Ransomwares : des outils pour les contrer

Le ransomware (aussi appelé rançongiciel ou cryptolocker) est un virus qui va **chiffrer les fichiers** de l'utilisateur contre son gré, puis exiger le paiement d'une **rançon** contre la clé de chiffrement utilisée par le ransomware.

Vos fichiers sont ainsi théoriquement "pris en otages" tant que la rançon n'a pas été payé au cybercriminel.

Ce type de logiciel d'extorsion s'est particulièrement développé au cours des dernières années car ils représentent une activité extrêmement lucrative pour les cybercriminels.

Si cela vous arrivait un jour malheureusement, nous vous conseillons de ne **jamais payer la rançon demandée.** Cela encourage ce type d'activité criminelle et vous n'avez aucune certitude que le pirate vous enverra vraiment la clé de déchiffrement.

Nous vous présentons ici une liste d'outils de déchiffrement gratuits des ransomwares. Ces outils ont été développés par **Kaspersky**, la célèbre société d'antivirus.

Ces outils sont disponibles sur cette page : https://noransom.kaspersky.com/fr/
En fonction du type de ransomware qui vous aurait attaqué (il en existe des dizaines), il faut télécharger l'outil correspondant.

Si vous ne savez pas quel type de ransomware a chiffré vos fichiers, le site web « No More Reason » (une initiative commune entre des services de police néerlandais, de l'organisme européen de lutte contre la criminalité Europol et des entreprises spécialisées dans la sécurité informatique) propose un **outil appelé Crypto Sheriff** qui permet de découvrir **l'identité d'un ransomware** de manière simple et rapide : https://www.nomoreransom.org/crypto-sheriff.php?lang=fr

Après avoir récupéré vos fichiers, **sauvegardez** les si cela n'était pas encore le cas et procédez à une **réinstallation de Windows** afin de vous assurer qu'aucune trace du virus ne demeure. Ainsi vous serez sûr que les cybercriminels ne pourront plus prendre la main sur votre machine.