CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ

ÉVALUATION DES CYBERMENACES NATIONALES 2018

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

À PROPOS DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Lancé le 1er octobre 2018 sous l'égide du Centre de la sécurité des télécommunications (CST), le Centre canadien pour la cybersécurité (CCC) est un nouvel organisme qui hérite d'une riche histoire. Le CCC réunit sous un même toit des spécialistes en cybersécurité de l'ensemble du gouvernement du Canada. En phase avec la *Stratégie nationale de cybersécurité*, le lancement du CCC marque un tournant vers une approche plus unifiée à la cybersécurité au Canada.

Le CCC est formé d'une équipe d'experts en cybersécurité dignes de confiance, et son mandat clair et précis consiste à collaborer avec le gouvernement, le secteur privé et le milieu universitaire. Cette équipe, qui se compose de concepteurs, de créateurs, de développeurs, de chercheurs et de scientifiques, a pour rôle d'accroître la cybersécurité au Canada.

LE CCC ASSURE LA SÉCURITÉ DU CANADA ET DES CANADIENS :

Il fait office de **source fiable et crédible d'information sur la cybersécurité** pour les Canadiens, les entreprises canadiennes, ainsi que les propriétaires et exploitants d'infrastructures essentielles.

Il offre **des conseils ciblés et de l'orientation précise** sur la façon de protéger les cybersystèmes les plus importants pour le Canada.

Il développe et diffuse **ses technologies de cyberdéfense spécialisées et ses connaissances** afin de renforcer la cybersécurité pour tous les Canadiens.

Il assure la **défense des cybersystèmes**, dont ceux du gouvernement du Canada, en développant et déployant des outils et des technologies de cyberdéfense sophistiqués.

Il dirige les **activités d'intervention opérationnelle du gouvernement lors de cyberincidents**, tirant parti de son expertise et de ses accès de manière à fournir de l'information opportune et utile à la gestion des incidents.

La cyberdéfense, c'est un sport d'équipe. Le CCC met à profit cet avantage unique afin que le Canada puisse se défendre plus efficacement contre les cybermenaces et fasse preuve d'une plus grande résilience lorsque surviennent des cyberincidents.

POUR EN SAVOIR PLUS À CE SUJET, VISITEZ LE CYBER.GC.CA
OU SUIVEZ-NOUS SUR TWITTER @CENTRECYBER_CA

AVANT-PROPOS

Le Centre canadien pour la cybersécurité (CCC) est l'autorité du gouvernement du Canada en matière de cybersécurité. Il relève du CST, un organisme qui protège les renseignements et les réseaux les plus sensibles du Canada depuis plus de 70 ans. En phase avec la *Stratégie nationale de cybersécurité* publiée en juin 2018, le CCC a été mis en place afin que des experts en matière de sécurité puissent fournir des conseils et de l'orientation au gouvernement, aux partenaires du secteur privé, comme les propriétaires et exploitants des infrastructures essentielles, et à l'ensemble des Canadiens.

La présente évaluation des cybermenaces nationales donne un aperçu de l'environnement de cybermenaces auquel font face le Canada et les Canadiens. Elle vise à s'assurer que les Canadiens sont bien informés des cybermenaces qui pèsent sur le pays alors que les auteurs de cybermenaces cherchent de nouvelles façons d'utiliser le Web et les dispositifs connectés à Internet à des fins malveillantes. Vous constaterez que les noms de ceux qui ont été touchés par les cybercompromissions ne sont pas mentionnés, ce qui est délibéré. Cette évaluation a pour objectif d'analyser les auteurs de cybermenaces et leurs activités.

Le Canada est l'un des pays les plus branchés à l'échelle mondiale. Un cyberespace sécurisé est une condition essentielle à la sécurité, à la stabilité et à la prospérité nationales. Comme en témoigne la nature interconnectée des menaces mentionnées dans la présente évaluation, une cybersécurité efficace exige un effort collectif. C'est pourquoi le CCC travaille en étroite collaboration avec le gouvernement, les partenaires du secteur privé et le public afin de mettre en commun leurs connaissances uniques et l'expérience nécessaire pour améliorer la cybersécurité du Canada et de tous les Canadiens. Après tout, le renforcement de la cybersécurité du Canada est l'affaire de tous.

On sait déjà avec certitude que les Canadiens seront touchés par une cyberactivité malveillante au cours de la prochaine année. Cela dit, nous espérons qu'une bonne connaissance des menaces nous permettra de prendre les mesures nécessaires afin de les prévenir, de les détecter et d'assurer une intervention adéquate.

Bien que les cybermenaces envers le Canada et les Canadiens soient sérieuses, je suis convaincu qu'en travaillant ensemble, nous arriverons à assurer la résilience de notre pays contre les auteurs de cybermenaces.

Scott Jones
Dirigeant, Centre canadien pour la cybersécurité

www.cyber.gc.ca

RÉSUMÉ

Dans la société numérique hautement connectée qui est la nôtre, les Canadiens et les organismes canadiens dépendent d'Internet pour vaquer à plusieurs de leurs activités personnelles et professionnelles. C'est dans cette optique que nous évaluons les cybermenaces qui visent les citoyens, les entreprises et les infrastructures essentielles du Canada, ce qui comprend le gouvernement.

Les activités de cybermenace qui touchent les Canadiens comportent souvent des implications financières ou liées à la vie privée. Pourtant, celles qui ciblent les entreprises et les infrastructures essentielles du Canada peuvent avoir d'importantes conséquences, comme la perturbation des activités du secteur financier, le vol de vastes quantités de renseignements personnels et même de potentiels dommages à l'infrastructure.

FAITS SAILLANTS

- **La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes en 2019.** Elle prend de l'essor à mesure que les cybercriminels tirent parti de la croissance des marchés en ligne pour vendre des biens et services illicites et optimiser leurs profits. Les cybercriminels tendent à trouver leurs cibles par hasard en exploitant des vulnérabilités techniques et en tirant avantage de l'erreur humaine.
- **Les auteurs de cybermenaces – quel que soit leur degré de sophistication – accroîtront l'étendue de leurs activités en vue de voler de grandes quantités de données personnelles et commerciales.** Les données, comme la propriété intellectuelle et les renseignements personnels des Canadiens, sont utilisées à des fins de revente, de fraude, d'extorsion ou d'espionnage.
- **Il est fort probable que les Canadiens fassent l'objet d'activités malveillantes d'influence en ligne en 2019.** Au cours de la prochaine année, on s'attend à ce que les auteurs de cybermenaces parrainés par des États tentent de mener à bien leurs objectifs stratégiques nationaux en ciblant les opinions des Canadiens dans le cadre d'activités malveillantes d'influence en ligne.
- **Les auteurs de cybermenaces parrainés par des États continueront de mener des tentatives de cyberespionnage contre les entreprises et les infrastructures essentielles du Canada afin de réaliser leurs objectifs stratégiques nationaux.** Un plus grand nombre d'États-nations développent des cyberoutils conçus pour pratiquer le cyberespionnage.
- **Il est fort improbable que des auteurs de cybermenaces parrainés par des États perturbent volontairement les infrastructures essentielles du Canada s'il n'y a aucun climat d'hostilité à l'échelle internationale.** Par contre, il a également été déterminé que l'introduction d'un plus grand nombre de dispositifs connectés à Internet rendait les fournisseurs d'infrastructures essentielles plus susceptibles d'être la cible d'auteurs de cybermenaces moins sophistiqués, tels que les cybercriminels.
- **Les auteurs de cybermenaces sophistiqués continueront probablement de tirer parti des relations de confiance entre les entreprises et leurs fournisseurs de services** pour mener des activités cybercriminelles et d'espionnage.
- **Les auteurs de cybermenaces adoptent des méthodes plus avancées**, comme la compromission des chaînes d'approvisionnement du matériel et des logiciels, ce qui rend le processus de détection et d'attribution plus difficile.

L'adoption des pratiques les plus fondamentales en matière de cybersécurité peut permettre de contrer les auteurs de cybermenaces et de réduire les menaces visant les Canadiens et les entreprises canadiennes.

TABLE DES MATIÈRES

À PROPOS DU PRÉSENT DOCUMENT

Le présent document fait état des cybermenaces qui visent les citoyens, les entreprises et les infrastructures essentielles du Canada. À la lecture de cette évaluation, nous vous recommandons de consulter le document Introduction à l'environnement de cybermenaces. Cette introduction donne un aperçu des auteurs de cybermenaces, de leurs motivations et des cyberoutils à leur disposition, en plus de comprendre une annexe contenant les principales techniques et les principaux outils liés à la cybersécurité qui ont été utilisés dans la présente évaluation.

Comme le prévoit la *Stratégie nationale de cybersécurité*, le présent document a été préparé en vue d'aider les Canadiens à façonner et maintenir la cyberrésilience du pays. En effet, ce n'est qu'en misant sur la collaboration du gouvernement, du secteur privé et du public qu'il sera possible de renforcer la résilience du Canada contre les cybermenaces.

RESTRICTIONS

La présente évaluation n'a pas pour objet de fournir une liste exhaustive des activités de cybermenace ciblant le Canada ou des conseils en matière d'atténuation. Son objectif est plutôt de décrire et d'évaluer les menaces visant le Canada. Elle cherche à comprendre la nature de l'environnement de cybermenaces actuel et la façon dont les activités de cybermenace peuvent toucher les citoyens et les organismes canadiens. Il est également possible de trouver des conseils généraux sur le site Web du Centre canadien pour la cybersécurité, notamment Les 10 mesures de sécurité des TI et la campagne Pensez cybersécurité.

SOURCES

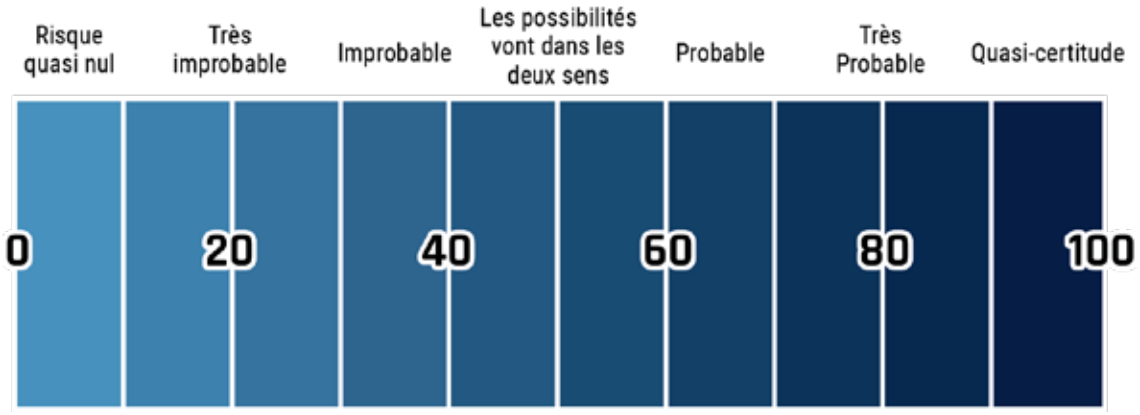
Les jugements formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du CCC en matière de cybersécurité. Le rôle que joue le CCC dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans l'environnement de cybermenaces, ce qui a contribué à la présente évaluation. Le mandat de renseignement étranger du CST lui procure de précieuses informations sur le comportement des adversaires dans le cyberespace. Bien qu'il soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses jugements.

PROCESSUS D'ÉVALUATION

Les évaluations des cybermenaces effectuées sont basées sur un processus d'analyse qui comprend l'évaluation de la qualité des renseignements disponibles, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploiera des termes comme « on considère que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « susceptible », « probable » et « très probable » pour exprimer les probabilités.

La présente évaluation des menaces se fonde sur des renseignements disponibles en date du 15 octobre 2018.

Le tableau ci-dessous fait coïncider le lexique des estimations à une échelle de pourcentage approximative. Ces nombres ne proviennent pas d'analyses statistiques, mais sont plutôt basés sur la logique, les renseignements disponibles, des jugements antérieurs et des méthodes qui accroissent la précision des estimations.



LES EFFETS D'UNE ACTIVITÉ DE CYBERMENACE

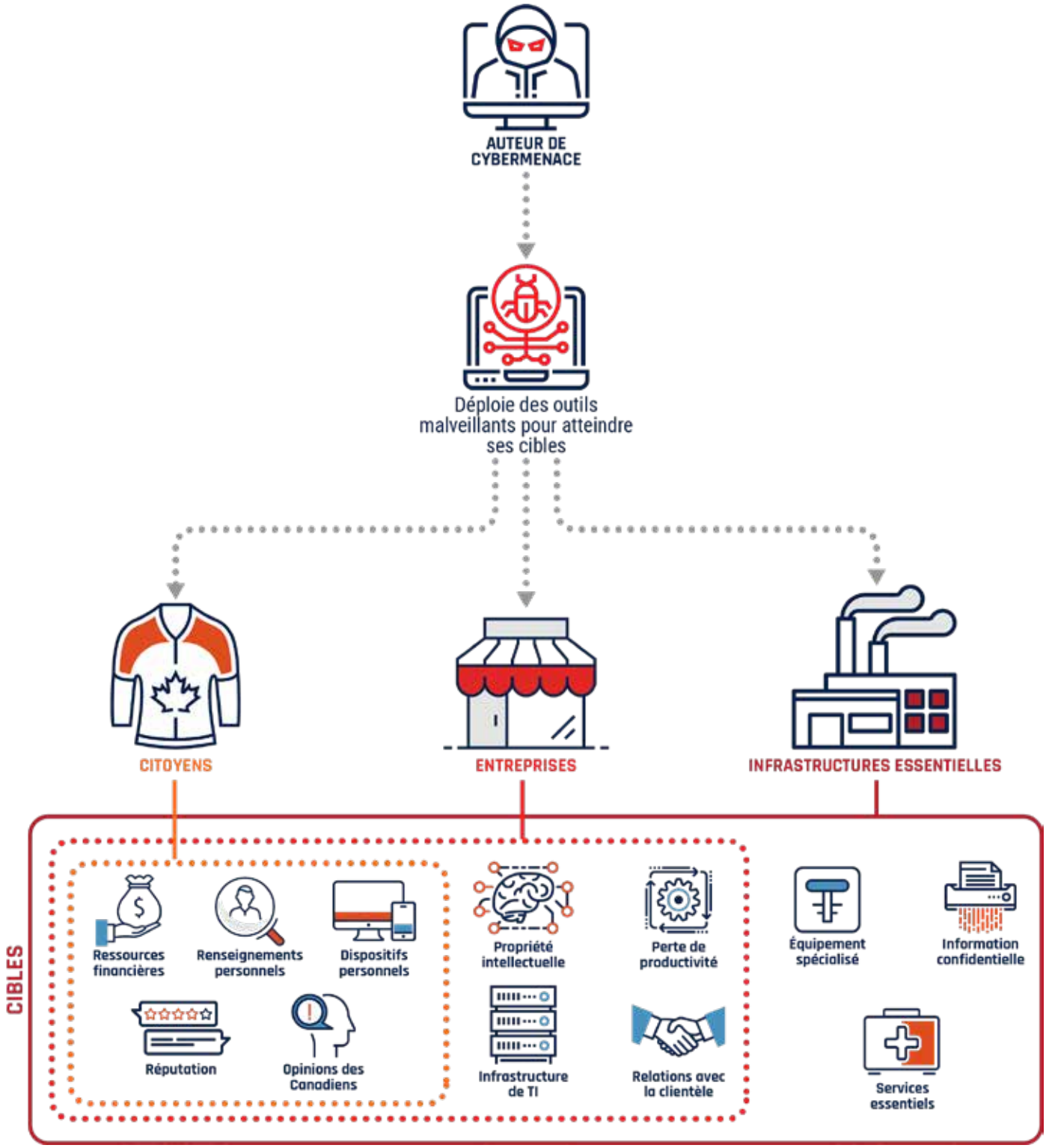
Les citoyens et les organismes canadiens sont de plus en plus « connectés ». Les auteurs de cybermenaces malveillantes – plusieurs d'entre eux opérant hors de nos frontières – se servent des lacunes en matière de sécurité, du manque de connaissances sur la cybersécurité et des récents développements technologiques pour tenter de compromettre les cybersystèmes. Dans la présente évaluation, on examinera la façon dont les activités de cybermenace touchent les citoyens, les entreprises et les fournisseurs d'infrastructures essentielles du Canada.[1]

Les auteurs de cybermenaces ciblent tout ce qui est connecté à Internet ou qui se trouve sur le Web, entre autres :

- la **technologie**, comme les dispositifs personnels et l'équipement industriel;
- l'**information**, comme la propriété intellectuelle, ainsi que les renseignements personnels et confidentiels;
- les **ressources**, comme les actifs financiers et la productivité;
- les **relations**, comme les chaînes d'approvisionnement et les services essentiels;
- nos **opinions** et notre **réputation**.

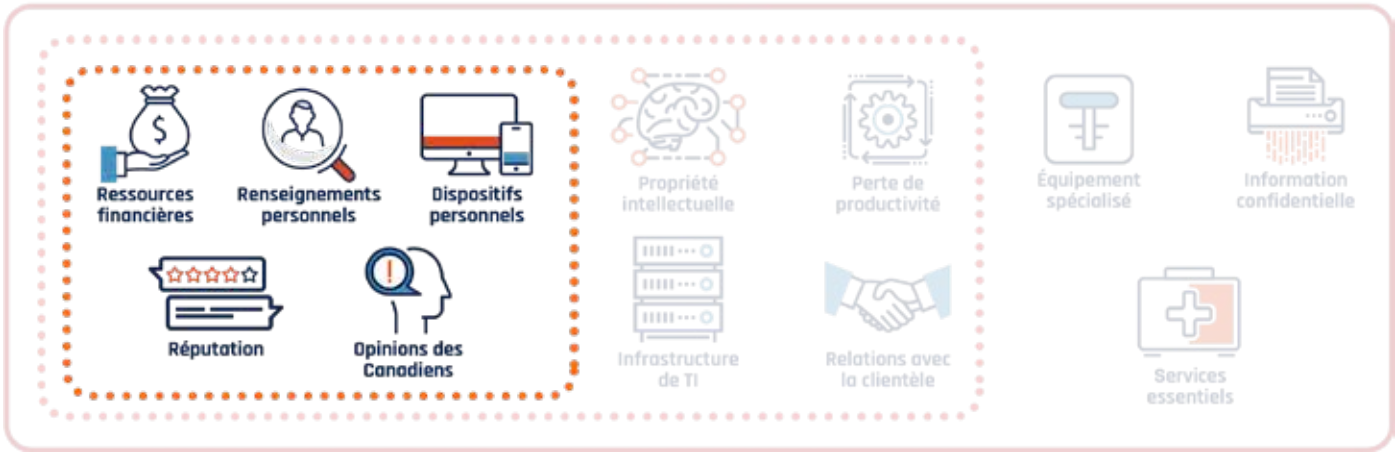
Figure 1 : Ciblage par des auteurs de cybermenaces

Les auteurs de cybermenaces déploient une panoplie d'outils malveillants pour atteindre leurs cibles. Certains types de cibles, comme l'information financière et bancaire ou les renseignements personnels, appartiennent à des personnes et des organismes. Certains systèmes susceptibles d'être ciblés par les auteurs de cybermenaces, comme les réseaux du gouvernement utilisés pour assurer des services essentiels, sont détenus par des fournisseurs d'infrastructures essentielles.



LES CYBERMENACES CONTRE LES CANADIENS

CIBLES



CYBERCRIMINALITÉ

Les Canadiens stockent davantage d'information en ligne, ce qui fait d'eux une cible de plus en plus attrayante pour les auteurs de cybermenaces. Dans la mesure où les cybercriminels continuent de s'adapter et d'améliorer leurs cybercapacités afin de voler les Canadiens, de les frauder et de leur soutirer de l'argent, on considère que la cybercriminalité est la cybermenace à laquelle les citoyens et les organismes canadiens sont plus susceptibles d'être confrontés.[2]

Vol de renseignements personnels et financiers

Le vol de renseignements personnels et financiers s'avère fort lucratif pour les cybercriminels, et on peut s'attendre à ce que cette pratique prenne de l'ampleur. Les cybercriminels font des profits au détriment des Canadiens en usurpant les justificatifs d'ouverture de session de leurs comptes, les détails relatifs à leurs cartes de crédit et d'autres renseignements personnels. Ils exploitent cette information dans le but de la revendre sur les marchés noirs de la cybercriminalité, de voler de l'argent ou encore de commettre une fraude ou de l'extorsion. De plus en plus, on voit les cybercriminels s'organiser et mettre en place des processus « d'affaires » pour étendre leurs activités et tirer avantage des vulnérabilités liées aux logiciels, au matériel et au comportement humain en ligne. Par exemple, des cybercriminels ont conçu au cours des dernières années des **chevaux de Troie bancaires** spécifiques aux téléphones mobiles afin de voler les données des utilisateurs et de cibler les ressources financières.

La cybercriminalité est maintenant si répandue et sophistiquée qu'elle arrive à alimenter les marchés clandestins en ligne. Ces marchés noirs de la cybercriminalité proposent des biens illicites, des renseignements volés et des **maliciels**. Certains offrent même du soutien à leurs utilisateurs et des fonctions d'évaluation. La grande accessibilité et la convivialité des cyberoutils favorisent l'expansion de la cybercriminalité et permettent aux cybercriminels de mener leurs activités à l'échelle mondiale, souvent depuis des zones hors d'atteinte des organismes canadiens de l'application de la loi.

Exposition accrue aux cybermenaces

L'exposition des Canadiens aux cybermenaces est plus grande en raison du nombre croissant de dispositifs connectés à Internet, comme les téléviseurs, les appareils électroménagers, les thermostats et les voitures. Les fabricants se sont empressés de connecter à Internet des dispositifs de différents types, accordant souvent plus d'importance à la convivialité qu'à la sécurité. Selon nos observations, les auteurs de cybermenaces exploitent régulièrement les vulnérabilités informatiques de ces dispositifs, que ce soit en nuisant à leur bon fonctionnement ou en les utilisant comme plateformes pour lancer d'autres cyberactivités malveillantes.

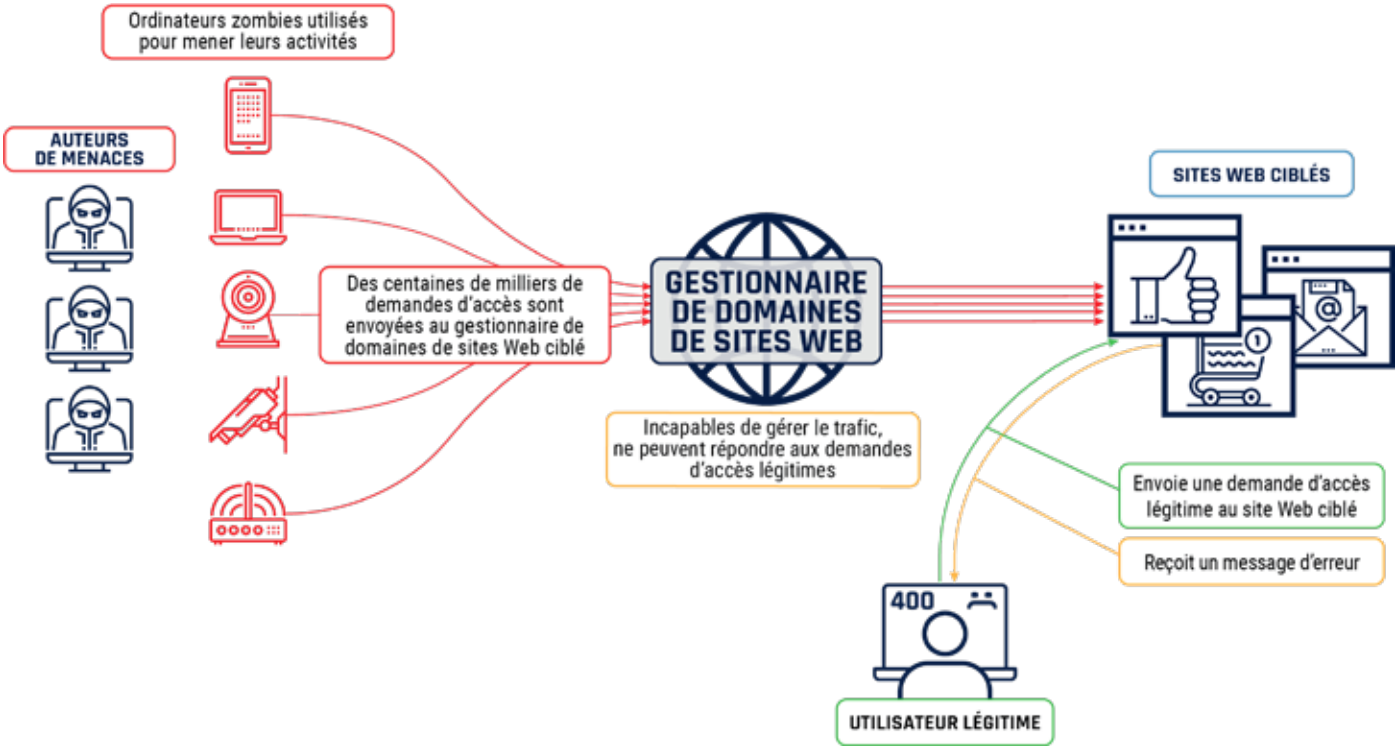
On a également pu constater que des maliciels avaient été utilisés pour trouver les vulnérabilités de systèmes, permettant ainsi aux auteurs de cybermenaces de mener des activités non autorisées, comme la mise en place d'un **réseau de zombies**. De fait, on considère que les auteurs de cybermenaces sont maintenant plus susceptibles d'utiliser des dispositifs connectés à Internet plutôt que des ordinateurs personnels pour mettre en place leurs réseaux de zombies.

PERTURBATION DU FOURNISSEUR DU SYSTÈME D'ADRESSAGE PAR DOMAINES

En octobre 2016, des cybercriminels ont utilisé un réseau de zombies composé de milliers de dispositifs connectés à Internet et mal sécurisés pour tenter de gonfler artificiellement leurs recettes publicitaires en ligne. Parmi les dispositifs compromis, on retrouvait des routeurs, des dispositifs de surveillance de la qualité de l'air, des interphones de surveillance, des caméras de surveillance et d'autres types d'équipement utilisant des noms d'utilisateurs et mots de passe par défaut. Le réseau de zombies a mené une massive attaque par déni de service distribué qui a provoqué l'arrêt du gestionnaire de domaines d'un important site Web, désactivant temporairement, pour des millions d'utilisateurs, l'accès à certains des plus populaires sites de commerce en ligne, de divertissement et de médias sociaux. L'un des cybercriminels a diffusé ce maliciel dans un groupe de discussion consacré à la cybercriminalité, ce qui a permis à d'autres auteurs de cybermenaces de créer des variantes du réseau de zombies pour mener d'autres activités malveillantes.[3]

Cette étude met en évidence la façon dont les cybercriminels peuvent exploiter une panoplie de dispositifs pour mener des opérations d'envergure et faire la promotion de leurs capacités. Les cybercriminels mettent en commun et modifient le code source des maliciels dans le but de masquer leur identité pour ainsi éviter les conséquences juridiques.

Figure 2 : Attaque par déni de service distribué



Financement des activités criminelles

Le nombre sans cesse grandissant de dispositifs connectés à Internet a également offert aux cybercriminels l'occasion de mener des activités de cryptominage au moyen de maliciels. Ils utilisent des maliciels pour contrôler la puissance de traitement d'un dispositif de manière à servir leurs propres intérêts, nuisant ainsi au bon fonctionnement du dispositif. Selon le type de maliciels, certains utilisateurs touchés peuvent ne rien voir d'inhabituel avec leur dispositif, tandis que d'autres peuvent constater des problèmes de ralentissement, une décharge rapide de la pile, des frais de données accrus ou une durée de vie plus courte de l'appareil.[4] En 2019, on s'attend à ce que les cybercriminels continuent de développer des maliciels afin d'effectuer du cryptominage non autorisé, en particulier si la valeur de la cryptomonnaie augmente.

Figure 3 : Rançongiciel

Fraude et extorsion

Selon nos observations, les types de tentatives de cyberfraude et d'extorsion visant les Canadiens ont gagné en sophistication. On s'attend à ce que cette tendance se poursuive à mesure que les cybercriminels acquièrent de nouveaux outils. Les auteurs de cybermenaces commettent des fraudes en se faisant passer pour des organismes légitimes, tels que des institutions gouvernementales, des établissements financiers ou des cabinets d'avocats, afin d'inciter les Canadiens à télécharger les maliciels sur leurs dispositifs en cliquant sur les liens ou les fichiers joints malveillants. On a également pu constater que les auteurs de cybermenaces se faisaient passer pour des fournisseurs de logiciels dignes de confiance en diffusant des publicités destinées à tromper les utilisateurs peu méfiants et à les amener à télécharger des maliciels.

FAUX MESSAGE DE L'AGENCE DU REVENU DU CANADA

Des auteurs de cybermenaces se faisant passer pour l'Agence du revenu du Canada (ARC) ont envoyé des courriels et des messages texte malveillants aux Canadiens, leur demandant de fournir de l'information personnelle comme leur numéro d'assurance sociale, l'information relative à leur carte de crédit ou le numéro de leur passeport. Dans certains cas, on prétendait que le contribuable devait fournir des renseignements personnels afin de recevoir un remboursement. Dans d'autres, on menaçait les destinataires et les sommait de payer une dette imaginaire.[5]

Des arnaques de ce genre nous rappellent qu'il n'est pas si difficile pour les auteurs de cybermenaces de trouver ou développer du contenu semblant provenir d'une source légitime et digne de confiance. Les messages d'hameçonnage conçus pour paraître légitimes sont une forme de compromission simple, courante et souvent fort efficace. Il est probable que les liens et documents joints à ces messages soient malveillants et contiennent des chevaux de Troie bancaires ou d'autres maliciels que les auteurs de cybermenaces pourront utiliser pour voler l'argent ou l'identité des Canadiens.

Les cybercriminels ont recours à des cyberoutils et au piratage psychologique pour soutirer de l'argent ou de l'information aux Canadiens.[6] Le **rançongiciel** est le type de maliciel le plus souvent utilisé dans les tentatives d'extorsion. Après avoir infecté les dispositifs au moyen d'un rançongiciel, les auteurs de cybermenaces tentent d'extorquer de l'argent aux propriétaires en chiffrant leurs données. Les rançongiciels ne sont plus considérés comme des cyberoutils de pointe, puisque des auteurs de cybermenaces peu sophistiqués peuvent désormais se les procurer sous forme de service qu'ils louent ou achètent sur les marchés noirs de la cybercriminalité.

LES STRATAGÈMES D'EXTORSION ET LE MARCHÉ NOIR DE LA CYBERCRIMINALITÉ

À l'été 2018, certains Canadiens ont indiqué avoir reçu un message les menaçant de diffuser une vidéo compromettante supposément enregistrée alors qu'ils regardaient de la pornographie. Dans leur message, les auteurs de cybermenaces avaient inclus un mot de passe, suggérant qu'ils avaient réussi à compromettre les dispositifs des destinataires. Les auteurs de cybermenaces demandaient ensuite que des bitcoins leur soient transférés, sans quoi ils enverraient la vidéo à tous les contacts des destinataires. En réalité, les dispositifs des utilisateurs n'avaient pas été compromis, et les auteurs de cybermenaces n'avaient pas enregistré de vidéo. Les personnes qui n'ont pas payé la somme demandée n'ont reçu aucun autre message.[7]

Cette étude illustre la façon dont les cybercriminels se rendent mutuellement service. Il est fort probable que les mots de passe utilisés dans ce stratagème provenaient d'une des nombreuses violations de données dans le cadre desquelles des justificatifs d'ouverture de session avaient été volés sur un site Web. Ces justificatifs composés des adresses courriel et des mots de passe ont probablement été mis en vente sur le marché noir de la cybercriminalité par un cybercriminel, avant d'être achetés par un autre dans le but d'envoyer des messages de menace. Ce stratagème mise sur les peurs les plus courantes, comme la violation de la vie privée et l'embarras.

ACTIVITÉS MALVEILLANTES D'INFLUENCE EN LIGNE

En plus de commettre des cybercrimes, les auteurs de cybermenaces cherchent également à manipuler nos opinions. Plusieurs plateformes Web, dont les médias sociaux, connectent les utilisateurs à leur contenu et leurs produits au moyen d'outils légitimes conçus aux fins de publicité et d'échange d'information. Or, les auteurs de cybermenaces parrainés par des États tentent d'exploiter ces outils légitimes afin de mener des activités malveillantes d'influence en ligne et de réaliser les objectifs stratégiques de leur pays. On estime qu'en 2019, il est fort probable que les auteurs de cybermenaces parrainés par des États s'efforcent de mener à bien les objectifs stratégiques de leur pays en ciblant les opinions des Canadiens dans le cadre d'activités malveillantes d'influence en ligne.

Les auteurs de cybermenaces parrainés par des États peuvent mener des activités sophistiquées d'influence en ligne en se faisant passer pour des utilisateurs légitimes. Ils créent des comptes sur les médias sociaux ou s'approprient des profils existants pour promouvoir du contenu dans le but de manipuler les gens. Ils mettent en place des « usines à trolls » qui se composent d'employés payés pour envoyer des commentaires et partager du contenu sur les sites Web des médias traditionnels, les médias sociaux et tout autre site susceptible d'atteindre le public ciblé. Les auteurs de cybermenaces tentent également de voler de l'information en vue d'en faire la divulgation, de la modifier de manière à ce qu'elle soit plus intéressante ou distrayante, de créer des « nouvelles » frauduleuses ou erronées, ou encore de faire valoir des opinions radicales.[8]

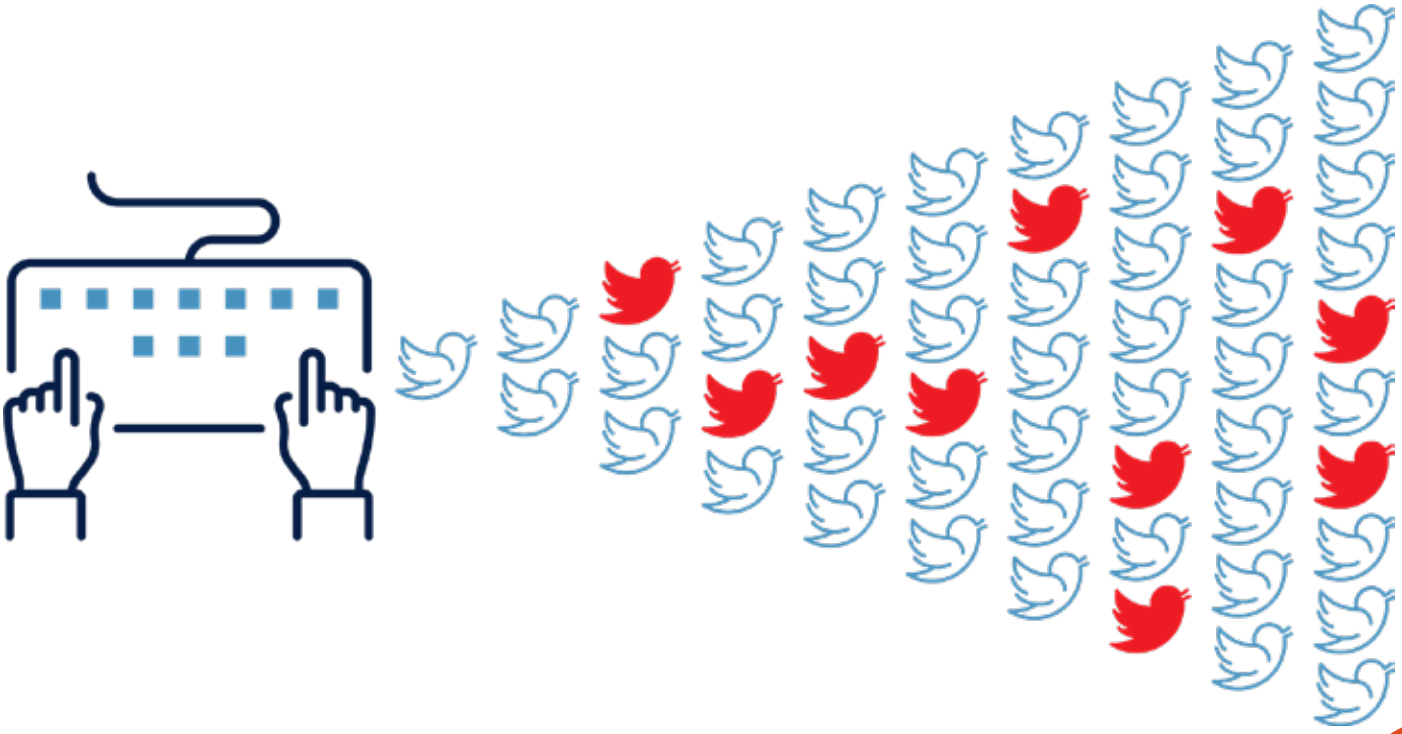
Par ailleurs, les auteurs de cybermenaces peuvent amplifier – ou étouffer – le contenu des médias sociaux au moyen de réseaux de zombies, ce qui permet d'automatiser les interactions en ligne et d'échanger du contenu avec des utilisateurs peu méfiants. Les réseaux de zombies peuvent partager des mèmes, promouvoir des mots-clics et harceler des utilisateurs légitimes pour créer l'illusion que des centaines, des milliers, voire des millions de gens sont d'accord avec le point de vue des auteurs de cybermenaces. Ces derniers peuvent promouvoir un point de vue en particulier et influencer les Canadiens en diffusant le contenu qu'ils privilégient à de grands nombres d'utilisateurs, tant légitimes qu'illégitimes. Alors que les plateformes Web les plus populaires s'efforcent d'atténuer les effets négatifs de l'échange d'informations manipulatrices, les opinions des Canadiens demeurent une cible alléchante pour les auteurs de cybermenaces qui cherchent à influencer le processus démocratique du Canada.

DES TROLLS RUSSES SE SAISISSENT DES ENJEUX CANADIENS

Une récente étude a révélé que des comptes Twitter associés à l'Internet Research Agency, une organisation russe ayant fait la promotion de contenu incendiaire destiné à semer la division avant les élections présidentielles de 2016 aux États-Unis, avaient également publié des gazouillis concernant des événements au Canada. Parmi les 3 millions de gazouillis archivés à partir de comptes qui ont depuis été supprimés, environ 8 000 mettaient l'accent sur des enjeux canadiens, notamment les incendies à Fort McMurray en mai 2016, la fusillade dans une mosquée de Québec en janvier 2017, et l'augmentation du nombre de demandeurs d'asile ayant traversé la frontière à l'été 2017. Les trolls russes ont tenté de créer de la confusion en faisant circuler de la fausse information dans les discussions en ligne et en exacerbant les différences d'opinions existantes.[9] Cette étude démontre que les utilisateurs canadiens de médias sociaux peuvent être exposés à des activités malveillantes d'influence de l'étranger.

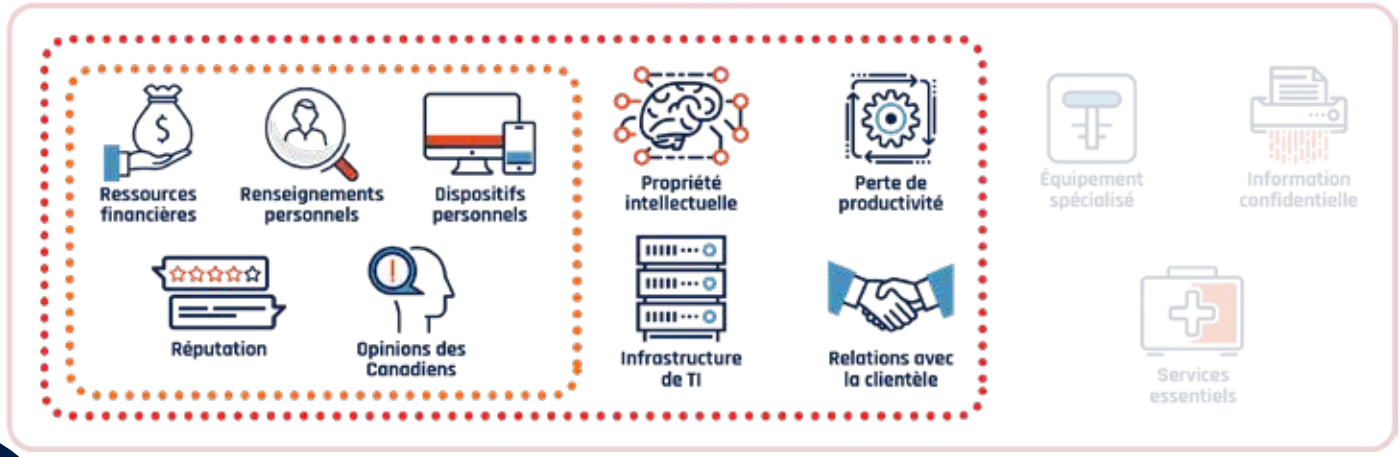
Les auteurs de cybermenaces parrainés par des États qui tentent d'influencer le processus démocratique ont également les capacités nécessaires pour cibler les organismes qui prennent part aux élections, ainsi que les politiciens, les partis politiques et les médias traditionnels. Pour une analyse plus poussée, prière de consulter le rapport intitulé Cybermenaces contre le processus démocratique du Canada (2017) du Centre de la sécurité des télécommunications.

Figure 4 : Les auteurs de cybermenaces publient en ligne du contenu faux et trompeur



CYBERMENACES CONTRE LES ENTREPRISES CANADIENNES

CIBLES



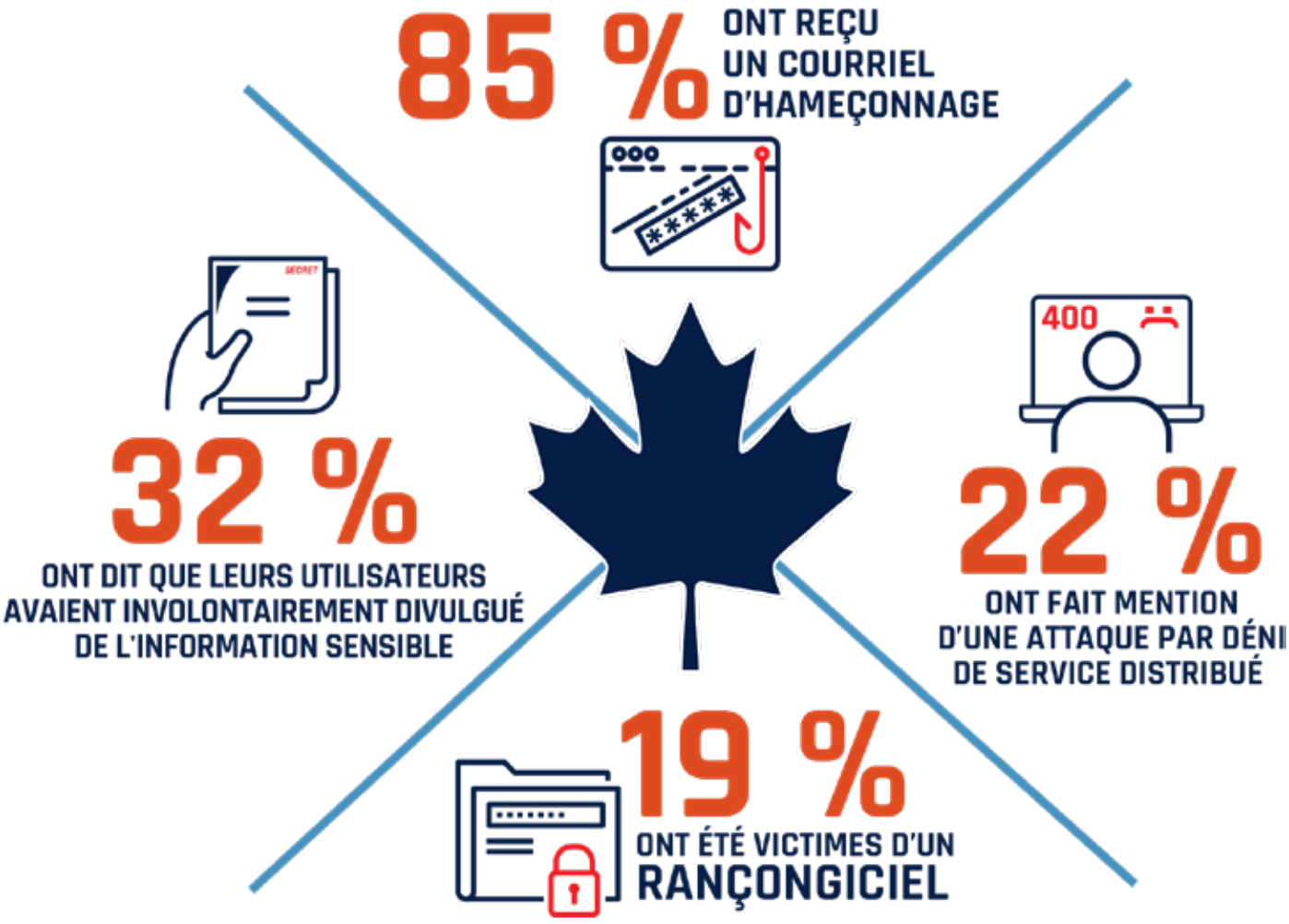
On considère que les cybercriminels sont la plus grande cybermenace contre les entreprises de toutes tailles et continueront de l'être en 2019. Les auteurs de cybermenaces ciblent les entreprises canadiennes pour obtenir des données relatives à leurs clients, partenaires et fournisseurs, des données financières, des renseignements sur leurs systèmes de paiement, ainsi que de l'information exclusive.

L'information volée fait souvent l'objet d'une demande de rançon. Elle peut aussi être vendue et utilisée afin de tirer un avantage concurrentiel. En plus des pertes financières résultant du vol ou du paiement de rançons, les cyberincidents peuvent porter atteinte à la réputation, entraîner une perte de productivité, mener au vol de propriété intellectuelle, donner lieu à des perturbations et exiger des dépenses relatives à la reprise.

Ciblage des dirigeants d'entreprise

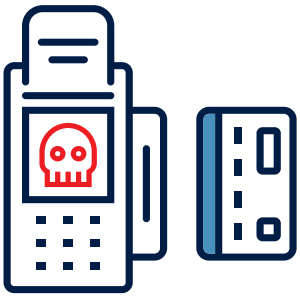
Les auteurs de cybermenaces emploient des techniques de piratage psychologique propres aux entreprises. La **chasse à la baleine** est une méthode de plus en plus courante. Ce type de harponnage vise spécifiquement les cadres supérieurs et les autres destinataires de grande notoriété disposant d'un accès privilégié aux ressources de l'entreprise. Une telle cybermenace survient lorsqu'un cadre supérieur autorisé à effectuer de larges paiements reçoit un message qui semble provenir d'un service ou employé pertinent, lui enjoignant de transférer des fonds dans un compte contrôlé par un auteur de cybermenace. Ce type de piratage psychologique peut mener à des pertes financières considérables et à une atteinte à la réputation. Or, il exige des renseignements internes souvent difficiles à obtenir. Comme c'est le cas pour les autres techniques de piratage psychologique, la chasse à la baleine a pour but d'exploiter un comportement humain prévisible.

Figure 5 : Sondage de l'Autorité canadienne pour les enregistrements Internet de 2017-2018[10]
Selon un sondage auprès de 1 985 Canadiens ayant été propriétaires d'un domaine « .ca » entre novembre 2017 et janvier 2018, dont des sites Web personnels et d'entreprise



Exploitation de la technologie du commerce de détail

Les auteurs de cybermenaces ciblent également les systèmes des points de vente utilisés dans le secteur du commerce de détail et dans l'industrie du tourisme d'accueil. En ciblant les systèmes de TI désuets, les auteurs de cybermenaces sont en mesure d'installer des maliciels afin de voler l'information des clients, de nuire aux activités de l'entreprise, d'effectuer des achats frauduleux, de manipuler les prix et de provoquer d'autres formes de perturbation.



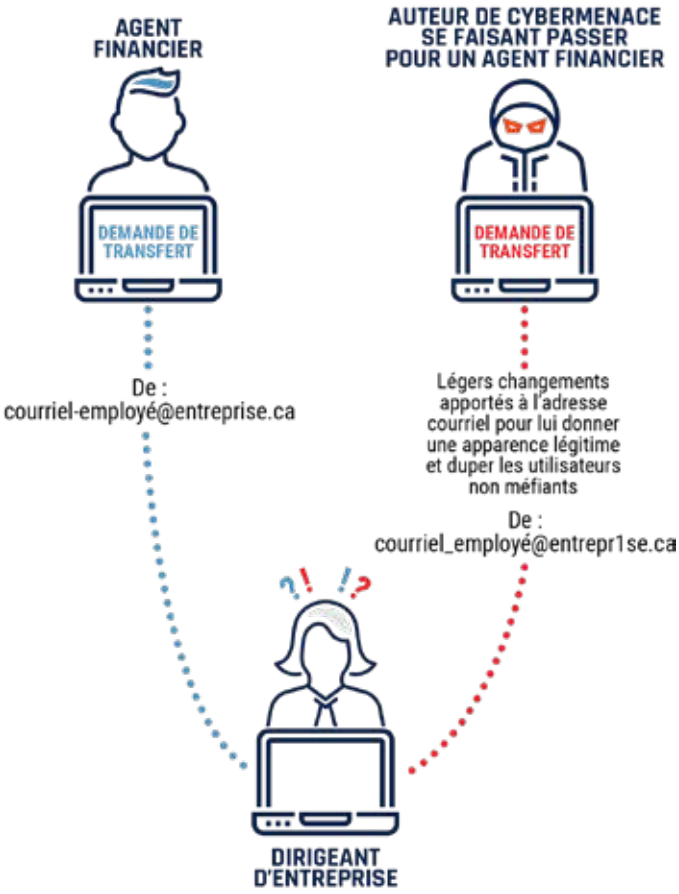
Les numéros de cartes de crédit volés se vendent sur les marchés noirs de la cybercriminalité à des prix variés, mais dérisoires. De plus, les cybercriminels peuvent jumeler les numéros de cartes de crédit avec les renseignements personnels de leurs détenteurs, comme leur adresse et le nom de jeune fille de leur mère. Comme les marchés noirs de la cybercriminalité offrent également les données stockées dans la bande magnétique des cartes de crédit, les criminels peuvent recréer les cartes. À l'instar des marchés légaux, les vendeurs proposent des rabais pour les achats en lot.

PROJET ADORATION

En janvier 2017, la Gendarmerie royale du Canada (GRC) a démantelé un site Web hébergeant 3 milliards de dossiers personnels obtenus dans le cadre de violations de données d'envergure commises à travers le monde. Bien que les serveurs repérés par la GRC se trouvaient au Canada, des utilisateurs de partout dans le monde pouvaient accéder à l'information moyennant des frais modiques. En décembre 2017, la GRC a inculpé un individu soupçonné d'avoir trafiqué l'information nominative.[11]

Cette étude illustre la façon dont les cybercriminels tirent profit des renseignements personnels volés dans le cadre de violations de données. Alors que les cybercriminels exploitent la nature transnationale d'Internet, des opérations comme le Projet Adoration, auquel ont coopéré la GRC, la Police nationale des Pays-Bas et le Federal Bureau of Investigation des États-Unis, rendent compte de l'évolution des méthodes et des systèmes utilisés par les organismes chargés de l'application de la loi pour s'attaquer à la cybercriminalité. Cette étude met en lumière le fait que les partenariats internationaux sont souvent indispensables à la tenue des enquêtes et à l'engagement de poursuites contre les cybercriminels.

Figure 6 : Chasse à la baleine



ATTEINTES À LA PROTECTION DES DONNÉES

Vol des données relatives aux clients

Les auteurs de cybermenaces ont la volonté et les moyens d'obtenir de l'information sensible, comme en témoignent les nombreuses atteintes à la protection des données très médiatisées qui ont ciblé les données de millions de consommateurs à l'échelle internationale. Ils attachent une valeur considérable aux grandes bases de données qui contiennent des renseignements personnels, tels que des noms, des adresses, des numéros de téléphone, des données financières et de l'information relative à l'emploi. L'agrégation des données obtenues lors de multiples compromissions permet aux auteurs de cybermenaces de bâtir des profils exhaustifs qu'ils pourront utiliser pour cibler des groupes ou des personnes en particulier.

Selon la présente évaluation, il est fort probable qu'en 2019, les grandes bases de données demeurent une cible de choix pour les auteurs de cybermenaces qui cherchent à vendre l'information ou qui se livrent à l'espionnage pour le compte d'un État.

L'EXTORSION AU MOYEN DES DONNÉES DE CLIENTS

En mai 2018, des cybercriminels ont communiqué avec deux institutions financières canadiennes. Ils prétendaient avoir eu accès aux renseignements personnels de dizaines de milliers de clients et menaçaient de divulguer ces renseignements à moins qu'une rançon de 1 million de dollars ne leur soit versée. Les deux institutions financières ont refusé de payer, offert aux clients une surveillance gratuite de leur crédit, et promis de rembourser toute somme frauduleusement prélevée dans les comptes bancaires touchés.[12]

Cette étude illustre comment il est possible d'exploiter l'engagement d'une entreprise à protéger la vie privée de ses clients pour tenter de lui soutirer de l'argent. La conduite d'une opération similaire contre une entreprise avec moins de ressources risque d'avoir des conséquences catastrophiques dans la mesure où l'extorsion de fonds pourrait mettre un frein aux activités de l'entreprise ou encore mener à la divulgation de l'information, portant ainsi atteinte à la réputation de cette dernière.

Les auteurs de cybermenaces cherchent également à extorquer de l'argent aux entreprises en les menaçant de divulguer l'information confidentielle de leurs clients. Certaines entreprises concluent qu'il est moins coûteux de payer la somme demandée que de subir les coûts associés au refus de payer la rançon. Or, les auteurs de cybermenaces peuvent décider de supprimer, modifier ou divulguer l'information même si un paiement a été effectué. La protection des données importantes repose donc sur l'adoption de pratiques rigoureuses en matière de cybersécurité et de continuité des activités.

Espionnage industriel

Les entreprises canadiennes, particulièrement celles qui sont actives dans des secteurs stratégiques de l'économie, peuvent être la cible d'activités de cyberespionnage visant à obtenir de l'information commerciale sensible ou des renseignements sur la propriété intellectuelle. Les auteurs de cybermenaces ciblent les renseignements commerciaux afin de pouvoir copier des produits existants, de supplanter la concurrence ou de bénéficier d'un avantage lors de négociations commerciales. En règle générale, l'espionnage industriel exige des capacités avancées et une approche soutenue.

Selon nos observations, certains États-nations rivaux cherchant à stimuler la croissance de leurs secteurs des technologies et de la défense pratiquent le cyberespionnage industriel partout dans le monde, y compris le Canada. Une telle activité de cybermenace peut nuire aux avantages commerciaux concurrentiels du Canada et compromettre sa position stratégique sur les marchés mondiaux. On considère que les entreprises canadiennes sont plus à risque de faire l'objet de cyberespionnage si elles font des affaires à l'étranger. Plusieurs pays ont mis en place un cadre juridique et technologique qui permet aux forces policières et de sécurité d'accéder secrètement aux données qui sont transmises au moyen de leur infrastructure de communication nationale ou qui résident sur celle-ci. Les entreprises canadiennes qui exercent leurs activités à l'étranger devraient porter attention aux lois, aux pratiques commerciales et aux règlements locaux, ainsi qu'aux menaces qu'ils font peser sur leur information exclusive, leurs données personnelles ou leur propriété intellectuelle.

EXPLOITATION DES RELATIONS DE CONFIANCE

On considère que les auteurs de cybermenaces sophistiqués continueront probablement de tirer parti des relations de confiance entre les entreprises et leurs fournisseurs de services. Les auteurs de cybermenaces peuvent obtenir accès au réseau d'une entreprise en exploitant l'équipement d'un fournisseur avant même que le produit ne soit livré, ou en compromettant les liens que le fournisseur de service a tissés avec un partenaire ou un client.

Figure 7 : Processus de la chaîne d'approvisionnement[13]

COMPROMISSION DES MISES À JOUR LOGICIELLES

En septembre 2017, des maliciels ont compromis la mise à jour logicielle d'un programme conçu pour améliorer les performances, permettant ainsi aux auteurs de cybermenaces de contourner l'authentification et le chiffrement du dispositif. Le maliciel a infecté 2,2 millions d'utilisateurs à travers le monde. Selon les reportages dans les médias, les auteurs de cybermenaces ont ciblé les données et la propriété intellectuelle de 18 entreprises dans le cadre d'activités d'espionnage, notamment de grands fabricants de produits technologiques mondiaux.[15]

Cette étude illustre la façon dont les auteurs de cybermenaces peuvent se servir d'un logiciel digne de confiance pour compromettre des dispositifs et accéder aux données exclusives des fabricants de produits technologiques. Elle démontre également comment des millions de dispositifs peuvent être infectés dans le cadre d'une campagne malveillante, même s'ils ne sont pas la cible initiale de la campagne. Compromettre plusieurs dispositifs permet aux auteurs de cybermenaces de dissimuler leurs motivations, ce qui rend l'attribution plus difficile.

Compromission de la chaîne d'approvisionnement

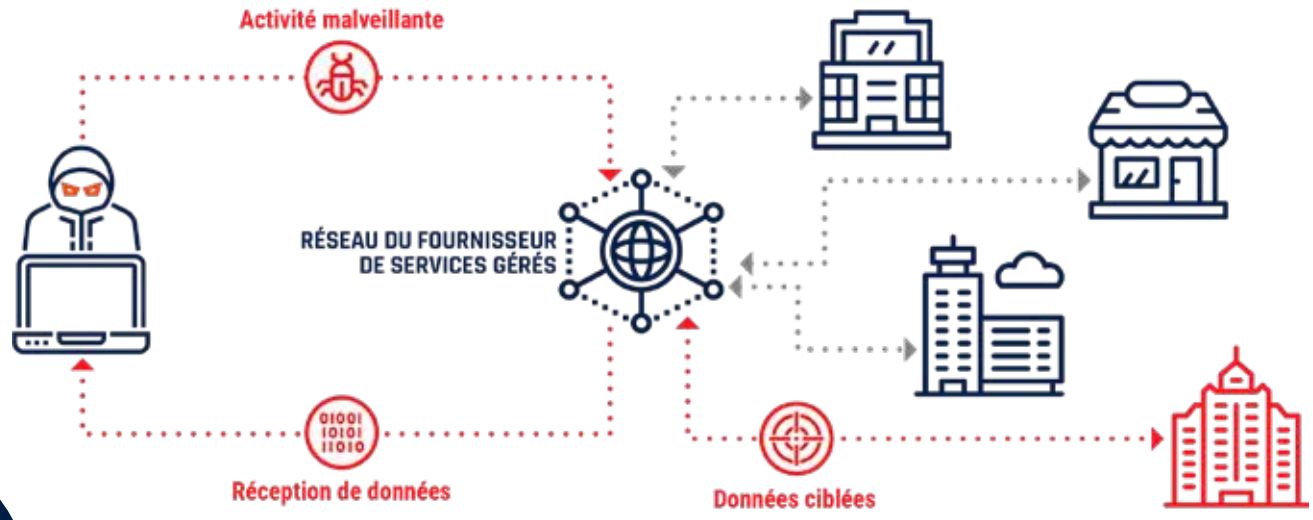
Plusieurs entreprises comptent sur une chaîne d'approvisionnement complexe – et souvent répartie mondialement – qui se compose de plusieurs niveaux de fournisseurs et développeurs de composants[14] Les progrès réalisés sur le plan de la sécurité ont permis d'assurer une meilleure protection des dispositifs et de l'information qu'ils contiennent. Comme il est plus difficile de les cibler directement, il est probable que les auteurs de cybermenaces tenteront de plus en plus d'exploiter les vulnérabilités liées à la chaîne d'approvisionnement.

Étant donné la nature interdépendante de plusieurs entreprises modernes, le niveau de sécurité de la chaîne d'approvisionnement est forcément déterminé par son maillon le plus faible. Tel qu'il est illustré dans la figure 7 à la page précédente, chaque maillon d'une chaîne d'approvisionnement mondiale peut représenter une menace pour la cybersécurité. La compromission d'une chaîne d'approvisionnement permet aux auteurs de cybermenaces d'exploiter un dispositif, ou l'un de ses composants, avant même que celui-ci n'ait été connecté au réseau sécurisé d'une entreprise. Les compromissions de la chaîne d'approvisionnement peuvent survenir avant ou après la livraison d'un produit ou service, ou au cours des mises à jour logicielles et des mises à niveau matérielles.

Fournisseurs de services gérés

On considère qu'en 2019, les auteurs de cybermenaces continueront probablement d'exploiter les relations de confiance en identifiant les parties vulnérables et en accédant aux réseaux partagés pour atteindre leur cible principale. Un **fournisseur de services gérés** (FSG) est une entreprise qui permet aux clients d'externaliser leurs besoins en TI de manière à réduire les coûts associés au maintien de personnel des TI en interne. Pour accomplir le travail d'un professionnel des TI, les FSG disposent généralement d'un accès complet au réseau du client. Ceux qui ont de nombreux clients deviennent donc un point de connexion à plusieurs réseaux. En compromettant un FSG important, les auteurs de cybermenaces peuvent obtenir accès à une partie ou la totalité des réseaux de ses clients, ainsi qu'à leur propriété numérique. On estime qu'il est fort probable que les FSG demeurent des cibles de choix pour les auteurs de cybermenaces sophistiqués en raison de leurs connexions privilégiées aux entreprises, aux réseaux et à l'information.

Figure 8 : Ciblage des FSG

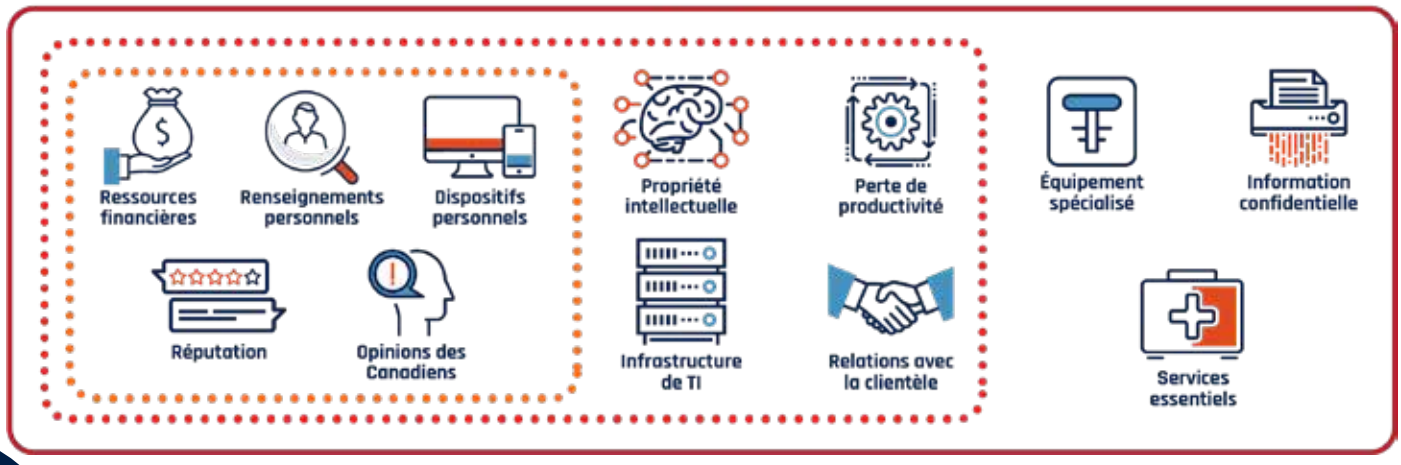


COMPROMISSION DE FSG STRATÉGIQUES

En avril 2017, des chercheurs en cybersécurité ont découvert une campagne de cyberespionnage d'envergure contre des FSG mondiaux. L'exploitation des connexions réseau entre les FSG et leurs clients a permis aux auteurs de cybermenaces de passer du petit nombre de FSG initialement compromis aux réseaux de milliers de clients, dont certains au Canada. Les auteurs de cybermenaces ont volé la propriété intellectuelle et les données sensibles des FSG et de leurs clients dans des secteurs tels que l'ingénierie et la construction, le commerce de détail, la fabrication industrielle, l'énergie et l'exploitation minière, les métaux précieux, la technologie, la pharmaceutique et les sciences biologiques, ainsi que les services professionnels et aux entreprises.[16]

Cette étude démontre comment la compromission d'un FSG peut entraîner de sérieuses répercussions intersectorielles à l'échelle mondiale. Dans ce cas précis, la portée et l'ampleur de la compromission ont aidé les auteurs de cybermenaces à masquer leurs motivations, leurs identités et leurs principales cibles d'intérêt.

CYBERMENACES CONTRE LES INFRASTRUCTURES ESSENTIELLES CANADIENNES



Les activités de cybermenace contre les infrastructures essentielles peuvent avoir des répercussions beaucoup plus sérieuses et étendues que celles visant les citoyens et les entreprises dans la mesure où de tels cyberincidents peuvent potentiellement compromettre la sécurité publique et nationale.

On considère que la prolifération des cyberoutils malveillants a offert aux auteurs de cybermenaces moins sophistiqués de nouvelles occasions de tenter d'interférer avec les infrastructures essentielles. Avec l'augmentation du nombre de dispositifs utilisés pour soutenir, surveiller et contrôler les infrastructures essentielles et comme ces dispositifs sont davantage interconnectés, il est de plus en plus probable que les auteurs de cybermenaces perturbent les infrastructures essentielles.

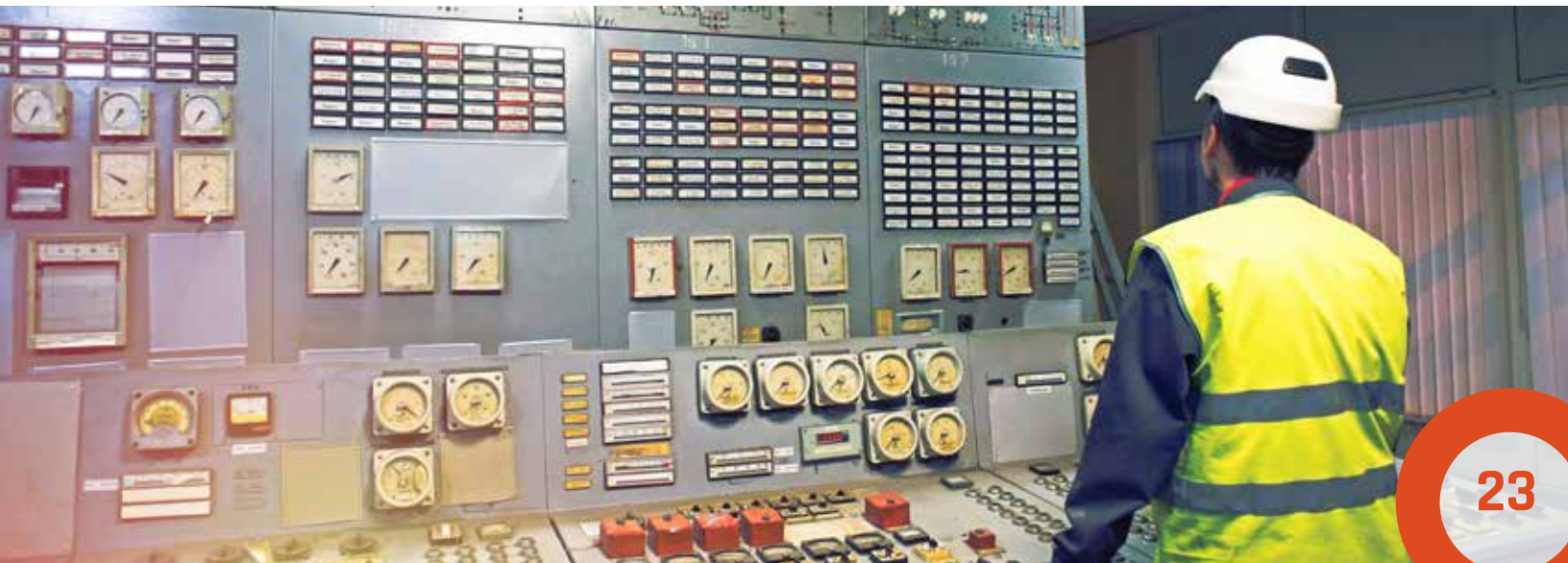
Par exemple, des cybercriminels ont involontairement compromis les systèmes des infrastructures essentielles alors qu'ils tentaient d'exploiter une vulnérabilité dans un contexte plus général. Selon nos observations, ces maliciels se propagent de façon incontrôlable, infectant les réseaux des infrastructures essentielles sans qu'ils aient été ciblés par les auteurs de cybermenaces.

Comme les fournisseurs d'infrastructures essentielles jouent un rôle capital dans la vie de tous les jours, ils sont vulnérables aux activités menées sans discrimination par les cybercriminels. C'est pourquoi leur équipement et leurs services sont de potentielles cibles s'il y a un climat d'hostilité entre les pays. Des auteurs de cybermenaces parrainés par des États se sont livrés au cyberespionnage contre les réseaux des infrastructures essentielles au Canada et dans les pays alliés.[19] Au Canada, ces auteurs de menaces ont mené des activités de reconnaissance et de collecte de renseignement dans les secteurs de l'énergie, de l'aérospatiale et de la défense. Or, pour le moment, on considère qu'il est fort improbable que des auteurs de cybermenaces parrainés par des États cherchent à perturber volontairement les infrastructures essentielles du Canada et à causer de graves dommages s'il n'y a aucun climat d'hostilité à l'échelle internationale.

WANNACRY

En mai 2017, le rançongiciel WannaCry a infecté plus de 200 000 ordinateurs vulnérables dans au moins 100 pays. Le rançongiciel s'est notamment propagé dans 25 installations d'un établissement de santé national offrant des services d'urgence. L'incident a forcé l'annulation de plus de 19 000 rendez-vous, dont des chirurgies.[17] Le Centre de la sécurité des télécommunications et ses organismes partenaires ont attribué WannaCry à des auteurs de cybermenaces de la Corée du Nord.[18]

Bien que dans cet exemple, les auteurs de cybermenaces n'aient pas ciblé spécifiquement les services de santé, WannaCry met en lumière la menace que les rançongiciels représentent pour les infrastructures essentielles qui sont connectées à Internet et les conséquences réelles qui en découlent. Cet incident démontre également que les répercussions de certaines cyberactivités peuvent être plus grandes que ce qui avaient été anticipé par les auteurs de cybermenaces. Alors que l'objectif premier de WannaCry était d'extorquer une rançon, son principal effet a été de perturber les activités commerciales à travers le monde.

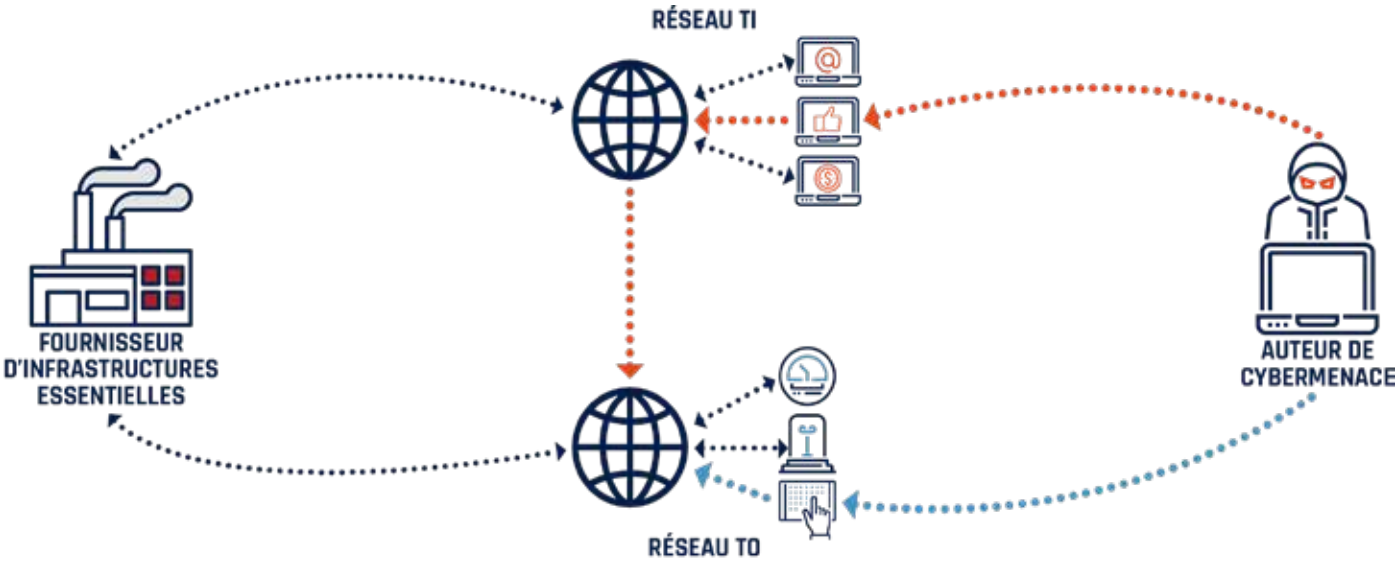


EXPOSITION ACCRUE AUX CYBERMENACES

Les fournisseurs d'infrastructures essentielles font généralement appel à un mélange de technologies pour gérer les processus administratifs et industriels. Ils utilisent les TI pour gérer les fonctions opérationnelles quotidiennes, et les technologies opérationnelles (TO) pour contrôler l'équipement spécialisé comme la machinerie employée dans des environnements physiques complexes et dangereux. Ces fournisseurs ont également recours à des dispositifs de télésurveillance et d'acquisition de données (SCADA pour *Supervisory Control and Data Acquisition*) pour gérer les systèmes de contrôle industriel (SCI).

Dans la poursuite de leurs efforts de modernisation et d'efficacité, les fournisseurs d'infrastructures essentielles continuent d'automatiser leurs processus et de connecter les dispositifs de TI et TO à Internet. Bien que la connexion à Internet des produits de TO, comme les dispositifs SCADA et les SCI, comporte plusieurs avantages – notamment, la gestion à distance –, elle peut également exposer les infrastructures essentielles à des activités de cybermenace. Selon nos observations, il est fort probable que la prolifération des cyberoutils sur les marchés noirs de la cybercriminalité ait facilité l'accès aux TO des infrastructures essentielles pour les auteurs de cybermenaces.

Figure 9 : Des auteurs de cybermenaces tentent d'accéder aux produits de TI et TO d'un fournisseur d'infrastructures essentielles



CYBEROPÉRATIONS CONTRE LES INFRASTRUCTURES ESSENTIELLES UKRAINIENNES

En juin 2017, le maliciel NotPetya a infecté des dizaines de milliers de dispositifs, dont ceux des réseaux d'infrastructures essentielles de l'Ukraine et du monde entier. Les auteurs de cybermenaces ont installé NotPetya par l'intermédiaire d'un progiciel de production de déclarations de revenus couramment utilisés par les entreprises ukrainiennes. En intégrant le maliciel à une mise à jour du logiciel, les auteurs de cybermenaces ont réussi à infecter les dispositifs des utilisateurs et à propager le maliciel dans les réseaux, ce qui a mené au chiffrement des disques durs. NotPetya a infecté des systèmes dans au moins 74 pays. L'infrastructure du gouvernement, des banques, des transports et des télécommunications de l'Ukraine a été particulièrement touchée.[20] Le Centre de la sécurité des télécommunications et ses organismes partenaires ont attribué NotPetya à des auteurs de cybermenaces de la Russie.[21]

Un peu plus tôt, en décembre 2015, des auteurs de cybermenaces avaient compromis les systèmes d'information des sociétés de production et de distribution d'énergie de l'Ukraine, coupant temporairement l'alimentation en électricité dans 225 000 foyers. En installant par harponnage le maliciel sur le système informatique d'un fournisseur d'énergie, les auteurs de cybermenaces ont été en mesure de couper le courant à distance. Ils ont ensuite désactivé les lignes téléphoniques du service à la clientèle pour que les clients ne puissent pas signaler la panne. En décembre 2016, un incident semblable est survenu à Kiev, la capitale ukrainienne. Un cinquième de la ville s'était alors vu plonger dans le noir pendant une heure.[22]

L'étude démontre que lors de tensions ou de conflits entre les États-nations, les chaînes d'approvisionnement des infrastructures essentielles peuvent devenir des cibles. Les cyberopérations comme celles qui ont été menées en Ukraine exigent généralement un cyberespionnage et une planification à long terme.

Accès aux systèmes de contrôle industriel

Les systèmes de contrôle industriels (SCI) appartiennent à un type de technologie opérationnelle qui permet d'assurer la surveillance et le contrôle de l'équipement matériel utilisé dans les infrastructures essentielles, comme les processus liés à la production d'énergie ou à la gestion d'un système de transport.

Dans le passé, les fabricants ont conçu les dispositifs SCI de manière à garantir une longue durée de vie et plusieurs de ces anciens systèmes sont toujours utilisés aujourd'hui. Ces derniers sont conçus pour assurer une fiabilité et un fonctionnement optimaux; ils ne tiennent pas compte de la cybersécurité. Les dernières années ont été marquées par l'apparition de dispositifs et protocoles sécurisés, et ceux-ci sont maintenant déployés dans les nouvelles installations SCI par les fournisseurs d'infrastructures essentielles. On estime qu'il est probable que les auteurs de cybermenaces ciblent les dispositifs et les anciens systèmes non sécurisés jusqu'à ce que l'équipement et les logiciels vieillissants soient mis hors service et remplacés.

On considère qu'une tentative délibérée de compromettre un SCI exigerait fort probablement une connaissance approfondie de l'information exclusive, comme la conception du réseau et les protocoles de communication, et une compréhension du fonctionnement de l'équipement utilisé aux fins d'un procédé industriel en particulier. Pour obtenir de l'information exclusive, les auteurs de cybermenaces doivent généralement s'introduire discrètement sur le réseau et observer l'activité qui s'y déroule pour une période donnée. Comme des SCI inadéquatement sécurisés sont connectés à Internet, ils sont susceptibles d'être la cible d'auteurs de cybermenaces moins sophistiqués, tels que les cybercriminels.

COMPROMISSION DU SECTEUR DE L'ÉNERGIE

En 2017, le Centre de la sécurité des télécommunications a informé ses partenaires des États-Unis de la cybercompromission d'un SCI du secteur de l'énergie. Selon les représentants du département de la Sécurité intérieure, les auteurs de cybermenaces russes avaient réussi à atteindre les systèmes sécurisés et les réseaux isolés, s'introduisant à un point tel qu'ils auraient pu interrompre le transit d'énergie en Amérique du Nord. Les auteurs de cybermenaces ont tiré avantage des relations entre les infrastructures essentielles et les tierces parties de confiance ayant accédé aux SCI afin de procéder à la mise à jour des logiciels et d'effectuer des tests de diagnostic. Pour compromettre les tierces parties, les auteurs de cybermenaces ont fait appel à des techniques relativement simples, comme des courriels de harponnage, pour découvrir les justificatifs d'ouverture de session des employés des entreprises de sous-traitance, y compris celles de petite taille.[23]

Cette étude met en lumière la vulnérabilité des infrastructures essentielles face aux compromissions de la chaîne d'approvisionnement. Elle démontre également qu'un auteur de cybermenace peut avoir recours à une technique peu sophistiquée pour compromettre un SCI puissant. Les auteurs de cybermenaces se livrent à des activités destructrices qui peuvent entraîner une panne de courant à grande échelle, en plus de nuire aux opérations des entreprises et aux services publics essentiels. Comme les réseaux électriques nord-américains sont interconnectés, un cyberincident important aux États-Unis ou au Canada peut avoir des effets perturbateurs dans les deux pays. Les partenariats internationaux revêtent donc une importance capitale.

INSTITUTIONS PUBLIQUES ET INFORMATION SENSIBLE

Selon nos observations, il est probable que les activités de cybermenace contre les institutions publiques – comme les ministères gouvernementaux, les universités et les hôpitaux – persistent étant donné la nature essentielle des services offerts et la sensibilité de l'information qu'elles gèrent.

Les institutions publiques sont une cible alléchante pour les auteurs de cybermenaces en raison de leurs rapports étroits avec les entreprises et les Canadiens. La propriété intellectuelle précieuse qu'elles détiennent appartient parfois à des organismes partenaires comme des centres de recherche ou des sociétés privées.

COMPROMISSION PAR RANÇONGICIEL D'UNE MUNICIPALITÉ CANADIENNE

En avril 2018, onze serveurs d'une municipalité de l'Ontario ont été compromis lors d'une attaque par rançongiciel menée par des auteurs de cybermenaces. Le maliciel de chiffrement utilisé par ces derniers empêchait les responsables d'accéder aux données municipales, minant ainsi la capacité des autorités locales à vaquer à leurs activités. Les auteurs de cybermenaces ont demandé 11 bitcoins (soit 144 000 $ à l'époque) pour déverrouiller les serveurs. Après sept semaines de consultations et de négociations, les autorités municipales ont versé 3 bitcoins (l'équivalent de 34 950 $) aux auteurs de cybermenaces afin de regagner accès à quatre serveurs contenant les données les plus importantes. Aucune information personnelle n'avait été compromise lors de l'incident.[24]

Paiement de la rançon	34 950 $
Conseillers en informatique	37 181 $
Service de sécurité physique	4 725 $
Acquisition de matériel TI	1 901 $
Fournisseurs de logiciels tiers	9 590 $
Heures supplémentaires du personnel interne	31 370 $
Perte de productivité	132 042 $
Coût total de la compromission par rançongiciel	251 759 $

Selon nos observations, il est fort probable que les données confidentielles demeurent une cible alléchante pour les auteurs de cybermenaces. Les Canadiens fournissent des renseignements personnels à leur sujet lorsqu'ils utilisent les services publics essentiels et s'attendent à ce que ces renseignements soient protégés. Les auteurs de cybermenaces peuvent menacer les responsables des institutions publiques de divulguer les renseignements personnels auxquels ils ont eu accès dans le but de les contraindre à payer une rançon afin de protéger la confidentialité des citoyens, d'assurer le maintien des activités et de préserver leur réputation.

Les institutions publiques créent et recueillent également d'autres types d'informations sensibles de valeur, informations que les auteurs de cybermenaces pourraient cibler à des fins mercantiles ou pour extorquer une rançon. Afin de vendre de l'information importante ou de se livrer à l'espionnage, les auteurs de cybermenaces ciblent, par exemple, les détails entourant des activités confidentielles, comme des négociations ou des délibérations.

Les organismes de renseignement étrangers espionnent les gouvernements fédéraux et infranationaux depuis des décennies, mais la numérisation des services gouvernementaux a changé la donne dans la mesure où il est désormais possible d'accéder à l'information confidentielle au moyen de cybercapacités.

Les États-nations adversaires ont les moyens et la volonté de mener des activités de cybermenace contre les institutions publiques canadiennes. Le degré de sophistication des auteurs de cybermenaces parrainés par des États varie et il est probable que certains auteurs plus sophistiqués arrivent à dissimuler leurs activités. Les institutions publiques canadiennes sont souvent la cible d'activités de cybermenace lorsque le Canada prend part à des enjeux internationaux ou bilatéraux de nature sensible ou s'impose comme chef de file mondial sur le plan de la recherche.

On considère que les États-nations à travers le monde continuent d'investir dans leurs cybercapacités dans le but de réaliser leurs objectifs nationaux sur le plan de la sécurité et de l'économie.

CONCLUSION

L'environnement de cybermenaces au Canada est en constante évolution. On s'attend à ce que les méthodes et les cibles des auteurs de cybermenaces se transforment suivant l'évolution de leurs priorités, motivations et capacités.

La présente évaluation visait à relever les tendances actuelles de l'environnement de cybermenaces. Autant que possible, on a tenté d'indiquer le degré de probabilité des activités de cybermenace et d'examiner la façon dont ces activités touchent les Canadiens, ainsi que les entreprises et les infrastructures essentielles du Canada.

En règle générale, la plupart des cybermenaces mentionnées dans la présente peuvent être atténuées grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de sécurité et de continuité des activités. De nos jours, les cybermenaces et les opérations d'influence sont souvent fructueuses, car elles ne reposent pas uniquement sur les vulnérabilités technologiques, mais exploitent des habitudes sociales et des comportements humains profondément ancrés. Pour défendre le Canada contre les cybermenaces et les opérations d'influence connexes, il faut se pencher sur les aspects techniques et sociaux des activités de cybermenace.

Comme l'indique la *Stratégie nationale de cybersécurité*, il est primordial que les citoyens, les entreprises et les fournisseurs d'infrastructures essentielles du Canada puissent avoir confiance dans les cybersystèmes dont ils dépendent chaque jour. Puisque son approche collaborative en matière de sécurité permet de combiner l'expertise du gouvernement, du secteur privé et du milieu universitaire afin de s'attaquer aux plus grands défis que pose la cybersécurité au Canada, le Centre canadien pour la cybersécurité joue un rôle déterminant dans leur vie. En travaillant ensemble, nous rendrons le Canada plus fort et plus résilient face aux cybermenaces.

RESSOURCES UTILES

Pour de plus amples renseignements sur les mesures d'atténuation des cybermenaces, il est fortement recommandé de consulter les sites suivants :

- Introduction à l'environnement de cybermenaces
- Les 10 mesures de sécurité des TI
- Pratiques exemplaires en cybersécurité du CCC
- Conseils du CCC sur la sécurité des dispositifs mobiles
- Campagne Pensez cybersécurité
- Le petit livre noir de la fraude
- Programme d'examen de la sécurité
- Contrats avec des fournisseurs de services gérés : facteurs relatifs à la cybersécurité à considérer
- Lignes directrices sur la chaîne d'approvisionnement des technologies (TSCG-01)
- Cyberactivité malveillante ciblant les fournisseurs de services gérés
- Protégez votre entreprise
- En savoir plus sur Chaîne de montage (Assemblyline)
- Utilisation d'une liste blanche des applications
- Protéger vos dispositifs et vos réseaux
- Appliquer les contrôles d'architecture pour la séparation des réseaux
- Enregistreurs de frappe et logiciels espions (ITSB-49)
- Comment reconnaître l'information trompeuse en ligne et ce qu'il faut faire pour y remédier
- Rapport conjoint sur les outils de piratage publiquement accessibles
- Reconnaître les courriels malveillants
- Hameçonnage
- Protégez-vous contre la fraude
- Campagnes de fraudes par nom de sosie de domaine et par virement bancaire

NOTES EN FIN D'OUVRAGE

[1] Par infrastructures essentielles, on entend les processus, les systèmes, les installations, les technologies, les réseaux et les services essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens ainsi qu'au fonctionnement efficace du gouvernement. Sécurité publique Canada, 12 juin 2018 (consulté en septembre 2018).

[2] Dans la présente évaluation, le terme « cybercriminalité » désigne les activités criminelles visant un réseau ou un dispositif connecté à un réseau.

[3] Département de la Justice des États-Unis, 13 décembre 2017 (consulté en septembre 2018). PERLROTH, Nicole, *The New York Times*, 21 octobre 2016 (consulté en septembre 2018).

[4] Alliance contre les cybermenaces, 19 septembre 2018 (consulté en septembre 2018).

[5] Agence du revenu du Canada, 31 août 2018 (consulté en septembre 2018).

[6] Par extorsion, on entend l'acte qui consiste à extorquer illégalement de l'argent, un bien ou des services à une personne ou une institution, sous la menace ou la force.

[7] Centre antifraude du Canada, août 2018 (consulté en septembre 2018).

[8] Centre canadien pour la cybersécurité, juin 2017.

[9] ROCHA, Roberto, *CBC News*, 31 août 2018 (consulté en septembre 2018). Ensemble de données initiales accessibles sur le site Data Source.

[10] Autorité canadienne pour les enregistrements Internet, 22 mars 2018 (consulté en septembre 2018).

[11] Gendarmerie royale du Canada, 15 janvier 2018 (consulté en septembre 2018).

[12] *The Globe and Mail*, 18 juin 2018 (consulté en septembre 2018). EVANS, Pete. *CBC News*, 28 mai 2018 (consulté en septembre 2018). Canadian Financial Group, 28 mai 2018 (consulté en septembre 2018).

[13] Avant de se retrouver entre les mains d'un consommateur canadien, un téléphone intelligent ou ordinateur portable peut avoir été conçu dans un pays, les matières premières et certains composants, comme l'écran, le microphone et la caméra peuvent provenir d'entreprises à travers le monde, et le dispositif en soi peut avoir été assemblé dans un autre endroit.

[14] Par chaîne d'approvisionnement, on entend un système d'organisations, de personnes, de technologies, d'activités, d'informations et de ressources permettant d'offrir un produit ou un service dans le cadre d'une relation fournisseur-client. Voir le site de la National Institute for Standards and Technology, avril 2015 (consulté en septembre 2018).

[15] CORERA, Gordon, *BBC News*, 26 juillet 2018 (consulté en août 2018). MENN, Joseph, *Reuters*, 18 septembre 2018 (consulté en septembre 2018).

[16] PricewaterhouseCoopers (Royaume-Uni), 10 avril 2017 (consulté en septembre 2018). NISH, Adrian et ROWLES, Tom, BAE Systems, 3 avril 2017 (consulté en septembre 2018).

[17] National Audit Office (Royaume-Uni), 25 avril 2018 (consulté en septembre 2018).

[18] Centre de la sécurité des télécommunications, 19 décembre 2017.

[19] United States Computer Emergency Readiness Team (US-CERT, département de la Sécurité interne), 15 mars 2018 (consulté en septembre 2018).

[20] PERLROTH, Nicole, et al, *The New York Times*, 27 juin 2018 (consulté en septembre 2018).

[21] Centre de la sécurité des télécommunications, 15 février 2018.

[22] *BBC News*, 26 février 2016 (consulté en septembre 2018). *BBC News*, 11 janvier 2017 (consulté en septembre 2018).

[23] SMITH, Rebecca, *The Wall Street Journal*, 24 juillet 2018 (consulté en septembre 2018). United States Computer Emergency Readiness Team (US-CERT, département de la Sécurité interne), 15 mars 2018 (consulté en septembre 2018).

[24] *CTV News*, 24 juillet 2018 (consulté en septembre 2018). Ordre du jour d'une municipalité canadienne, 24 juillet 2018 (consulté en septembre 2018).