MISE EN GARDE – Rançongiciel

La Sûreté du Québec désire mettre en garde les entreprises contre les attaques informatiques de type « rançongiciel ».

Qu'est-ce qu'un rançongiciel?

- Il s'agit d'un logiciel malveillant qui, lorsqu'il infecte un ordinateur, verrouille l'accès aux fichiers ou au système.
- Une demande de rançon, payable notamment par monnaie virtuelle (comme le *Bitcoin)*, apparaît à l'écran en échange de la clé de déchiffrement.
- L'ordinateur infecté reste généralement fonctionnel, mais les documents de travail ne sont pas utilisables.
- L'utilisateur se retrouve incapable de les ouvrir avec les logiciels habituels.

Exemple de message apparaissant à l'écran :

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail zara2018@cock.li
Write this ID in the title of your message AC515015
In case of no answer in 24 hours write us to theese e-mails: zara2018@tutanota.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Comment les cybercriminels s'y prennent-ils ?

Ils utilisent l'exploitation du service de bureau à distance de Windows, en misant principalement sur la faiblesse du mot de passe afin de se connecter au service qui leur donne le contrôle de l'appareil et leur permet d'y installer eux-mêmes le logiciel malveillant.

Lorsque le rançongiciel est installé, les cybercriminels peuvent exécuter d'autres actions sur le système telles qu'installer d'autres programmes, désactiver l'antivirus, effacer les journaux d'événements, etc.

Les rançongiciels sont aussi transmis par l'entremise de pièces jointes de courriels ou encore, lorsque l'utilisateur clique sur un lien qui le redirige vers des sites web contrôlés par les cybercriminels.

Comment prévenir les attaques par rançongiciels?

- **Sensibiliser les employés de manière active :** leur indiquer d'éviter de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue dans un courriel ou un texto. Toujours demander l'aide des techniciens attitrés et éviter les solutions de type « technicien en ligne ».
- **Effectuer les mises à jour régulièrement :** la plupart des rançongiciels exploitent des failles que l'on peut éviter.
- **Avoir une solution de sécurité complète qui offre une protection contre les rançongiciels, les pourriels et la navigation Web.**
- **Sécuriser le service de bureau à distance :** utiliser des services d'accès à distance sécurisés tels que des « VPN » qui exigent la double authentification et des mots de passe robustes.
- **Limiter l'utilisation de comptes de type administrateur sous Windows.**
- **Instaurer une procédure de sauvegarde** : tenir compte de la fréquence des sauvegardes en fonction de la nature et de la valeur des données, et s'assurer que les sauvegardes sont stockées à l'extérieur du réseau commun. Si vous êtes victime d'un rançongiciel, votre sauvegarde risque d'être votre seule solution.

Quoi faire si vous êtes victime d'un rançongiciel?

Ne pas payer la rançon. Le paiement de la rançon ne garantit pas la récupération des données et encourage la récidive.

POUR SIGNALER CE TYPE D'ÉVÉNEMENT, COMMUNIQUER AVEC :

- **La Sûreté du Québec au 9-1-1**
  *Municipalités non desservies par le 9-1-1: composer le 310-4141 ou *4141 (cellulaire)

- **Votre service de police local.**