03

SGI INFORMA
MÊS DA SEGURANÇA
DA INFORMAÇÃO
NOVEMBRO - 2020

SGI INFORMA

ESPECIAL - SEGURANÇA DA INFORMAÇÃO

RANSOMWARE: UMA AMEAÇA FREQUENTE E DEVASTADORA

Você já imaginou tentar abrir seus arquivos e receber uma mensagem dizendo que suas informações foram sequestradas e que terá de realizar um pagamento para recuperá-las?

Conhecido pelo seu poder devastador de bloquear o acesso às informações e solicitar um pagamento pelo seu regaste, o *ransomware* vem se tornando uma ferramenta amplamente explorada por cibercriminosos.

Em virtude do aumento dos canais disponíveis para conversão de dinheiro real em moedas digitais, estes criminosos têm adotado novas estratégias para este tipo de ataque.

Este é o ataque da moda que vem afetando organizações em todo o mundo, inclusive no Brasil. E você, usuário, é um alvo em potencial!

Caso perceba um comportamento estranho em seu equipamento, suspeite de que possa estar sofrendo um ataque de *ransomware*. Confira nossas dicas!

EXPEDIENTE

Secretaria
da Administração - SAEB
Superintendência
de Gestão e Inovação - SGI
Diretoria de Gestão Estratégica
de TIC - DGE
Coordenação de Segurança
da Informação - CSI

Textos: Suane Freitas Coutinho
suane.coutinho@saeb.ba.gov.br

Edição: Ascom/Saeb
ascom@saeb.ba.gov.br

GOVERNO DO ESTADO | SECRETARIA DA ADMINISTRAÇÃO

O QUE É RANSOMWARE?

Tipo de malware (código malicioso) que criptografa, ofusca ou impede o acesso a arquivos e sistemas, utilizado para infectar computadores e smartphones, extorquindo a vítima por meio da exigência de pagamento de um valor para o resgate dos dados.

COMO SE PROPAGA?

- **Através de e-mails com código malicioso no anexo ou que induzam o usuário a clicar num determinado link;**
- **Falsas conversas recebidas por aplicativos de mensagens instantâneas, bem como SMS contendo links suspeitos;**
- **Por meio de propagandas falsas publicadas em sites legítimos, com anúncios contendo arquivos infectados;**
- **Explorando vulnerabilidades em sistemas que estão desatualizados;**
- **De forma automática, a partir de um computador infectado na rede.**

COMO SE PREVENIR

- **Evite abrir links de arquivos recebidos de e-mails desconhecidos;**
- **Não baixe programas de sites não confiáveis;**
- **Não acesse anúncios localizados em sites suspeitos. Verifique a veracidade da propaganda no site oficial da empresa;**
- **Sempre salve os arquivos de trabalho no compartilhamento de rede, a fim de garantir o backup dos dados, que é realizado pela área de TI;**
- **Quanto ao uso de computadores pessoais, faça regularmente o backup de seus dados em outra mídia de armazenamento ou na nuvem, de forma a mantê-los seguros, caso seu dispositivo seja infectado.**

FUI INFECTADO! O QUE FAZER?

- **É recomendado não pagar o valor do resgate, pois não se pode assegurar que os dados serão decodificados e que o usuário passará a ter acesso a suas informações;**
- **Procure a área de TI de sua organização para analisar o dispositivo afetado e restaurar o backup ou um técnico de sua confiança, caso o fato ocorra em seu dispositivo pessoal.**

QUAIS SINAIS PODEM INDICAR UM ATAQUE?

Bloqueio da tela inicial
Você liga o seu computador e não consegue efetuar o login com usuário e senha cadastrados.

Acesso limitado
Repentinamente ocorre falha na abertura de alguns arquivos que antes estavam abrindo normalmente.

Arquivos com extensões estranhas
Ao exibir os detalhes dos arquivos, você identifica que alguns deles estão com extensões estranhas, como “.doc.crypted” e .jpg.WNCRY”, dentre outros.

Exibição frequente de alertas na tela
Mensagens que são exibidas de forma irritante na tela, simulando a execução de um antivírus ou de um aplicativo de limpeza, que informa sobre problemas encontrados no seu dispositivo.

Instrução para pagamento de resgate
Informações exibidas na tela solicitando dinheiro pela recuperação dos dados. Geralmente contém instruções sobre como realizar pagamento, apresentando um tom de ameaça de perda total dos dados caso o pagamento não seja executado.