

Cartilha de Segurança para Internet

Publicação
cert.br

Fascículo Códigos Maliciosos



<https://cartilha.cert.br/>

nic.br

egi.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

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



A blue worm-like virus with a network cable as its body and a computer monitor head with eyes.


Worm

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

A computer monitor with a red coiled cable as a tongue and a satellite dish antenna on top.

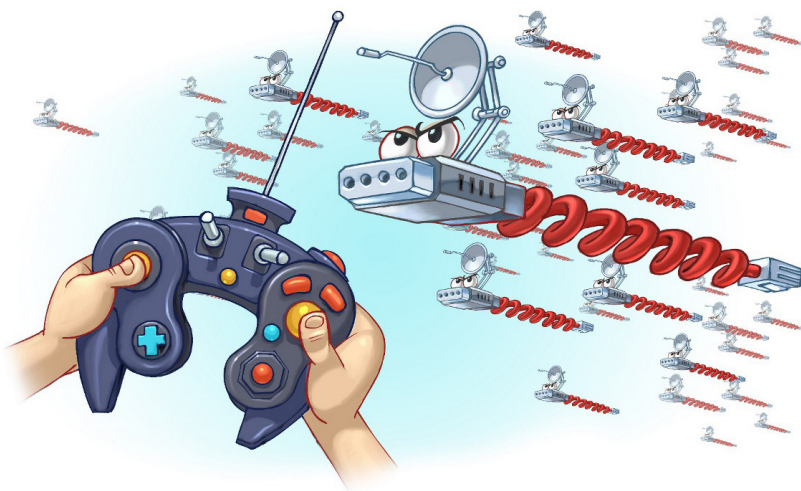
Bot

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

A computer monitor with a red target symbol on the screen and a mouse as a hand.

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

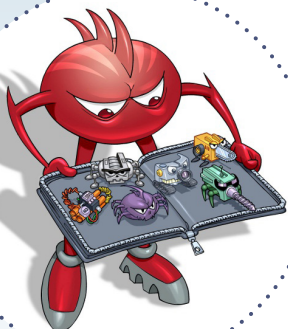


Keylogger é um tipo de *spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento

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

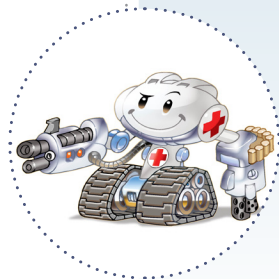


Mantenha seus equipamentos atualizados:

- ✓ 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



Consulte a **Cartilha de Segurança** para a Internet para mais detalhes sobre códigos maliciosos:

<https://cartilha.cert.br/malware/>



Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!

<http://internetsegura.br/>

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

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 <https://www.cert.br/>.

nic.br

Núcleo de Informação e Coordenação do Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (<http://www.nic.br/>) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (<http://www.registro.br/>), estudar e tratar incidentes de segurança no Brasil - CERT.br (<https://www.cert.br/>), estudar e pesquisar tecnologias de redes e operações - CEPTRO.br (<http://www.ceptro.br/>), produzir indicadores sobre as tecnologias da informação e da comunicação - CETIC.br (<http://www.cetic.br/>) e abrigar o escritório do W3C no Brasil (<http://www.w3c.br/>).

cgi.br

Comitê Gestor da Internet no Brasil

O Comitê Gestor 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 de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (<http://www.cgi.br/principios>). Mais informações em <http://www.cgi.br/>.