# RANSOMWARE - DADOS CRIPTOGRAFADOS

25/04/2023

**O QUE É?**

Trata-se do "sequestro" de informações e dados armazenados geralmente em servidores - podendo ser até em nuvens - e outros dispositivos através da encriptação dessas informações, quando a vítima deixa de ter acesso a esses arquivos. Então o autor passa a cobrar um valor - geralmente em criptomoedas e através de um endereço de email descartável - para fornecer uma chave para que a vítima volte a ter acesso aos seus arquivos.

As invasões ocorrem geralmente através de uma máquina contaminada com o software que é conectada a rede da empresa.

**O QUE FAZER ?**

1 - Procure a delegacia da sua cidade e se oriente de como registrar ocorrência; caso a empresa ou a vitima residam em Curitiba, ligue para o NUCIBER e se oriente de como proceder;

2 - Procure empresas especializadas em segurança de informação para possível recuperação dos dados encriptados;

3 - Verifique sites como www.nomoreransom.org, www.cisa.gov/stopransomware, www.ransomwhe.re

**NÃO É ATRIBUIÇÃO DO NUCIBER A RECUPERAÇÃO OU QUALQUER ASSISTÊNCIA TÉCNICA A RESPEITO DE RECUPERAÇÃO DE DADOS**

**A ATRIBUIÇÃO DA POLÍCIA CIVIL É O REGISTRO DA OCORRÊNCIA E, SE INSTAURADO INQUÉRITO, APURAR A AUTORIA DOS FATOS**

**COMO PREVENIR ?**

1 - Não utilize softwares sem saber da sua real procedência. Softwares "crackeados" são o principal canal de entada desse malware;

2 - Utilize políticas de segurança de rede e backups sólidas com um setor de Segurança da Informação ou empresa terceirizada para essa área de atuação;