QUE FAIRE POUR ÉVITER QUE VOTRE ENTREPRISE OU ORGANISME SOIT VICTIME D'UN RANÇONGICIEL?

Sensibiliser les employés de manière active : évitez l'ouverture de pièces jointes aux courriels de sources inconnues et ne suivez pas de liens apparaissant dans un courriel ou dans un message texte lorsque vous ne connaissez pas l'expéditeur. Il vous faut toujours faire appel à des techniciens attitrés. Les solutions de type « techniciens en ligne » sont fortement déconseillées.

Effectuer les mises à jour régulièrement : la plupart des rançongiciels exploitent des vulnérabilités pour lesquelles il existe déjà des correctifs.

Opter pour une solution de sécurité complète qui offre une protection contre les rançongiciels, les pourriels ainsi que contre les autres dangers liés à la navigation Web.

Sécuriser le service de bureau à distance : utilisez des services d'accès à distance sécurisés tels que des « VPN », en choisissant 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 selon la nature et 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, sachez que votre sauvegarde risque d'être votre seule solution.

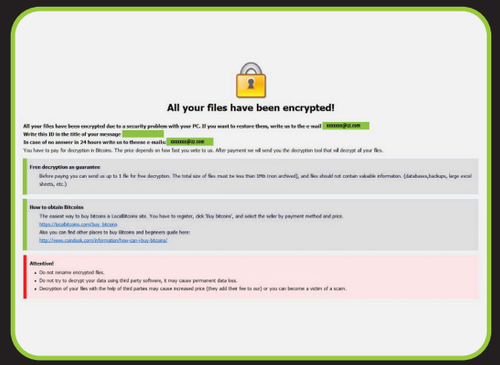
SÛRETÉ DU QUÉBEC

Avec vous, pour vous

DIVISION DES ENQUÊTES SUR LA CYBERCRIMINALITÉ

Veuillez contacter votre service de police local si vous désirez porter plainte pour une attaque informatique par rançongiciel.

LES ATTAQUES INFORMATIQUES DE TYPE « RANÇONGICIEL »



QU'EST-CE QU'UN RANÇONGICIEL ?

Il s'agit de logiciels malveillants qui, lorsqu'ils infectent un ordinateur, verrouillent l'accès aux fichiers ou au système. Une fois qu'un tel logiciel est exécuté, une demande de rançon, payable par monnaie virtuelle telle que le bitcoin, apparaît à l'écran en échange de la clé de déchiffrement.

L'ordinateur infecté reste généralement fonctionnel. Le rançongiciel utilise un mécanisme de déchiffrement pour verrouiller l'accès aux fichiers, principalement les documents de travail tels que les bases de données, les fichiers associés aux formats PDF, Word, Excel, PowerPoint, ainsi que les images. Les noms des fichiers sont modifiés par le rançongiciel et l'utilisateur se retrouve incapable de les ouvrir avec les logiciels habituels.

Les rançongiciels peuvent aussi s'en prendre aux systèmes de sauvegarde et de restauration du système et peuvent se propager aux autres ordinateurs et appareils connectés au même réseau.

Autrefois, les cybercriminels derrière ce type d'attaques se contentaient de chiffrer les systèmes informatiques et demandaient une rançon en échange de la clé de déchiffrement. Depuis 2020, plusieurs de ces cybercriminels procèdent aussi à de l'exfiltration de données avant de chiffrer les systèmes et menacent de rendre ces données publiques si la rançon n'est pas payée.

QUELLES SONT LES VULNÉRABILITÉS ?

Depuis quelques années, la Sûreté du Québec observe une multiplication des infections par l'entremise de l'exploitation de vulnérabilités, au niveau des services de contrôle à distance tels que : le bureau à distance de Windows (RDP ou Remote Desktop protocol) ou l'accès au service VPN (Virtual Private Network).

Les cybercriminels exploitent souvent la faiblesse d'un mot de passe afin de se connecter au service. Ils obtiennent ainsi un accès au réseau interne, ce qui leur permet d'installer eux-mêmes le rançongiciel à distance. Ces derniers peuvent exécuter plusieurs autres actions sur le système tel qu'installer d'autres programmes, désactiver l'antivirus, effacer les journaux d'événements, etc.

Les rançongiciels sont aussi transmis par l'entremise des programmes malveillants en pièces jointes dans les courriels qui semblent provenir de collègues ou de partenaires d'affaires ou encore, lorsque l'utilisateur clique sur un lien qui le dirige vers des sites web contrôlés par les cybercriminels.

COMMENT PRÉVENIR LES ATTAQUES PAR RANÇONGICIELS ?

Sans sauvegarde, l'organisation victime d'une attaque se sent confrontée à deux choix possibles : payer ou ne pas payer la rançon.

La Sûreté du Québec recommande de ne pas payer la rançon :

- **Payer la rançon ne garantit pas la récupération des données.**
- **Payer la rançon contribue à accentuer le problème en encourageant d'autres criminels à se lancer dans ce type d'activité.**

Vous devez porter plainte à votre service de police local qui devra communiquer sans délai avec la Division des enquêtes sur la cybercriminalité de la Sûreté du Québec.