INSTITUTO FEDERAL
São Paulo
Câmpus São Paulo

Ransomware

Diretoria Adjunta de Tecnologia da Informação

IFSP – Câmpus São Paulo

suporte.spo@ifsp.edu.br

Agenda

- *Ransomware*
- Como se prevenir
- Outros cuidados a serem tomados
- Mantenha-se informado
- Créditos

Ransomware (1/4)

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 (2/4)

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

Ransomware (3/4)

- **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**

Fonte - https://cartilha.cert.br/

Ransomware (4/4)

- **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**
- **Não se propaga sozinho**

Fonte - https://cartilha.cert.br/

Como se prevenir

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**

Fonte - https://cartilha.cert.br/

Faça *backups* regularmente (1/3)

Backup* é a solução mais efetiva contra *ransomware

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 que eles estejam realmente sendo feitos**
  - **de conseguir recuperá-los**

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 eles não sejam também criptografados pelo *ransomware***
- **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

Mantenha os equipamentos atualizados

- Tenha sempre as versões mais recentes dos programas
- Remova os programas que você não utiliza mais, pois 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

Fonte - https://cartilha.cert.br/

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**

Fonte - https://cartilha.cert.br/

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

Fonte - https://cartilha.cert.br/

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**

Fonte - https://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**

Fonte - https://cartilha.cert.br/

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**

Mantenha-se informado (1/2)

Cartilha de Segurança para Internet

https://cartilha.cert.br/

RSS

https://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

http://twitter.com/certbr

Fonte - https://cartilha.cert.br/

Mantenha-se informado (2/2)

Antispam.br

http://antispam.br/

INTERNET SEGURA.BR

Internet Segura

http://internetsegura.br/

Créditos

- **Fascículo Códigos Maliciosos**
  https://cartilha.cert.br/fasciculos/

- **Cartilha de Segurança para Internet**
  https://cartilha.cert.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

Fonte - https://cartilha.cert.br/