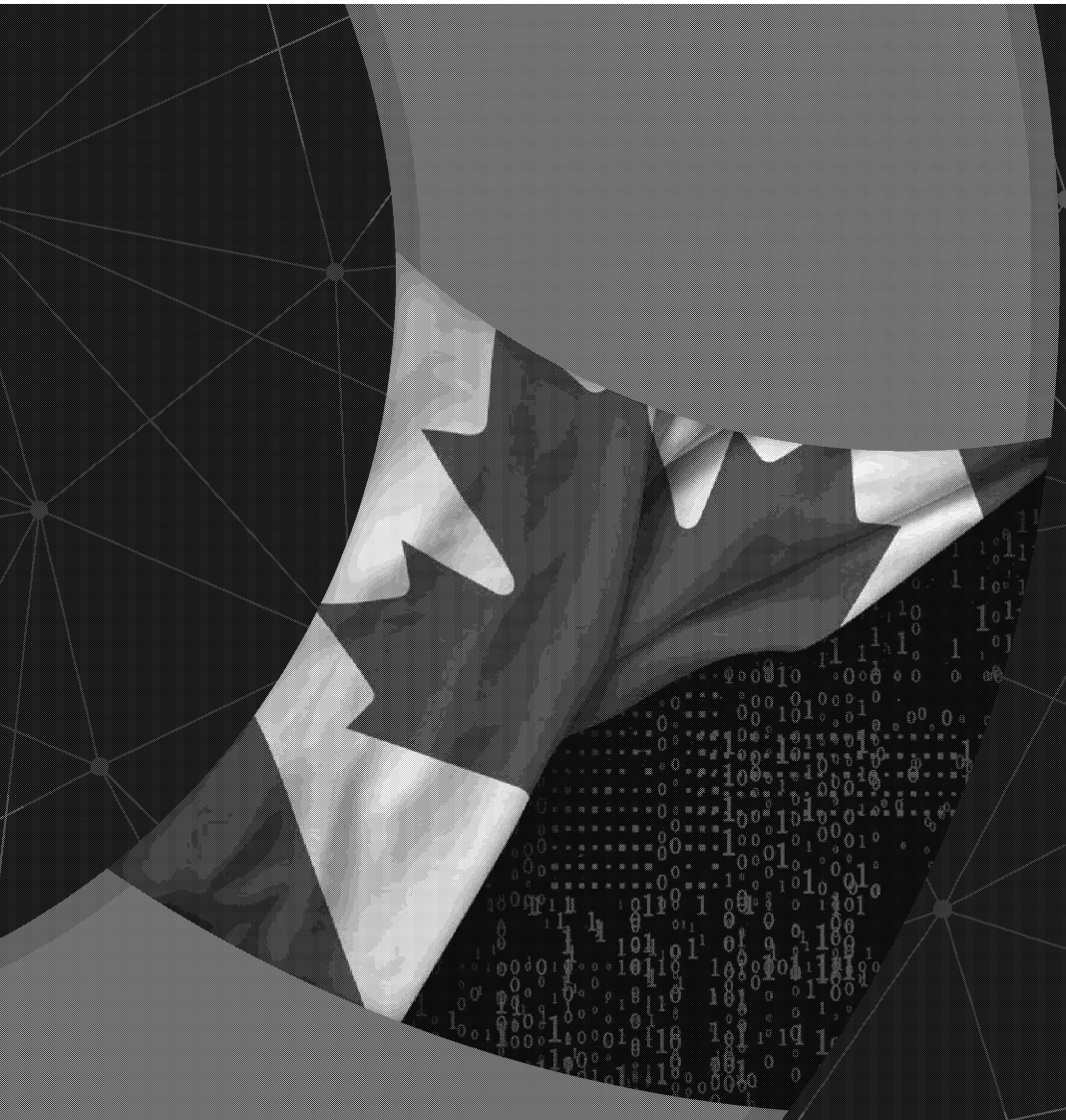


CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

ÉVALUATION DES CYBERMENACES NATIONALES 2020

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

À PROPOS DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (CCC) est l'autorité canadienne en matière de cybersécurité. Faisant partie du Centre de la sécurité des télécommunications (CST), le CCC est une organisation en plein essor qui jouit d'une riche histoire. Il regroupe sous un même toit des spécialistes en sécurité opérationnelle de l'ensemble du gouvernement du Canada. En phase avec la *Stratégie nationale de cybersécurité*, le 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 réalisateurs, de concepteurs, de développeurs, de chercheurs et de scientifiques, a pour rôle d'accroître la cybersécurité au Canada.

LE CCC CONTRIBUE À LA SÉCURITÉ DU CANADA ET DES CANADIENS DANS LE CYBERESPACE EN JOUANT LES RÔLES SUIVANTS :

- Il est une **source claire et fiable de renseignements pertinents sur la cybersécurité** pour les Canadiens, les entreprises canadiennes ainsi que les propriétaires et les exploitants d'infrastructures essentielles;
- Il offre des **avis et des conseils ciblés sur la cybersécurité** afin de protéger les plus importants cybersystèmes canadiens;
- Il travaille **en collaboration avec les gouvernements provinciaux et territoriaux, les administrations municipales et des partenaires du secteur privé** pour résoudre les défis les plus complexes du Canada en matière de cybermenace;
- Il développe et diffuse des **technologies et connaissances de cyberdéfense spécialisées**;
- Il **défend les cybersystèmes**, dont ceux du gouvernement du Canada, en élaborant et en déployant des outils et des technologies de cyberdéfense sophistiqués;
- Il agit à titre de **chef de file opérationnel du gouvernement lors d'incidents de cybersécurité** et tire parti de son expertise et de ses accès pour fournir de l'information opportune et utile à la gestion des incidents.

La cyberdéfense, c'est un sport d'équipe. L'avantage unique du CCC permet au Canada de résister plus efficacement aux cybermenaces et d'accroître sa résilience pendant et après des cyberincidents.

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

AVANT-PROPOS DU MINISTRE

La cybersécurité est l'un des enjeux les plus sérieux auxquels nous faisons face sur le plan de l'économie et de la sécurité nationale. Protéger le Canada et les Canadiens des cybermenaces est une responsabilité partagée et une affaire d'équipe. Je ne saurais trop insister sur l'importance de lire le présent rapport, tout particulièrement si vous pensez que la cybersécurité n'a rien à voir avec vous.

D'ailleurs, je tiens à remercier l'équipe du Centre pour la cybersécurité pour cette évaluation fort opportune. En partageant ses connaissances, elle s'assure que les décideurs politiques, les chefs d'entreprise et les citoyens canadiens ont l'information nécessaire pour contrer ces menaces.

Nous savons que les Canadiens sont parmi les peuples les plus connectés au monde et la pandémie de la COVID-19 n'a fait qu'accroître cette dépendance à Internet. Comme on peut le voir régulièrement dans l'actualité, les cyberattaquants trouvent sans cesse des moyens plus sophistiqués d'exploiter notre connectivité.

Les cybermenaces mettent à risque la vie privée, la stabilité financière et la sécurité personnelle des Canadiens, ainsi que la rentabilité des entreprises au pays. Le préfixe « cyber » ne reflète en fait que l'approche adoptée pour mener de telles activités.

Tirant avantage de l'expertise de pointe du Canada en la matière, l'approche unifiée du Centre pour la cybersécurité offre aux Canadiens l'assurance que le gouvernement est prêt à s'attaquer aux enjeux qui nous guettent sur le plan de la cybersécurité.

Les principales constatations soulevées dans le présent rapport du Centre pour la cybersécurité nous rappellent à quel point il est important de ne pas baisser notre garde.

On constate une recrudescence des cybermenaces, alors que les cybercriminels sophistiqués vendent leurs outils et leurs services en ligne par l'entremise de marchés illégaux.

Les cyberprogrammes parrainés par des États sondent nos infrastructures essentielles à la recherche de vulnérabilités.

Il est de plus en plus courant de voir les nations étrangères chercher à influencer les débats publics au moyen des médias sociaux.

De fait, Internet se trouve à la croisée des chemins, puisque des pays comme la Chine et la Russie s'efforcent de changer la façon dont nous régissons le cyberespace et d'en faire un outil susceptible de conférer à l'État un pouvoir de censure, de surveillance et de contrôle.

Nous continuerons de collaborer avec nos partenaires des secteurs privé et public, ainsi qu'avec les citoyens canadiens, en vue de créer un cyberespace fort et résilient dans l'ensemble du Canada.

L'honorable Harjit Sajjan
Ministre de la Défense nationale

MESSAGE DU DIRIGEANT PRINCIPAL DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Deux années se sont écoulées depuis la publication de la première Évaluation des cybermenaces nationales 2018 du Canada, et au cours de cette période, beaucoup de ce qui a été annoncé s'est concrétisé. L'*Évaluation des cybermenaces nationales 2020* arrive à un moment où les Canadiens et l'économie canadienne ont de plus en plus tendance à réorienter leurs activités vers les services en ligne. Cette transition s'est accélérée depuis l'arrivée de la COVID-19.

La pandémie de COVID-19 illustre bien jusqu'à quel point l'économie canadienne dépend de l'infrastructure numérique. Face à la hausse subite du nombre de Canadiens travaillant à la maison, il est essentiel de protéger les cyberinfrastructures, les infrastructures de télécommunications, le matériel, les logiciels et les chaînes d'approvisionnement qui les prennent en charge, pour assurer la sécurité nationale et la prospérité économique du Canada. Ces aspects sont au cœur de nos activités quotidiennes et, pour la majorité des Canadiens, l'infrastructure numérique à la base de notre société est souvent hors de vue ou cachée.

Le présent document ne se veut pas un examen de l'*Évaluation des cybermenaces nationales* de 2018. Certaines prévisions se sont révélées exactes, d'autres se sont réalisées à des rythmes différents. On dit qu'avec le recul, tout devient plus clair. En 2018, j'avais mis au défi les équipes d'évaluation, comme je l'ai fait encore cette année, de faire preuve d'audace et d'y aller de prévisions. Seul l'avenir nous dira si ces dernières sont exactes. Elles s'appuient sur toute l'expertise du CST et ses connaissances en matière de cybersécurité tant au Canada qu'ailleurs dans le monde, et mettent à profit toutes les sources d'information classifiée et librement disponible.

L'*Évaluation des cybermenaces nationales* est à la base d'un grand nombre des activités du Centre canadien pour la cybersécurité (CCC). Son objectif est d'établir nos priorités. Nous travaillons à atténuer les menaces décrites dans le présent rapport et à accroître la cybersécurité de base dans l'ensemble du Canada. Mais le CCC ne saurait faire cavalier seul. Un bon exemple de cet esprit de collaboration est le partenariat conclu avec l'Autorité canadienne pour les enregistrements Internet (ACEI) et le lancement du service Bouclier canadien. L'utilisation de ce service offert gratuitement par l'ACEI à tous les Canadiens permet de réduire directement l'incidence et la portée de la cybercriminalité qui seraient liées, par exemple, à un rançongiciel. En bref, il s'agit d'une réponse directe à l'énoncé que l'on retrouve dans l'évaluation de 2018 selon lequel la menace la plus susceptible d'avoir une incidence sur les Canadiens est la cybercriminalité.

Mais ces deux dernières années ont aussi démontré que ce qui compte réellement est de faire le nécessaire sur le plan de la cybersécurité. La grande majorité des cyberincidents qui se sont produits au Canada résultaient du non-respect des pratiques de base en matière de cybersécurité. Les Canadiens peuvent compter sur les étapes simples, réalistes et faciles à réaliser, qui sont proposées par la campagne du site Pensezcybersecurite.gc.ca pour accroître leur sécurité. Si vous êtes un organisme canadien à but non lucratif, une entreprise canadienne de toutes tailles ou un organisme faisant partie d'un autre ordre du gouvernement, vous trouverez de l'information sur le site cyber.gc.ca. Chacun doit faire sa part pour rendre le Canada plus sécuritaire.

J'espère que l'*Évaluation des cybermenaces nationales* de 2020 vous sera utile et qu'elle incitera chaque Canadien à entreprendre ne serait-ce qu'une initiative pour renforcer sa sécurité en ligne. Chaque étape franchie est un pas de plus vers notre objectif d'assurer la sécurité numérique du Canada.

Scott Jones
Dirigeant principal, Centre canadien pour la cybersécurité

www.cyber.gc.ca

RÉSUMÉ

Les Canadiens et les entreprises canadiennes dépendent de plus en plus d'Internet pour vaquer à leurs activités quotidiennes. Dans le contexte de la COVID-19, cette tendance s'est accélérée pour permettre aux Canadiens de travailler, de magasiner et de socialiser à distance conformément aux directives de distanciation physique émises par la santé publique. Cependant, alors que les dispositifs, l'information et les activités se tournent vers Internet, ils deviennent également vulnérables face aux auteurs de cybermenace.

Les auteurs de cybermenace représentent un risque pour l'économie canadienne en raison des coûts élevés que doivent subir les particuliers et les entreprises, notamment lors du vol de propriété intellectuelle et de renseignements exclusifs. Ils mettent en péril la vie privée des Canadiens en volant leurs renseignements personnels, ce qui favorise la criminalité, dont le vol d'identité et la fraude financière. Alors que les infrastructures matérielles et les processus restent liés à Internet, les cybermenaces présentent de plus en plus un danger sur le plan du fonctionnement de l'équipement et de la sécurité des Canadiens.

FAITS SAILLANTS

- **Le nombre d'auteurs de cybermenace est en hausse et ceux-ci deviennent de plus en plus sophistiqués.** La vente commerciale d'outils liés à la cybercriminalité, à laquelle s'ajoute un bassin mondial d'experts en la matière, a entraîné une hausse du nombre d'auteurs de cybermenace et donné lieu à des attaques plus sophistiquées. Les marchés en ligne servant à la vente d'outils et de services illicites ont également permis aux cybercriminels de mener des activités plus complexes et sophistiquées.

- **La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes.** Nous estimons qu'au cours des deux prochaines années, les Canadiens et les entreprises canadiennes devraient continuer d'être visés par la fraude en ligne et des tentatives de vol de données personnelles, financières et commerciales.

- **Nous considérons que les activités malveillantes dirigées contre le Canada continueront fort probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles.** Comme ces derniers ne peuvent pas se permettre de subir des perturbations importantes, ils sont prêts à verser jusqu'à plusieurs millions de dollars pour rétablir leurs opérations. Il est probable que beaucoup de victimes canadiennes continueront de consentir à payer les rançons en raison des coûts élevés liés aux pertes commerciales et à la reconstruction de leurs réseaux, ainsi qu'aux conséquences potentiellement dévastatrices qui pourraient résulter advenant un refus.

- **Bien que la cybercriminalité représente la menace la plus importante, les programmes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord posent les plus graves menaces stratégiques pour le Canada.** Les cybermenaces parrainées par des États sont habituellement les menaces les plus sophistiquées auxquelles sont confrontés les Canadiens et les entreprises canadiennes.

- **Il est fort probable que des auteurs de cybermenace parrainés par des États cherchent à développer des moyens pour perturber les infrastructures essentielles du Canada, comme l'approvisionnement en électricité, pour atteindre leurs buts.** Nous croyons toutefois qu'il est fort improbable que des auteurs de cybermenace tentent de perturber volontairement les infrastructures essentielles du Canada et de causer de sérieux dommages ou des pertes de vie s'il n'y a aucun climat d'hostilité à l'échelle internationale. Néanmoins, les auteurs de cybermenace pourraient cibler des entreprises canadiennes essentielles dans l'objectif de recueillir des données, de se prépositionner en vue d'activités ultérieures, ou de les intimider.

- **Les auteurs de cybermenace continueront probablement de mener des activités d'espionnage industriel contre les entreprises, le milieu universitaire et les gouvernements du Canada afin de voler la propriété intellectuelle et des renseignements canadiens de nature exclusive.** Nous estimons que ces auteurs malveillants continueront à tenter de voler la propriété intellectuelle portant sur la lutte contre la COVID-19 pour appuyer leurs programmes de santé publique nationaux ou tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés. La menace de cyberespionnage est certainement beaucoup plus grande pour les entreprises canadiennes qui font des affaires à l'étranger ou qui travaillent directement avec des sociétés détenues par des États étrangers.

- **Les campagnes d'influence étrangère en ligne sont pratique courante et ne se limitent pas à des événements politiques importants, comme des élections.** Elles font maintenant partie de la nouvelle normalité, et les adversaires tentent non seulement d'influencer des événements à l'échelle nationale, mais ils veulent aussi avoir un impact sur les débats publics qui se tiennent sur la scène internationale. Nous estimons que, comparativement à d'autres pays, les Canadiens ne présentent pas une cible prioritaire en ce qui a trait à l'influence étrangère en ligne. Il faut toutefois noter qu'au Canada, l'écosystème des médias est étroitement lié à celui des États-Unis et d'autres alliés. Cela signifie que lorsque les populations de ces derniers sont ciblées, les Canadiens s'exposent à des dommages collatéraux en raison de l'influence en ligne.

TABLE DES MATIÈRES

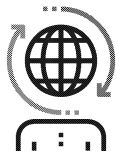
À PROPOS DU PRÉSENT DOCUMENT

Le présent document fait état des cybermenaces qui visent les citoyens et les entreprises du Canada. Il constitue une mise à jour de l'*Évaluation des cybermenaces nationales 2018*, ainsi qu'une analyse des années intermédiaires et des prévisions d'ici 2022. Nous vous recommandons de lire la présente évaluation et de consulter l'*Introduction à l'environnement de cybermenace*, qui a également été mise à jour. Cette introduction donne un aperçu général des auteurs de cybermenace, de leurs motivations et des outils à leur disposition. Elle comprend de plus une annexe indiquant les principales techniques et les principaux outils qui ont été mentionnés dans la présente.

Conformément à l'optique de la *Stratégie nationale de cybersécurité*, nous avons préparé ce document pour aider à façonner et à soutenir la résilience du Canada en matière de cybersécurité. Ce n'est qu'en travaillant ensemble (le gouvernement, le secteur privé et les particuliers) que nous pourrons assurer la résilience du Canada face aux cybermenaces.

RESTRICTIONS

L'objectif de la présente évaluation n'est pas de fournir une liste exhaustive des activités de cybermenace ciblant le Canada ou des conseils en matière d'atténuation. Elle a plutôt pour but de décrire et d'évaluer les menaces visant le Canada. Cette évaluation cherche à comprendre la nature et le contexte de cybermenace actuel, ainsi que la façon dont les activités de ce type 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 dans les documents liés à la campagne Pensez cybersécurité.



SOURCES

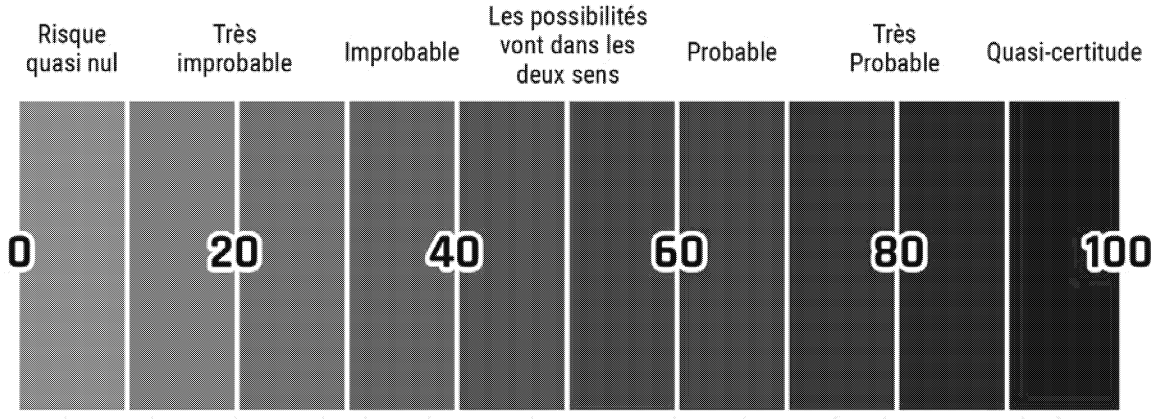
Les jugements formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du CCC en matière de cybersécurité. Le rôle que joue le CCC dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans un contexte de cybermenace, 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 de cybermenace 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 est basée sur des renseignements disponibles en date du 20 octobre 2020.

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.



UN CONTEXTE DES CYBERMENACES EN ÉVOLUTION

L'*Évaluation des cybermenaces nationales 2018* décrivait les cybermenaces auxquelles ont fait face les citoyens, les entreprises et les fournisseurs d'infrastructures essentielles du Canada. Elle annonçait également comment ces menaces allaient évoluer au cours des prochaines années. Beaucoup de ces jugements demeurent pertinents. La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens. Il y a aussi les auteurs de cybermenace parrainés par des États qui continuent de se livrer au cyberespionnage contre des organismes canadiens, notamment les entreprises et les infrastructures essentielles; et il ne faut pas oublier les auteurs de cybermenace qui continuent d'adapter leurs techniques et d'adopter des méthodes plus avancées. Or, les menaces qui pèsent sur les Canadiens ont elles aussi évolué au même rythme que les façons dont ils utilisent la technologie et Internet.

Internet est un outil indispensable pour les gens à travers le monde et pour les Canadiens. Les changements qui ont dû être apportés en mars 2020 en raison de la pandémie de COVID-19 ont rapidement bouleversé le portrait de la cybersécurité alors que plus de Canadiens doivent travailler, magasiner et socialiser à distance. Nous prévoyons que cette tendance se poursuivra et que plus de facettes de la vie économique, sociale et politique des Canadiens passeront par Internet, ce qui les exposera à des cybermenaces qui ne cessent d'évoluer pour tirer avantage de l'importance accrue d'Internet et des technologies connexes.

Afin de bien comprendre le reste de l'évaluation, nous avons relevé dans la prochaine section cinq tendances qui guideront l'évolution du contexte des cybermenaces.

LA TECHNOLOGIE CHANGE LA SOCIÉTÉ ET MODIFIE LE CONTEXTE DES CYBERMENACES

Les changements technologiques amènent des changements sociaux

Les Canadiens dépendent de plus en plus d'Internet. Un nombre grandissant d'activités quotidiennes importantes se font maintenant en ligne pour des raisons de commodité et d'efficacité. On peut penser ici à tout ce qui touche les transactions bancaires, les services gouvernementaux, les services de santé, le commerce et l'éducation. Dans le contexte de la COVID-19, cette tendance s'est accélérée pour permettre aux Canadiens de travailler, de magasiner et de socialiser à distance conformément aux directives de distanciation physique émises par la santé publique. Ces changements sont engendrés par des technologies émergentes et arrivant à maturité, qui continuent de créer de nouveaux moyens pour utiliser Internet. Ces technologies permettent une meilleure qualité de vie et changent la façon dont les gens et les organismes interagissent.

Des technologies comme l'intelligence artificielle (IA), l'Internet des objets (IdO), l'Internet des objets industriel (IIoT pour *Industrial Internet of Things*) et l'infonuagique soutiennent une vaste gamme d'activités personnelles, commerciales et industrielles. Au cours des deux prochaines années, l'avancement de ces technologies et les progrès réalisés dans d'autres technologies de l'information, comme le déploiement du réseau 5G, changeront les pratiques commerciales des Canadiens, leurs façons d'exploiter des établissements industriels, d'acheter et d'obtenir des produits de consommation, de recevoir des soins médicaux, et plus encore. Les Canadiens seront en mesure de constater des changements apportés dans d'autres aspects de leur vie, notamment l'aménagement des villes et des moyens de transport, ainsi que le déroulement des élections et des processus démocratiques.

Le contexte des cybermenaces

Alors que les dispositifs, l'information et les activités prisés par les Canadiens et les entreprises canadiennes se tournent vers Internet, ils s'exposent également aux cybermenaces. Les auteurs de cybermenace, plus particulièrement les cybercriminels et les auteurs parrainés par des États, continuent d'adapter leurs activités afin de trouver l'information importante pour les Canadiens. Leur objectif est de s'approprier de cette information, de la détenir en vue d'une demande de rançon ou de la détruire.

On considère que les cybercriminels, qui sont motivés par un gain financier, représentent presque assurément la plus grande cybermenace pour les Canadiens. Ils se livrent à la majorité des activités de cybermenace contre les Canadiens, dont les attaques par rançongiciel, le vol de données personnelles, financières et confidentielles, et les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*). Comme nous l'abordons un peu plus dans la présente, les marchés illégaux des produits et services liés à la cybercriminalité donnent aux cybercriminels accès à des outils plus sophistiqués.

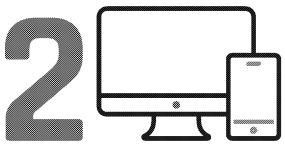
Or, les moyens les plus sophistiqués appartiennent aux auteurs de cybermenace parrainés par des États qui sont motivés par des visées économiques, idéologiques et géopolitiques. Ils comptent parmi leurs activités le cyberespionnage, le vol de propriété intellectuelle, les campagnes d'influence en ligne et les cyberattaques perturbatrices. Nous sommes presque assurés que les programmes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord posent les plus graves cybermenaces pour les Canadiens et les entreprises canadiennes. Toutefois, beaucoup d'autres États développent rapidement leurs propres programmes et profitent de divers marchés légaux et illégaux pour se procurer des produits et services qu'ils pourront ensuite utiliser dans le cadre de leurs activités de cybermenace.

Les activités des hacktivistes ou des amateurs de sensations fortes posent une menace moins fréquente et moins sophistiquée pour les Canadiens. En règle générale, les activités des hacktivistes et des amateurs de sensations fortes sont moins répandues que les autres types d'activités. De plus, ces auteurs de cybermenace ont souvent moins de ressources à consacrer à leurs activités, ce qui limite la sophistication de leurs opérations. Les hacktivistes ont toutefois mené des cyberactivités d'importance majeure en 2020. Un des incidents les concernant ciblait principalement des victimes américaines, mais a quand même eu une incidence sur des organismes au Canada, alors que des données appartenant à 38 services de police canadiens ont été exposées.[1]

Nous présentons ci-dessous cinq tendances qui guideront l'évolution du contexte des cybermenaces et les activités de cybermenace.

LA SÉCURITÉ PHYSIQUE DES CANADIENS EST MENACÉE

La sécurité des Canadiens dépend des infrastructures essentielles (comme l'énergie ou la gestion de l'eau), ainsi que de biens de consommation et de produits médicaux (voiture, système de sécurité à domicile, stimulateur cardiaque et autres) qui sont, dans plusieurs cas, contrôlés par des dispositifs informatiques implantés à même le corps. On remarque de plus en plus que ces dispositifs informatiques sont branchés à Internet par leurs fabricants, parfois à l'insu des consommateurs. Cette façon de procéder permet d'activer de nouvelles fonctions ou de fournir des données à des tiers. Une fois connectés, ces produits représentent toutefois une cybermenace. Assurer leur sécurité nécessite, au fil du temps, des investissements que les fabricants et les propriétaires pourraient avoir de la difficulté à maintenir. Un aspect important de cette tendance est la technologie opérationnelle (TO) qui, en termes génériques, fait référence à la technologie utilisée pour contrôler les processus physiques comme l'ouverture de barrage, le fonctionnement d'une chaudière, la transmission d'électricité et l'exploitation des pipelines. Contrairement à la technologie de l'information (TI) qui englobe le matériel et les logiciels que l'on trouve dans la plupart des maisons et des entreprises, la technologie opérationnelle a été relativement à l'abri des activités de cybermenace parce qu'elle n'a pas été initialement conçue pour être connectée à Internet. Or, les fabricants convergent maintenant vers la TI et la TO. Ces changements ont pour but d'accroître l'efficacité et de soutenir une planification à long terme, mais ils augmentent également le risque de voir les systèmes de TO être touchés par des activités de cybermenace. Une enquête effectuée en 2019 a démontré que 68 % des fabricants envisageaient d'accroître leurs investissements dans des solutions de convergence vers les TI et TO pour leurs organismes au cours des deux prochaines années.[2] Il est fort probable que les menaces les plus pressantes à la sécurité physique des Canadiens visent la TO et les infrastructures essentielles. Cependant, cibler des petites villes et des dispositifs de l'IdO, comme un dispositif médical personnel ou un véhicule connecté à Internet, pourrait éventuellement mettre les Canadiens en danger.



LA VALEUR ÉCONOMIQUE EST MENACÉE

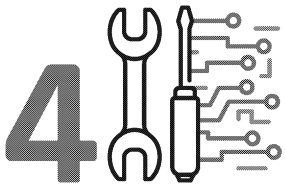
Comme il est indiqué dans l'évaluation de 2018, les auteurs de cybermenace parrainés par des États et les cybercriminels continuent de soutirer des sommes importantes aux Canadiens et aux entreprises canadiennes et de mettre en péril l'économie. Les cybercriminels fraudent les citoyens et les entreprises et leur soutirent de l'argent au moyen de rançongiciels. Les auteurs de cybermenace parrainés par des États, quant à eux, volent plutôt la propriété intellectuelle et des renseignements de nature exclusive. En outre, de plus en plus de Canadiens effectuent leurs transactions financières en ligne, ce qui en fait des proies intéressantes pour les cybercriminels. En 2019, 94 % des Canadiens avaient un accès Internet à domicile (une hausse comparativement à 79 % en 2010), et 71 % des Canadiens utilisaient des services bancaires en ligne (le pourcentage atteignait 67 % en 2010).[3]

En raison des restrictions liées à la pandémie de COVID-19, les Canadiens se sont tournés rapidement et en grand nombre vers le télétravail. Ils accèdent à la propriété intellectuelle et à d'autres données sensibles en utilisant des dispositifs personnels et des réseaux Wi-Fi peu sécurisés comparativement à l'infrastructure de TI de leur entreprise. La protection de la propriété intellectuelle est cruciale pour la productivité et la compétitivité des entreprises canadiennes, et elle est vitale pour assurer la croissance économique du Canada ainsi que la défense nationale. Certains pays continuent d'avoir recours à des programmes avancés de cyberespionnage pour obtenir des avantages déloyaux sur les marchés mondiaux et améliorer leur technologie militaire. Le cyberespionnage industriel contre des entreprises est répandu dans de nombreux secteurs, dont ceux de l'aviation, de la technologie, de l'intelligence artificielle et de l'industrie biopharmaceutique.[4]

PLUS NOMBREUSES SONT LES DONNÉES RECUEILLIES PLUS GRAND EST LE RISQUE D'ENTRAVE À LA VIE PRIVÉE

Les Canadiens génèrent une incroyable quantité de données concernant les endroits où ils vont, leurs habitudes d'achat, leur mode de vie et leur santé lorsqu'ils utilisent leurs téléphones, ordinateurs ou services bancaires en ligne. C'est aussi le cas lorsqu'ils magasinent en ligne, portent des montres intelligentes et des moniteurs d'activité physique, arment leur système de sécurité à domicile ou contrôlent leur niveau d'insuline au moyen de dispositifs médicaux intelligents. Alors que les Canadiens génèrent, stockent et partagent de plus en plus de renseignements personnels en ligne, ces données sont plus susceptibles d'être la cible d'auteurs de cybermenace si les entreprises ou les gouvernements étrangers qui les recueillent sont victimes d'une atteinte à la sécurité ou les utilisent de façon abusive. Le nombre croissant de dispositifs connectés à Internet s'ajoute à la quantité de données recueillies sur les Canadiens. Le Commissariat à la protection de la vie privée du Canada (CPVP) a enregistré pas moins de 680 atteintes à la protection des données, qui ont touché 28 millions de Canadiens au cours de l'exercice s'étant terminé le 1er novembre 2019.[5]

Pendant ce temps, les progrès réalisés par la science des données font en sorte qu'il est plus difficile d'assurer l'anonymat et la confidentialité des données. Ces progrès technologiques permettent d'associer des renseignements qui étaient auparavant anonymes à d'autres ensembles de données et de les désanonymiser. La confidentialité des données est un enjeu important pour les Canadiens. Selon une étude commandée par le CPVP, 92 % des Canadiens ont soulevé des inquiétudes concernant la protection de leur vie privée, et 37 % se sont dits très préoccupés.[6]



4 DES COMPÉTENCES ET DES OUTILS AVANCÉS ACCESSIBLES À UN PLUS GRAND NOMBRE D'AUTEURS DE MENACE

La croissance du marché commercial des outils destinés aux activités de cybermenace et des services d'experts en la matière

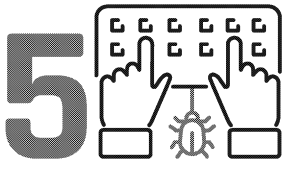
La vente commerciale d'outils liés à la cybercriminalité, à laquelle s'ajoute un bassin mondial d'experts en la matière, a entraîné une hausse du nombre d'auteurs de menace et donné lieu à une plus grande sophistication de leurs activités, ce qui complique le processus de reconnaissance, d'attribution et de défense contre les activités de cybermenace. On a remarqué sur ces marchés qu'il faut moins de temps à un État pour mettre en place un programme d'activités de cybermenace, et qu'un plus grand nombre d'États sont dotés de tels programmes. Depuis 2005, le Council on Foreign Relations tient une liste de plus en plus longue de pays soupçonnés de parrainer des activités malveillantes. La liste compte actuellement 33 pays.[7]

On s'attend à ce que la croissance du marché mondial des produits et services liés à la cybercriminalité passe d'environ 204 milliards $ CA en 2018 à 334 milliards $ CA en 2023.[8] Dans le but de développer rapidement leurs programmes nationaux, les auteurs de cybermenace parrainés par des États recrutent des expatriés qualifiés en leur offrant des salaires avantageux. Cela représente un changement important par rapport à l'époque où les États devaient développer leur propre bassin d'experts en la matière.

Un écosystème de cybercriminalité en plein essor

Au vaste marché commercial légitime s'ajoute un marché illégitime offrant des outils et des services liés à la cybercriminalité. De nombreux marchés en ligne autorisent la vente d'outils et de services spécialisés à des acheteurs qui s'en servent ensuite à des fins malveillantes, comme la défiguration de sites Web, l'espionnage, les attaques par DDoS et les attaques par rançongiciel. L'achat de ces outils et services permet aux cybercriminels de réduire considérablement leur temps de préparation et d'utiliser de meilleurs outils.

L'évolution de la cryptomonnaie a facilité les activités des cybercriminels et des États qui s'en servent pour échanger et blanchir de l'argent en préservant mieux leur anonymat. Si les cybercriminels n'avaient pas accès à la cryptomonnaie, les coûts associés à certains cybercrimes seraient prohibitifs. Des lois sur le blanchiment d'argent ont été adoptées dans beaucoup de pays pour contrer la cybercriminalité. Toutefois, le succès des cybercriminels est en partie attribuable aux lois trop clémentes ou inexistantes d'autorités gouvernementales partout dans le monde, ainsi qu'à l'application qui est faite de ces lois. Par exemple, en Russie, en Chine et en Iran, il est peu probable que des cybercriminels soient poursuivis pour avoir mené des activités de cybermenace motivées par un intérêt financier contre des cibles à l'extérieur du pays.[9]



5 INTERNET À LA CROISÉE DES CHEMINS

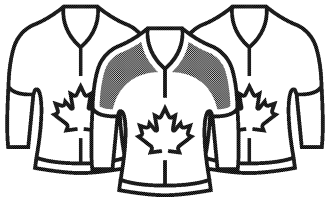
Gouvernance d'Internet

Beaucoup d'États exercent une forte pression pour changer l'approche reconnue à l'égard de la gouvernance d'Internet et suggèrent de passer d'une approche plurilatérale à une approche de souveraineté étatique. Ils considèrent les idées et l'information en termes de stabilité et de sécurité nationale, et ils veulent qu'Internet puisse leur permettre de surveiller leurs citoyens et de censurer l'information. Certains de ces régimes utilisent Internet pour réprimer les protestations, arrêter les dissidents, alimenter la désinformation et surveiller les citoyens.[10] La Chine et la Russie, qui sont des leaders du modèle de gouvernance fondée sur la souveraineté étatique, continuent de faire valoir leurs intérêts sur la scène internationale auprès d'agences comme l'Union internationale des télécommunications (UIT) et d'autres organisations des Nations Unies, en déposant des propositions politiques et relatives aux normes techniques. Ces dernières peuvent avoir des répercussions exceptionnelles et concrètes, comme le démontre la proposition du nouveau protocole Internet formulée par la Chine et les entreprises de télécommunications chinoises. Selon elles, le nouveau protocole pourrait transformer radicalement le fonctionnement d'Internet.[11] En plus d'offrir certains avantages sur le plan de la cybersécurité, ce nouveau protocole Internet conférerait à l'État un important pouvoir de censure, de surveillance et de contrôle.[12]

Historiquement, l'approche préconisée en ce qui a trait à la gouvernance d'Internet est l'approche plurilatérale adoptée par le Canada et d'autres pays aux vues similaires. Cette approche demande une grande participation de la part des gouvernements, des industries, de la société civile et du milieu universitaire, qui se réunissent pour établir des lignes directrices techniques et de politiques. Elle considère Internet comme un outil de développement global qui doit offrir un juste équilibre entre, d'une part, l'accès universel et l'interopérabilité et, d'autre part, la vie privée et la sécurité.

Influence étrangère en ligne

Comme nous l'avons indiqué dans notre *Évaluation des cybermenaces contre le processus démocratique du Canada*, les adversaires utilisent l'influence en ligne pour servir leurs intérêts fondamentaux, à savoir la sécurité nationale, la prospérité économique et leurs visées idéologiques. Les campagnes d'influence étrangère en ligne font maintenant partie de la nouvelle normalité et les adversaires tentent d'influencer des événements à l'échelle nationale (comme les élections) et d'avoir un impact sur les débats publics qui se tiennent sur la scène internationale. Un engagement démocratique en ligne fait appel à un Internet juste et transparent, à l'abri des manipulations des acteurs étrangers. De plus en plus d'États ont développé des cyberoutils qu'ils utilisent pour mener des activités d'influence en ligne à grande échelle. Ils profitent des médias sociaux, de publicités légitimes et d'outils d'échange d'information pour atteindre un large public et rendre leurs messages plus efficaces. La technologie d'hypertrucage, qui permet la création réaliste de vidéos et d'événements, ajoute un facteur d'incertitude et de confusion auprès des groupes ciblés par les campagnes de désinformation. Ce procédé de manipulation audiovisuelle s'est rapidement développé en raison de la forte augmentation de la demande pour diverses applications capables de changer les visages, des produits permettant de produire une vidéo d'une personne à partir de rien[13] et un logiciel d'hypertrucage audio capable de cloner des voix humaines.[14]



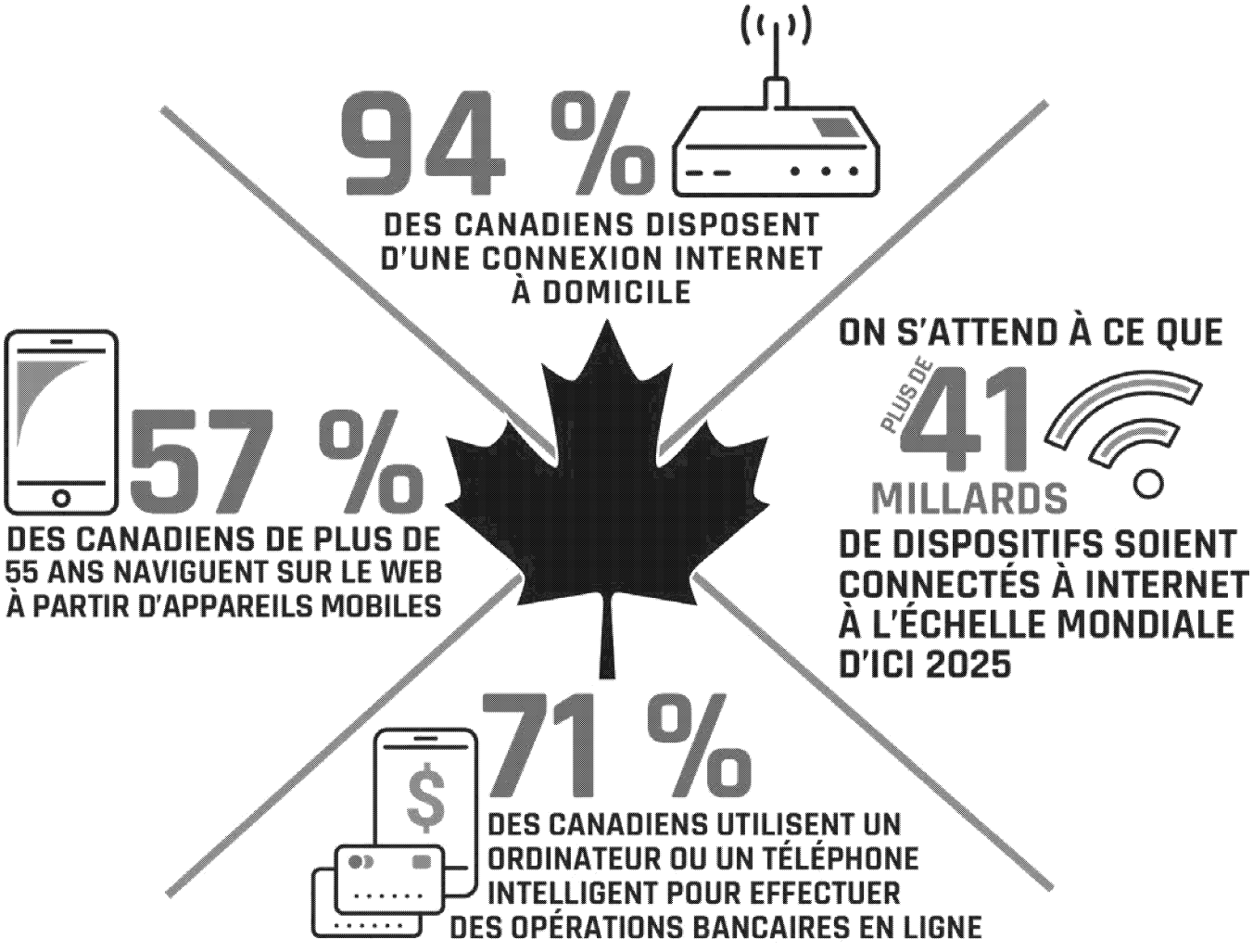
LES CYBERMENACES CONTRE LES CANADIENS

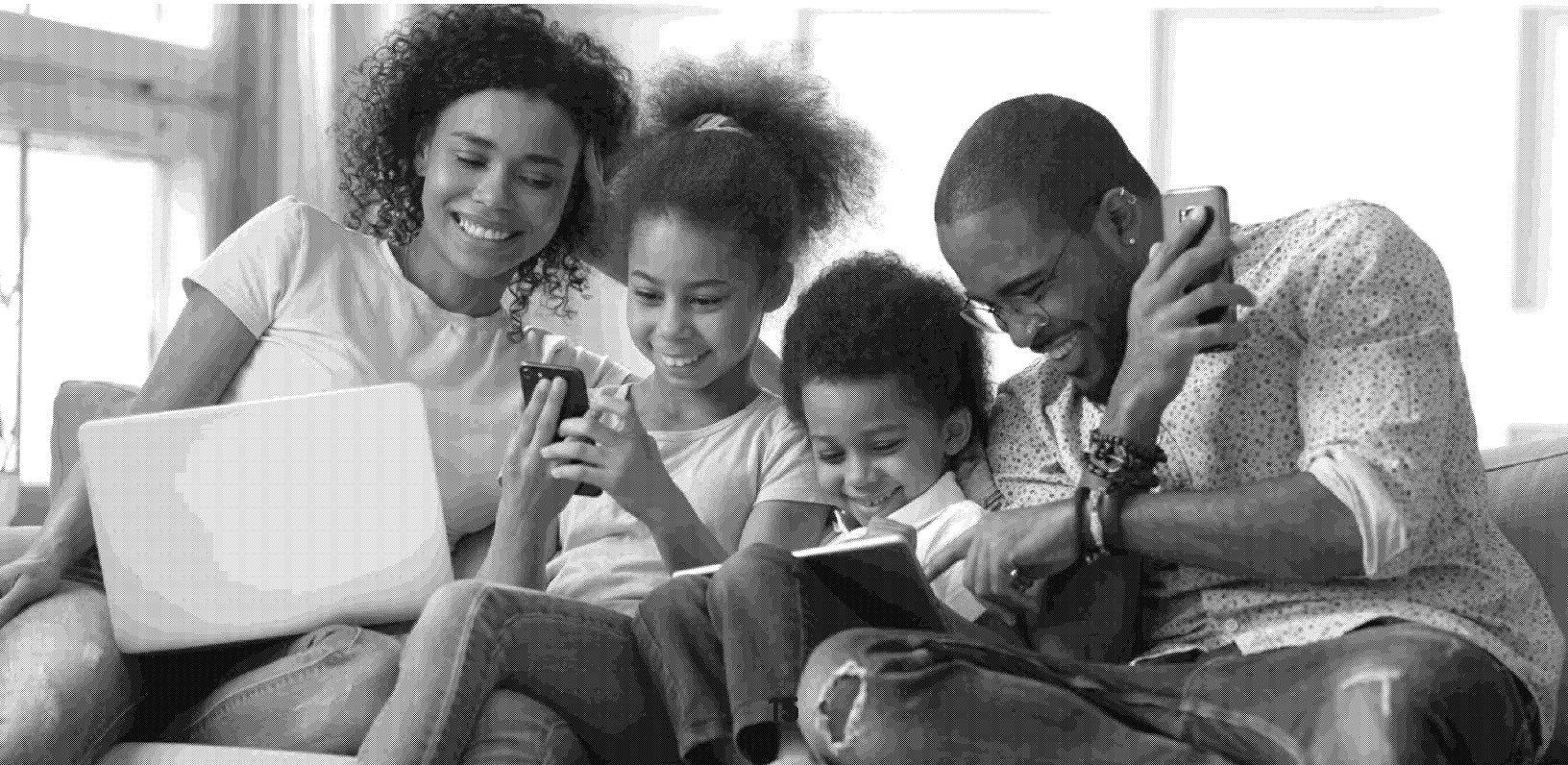
Les Canadiens mettent de plus en plus de renseignements personnels sur Internet, et ils dépendent aussi davantage de dispositifs connectés à Internet pour les communications, les finances, le divertissement, le confort et la sécurité. À mesure qu'évolue la technologie et que les habitudes changent, les auteurs de cybermenace s'adaptent rapidement pour tirer profit de nouvelles occasions et suivre les événements actuels. Ils vont par exemple modifier leur activité de cybermenace pendant la pandémie de COVID-19.

Les Canadiens continuent d'être victimes de fraudes en ligne. Comme prévu dans l'évaluation de 2018, il est fort probable que la cybercriminalité demeure la cybermenace la plus répandue auprès des Canadiens. Depuis la publication de l'évaluation de 2018, les auteurs de cybermenace ont amélioré leur façon de procéder de manière à rendre les arnaques pertinentes et attrayantes en associant leurs cyberfraudes à des événements d'actualité. Les élections, la période des impôts et les nouvelles qui font l'actualité ont toutes servi de toile de fond à la cybercriminalité. Par exemple, les auteurs de menace ont profité de la pandémie de COVID-19 pour inciter les victimes à cliquer sur des liens malveillants. Ces auteurs volent également des renseignements financiers et médicaux, ainsi que d'autres renseignements personnels qu'ils vendent en ligne ou utilisent dans le cadre de cybercrimes. Les importantes atteintes à la protection des données qui touchent les entreprises ont de sérieuses répercussions sur leurs clients. Ces atteintes révèlent des renseignements personnels pouvant servir à d'éventuels crimes.

Les Canadiens sont toujours victimes des opérations d'influence étrangère en ligne. L'objectif de celles-ci est d'influencer l'opinion publique et le discours politique au Canada. Et pour terminer, il importe de souligner que l'évolution des technologies comme les dispositifs médicaux de l'IdO, les véhicules connectés à Internet et les systèmes de sécurité à domicile procure aux auteurs de cybermenace de nouvelles cibles pour mettre en péril la sécurité physique des Canadiens.

Figure 1 : Utilisation d'Internet par les Canadiens; données tirées de l'Enquête canadienne sur l'utilisation de l'Internet 2018 de Statistique Canada[15], du Dossier documentaire sur Internet au Canada 2019 de l'ACEI[16] et des prévisions de l'International Data Corporation[17]





FRAUDE ET EXTORSION

Selon les statistiques obtenues du Centre antifraude du Canada, en 2019, les Canadiens ont perdu plus de 43 millions $ CA à la suite de fraudes liées à la cybercriminalité.[18] Ce chiffre ne tient compte que des cas rapportés de fraudes. On considère que le chiffre réel est fort probablement plus élevé. Comme prévu dans l'évaluation de 2018 et selon nos observations, au cours des deux dernières années, les types de tentatives de cyberfraude et d'extorsion visant les Canadiens ont gagné en sophistication. Cette tendance risque de se poursuivre, facilitée par les marchés de la cybercriminalité qui permettent aux auteurs de menace d'acheter des outils et services qu'ils utiliseront ensuite dans le cadre d'activités de cybermenace.

Les auteurs de cybermenace 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 des maliciels sur leurs dispositifs en cliquant sur des pièces jointes ou des liens malveillants. Par exemple, certains fraudeurs créent de faux sites Web et de fausses publicités en ligne offrant des services d'immigration bon marché, ou garantissant des emplois bien rémunérés aux nouveaux immigrants. Beaucoup de ces faux sites Web ressemblent à des sites officiels du gouvernement, mais exigent que les victimes paient des frais pour avoir accès à des « formulaires importants ».[19] Depuis mars 2020, le CCC a travaillé avec ses partenaires pour fermer plus de 3 500 sites Web, comptes de médias sociaux et serveurs de courrier électronique qui représentaient frauduleusement le gouvernement du Canada.

Les auteurs de cybermenace peuvent également soutirer de l'argent à leurs victimes en les menaçant de cyberattaques ou en volant ou prétendant leur avoir volé des renseignements incriminants. Ces arnaqueurs créent également de faux profils sur les médias sociaux et les sites de rencontre afin d'inciter leurs victimes à s'engager dans une relation sur Internet qui facilite l'extorsion et la fraude. Dans certains cas, ils obtiennent des vidéos intimes de leur victime et menacent d'envoyer la vidéo aux contacts de celle-ci si la rançon n'est pas versée.[20]

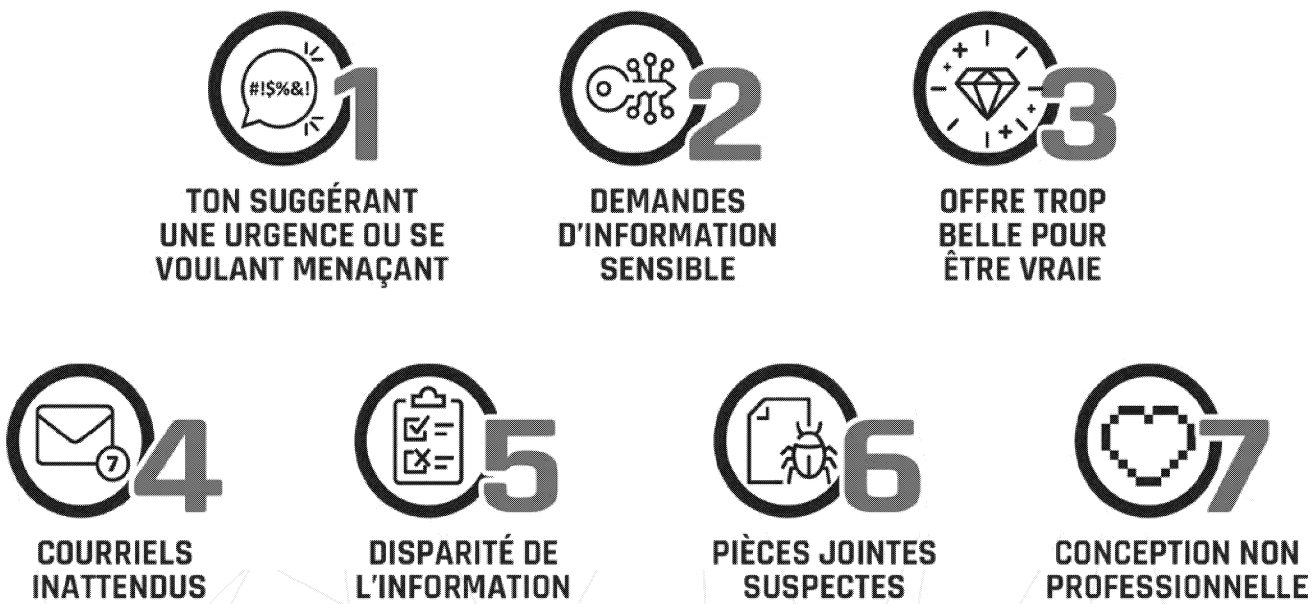
Depuis la publication de l'évaluation de 2018, nous avons remarqué que les auteurs de cybermenace se sont adaptés aux événements actuels en associant davantage leur façon de procéder à des événements d'actualité. Les élections, la période des impôts et les nouvelles qui font l'actualité ont toutes servi de toile de fond à la cybercriminalité pour inciter les victimes à cliquer sur des pièces jointes et des liens malveillants.

LES AUTEURS DE MENACE INFLUENCENT UNE CRISE MONDIALE : LA COVID-19

En 2020, nous avons observé les auteurs de cybermenace développer du contenu lié à la COVID 19 pour inciter les victimes à cliquer sur des pièces jointes et des liens malveillants. Les auteurs de cybermenace savent à quel point les gens sont inquiets quant à l'avenir et comptent sur le fait que leurs potentielles victimes sont moins portées à agir avec prudence lorsqu'elles reçoivent des courriels, des textos ou de la publicité concernant la COVID 19.

Les leurres liés à la COVID-19 impliquent souvent la reproduction ou l'imitation d'une marque ou d'un style propre à des organismes légitimes, comme des organismes internationaux et des services de santé publique. Les auteurs de cybermenace peuvent produire des copies convaincantes de sites Web du gouvernement et de correspondances officielles. Une campagne utilisant des courriels d'hameçonnage par SMS prétendait donner accès au paiement de la Prestation canadienne d'urgence, mais seulement après que la victime ait divulgué ses renseignements financiers personnels. Les auteurs d'une autre campagne se faisaient passer pour un médecin-conseil en santé de l'Agence de la santé publique du Canada pour implanter un maliciel au moyen d'une fausse mise à jour sur la COVID-19 qui semblait officielle et légitime.

Figure 2 : Éléments d'une communication malveillante



MENACES D'INGÉRENCE DANS LA VIE PRIVÉE

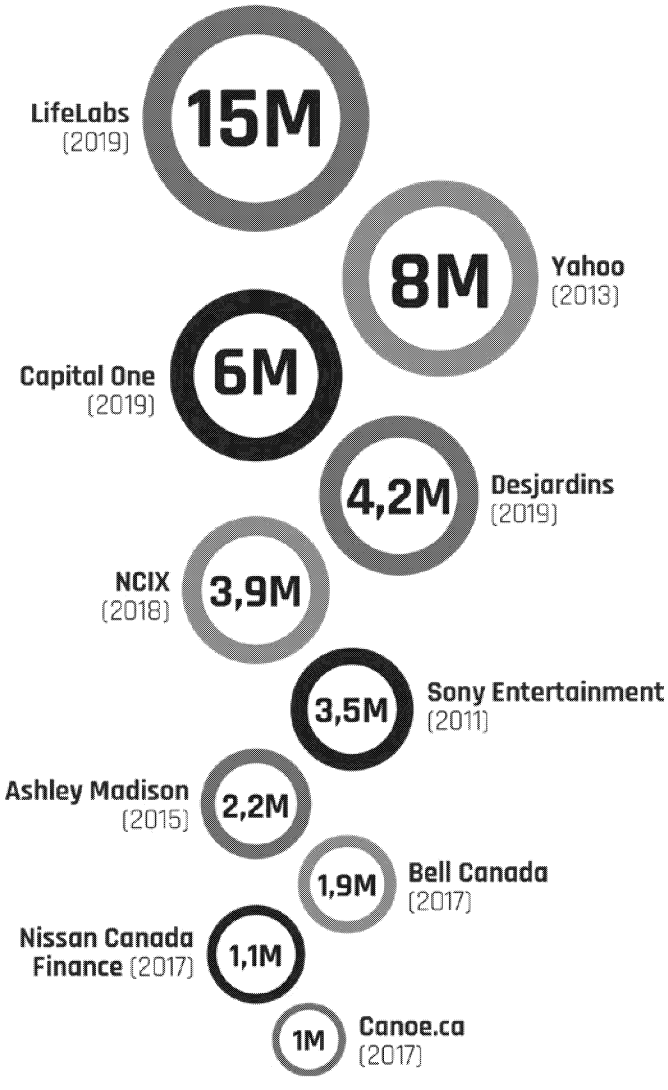
Dans l'évaluation de 2018, nous décrivons l'attrait des renseignements financiers et personnels pour les cybercriminels et voyons comment ces derniers profitent des renseignements volés pour obtenir un gain financier. La menace s'est maintenant intensifiée en raison de l'augmentation de la quantité de renseignements qui sont stockés en ligne, et dans la foulée des améliorations apportées à la science des données qui favorisent de nouvelles méthodes pour ce qui est d'exploiter les renseignements personnels, financiers et même médicaux. En outre, les cybercriminels ne sont pas les seuls auteurs de cybermenace intéressés à ces données. Il y a aussi les auteurs de cybermenace parrainés par des États qui compromettent d'importantes bases de données pour faire avancer les priorités nationales.

Renseignements financiers

La progression de la menace visant la vie privée des citoyens s'accroît avec le nombre de données échangées et stockées en ligne. Les atteintes à la protection des données menacent les renseignements financiers des Canadiens que détiennent les sociétés, et ces renseignements deviennent la proie des auteurs de cybermenace. Le vol des renseignements personnels et financiers des Canadiens est payant pour les cybercriminels, et on considère que ce type de fraude devrait augmenter au cours des deux prochaines années. Les cybercriminels font des profits au détriment des victimes en volant leurs justificatifs d'ouverture de session, les détails relatifs à leurs cartes de crédit et d'autres renseignements personnels. Ils peuvent ensuite décider de se servir de ces renseignements pour voler de l'argent ou commettre une fraude, ou tout simplement de les vendre sur les marchés de la cybercriminalité. En juin 2019, les données de 4,2 millions de membres canadiens de Desjardins ont été compromises.[21]

Cette fuite de données touchait, entre autres, les noms et les dates de naissance, les numéros d'assurance sociale, les coordonnées et les renseignements bancaires des victimes. Tout comme dans le cas de Desjardins, 6 millions de clients canadiens de la Capital One ont appris qu'ils avaient été victimes du vol de leurs renseignements personnels en mars 2019. Parmi les données volées, on retrouvait des renseignements personnels et des cotes de crédit, des données sur les opérations et des numéros de compte bancaire.[22]

Figure 3 : Dix des plus importantes atteintes à la protection des données ayant eu une incidence sur les Canadiens de 2011 à aujourd'hui, par nombre de dossiers



CRYPTOMONNAIE ET CRYPTOMINAGE PIRATE

Les cybercriminels ont recours à des maliciels pour prendre le contrôle d'ordinateurs et utiliser leur puissance de calcul pour générer ou « miner » de la cryptomonnaie sans autorisation. C'est ce que l'on appelle le cryptominage. Les systèmes informatiques désuets ou non corrigés sont particulièrement vulnérables à cette cybermenace, et certains utilisateurs touchés peuvent ne rien voir d'inhabituel avec leur dispositif, tandis que d'autres constatent des problèmes de ralentissement ou une décharge rapide de la pile.[23]

Comme prévu dans l'évaluation de 2018, les cybercriminels ont continué de développer des maliciels en vue de les déployer dans le cadre d'opérations de cryptominage pirate. Selon nos observations, cette activité devrait fort probablement continuer au cours des deux prochaines années dans la mesure où les niveaux d'activité sont liés aux fluctuations de la valeur de la cryptomonnaie.

Données médicales et personnelles

En 2019, l'entreprise de laboratoire médical LifeLabs a été victime d'une cyberattaque qui a compromis les données personnelles et médicales de 15 millions de Canadiens avant que l'entreprise paie la rançon demandée pour récupérer les données.[24] Les auteurs de menace, et tout particulièrement les auteurs de cybermenace parrainés par des États, ont recours à la science des données pour mieux utiliser les grands ensembles de données. Ils peuvent ainsi identifier, profiler et suivre les citoyens en combinant et en désanonymisant les données provenant de plusieurs ensembles de données.

Les auteurs de cybermenace peuvent utiliser les renseignements personnels volés en se servant d'une technique appelée « attaque de bourrage de justificatifs » par laquelle un grand nombre de combinaisons de noms d'utilisateur et de mots de passe compromis sont entrées dans des sites Web dans l'espoir qu'une de celles-ci corresponde à un compte existant. Les renseignements personnels volés peuvent comprendre des justificatifs d'identité qui faciliteront ce type d'activité de même qu'un accès aux réponses aux questions de sécurité, rendant ainsi inefficace cette protection. Après avoir recueilli des données lors de multiples atteintes à la sécurité, les cybercriminels sont en mesure de combiner les renseignements personnels d'une personne et de cibler plus efficacement leurs activités de cybermenace.

ATTEINTE À LA PROTECTION DE DONNÉES DE LA CAPITAL ONE ET DES HÔTELS MARRIOTT

Une accumulation de données attire les cybercriminels et les auteurs de cybermenace parrainés par des États. En 2019, un cybercriminel a volé les données des clients de la Capital One, une société de services financiers américaine. Cette atteinte à la sécurité a touché 106 millions de clients, dont six millions de Canadiens. Parmi les renseignements privés recueillis se trouvaient des numéros d'assurance sociale et de sécurité sociale ainsi que des renseignements bancaires.[25] En 2018, la chaîne hôtelière Marriott a annoncé que sa base de données de réservation avait été compromise, et que les renseignements personnels d'environ 500 millions d'invités avaient été volés. Cette attaque a été liée à des pirates informatiques parrainés par des États. Ils ont pu mettre la main sur de nombreux renseignements, dont des noms, des adresses et des numéros de passeport.[26]

INFLUENCE ÉTRANGÈRE EN LIGNE

Un nombre croissant d'États ont élaboré et déployé des programmes visant à mener une activité d'influence en ligne dans le cadre de leurs pratiques quotidiennes. Des adversaires ont recours à des campagnes d'influence pour tenter de changer le discours public, les choix des décideurs politiques, les relations gouvernementales et la réputation des politiciens et des pays, tant à l'échelle nationale qu'internationale. Ils tentent de délégitimiser le concept de la démocratie ainsi que d'autres valeurs, comme les droits de la personne et ceux touchant aux libertés, qui peuvent aller à l'encontre de leurs propres positions idéologiques. Ils cherchent également à aggraver la friction actuelle dans les sociétés démocratiques en ce qui concerne diverses questions controversées d'ordre social, politique et économique. Bien que les activités d'influence en ligne aient tendance à augmenter en périodes électorales, la portée de ces campagnes continues s'est élargie depuis 2018, de façon à réagir et à s'adapter aux événements actuels, et à changer les stratégies en fonction des nouvelles qui font l'actualité et des enjeux politiques populaires.

Comme prévu dans l'évaluation de 2018, les Canadiens continuent d'être la cible d'activités d'influence en ligne. Par exemple, nous avons noté que l'attention des récentes campagnes s'est tournée sur la COVID-19 et les mesures prises par les gouvernements face à la pandémie. Les campagnes de désinformation ont également cherché à discréditer et à critiquer les politiciens canadiens dans le but de nuire à leur réputation. Nous estimons néanmoins que, comparativement à d'autres pays, les Canadiens ne présentent pas une cible prioritaire en ce qui a trait aux campagnes d'influence étrangère en ligne, mais les positions prises par le Canada sur des enjeux prioritaires d'ordre géopolitique pourraient faire augmenter la menace. Il faut toutefois noter qu'au Canada, les écosystèmes des médias sont étroitement liés à ceux des États-Unis et d'autres alliés. Conséquemment, lorsque les populations de ces pays sont ciblées, les Canadiens s'exposent à des dommages collatéraux en raison de l'influence en ligne.

On considère que l'exposition à l'influence étrangère en ligne se poursuivra certainement pendant au moins les deux prochaines années pour autant que les auteurs de cybermenace adaptent leurs activités à l'évolution des politiques des sociétés Internet comme Google, Facebook et Twitter.

LES AUTEURS DE CYBERMENACE TENTENT DE DIVISER LES CANADIENS

Une analyse des données Tweeter a révélé que des trolls d'Internet russes et iraniens ont utilisé des comptes de façon frauduleuse pour mettre en évidence les divisions entre les Canadiens en amplifiant des propos incendiaires sur des questions politiques qui attisent la discorde, comme le terrorisme, les changements climatiques, la construction de pipelines, ainsi que les politiques sur l'immigration et à l'égard des réfugiés. Bon nombre de ces gazouillis réagissaient à des événements importants, comme ce fut le cas en janvier 2017 à la suite de la tuerie de la mosquée de Québec, ou en juin 2019 après l'approbation de l'expansion du pipeline Trans Mountain.[27]

MENACES À LA SÉCURITÉ PHYSIQUE

Les dispositifs personnels connectés à Internet, notamment les dispositifs médicaux de l'IdO, les véhicules connectés à Internet et les systèmes de sécurité à domicile, font partie du quotidien et constituent de nouvelles cibles pour les auteurs de cybermenace. Cela dit, bien que d'autres cybermenaces, comme les atteintes à la protection des données, soient plus répandues et aient des répercussions plus larges, les utilisateurs courent quand même le risque que leurs dispositifs et systèmes soient éventuellement ciblés par des activités de cybermenace pouvant avoir une incidence sur leur sécurité physique. Par exemple, les dispositifs médicaux connectés à Internet sont de plus en plus courants et susceptibles d'être la cible d'auteurs de cybermenace qui chercheront à en altérer ou en perturber le fonctionnement.

Un autre exemple démontre que des harceleurs et des partenaires violents tirent avantage des vulnérabilités des dispositifs personnels de l'IdO pour voler les renseignements recueillis par les montres intelligentes et les moniteurs d'activité physique dans le but d'identifier et de localiser leurs victimes. Ils sont également en mesure de manipuler les systèmes de maison intelligente afin de contrôler l'environnement de leurs victimes et de les intimider. Dans un cas en particulier, un homme s'est servi d'une application de véhicule intelligent pour démarrer, éteindre et suivre le véhicule de sa victime à partir de son téléphone.[28] Un organisme offrant du soutien aux victimes de violence conjugale a indiqué qu'en date de janvier 2019, plus de 2 500 femmes qui y trouvent refuge ont déclaré avoir été victimes d'abus facilités par la technologie.[29]

DISPOSITIFS MÉDICAUX PERSONNELS CONNECTÉS À INTERNET

En mars 2020, Santé Canada a publié une alerte informant les Canadiens de vulnérabilités de cybersécurité touchant des dispositifs médicaux, comme les simulateurs cardiaques, les glucomètres et les pompes à insuline, dotés d'un certain type de puce Bluetooth. Des auteurs de menace pourraient exploiter ces vulnérabilités pour provoquer une panne du dispositif, le déverrouiller ou contourner les mesures de sécurité afin d'accéder à des fonctionnalités qui sont réservées à un utilisateur autorisé.[30]

LES CYBERMENACES CONTRE LES ORGANISMES CANADIENS

Comme prévu dans l'évaluation de 2018, la cybercriminalité demeure la menace la plus répandue à laquelle font face les entreprises canadiennes de toutes tailles. Toutefois, d'autres activités de cybermenace, comme le cyberespionnage, peuvent avoir une incidence plus grande. 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. Depuis les deux dernières années, cibler des procédés industriels et mener des attaques par rançongiciel sont pratique courante. Les incidences de ces cyberincidents peuvent être majeures, notamment porter atteinte à la réputation, entraîner une perte de productivité, avoir des répercussions juridiques, exiger des dépenses relatives à la reprise et entraîner des dommages à l'infrastructure et aux opérations. On considère que les activités malveillantes dirigées contre le Canada continueront probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles au cours des deux prochaines années.

Les auteurs de cybermenace mettent également en danger l'information que détiennent les organisations canadiennes ainsi que les données des clients. Le vol de cette information peut avoir des conséquences financières à court et à long termes pour les victimes, notamment des impacts sur leur compétitivité à l'échelle internationale et sur leur réputation. Pendant la pandémie de COVID-19, des auteurs de cybermenace parrainés par des États ont ciblé la propriété intellectuelle canadienne liée à la lutte contre la COVID-19, et on estime que ces auteurs continueront probablement à le faire afin d'appuyer leurs programmes de santé publique nationaux ou de tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés.

Les auteurs de cybermenace ciblent les systèmes de paiement en ligne et en personne, profitent des vulnérabilités des chaînes d'approvisionnement et tirent parti de l'accès privilégié que maintiennent les fournisseurs de services gérés aux réseaux de leurs clients. Ces activités peuvent servir à frauder des organisations, à se livrer à des attaques par rançongiciel ou à voler des renseignements exclusifs ou les données des clients.

Les organisations canadiennes de toutes tailles, comme les petites et moyennes entreprises, les municipalités, les universités et les fournisseurs d'infrastructures essentielles, sont confrontées à un nombre croissant de cybermenaces.[31]

Ces organisations contrôlent un vaste éventail d'actifs pouvant intéresser les auteurs de cybermenace, dont la propriété intellectuelle, les données financières, les systèmes de paiement, les données des clients, les partenaires et les fournisseurs, ainsi que les installations industrielles et leur machinerie. En règle générale, plus une organisation possède d'actifs connectés à Internet, plus elle court le risque de faire face à une cybermenace.

Figure 4 : Liste des actifs appartenant à des organisations qui augmentent le risque pour la cybersécurité

CIBLER LA SÉCURITÉ DES CANADIENS

Cibler les systèmes de contrôle industriels et les infrastructures essentielles

La sécurité des Canadiens est menacée lorsque les auteurs de cybermenace ciblent des organisations responsables de l'exploitation des services publics ou de la prestation de soins de santé ou de services gouvernementaux essentiels. Or, à en juger par l'évaluation de 2018, il est fort improbable que des auteurs de cybermenace tentent de perturber volontairement les infrastructures essentielles du Canada et de causer de sérieux dommages ou des pertes de vie s'il n'y a aucun climat d'hostilité à l'échelle internationale. Ils pourraient néanmoins cibler des entreprises canadiennes essentielles dans le but de recueillir des données, de se prépositionner en vue d'activités ultérieures ou de les intimider. Il est fort probable que des auteurs de cybermenace parrainés par des États cherchent à développer les moyens nécessaires pour perturber l'approvisionnement en électricité au Canada.

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 le cadre des procédés industriels ou des processus liés aux infrastructures essentielles. Les SCI, et plus particulièrement ceux du secteur de l'électricité, sont ciblés dans le monde entier. Les auteurs de cybermenace parrainés par des États sont souvent à l'origine de ces attaques. En 2019, des pirates associés à la Russie ont accédé aux réseaux de fournisseurs d'électricité aux États-Unis et au Canada.[32] Des groupes de pirates informatiques iraniens ont ciblé des infrastructures dans des nations rivales, notamment les États-Unis, Israël et l'Arabie saoudite.[33] Un maliciel nord-coréen a été trouvé dans les réseaux informatiques d'une centrale électrique indienne, et des employés des services publics américains ont été visés par des auteurs de cybermenace parrainés par la Chine.[34]

Depuis les dernières années, les rançongiciels ont de plus en plus d'incidences sur les SCI. On estime que les programmes des rançongiciels peuvent maintenant s'infiltrer plus efficacement dans les réseaux informatiques et devenir une menace pour les environnements SCI connexes. Dans certains cas, les victimes choisissent de désactiver leurs procédés industriels par mesure de précaution lorsque l'entreprise fait l'objet d'une attaque par rançongiciel. Par exemple, en mars 2019, une aluminerie norvégienne a été paralysée par un rançongiciel qui a attaqué ses données logistiques et de production, ce qui l'a forcée à arrêter les SCI et à passer à la production en mode manuel.[35] Les cybercriminels devraient cibler davantage les SCI au cours des deux prochaines années afin d'accroître la pression sur les infrastructures essentielles et ainsi inciter les victimes de l'industrie à consentir rapidement au paiement de la rançon demandée.

EXEMPLE DE RANÇONGICIEL VISANT LES SCI

Depuis janvier 2019, au moins sept variantes de rançongiciel contenaient des instructions visant à interrompre les procédés liés aux SCI.[36] L'impact de ces attaques sur les SCI varie en fonction des circonstances particulières du procédé industriel et de la réaction du personnel en place.[37] En juin 2020, un constructeur automobile a suspendu la production dans la majorité de ses usines en Amérique du Nord, dont une au Canada, pour « assurer la sécurité de ses activités » après avoir été la cible d'une attaque faisant appel à une de ces variantes de rançongiciel.[38]

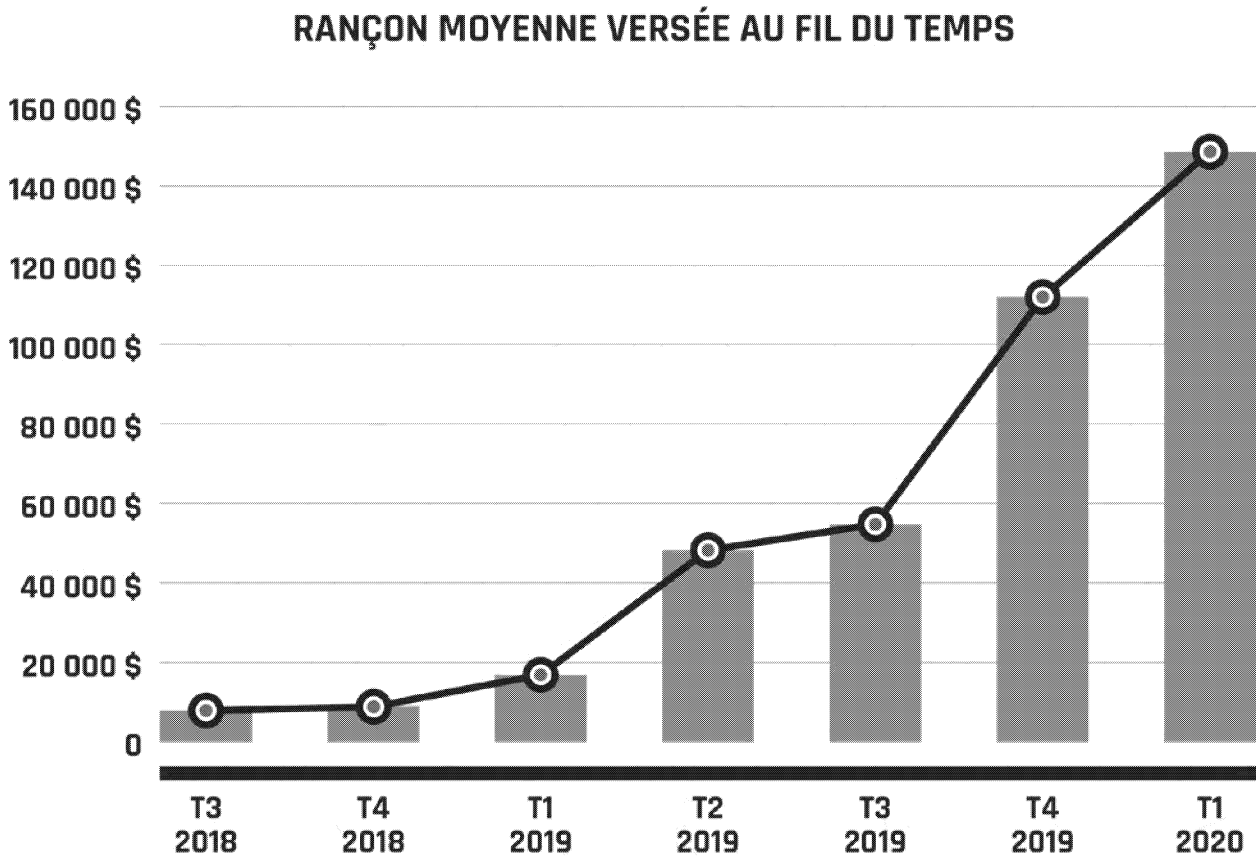
MENACES À LA SANTÉ FINANCIÈRE ET ÉCONOMIQUE DES CANADIENS

Les activités de cybermenace entraînent des dépenses imprévues pour les organisations. Il peut s'agir des rançons versées ou de fonds volés, des pertes occasionnées par l'interruption des opérations, des coûts nécessaires pour assurer la sécurité des réseaux, d'une atteinte à la réputation et de la perte de clients qui en découle, et sans oublier du vol de propriété intellectuelle et de renseignements confidentiels.[39] Ces coûts siphonnent les ressources limitées des organisations et diminuent la compétitivité de ces dernières face à d'autres entreprises. Combinés, ils représentent en fait un fardeau sur l'ensemble de l'économie canadienne.

Rançongiciel et chasse au gros gibier

Selon l'évaluation de 2018, le rançongiciel a été identifié comme étant la forme la plus répandue de maliciel utilisé pour extorquer de l'argent aux Canadiens. Les cybercriminels ont toutefois changé leurs tactiques pour leur permettre d'augmenter le montant des rançons demandées et d'accroître leur probabilité de réussite. Au cours des dernières années, les cybercriminels chassent de plus en plus le gros gibier et concentrent leurs activités sur de grandes entreprises qui doivent éviter que leurs réseaux soient perturbés, et qui sont prêtes à payer de lourdes rançons pour rétablir rapidement leurs opérations.[40] Avec la recrudescence de ce type de campagne de rançongiciel, le montant des rançons demandées a aussi augmenté. Les chercheurs en rançongiciel estiment que la moyenne des demandes de rançon a augmenté de 33 % depuis le T4 de 2019 pour atteindre environ 148 700 $ CA au cours du T1 de 2020 en raison de l'impact de ce type de cybermenace sur les opérations visées par des rançongiciels.[41] À l'extrémité du spectre se trouvent les demandes de rançon de plusieurs millions de dollars, qui sont devenues de plus en plus courantes. En octobre 2019, une compagnie d'assurance canadienne a payé 1,3 million $ CA pour récupérer 20 serveurs et 1 000 postes de travail.[42] De plus, nous croyons que les auteurs de cybermenace parrainés par des États pourraient utiliser un rançongiciel afin de masquer l'origine de leurs activités et leurs intentions. Il est presque assuré que les services de renseignement de nombreux pays collaborent avec des cybercriminels qui se livrent à des stratagèmes par rançongiciel. Dans cette collaboration avec bénéfices mutuels, les cybercriminels échangent des données avec les services de renseignement et ces derniers leur permettent de poursuivre leurs opérations sans avoir à respecter les lois.

Figure 5 : Rançon moyenne versée lors d'attaques par rançongiciel entre 2018 et 2020 (données de Coveware[43] avec conversion de $ US à $ CA)



Nous croyons que les activités malveillantes dirigées contre le Canada continueront fort probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles. En outre, il est probable que bon nombre de victimes canadiennes continueront de consentir à payer les rançons pour éviter les conséquences économiques graves et potentiellement dévastatrices qui pourraient survenir advenant un refus. Depuis la fin de 2019, de nombreuses entreprises canadiennes et plusieurs gouvernements provinciaux ont vu leurs données divulguées par des opérateurs de rançongiciels après avoir refusé de verser la rançon demandée. Ce fut entre autres le cas pour une entreprise de construction et un consortium d'entreprises agricoles canadiennes.[44]

LE SECTEUR DE LA SANTÉ FRÉQUEMMENT CIBLÉ PAR LES RANÇONGICIELS

En 2019 et 2020, de nombreux organismes canadiens du secteur de la santé ont été ciblés dans le cadre d'attaques par rançongiciel. Par exemple, en octobre 2019, trois hôpitaux de l'Ontario ont été victimes de telles attaques, et un centre de diagnostic et de tests spécialisés a vu ses données compromises par un rançongiciel en décembre 2019. Au début de 2020, une attaque par rançongiciel a aussi ciblé une société médicale de la Saskatchewan.[45] Beaucoup d'organismes mondiaux du secteur de la santé ont dû faire face à des attaques par rançongiciel pendant la pandémie de COVID-19, notamment des hôpitaux et des centres de soins de santé en République tchèque, aux États-Unis, en Espagne et en Allemagne.[46] Ces organismes sont des cibles populaires parmi les opérateurs de rançongiciels en raison de leurs importantes ressources financières et du fait qu'ils sont plus susceptibles de payer la rançon, puisqu'une panne de réseau peut mettre en danger la vie de patients.

Vol de propriété intellectuelle et de renseignements exclusifs

Dans l'évaluation de 2018, il a été question de la menace qui pèse sur les entreprises canadiennes en raison du cyberespionnage industriel. La menace est toujours présente aujourd'hui, puisque des auteurs de cybermenace parrainés par des États continuent de mener des activités d'espionnage contre les réseaux d'organismes au Canada et dans des nations alliées dans le but de voler la propriété intellectuelle, des secrets commerciaux et d'autres renseignements commerciaux de nature exclusive. Au Canada, ces auteurs de cybermenace ont mené des activités d'espionnage contre une grande diversité d'organismes canadiens, dont ceux du secteur privé, du milieu universitaire et du gouvernement. Ils ciblent plus particulièrement les organismes du secteur de la santé et de la biotechnologie, de l'énergie, des télécommunications et de la défense.[47]

Une campagne de longue date menée par des auteurs de cybermenace parrainés par des États a compromis des fournisseurs de services gérés (FSG) dans le but de mettre la main sur la propriété intellectuelle et des renseignements commerciaux et technologiques confidentiels liés à l'aviation, à la santé, à la biotechnologie, aux télécommunications, ainsi qu'à d'autres secteurs. Ils ont ciblé des entreprises tant au Canada que dans pas moins de 12 pays depuis 2006.[48] On a signalé en 2019 qu'une campagne parrainée par des États avait ciblé plus de deux douzaines d'universités au Canada, aux États-Unis et en Asie du Sud-Est pour tenter d'obtenir de l'information liée à la technologie et à la recherche maritimes à des fins militaires.[49]

Durant la pandémie de COVID-19, plusieurs grandes entreprises des industries médicale et biopharmaceutique du Canada et de l'étranger ont été la cible d'auteurs de cybermenace parrainés par des États qui tentaient de voler la propriété intellectuelle liée aux essais, aux traitements et aux vaccins contre la COVID-19. Selon nos observations, il est probable que ces auteurs de cybermenace continuent à tenter de voler la propriété intellectuelle canadienne touchant la lutte contre la COVID-19 pour appuyer leurs programmes de santé publique nationaux ou tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés.[50]

Les organisations ayant des activités et des infrastructures à l'étranger sont exposées à des cybermenaces supplémentaires. Leurs opérations à l'étranger peuvent être régies par des lois sur la propriété intellectuelle, la protection de la vie privée ou la sécurité nationale, qui sont différentes et parfois plus laxistes. De nombreux pays disposent d'un pouvoir juridique et ont la compétence technique nécessaire pour accéder secrètement aux données qui passent par leur pays ou y sont conservées. Cela a de sérieuses conséquences sur les données et la propriété intellectuelle canadiennes envoyées dans des bureaux à l'étranger ou sur celles qui transitent par des réseaux qui se trouvent dans d'autres pays. Même les données qui sont échangées entre deux organismes au Canada peuvent transiter par des réseaux étrangers avant d'arriver à destination. Toutefois, conformément aux jugements formulés dans l'évaluation de 2018, on considère que la menace de cyberespionnage est certainement beaucoup plus grande pour les entreprises canadiennes qui font des affaires à l'étranger ou qui travaillent directement avec des sociétés détenues par des États étrangers.

CYBERATTAQUES RUSSES CIBLANT LA RECHERCHE DE VACCIN CONTRE LA COVID-19

En juillet 2020, dans un communiqué conjoint, le Centre canadien pour la cybersécurité, le National Cyber Security Centre du Royaume Uni et la National Security Agency des États-Unis ont dressé un rapport des tactiques, des techniques et des procédures utilisées par un auteur de cybermenace parrainé un État qui ciblait des organisations impliquées dans le développement de vaccins contre la COVID-19 au Canada, aux États-Unis et au Royaume-Uni.[51] On considère que l'auteur de cette attaque pourrait fort probablement faire partie des services de renseignement russes et que son objectif est vraisemblablement de voler l'information et la propriété intellectuelle liées au développement et aux essais de vaccins contre la COVID-19.

Vol de données des clients

Comme prévu dans l'évaluation de 2018, les auteurs de cybermenace continuent de cibler les grands ensembles de données détenus par des entreprises au Canada et à travers le monde. Les bases de données volumineuses qui contiennent des renseignements personnels, tels que des noms, des adresses, des numéros de téléphone, de l'information relative à l'emploi, des références et des données financières ont pour eux une valeur inestimable. L'agrégation des données obtenues lors de multiples compromissions permet aux cybercriminels d'obtenir suffisamment d'information pour demander frauduleusement des prêts ou des cartes de crédit, produire une fausse déclaration d'impôt, transférer de l'argent illégalement, extorquer de l'argent à des victimes, avoir accès à des comptes en ligne ou concevoir des courriels d'hameçonnage persuasifs.[52] Les auteurs de cybermenaces parrainés par des États peuvent également se servir de ces données pour traquer des dissidents, des minorités ou des cibles d'espionnage dans leur pays ou à l'étranger.

Les cybercriminels qui s'adonnent au vol de données sont généralement des opportunistes motivés par l'appât du gain, alors que les auteurs de cybermenace parrainés par des États cherchent à obtenir de grandes quantités d'informations sensibles pour soutenir des objectifs stratégiques plus larges, comme la collecte de renseignements. Selon la présente évaluation, il est fort probable qu'au cours des deux prochaines années, les organisations canadiennes demeurent une cible de choix pour les cybercriminels et les auteurs de cybermenace parrainés par des États qui cherchent à obtenir de l'information nominative et d'autres données sensibles.

Les attaques par rançongiciel menées par les auteurs de cybermenace ont également gagné en sophistication. Ces derniers menacent les entreprises de divulguer l'information confidentielle de leurs clients à moins qu'une rançon soit versée, incitant ainsi les victimes à acquiescer à leurs demandes.[53] Toutefois, même si un paiement est effectué, les auteurs de cybermenace peuvent décider de supprimer, de modifier ou de divulguer l'information, ou encore utiliser les données volées lors d'une fraude ultérieure.

LA PLUS IMPORTANTE ATTEINTE À LA PROTECTION DES DONNÉES DE L'HISTOIRE CANADIENNE

En octobre 2019, une cyberattaque menée par des pirates informatiques a compromis les données de l'entreprise canadienne de laboratoire médical LifeLabs. Les renseignements personnels et confidentiels d'environ 15 millions de Canadiens ont été exposés, ce qui représente la fuite la plus massive de données personnelles jamais enregistrée au Canada. Les voleurs se sont emparés de résultats d'examen, de numéros de carte d'assurance maladie, de noms, de dates de naissance, d'adresses privées et d'adresses de courriel. Bien que LifeLabs ait payé la rançon pour récupérer les données, on ne peut garantir que les voleurs n'ont pas fait une copie des données pour profiter de ces renseignements ou les vendre à d'autres criminels.[54]

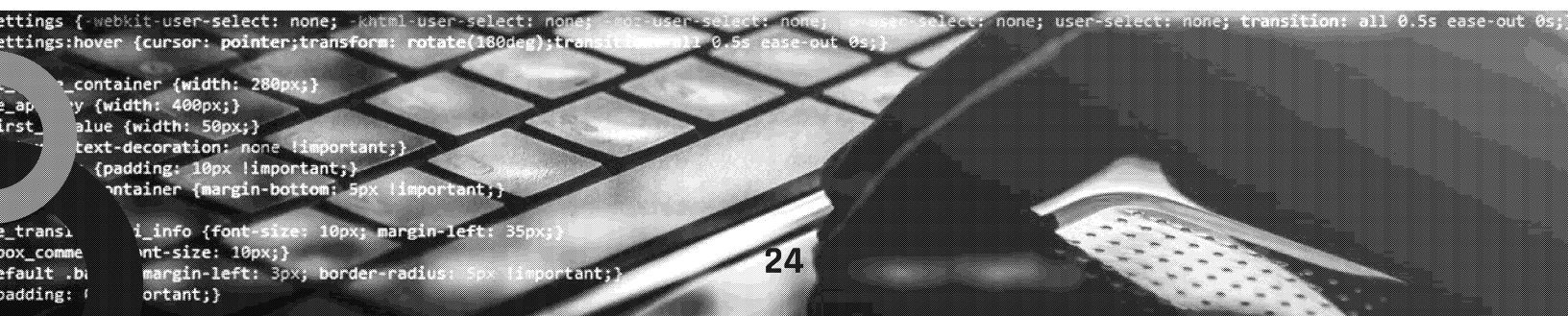
Exploitation des relations de confiance

Les prévisions faites dans l'évaluation de 2018 étaient justes, puisqu'on y indiquait que les auteurs de cybermenace continueraient probablement de tirer parti des relations de confiance entre les entreprises et leurs fournisseurs de services. Depuis 2018, les auteurs de cybermenace motivés par un intérêt financier ont nettement accentué le recours à certaines techniques de piratage psychologique pour cibler des organisations.[55] Une des techniques les plus répandues et parmi les plus coûteuses est appelée la « compromission de courriel d'affaires » ou la « fraude du faux PDG ». Ce type de fraude consiste à envoyer un courriel à un employé d'une entreprise pour le convaincre de transférer directement des fonds à l'expéditeur malveillant. Souvent, les auteurs de cybermenace se font passer pour des cadres supérieurs ou des tiers de confiance. En raison des incertitudes entourant la pandémie de COVID-19, les auteurs de cybermenace se servent de la situation pour cibler des victimes.

LA FRAUDE UTILISANT LA COMPROMISSION DE COURRIEL D'AFFAIRES NE TOUCHE PAS QUE LES ENTREPRISES

En mai 2019, une municipalité de l'Ontario a été victime d'une fraude par compromission de courriel d'affaires. L'auteur de menace s'est fait passer pour un fournisseur de confiance de la ville. Dans son faux courriel, il a demandé de changer l'information bancaire du fournisseur et une fois les changements effectués, 503 000 $ CA avaient été virés sur le nouveau compte appartenant au cybercriminel.[56]

Au cours des deux dernières années, les auteurs de cybermenace ont étendu leur utilisation de la compromission de courriel d'affaires pour cibler des organisations religieuses, à vocation éducative et à but non lucratif.[57] Les cybercriminels devraient en principe continuer à utiliser de plus en plus la compromission par courriel d'affaires en raison de la simplicité et de la rentabilité de cette technique.[58] Selon certaines évaluations, entre 2016 et 2019, on comptait plus de 1 200 cas reportés de fraude par compromission de courriel d'affaires au Canada, ce qui a entraîné des pertes de plus de 45 millions $ CA.[59] La perte moyenne liée à cette fraude et impliquant des virements bancaires se chiffre à environ 47 000 $ CA.[60]



Exploitation des systèmes de paiement

Les cybercriminels ciblent les données des cartes de paiement dans le but de voler les détails relatifs aux cartes de crédit ainsi que d'autres renseignements que les victimes entrent sur les sites de commerce électronique. C'est ce que l'on appelle le détournement de formulaire.[61] En 2018, environ 4 800 sites Web étaient victimes de détournement de formulaire chaque mois.[62] Plusieurs grands sites Web ont été compromis par cette technique, dont des compagnies aériennes, des vendeurs de billets et bien d'autres.[63] En 2019, plus de 200 librairies universitaires au Canada et aux États-Unis ont été touchées par le détournement de formulaire.[64] On considère que cette tendance devrait augmenter au cours des deux prochaines années, car de plus en plus de Canadiens ont recours au commerce électronique en raison notamment de la pandémie de COVID-19.[65]

Comme nous l'avons vu dans l'évaluation de 2018, les auteurs de cybermenace continuent également à cibler les systèmes de point de vente (PDV) qu'utilisent les boutiques traditionnelles. Ils le font en installant 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. À la fin de 2019, des cybercriminels ont ciblé les systèmes PDV de certaines stations-service en Amérique du Nord pour voler leurs données financières.[66] Les données stockées dans la bande magnétique des cartes de crédit et recueillies à partir de terminaux de PDV infectés sont vendues sur les marchés noirs de la cybercriminalité. Elles permettent aux criminels de recréer ou de cloner les cartes.

Compromission de la chaîne d'approvisionnement

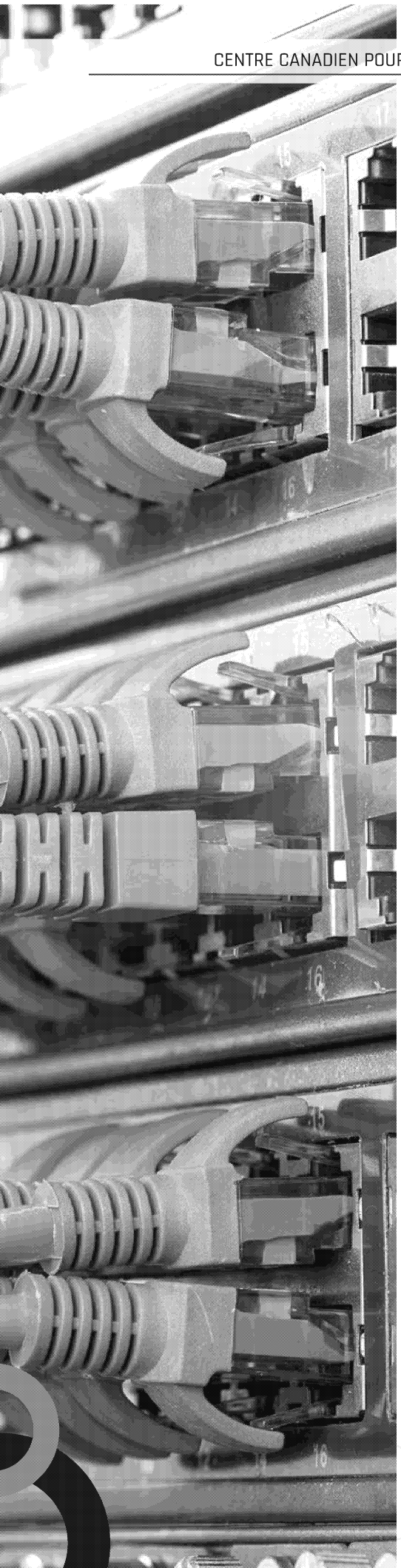
Plusieurs entreprises comptent sur une chaîne d'approvisionnement complexe – et souvent répartie mondialement – pour de nombreux aspects de leurs opérations, dont la fabrication de précurseurs, l'infrastructure de TI, le soutien informatique et les services financiers.[67] Les auteurs de cybermenace ciblent les réseaux de fournisseurs de confiance pour ensuite profiter de leurs accès et s'infiltrer dans les réseaux de leurs véritables cibles. 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. Les auteurs de cybermenace ciblent particulièrement les mises à jour et les mises à niveau parce qu'ils savent qu'elles seront téléchargées et installées des milliers, voire des millions de fois dans plusieurs entreprises, ce qui multiplie ainsi les occasions de fraude. Tel qu'il est illustré dans la figure 6, chaque maillon d'une chaîne d'approvisionnement mondiale peut représenter un risque pour la cybersécurité. Les prévisions faites dans l'évaluation de 2018 étaient justes, puisqu'on y indiquait que les auteurs de cybermenace continueraient de tirer profit des chaînes d'approvisionnement. On considère qu'il est probable que les auteurs de cybermenace continuent d'exploiter ces vulnérabilités au cours des deux prochaines années.

EXPLOITATION DES VULNÉRABILITÉS DE LA CHAÎNE D'APPROVISIONNEMENT

Depuis le début de la pandémie de COVID-19, les auteurs de cybermenace ont pu obtenir accès à un grand nombre d'hôpitaux à l'échelle mondiale, compromettant ainsi les réseaux informatiques et les composants des SCI ainsi que les produits d'imagerie utilisés dans le secteur de la santé.[68] En 2018, ces mêmes auteurs ont ciblé des organismes du domaine de la santé dans au moins 24 pays, dont le Canada, ainsi que des organismes dans d'autres domaines, comme le secteur manufacturier, l'informatique, la logistique et l'agriculture.[69]

On considère que ces auteurs malveillants ont probablement utilisé les mises à jour logicielles provenant de fournisseurs de confiance pour propager les maliciels et compromettre les données de leurs victimes.[70] Il est fort probable que les responsables de cette attaque aient été parrainés par un État et aient cherché à obtenir de l'information sensible ou exclusive pour faire avancer les priorités de leur pays.

Figure 6 : Vulnérabilités liées à la chaîne d'approvisionnement

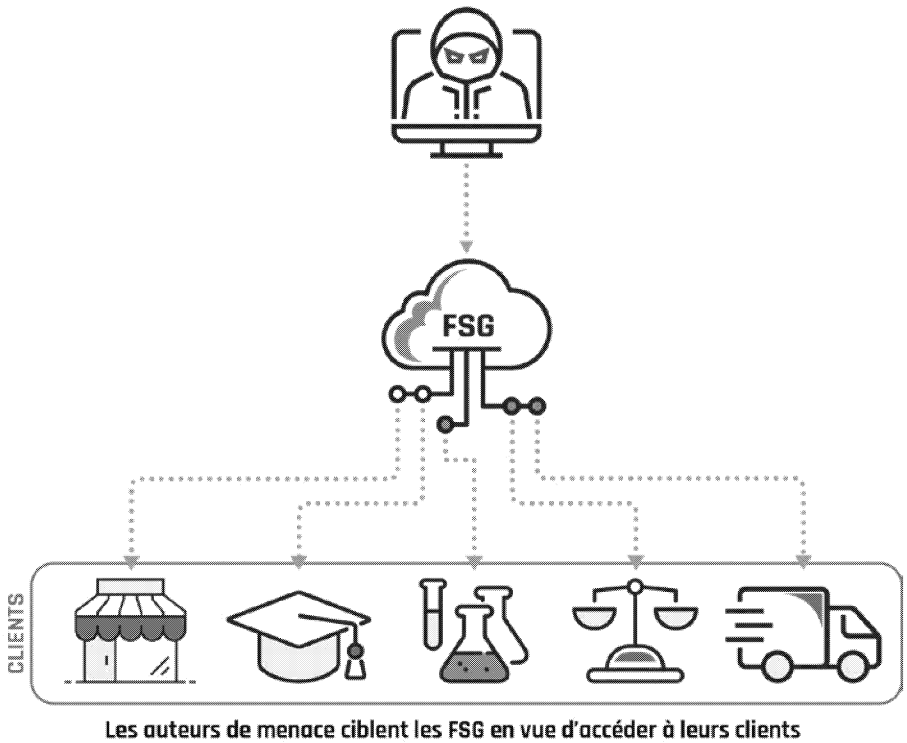


Exploitation de fournisseurs de services gérés

Un fournisseur de services gérés (FSG) est une entreprise utilisée par des organisations pour répondre à leurs besoins en TI et réduire les coûts associés au maintien de l'infrastructure et du personnel des TI en interne. Lorsqu'un réseau d'entreprise est bien protégé contre des attaques directes, les auteurs de cybermenace peuvent cibler les FSG pour avoir un accès indirect aux réseaux des clients. De plus, les auteurs de menace qui réussissent à compromettre un FSG peuvent atteindre un grand nombre de victimes, soit les clients de ce dernier.

Les prévisions faites dans l'évaluation de 2018 étaient justes, puisqu'on y indiquait que les FSG allaient demeurer des cibles intéressantes pour les auteurs de cybermenace. Tout au long de l'année 2019, des cybercriminels ont compromis des FSG afin de tirer parti des logiciels de gestion à distance des systèmes de TI et installer automatiquement et simultanément des rançongiciels sur plusieurs réseaux de clients.[71] On s'attend à ce qu'au cours des deux prochaines années les campagnes de rançongiciel ciblent de plus en plus les FSG dans le but de compromettre leurs clients et d'accroître la portée de ces campagnes.

Figure 7 : Exploitation de fournisseurs de services gérés (FSG)



Les auteurs de menace ciblent les FSG en vue d'accéder à leurs clients (notamment les entreprises, les établissements d'enseignement et les autres institutions) sans avoir à compromettre chaque client directement.

CONCLUSION

Au Canada, le contexte des cybermenaces est en pleine évolution et les auteurs malveillants continuent d'adapter leurs activités en conséquence. La présente évaluation des cybermenaces nationales visait à relever les tendances actuelles et à faire le point sur l'évolution des activités de cybermenace auxquelles font face les entreprises et les citoyens canadiens. L'adoption par les Canadiens de nouvelles technologies et de nouveaux dispositifs connectés à Internet donnera certainement lieu à de nouvelles menaces.

Selon les observations consignées dans l'évaluation de 2018, il est possible d'atténuer plusieurs des cybermenaces 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. Des investissements en cybersécurité permettront aux Canadiens de tirer avantage des nouvelles technologies tout en s'assurant qu'elles ne posent aucun risque sur le plan de la sécurité, de la protection de la vie privée, de la prospérité économique et de la sécurité nationale.

Le CCC s'est engagé à faire avancer la cybersécurité et à accroître la confiance des Canadiens dans les systèmes qu'ils utilisent au quotidien, en soutenant les réseaux des infrastructures essentielles et les autres systèmes qui sont importants pour le Canada.

Son approche collaborative en matière de sécurité permet de combiner l'expertise du gouvernement, du secteur privé et du milieu universitaire. En travaillant ensemble, nous rendrons le Canada plus fort et plus résilient face aux cybermenaces.

RESSOURCES UTILES

- Introduction à l'environnement de cybermenaces
- Pratiques exemplaires en cybersécurité
- Campagne Pensez cybersécurité
- Reconnaître les courriels malveillants
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage
- À bas l'arnaque – Protégez-vous contre la fraude
- Utilisation sûre des services bancaires en ligne
- Comment faire des achats en ligne en toute sécurité
- Utiliser son dispositif mobile en toute sécurité
- Application des mises à jour sur les dispositifs
- Pratiques exemplaires de création de phrases de passe et de mots de passe
- Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques
- Biométrie
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur
- Conseils de sécurité sur les gestionnaires de mots de passe
- Utiliser la technologie Bluetooth
- Intelligence artificielle
- Rapport conjoint sur les outils de piratage publiquement accessibles
- Protéger l'organisme contre les maliciels
- Rançongiciels : comment les prévenir et s'en remettre
- Protéger son organisation contre les attaques par déni de service
- Contrats avec des fournisseurs de services gérés : facteurs relatifs à la cybersécurité à considérer
- Utilisation de comptes personnels de médias sociaux au travail
- Utiliser un poste de travail virtuel à la maison et au bureau
- Les réseaux privés virtuels
- Conseils de cybersécurité pour le télétravail
- Conseils de sécurité pour les organisations dont les employés travaillent à distance
- Sécurité de l'Internet des objets pour les petites et moyennes organisations
- Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations
- Facteurs à considérer sur le plan de la recherche et du développement
- La cybersécurité pour les organismes de santé : se protéger contre des cyberattaques courantes
- La COVID-19 et les sites Web malveillants
- Conseils ciblés sur la cybersécurité applicables durant la pandémie de COVID-19 : Liste des publications par public cible
- Avis et conseils en matière de cybersécurité à l'intention des organismes de recherche et de développement durant la pandémie de la COVID-19
- Bouclier canadien – Le Centre pour la cybersécurité fournit des renseignements sur les menaces afin de protéger les Canadiens pendant la pandémie de COVID-19

NOTES DE FIN DE TEXTE

[1] *BlueLeaks Data Breach Involved 38 Canadian Police Forces*, CBC News, 22 septembre 2020. https://www.cbc.ca/news/canada/ottawa/blueleaks-published-thousands-of-documents-from-canadian-police-agencies-1.5734311.

[2] *IoT Makes Industrial Manufacturers "Smart"*, PwC, (consulté le 15 juillet 2020). https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov/manufacturing-iot-snapshot.html.

[3] *Dossier documentaire sur Internet au Canada 2019*, Autorité canadienne pour les enregistrements Internet, 2019. https://www.cira.ca/fr/resources/corporation/dossier-documentaire/canadas-internet-factbook-2019.
Enquête canadienne sur l'utilisation d'Internet, Statistique Canada, 10 mai 2010. https://www150.statcan.gc.ca/n1/daily-quotidien/100510/dq100510a-fra.htm.
Enquête canadienne sur l'utilisation d'Internet, Statistique Canada, 10 novembre 2013. https://www150.statcan.gc.ca/n1/daily-quotidien/131126/dq131126d-fra.htm.
Enquête canadienne sur l'utilisation d'Internet, Statistique Canada, 29 octobre 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm.

[4] David Vigneault, *Allocution de David Vigneault au Economic Club of Canada*, Gouvernement du Canada, 4 décembre 2018. https://www.canada.ca/fr/service-renseignement-securite/nouvelles/2018/12/allocution-pour-david-vigneault-au-economic-club-of-canada.html.

[5] *Un an après l'entrée en vigueur des déclarations obligatoires des atteintes à la protection des données : ce que nous avons appris et ce que les entreprises doivent savoir*, Commissariat à la protection de la vie privée du Canada, 31 octobre 2019. https://www.priv.gc.ca/fr/blogue/20191031/.

[6] *Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019*, Commissariat à la protection de la vie privée du Canada, 11 mars 2019. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/

[7] *Cyper Operations Tracker*, Council on Foreign Relations, (consulté le 15 septembre 2020). https://www.cfr.org/cyber-operations/.

[8] *Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023*, Markets and Markets, septembre 2018. https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html.

[9] *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware*, Département du Trésor des États-Unis, 5 décembre 2019. https://home.treasury.gov/news/press-releases/sm845; Tim Maurer, *Why the Russian Government Turns a Blind Eye to Cybercriminals*, Slate, 2 février 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html. *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, Département de la Justice des États-Unis, 16 septembre 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer; *Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East*, Département de la Justice des États-Unis, 16 septembre 2020. https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

[10] *Rapport Forum canadien sur la gouvernance de l'Internet 2019*, ACEI, 27 février 2019. https://canadianigf.ca/wp-content/uploads/2019/06/2019_CIGF_report_FR.pdf.

[11] Hascall Sharp et Oaf Kolkman. *Discussion Paper: An Analysis of the 'New IP' Proposal to the ITU-T*, Internet Society, 24 avril 2020. https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.

[12] Jon Fingas, *China, Huawei propose internet protocol with a built-in killswitch*, Engadget, 30 mars 2020. https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.

[13] Craig Silverman, *How to Spot a Deepfake Like the Barack Obama - Jordan Peele Video*, Buzzfeed News, 17 avril 2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed.

[14] *XR Belgium posts deepfake of Belgian premier linking COVID-19 with climate crisis*, The Brussels Times, 14 avril 2020. https://www.brusselstimes.com/all-news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/.

[15] *Enquête canadienne sur l'utilisation d'Internet*, Statistique Canada, 29 octobre 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm.

[16] *Dossier documentaire sur Internet au Canada*, Autorité canadienne pour les enregistrements Internet, 2019. https://www.cira.ca/fr/resources/corporation/dossier-documentaire/canadas-internet-factbook-2019.

[17] *The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.* International Data Corporation, 18 juin 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[18] Sawyer Bogdan, *Canadians have lost $43 Million to Cybercrime in 2019: OPP*, Global News, 24 octobre 2019. https://globalnews.ca/news/6077016/canadians-lost-43-million-cybercrime-2019/.

[19] *Fraudes par moyen utilisé*, Centre antifraude du Canada, 13 février 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-fra.htm

[20] *Fraudes par moyen utilisé*, Centre antifraude du Canada, 13 février 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-fra.htm

[21] John MacFarlane, *4.2 million Desjardins members affected by data breach, credit union now says*, CBC News, 1er novembre 2019. https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216.

[22] Aidan Wallace, *Major Data Breaches in 2019*, Toronto Sun, 1er janvier 2020. https://torontosun.com/news/world/major-data-breaches-in-2019.

[23] Ken Hsu, Durgesh Sangvikar, Zhibin Zhang et Chris Navarrete, *Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices*, Palo Alto Networks: Unit 42, 24 juin 2020. https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/.

[24] *LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario*, CBC News, 17 décembre 2019. https://www.cbc.ca/news/canada/british-columbia/lifelabs-cyberattack-15-million-1.5399577.

[25] Maham Abedi, *Capital One data breach: here's what Canadians need to know*, Global News, 30 juillet 2019. https://globalnews.ca/news/5702026/capital-one-data-breach-what-to-know/.

[26] Josh Fruhlinger, *Marriott data breach FAQ: How did it happen and what was the impact?* CSO Online, 12 février 2020. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.

[27] Roberto Rocha et Jeff Yates, *Twitter Trolls Stoked Debates About Immigrants and Pipelines in Canada, Data Shows*, CBC News, 12 février 2019. https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

[28] Reis Thebault, *A woman's stalker used an app that allowed him to stop, start, and track her car*, The Washington Post, 6 novembre 2019. https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/.

[29] *Tech Abuse and Empowerment Service*. Refuge, (consulté le 15 juillet 2020). https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/.

[30] *Vulnérabilités de cybersécurité associées à certains dispositifs médicaux dotés de puces Bluetooth Low Energy*, Santé Canada, 11 mars 2020. https://canadiensensante.gc.ca/recall-alert-rappel-avis/hc-sc/2020/72555a-fra.php.

[31] *Infrastructures essentielles du Canada*, Sécurité publique Canada, 19 mai 2020. https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-fr.aspx.

[32] Andy Greenberg, *The Highly Dangerous 'Triton' Hackers Have Probed the US Grid*, Wired, 14 juin 2019. https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

[33] Andy Greenberg, *A Notorious Iranian Hacking Crew is Targeting Industrial Control Systems*, Wired, 20 novembre 2019. https://www.wired.com/story/iran-apt33-industrial-control-systems/.

[34] *Top 2019 Cyber Attacks on ICS*, Waterfall Security, 19 décembre 2019. https://waterfall-security.com/top-2019-attacks-on-ics/.

[35] Joe Tidy, *How a Ransomware Attack Cost One Firm £45m*, BBC News, 25 juin 2019. https://www.bbc.com/news/business-48661152.

[36] Andy Greenberg, *Mysterious New Ransomware Targets Industrial Control Systems*, Wired, 3 février 2020. https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; Nathan Brubaker, et. al. *Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families*, FireEye Threat Research, 15 juillet 2020. https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html.

[37] *EKANS Ransomware and ICS Operations*, Dragos, 3 février 2020. https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[38] Ben Dooley et Hsako Ueno, *Honda Hackers May Have Used Tools Favored by Countries*, New York Times, 12 juin 2020. https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html.

[39] James Lewis, *Economic Impact of Cybercrime—No Slowing Down*, Center for Strategic and International Studies and McAfee, février 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

[40] *2019 Internet Security Threat Report*, Symantec, 26 juin 2019. https://www.bankinfosecurity.com/whitepapers/2019-internet-security-threat-report-w-5357.

[41] *Q1 2020 Ransomeware Marketplace Report*, Coveware, 29 avril 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[42] Ryan Flanagan, *Canadian Insurance Company Lost Nearly US$1M in Ransomware Attack*, CTV News, 30 janvier 2020. https://www.ctvnews.ca/sci-tech/canadian-insurance-company-lost-nearly-us-1m-in-ransomware-attack-1.4790490.

[43] *Ransomware Payments up 33% as Maze and Sodinokibi Proliferate in Q1 2020*, Coveware, 29 avril 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

[44] Catharine Tunney, *Ransomware Attack on Construction Company Raises Questions About Federal Contracts*, CBC News, 26 janvier 2020. https://www.cbc.ca/news/politics/ransowmare-bird-construction-1.5434308; *Time's Up for Agromart Group and their Data Got Leaked by REvil Ransomware Operators*, Cyble, Inc., 2 juin 2020. https://cybleinc.com/2020/06/02/times-up-for-agromart-group-and-their-data-got-leaked-by-revil-ransomware-operators/.

[45] David Burke, *Hospitals 'Overwhelmed' by Cyberattacks Fuelled by Booming Black Market*, CBC, 2 juin 2020. https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422.

[46] *Alerte : Cybermenaces pesant sur les organismes de santé canadiens*, Centre canadien pour la cybersécurité, 31 mars 2020. https://cyber.gc.ca/fr/avis/cybermenaces-pesant-sur-les-organismes-de-sante-canadiens.

[47] Catharine Tunney, *CSIS chief calls commercial espionage 'the greatest threat to our prosperity'*, CBC News, 4 décembre 2018. https://www.cbc.ca/news/politics/david-vigneault-csis-economy-1.4932407/.

[48] *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, Département de la Justice des États-Unis, 20 décembre 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[49] Dustin Volz, *Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets*, The Wall Street Journal, 5 mars 2019. https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800.

[50] *Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les activités de cybermenaces*, Centre canadien pour la cybersécurité, 27 avril 2020. https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-incidence-de-la-covid-19-sur-les-activites-de.

[51] *Advisory: APT29 targets COVID-19 vaccine development*, National Cyber Security Centre, 16 juillet 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

[52] *What do Cybercriminals do with the Data They Steal?* Sysnet Global Solutions, (consulté le 10 juillet 2020). https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/.

[53] Scott Ikeda, *Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit*, CPO Magazine, 8 janvier 2020. https://www.cpomagazine.com/cyber-security/lifelabs-data-breach-the-largest-ever-in-canada-may-cost-the-company-over-1-billion-in-class-action-lawsuit/.

[54] Danny Palmer, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, ZDNet, 14 juillet 2020. https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[55] *2020 Data Breach Investigations Report*, Verizon, 2 juin 2020. https://enterprise.verizon.com/resources/reports/dbir/.

[56] Bruce Sussman, *BEC Scam Costs Canadian City $500k*, SecureWorld, 18 juin 2019. https://www.secureworldexpo.com/industry-news/canada-bec-scam-example.

[57] *The Sprawling Reach of Complex Threats: 2019 Annual Security Roundup*, Trend Micro, 25 février 2020. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats.

[58] *2019 Internet Crime Report*, Federal Bureau of Investigation, 11 février 2020. https://pdf.ic3.gov/2019_IC3Report.pdf.

[59] C. Steven Baker, *Is That Email Really From "The Boss"? The Explosion of Business Email Compromise (BEC) Scams*, The Better Business Bureau, septembre 2019. https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-explosion-of-bec-scams.pdf.

[60] *Behind the 'From' Lines: Email Fraud on a Global Scale*, Agari Cyber Intelligence Division, (consulté le 15 août 2020). https://www.agari.com/insights/whitepapers/behind-the-from-lines/.

[61] *2019 Internet Security Threat Report*, Symantec, 26 juin 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[62] *2019 Internet Security Threat Report*, Symantec, 26 juin 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[63] Jin Chen, Tao Yan, Taojie Wang et Zhanglin He. *Anatomy of FormJacking Attacks*, Palo Alto Networks, Unit 42, 27 avril 2020. https://unit42.paloaltonetworks.com/anatomy-of-formjacking-attacks/.

[64] Joseph Chen, *Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada*, Trend Micro, 3 mai 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/.

[65] Aanand Krishnan, *Web scammers are using the COVID-19 crisis to attack your customers with Magecart and other client-side exploits, Security Boulevard*, 9 juin 2020. https://securityboulevard.com/2020/06/web-scammers-are-using-the-covid-19-crisis-to-attack-your-customers-with-magecart-and-other-client-side-exploits/.

[66] Merna Emara, *Cybercrime Attacks on the Rise at North American Gas Stations, Warns Card Giant Visa*, National Post, 17 décembre 2019. https://nationalpost.com/news/world/cybercrime-attacks-on-the-rise-at-north-american-gas-stations-warns-card-giant-visa.

[67] 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 « Supply Chain Risk Management Practices for Federal Information Systems and Organizations. » National Institute for Standards and Technology, avril 2015. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

[68] Catalin Cimpanu, *FBI re-sends alert about supply chain attacks for the third time in three months*. ZDNet, 31 mars 2020. https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/.

[69] Howard Solomon, *Canadian Organizations Among Victims of Global Attack on Healthcare-related Industries*, IT World, 24 avril 2018. https://www.itworldcanada.com/article/canadian-organizations-among-victims-of-global-attack-on-healthcare-related-industries/404475.

[70] Johannes B. Ullrich, *Kwampirs Targeted Attacks Involving Healthcare Sector*, SANS Internet Storm Center, 31 mars 2020. https://isc.sans.edu/forums/diary/Kwampirs+Targeted+Attacks+Involving+Healthcare+Sector/25968/?utm_medium=Social&utm_source=Twitter&utm_campaign=SANS+Central.

[71] Catalin Cimpanu, *GandCrab Ransomware Gang Infects Customers of Remote IT Support Firms*, ZDNet, 14 février 2019. https://www.zdnet.com/article/gandcrab-ransomware-gang-infects-customers-of-remote-it-support-firms/; Catalin Cimpanu, *Ransomware Gang Hacks MSPs to Deploy Ransomware on Customer Systems*, ZDNet, 20 juin 2019. https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/; Catalin Cimpanu, *Ransomware Hits Hundreds of Dentist Offices in the US*, ZDNet, 29 août 2019. https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.