FICHE N°2 : LES RANÇONGICIELS (RANSOMWARES)

Des logiciels malveillants qui peuvent s'infiltrer dans vos ordinateurs

Qu'est-ce qu'un rançongiciel ou ransomware ? Précision sur le mode opératoire

Un ransomware, ou rançongiciel, est un **logiciel** malveillant, **prenant en otage les données**. Il infecte les ordinateurs, chiffre les fichiers contenus dans le système infecté et **demande une rançon** (en cryptomonnaie) en échange d'une clé ou d'un mot de passe permettant de les déchiffrer.

MESSAGE DE PRÉVENTION

1- Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

2- Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.

3- N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

4- Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

5- N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.

6- Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

7- N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

8- Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés.

9- Éteignez votre machine lorsque vous ne vous en servez pas.

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime de rançongiciels (ransomwares), que faire ?

- **Débranchez la machine d'internet** ou du réseau Informatique.

- **Isolez** les supports touchés par le Ransomware.

- **En entreprise, alertez immédiatement** votre service informatique.

- **Ne payez pas la rançon**, vous alimenteriez le système mafieux, sans certitude de récupérer les données.

- **Déposez plainte** auprès de la police ou de la gendarmerie ou en écrivant au procureur de la République dont vous dépendez.

- Se rapprochez de sa société fournisseur d'anti-virus ou prestataire de service.
  A défaut vous trouverez de l'aide sur le site cybermalveillance.gouv.fr

- Vous pouvez trouver quelques clés et outils de déchiffrement sur le site : nomoreransom.org/fr/index.4html.