Les rançongiciel

C’est quoi ?

Un rançongiciel (**ransomware** en anglais) est un **logiciel malveillant** qui **bloque l’accès à l’ordinateur** ou **à des fichiers en les chiffrant** et **qui réclame à la victime le paiement d’une rançon pour en obtenir de nouveau l’accès**. La machine peut être infectée après l’ouverture d’une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n’ont pas été mis à jour par les victimes.

Le but recherché est d’extorquer de l’argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l’accès aux données corrompues. Certaines attaques visent juste à endommager le système de la victime pour lui faire subir des pertes d’exploitation et porter atteinte à son image**.**

Si vous êtes victime

- **Débranchez la machine** d’internet ou du réseau informatique.
- En entreprise **alertez immédiatement** votre service ou prestataire informatique.
- **Ne payez surtout pas la rançon réclamée** car **vous n’êtes pas certain de récupérer vos données** et **vous alimenteriez le système mafieux**.
- **Conservez les preuves** : message piégé, fichiers de journalisation (logs) de votre pare-feu, copies physiques des postes ou serveurs touchés. À défaut, **conservez les disques durs**.
- **Déposez plainte** au commissariat de police ou à la gendarmerie ou en écrivant au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.
- **Identifiez la source de l’infection** et **prenez les mesures nécessaires** pour qu’elle ne puisse pas se reproduire.
- **Appliquez une méthode de désinfection et de déchiffrement**. En cas de doute, effectuez une restauration complète de votre ordinateur**. Reformatez les postes et/ou serveurs touchés** et **réinstallez un système sain** puis **restaurez les copies de sauvegarde des fichiers perdus** lorsqu’elles sont disponibles.
- **Faites-vous assister au besoin** par des professionnels qualifiés. Vous trouverez sur *www.cybermalveillance.gouv.fr* des professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.