# SÉCURITÉ ÉCONOMIQUE & PROTECTION DES ENTREPRISES

La Gendarmerie nationale, acteur de la politique publique d'intelligence économique

ALERTE SECURITE SECOPE 80 entreprises

## LE FLÉAU DES CYBERATTAQUES PAR RANÇONGICIEL

Les **attaques par rançongiciel** connaissent une augmentation sans précédent. La situation de crise liée à l'épidémie COVID-19 a engendré une intensification du recours au télétravail, ce qui a rendu les **entreprises** davantage **vulnérables aux cyberattaques**.

En zone gendarmerie, au cours des huit premiers mois de 2020, le nombre d'atteintes aux systèmes de traitement automatisé de données a augmenté de 57% par rapport à 2019, passant de 109 à 254 faits en région de gendarmerie Hauts-de-France.

### ***MAIS QU'EST-CE QUE C'EST ?***

Un rançongiciel est un **programme malveillant** reçu par courriel ou mis à disposition sur un site Internet, qui provoque le chiffrement de tous les fichiers d'un ordinateur (*et des fichiers accessibles en écriture sur les dossiers partagés si votre ordinateur est connecté à un réseau informatique*).

Avec ces programmes malveillants, les **pirates** peuvent prendre à distance le contrôle d'un ordinateur ou d'un système d'information et empêcher de consulter ou d'utiliser les données. Ils exigent alors de l'utilisateur ou de l'entité touchée de payer une **rançon**, souvent en cryptomonnaie.

Parmi les entités les plus visées, les **entreprises du secteur industriel**, la **santé** et les **collectivités territoriales**.

### ***CINQ CONSEILS POUR SE PRÉMUNIR DES « RANÇONGICIELS » (ou RANSOMWARE)***

- **Effectuez des sauvegardes régulières de vos données** : c'est le meilleur moyen de couper l'herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu'elle fonctionne ;
- **N'ouvrez pas les messages dont la provenance ou la forme est douteuse, il pourrait s'agir d'un rançongiciel** : ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (*les noms de vos clients par exemple*) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels. Restez donc très vigilants ! Certains messages paraissent tout à fait originaux. En cas de doute, contactez le messager par un autre biais ;
- **Apprenez à identifier les extensions de fichiers douteuses** : vous recevez habituellement des fichiers en .doc ou .mp4 (*par exemple*) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ? Ne les ouvrez surtout pas ! Attention à l'ouverture de pièces jointes de type .scr ou .cab. Il s'agit des extensions utilisées lors de campagnes sévissant chez les particuliers, les PME ou les mairies ;
- **Mettez à jour vos principaux outils** : on ne vous le dira jamais assez : Windows, antivirus, lecteur PDF, navigateur… Veillez à leurs mises à jour ! Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications. Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes ;
- **Utilisez un compte « *utilisateur* » plutôt qu' « *administrateur* »** : ne naviguez pas depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

Sécurité Économique et Protection des Entreprises
Groupement de Gendarmerie Départementale de la Somme.

*Nous contacter* ggd80+secope@gendarmerie.interieur.gouv.fr

Gendarmerie de la Somme