *malware* em casos onde ele fica apenas na memória, como acontece em dispositivos IoT e roteadores de banda larga
- Se não for possível remover o *malware* ou os sintomas persistirem:
  - reinstale o sistema, ou
  - restaure as configurações de fábrica
- Altere as senhas dos serviços que costuma acessar do dispositivo

Reinstalar o sistema ou restaurar as configurações de fábrica, apesar de trabalhosas, são as soluções mais recomendáveis pois nem sempre é possível ter certeza de que o código malicioso foi totalmente excluído.

CONHEÇA OS PRINCIPAIS TIPOS

Códigos maliciosos são programas que executam ações danosas e atividades maliciosas. São muitas vezes chamados genericamente de "vírus", mas existem diversos tipos com características próprias.

Conhecer estas características ajuda a identificar comportamentos estranhos no dispositivo e entender as melhores formas de resolver. Também permite estimar o tipo de dano e como atuar, pois alguns furtam dados, outros cifram seus dispositivos e outros podem ser usados para fraudes.

Conheça aqui alguns dos principais tipos de códigos maliciosos.

VÍRUS

Torna-se parte de programas e arquivos. Propaga-se enviando cópias de si mesmo por *e-mails* e mensagens.

Atualmente não é muito comum, mas seu nome costuma ser usado como sinônimo para qualquer tipo de código malicioso.

RANSOMWARE

Torna inacessíveis os dados armazenados no dispositivo, geralmente usando criptografia, e exige pagamento de resgate para restabelecer o acesso ao usuário e não vazar os dados.

Após infectar o dispositivo, exibe uma mensagem informando ao usuário o procedimento a ser seguido para restabelecer o acesso, incluindo: valor do resgate (geralmente em criptomoedas), prazo para pagamento, identificação do dispositivo do usuário e forma de contato com o atacante, como um *link* ou endereço de *e-mail*.

SPYWARE

Projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Keylogger, *screenlogger*, *adware* e *stalkerware* são tipos específicos de *spyware* apresentados a seguir.

KEYLOGGER

Captura e armazena as teclas digitadas. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*.

SCREENLOGGER

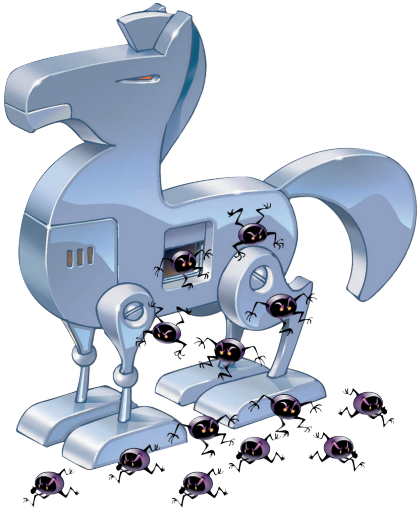
Armazena a posição do cursor e a tela apresentada no monitor, ou a região que circunda determinada posição, nos momentos em que o *mouse* é clicado. Usado para capturar teclas digitadas em teclados virtuais.

ADWARE

Projetado para apresentar propagandas.

STALKERWARE

Projetado para espionar o dono do dispositivo, que não autorizou e não sabe que tal código está instalado. As informações coletadas são enviadas para quem o instalou ou induziu sua instalação (nesse caso, chamado *stalker*).



TROJAN

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

De acordo com a mitologia grega, o *trojan horse* (cavalo de Troia) foi uma estátua usada pelos gregos para acessar a cidade de Troia. Foi recheada com soldados que, durante a noite, saíram e abriram os portões da cidade, permitindo a entrada dos gregos e a dominação de Troia.

BACKDOOR

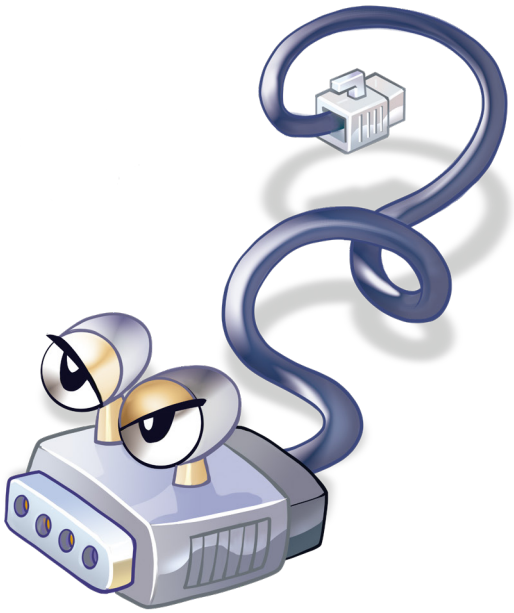
Permite o retorno de um invasor a um dispositivo comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

Pode ser incluído pela ação de outros códigos maliciosos que tenham infectado o dispositivo ou por atacantes que exploram vulnerabilidades no sistema ou aplicativos para invadi-lo.

REMOTE ACCESS TROJAN (RAT)

Trojan de acesso remoto, permite a um atacante remoto acessar um dispositivo infectado de forma direta e interativa.

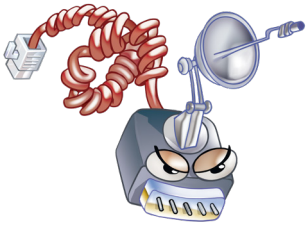
Combina as características de *trojan* e *backdoor*, pois tenta enganar o usuário, assim como o *trojan*, e permite que um atacante acesse remotamente o dispositivo e execute ações como se fosse o usuário, assim como o *backdoor*.



WORM

Propaga-se automaticamente pelas redes, explorando vulnerabilidades nos sistemas e aplicativos instalados e enviando cópias de si mesmo de dispositivo para dispositivo.

É responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de dispositivos.



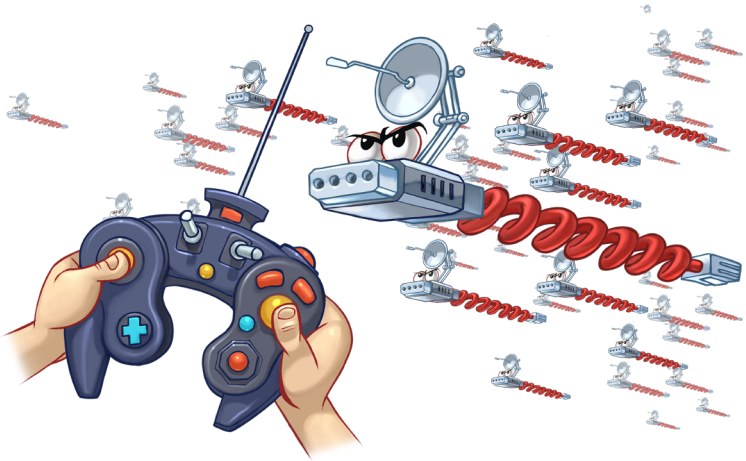
BOT

Similar ao *worm*, possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado. Nome dado ao dispositivo infectado por esse *malware*.

ZUMBI

Outro nome dado ao dispositivo infectado por *bot*.

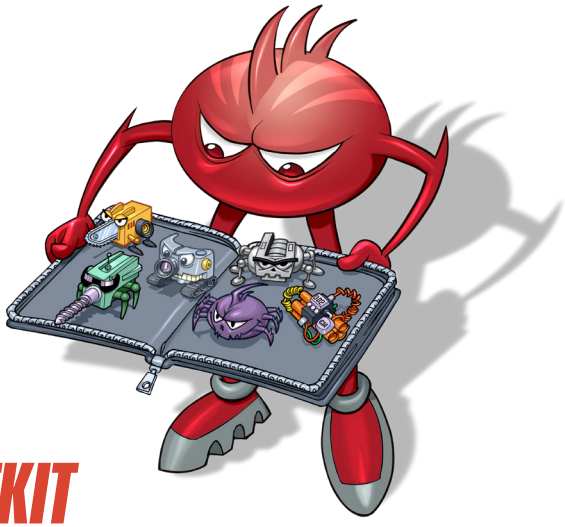
O termo *bot*, originado de *robot* (robô), refere-se genericamente a programas que permitem automatizar tarefas. Conforme o contexto, pode ter significados diferentes, como contas falsas de redes sociais usadas para propagação de boatos.



BOTNET

Rede formada por inúmeros dispositivos zumbis. Permite potencializar as ações danosas executadas pelos *bots*. Quanto mais zumbis participarem da *botnet* e quanto maiores forem as capacidades de conexão e processamento desses zumbis, mais potente ela será.

Algumas ações executadas por meio de *botnets* são: ataques de negação de serviço (DDoS), propagação de *malware* (inclusive do próprio *bot*), coleta de informações pessoais, envio de *spam* e mineração de criptomoeda.



ROOTKIT

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

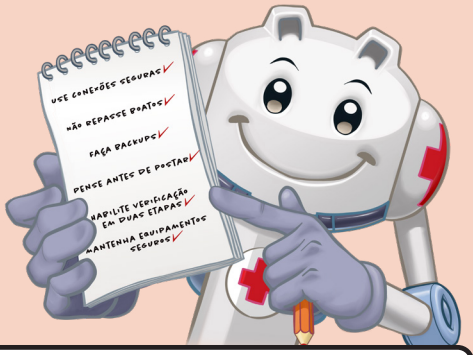
O termo *rootkit* não indica que os programas e as técnicas que o compõem são usadas para obter acesso privilegiado a um dispositivo, mas sim para mantê-lo. Origina-se da junção das palavras "*root*" (conta de superusuário ou administrador do dispositivo em sistemas Unix) e "*kit*" (conjunto de programas usados para manter os privilégios de acesso dessa conta).

SCAREWARE

Usa técnicas de engenharia social para assustar e enganar o usuário, fazendo-o acreditar na existência de um problema de segurança em seu dispositivo e oferecendo uma solução para corrigi-lo, mas que, na verdade, poderá comprometê-lo.

Exemplos de *scareware* são janelas de *pop-up* que informam que o dispositivo está infectado e, para desinfetá-lo, é preciso instalar um (falso) antivírus, que é na verdade um código malicioso.

A exibição da mensagem de alerta não significa que o dispositivo está infectado. A ação executada após a mensagem é que pode fazer isso.



SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **https://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: **https://internetsegura.br/**

cert.br

O CERT.br **(https://cert.br/)** é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

nic.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br **(https://nic.br/)** é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

cgi.br

O Comitê Gestor da Internet no Brasil **(https://cgi.br/)**, 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.

https://cartilha.cert.br/cc/

julho / 2023