Journée de lutte contre les rançongiciels 2022

12 mai 2022

Les rançongiciels sont le type de cybermenace le plus courant touchant les Canadiens et les Canadiennes. Le 12 mai, c'est la Journée de lutte contre les rançongiciels et il s'agit d'une excellente occasion pour le Centre antifraude du Canada (CAFC), le Groupe national de coordination de la lutte contre la cybercriminalité (GNC3) et d'autres partenaires de mettre l'accent sur la prévention, la sensibilisation et le signalement des incidents liés aux rançongiciels.

Le CAFC et le GNC3 entretiennent une relation de travail étroite en raison des liens importants et en évolution constante entre la fraude et la cybercriminalité. Les deux programmes – qui fournissent des services distincts à la collectivité de l'application de la loi pour lutter contre la criminalité liée à ces domaines – assureront de plus en plus de services hautement coordonnés lorsqu'il y a un lien entre les activités de fraude et de cybercriminalité.

Qu'est-ce qu'un rançongiciel?

Dans les attaques par rançongiciel, des criminels accèdent habituellement à un réseau ou à un dispositif et chiffrent des données afin de rendre le système ou les données inaccessibles à l'utilisateur. Les cybercriminels exigent le paiement d'une rançon afin que la victime puisse déchiffrer ses données et retrouver l'accès au réseau.

Divers dispositifs, qu'il s'agisse d'appareils mobiles personnels (au moyen d'applications malveillantes) ou de réseaux d'entreprise, peuvent être compromis lors d'attaques par rançongiciel. Les cybercriminels peuvent aussi tenter d'extorquer de l'argent aux victimes en menaçant de divulguer leurs données en ligne, et harceler les clients et les employés d'une organisation victime afin de lui soutirer des paiements de rançongiciel. Les attaques peuvent varier en terme de degré de sophistication technique et de niveau de compromission, et cibler des organisations de tous les types et secteurs.

La plupart des incidents liés à des rançongiciels commencent avec l'envoi d'un courriel dans une tentative d'hameçonnage. Celui renferme une pièce jointe; il peut s'agir d'un fichier exécutable, d'un document d'archive ou d'une image ou d'un lien. Une fois que la personne ouvre la pièce jointe ou clique sur le lien, le maliciel est installé sur le système de l'utilisateur. Celui-ci peut demeurer inactif pendant plusieurs jours ou mois avant que les fichiers ou les systèmes soient chiffrés ou verrouillés. Voici d'autres façons dont des réseaux ou des appareils peuvent être compromis :

- Vous visitez des sites Web non sécurisés, suspects ou compromis;

- Vous connectez un appareil externe infecté (p. ex. clé USB) à votre ordinateur;
- Vous exposez vos systèmes à Internet inutilement ou sans prendre de mesures robustes en matière de sécurité et de maintenance.

Pourquoi doit-on signaler les incidents liés aux rançongiciels au service de police local et au CAFC?

Pour que les organismes d'application de la loi puissent lutter contre la fraude et la cybercriminalité, il est essentiel que les personnes qui en sont témoins, ou qui en sont victimes, le signalent au service de police local et au CAFC. Le service de police local est en mesure de répondre aux victimes sur son territoire, et le CAFC appuie les organismes d'application de la loi en communiquant l'information recueillie au moyen des signalements faits au GNC3 et à ses partenaires.

Raisons de faire un signalement au CAFC :

- L'information pourrait permettre d'établir un lien entre plusieurs crimes, au Canada et à l'étranger;
- L'information pourrait aider à faire avancer ou à conclure une enquête;
- Les signalements révèlent les tendances de la criminalité et permettent d'effectuer des prévisions de la criminalité;
- Les signalements permettent aux services de police et aux organisations des secteurs public et privé d'en apprendre davantage sur ces crimes et de contribuer aux efforts de prévention et de sensibilisation.

Indices – Comment vous protéger

- Méfiez-vous des courriels non sollicités;
- Ne répondez pas aux courriels suspects et ne cliquez jamais sur les liens qu'ils renferment;
- Assurez-vous d'avoir un plan pour sauvegarder vos données systématiquement et fréquemment;
- Utilisez l'authentification à plusieurs facteurs et un anti-maliciel;
- Assurez-vous que des mises à jour et des correctifs sont apportés régulièrement aux logiciels et au système, et que tous les mots de passe du système sont changés fréquemment;
- Publiez et mettez en application une politique sur la sécurité des employés;
- Collaborez avec les organismes d'application de la loi au moment d'élaborer et de mettre à l'essai un plan d'intervention en cas d'incident;

- Faites des signalements;
- Consultez le site du CAFC pour obtenir d'autres trucs et conseils pour vous protéger;
- Consultez le site du Centre canadien pour la cybersécurité pour obtenir d'autres renseignements sur les rançongiciels et des conseils, des directives et des services en matière de cybersécurité.

Si vous croyez avoir été victime de fraude ou de cybercriminalité, signalez-le à votre service de police local et au CAFC sur son système de signalement en ligne ou en composant le 1-888-495-8501. Si un incident s'est produit, mais que vous n'êtes pas tombé dans le piège, signalez-le tout de même au CAFC.