APCS/DGPAd

Departamento Estadual
de Investigações Criminais
DEIC

DIVISÃO DE CRIMES
CIBERNÉTICOS

Guia de prevenção:
“Ransomware”
(sequestro de dados)

“Ransomware” (sequestro de dados)

“Ransomware” é um tipo de código malicioso (também conhecido como “malware”) que, ao ser executado no computador da vítima, torna seus dados armazenados inacessíveis (geralmente através de criptografia). Logo em seguida, o cibercriminoso exige pagamento de resgate para restabelecer o acesso aos dados. Também pode ocorrer a exfiltração (transferência não autorizada de informações confidenciais de um dispositivo) durante esse tipo de ataque, normalmente com o intuito de se extorquir a vítima, com a ameaça de exposição indevida de seus dados.

Existem alguns cuidados que você pode tomar para se recuperar de um ataque de “ransomware”, mas a melhor coisa a se fazer, em primeiro lugar, é entender **como evitar este tipo de ataque**:

1. Sempre atualize seu sistema operacional e seus aplicativos quando novas versões estiverem disponíveis. Você pode configurar para isso acontecer automaticamente com o Windows e muitos outros aplicativos, como o Office. Use sempre softwares originais.

2. Certifique-se de fazer backup de seus arquivos regularmente. Isso inclui os arquivos em seus computadores, telefones e quaisquer outros dispositivos que você tenha.

2.1. Faça um “backup” “offline” ou “frio”.
2.2. Faça “backup” dos dados em um disco rígido externo e remova o disco rígido do seu dispositivo.
2.3. Faça um “backup” em nuvem ou em serviço de hospedagem online similar.

3. Instale um software antivírus e “anti-ransomware” no seu computador e atualize-o regularmente. Sempre verifique um arquivo recebido antes de abri-lo.

4. Não habilite macros no Microsoft Office.

5. Ao instalar aplicativos faça download apenas de fontes confiáveis. Escolha os aplicativos com as melhores avaliações e com a maior quantidade de usuários.

6. Utilize um “firewall” e mantenha-o ativo.

7. Não clique em links recebidos por remetentes desconhecidos, e não considere que mensagens recebidas de conhecidos são sempre confiáveis, pois o campo “remetente” pode ser fraudado. O “phishing” (pescaria de dados) é a forma mais utilizada para disseminar “ransomware”.

8. Desabilite, em seu computador, a auto execução de mídias removíveis como pendrives ou HDs externos por exemplo.

“Ransomware”

Se você for afetado por um “ransomware:

1. Restaure seu sistema a partir do seu “backup” mais recente.

2. Reinstale seu sistema operacional se você não tiver um “backup”, **mas saiba que isso pode apagar todos os seus arquivos.**

3. Converse com algum suporte de TI ou com uma empresa de serviços de informática se precisar de ajuda. Eles podem verificar se você tem “ransomware” ‘real’ no seu computador. **Golpistas as vezes afirmam falsamente terem instalado “ransomware” no seu computador para que você os pague.**

4. Jamais pague resgates porque não há garantia de que você receberá seus dados de volta. Pagar o valor do resgate também pode colocá-lo em risco de novos ataques, pois o invasor perceberá que você está disposto a realizar novos pagamentos.

Se você for vítima de um golpe baseado em “ransomware”:

a) Não apague os “e-mails” e/ou mensagens recebidas do criminoso;
b) Se houver conversa com o criminoso via rede social, salve o nome do perfil e o “link” completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação de todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias, inclusive carteiras eletrônicas de bitcoins informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através da Delegacia Eletrônica:
https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home

POLÍCIA
POLÍCIA CIVIL
SÃO PAULO
CIVIL
SP