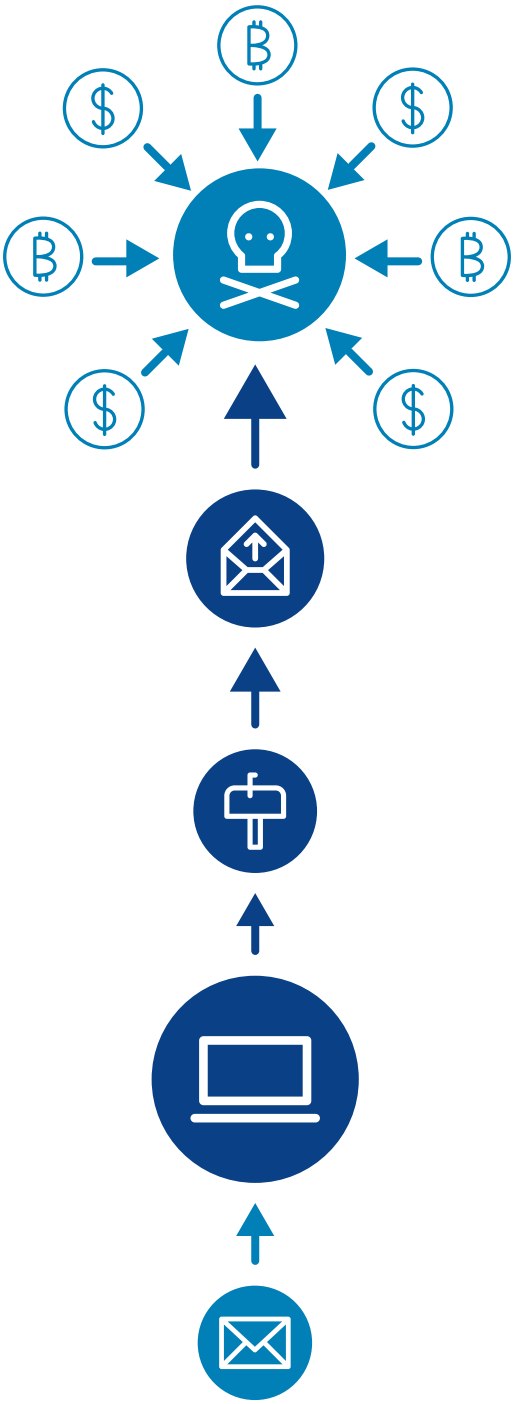
Deloitte.

Données prises en otage : l'essor des logiciels de rançon

Table des matières

Introduction



C'est une journée de travail comme les autres. Vous recevez un courriel vous informant qu'une facture destinée à votre service vient d'arriver et que vous devez la télécharger en cliquant sur le lien fourni. Machinalement, vous téléchargez et ouvrez le fichier. Quelque temps plus tard, vous vous apercevez que vous ne pouvez plus accéder à vos fichiers et que plusieurs copies d'un fichier intitulé « DECRYPT_YOUR_DATA.txt » ont été créées.

La panique vous gagne. Les fichiers sensibles qui sont sur votre ordinateur ont été chiffrés et il est probable que ce soit aussi le cas de ceux qui sont sur le réseau auquel vous êtes connecté. Ils ont été pris en otage au cours d'une **attaque par logiciel de rançon**, un crime informatique en plein essor.

Comme son nom l'indique, le logiciel de rançon, est un logiciel malveillant qui vise à rendre les données de la victime inutilisables ou à empêcher l'accès au système informatique jusqu'au versement d'une rançon, habituellement dans une monnaie numérique difficile à retracer. Le scénario décrit plus haut est un exemple d'attaque par un logiciel de rançon, un piège qui guette n'importe quel utilisateur. Une nouvelle version encore plus sinistre consiste à cibler des organisations. Une fois celles-ci infectées, le virus se propage pendant quelques mois et finit par paralyser le système, et c'est alors qu'une rançon est exigée.

Le logiciel de rançon est de plus en plus perfectionné : certaines variantes récentes peuvent pénétrer un système sans passer par internet, de sorte que leur source est presque impossible à retracer. La possibilité de réaliser un gain rapidement, conjuguée à son caractère furtif et au quasi-anonymat des opérations, rend ce type de cyberattaque attrayant pour les criminels.

De fait, les attaques par logiciels de rançon ont atteint des niveaux sans précédent partout dans le monde. On a dénombré plus d'incidents de ce genre dans les six premiers mois de 2016 qu'au cours des cinq dernières années combinées, et leur nombre devrait augmenter de manière exponentielle. La gravité de ces attaques est encore plus grande; des campagnes encore plus ingénieuses sont lancées contre des cibles qui ont la capacité de payer davantage et des raisons de le faire rapidement.

Le Canada n'est pas épargné : des attaques par logiciels de rançon se sont produites au pays au cours des trois dernières années, et leur nombre est en forte progression depuis quelques mois. Elles figurent maintenant parmi les trois principales préoccupations en matière de cybersécurité des organisations canadiennes.

Les victimes sont souvent prêtes à payer la rançon, quel qu'en soit le montant, pour reprendre le cours normal de leurs activités le plus rapidement possible. Elles ne sont pas différentes des familles qui n'hésitent pas à payer aux ravisseurs la somme qu'ils exigent pour libérer l'être cher. Étant donné les parallèles en matière de stratégie criminelle, il serait sans doute possible d'adapter avec succès les méthodes employées par les équipes d'intervention lors d'enlèvements de personnes à un cyberenvironnement. Nous avons pu constater lors des négociations que nous avons menées auprès de pirates informatiques que ces stratégies permettaient de gagner du temps, de réduire le montant de la rançon et de régler le problème rapidement.

Avant d'examiner les parallèles, il est important de comprendre ce qu'est un logiciel de rançon et pourquoi il est devenu le logiciel malveillant de prédilection des cybercriminels.

Une classe à part

L'attaque par logiciel de rançon se distingue des autres cyberattaques, puisque son objectif est d'amener la victime à verser de l'argent directement aux criminels. Lorsqu'ils ont recours à d'autres logiciels malveillants, les pirates doivent déployer plus d'efforts pour monnayer leur butin : par exemple, ils doivent répartir les cartes de crédit volées en lots d'une certaine taille et les vendre à différentes personnes, ce qui leur rapportera environ 5 $ par carte.

Une autre différence est que le but des logiciels de rançon n'est pas de voler des données, mais plutôt de bloquer l'accès à celles-ci jusqu'à ce qu'une somme d'argent change de mains. C'est une question d'accessibilité, tandis que les autres cyberattaques visent à enfreindre les principes de confidentialité (vol de données personnelles, renseignements relatifs à des cartes de crédit, etc.) et à compromettre l'intégrité (puisque les violations de la vie privée doivent être divulguées aux autorités).

Avec les logiciels de rançon traditionnels, la stratégie consiste à s'introduire dans un système informatique, à soutirer le plus d'argent possible et à en sortir rapidement, parce que plus il faut de temps pour obtenir la rançon, plus le plan risque d'échouer. C'est ce qui distingue ces attaques des cyberattaques habituelles. Mais les choses évoluent : le logiciel de rançon ciblé, qui gagne en popularité auprès des criminels, mise sur le temps.

Une fois introduit dans le système, ce logiciel malveillant repère les données les plus sensibles ou les plus précieuses de l'organisation, altère les sauvegardes pour les rendre inutilisables, crée des portes dérobées afin de faciliter une infiltration ultérieure et chiffre les données, et ce, avant même qu'une rançon ne soit exigée. Il peut causer des ravages discrètement pendant des mois avant que la victime ne se rende compte du problème. Et à ce moment-là, l'organisation est impuissante.

La perspective d'un gain rapide attire de nouveaux joueurs et change la donne

Pendant des années après la première attaque par logiciel de rançon connue, qui a été menée en 1989 au moyen de disquettes pour une rançon de 189 $ US, les criminels ont eu tendance à exiger un montant d'argent relativement peu élevé à un grand nombre de victimes, dont des particuliers. Même si l'accès opportuniste demeure le principal vecteur de virus, les criminels ciblent aujourd'hui des organisations précises; des cibles privilégiées disposant de ressources plutôt limitées en matière de cybersécurité et de données qui peuvent être nécessaires en situation de vie ou de mort, comme les hôpitaux. D'ailleurs, plusieurs hôpitaux ont fait l'objet d'une cyberattaque au début de 2016, notamment un centre de soins de santé de Los Angeles qui aurait versé une rançon de 17 000 $ US pour reprendre le contrôle de son système informatique. Les enjeux sont considérables – imaginez combien une organisation pourrait payer pour récupérer les données des dix dernières années de recherche sur le cancer.

Les criminels ont changé non seulement de cibles, mais aussi de méthodes. Il y a quelques années, ils privilégiaient la tactique passive du téléchargement furtif. Aujourd'hui, l'ingénierie sociale est leur arme de prédilection. On estime que 80 % des logiciels de rançon sont introduits lors du téléchargement de documents Office prenant en charge des macros, qui sont envoyés par un expéditeur se faisant passer pour une source légitime.

Aujourd'hui, la rançon négociée varie en moyenne entre 20 000 $ et 30 000 $, mais peut être beaucoup plus élevée. Des rapports indiquent que les victimes aux États-Unis ont versé plus de 325 millions de dollars américains aux créateurs du virus CryptoWall en 2015. Le potentiel de gain qu'offre ce logiciel malveillant a attiré des criminels plus astucieux, et ces attaques par logiciels de rançon risquent de se multiplier dans les années à venir.

Leçons tirées des services de gestion d'enlèvements et de rançons

Comme nous l'avons déjà fait remarquer, notre expérience de la gestion de crises provoquées par des logiciels de rançon auprès de clients nous a appris qu'il existe des similitudes entre les situations d'enlèvement et de demande de rançon qui visent des données et celles qui ciblent les personnes.

Enlever une personne et la garder en captivité jusqu'au paiement d'une rançon nécessite beaucoup de planification et est très risqué. En revanche, les logiciels de rançon permettent aux criminels de repérer les données sensibles d'une organisation sans même mettre les pieds dehors, ce qui réduit les risques et les coûts tout en augmentant le gain potentiel. Ils peuvent paralyser une organisation mal préparée bien plus que ne le ferait une prise d'otages.

Compte tenu des parallèles entre ces types d'actes criminels, il est important, selon nous, d'examiner les services et les tactiques de gestion de prises d'otages afin de concevoir un plan de défense et une stratégie de négociation en cas d'attaques par logiciel de rançon.

	Services types de gestion de prises d'otages humains	Services potentiels de gestion de prises d'otages informatiques
Prévention	• Évaluer la vulnérabilité du client (généralement, une personne nantie ou en vue). • Informer le client des risques ainsi que des moyens de détection des attaques et de protection.	• Évaluer la vulnérabilité du client (une entreprise ou une organisation). • Informer le client des risques, et lui apprendre à détecter et à prévenir les attaques. S'assurer qu'il instaure de saines pratiques en matière de cybersécurité. • S'assurer que le client possède une stratégie ou une méthode qu'il respectera à la lettre en cas d'attaque.
Assurance	• Vendre une assurance qui couvre la rançon, les honoraires d'avocats et de consultants, les pertes commerciales et le remplacement des employés.	• Vendre une assurance qui couvre la rançon, les honoraires d'avocats et de consultants ainsi que les pertes commerciales causées par le ralentissement ou l'interruption des activités, la destruction des données et l'atteinte à la réputation.
Gestion de crises	• Prendre des mesures d'intervention immédiate. • Gérer les relations avec les médias et les communications. • Appeler les consultants sur place. • Obtenir l'aide de la famille et de l'employeur.	• Mettre en œuvre la stratégie d'intervention étape par étape. • Résister à la tentation de se déconnecter du réseau. • Appeler les consultants sur place.
Négotiation	• Demander une preuve que l'otage est en vie. • Déterminer le motif de la prise d'otages (raison politique ou recherche d'un gain?). • Réduire progressivement le montant de la rançon exigée. • Évaluer le risque que les ravisseurs demandent une deuxième rançon.	• Demander une preuve de la capacité des pirates à déchiffrer les données (p. ex., une preuve de la clé de déchiffrement). • Réduire progressivement le montant de la rançon exigée. • Évaluer le risque que les pirates demandent une deuxième rançon.
Bilan	• Effectuer une évaluation des compromis. • Offrir un soutien psychologique. • Établir le profil des ravisseurs (recueillir des données qui pourraient être utiles ultérieurement). • Revenir à la phase de prévention.	• Effectuer une évaluation des compromis. • Suivre le plan de reprise des activités. • Établir le profil des pirates informatiques. • Revenir à la phase de prévention.

Soyez prêt

Comme pour toute menace informatique, la prévention est le meilleur moyen de défense. Sachez qu'à la différence des autres types de logiciels malveillants, les logiciels de rançon récents sont très difficiles à détecter : ils se déploient dès que l'utilisateur se connecte à internet, si tant est que cela soit nécessaire. Assurez-vous d'abord que votre organisation a un système de cybersécurité adéquat. Élaborez une stratégie de sauvegarde pour les données et les systèmes essentiels. Adoptez de bonnes pratiques de cybersécurité : par exemple, tenez à jour les programmes en installant tous les correctifs, surveillez l'activité sur le réseau et gérez en amont les niveaux d'autorisation. Offrez une formation aux employés afin qu'ils fassent preuve de prudence à l'égard des courriels, car l'ingénierie sociale est le principal moyen de pénétration des logiciels malveillants dans les réseaux des organisations ciblées.

Même si la prévention constitue la première étape essentielle de la protection d'une organisation, elle ne peut pas éliminer complètement les risques. Votre organisation doit également se préparer à une intrusion réussie de son système informatique en élaborant une stratégie en cas d'attaque par logiciel de rançon et un protocole d'intervention. Vous disposerez ainsi de lignes directrices de négociation claires que vous pourrez utiliser afin de gagner du temps, de récupérer vos données ou de prévenir une autre attaque. Dans certains cas, un protocole d'intervention clair peut permettre aux organisations d'évaluer si leurs données seront libérées une fois la rançon versée, ce qui n'a pas toujours été le cas récemment.

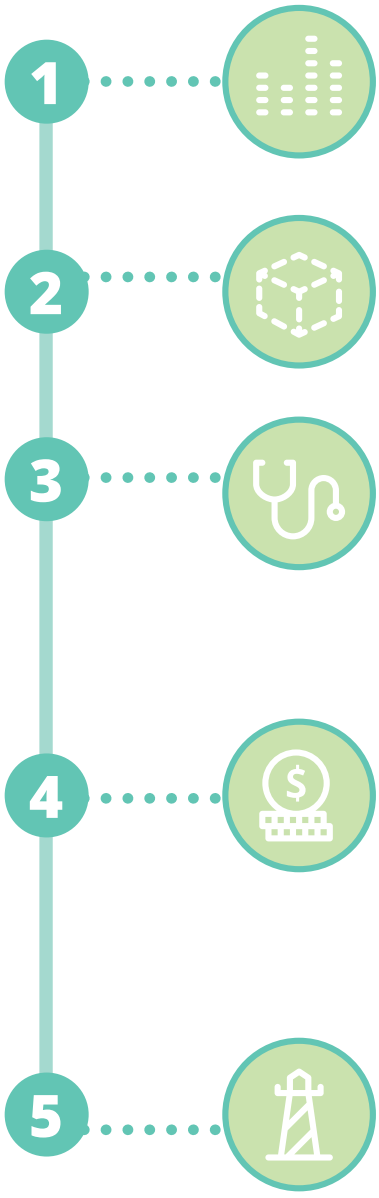
Il est important de suivre étape par étape la stratégie mise en place. La première de ces étapes devrait être : « Résister à la tentation de vous déconnecter du réseau ». Si vous vous débranchez, vous perdrez un avantage tactique, puisque vous ne pourrez pas surveiller le logiciel de rançon à l'œuvre ni constater l'ampleur des dommages. Vous ne pourrez pas voir si le logiciel malveillant s'est reproduit, a supprimé des points de récupération ou a créé une porte dérobée qui facilitera de futures infiltrations. Il vous sera donc impossible de savoir si vous pourriez faire l'objet d'une nouvelle tentative d'extorsion un jour.

Une organisation devrait aussi prendre des mesures pour réduire la probabilité de demande de rançon, notamment les suivantes :

- Utiliser des solutions perfectionnées de renseignements sur les menaces afin de repérer les indicateurs de compromis et d'intervenir plus rapidement lors des incidents.
- Mettre en œuvre de robustes technologies de sécurité des points d'extrémité à plusieurs niveaux, de sécurité de réseau, de chiffrement, d'authentification et de protection de la réputation. S'associer avec un fournisseur de services de sécurité gérés qui apportera son soutien à l'équipe des TI de l'organisation.
- S'assurer de la disponibilité d'un expert indépendant au moyen d'une avance sur honoraires, pour qu'il puisse aider l'organisation à gérer les crises. Mettre en œuvre un système de gestion des incidents pour optimiser l'infrastructure de sécurité à l'aide de processus mesurables et reproductibles, et améliorer de façon continue la sécurité de l'organisation en tirant profit des leçons apprises.
- Établir des lignes directrices, des politiques et des procédures relatives à la protection des données sensibles qui se trouvent dans les ordinateurs et les appareils mobiles de l'organisation. Évaluer régulièrement l'efficacité des équipes d'analyse internes et procéder à des exercices pour vérifier si l'organisation dispose des compétences nécessaires pour contrer les menaces informatiques.
- Conclure une entente tripartite avec un cabinet d'avocats et une entreprise spécialisée en cybersécurité. Si le système informatique est piraté et que les conseillers en cybersécurité retenus par l'organisation estiment que celle-ci n'a pas pris les précautions nécessaires, leur rapport pourrait constituer un élément de preuve dans l'éventualité d'une poursuite par les parties prenantes. Toutefois, dans le cadre d'une entente tripartite, le rapport appartiendrait au cabinet d'avocats et constituerait donc de l'information privilégiée.
- Élaborer une solide stratégie de sauvegarde qui repose sur des solutions hors site ou d'infonuagique afin d'assurer la récupération efficace des données en cas d'attaque par logiciel de rançon.

Vos données sont prises en otage? Ne cédez pas à la panique!

Dès que vous constatez que votre système fait l'objet d'une attaque par logiciel de rançon, appliquez le protocole et suivez les étapes dans l'ordre. En règle générale, ces étapes comprennent, entre autres, les suivantes :



Déterminez l'ampleur des dommages

Déterminez combien de fichiers ont été chiffrés et de quelle façon cette variante de logiciel de rançon perturbe vos activités. Évaluez aussi l'incidence que cette attaque pourrait avoir sur votre réputation si elle était rendue publique.

Isolez les systèmes touchés

La plupart des logiciels de rançon se propagent dans l'ensemble du réseau rapidement et discrètement. Déterminez quels systèmes sont touchés et isolez-les rapidement pour circonscrire le virus.

Vérifiez si les sauvegardes sont infectées

L'utilisation des sauvegardes est le meilleur moyen de rétablir les activités rapidement, mais seulement si elles ne sont pas également infectées. Inspectez-les avant de les déployer.

Devriez-vous verser la rançon?

Si votre réseau est fragilisé et que vous avez épuisé vos options (déployer les sauvegardes, gagner du temps, etc.), consultez des spécialistes avant de décider de payer la rançon. Les spécialistes chevronnés en cybersécurité peuvent négocier avec votre adversaire afin de régler la situation de manière efficace et en toute discrétion. Entre-temps, ne refusez pas de payer puisque vous ne savez pas ce que seraient les conséquences; le pirate pourrait, par exemple, détruire la seule clé de déchiffrement qui existe pour que vous ne puissiez jamais récupérer vos données. Dites-lui que vous paierez la rançon, mais que vous devez régler les détails du paiement. Vous gagnerez du temps, ce qui vous permettra de suivre les étapes de votre protocole.

Après l'incident, améliorez votre stratégie de prévention.

Utilisez les renseignements recueillis lors de l'attaque pour élaborer des politiques claires en matière de sécurité et en informer vos équipes.

Résumé

Lucratives et offrant un potentiel de gain rapide, les attaques par logiciel de rançon constituent une tactique intéressante qui ne devrait pas perdre de sa popularité. Les grandes organisations au portefeuille bien garni demeureront les cibles de choix, mais celles qui ont des moyens financiers plus limités, mais des données sensibles – comme dans les situations de vie ou de mort – pourraient se retrouver dans la ligne de mire des criminels.

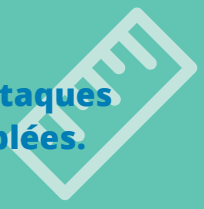
De la même manière que l'on prépare une personne fortunée en cas d'enlèvement, il est important de réduire le risque et de limiter les dommages potentiels d'une attaque par logiciel de rançon. Les organisations doivent commencer par se doter d'un bon système de cybersécurité, adopter de saines pratiques en matière de cybersécurité, établir un solide protocole pour ce genre d'incidents et sensibiliser le personnel aux enjeux liés aux logiciels malveillants.

Personne ne veut se sentir impuissant. Ayez un plan pour reprendre le contrôle de votre système avant que cela ne soit nécessaire.

Les réalités des attaques par logiciels de rançon

Perturbations majeures.

L'attaque par logiciel de rançon empêche la victime d'exercer normalement ses activités. Elle peut également entraîner une violation de la vie privée, une atteinte à la réputation, une fraude financière et des infections à d'autres entités dans la chaîne d'approvisionnement.



Attaques ciblées.

Des logiciels plus perfectionnés visent à pénétrer le système informatique et à perturber des organisations précises. En employant une tactique d'ingénierie sociale (leurrer des gens par des messages qui semblent légitimes), les criminels peuvent obtenir accès à des renseignements sur la structure de la société afin d'accroître la pénétration du logiciel malveillant et les dommages qui seront causés à ses données et sauvegardes les plus importantes.

Hameçonnage.

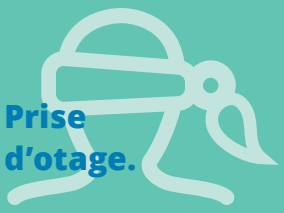
La grande majorité des logiciels de rançon se propagent par des campagnes d'envoi de courriels d'hameçonnage, ou harponnage, destinées aux employés d'organisations ciblées. Les destinataires sont invités à ouvrir des pièces jointes, la plupart prenant en charge les macros. Les criminels peuvent aussi infecter un système au moyen de publicités sur des sites Web légitimes, en profitant des réseaux publicitaires mal sécurisés.

Nouveau modèle d'affaires.

Un nouveau modèle de menace a vu le jour en 2015 : le logiciel de rançon-service (Ransomware-as-a-Service ou RaaS). Les pirates réinvestissent leurs profits dans la conception de logiciels malveillants et d'attaques encore plus complexes. Ils peuvent même exploiter un service d'assistance téléphonique 24 heures sur 24, 7 jours sur 7 pour aider les victimes ayant des problèmes techniques à payer la rançon en bitcoins ou à déchiffrer leurs données.

Monétisation garantie.

Les pirates choisissent désormais des victimes qui ont les moyens financiers et de bonnes raisons de verser une rançon. Les entreprises sont des cibles intéressantes, car elles sont souvent prêtes à payer rapidement le montant exigé afin de reprendre le contrôle de leurs données et de leurs activités. Et comme elles ne sont pas tenues de divulguer aux organismes de réglementation les intrusions qui ne contreviennent pas aux lois sur la protection de la vie privée (par exemple, les renseignements personnels au sujet des clients), elles sont donc plus susceptibles de ne pas rendre l'incident public et de payer les criminels pour qu'ils gardent le silence.



Prise d'otage.

Le pirate qui réussit à s'introduire dans un système informatique détermine le sort de vos données les plus importantes. Le temps de réaction est limité et la rançon peut augmenter rapidement si aucune mesure n'est prise. Les criminels peuvent détruire la seule clé de déchiffrement qui existe si la rançon n'est pas versée rapidement.

Pour en savoir plus

Si vous êtes victime d'une attaque par Logiciel de rançon ou si vous souhaitez en savoir plus, communiquez avec nous.

La réponse aux cyberincidents est devenue un processus à multifacette qui nécessite « Une seule réponse »; une approche proactive, coordonnée et orchestrée. Pour savoir comment votre organisation peut mettre en oeuvre cette approche, veuillez communiquer avec nous.

Rob Masse

Leader national du groupe de résilience
Associé, Services liés aux cyberrisques

514-393-7003
rmasse@deloitte.ca

Deloitte.

Deloitte, l'un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de la certification, de la fiscalité, de la consultation et des conseils financiers. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.