

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

- **Ransomware**
- **Como se prevenir**
- **Outros cuidados a serem tomados**
- **Saiba mais**
- **Créditos**

RANSOMWARE fonte: cartilha.cert.br

- **Ransomware:** define o que é o *ransomware*.
- **Como se prevenir:** apresenta as principais medidas preventivas para evitar o *ransomware*.
- **Outros cuidados a serem tomados:** apresenta os cuidados extras a serem tomados para evitar que os equipamentos sejam infectados com *ransomware*.
- **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*.

Ransomware (1/5)

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



RANSOMWARE



fonte: cartilha.cert.br

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 nestes *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.

Ransomware (2/5)

- **Tipo de código malicioso**
 - assim como *vírus, trojan, backdoor, worm, bot e spyware*
- **Pode infectar:**
 - **computadores**
 - como *desktop, notebook* e servidores
 - **equipamentos de rede**
 - como *modems, switches* e roteadores
 - **dispositivos móveis**
 - como *tablets, celulares* e smartphones



RANSOMWARE



fonte: cartilha.cert.br

Ransomware (3/5)

- **Ações mais comuns**
 - impede o acesso ao equipamento (*Locker ransomware*)
 - impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia (*Crypto ransomware*)
- **Extorsão é o principal objetivo dos atacantes**
 - pagamento feito geralmente via *bitcoins*
 - não há garantias de que o acesso será restabelecido
 - mesmo que o resgate seja pago
 - normalmente usa criptografia forte
- **Costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também**

RANSOMWARE



fonte: cartilha.cert.br

Ransomware (4/5)

- **Infecção pode ocorrer pela execução de arquivo infectado:**
 - **recebido:**
 - via *links* em *e-mails*, redes sociais e mensagens instantâneas
 - anexado a *e-mails*
 - **baixado de sites na Internet**
 - **acessado:**
 - via arquivos compartilhados
 - via páginas *web* maliciosas, usando navegadores vulneráveis

RANSOMWARE



fonte: cartilha.cert.br

Ransomware (5/5)

- **Formas de propagação:**
 - através de *e-mails* com o código malicioso em anexo ou que induzam o usuário a seguir um *link*
 - explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança

RANSOMWARE



fonte: cartilha.cert.br

Como se prevenir



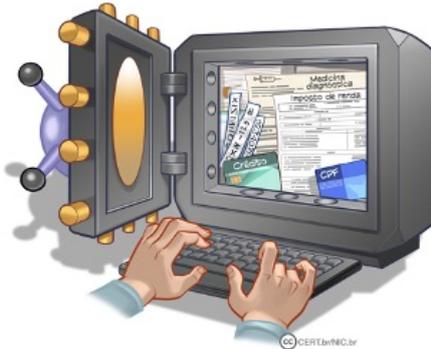
CC CERT.br/NIC.br



fonte: cartilha.cert.br

Não deixe que a infecção ocorra

- **A melhor prevenção é impedir a infecção inicial**
- **Nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente os dados**



RANSOMWARE



fonte: cartilha.cert.br

Faça *backups* regularmente (1/3)

Backup é a solução
mais efetiva contra
ransomware



RANSOMWARE

 fonte: cartilha.cert.br

Faça *backups* regularmente (2/3)

- Mantenha os *backups* atualizados
 - de acordo com a frequência de alteração dos dados
- Configure para que seus *backups* sejam realizados automaticamente
- Certifique-se:
 - de conseguir recuperá-los
 - de que eles estejam realmente sendo feitos



RANSOMWARE



fonte: cartilha.cert.br

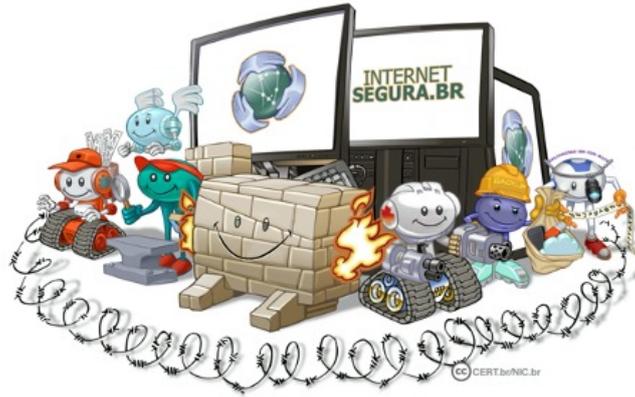
- Mantenha *backups* em locais seguros, bem condicionados e com acesso restrito;
- além dos *backups* periódicos, sempre faça *backups* antes de efetuar grandes alterações no sistema e de enviar o equipamento para manutenção;
- armazene dados sensíveis em formato criptografado;
- cuidado com mídias obsoletas;
- 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 (3/3)

- Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis
- Mantenha os *backups* desconectados do sistema
 - para que não sejam também criptografados
- Faça cópias redundantes
 - para evitar perder seus dados:
 - em incêndio, inundação, furto ou pelo uso de mídias defeituosas
 - caso uma das cópias seja infectada



Outros cuidados a serem tomados



 fonte: cartilha.cert.br

Mantenha os equipamentos atualizados

- **Tenha sempre as versões mais recentes dos programas**
- **Remova os programas que não usa mais, eles tendem a:**
 - ser esquecidos
 - ficar com versões antigas e potencialmente vulneráveis
- **Configure a atualização automática dos programas**
 - atualizações devem ser baixadas e aplicadas em horários em que o equipamento esteja ligado e conectado à Internet
- **Cheque periodicamente por novas atualizações usando as opções disponíveis nos programas**
- **Use apenas programas originais**

RANSOMWARE



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.

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**

RANSOMWARE



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**
- **Utilize *antispam* para filtrar as mensagens indesejadas**
- **Desabilite a auto-execução de:**
 - mídias removíveis
 - arquivos anexados



RANSOMWARE

 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**
- **Selecione os aplicativos, escolhendo aqueles:**
 - **bem avaliados**
 - **com grande quantidade de usuários**



RANSOMWARE



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.

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



RANSOMWARE



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.

Restrinja o acesso

- **Use a conta de administrador do sistema apenas quando necessário**
 - a ação do *ransomware* será limitada às permissões de acesso do usuário que estiver acessando o sistema

RANSOMWARECC BY-NC-SA 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 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 character with a white body, blue arms and legs, and a red cross on its chest. It is holding a spiral-bound notepad with a checklist. The checklist items are: 'USE CONDIÇÃO RESERVADA', 'NÃO REPARTE DADOS', 'CASA DESLIGADA', 'PENSE ANTES DE POSTAR', 'SAPILITE VERIFICAÇÃO EM DUAS ETAPAS', and 'MANTENHA EQUIPAMENTOS SEGUROS'. The robot is also holding a pencil.

RANSOMWARE  fonte: cartilha.cert.br

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

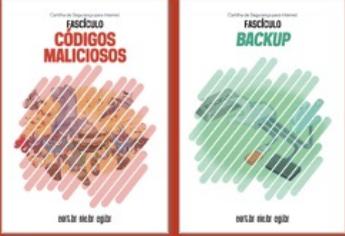
- Twitter: <https://twitter.com/certbr>
- RSS: <https://cartilha.cert.br/rss/cartilha-rss.xml>

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
Fascículo Backup
cartilha.cert.br/fasciculos
- **Livro Segurança na Internet**
cartilha.cert.br/livro



cert.br nic.br cgi.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-Compartilhalgual 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.
- **Compartilhalgual** — 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>