BIM
COMUNICAR PARA EDUCAR
Edição Extra
Boletim Informativo Mensal - Agosto/2021 - Ano 2

RANSOMWARES

Você sabe o que é um ransomware?

Ransomware (software de resgate, em tradução literal) é um tipo de código malicioso que, ao ser executado, impede o acesso aos dados de um sistema. Para recuperar esse acesso, é necessário o pagamento de um valor estipulado como "resgate". *Ransomware* é um ataque cibernético para **sequestro de dados**.

Existem duas variantes principais:

- *lockscreen* - é um *ransomware* de bloqueio de tela, e impede o acesso ao equipamento – o principal alvo é o usuário comum;
- *cryptolocker* - é um *ransomware* que criptografa arquivos na rede, para comprometer a disponibilidade deles e interromper atividades, causando quebra de confidencialidade de dados e perdas financeiras – o principal alvo são as organizações.

Como ocorre o ataque?

A forma mais comum de ataque é por meio de "*phishing*" (em inglês, pescaria), um *e-mail* falso que atrai a atenção e induz o usuário a executar um arquivo (tipo "clique aqui") que instala o *ransomware*.

Outras formas de infecção:

- *download* de *softwares* "piratas", que contém chaves de ativação com códigos maliciosos;
- utilização de mídias infectadas (*pen drives*, HDs removíveis);
- acesso a *sites* maliciosos, que identificam vulnerabilidades e ativam a execução de códigos remotos; e
- no caso de dispositivos móveis, a instalação de aplicativos modificados, hospedados fora das lojas oficiais.

Como se prevenir contra um ataque?

1. Não clicar em link desconhecido ou suspeito

A ação do usuário é, na maioria dos casos, o vetor de infecção por *ransomware*. Utilizando-se da engenharia social*, os criminosos induzem o usuário a clicar em um *link,* que levará ao *download* e execução de códigos maliciosos. A tática manipula o usuário e se aproveita da falta de maturidade dele em relação à segurança da informação, para burlar as proteções lógicas existentes.

*Engenharia social é uma prática usada por indivíduos de má fé, para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar, ou obter informações sigilosas e importantes. É baseada na interação humana, e é conduzida por pessoas que usam o engano, para violar os procedimentos de segurança que normalmente deveríamos seguir.

Evite ataques de engenharia social:

- esteja ciente dos riscos e saiba como identificar ameaças;
- eduque! – treinamento e conscientização de usuários podem reduzir o risco de ataques e tornam a organização e o indivíduo menos vulneráveis;
- mantenha sistemas operacionais e aplicativos sempre atualizados;
- utilize ferramentas de proteção, como *firewall*, *antispam*, *antiphishing* e antivírus; e
- evite rede não-confiável (*hotspots*, cybercafé), quando for acessar sistema corporativo.

2. Tenha sempre um ***backup*** (cópia de segurança)

A existência de cópias dos arquivos (***backup***), testados periodicamente, é importante não apenas para fazer frente às ameaças de *ransomware*, mas também para recuperar dados em casos de pane ou perda de equipamentos.

Teste periodicamente o ***backup*** e o armazene em mídia externa, desconectada da rede e separada fisicamente dos computadores ou servidores de arquivos.

Foi atacado?! Saiba como proceder!

- Analise o ***backup*** com ferramenta de antivírus.
- Identifique a vulnerabilidade que permitiu a infecção do ambiente pelo *ransomware.* Essa ação irá minimizar a expansão do evento, atenuar seus efeitos e diminuir a probabilidade de novas ocorrências.

Na maioria dos ataques, são utilizados criptografia e algoritmos fortes, que impedem a recuperação dos arquivos sem a chave apropriada para a decifragem dos dados. Assim, a principal ferramenta para recuperar acesso aos dados é possuir uma cópia atualizada (***backup***) dos dados.

Fonte: http://www.gov.br/gsi/dsi https://www.ctir.gov.br/
Editorial/redação/diagramação: ASSESI Sugestões: asscom.dsi@presidencia.gov.br