



Esta obra foi originalmente desenvolvida pelo CERT.br/NIC.br, com o propósito de promover a conscientização sobre o uso seguro da Internet e baseia-se nos materiais da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>).

Esta obra foi licenciada sob a licença Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional (CC BY-NC-SA 4.0).

O CERT.br/NIC.br concede a Você uma licença de abrangência mundial, sem *royalties*, não-exclusiva, sujeita aos termos e condições desta Licença, para exercer os direitos sobre a Obra definidos abaixo:

- Reproduzir a Obra, incorporar a Obra em uma ou mais Obras Coletivas e Reproduzir a Obra quando incorporada em Obras Coletivas;
- Criar e Reproduzir Obras Derivadas, desde que qualquer Obra Derivada, inclusive qualquer tradução, em qualquer meio, adote razoáveis medidas para claramente indicar, demarcar ou de qualquer maneira identificar que mudanças foram feitas à Obra original. Uma tradução, por exemplo, poderia assinalar que "A Obra original foi traduzida do Inglês para o Português," ou uma modificação poderia indicar que "A Obra original foi modificada";
- Distribuir e Executar Publicamente a Obra, incluindo as Obras incorporadas em Obras Coletivas; e,
- Distribuir e Executar Publicamente Obras Derivadas.

Desde que respeitadas as seguintes condições:

- Atribuição** — Você deve fazer a atribuição do trabalho, da maneira estabelecida pelo titular originário ou licenciante (mas sem sugerir que este o apoia, ou que subscreve o seu uso do trabalho). No caso deste trabalho, deve incluir a URL para o trabalho original (Fonte – cartilha.cert.br) em todos os *slides*.
- NãoComercial** — Você não pode usar esta obra para fins comerciais.
- CompartilhaIgual** — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Aviso — Em todas as reutilizações ou distribuições, você deve deixar claro quais são os termos da licença deste trabalho. A melhor forma de fazê-lo, é colocando um *link* para a seguinte página:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR

A descrição completa dos termos e condições desta licença está disponível em:

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pt>

Agenda

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



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

- **Códigos maliciosos:** define o que são códigos maliciosos e os danos que costumam causar.
- **Tipos principais:** apresenta os principais tipos de códigos maliciosos.
- **Cuidados a serem tomados:** apresenta os cuidados a serem tomados para evitar que um equipamento seja infectado ou invadido por códigos maliciosos.
- **Saiba mais:** apresenta materiais de consulta onde você pode buscar mais informações e manter-se informado.
- **Créditos:** apresenta a lista de materiais usados como fonte das informações contidas nestes *slides*.

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



fonte: cartilha.cert.br

Dispositivos móveis, como *tablets*, *smartphones*, celulares e PDAs, têm se tornado cada vez mais populares e capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação *web*, *Internet Banking* e acesso a *e-mails* e redes sociais. Infelizmente, as semelhanças não se restringem apenas às funcionalidades apresentadas, elas também incluem os riscos de uso que podem representar.

Assim como seu computador, o seu dispositivo móvel também pode ser usado para a prática de atividades maliciosas, como furto de dados, envio de *spam* e a propagação de códigos maliciosos, além de poder fazer parte de *botnets* e ser usado para disparar ataques na Internet.

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



fonte: cartilha.cert.br

Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um equipamento são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como *pen drives*;
- pelo acesso a páginas *web* maliciosas, utilizando navegadores *web* vulneráveis;
- pela ação direta de atacantes que, após invadirem o equipamento, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via *links* recebidos por mensagens eletrônicas e redes sociais, via mídias removíveis, em páginas *web* ou diretamente de outros equipamentos (através do compartilhamento de arquivos).

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



fonte: cartilha.cert.br

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção, o vandalismo e a extorsão.

Os equipamentos infectados podem ser usados para a prática de atividades maliciosas, como furto de dados, envio de *spam* e a propagação de códigos maliciosos, além de poder fazer parte de *botnets* e ser usado para disparar ataques na Internet.

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



fonte: cartilha.cert.br

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no equipamento e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.


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




Definir e identificar as características dos diferentes tipos de códigos maliciosos têm se tornado tarefas cada vez mais difíceis, devido às diferentes classificações adotadas pelos fabricantes de antivírus e ao surgimento de variantes que mesclam características dos demais códigos. Dessa forma, as definições apresentadas nos próximos *slides* baseiam-se no entendimento dos autores da Cartilha de Segurança para Internet e, portanto, não são definitivas e podem ser diferentes de outras fontes de consulta.

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**

CÓDIGOS MALICIOSOS  fonte: cartilha.cert.br


Vírus é um 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.


Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu equipamento seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de *e-mail*. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen drives*.

Tipos mais comuns de vírus

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




CÓDIGOS MALICIOSOS fonte: cartilha.cert.br

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

- **Vírus propagado por e-mail:** recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no equipamento.
- **Vírus de *script*:** escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador e do programa leitor de *e-mails*.
- **Vírus de macro:** tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem, como os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).
- **Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS. A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria.


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

CÓDIGOS MALICIOSOS

 fonte: cartilha.cert.br

Cavalo de troia, *trojan* ou *trojan-horse*, é um 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.

Exemplos de *trojans* são programas que você recebe ou obtém de *sites* na Internet e que parecem ser apenas álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no equipamento.

Trojans também podem ser instalados por atacantes que, após invadirem um equipamento, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia.

Tipos de *trojans*

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



CÓDIGOS MALICIOSOS

 fonte: cartilha.cert.br

Há diferentes tipos de *trojans*, classificados de acordo com as ações maliciosas que costumam executar ao infectar um equipamento. Alguns destes tipos são:

- ***Trojan Downloader***: instala outros códigos maliciosos, obtidos de *sites* na Internet.
- ***Trojan Dropper***: instala outros códigos maliciosos, embutidos no próprio código do *trojan*.
- ***Trojan Backdoor***: inclui *backdoors*, possibilitando o acesso remoto do atacante ao equipamento.
- ***Trojan DoS***: instala ferramentas de negação de serviço e as utiliza para desferir ataques.
- ***Trojan Destrutivo***: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
- ***Trojan Clicker***: redireciona a navegação do usuário para *sites* específicos, com o objetivo de aumentar a quantidade de acessos a estes *sites* ou apresentar propagandas.
- ***Trojan Proxy***: instala um servidor de *proxy*, possibilitando que o equipamento seja utilizado para navegação anônima e para envio de *spam*.
- ***Trojan Spy***: instala programas *spyware* e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
- ***Trojan Banker ou Bancos***: coleta dados bancários do usuário, através da instalação de programas *spyware* que são ativados quando *sites* de *Internet Banking* são acessados. É similar ao *Trojan Spy* porém com objetivos mais específicos.

Esta classificação baseia-se em coletânea feita sobre os nomes mais comumente usados pelos programas *antimalware*.

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




CÓDIGOS MALICIOSOS




fonte: cartilha.cert.br

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

CÓDIGOS MALICIOSOS fonte: cartilha.cert.br

O *backdoor* pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o equipamento, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no equipamento para invadi-lo.

Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao equipamento comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como *backdoors*.

Há casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um equipamento que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o equipamento.


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
- **Consumem muitos recursos**
 - devido à grande quantidade de cópias geradas
 - podem afetar:
 - o desempenho de redes
 - o uso dos equipamentos

CÓDIGOS MALICIOSOS


 fonte: cartilha.cert.br

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de equipamento para equipamento.

Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados nos equipamentos.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização 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**


CÓDIGOS MALICIOSOS

 fonte: cartilha.cert.br

O processo de propagação e infecção do *worm* ocorre da seguinte maneira:

- 1. Identificação dos equipamentos alvos:** após infectar um equipamento, o *worm* tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os equipamentos alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras: efetuar varredura na rede e identificar equipamentos ativos; aguardar que outros equipamentos contatem o equipamento infectado; utilizar listas contendo a identificação dos alvos; usar informações contidas no equipamento infectado.
- 2. Envio das cópias:** após identificar os alvos, o *worm* efetua cópias de si mesmo e tenta enviá-las para estes equipamentos, por uma ou mais das seguintes formas: como parte da exploração de vulnerabilidades existentes em programas instalados no equipamento alvo; anexadas a *e-mails*; via canais de IRC (*Internet Relay Chat*); via programas de troca de mensagens instantâneas; incluídas em pastas compartilhadas em redes locais ou do tipo P2P (*Peer to Peer*).
- 3. Ativação das cópias:** após realizado o envio da cópia, o *worm* necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:
 - imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no equipamento alvo no momento do recebimento da cópia;
 - diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu equipamento;
 - pela realização de uma ação específica do usuário, a qual o *worm* está condicionado como, por exemplo, a inserção de uma mídia removível.
- 4. Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o equipamento que antes era o alvo passa a ser também o equipamento originador dos ataques.


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.

CÓDIGOS MALICIOSOS

 fonte: cartilha.cert.br

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados nos equipamentos.

A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer via canais de IRC, servidores *web* e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do equipamento infectado e enviar *spam*.

Zumbi

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



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Um equipamento infectado por um *bot* também pode ser chamado de *spam zombie* quando o *bot* instalado o transforma em um servidor de *e-mails* e o utiliza para o envio de *spam*.

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



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques distribuídos de negação de serviço (DDoS), propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de equipamentos, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

Spyware

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



CÓDIGOS MALICIOSOS

 fonte: cartilha.cert.br

Spyware pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

- **Legítimo:** quando instalado em um equipamento pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.
- **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do equipamento, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

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



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Alguns tipos específicos de programas *spyware* são:

- **Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento. 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:** similar ao *keylogger*, 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. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*.
- **Adware:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

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



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

É importante ressaltar que o nome *rootkit* não indica que os programas e as técnicas que o compõe são usadas para obter acesso privilegiado a um equipamento, mas sim para mantê-lo. O termo *rootkit* origina-se da junção das palavras "*root*" (que corresponde à conta de superusuário ou administrador do equipamento em sistemas Unix) e "*kit*" (que corresponde ao conjunto de programas usados para manter os privilégios de acesso desta conta).



Nos próximos *slides* são apresentados alguns dos principais cuidados que devem ser tomados para proteger seus equipamentos dos códigos maliciosos.

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

CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Fabricantes de programas (*software*) costumam lançar novas versões quando há recursos a serem adicionados e vulnerabilidades a serem corrigidas. Sempre que uma nova versão for lançada, ela deve ser prontamente instalada, pois isto pode ajudar a proteger seu equipamento da ação de atacantes e códigos maliciosos. Além disto, alguns fabricantes deixam de dar suporte e de desenvolver atualizações para versões antigas, o que significa que vulnerabilidades que possam vir a ser descobertas não serão corrigidas.

- Remova programas que você não utiliza mais. Programas não usados tendem a ser esquecidos e a ficar com versões antigas (e potencialmente vulneráveis);
- remova as versões antigas. Existem programas que permitem que duas ou mais versões estejam instaladas ao mesmo tempo. Nestes casos, você deve manter apenas a versão mais recente e remover as mais antigas;
- tenha o hábito de verificar a existência de novas versões, por meio de opções disponibilizadas pelos próprios programas ou acessando diretamente os *sites* dos fabricantes.

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**

CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Quando vulnerabilidades são descobertas, certos fabricantes costumam lançar atualizações específicas, chamadas de *patches*, *hot fixes* ou *service packs*. Portanto, para manter os programas instalados livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis.

- Configure para que os programas sejam atualizados automaticamente;
- programe as atualizações automáticas para serem baixadas e aplicadas em horários em que seu equipamento esteja ligado e conectado à Internet;
- no caso de programas que não possuam o recurso de atualização automática, ou caso você opte por não utilizar este recurso, é importante visitar constantemente os *sites* dos fabricantes para verificar a existência de novas atualizações.

Discos de recuperação são úteis em caso de emergência, como atualizações malsucedidas ou desligamentos abruptos que tenham corrompido arquivos essenciais ao funcionamento do sistema (causados geralmente por queda de energia). Além disso, também podem ocorrer caso seu equipamento seja infectado e o código malicioso tenha apagado arquivos essenciais. Podem ser criados por meio de opções do sistema operacional ou de programas antivírus que ofereçam esta funcionalidade.

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**



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Ferramentas *antimalware* (antivírus, *antispyware*, *antirootkit* e *antitrojan*) são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um equipamento. Entre as diferentes ferramentas existentes, a que engloba a maior quantidade de funcionalidades é o antivírus.

- Configure seu antivírus para verificar todos os formatos de arquivo pois, apesar de inicialmente algumas extensões terem sido mais usadas para a disseminação de códigos maliciosos, atualmente isso já não é mais válido.

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**



CÓDIGOS MALICIOSOS



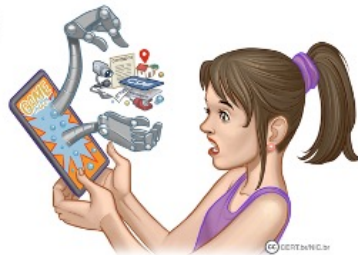
fonte: cartilha.cert.br

Firewall pessoal é um tipo específico de *firewall* que é utilizado para proteger um equipamento contra acessos não autorizados vindos da Internet. Os programas antivírus, apesar da grande quantidade de funcionalidades, não são capazes de impedir que um atacante tente explorar, via rede, alguma vulnerabilidade existente em seu equipamento e nem de evitar o acesso não autorizado. Devido a isto, além da instalação do antivírus, é necessário que você utilize um *firewall* pessoal.

- Verifique periodicamente os *logs* gerados pelo seu *firewall* pessoal, sistema operacional e antivírus (observe se há registros que possam indicar algum problema de segurança).

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



CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Plug-ins, complementos e extensões são programas geralmente desenvolvidos por terceiros e que podem prover funcionalidades extras. Costumam ser disponibilizados em repositórios, onde podem ser baixados livremente ou comprados. Alguns repositórios efetuam controle rígido antes de disponibilizá-los, outros utilizam classificações referentes ao tipo de revisão, enquanto outros não efetuam controle. Apesar de grande parte ser confiável, há a chance de existir programas especificamente criados para executar atividades maliciosas ou que, devido a erros de implementação, possam executar ações danosas em seu equipamento.

- Assegure-se de ter mecanismos de segurança instalados e atualizados, antes de instalar programas desenvolvidos por terceiros;
- mantenha os programas instalados sempre atualizados;
- procure obter arquivos apenas de fontes confiáveis;
- veja comentários de outros usuários sobre o programa, antes de instalá-lo;
- seja cuidadoso ao instalar programas que ainda estejam em processo de revisão;
- denuncie aos responsáveis pelo repositório caso identifique programas maliciosos.

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



CÓDIGOS MALICIOSOS

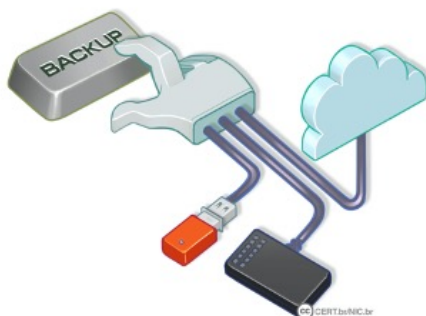


fonte: cartilha.cert.br

- Mantenha *backups* em locais seguros, bem condicionados e com acesso restrito;
- além dos *backups* periódicos, sempre faça *backups* antes de efetuar grandes alterações no sistema e de enviar o equipamento para manutenção;
- armazene dados sensíveis em formato criptografado;
- cuidado com mídias obsoletas;
- assegure-se de conseguir recuperar seus *backups*;
- mantenha seus *backups* organizados e identificados;
- copie dados que você considere importantes e evite aqueles que podem ser obtidos de fontes externas confiáveis, como os referentes ao sistema operacional ou aos programas instalados.

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***

CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

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

CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Alguns mecanismos, como os programas antivírus, são importantes para proteger seu equipamento contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança e, por isto, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas.

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

CÓDIGOS MALICIOSOS



fonte: cartilha.cert.br

Quando um programa é executado, ele herda as permissões da conta do usuário que o executou e pode realizar operações e acessar arquivos de acordo com estas permissões. Se o usuário em questão estiver utilizando a conta de administrador, então o programa poderá executar qualquer tipo de operação e acessar todo tipo de arquivo.


A conta de administrador, portanto, deve ser usada apenas em situações nas quais uma conta padrão não tenha privilégios suficientes para realizar uma operação. E, sobretudo, pelo menor tempo possível.

Muitas pessoas, entretanto, por questões de comodidade ou falta de conhecimento, utilizam esta conta para realizar todo tipo de atividade. Utilizar nas atividades cotidianas uma conta com privilégios de administrador é um hábito que deve ser evitado, pois você pode, por exemplo, apagar acidentalmente arquivos essenciais para o funcionamento do sistema operacional ou instalar inadvertidamente um código malicioso, que terá acesso irrestrito ao seu equipamento.

Tenha cuidado com extensões ocultas. Alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos conhecidos. Exemplo: se um atacante renomear o arquivo "exemplo.scr" para "exemplo.txt.scr", ao ser visualizado o nome do arquivo será mostrado como "exemplo.txt", já que a extensão ".scr" não será mostrada.


Saiba mais

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



A cartoon robot with a white body, blue joints, and a red cross on its chest. It is holding a spiral-bound notepad with a checklist of internet security tips in Portuguese. The tips include: 'USE CONDIÇÃO DE SEGURANÇA', 'NÃO REPACE QUANTO', 'CASA DIGITAL', 'SENHAS ANTES DE POSTAR', 'CAPILITE VERIFICAÇÃO EM DUAS ETAPAS', and 'MANTENHA EQUIPAMENTOS'. The robot is also holding a yellow pencil.

CÓDIGOS MALICIOSOS

 fonte: cartilha.cert.br

Novidades e dicas diárias podem ser obtidas por meio do RSS da Cartilha e do Twitter do CERT.br:


- Twitter: <https://twitter.com/certbr>
- RSS: <https://cartilha.cert.br/rss/cartilha-rss.xml>

No *site* da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>) você encontra diversos materiais, como dicas rápidas sobre vários assuntos e outros fascículos, com temas como Boatos, *Internet Banking*, Senhas e Verificação em Duas Etapas, entre outros.

No *site* Internet Segura (<https://internetsegura.br/>) você encontra materiais de interesse geral e para diversos públicos específicos, como crianças, adolescentes, pais, educadores, pessoas com mais de 60 anos e técnicos. Além dos materiais produzidos pelo NIC.br, há também iniciativas de outras entidades e instituições, com diversas informações sobre uso seguro da Internet.

Créditos

- **Cartilha de Segurança para Internet**
Fascículo Códigos Maliciosos
cartilha.cert.br/fasciculos
- **Livro Segurança na Internet**
cartilha.cert.br/livro



cert.br nic.br egi.br

ESTE SLIDE NÃO PODE SER REMOVIDO. DEVE SER EXIBIDO EM TODAS AS REPRODUÇÕES, INCLUSIVE NAS OBRAS DERIVADAS.

Esta obra foi originalmente desenvolvida pelo CERT.br/NIC.br, com o propósito de promover a conscientização sobre o uso seguro da Internet e baseia-se nos materiais da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>).

Esta obra foi licenciada sob a licença Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional (CC BY-NC-SA 4.0).

O CERT.br/NIC.br concede a Você uma licença de abrangência mundial, sem *royalties*, não-exclusiva, sujeita aos termos e condições desta Licença, para exercer os direitos sobre a Obra definidos abaixo:

- Reproduzir a Obra, incorporar a Obra em uma ou mais Obras Coletivas e Reproduzir a Obra quando incorporada em Obras Coletivas;
- Criar e Reproduzir Obras Derivadas, desde que qualquer Obra Derivada, inclusive qualquer tradução, em qualquer meio, adote razoáveis medidas para claramente indicar, demarcar ou de qualquer maneira identificar que mudanças foram feitas à Obra original. Uma tradução, por exemplo, poderia assinalar que “A Obra original foi traduzida do Inglês para o Português,” ou uma modificação poderia indicar que “A Obra original foi modificada”;
- Distribuir e Executar Publicamente a Obra, incluindo as Obras incorporadas em Obras Coletivas; e,
- Distribuir e Executar Publicamente Obras Derivadas.

Desde que respeitadas as seguintes condições:

- **Atribuição** — Você deve fazer a atribuição do trabalho, da maneira estabelecida pelo titular originário ou licenciante (mas sem sugerir que este o apoia, ou que subscreve o seu uso do trabalho). No caso deste trabalho, deve incluir a URL para o trabalho original (Fonte – cartilha.cert.br) em todos os *slides*.
- **NãoComercial** — Você não pode usar esta obra para fins comerciais.
- **CompartilhaIgual** — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Aviso — Em todas as reutilizações ou distribuições, você deve deixar claro quais são os termos da licença deste trabalho. A melhor forma de fazê-lo, é colocando um *link* para a seguinte página:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR

A descrição completa dos termos e condições desta licença está disponível em:

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pt>