DÉPÔT D'UNE PLAINTE À LA POLICE

AIDE-MÉMOIRE POUR VICTIME D'UN RANÇONGICIEL

N° de carte d'appel : _____

N° de dossier : _____

Votre organisation ou votre entreprise a récemment été victime d'une attaque par rançongiciel :

- Ne payez aucune rançon. Le paiement de la rançon ne garantit ni la récupération ni la non-publication des données et encourage la récidive;
- Ayez recours aux services d'une firme privée de cyber sécurité pour vous assister, si nécessaire;
- Portez plainte auprès de votre service de police local ou à votre poste local de la Sûreté du Québec. Un policier vous rencontrera afin de prendre votre déclaration.

Dans l'objectif de faciliter la démarche, tentez de rassembler les documents informatiques pertinents (Étape 1 : Préparez les documents informatiques) et de recueillir l'information applicable à votre situation (Étape 2 : Préparez votre déclaration)

Veuillez noter que vous avez des obligations lors d'atteintes aux mesures de sécurité si vous avez été également victime de vol de données.

PRÉPAREZ LES DOCUMENTS INFORMATIQUES

SI POSSIBLE AVEC L'AIDE DE VOTRE TECHNICIEN INFORMATIQUE (TI) :

1. Identifiez et préservez, si possible, le premier poste de travail infecté (patient 0). N'effectuez aucune manipulation ou réinitialisation. Éteignez le poste en le débranchant de la prise électrique, ne l'éteignez pas via Windows.
2. Si le patient 0 n'est pas identifié ou si cela ne s'applique pas, préservez un ou plusieurs postes de travail infectés.
3. Si la préservation est impossible, faites une copie image ou intégrale d'un ou plusieurs postes infectés avant la restauration de ceux-ci.
4. Si les points précédents ne peuvent être réalisés, enregistrez, si possible, les éléments de preuve numériques suivants sur un support électronique (clé USB, CD, disque dur) :
   - Copie de demande(s) de rançon (copie du fichier txt, pas une capture d'écran);
   - Copie de programme(s) malveillant(s);
   - Copie des échanges de courriels avec entête du courriel original (pas un pdf ni un transfert);
   - Relevés de transactions en cryptomonnaie, s'il y a lieu;
   - Journaux d'événements (Event logs - *.evtx ou /var/logs) et autres journaux disponibles s'ils ne se trouvent pas sur un ordinateur récupéré (p. ex. : serveur de courriel, service VPN, serveur mandataire, pare-feu, etc.)
   - Copie du registre Windows (notamment SOFTWARE et les NTUSER.DAT de tous les utilisateurs);
   - Copie du répertoire Prefetch;
   - Plan de réseau.
5. Si vous avez eu recours aux services d'une firme privée de cyber sécurité, prévoyez devoir remettre au policier, une copie du rapport d'analyse que la firme vous aura transmis.

DÉPÔT D'UNE PLAINTE À LA POLICE

AIDE-MÉMOIRE POUR VICTIME D'UN RANÇONGICIEL

N° de carte d'appel : _____

N° de dossier : _____

PRÉPAREZ VOTRE DÉCLARATION

SI POSSIBLE AVEC L'AIDE DE VOTRE TECHNICIEN INFORMATIQUE (TI) :

1. Commencez à rédiger les faits entourant l'attaque informatique en répondant aux questions de la Liste de renseignements (ci-dessous). Tous les documents récupérés à l'étape précédente devraient être expliqués dans votre déclaration. Il est possible qu'une déclaration soit demandée à votre TI.
2. Répondez aux questions du formulaire Questionnaire rançongiciel.

LISTE DES RENSEIGNEMENTS

QUI ? LES PERSONNES CONNUES IMPLIQUÉES :

- Vos coordonnées, votre occupation ou votre rôle au sein de l'entreprise;
- Les coordonnées de toute autre personne impliquée, telles que des suspects ou des témoins.

QUAND ? LE MOMENT OÙ L'ATTAQUE INFORMATIQUE EST SURVENUE :

- La date et l'heure où l'attaque informatique est survenue;
- La date et l'heure où vous avez découvert qu'il y avait eu une attaque informatique.

OÙ ? LES LIEUX OÙ SONT SURVENUS LES ÉVÉNEMENTS :

- L'adresse complète ou l'intersection la plus proche;
- Les coordonnées de toute autre personne impliquée, telles que des suspects ou des témoins.

QUOI ? L'HISTORIQUE DES ÉVÉNEMENTS EN ORDRE CHRONOLOGIQUE :

- La séquence des actions ayant mené à l'attaque informatique;
- Le montant total du préjudice (perte financière incluant les dommages directs et indirects);
- Les renseignements personnels compromis;
- Les applications ou logiciels téléchargés en lien avec l'attaque informatique. Spécifiez les noms d'utilisateurs, les mots de passe et les noms des personnes ayant accès aux mots de passe.

COMMENT ? LA MANIÈRE DONT L'ÉVÉNEMENT S'EST DÉROULÉ :

- La description la plus précise des étapes de l'attaque informatique;
- Les démarches que vous avez effectuées jusqu'à maintenant;
- Les répercussions de l'attaque informatique sur votre organisme et vos clients.