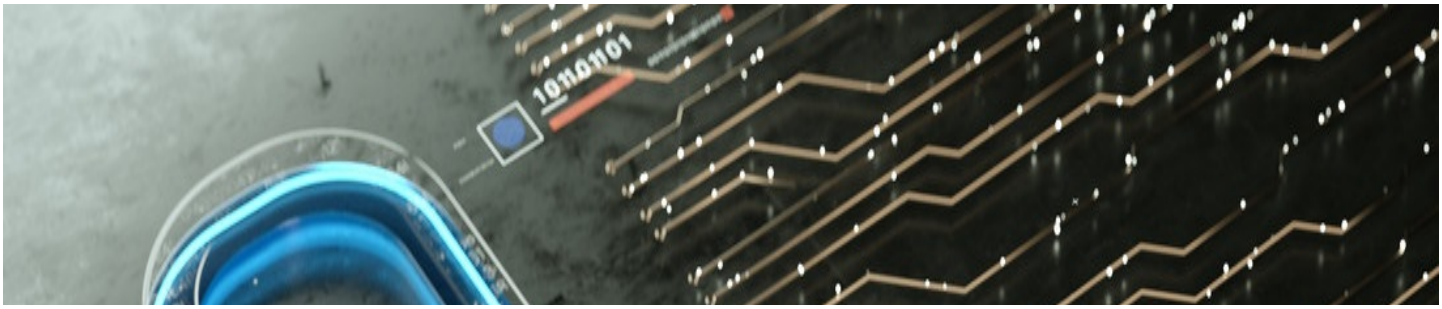

Ransomware

Version PDF

Qu'est ce qu'un Ransomware ?

Vous n'avez plus accès aux données de votre ordinateur. Ces données ont été cryptées. Une rançon est demandée sous forme de monnaie virtuelle, comme le bitcoin, pour rendre les données à nouveau disponibles ou les décrypter.

Les *ransomwares* sont des logiciels malveillants qui effectuent une action non désirée sur un système informatique, cryptent des fichiers/données et exigent ensuite une rançon ("ransom") pour annuler cette action.

Le malware se propage généralement :

- par e-mail dans les réseaux d'entreprises, d'administrations, d'associations ou même de particuliers par un simple clic sur une pièce jointe (.pdf, .zip ou .exe) ou sur un lien infecté ;
- en consultant un site web précédemment infecté.

Le paiement de la rançon doit généralement être effectué par le biais de cryptomonnaies (principalement le bitcoin).

Attention : Les ransomwares ne doivent pas être confondus avec d'autres types d'escroqueries (arnaques ou extorsions) avec lesquelles ils partagent certaines caractéristiques.

De quoi avez-vous besoin pour déposer plainte ?

Si cela est possible ou disponible, vous pouvez inclure les éléments suivants pour aider à traiter la plainte plus rapidement :

- Capture d'écran de l'écran "ransomware" que vous voyez sur l'ordinateur. Ou une image claire de cela.
- L'adresse Bitcoin à laquelle le paiement doit être effectué. (Une adresse Bitcoin peut ressembler à ceci : *15KJMTunaXuSjGuVX68k4hZvG6Y7hqauy3*)
- Informations sur le système infecté (marque et modèle, système d'exploitation, numéro de série, etc...)
- Si vous savez ou soupçonnez comment l'infection a été contractée, recueillez autant d'informations que possible à ce sujet (par exemple : site web, pop-up, e-mail, fichier, etc.).
- Toutes les informations dont vous disposez sur les transactions financières.
- Toutes les informations en votre possession concernant d'éventuelles communications avec l'auteur de l'infraction.

Que pouvez-vous encore faire ?

- Éteignez complètement l'ordinateur dès que possible et déconnectez-le d'Internet et des disques durs externes.
- Supprimez d'abord le logiciel malveillant, afin que les fichiers ne soient pas à nouveau cryptés. Demandez l'aide d'un expert si nécessaire.
- Faites une sauvegarde des fichiers. Bien entendu, la condition préalable est qu'il existe une sauvegarde (récente) et qu'elle n'ait pas été cryptée par le cryptoware.
- Les méthodes de cryptage diffèrent selon le type de logiciel. Certaines clés de décryptage (de logiciels malveillants connus) sont publiées sur le site : **nomoreransom.org**

Comment éviter d'être à nouveau victime ?

- Installez un programme anti-virus et effectuez des mises à jour régulières. Une fonction anti-ransomware est importante.
- Maintenez tous les logiciels à jour, y compris le système d'exploitation, le navigateur Internet, les modules complémentaires du navigateur et les programmes courants, tels qu'Adobe Reader.
- Ne cliquez pas sur les pièces jointes et les liens contenus dans les courriels, sauf si vous êtes sûr qu'ils sont de confiance.
- Les rançongiciels sont souvent des fichiers .exe exécutables déguisés en un autre type de fichier, tel qu'un document PDF. Désactivez les extensions de fichiers pour que vous puissiez voir à travers le déguisement.

- Faites des sauvegardes. C'est de toute façon une bonne idée, mais avec l'infection par un ransomware, c'est souvent le seul recours pour éviter la perte de toutes vos données.

Où pouvez-vous trouver plus d'informations ?

nomoreransom.org et stopransomware.fr

https://www.safeonweb.be/fr/actualite/ne-laissez-pas-des-ransomware-paralyser-la-belgique

https://www.nomoreransom.org/declarations/declaration-de-ransomware-french.htm