Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

La cybermenace ciblant des laboratoires de recherche

Canada

À propos du présent document

Auditoire

Le rapport fait partie d'une série d'évaluations des cybermenaces portant sur des recommandations relatives aux cybermenaces susceptibles de cibler les infrastructures essentielles du Canada. Il s'adresse aux dirigeantes et dirigeants des secteurs des sciences de la vie et de la biofabrication, aux professionnelles et professionnels de la cybersécurité devant protéger l'infrastructure de laboratoire et aux lectrices et lecteurs non spécialisés qui s'intéressent à la cybersécurité des infrastructures essentielles. Pour obtenir des conseils sur des mesures techniques pour atténuer ces menaces, consultez les conseils du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) ou communiquez avec le Centre pour la cybersécurité.

La mention TLP:CLEAR doit être utilisée conformément aux règles et aux procédures applicables à la diffusion publique lorsque le risque prévisible d'une utilisation abusive est faible ou négligeable. Tout en étant soumise aux règles standard de droit d'auteur, l'information TLP:CLEAR peut être divulguée sans aucune restriction. Pour en savoir plus, consultez le lien suivant : Traffic Light Protocol.

Coordonnées

Prière de transmettre toute question ou tout enjeu relatif au présent document au Centre canadien pour la cybersécurité (CCC) à contact@cyber.gc.ca.

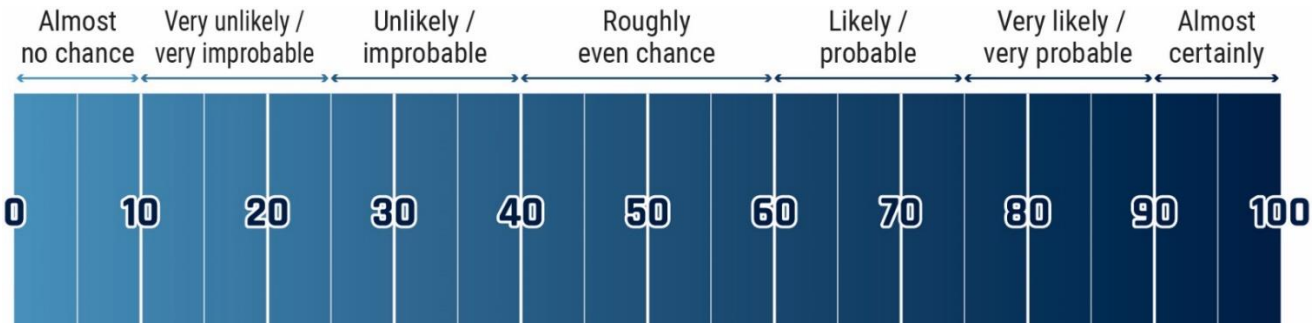
Méthodologie et fondement de l'évaluation

Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise en matière de cybersécurité du Centre pour la cybersécurité. Le rôle que joue le Centre pour la cybersécurité 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. Dans le cadre du volet du mandat du Centre de la sécurité des télécommunications touchant le renseignement étranger, le Centre pour la cybersécurité tire parti d'information précieuse sur les habitudes des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité 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 avis.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. Le Centre pour la cybersécurité utilise des formulations telles que « nous évaluons que » ou « nous jugeons que » pour présenter une évaluation analytique. Les qualificatifs tels que « possiblement », « probable » et « très probable » servent à évoquer une probabilité.

Les évaluations et analyses énoncées dans le présent document sont fondées sur des renseignements disponibles en date du 30 novembre 2023.

Lexique des estimations



Principaux avis

- Nous évaluons que les cybercriminelles et cybercriminels motivés par le gain financier représentent la cybermenace la plus susceptible de toucher les réseaux et les dispositifs de laboratoires par déploiement d'un rançongiciel et par extorsion ou par le vol et la vente de renseignements personnels ou exclusifs.
- Selon nos observations, des auteures et auteurs de cybermenace parrainés par des États devraient continuer à cibler des laboratoires canadiens pour soutenir leurs capacités nationales dans le domaine biopharmaceutique et celui de la biofabrication en se livrant à l'espionnage. En outre, nous évaluons que les auteures et auteurs de menace de la République populaire de Chine (RPC) représentent presque assurément la forme la plus courante de menace parrainée par des États visant les laboratoires du Canada.
- Nous évaluons que, pour mener des activités d'espionnage ou perturbatrices, des auteures et auteurs de menace parrainés par un État cibleront assurément des laboratoires axés sur la recherche liée aux exigences en matière de renseignement essentiel d'un État étranger ou à une menace existentielle perçue.
- Selon nos observations, des auteures et auteurs de menace parrainés par des États auront assurément recours à des campagnes de désinformation pour cibler des laboratoires axés sur la recherche dans le but de potentiellement causer une atteinte à la réputation d'États étrangers. Ces campagnes peuvent impliquer la compromission et l'exfiltration de réseaux de laboratoire, la modification et la diffusion de renseignements sensibles.
- Nous évaluons qu'il est possible que les laboratoires soient touchés par une cybermenace peu sophistiquée, comme des attaques par déni de service distribué (DDoS pour *Distributed denial-of-service*) menées par des hacktivistes qui sont peu susceptibles de perturber les opérations en laboratoire.

Introduction

La recherche médicale et sur les sciences de la vie est une partie importante de l'économie canadienne, et elle apporte une contribution essentielle à la sécurité nationale et à la sécurité sanitaire du Canada. En plus d'une contribution de 89,6 milliards de dollars au PIB du Canada en 2022, cette recherche permet de développer de nouveaux vaccins et de produire des substances thérapeutiques pour aider le Canada à mieux faire face aux crises sanitaires. Les chercheuses et chercheurs canadiens sont reconnus à l'échelle internationale pour la découverte de l'insuline, leur participation au développement d'un vaccin contre le virus d'Ebola, et pour avoir réussi à isoler et à mettre en culture le virus responsable de la COVID-19, ouvrant la voie à d'autres recherches sur les vaccins.[1]

Des laboratoires canadiens de recherche biologique, c'est-à-dire des laboratoires qui travaillent avec des agents pathogènes humains et animaux et des toxines, ont apporté énormément de contributions au Canada et au milieu mondial de la recherche. L'importance de la recherche canadienne en laboratoire est telle que les laboratoires deviennent des cibles intéressantes pour les auteures et auteurs de cybermenace. Tout au long de la pandémie de COVID-19, le Centre pour la cybersécurité a observé un grand volume d'activités de cybermenace menées par des auteures et auteurs de menace et des cybercriminelles et cybercriminels contre des organismes de santé et d'autres organismes au sein de la chaîne d'approvisionnement des vaccins, notamment des laboratoires.[2]

Après la pandémie de COVID-19, des laboratoires, des universités et des centres de recherche ont continué d'être ciblés par des auteures et auteurs de cybermenace parrainés par des États à des fins d'espionnage et d'être victimes de cybercriminelles et criminels cherchant à obtenir un gain financier. Au même moment, les systèmes sur lesquels s'appuient les laboratoires pour étudier les agents pathogènes et toxines considérés comme dangereux sont de plus en plus transformés et intégrés sur le plan numérique avec la technologie de l'information, ce qui les rend encore plus vulnérables aux cyberinterférence.[3]

Les activités de cybermenace ciblant les laboratoires canadiens mettent en péril l'avantage du Canada sur le plan de la recherche, ce qui comprend le vol de renseignements exclusifs ou des perturbations dans le cadre des opérations en laboratoire. Les perturbations peuvent entraîner des pertes de renseignements de recherche, des bris de confinement et l'exposition du personnel de laboratoire ou de collectivités en raison de matériel biologique dangereux.

Exposition des laboratoires aux cybermenaces

La recherche médicale et sur les sciences de la vie se fait dans des laboratoires exploités partout au Canada par des sociétés d'État et des sociétés privées. Ces laboratoires produisent, stockent, manipulent et étudient des agents pathogènes et des toxines, notamment ceux qui constituent un risque important pour la santé des chercheuses et chercheurs, et de l'ensemble de la collectivité s'ils ne sont pas correctement confinés. Les laboratoires s'appuient sur des mesures de confinement procédurales et physiques pour accomplir leur travail de façon sécuritaire. Ces mesures sont d'ailleurs mises en œuvre conformément au niveau de confinement (NC). Les laboratoires autorisés à travailler avec des agents biologiques à cote de sécurité élevée (ABCSE) sont assujettis à des contrôles additionnels de l'accès et à un filtrage de sécurité pour le personnel de laboratoire.

Les équipements et les systèmes de laboratoire deviennent de plus en plus complexes et interconnectés. En plus de l'introduction de systèmes de gestion d'immeubles connectés pour les dispositifs électriques, de circulation d'air et de contrôle de l'accès, les dispositifs de recherche en laboratoire et les systèmes de confinement vivent une transformation numérique. Le fait d'utiliser ces systèmes connectés procure aux opératrices et opérateurs de laboratoire des avantages, mais cela crée également un risque de voir des auteures et auteurs de cybermenace compromettre ces systèmes et d'en perturber le fonctionnement.

Principaux termes	
Niveau de confinement (NC)	Le niveau de confinement correspond aux exigences minimales liées aux mesures de protection matérielle dont a besoin un laboratoire pour la manipulation sécuritaire de matières biologiques potentiellement dangereuses. Il existe quatre niveaux de confinement (NC1 à NC4) allant du niveau de confinement de base pour les laboratoires conçus pour travailler avec des matières biologiques jusqu'au niveau de confinement le plus élevé pour les installations sophistiquées qui manipulent des agents pathogènes appartenant au groupe de risque élevé.[4]
Agents biologiques à cote de sécurité élevée (ABCSE)	Les ABCSE représentent un sous-ensemble d'agents pathogènes et de toxines qui ont augmenté la possibilité d'un double usage; c'est-à-dire qu'ils peuvent servir autant pour des applications scientifiques légitimes que pour une utilisation inappropriée comme armes biologiques.

Dispositifs de recherche en laboratoire

Les chercheuses et chercheurs comptent sur de nombreux équipements de recherche pour manipuler et étudier les agents pathogènes et les toxines, y compris des appareils de mappage génomique, des microscopes électroniques, des centrifugeuses, entre autres. Ces équipements sont de plus en plus connectés et mis en réseau. Au cours des deux dernières décennies, nous avons noté un « déluge de données » lié à la recherche en laboratoire résultant de grandes quantités de données générées par des dispositifs de recherche. Pour s'adapter à cet afflux de données, les laboratoires peuvent maintenir un réseau de sciences informatiques dédié qui permet d'effectuer le transfert, le stockage et le traitement des données de recherche.[5]

Si des auteures et auteurs de menace compromettent ces réseaux, par exemple après avoir exploité une segmentation réseau insuffisante, ils pourraient être en mesure d'interagir avec les dispositifs qui se trouvent sur le réseau et de les manipuler. En accédant à ces dispositifs, les auteures et auteurs de menace peuvent les forcer à fonctionner de façon inattendue, voler ou manipuler les résultats de recherche, ou voler des renseignements exclusifs comme des fichiers de projet qui expliquent le fonctionnement d'un dispositif.

Systèmes de confinement

Les laboratoires s'appuient sur une technologie opérationnelle complexe pour concevoir et maintenir le confinement tout en étudiant les agents pathogènes et les toxines. Ces systèmes comprennent :

- des systèmes de ventilation pour maintenir des pressions d'air différentielles entre les zones de confinement de niveau plus élevé et plus faible, pour permettre le flux d'air vers l'intérieur dans les zones de confinement de niveau plus élevé;
- des systèmes de décontamination des effluents;
- des outils comme des enceintes et des autoclaves de biosécurité.

Bien que la transformation numérique de ces dispositifs peut procurer au personnel de laboratoire des avantages, comme le contrôle et la surveillance à distance, cela signifie aussi que ces systèmes peuvent faire l'objet d'interférence de la part d'auteures et auteurs de menace. Les perturbations que pourraient subir les systèmes de confinement pourraient entraîner des interruptions opérationnelles ou une défaillance du système de confinement faisant en sorte que le personnel ou la collectivité risquerait une exposition à des agents pathogènes et toxines dangereux.

La menace émanant des cybercriminelles et cybercriminels

Nous évaluons que les laboratoires risquent d'être victimes de cybercriminalité engendrée par le déploiement de rançongiciels et par extorsion, ou par le vol et la vente de renseignements personnels ou exclusifs. Les cybercriminelles et cybercriminels peuvent s'en prendre aux organisations en les exploitant pour obtenir un gain financier. Les laboratoires soutiennent plusieurs secteurs qui connaissent des activités de cybercriminalité plus élevées que la moyenne, y compris le secteur des soins de santé et le milieu universitaire, ce qui augmente le potentiel d'exposition accidentelle à une activité de cybercriminalité et à une exploitation. Les laboratoires peuvent être des victimes intéressantes pour les activités de cybercriminalité en raison de la valeur des renseignements qu'ils renferment et de leur vulnérabilité aux tentatives d'extorsion liée aux perturbations des opérations.

L'écosystème de la cybercriminalité en évolution

L'écosystème de la cybercriminalité est en constante évolution et il devient plus efficace, sérialisé et rentable. Les cybercriminelles et cybercriminels interagissent en ayant recours à des marchés et à des forums illégaux pour entrer en contact avec des acheteuses et acheteurs, des vendeuses et vendeurs d'outils, de services ou d'accès réseau. Un exemple représentatif de cette interaction se trouve dans la **chaîne d'approvisionnement du rançongiciel comme service (RaaS pour *Ransomware-as-a-Service*)**.

La majorité des attaques par rançongiciel ciblant des organisations canadiennes sont vraisemblablement liées à des groupes de RaaS. Les groupes de RaaS développent et tiennent à jour des rançongiciels qu'ils louent à d'autres cybercriminelles et cybercriminels en échange d'un paiement.[6]

La chaîne d'approvisionnement du rançongiciel comme service

D'autres cybercriminelles et cybercriminels contribuent à cette chaîne d'approvisionnement en offrant des services spécialisés comme la vente d'accès réseau, la communication avec des victimes, le blanchiment d'argent provenant de rançons et plus encore. En 2021, le réseau d'un laboratoire a été compromis et ses systèmes chiffrés par un rançongiciel après qu'un étudiant ait téléchargé un logiciel de visualisation de données piraté. Des chercheuses et chercheurs en sécurité ont estimé qu'il est probable que ce soit l'auteure ou l'auteur de menace qui a obtenu accès au réseau par le logiciel piraté, et qu'il a ensuite vendu cet accès à une ou un cybercriminel différent qui a alors déployé le rançongiciel.[7] Le laboratoire a perdu une semaine de données de recherche, et les systèmes et réseaux ont dû être reconstruits complètement.[8]

Nous jugeons qu'avec le système RaaS et la disponibilité accrue de cyberoutils malveillants, les obstacles à l'entrée sont réduits pour les cybercriminelles et cybercriminels et ils augmentent leur capacité de mener des attaques perturbatrices contre des organisations ciblées.

Rançongiciels : Chiffrer des données ou des dispositifs et demander une rançon en échange

Les attaques par rançongiciel continuent d'être la forme la plus perturbatrice de menace à laquelle sont confrontées les organisations canadiennes, y compris les laboratoires. Les cybercriminelles ou cybercriminels appliquent généralement au moins deux méthodes d'extorsion contre leurs victimes lorsqu'une attaque par rançongiciel est déployée. La première méthode fait souvent appel au chiffrement de dispositifs ou de fichiers, et la deuxième à l'exfiltration de données pour ensuite menacer de rendre publiques les données de l'organisation si la rançon n'est pas payée.[9]

Les attaques par rançongiciel peuvent entraîner des coûts importants pour les organisations ciblées, et ce, sans même parler du coût de restauration des systèmes infectés. Ces attaques peuvent interrompre des processus opérationnels clés, ce qui peut se traduire par une perte sur le plan de la productivité de la recherche en laboratoire, et une perte de données et de résultats de recherche. En 2020, un laboratoire clinique aux États-Unis a été ciblé par une attaque par rançongiciel qui a rendu les systèmes inaccessibles pendant près d'un mois, forçant le travail de recherche à se faire sur papier et entraînant du fait des retards dans la recherche.[10]

Outre les répercussions sur les systèmes de technologie de l'information (TI), l'attaque par rançongiciel peut avoir une incidence directe ou indirecte sur la technologie opérationnelle (TO), comme les dispositifs de recherche en laboratoire et les systèmes de confinement. Certains groupes de la cybercriminalité déploient des variantes de rançongiciel qui ciblent spécifiquement la TO, et même les incidents liés à des rançongiciels isolés par TI peuvent avoir des répercussions sur la capacité d'une organisation à surveiller ou à contrôler sa TO, forçant des interruptions.[11] Une attaque par rançongiciel contre des systèmes essentiels de confinement de laboratoire pourrait entraîner un bris de confinement, ce qui risque d'exposer le personnel ou la collectivité à des agents pathogènes ou toxines dangereux.

Exfiltration de données : Vente de renseignements pour la vente ou l'exploitation

Les réseaux de laboratoires contiennent diverses formes de renseignements pouvant avoir beaucoup de valeur pour les cybercriminelles et cybercriminels, y compris les renseignements personnels des employées et employés ou des patientes et patients, les renseignements sur les fournisseurs et les partenaires, et les renseignements commerciaux exclusifs ou sensibles. De tels renseignements peuvent servir dans le cadre d'autres activités frauduleuses contre le laboratoire, le personnel du laboratoire ou ses partenaires. L'exfiltration de données peut également être utilisée comme levier pour extorquer les organisations ciblées en vue d'une demande de rançon, au lieu ou en plus du traditionnel chiffrement de dispositif par rançongiciel. Il arrive aussi souvent que les données organisationnelles volées soient affichées pour vente sur les marchés criminels, permettant ainsi à d'autres cybercriminelles et cybercriminels de faire l'acquisition de données à des fins frauduleuses ou d'exploitation. Cela ouvre également la voie à des États-nations et à des concurrents commerciaux qui désirent se procurer des renseignements exclusifs acquis de manière illicite, et ce, sans avoir à prendre part à une activité de cybermenace.

La menace émanant des auteures et auteurs de menace parrainés par des États

Les activités de cybermenace parrainées par des États contre des installations de recherche, dont des laboratoires, ont atteint un sommet durant la pandémie de COVID-19. Durant cette période, les services de renseignement étranger ont réaffecté des cybercapacités sophistiquées provenant d'autres efforts pour recueillir des renseignements sur des mesures occidentales en lien à la santé publique et au développement de vaccins.[12] Beaucoup de pays continuent de donner la priorité à l'amélioration de leur capacité biopharmaceutique et de biofabrication nationale, et dans certains cas, cela implique de recueillir des renseignements par des activités de cybermenace. De plus, les laboratoires participant à d'importants travaux de recherche sur le plan géopolitique, plus particulièrement lorsque les intérêts d'États clés sont impliqués, sont des cibles intéressantes pour les activités de cybermenace conçues pour voler ou modifier des résultats de recherche ou créer de la désinformation au sujet de la recherche.

Publications du Centre pour la cybersécurité traitant de la COVID-19

- Bulletin sur les cybermenaces : Incidence continue de la COVID-19 sur les activités de cybermenace
- Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les cybermenaces pesant sur le secteur de la santé
- Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les activités de cybermenaces
- Avis et conseils en matière de cybersécurité à l'intention des organismes de recherche et de développement durant la pandémie de la COVID-19

Espionnage économique et sur la recherche : Vol des travaux de recherche et de la propriété intellectuelle du Canada

Selon nos observations, des auteures et auteurs de cybermenace parrainés par des États devraient continuer à cibler des laboratoires canadiens pour soutenir leurs capacités nationales dans le domaine biopharmaceutique et celui de la biofabrication en se livrant à l'espionnage. La capacité de recherche en laboratoire est une ressource limitée, en particulier pour les laboratoires fonctionnant sous le niveau NC3 ou NC4, ou qui travaillent avec agents biologiques à cote de sécurité élevée (ABCSE).[13] Le vol de renseignements exclusifs issus de laboratoires est un moyen économique d'obtenir de précieux travaux de recherche sans avoir à faire d'importants investissements dans des capacités de recherche nationale.

Les laboratoires renferment une multitude de renseignements qui peuvent venir appuyer les capacités de biorecherche d'un État étranger et nuire aux intérêts économiques du Canada. Les recherches poussées dans différents secteurs sont couramment ciblées à des fins d'espionnage. Des auteures et auteurs de menace parrainés par des États mènent fréquemment des campagnes de harponnage contre des chercheuses et chercheurs occidentaux, y compris au sein des secteurs biopharmaceutiques et de fabrication. Nous évaluons que les auteures et auteurs de menace parrainés par la RPC représentent presque assurément la forme la plus courante de menace parrainée par un État visant des laboratoires du Canada. La RPC a su se doter d'une solide capacité biopharmaceutique et de biofabrication nationale, et a dans le passé utilisé une propriété intellectuelle volée pour créer un avantage concurrentiel.[14] En plus de l'espionnage à caractère commercial, nous évaluons que les auteures et auteurs de menace parrainés par des États cherchent vraisemblablement à voler des renseignements de recherche à double usage, y compris des renseignements liés aux ABCSE, ayant une utilité militaire défensive ou offensive.

Compromission propre à des sujets précis : Surveillance et manipulation d'une recherche d'intérêt mondial

Nous évaluons que, pour mener des activités d'espionnage ou perturbatrices, des auteures et auteurs de menace parrainés par des États cibleront assurément des laboratoires axés sur la recherche liée aux exigences en matière de renseignement essentiel de cet État ou à une menace existentielle perçue. Les laboratoires contribuent à la recherche et à d'autres formes de tests qui ont d'importantes incidences géopolitiques pour des États étrangers, par exemple dans le cas d'interventions lors d'une crise sanitaire commune ou d'efforts de non-prolifération d'armes biologiques et chimiques. Nous évaluons que les laboratoires qui participent à de telles recherches, par exemple en lien avec la pandémie de COVID-19, vont presque certainement attirer des activités de cybermenace parrainées par des États avec tolérance au risque conçues pour voler, manipuler ou détruire des renseignements de recherche. En 2018, des auteures et auteurs de menace parrainés par la Russie ont projeté de compromettre un laboratoire suisse qui procédait à des tests en lien à l'empoisonnement de Serguï Skripal et de sa fille en Angleterre et à l'utilisation alléguée d'armes chimiques russes en Syrie.[15] L'opération visait l'accès physique au laboratoire et le recours à la cyberexploitation, mais elle a pu être évitée grâce aux autorités néerlandaises et suisses.

Désinformation : Contrôler le discours international et miner la crédibilité de la recherche canadienne

Selon nos observations, il est fort probable que des auteures et auteurs de menace parrainés par des États utilisent des campagnes de désinformation pour cibler des laboratoires impliqués dans la recherche pour potentiellement porter atteinte à la réputation d'États étrangers. Ces campagnes peuvent impliquer la compromission et l'exfiltration de réseaux de laboratoire, la modification et la diffusion de renseignements sensibles. Lorsque les intérêts d'États clés sont impliqués, des États-nations peuvent avoir recours à des opérations de piratage et de divulgation pour infirmer des résultats de laboratoire et appuyer des campagnes de désinformation de l'État. Ces opérations peuvent comprendre le vol et la diffusion publique d'information sensible qui en découle; information qui a été modifiée et présentée hors contexte pour miner la légitimité des résultats. Des cas de désinformation à l'échelle internationale ont été constatés, et ceux-ci visaient à influencer la mésinformation nationale sur les questions de recherches biologiques.[16] Les thèmes liés à la désinformation peuvent remettre en cause la légitimité des résultats, alléguer des actes tout aussi répréhensibles ou plus répréhensibles de la part de l'occident, ou miner la confiance dans la sécurité des opérations en laboratoire.

À la suite de l'interdiction pour les athlètes russes de participer aux Jeux olympiques de 2016 après qu'il ait été découvert que la Russie fournissait à ses athlètes des substances interdites, des auteures et auteurs de menace russes ont ciblé des organismes antidopage à travers le monde, notamment l'Agence mondiale antidopage de Montréal et le Centre canadien pour l'éthique dans le sport (CCES).[17] Les réseaux du CCES ont été compromis après que des pirates informatiques russes aient mené une opération à accès fermé ciblant de hauts fonctionnaires qui assistaient à une conférence à l'étranger. Dès que les réseaux du CCES ont été compromis, les pirates ont exfiltré de l'information sensible, notamment des renseignements médicaux confidentiels sur les athlètes, comme des dérogations relatives à la consommation de substances normalement interdites.[18] Les renseignements volés ont été publiés en ligne et intégrés aux campagnes de désinformation. Dans certains cas, le piratage psychologique a été utilisé pour amener par la ruse des journalistes à publier des renseignements comme véridiques, sans savoir qu'ils avaient été manipulés.

Propriété étrangère
La propriété étrangère de laboratoires ou d'organismes auxiliaires clés, ce qui comprend les fournisseurs qui ont obtenu des contrats pour fournir du matériel, de l'expertise ou des services durant la construction et l'exploitation des laboratoires, donne aux auteures et auteurs de menace parrainés par des États un vecteur de menace additionnel qu'ils peuvent exploiter. Selon nos observations, il est presque certain que la RPC et la Russie ont la capacité nécessaire pour obliger leurs chercheuses et chercheurs ainsi que leurs industries nationales à collaborer avec les efforts de collecte de renseignement et à agir contre les intérêts des organisations canadiennes contractantes.[19] Ils peuvent être contraints de collaborer en utilisant des programmes d'accès légal qui ciblent l'information sensible transférée en transitant par leurs territoires ou conservée dans leurs territoires. Cette contrainte peut aussi se traduire de façon plus générale par le recours à une coercition extrajudiciaire pouvant inclure l'envoi direct de renseignements de recherche provenant de laboratoires étrangers établis au Canada à des États étrangers. Nous évaluons que, si l'occasion se présente, il est fort probable que la RPC et la Russie utilisent leurs relations avec des intérêts étrangers pour voler des renseignements exclusifs de laboratoires ou obtenir l'accès à des réseaux de laboratoires.

Hacktivistes et terroristes

Nous évaluons qu'il est improbable que des groupes terroristes ciblent des laboratoires en prenant divers moyens pour exfiltrer des données ou pour provoquer des perturbations opérationnelles. Les groupes terroristes pourraient vouloir recueillir des renseignements sur des ABCSE et leur application pour les armes biologiques comme outil pour faire avancer leurs objectifs idéologiques. Toutefois, nous ne sommes pas au courant de groupes ayant la sophistication nécessaire et l'intention de le faire par l'intermédiaire de cybercompromissions contre des laboratoires.

Nous évaluons qu'il est possible que les laboratoires soient touchés par une cybermenace peu sophistiquée, comme des attaques par DDoS menées par des hacktivistes qui sont peu susceptibles de perturber les opérations en laboratoire. Des hacktivistes prorusses ont ciblé des infrastructures essentielles occidentales depuis le début de l'invasion de l'Ukraine par la Russie, en ayant recours à des activités de cybermenace peu sophistiquées visant à intimider et à décourager le soutien envers l'Ukraine. Ces activités comprennent principalement des techniques telles que les attaques par DDoS contre des sites Web

publics d'organisations du secteur des infrastructures essentielles très connues. Par exemple, en avril 2023, des hacktivistes prorusses ont mené des attaques par DDoS contre des sites Web d'infrastructures essentielles canadiennes et du gouvernement du Canada, dont celui du premier ministre.[20]

Perspective

La cybercompromission de laboratoires peut avoir des implications importantes sur la sécurité physique, économique et nationale du Canada. Le vol de renseignements exclusifs peut mettre en péril l'avantage du Canada. La plus grande connectivité de la TO impliquée dans la recherche en laboratoire et le maintien du confinement augmente le risque qu'une cybercompromission ait des répercussions physiques, y compris l'exposition du personnel de laboratoire et de la collectivité élargie à des agents pathogènes et des toxines mortels et virulents.

Un grand nombre de cybermenaces peuvent être atténuées grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de sécurité et de continuité des activités. Le Centre pour la cybersécurité recommande à tous les propriétaires de réseaux des infrastructures essentielles, y compris ceux qui sont responsables des réseaux de laboratoires, de prendre les mesures nécessaires pour protéger leurs systèmes contre les cybermenaces décrites dans la présente évaluation.

Consultez les ressources en ligne ci-dessous pour obtenir de l'information supplémentaire ainsi que des avis et conseils utiles :

- Introduction à l'environnement de cybermenaces
- Évaluation des cybermenaces nationales
- Évaluation des cybermenaces de base : Cybercriminalité
- Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles
- Guide sur les rançongiciels (ITSM.00.099)
- Défense contre les menaces d'exfiltration de données (ITSM.40.110)
- Facteurs à considérer sur le plan de la recherche et du développement (ITSAP.00.130)
- Protéger le matériel de recherche médicale contre les cybermenaces (ITSAP.00.134)
- Piratage psychologique (ITSAP.00.166)

[1] Nicole Bogart, Canadian scientists make COVID-19 research breakthrough, isolating virus, CTV News, 13 mars 2020.

[2] Centre canadien pour la cybersécurité, Bulletin sur les cybermenaces : Incidence continue de la COVID-19 sur les activités de cybermenaces, 21 décembre 2020.

[3] Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2023-2024, 28 octobre 2022.

[4] Agence de la santé publique du Canada, Norme canadienne sur la biosécurité, troisième édition, Section 1.3.6.4, 24 novembre 2022.

[5] Gordon Bell, Tony Hey et Alex Szalay, Beyond the Data Deluge, Science 323:5919, 6 mars 2009; pour avoir un exemple, consultez Steven R. Spurgeon et coll., Towards data-driven next-generation transmission electron microscopy, Natural Materials 20:3, 2021.

[6] Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2023– 2024, octobre 2022, page 7.

[7] Tilly Travers, MTR in Real Time: Pirates pave way for Ryuk ransomware, Sophos, 6 mai 2021.

[8] Tilly Travers, MTR in Real Time: Pirates pave way for Ryuk ransomware, Sophos, 6 mai 2021.

[9] Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2023– 2024, octobre 2022.

[10] Toby Cornish, David McClintock, Are you Prepared? Laboratory Downtime in the Ransomware Era, American Journal of Clinical Pathology 157:4, avril 2022.

[11] TrendMicro, IoT and Ransomware: A Recipe for Disruption, 28 septembre 2021; voir aussi, David Sanger, Clifford Krauss, Nicole Perlroth, Cyberattack Forces a Shutdown of a Top U.S. Pipeline, The New York Times, 8 mai 2021.

[12] Centre canadien pour la cybersécurité, Bulletin sur les cybermenaces : Incidence continue de la COVID-19 sur les activités de cybermenaces, 21 décembre 2021.

[13] King's College London, Global BioLabs Report 2023, 15 mars 2023.

[14] Alex Keown, Extradited Scientist Found Guilty of Stealing GSK Secrets, BioSpace, 3 mai 2022.

[15] Sean Gallagher, Russians tried to hack Swiss lab testing samples from Skripal attack, Ars Technica, 17 septembre 2018.

[16] Karen Pauls, Jeff Yates, Online claims that Chinese scientists stole coronavirus from Winnipeg lab have 'no factual basis', CBC, 27 janvier 2020; Justin Ling, How 'Ukraine bioweapons labs' myth went from QAnon fringe to Fox News, The Guardian, 18 mars 2020.

[17] Murray Brewster, Canadian agency astonished to be targeted by alleged Russian cyberattack, CBC, 5 octobre 2018.

[18] Andy Greenberg, How Russian spies infiltrated hotel Wi-Fi to hack their victims up close, Wired, 4 octobre 2018.

[19] Centre canadien pour la cybersécurité, La cybermenace provenant des chaînes d'approvisionnement, 8 février 2023.

[20] Centre de la sécurité des télécommunications, Déclaration de la ministre de la Défense nationale – Cybermenaces ciblant les infrastructures essentielles, 13 avril 2023; Rachel Aiello, Russia being able to 'bring down' Canadian gov't websites won't dissuade support for Ukraine: Trudeau, CTV News, 11 avril 2023.

CAT. D96-108/2024F-PDF
ISBN 978-0-660-70776-1

Centre de la sécurité des télécommunications Communications Security Establishment

Canada