IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

AVIS DE L'OCRCVM

Avis relatif à la formation
Note d'orientation

Destinataires à l'interne :
Affaires juridiques et conformité
Audit interne
Comptabilité réglementaire
Crédit
Détail
Financement des entreprises
Formation
Haute direction
Inscription
Institutions
Opérations
Pupitre de négociation
Recherche
Technologie et cybersécurité

Personnes-ressources :
Suzanne Lasrado
Directrice de la réglementation des membres
et des stratégies (intérimaire)
416 943-5880
slasrado@iiroc.ca

Ryan Li
Directeur de la sécurité de l'information
416 943-5890
rli@iiroc.ca

21-0050
Le 16 mars 2021

Cybersécurité – Rançongiciels

Le présent avis décrit ce que les sociétés membres de l'OCRCVM et leurs employés doivent faire pour se prémunir contre une attaque par rançongiciel, la détecter si elle survient, y réagir et rétablir leurs activités. L'avis fournit également quelques renseignements sur le Groupe national de coordination contre la cybercriminalité de la GRC ou GNC3.

Aperçu

L'OCRCVM a constaté une augmentation des attaques par rançongiciel contre ses sociétés membres, en particulier au cours des derniers mois. Ces attaques, en constante évolution, constituent la forme de cybercriminalité la plus courante. Elles représentent une menace critique à laquelle les sociétés membres doivent continuer de prêter attention[1].

Un rançongiciel est un logiciel malveillant qui crypte et verrouille un dispositif (serveur, ordinateur, tablette ou téléphone cellulaire) et bloque ainsi l'accès aux informations qui s'y trouvent, jusqu'à ce qu'une rançon (comme des bitcoins) soit versée[2].

Si l'attaquant promet qu'il fournira une clé ou un code pour décrypter le dispositif lors du versement de la rançon, ce n'est pas toujours le cas dans les faits. Parfois, même si la rançon est payée, l'attaquant détruira l'information ou divulguera les données, en les mettant en vente sur le Web invisible.

Vecteurs de menace

Les rançongiciels sont généralement installés sur des appareils ou des réseaux par l'intermédiaire :

1) d'attaques d'hameçonnage, qui prennent la forme de liens ou de pièces jointes nuisibles envoyés par courrier électronique, messagerie texte et autres technologies de communication; il s'agit du vecteur de menace le plus courant;
2) de téléchargements furtifs, qui se produisent lorsqu'une personne accède à un site Web compromis ou clique sur une publicité malveillante sur un site Web légitime;
3) d'identifiants volés, disponibles sur le Web invisible en raison d'une exposition ou d'une attaque précédente;
4) d'une pénétration forcée de réseaux et serveurs Web vulnérables.

[1] Le Centre canadien pour la cybersécurité du gouvernement du Canada souligne également la menace que représentent les rançongiciels dans son Évaluation des cybermenaces nationales 2020.

[2] Pour plus d'informations, consultez le bulletin du gouvernement du Canada intitulé Le rançongiciel moderne et son évolution.

Mesures de protection, de reconnaissance et de détection recommandées

La meilleure façon de faire face à une attaque par rançongiciel consiste à empêcher son déploiement. Les sociétés membres doivent donc mettre en place des mesures de contrôle pour prévenir et reconnaître les rançongiciels, entre autres les suivantes :

1) **La mise en œuvre de contrôles, de politiques et de procédures** qui, au minimum :
   - établissent des processus pour :
     - réagir rapidement aux anomalies, ainsi qu'aux plaintes, aux appels et aux demandes de renseignements concernant des activités inhabituelles;
     - enquêter rapidement sur une attaque présumée afin d'en déterminer la cause et l'ampleur;
   - indiquent quel montant et quels types d'assurance couvrant la cybersécurité sont nécessaires, s'il y a lieu, en fonction des niveaux de risque de l'entreprise.
2) La mise en œuvre de **contrôles de sauvegarde des informations,** notamment :
   - en effectuant des sauvegardes de tous les systèmes et données, ce qui inclut les informations critiques, à faire aussi souvent que possible;
   - en testant les sauvegardes pour en assurer l'intégrité;
   - en conservant les données sauvegardées séparément du réseau de production et en maintenant des serveurs et un système de stockage distincts pour les données.
3) La mise en œuvre de **contrôles technologiques** pour protéger appareils et réseaux, notamment :
   - en mettant en œuvre de solides contrôles de gestion des accès, ce qui inclut la gestion des mots de passe, l'authentification à plusieurs facteurs et des outils de gestion des accès privilégiés pour les comptes dont les droits sont de niveau élevé (comme les comptes administrateurs) et qui permettent l'utilisation des fonctions de déploiement de logiciels;
   - en maintenant les systèmes d'exploitation à jour pour se protéger contre toute nouvelle vulnérabilité;
   - en mettant en place des outils de filtrage Web pour limiter l'accès des utilisateurs aux sites potentiellement malveillants;
   - en limitant ou en désactivant l'accès des bureaux à distance directement par Internet;

- en mettant en place une capacité antimaliciel ou antivirus aux points clés de l'environnement (p. ex., pour les couches régissant le réseau, le courriel et les points d'accès) – il faut envisager des services additionnels, comme des environnements de « bac de sable », processus qui consiste à tester les pièces jointes afin de chercher les activités malveillantes dans un environnement virtuel sûr);
- en mettant en œuvre une plate-forme de gestion des informations et des événements de sécurité (SIEM) regroupant les données liées aux incidents et à la sécurité provenant de sources multiples, afin de pouvoir réagir à une attaque et s'en relever.

4) **La sensibilisation des employés, des entrepreneurs et des consultants**, qui doivent faire preuve de vigilance lorsqu'ils cliquent sur les liens se trouvant dans les courriels et sur Internet, notamment :

   - en organisant fréquemment des formations et des tests de sensibilisation à l'hameçonnage, notamment en ce qui concerne l'importance de vérifier toutes les demandes d'authentification non initiées par l'utilisateur;
   - en rappelant aux employés :
     - d'informer immédiatement les Services informatiques s'ils remarquent une activité inhabituelle, par exemple un ralentissement de leurs appareils ou de leurs applications sans raison apparente;
     - l'importance de connaître les protocoles de réaction si leur appareil a été verrouillé par un rançongiciel.

5) **La surveillance des anomalies** pour détecter et atténuer une attaque :

   - en mettant en œuvre une fonction de surveillance continue de la sécurité (CSM) pour automatiser la veille antimenaces, ainsi que des solutions de détection et de réaction aux menaces au niveau des points d'accès (ETDR) pour détecter les logiciels malveillants et appuyer les activités d'enquête en cas d'attaque;
   - en mettant en place des outils permettant de surveiller en permanence les listes d'adresses IP malveillantes et frauduleuses connues, et de bloquer l'accès aux systèmes de l'entreprise depuis ces adresses;
   - en inspectant le trafic réseau pour y détecter toute activité malveillante;

- en surveillant les écarts anormaux dans les demandes de connexion ou l'activité informatique, y compris l'activité de mouvement latéral[3].

Méthodes d'intervention et de rétablissement recommandées

Les sociétés membres doivent mettre en place des contrôles pour répondre aux attaques par rançongiciels, notamment :

1) **en isolant immédiatement les dispositifs infectés** pour limiter la portée de l'attaque. Pour ce faire, elles doivent :
    - déterminer l'ampleur de l'attaque et isoler les appareils touchés ou les retirer du réseau;
    - protéger le réseau, notamment en effectuant des mises à jour, en suspendant les comptes suspects et en demandant aux clients d'établir de nouveaux mots de passe ou de créer de nouveaux comptes.
2) en déterminant **si elles disposent d'une sauvegarde récupérable** et quelles sont les informations perdues, le cas échéant. Ainsi, elles doivent :
    - restaurer les données de la dernière sauvegarde propre et s'assurer que :
        i. la sauvegarde ne contient aucun logiciel malveillant;
        ii. la capacité à mener une enquête informatique approfondie n'est pas entravée (p. ex., si la récupération des données entraîne la neutralisation d'anciens serveurs ou de machines virtuelles);
    - vérifier si un décrypteur est disponible pour déverrouiller toute information critique manquante depuis la dernière sauvegarde propre;
    - analyser soigneusement avec leur conseiller juridique toute décision de payer ou non la rançon en gardant à l'esprit le caractère nécessaire ou essentiel des informations perdues, la probabilité que l'agresseur tienne sa promesse et la visibilité possible que cette décision entraînera pour de futurs attaquants. Les responsables de l'application des lois déconseillent généralement de payer les rançons.
3) **en faisant enquête sur l'incident** pour déterminer la portée et l'étendue de l'attaque

[3] Le mouvement latéral désigne une tactique que les cyberattaquants utilisent – après s'être infiltrés et avoir obtenu un accès – pour pénétrer plus profondément dans le réseau et obtenir des privilèges élevés, et ce, dans le but de relever davantage de vulnérabilités et d'informations sensibles ou critiques.

(même si elle semble isolée de quelques dispositifs ou réseaux), c'est-à-dire :

- engager une équipe d'enquête informatique externe pour mener une enquête complète afin de déterminer la cause profonde et l'étendue de l'attaque. Souvent, le déploiement d'un rançongiciel constitue la dernière étape de l'attaque. En effet, le logiciel malveillant peut avoir séjourné dans le réseau ou l'appareil et avoir recueilli des informations avant d'être déployé;
- déterminer si une violation de données s'est produite et si l'attaquant derrière le rançongiciel aurait pu avoir accès à des informations exclusives et confidentielles. Si une violation s'est produite, il faut suivre tous les protocoles de réaction aux incidents, y compris la notification des personnes concernées.

4) **en signalant l'incident aux autorités compétentes**, aux commissaires à la protection de la vie privée, aux organismes de réglementation, et/ou aux responsables de l'application des lois. Si l'incident satisfait aux exigences de la Partie B.1.1 de la Règle 3100 des courtiers membres, *Déclaration liée à la cybersécurité*, la société doit communiquer avec le chef de la conformité des finances et des opérations de l'OCRCVM dont elle relève et lui fournir les renseignements exigés.

Groupe national de coordination contre la cybercriminalité de la GRC (GNC3)

Dans certains cas, les autorités policières locales peuvent communiquer de manière proactive avec une entreprise ayant été victime d'un cybercrime[4]. Souvent, les autorités chargées de l'application de la loi reçoivent de telles informations du GNC3.

Le GNC3 est un service national de police géré par la GRC. Il coordonne et harmonise les renseignements pour les enquêtes cybercriminelles à tous les niveaux des services policiers et favorise l'efficacité des activités d'application de la loi des partenaires nationaux et internationaux qui ont trait à la cybercriminalité, notamment en arrêtant des cybercriminels et en perturbant leurs activités. Fondamentalement, le GNC3 a pour objectif de réduire la menace, les incidences et la victimisation liées à la cybercriminalité au Canada et contribue à réaliser la vision à long terme du gouvernement du Canada en matière de sécurité dans l'ère numérique.

[4] Comme pour toute interaction de cet ordre, il faut vérifier de manière indépendante la légitimité de la communication et de l'expéditeur (p. ex., en obtenant les coordonnées de l'autorité en question – comme une adresse électronique ou un numéro de téléphone répertorié – ou bien en effectuant une recherche sur l'autorité ou la personne sur un dispositif non infecté).

Le 1er avril 2020, le GNC3 a atteint sa capacité opérationnelle initiale. En collaboration avec des organismes d'application de la loi, des gouvernements et des partenaires du secteur privé du Canada, le GNC3 :

- coordonne les enquêtes sur la cybercriminalité au Canada;
- collabore avec des partenaires à l'étranger pour lutter contre un vaste éventail d'incidents de cybercriminalité;
- prodigue des conseils sur les enquêtes aux corps policiers canadiens et leur donne accès à des capacités techniques.

Grâce à ses activités régulières et à son travail de coordination avec les autorités policières nationales et étrangères, le GNC3 est fréquemment en possession d'informations sur les victimes de la cybercriminalité au Canada. Le GNC3 fournit ces informations aux services de police locaux pour s'assurer que les victimes sont informées de l'incident et pour les encourager à déposer officiellement une plainte auprès de leur service de police. Dans des situations idéales, c'est-à-dire quand de telles informations sont fournies en temps opportun, celles-ci permettent d'alerter rapidement les victimes, ce qui contribue à atténuer les conséquences de l'incident.

Pour en savoir plus sur le GNC3, veuillez consulter le site Web de la GRC à l'adresse https://www.rcmp-grc.gc.ca/fr/gnc3.

Autres ressources

Vous trouverez des renseignements supplémentaires sur la gestion des cybermenaces ainsi que des ressources telles que des guides et des webinaires sur le site Web de l'OCRCVM, à la page Cybersécurité.