TLP:WHITE

Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

BULLETIN SUR LES CYBERMENACES

L'incidence continue de la COVID-19 sur les activités de cybermenaces

Canada

À PROPOS DU PRÉSENT DOCUMENT

AUDITOIRE

Le présent bulletin sur les cybermenaces est destiné à la collectivité de la cybersécurité. Tout en étant soumise aux règles standard de droit d'auteur, l'information TLP:WHITE peut être distribuée sans aucune restriction. Pour obtenir de plus amples renseignements sur le protocole TLP (Traffic Light Protocol), prière de consulter la page Web https://www.first.org/tlp/.

COORDONNÉES

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

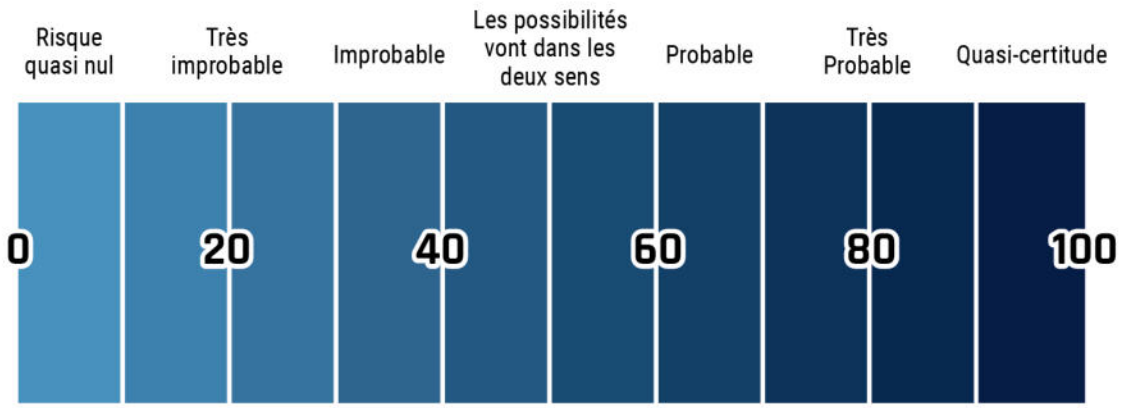
MÉTHODOLOGIE ET FONDEMENT DE L'ÉVALUATION

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 Centre canadien pour la cybersécurité (Centre pour la cybersécurité) en matière de 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 l'environnement de cybermenaces, ce qui a contribué à la présente évaluation. Le mandat de renseignement étranger du Centre de la sécurité des télécommunications (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.

Les évaluations des cybermenaces effectuées sont basées 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. On emploiera des termes tels que « 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 9 décembre 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.



INTRODUCTION

Le 11 mars 2020, l'Organisation mondiale de la Santé (OMS) qualifie officiellement la propagation de la maladie à coronavirus 2019 (COVID-19) de pandémie mondiale. Profitant de l'incertitude et de la panique de la population devant la propagation initiale de la COVID-19, les cybercriminels ont inondé l'Internet de courriels d'hameçonnage accompagnés de maliciels et de sites Web frauduleux dans lesquels ils publiaient des lignes directrices de santé publique prétendument officielles ou de l'information sur les prestations d'urgence et les mesures de stimulation économique qui aideraient les Canadiens pendant que le pays était toujours en état d'urgence. Au même moment, des auteurs de cybermenaces parrainés par des États ont rapidement profité de la déferlante de la pandémie pour obtenir du nouveau renseignement et, entre autres, voler de la propriété intellectuelle relative à la recherche et au développement de vaccins potentiels contre la COVID-19.

Le 27 avril 2020, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a publié le *Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les activités de cybermenaces* afin d'informer les Canadiens de l'intérêt grandissant des cybercriminels pour les leurres sur le thème de la COVID-19 utilisés pour lancer des arnaques et distribuer des maliciels; des répercussions possibles d'attaques par rançongiciel sur un système de santé surchargé au Canada et des risques importants qu'encourt le Canada en matière de cybersécurité devant la mise en place précipitée du télétravail dans l'ensemble du pays. En juin 2020, le Centre pour la cybersécurité a publié une évaluation subséquente, le Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les cybermenaces pesant sur le secteur de la santé, qui portait sur la vulnérabilité grandissante des travailleurs de première ligne du domaine de la santé publique et des employés des hôpitaux et des installations de recherche médicale, et sur le harcèlement auquel ils ont fait face au plus fort de la pandémie de la part des cybercriminels et des auteurs de cybermenaces parrainés par des États.

Au début de décembre 2020, plus de 400 000 Canadiens avaient contracté la COVID-19 et près de 13 000 d'entre eux étaient décédés.[1] Le 9 décembre 2020, Santé Canada a autorisé l'utilisation du premier vaccin contre la COVID-19. Bien qu'il soit justifié d'être optimiste, le Centre pour la cybersécurité est conscient qu'il est quasi-certain que d'importantes activités de cybermenaces cibleront la distribution mondiale des vaccins contre la COVID-19, y compris au Canada. C'est pourquoi le Centre pour la cybersécurité publie le présent bulletin sur les cybermenaces, qui évalue si les principaux jugements antérieurs sur l'incidence de la COVID-19 sur les activités de cybermenaces tiennent la route et établit les menaces auxquelles s'attendre lors de la distribution et de l'administration du vaccin contre la COVID-19 au Canada.

LES PRINCIPAUX JUGEMENTS ANTÉRIEURS DU CENTRE POUR LA CYBERSÉCURITÉ À PROPOS DE L'INCIDENCE DE LA COVID-19 SUR LES ACTIVITÉS DE CYBERMENACES TIENNENT-ILS LA ROUTE?

JUGEMENT : « Des États ont modifié leurs activités de collecte de renseignement en réponse à la pandémie de COVID-19. Nous estimons avec quasi-certitude que le cyberespionnage visant le Canada continuera de comporter des tentatives de vol de propriété intellectuelle canadienne relative à la recherche médicale sur la COVID-19 et d'informations classifiées sur les mesures d'intervention adoptées par le gouvernement du Canada. »

À la suite des premières évaluations portant sur le vol de propriété intellectuelle parrainé par des États, le Canada et ses alliés ont observé de multiples campagnes de cyberespionnage parrainées par des États ciblant des organismes de recherche médicale sur la COVID-19. De concert avec ses partenaires des États-Unis et du Royaume-Uni, le Canada a publié en juillet 2020 un avis de sécurité sur le groupe de cyberespionnage APT29, considéré presque assurément comme un groupe dirigé par les services de renseignement russes, qui cibleraient des organisations participant au développement d'un vaccin contre la COVID-19 au Canada, aux États-Unis et au Royaume-Uni.[2] Nous avons déterminé que le groupe APT29 avait fort probablement pour objectif de voler l'information et la propriété intellectuelle relatives au développement et à l'essai de vaccins contre la COVID-19, et avons publié des avis et des conseils pour prévenir de futures compromissions.

[1] Gouvernement du Canada, *Maladie à coronavirus (COVID-19)* (consulté le 9 décembre 2020). https://www.canada.ca/fr/sante-publique/services/maladies/maladie-coronavirus-covid-19.html

[2] National Cyber Security Centre, *APT29 targets COVID-19 vaccine development*, 16 juillet 2020. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

Nous estimons que les recherches relatives au vaccin contre la COVID-19 continueront d'être la cible d'auteurs de cybermenaces parrainés par des États dans un avenir rapproché en raison de la concurrence de plus en plus vive associée à la création d'une chaîne d'approvisionnement sécuritaire pour la production d'un vaccin au pays. Le 13 novembre 2020, Microsoft a déclaré que des pirates russes et nord-coréens ciblaient toujours activement des chercheurs de vaccins au Canada, en France, en Inde, en Corée du Sud et aux États-Unis[3]. Puis le 9 décembre 2020, les réseaux de l'Agence européenne des médicaments ont été compromis et la demande d'homologation pour les vaccins des sociétés Pfizer et BioNTech contre la COVID-19 a fait l'objet d'un accès illégal[4]. Parallèlement, les chercheurs en cybersécurité d'IBM ont dévoilé le 3 décembre dernier l'existence d'une campagne mondiale d'hameçonnage ciblant la chaîne du froid du vaccin contre la COVID-19, c'est-à-dire les fournisseurs qui veillent au transport et à la conservation sécuritaires des vaccins exigeant un entreposage à température contrôlée.[5]

JUGEMENT : « Des campagnes d'influence en ligne continuent de miner la confiance du public à l'égard des déclarations et des statistiques officielles, ce qui a pour effet d'affaiblir les mesures d'intervention en matière de santé publique et d'intensifier l'angoisse et l'incertitude, sur lesquelles repose l'efficacité des cybermenaces portant sur la COVID-19. »

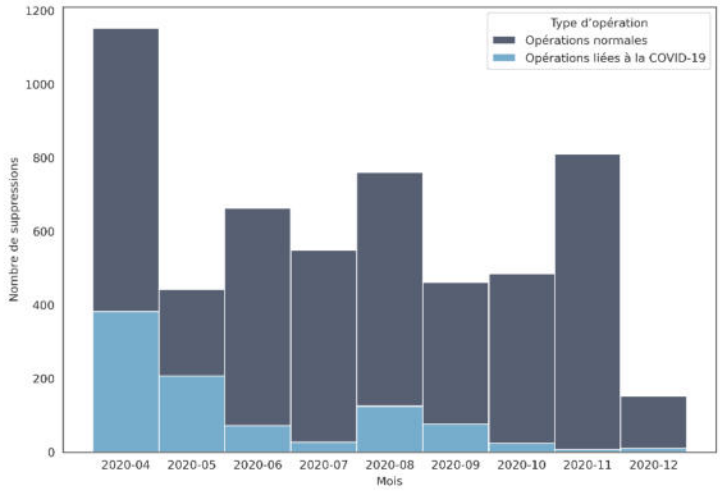
Le Centre pour la cybersécurité est au courant des campagnes étrangères d'influence en ligne actuellement menées qui amplifient les mensonges à propos de l'origine de la COVID-19 et des traitements médicaux contre la maladie ou encore à propos de l'efficacité des efforts continus en santé publique. Le Service européen d'action extérieure (SEAE) évalue actuellement que les activités d'influence en ligne relatives à la COVID-19 ont baissé, mais qu'elles se sont également réorientées vers le développement et la distribution de vaccins.[6] Bien que dans la majorité des cas les activités d'influence propagent et amplifient des faussetés à propos de l'innocuité des vaccins en général, le SEAE remarque que la Russie et la Chine, dans les médias contrôlés par l'État, se lancent dans la « diplomatie du vaccin », en promouvant leurs propres vaccins contre la COVID-19 tout en rejetant les efforts des États-Unis[7]. Bien que les effets des activités d'influence en ligne soient difficiles à évaluer, particulièrement celles qui sont éloignées des réseaux canadiens de médias numériques, **nous estimons qu'il est très probable que les faussetés qui sont répandues et amplifiées à propos des vaccins contre la COVID-19 dans les campagnes d'influence en ligne vont probablement réduire la confiance de certains Canadiens envers la sécurité de la distribution des vaccins au Canada.**

[3] Microsoft, *Cyberattacks targeting health care must stop,* 13 novembre 2020. https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/.
[4] BioNTech, *Statement Regarding Cyber Attack on European Medicines Agency*, 9 décembre 2020. https://investors.biontech.de/news-releases/news-release-details/statement-regarding-cyber-attack-european-medicines-agency
[5] IBM Security Intelligence, *IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain*, 3 décembre 2020. https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/
[6] Service européen d'action extérieure, *MISE À JOUR DU RAPPORT SPÉCIAL DU SEAE: Brève évaluation des récits et éléments de désinformation circulant à propos de la pandémie de COVID-19 (MISE À JOUR MAI – NOVEMBRE) EUvsDisInfo*, 2 décembre 2020. https://euvsdisinfo.eu/fr/mise-a-jour-du-rapport-special-du-seae-breve-evaluation-des-recits-et-elements-de-desinformation-circulant-a-propos-de-la-pandemie-de-covid-19-mise-a-jour-mai-novembre/
[7] Ibid.

JUGEMENT : « Des auteurs de cybermenaces aux motivations diverses et possédant des capacités de divers degrés de sophistication se servent de la pandémie de COVID-19 pour leurrer ou duper leurs victimes dans le cadre d'activités malveillantes comme le cyberespionnage et la cybercriminalité. »

Les cybercriminels demeurent opportunistes et très au courant de ce qui suscite l'intérêt de leurs cibles. En mars-avril 2020, il s'agissait des nouvelles concernant la propagation et l'impact de la COVID-19. Récemment, ce type d'informations s'est fait plus rare à la suite de l'apparition d'autres leurres thématiques qui ont pris une plus grande importance, comme les informations sur l'élection présidentielle américaine. Comme illustré dans la figure 1, les données d'un partenaire de troisième part du Centre pour la cybersécurité responsable de la suppression de sites Web malveillants montrent clairement une réduction du nombre de sites Web d'hameçonnage ayant la COVID-19 comme thème depuis avril-mai 2020. **Toutefois, ce jugement perd de sa validité, car le Centre pour la cybersécurité s'attend à ce que les auteurs de cybermenaces utilisent le vaccin contre la COVID-19 comme leurre thématique ou subterfuge pour leurs activités malveillantes, p. ex. le cyberespionnage ou le cybercrime. Nous estimons qu'il est quasi certain que des courriels d'hameçonnage et des sites Web frauduleux se feront passer pour des communications officielles du gouvernement du Canada au sujet de la distribution des vaccins contre la COVID-19 afin d'inciter les Canadiens à télécharger des maliciels, à cliquer sur des liens malveillants ou à divulguer des renseignements personnels ou financiers.**

Figure 1 — Suppression de sites Web malveillants, opérations liées à la COVID-19 et opérations normales



JUGEMENT : « À l'échelle mondiale, la pandémie de COVID-19 exerce une énorme pression sur le secteur de la santé. Nous estimons que des attaques par rançongiciel continueront presque certainement à cibler des établissements de soins de santé et de recherche médicale, à compromettre la santé des patients et à miner les efforts collectifs en matière de santé publique. »

La menace d'attaques par rançongiciel contre les établissements de santé et de recherche médicale de première ligne n'a fait qu'augmenter pendant la pandémie. De nombreux hôpitaux canadiens ont subi des attaques par rançongiciel au cours des derniers mois, notamment une attaque contre un conseil local de la santé qui a forcé l'Hôpital général juif de Montréal à se déconnecter d'Internet.[8] L'attaque faisait très probablement partie d'une campagne d'activités de rançongiciels sophistiqués ciblant le secteur de la santé en Amérique du Nord menée par des groupes cybercriminels organisés connus pour exploiter les trousses de logiciels malveillants TrickBot, Bazar, Ryuk et Conti[9]. Plus important encore, des procureurs allemands affirment que des cybercriminels ont contribué au décès d'une patiente qui a souffert d'un anévrisme aortique mortel après que son ambulance a été considérablement retardée en raison d'une attaque par rançongiciel en septembre[10]. **Nous estimons qu'il est presque certain que les cybercriminels continueront de mettre en danger la santé des patients et les efforts plus vastes en matière de santé publique en déployant des rançongiciels à des fins de gains financiers contre des secteurs de la santé vulnérables, y compris la chaîne d'approvisionnement des vaccins contre la COVID-19.**

[8] The Globe and Mail, *Quebec Health Network Targeted by Cyberattack,* 29 octobre 2020. https://www.theglobeandmail.com/canada/article-quebec-health-network-targeted-by-cyberattack/

[9] US-CERT, *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector*, 2 novembre 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[10] Wired, *The untold story of a cyberattack, a hospital and a dying woman,* 11 novembre 2020. https://www.wired.co.uk/article/ransomware-hospital-death-germany

JUGEMENT : « Il est presque certain que les services de renseignement étrangers et les cybercriminels continueront de cibler les télétravailleurs. Les auteurs de cybermenaces tentent déjà de découvrir les employés des secteurs d'intérêt stratégique qui travaillent de la maison et d'exploiter les technologies déployées pour soutenir les télétravailleurs, notamment les réseaux privés virtuels (RPV) ou les plateformes de vidéoconférence. »

Les prévisions du Centre pour la cybersécurité concernant les risques croissants de cybersécurité associés à la migration rapide d'une grande partie de la main-d'œuvre canadienne vers le travail à distance se sont largement confirmées, et nous estimons que les cybercriminels et les auteurs de cybermenaces parrainés par des États sont très probablement devenus de plus en plus aptes à compromettre les RPV et infrastructures infonuagiques mal gérées ou vulnérables. Depuis mars 2020, le Centre pour la cybersécurité et ses partenaires internationaux ont publié de nombreux avis et bulletins techniques au sujet de l'exploitation active de produits RPV et infonuagiques par des auteurs sophistiqués de cybermenaces. Ces produits sont largement utilisés par les employés en télétravail afin d'accéder à des réseaux et à des actifs organisationnels de nature sensible. Récemment, le 7 décembre 2020, la National Security Agency (NSA) des États-Unis a publié un avis de cybersécurité au sujet de l'exploitation parrainée par des États qui continuait de cibler des produits VMware de gestion des identités couramment utilisés pour sécuriser l'accès à distance aux réseaux d'entreprises et gouvernementaux.[11]

[11] National Security Agency, *Cybersecurity Advisory: Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials*, 7 décembre 2020.
https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF