EN BREF

Le point sur la sécurité de la recherche

Mai 2021

Le point sur la sécurité de la recherche est un regroupement de sources ouvertes non classifiées, produit par l'équipe Science en sécurité de Sécurité publique Canada, sur des questions jugées pertinentes pour les intérêts généraux du Canada en matière de sécurité de la recherche. Elle a pour but de fournir des renseignements spécialisés sur la sécurité de la recherche au milieu canadien de la recherche. Chaque mise à jour pourrait comprendre un tour d'horizon des développements récents et pertinents, de l'information sur un sujet particulier lié à la sécurité de la recherche, des résumés d'études de cas pertinentes, des statistiques liées à la cybersécurité, des tendances et des conseils.

Qu'est-ce que la sécurité de la recherche?

De manière générale, la sécurité de la recherche fait référence aux mesures protégeant les connaissances, les technologies et les données qui pourraient contribuer à la promotion des intérêts géopolitiques, économiques et sécuritaires d'un auteur de menaces étranger au détriment des intérêts du Canada. Les actifs ciblés peuvent varier des applications dans les programmes d'armes de destruction massive (c.-à-d. chimiques, biologiques, radiologiques et nucléaires) aux technologies à double usage (c.-à-d. technologies avec des applications à la fois civiles et militaires), telles que l'intelligence artificielle, l'informatique quantique, la biotechnologie et les nanotechnologies, à la propriété intellectuelle et aux informations confidentielles utilisées pour la recherche.

Développements notables en matière de sécurité de la recherche

Avril 2020 – Dans le contexte du développement du vaccin contre la COVID-19, le Service canadien du renseignement de sécurité (SCRS) a commencé à présenter des séances d'information sur les menaces au secteur biopharmaceutique, y compris les universités canadiennes.

14 mai 2020 – Le CST et le SCRS ont publié une déclaration conjointe avertissant la communauté canadienne de la recherche que les données et les technologies liées à la recherche sur les pandémies sont devenues des cibles attrayantes pour des acteurs parrainés par des États.

14 septembre 2020 – Les ministres de l'Innovation, des Sciences et du Développement économique, de la Sécurité publique et de la Santé ont publié un énoncé de politique encourageant tous les membres du milieu de la recherche au Canada à prendre des précautions supplémentaires pour protéger toutes les activités de recherche, de technologie et de développement liées aux vaccins et produits thérapeutiques contre la COVID-19.

14 septembre 2020 – Le gouvernement du Canada a lancé le portail Protégez votre recherche – élaboré par un groupe de travail mixte du gouvernement du Canada et des universités – afin de fournir aux chercheurs des conseils, des renseignements et des outils pour les aider à protéger leurs recherches et leur propriété intellectuelle.

17 septembre 2020 – Le Centre canadien pour la cybersécurité a publié un document sur les facteurs à considérer en matière de sécurité sur le plan de la recherche et du développement. On encourage les organismes de recherche à examiner la publication pour obtenir de l'information sur la façon de protéger leur environnement et leurs données de recherche, de comprendre les menaces courantes à la cybersécurité et de mettre en œuvre certaines mesures de sécurité de base.

16 novembre 2020 – Le Centre canadien pour la cybersécurité a publié l'Évaluation des cybermenaces nationales pour 2020.

ISBN : PS9-20/2021E-PDF 978-0-660-37941-8

15 janvier 2021 – Le gouvernement du Canada a confié au ministre de la Sécurité publique le mandat de travailler en étroite collaboration avec le milieu canadien de la recherche et le ministre de l'Innovation, des Sciences et de l'Industrie afin de continuer à protéger les recherches de calibre mondial du Canada.

Le 9 février 2021 – Dans son allocution devant le Centre pour l'innovation dans la gouvernance internationale, le directeur du SCRS a souligné que des entreprises canadiennes de presque tous les secteurs de l'économie ont été ciblées par des acteurs étrangers hostiles. Comme il l'a fait remarquer, « aujourd'hui, (nos adversaires) concentrent leurs efforts sur les propriétés intellectuelles et les recherches avancées effectuées au moyen de systèmes d'ordinateurs de jeunes entreprises, de laboratoires universitaires et de salles de conférences ».

Le 24 mars 2021 – Le ministre de l'Innovation, des Sciences et de l'Industrie, le ministre de la Sécurité publique et la ministre de la Santé ont publié un énoncé de politique dans lequel ils s'engageaient à soutenir un environnement de recherche ouvert et collaboratif tout en protégeant l'intégrité des activités de recherche, la sécurité nationale et la compétitivité et la prospérité économiques à long terme du Canada.

Efforts actuels portant sur la sécurité de la recherche

L'objectif de tous les efforts de sécurité de la recherche est de veiller à ce que la recherche canadienne durement obtenue ne soit pas utilisée à mauvais escient ou exploitée, et à ce que le milieu de la recherche au Canada profite au maximum de son travail. Ces enjeux sont expliqués dans le document *Sensibilisation de la communauté universitaire à la sécurité* publié par Sécurité publique Canada en 2019. Vous trouverez ci-dessous un bref aperçu de certains des efforts et des considérations actuels en matière de sécurité de la recherche (diverses initiatives, politiques, programmes, etc.) qui sont mis en œuvre au Canada et par un certain nombre de nos partenaires.

Australie

En novembre 2019, l'Australie a publié le document *Guidelines to counter foreign interference in the Australian university sector* (en anglais) (lignes directrices pour contrer l'ingérence étrangère dans le secteur universitaire australien). Ces lignes directrices ont été élaborées pour le secteur universitaire et en partenariat avec lui afin de renforcer la résilience face aux risques d'ingérence étrangère. Elles s'appuient sur les politiques de gestion des risques et les pratiques de sécurité déjà mises en œuvre par les universités australiennes et aident les décideurs à évaluer les risques liés à l'ingérence étrangère, tout en appuyant un environnement de confiance, afin que les universités australiennes puissent continuer de produire des recherches de calibre mondial.

Canada

Depuis 2016, le Canada mène des activités de sensibilisation portant sur les questions de sécurité liées à la recherche par l'entremise de Science en sécurité. Science en sécurité fait présentement l'objet d'un élargissement afin de fournir des ressources supplémentaires aux secteurs universitaire, de la recherche et du développement au Canada, ainsi que des programmes visant à améliorer la capacité des établissements à régler les problèmes de sécurité de la recherche. De plus, en septembre 2020, le Canada a lancé le portail Protégez votre recherche afin de diffuser des conseils et des outils à l'intention des chercheurs et des administrateurs de recherche.

Nouvelle-Zélande

Le gouvernement de la Nouvelle-Zélande collabore avec *Universities New Zealand* pour sensibiliser les gens aux questions d'intégrité et de sécurité de la recherche et pour élaborer des lignes directrices communes à l'intention du milieu universitaire. Cette collaboration s'appuiera sur les politiques existantes en matière d'intégrité et d'éthique de la recherche (en anglais) de la Société royale de la Nouvelle-Zélande et des universités.

États-Unis

Depuis le milieu de 2018, les États-Unis ont adopté une série de règles, de politiques et de règlements nouveaux et révisés pour répondre aux préoccupations concernant l'ingérence étrangère dans la recherche et le vol de capital intellectuel. Divers départements et organismes ont introduit de nouvelles mesures pour gérer les risques pour l'intégrité des activités de recherche, comme la création à la Maison-Blanche du *Joint Committee on Research Environment,* soit le comité mixte sur l'environnement de la recherche, par le *Office of Science and Technology Policy* (bureau de la politique scientifique et technologique).

Royaume-Uni

En 2019, le *Centre for the Protection of National Infrastructure* du Royaume-Uni a publié son document « Trusted Research Guidance for Academia » (en anglais), qui fournit des recommandations sur la façon dont la communauté de recherche du Royaume-Uni peut protéger ses données personnelles et liées à la recherche contre l'ingérence et le vol par des étrangers.

Sa Majesté la Reine du chef du Canada, représentée par le ministre de la Sécurité publique et de la Protection civile, 2021
ISBN : PS9-20/2021E-PDF 978-0-660-37941-8

Aperçu de la cybersécurité

Les établissements de recherche canadiens comptent beaucoup sur les cyberinfrastructures, qu'elles soient institutionnelles ou nationales, pour mener des recherches, stocker des données et mener des expériences. Cette dépendance, surtout pendant la pandémie de la COVID-19, a accru la vulnérabilité des institutions canadiennes, qui courent un plus grand risque de perdre de précieuses recherches à la suite de cyberattaques ou de tentatives d'infiltration des cyberinfrastructures canadiennes par des auteurs de menaces. Vous pouvez vous aider vous-même et aider votre établissement en tenant compte des conseils suivants :
Modes d'attaque courants : les auteurs de cybermenaces peuvent utiliser différentes méthodes pour modifier ou voler vos données de recherche et votre propriété intellectuelle. L'hameçonnage (*figure 1*) peut rendre vos systèmes vulnérables aux auteurs de menaces qui déploient des rançongiciels sur vos appareils/réseaux. Pour prévenir une attaque d'hameçonnage, surveillez les éléments de communication malveillante (*figure 2*).

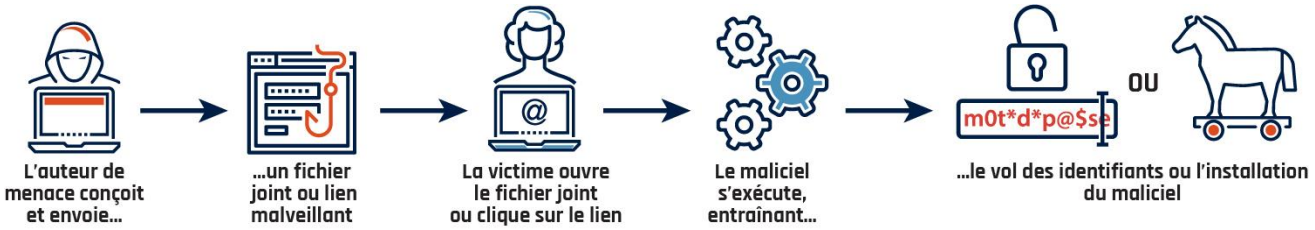

Figure 1 : Hameçonnage et harponnage (Référence : Annexe A : Les outils de l'auteur de cybermenaces)

Figure 2 : Les éléments de la communication malveillante (Référence : Évaluation des cybermenaces nationales 2020)

Le rançongiciel (*figure 3*) est un type de maliciel qui rendra vos données inaccessibles (p. ex., en verrouillant les systèmes et en chiffrant tous les fichiers) jusqu'à ce qu'une rançon soit payée. *Pour en savoir plus, consultez ITSAP.00.099 Rançongiciels : comment les prévenir et s'en remettre.*

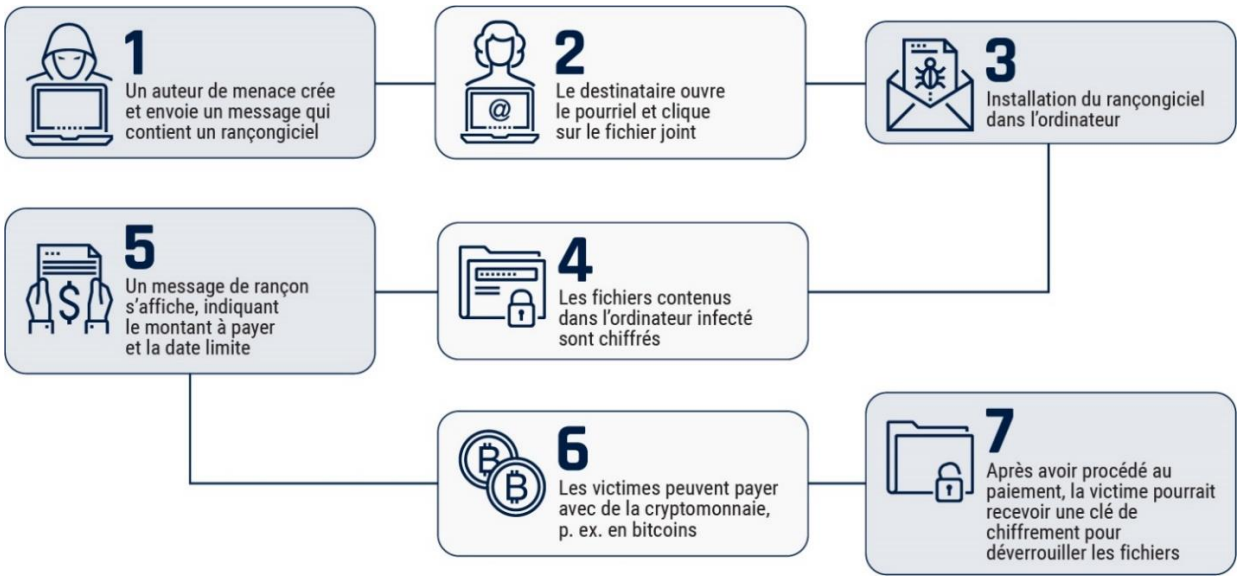

Figure 3 : Rançongiciel (Référence : Annexe A : Les outils de l'auteur de cybermenaces)

Sa Majesté la Reine du chef du Canada, représentée par le ministre de la Sécurité publique et de la Protection civile, 2021
ISBN : PS9-20/2021E-PDF 978-0-660-37941-8

Ne soyez pas le maillon faible! *« Les télétravailleurs sont de plus en plus ciblés par les auteurs de menaces et les cybercriminels parrainés par des États. Les auteurs de cybermenaces tentent d'identifier les personnes qui travaillent à la maison dans des domaines d'intérêt stratégique et exploitent les technologies déployées à l'appui d'une main-d'œuvre en télétravail, comme les réseaux privés virtuels (RPV) ou les plateformes de vidéoconférence. »*

Cinq conseils pour améliorer votre cybersécurité à la maison :

1. Utilisez un mot de passe complexe et unique. Ne le communiquez à personne d'autre.
2. Assurez la mise à niveau régulière de vos appareils.
3. Installez des outils de sécurité antivirus.
4. Soyez aux aguets des courriels d'hameçonnage.
5. Utilisez une méthode hors ligne pour sauvegarder vos données.

(Référence : Évaluation des cybermenaces nationales 2020)

Vous voulez en savoir plus?

Avez-vous des questions ou avez-vous besoin d'aide? Vous voulez rester au courant et en savoir plus sur tous les aspects de la sécurité de la recherche? Veuillez nous envoyer un courriel à safeguardingscience-scienceensecurite@ps-sp.gc.ca ou visitez notre page Web Science en sécurité.

Sécurité publique Canada vise à publier continuellement de l'information utile à la communauté de recherche canadienne sur des questions pertinentes reliées à la sécurité de la recherche. N'hésitez pas à nous faire part de vos commentaires. Y a-t-il des produits, des outils ou des renseignements particuliers que vous aimeriez recevoir (c.-à-d. sur les risques et les menaces émergents, les études de cas de recherche sur la sécurité, les statistiques, les conseils sur les principaux enjeux, les pratiques exemplaires en matière de sécurité, etc.)? Veuillez faire part de vos suggestions par l'entremise du courriel de Science en sécurité ci-dessus.

21 %

Pourcentage des organisations canadiennes interrogées qui ont subi plus de 10 attaques en 2019.

(Référence : Rapport sur la cybersécurité de 2020 de l'ACEI)

80 %

Pourcentage d'organisations canadiennes interrogées qui ont subi une cyberattaque en 2019.

(Référence : Rapport sur la cybersécurité de 2020 de l'ACEI)

Comment signaler un incident

GRC – Réseau info-sécurité nationale (RISN)
Pour signaler la présence d'inconnus ou des incidents ou activités informatiques suspects.

N° de téléphone : 1-800-420-5805 Courriel : NSIN_RISN@rcmp-grc.gc.ca

Service canadien du renseignement de sécurité (SCRS)
Pour signaler des menaces à la sécurité nationale ou des activités suspectes potentielles non urgentes.

N° de téléphone : 1-800-267-7685 Site Web : Signaler des informations relatives à la sécurité nationale

Centre canadien pour la cybersécurité (CCC)
Le Centre de contact du CCC est le guichet unique pour les questions sur la cybersécurité.

N° de téléphone : 1-833-CYBER-88 Courriel : contact@cyber.gc.ca

Veuillez noter qu'il n'y a pas de calendrier de publication prévu pour Le point sur la sécurité de la recherche. Sécurité publique Canada fournira de l'information à notre public à mesure qu'elle se présente ou devient disponible.

ISBN : PS9-20/2021E-PDF 978-0-660-37941-8