GRC·RCMP

GENDARMERIE ROYALE DU CANADA • ROYAL CANADIAN MOUNTED POLICE

REJETER LES RANÇONGICIELS

Ce qui se passe

1. L'utilisateur clique sur un lien ou ouvre une pièce jointe dans un pourriel/courriel contrefait.

2. L'utilisateur visite sans le savoir des site Web malveillants/compromis.

3. L'utilisateur insère dans l'ordinateur un appareil infecté, tels qu'une clé USB ou un disque dur USB.

4. Un cybercriminel installe un logiciel malveillant.

5. Un logiciel malveillant est libéré et l'infection se répand.

6. L'ordinateur est verrouillé et un message exigeant un paiement pour déverrouiller l'accès aux dossiers ou au système apparait.

7. Cela peut se produire sur un seul ordinateur ou sur un réseau entier.

8. Le message indique que seul l'arnaqueur peut déverrouiller l'accès aux dossiers. C'est faux!Consultez les sites ci-dessous pour en savoir plus.

Pour en savoir plus :
pensezcybersecurite.gc.ca
nomoreransom.org

Protéger et prévenir

Verser un paiement ne garantit pas que votre réseau sera déverrouillé. Il vaut mieux **PROTÉGER** vos systèmes par des moyens qui aident à **PRÉVENIR** toute infection.

Grandes entreprises – la meilleure approche est une approche multipoints :

- Protection des courriels et Web – bloquer les pourriels et l'accès aux liens malveillants.
- Protection des serveurs – protéger les serveurs en éliminant les vulnérabilités exploitables.
- Protection du réseau – empêcher que le rançongiciel ne se répande jusqu'au point terminal.
- Protection du point terminal – empêcher l'exécution du rançongiciel au point terminal.

Petites entreprises – une approche à deux volets est efficace :

- Protection des courriels et du Web – empêcher que les pourriels se rendent dans la boîte de réception.
- Protection du point terminal – bloquer l'accès aux sites malveillants/compromis et empêcher l'exécution du rançongiciel.

Ordinateur personnel – une protection en une étape est requise :

- Utiliser une solution de sécurité qui bloque les pourriels, empêche l'accès aux liens malveillants et stoppe l'infection.

Adopter des pratiques exemplaires de la cybersécurité

Utilisez des mots de passe efficaces – 12 caractères avec des chiffres, des symboles et des lettres majuscules et minuscules.

Installez un logiciel antivirus et antimaliciels digne de confiance; utilisez les pare-feu de réseau; protégez votre routeur.

Utilisez l'authentification multifactorielle – par exemple un code envoyé vers votre téléphone cellulaire lorsque vous entrez un mot de passe.

Évitez d'ouvrir les courriels d'expéditeurs que vous ne connaissez pas ou de cliquer sur les liens qu'ils contiennent.

Mettez régulièrement à jour vos logiciels afin d'éviter les plus récentes vulnérabilités. Suivez les instructions du fournisseur du logiciel.

Faites une sauvegarde de vos dossiers sur au moins deux dispositifs avec une sauvegarde conserver dans un endroit différent.