Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

RANSOMWARE

Edição nº13
Julho/2021

Ransomware é um tipo de malware que torna inacessíveis os dados armazenados em um equipamento. Por exemplo, em computadores ou celulares infectados, o ransomware é capaz de bloquear a tela inicial, pastas ou criptografar os dados armazenados no disco. Ou seja, sem a chave, você perde acesso a todos ou parte dos arquivos e não consegue usar o próprio equipamento. Após esta etapa, este malware exige o pagamento de resgate (ransom) para restabelecer o acesso ao usuário. Usado por cibercriminosos, geralmente esta praga virtual exige que o pagamento do resgate seja via bitcoins, tornando quase impossível rastrear o criminoso que pode vir a receber o valor.

Existem ransomwares de vários tipos. Os principais são:

- **Scareware: software falso (como antivírus ou ferramenta de limpeza) que diz ter encontrado problemas em seu PC e que exige um pagamento para repará-los;**
- **Bloqueadores de tela: bloqueia o acesso ao sistema operacional para impedir completamente o uso do computador, impossibilitando o acesso a qualquer aplicativo ou arquivo;**
- **Doxware: ameaça publicar suas informações online roubadas se você não efetuar um pagamento;**
- **Criptografia: pastas e arquivos são criptografados, impedindo o uso e acesso.**

O ransomware pode se propagar de diversas formas, embora as mais comuns sejam:

- **Através de spam malicioso, ou malspam, que é um e-mail não solicitado usado para entregar malware. O e-mail pode incluir armadilhas em anexo, como PDFs ou documentos do Word. Também podem conter links para sites maliciosos;**
- **Através de programas baixados de sites suspeitos na Internet;**
- **Explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.**

Seguem algumas dicas de prevenção a ransomware:

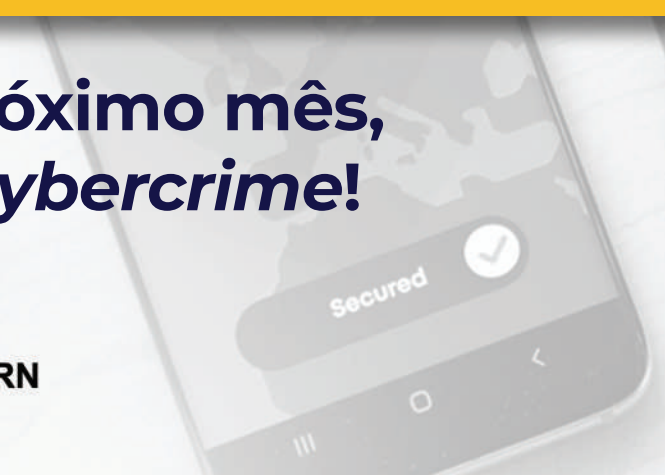
- **O email é um dos principais métodos de infecção. Tome cuidado com emails inesperados, principalmente se incluírem links e/ou anexos;**
- **Instale um software antivírus que detecte programas mal-intencionados como o Ransomware. Alguns desses antivírus impede que novos aplicativos sejam executados sem autorização, dificultando a ação dos invasores;**
- **Manter todos os seus softwares – incluindo os sistemas operacionais – com patches e atualizados;**
- **Remova os programas que você não usa mais, pois eles tendem a ficarem esquecidos e potencialmente vulneráveis;**
- **Use apenas programas originais. Programas piratas tendem a esconder malwares;**
- **Desabilite a função de reprodução automática no seu computador. Se houver algum "malware" no pendrive, ele será automaticamente ativado quando o pendrive for conectado à porta USB;**
- **Seja cuidadoso ao clicar em links. Use complementos que permitam visualizar o link de destino para tentar identificar se o link é suspeito ou não.**
- **O backup de dados importantes é a forma mais eficiente de combater uma infecção de ransomware.**

Pagar ou não o resgate? Este questionamento é bastante pertinente, principalmente pelo fato do ransomware ser tão assustador. Os cibercriminosos não discriminam. Sua única meta é infectar o máximo de computadores possível, pois é assim que eles ganham dinheiro. Isso também é um "negócio" muito lucrativo, com vítimas pagando centenas de milhares de dólares para recuperar seus dados. Saiba que você está lidando com golpistas e, por isso, pagar o resgate não garante nada. Às vezes, eles simplesmente aumentam o preço se encontrarem alguém desesperado o bastante para pagar. Já foi relatado que além do resgate dos dados, houve uma cobrança adicional para não divulgar os dados sequestrados.

A maioria das agências governamentais e especialistas na segurança da informação sugerem que nenhuma quantia seja paga aos invasores, pois atitudes como essa apenas encoraja os hackers a criarem mais ataques desse tipo.

Em caso de infecção por ransomware, procurar ajuda de empresas especializadas.

Fique ligado: no próximo mês, falaremos sobre *Cybercrime*!



Tribunal Regional Eleitoral - RN