TLP:WHITE

Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

BULLETIN SUR LES CYBERMENACES

Incidence de la COVID-19 sur les cybermenaces pesant sur le secteur de la santé

8 JUIN 2020

Canada

À PROPOS DU PRÉSENT DOCUMENT

AUDITOIRE

Le présent bulletin sur les cybermenaces est destiné à la collectivité de la cybersécurité. Tout en étant soumis 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 (CCC ou Centre pour la cybersécurité) à contact@cyber.gc.ca.

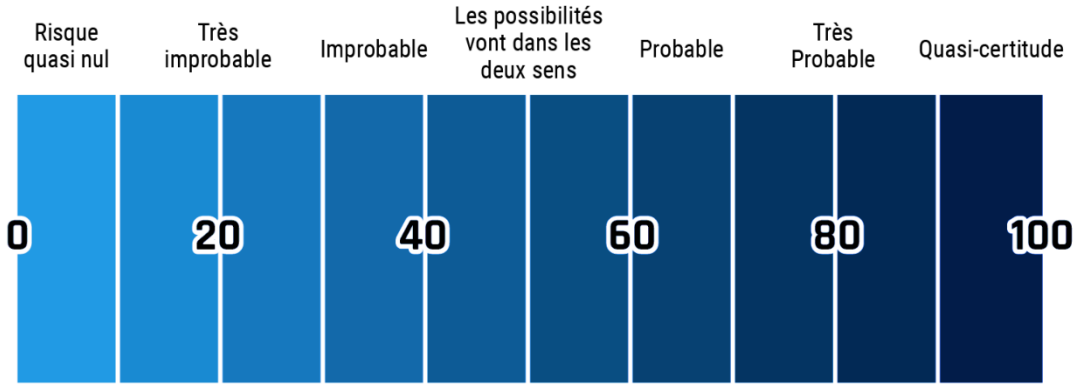
MÉTHODOLOGIE ET FONDEMENT DE L'ÉVALUATION

Les principaux jugements dans cette évaluation reposent sur des rapports provenant de diverses sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du CCC en matière de cybersécurité. En défendant les systèmes d'information du gouvernement du Canada, le Centre pour la cybersécurité bénéficie d'une perspective unique lui permettant d'observer les tendances dans l'environnement de cybermenaces et d'appuyer ses évaluations. Dans le cadre du volet du mandat du CST relatif au renseignement étranger, le CCC tire parti d'information précieuse sur les habitudes des adversaires dans le cyberespace. Bien que le CCC soit tenu de toujours protéger ses sources et méthodes classifiées, il s'efforce de justifier le plus possible ses jugements.

Les principaux jugements du CCC sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude d'autres explications possibles, la réduction de biais et l'utilisation d'un langage probabiliste. Le Centre pour la cybersécurité utilise des formulations telles que « nous évaluons » ou « nous estimons » pour présenter une évaluation analytique. Les qualificatifs tels que « possiblement », « probablement », « très probable » et « fort possible » servent à évoquer la probabilité.

Le contenu de ce document est fondé sur l'information disponible en date du 8 juin 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.



Principaux jugements

- Nous estimons que les organismes de santé publique nationaux et internationaux continueront presque assurément d'être la cible d'activités de cybermenaces, comme des attaques par rançongiciel ou par déni de service distribué (DDoS pour *Distributed Denial of Service*), ou encore des attaques visant à soutirer de l'argent ou de l'information.
- Nous jugeons que les auteurs de cybermenaces risquent fort probablement de persévérer dans leurs efforts de ciblage axés sur les hôpitaux, les cliniques et d'autres services de première ligne prenant part aux activités d'intervention à la COVID-19 à travers le monde. Bien que de nombreuses attaques par rançongiciel visant des hôpitaux aient été observées à l'étranger, le Centre pour la cybersécurité n'a pas été sollicité pour porter assistance lors d'un événement majeur de rançongiciel contre un hôpital canadien durant la pandémie. Les incidents ont probablement été localisés et gérés par des équipes de cybersécurité au sein des hôpitaux. Nous estimons toutefois que les hôpitaux canadiens représentent des cibles aussi attrayantes pour les auteurs de menaces que d'autres hôpitaux dans le monde, surtout s'ils sont au cœur d'une flambée épidémique locale.
- Selon nos estimations, les services de renseignement étrangers continueront presque certainement d'utiliser leurs cybercapacités pour recueillir du renseignement sur la recherche médicale et la propriété intellectuelle liées à la COVID-19. En effet, la propriété intellectuelle, notamment en ce qui concerne le développement de vaccins et de traitements, le dépistage de la COVID-19 et les dispositifs médicaux comme les respirateurs ou l'équipement de protection individuelle (EPI), apporterait presque certainement des avantages sur le plan de la santé publique, de l'économie et de la sécurité nationale.
- Nous estimons que les campagnes d'influence en ligne continueront presque certainement à répandre des mensonges et à susciter du scepticisme à l'égard des statistiques et des déclarations officielles concernant la pandémie de COVID-19.
- Bien que le Canada ne semble pas constituer une cible prioritaire pour les activités d'influence en ligne, il pourrait le devenir rapidement, surtout en réaction aux tensions politiques croissantes avec certains États. Par ailleurs, bon nombre de campagnes d'influence en ligne visent des pays alliés du Canada dont les écosystèmes d'information sont étroitement liés à ceux du Canada.
- Nous estimons que les efforts d'intervention déployés dans le cadre de la pandémie continueront d'être minés par des activités de fraude en ligne liées à la COVID-19 en raison du détournement de ressources et de la distribution de produits contrefaits de qualité inférieure.

Ciblage du secteur de la santé lors de la pandémie de COVID-19

Le 11 mars 2020, l'Organisation mondiale de la santé (OMS) a déclaré officiellement que la nouvelle maladie à coronavirus 2019 (COVID-19) constituait une pandémie mondiale. Dans un bulletin antérieur, nous avons évalué que des auteurs de cybermenaces ont profité de ce contexte pour réaliser toute une gamme d'activités de cybermenaces.[4] Les cybercriminels et les auteurs de cybermenaces parrainés par un État s'en prennent tous deux au secteur de la santé – que nous définissons comme étant les établissements de soins de santé, hôpitaux et autres fournisseurs de soins de santé de première ligne, les organisations de recherche, les sociétés pharmaceutiques et les entreprises qui vendent de l'équipement médical. Le Centre pour la cybersécurité estime qu'au Canada et que dans de nombreux autres pays, les organisations œuvrant dans le secteur de la santé font face à des menaces accrues pour leur cybersécurité en raison de la pandémie de COVID-19.[5]

Le télétravail présente des vulnérabilités

Les organisations œuvrant dans le secteur de la santé sont davantage exposées aux menaces lorsque leurs employés travaillent à distance.[1] En mars 2020, Microsoft a découvert que l'infrastructure de télétravail de plusieurs douzaines d'hôpitaux était vulnérable, notamment les passerelles réseaux et les réseaux privés virtuels (RPV).[2] Le Centre pour la cybersécurité a publié des alertes concernant les vulnérabilités touchant les logiciels de travail à distance fournis par des entreprises telles que Citrix, Fortinet, Palo Alto et Pulse, lesquels sont ciblés activement par des cybercriminels et auteurs de menace parrainés par un État.[3]

Établissements de santé publique

Nous jugeons que les organismes de santé publique nationaux et internationaux continueront presque assurément d'être la cible d'activités de cybermenaces, comme des attaques par rançongiciel ou par déni de service distribué (DDoS), ou encore des attaques visant à soutirer de l'argent ou de l'information. Les auteurs de menace étatiques s'intéressent à l'information portant sur les mesures d'intervention adoptées par les établissements de santé publique nationaux et internationaux en réponse à la pandémie. Les cybercriminels reconnaissent que ces établissements sont soumis à des pressions dues au fait qu'ils doivent sans cesse coordonner les efforts d'intervention et tenir la population informée, ce qui signifie qu'ils sont prêts à verser une rançon pour que leurs systèmes soient rétablis. À la fin mars, des auteurs de menace ont diffusé des courriels malveillants portant sur la COVID-19 pour tenter de transmettre un rançongiciel à un organisme de santé du gouvernement canadien prenant part aux activités d'intervention à la pandémie.[6] Au début du mois de mars, le responsable de la sécurité des systèmes d'information de l'OMS a déclaré que l'organisation avait enregistré une augmentation des activités de cybermenaces durant la pandémie de COVID-19.[7] Les courriels reçus par l'OMS visaient à recueillir des justificatifs d'identité en vue d'accéder à de l'information sensible ou de cibler d'autres victimes.

Lorsque les cybercriminels parviennent à compromettre les établissements de santé publique dans le cadre de leurs attaques par rançongiciel ou par DDoS, ils peuvent nuire aux efforts visant à ralentir la propagation de la COVID-19 en freinant la coordination et la diffusion de l'information. Par exemple, une attaque par DDoS contre un site Web du gouvernement néerlandais a mis temporairement hors service la page Web qui fournissait de l'information sur la COVID-19 au public.[8] Les cybercriminels peuvent orchestrer des attaques par DDoS pour commettre de l'extorsion, tandis que les auteurs de menaces parrainés par un État peuvent y avoir recours dans le cadre d'une campagne d'influence en ligne pour mettre leurs cibles dans l'embarras ou pour retirer des sources légitimes d'information.

Fournisseurs de soins de santé de première ligne

Nous évaluons que les auteurs de cybermenaces risquent fort probablement de persévérer dans leurs efforts de ciblage axés sur les hôpitaux, les cliniques et d'autres services de première ligne prenant part aux activités d'intervention à la COVID-19 à travers le monde. Bien que plusieurs opérateurs de rançongiciels aient promis de s'abstenir de cibler les fournisseurs de soins de santé de première ligne durant la pandémie,[10] de mars à avril 2020, des hôpitaux et centres de santé en République tchèque,[11] aux États-Unis,[12] en Espagne,[13] et en Allemagne[14] ont été victimes d'attaques par rançongiciel. Le Centre pour la cybersécurité n'a pas été sollicité pour porter assistance lors d'un événement majeur de rançongiciel contre un hôpital canadien durant la pandémie. Les incidents ont probablement été localisés et gérés par des équipes de cybersécurité au sein des hôpitaux. Nous estimons toutefois que les hôpitaux canadiens représentent très certainement des cibles aussi attrayantes pour les auteurs de menaces que d'autres hôpitaux dans le monde, surtout s'ils sont au cœur d'une flambée épidémique locale. Une campagne de rançongiciel a ciblé onze fournisseurs de soins de santé de première ligne aux États-Unis.[15] Le 11 mars, l'hôpital de l'université Brno en République tchèque, où l'on effectue notamment des tests de COVID-19, a été forcé de déconnecter ses systèmes à la suite d'une cyberintrusion et les activités à l'hôpital ont été interrompues.[16] Le 21 avril, un centre de santé au Colorado a été contraint d'utiliser des dossiers papier et manuels en raison d'une attaque par rançongiciel.[17]

Vulnérabilités liées aux dispositifs médicaux

Les hôpitaux et autres fournisseurs de soins de santé sont confrontés à d'uniques défis en matière de cybersécurité en raison de la grande variété de dispositifs médicaux connectés à leurs réseaux, surtout les dispositifs médicaux de l'internet des objets (IdO). D'après un sondage publié en mars 2020 par Palo Alto Networks, 83 % des imageurs médicaux aux États-Unis exécutent des systèmes d'exploitation qui ne sont plus pris en charge.[9] Les auteurs de cybermenaces peuvent se servir de dispositifs non corrigés ou de systèmes patrimoniaux pour compromettre des réseaux hospitaliers et voler des données ou lancer une attaque par rançongiciel.

Les fournisseurs de soins de santé de première ligne sont particulièrement susceptibles d'être la cible de rançongiciels, puisqu'ils disposent de ressources financières considérables et qu'une interruption réseau peut mettre en péril la vie des patients. Pour ces raisons, les cybercriminels savent qu'ils ont de bonnes chances de recevoir de fortes rançons. En plus des interruptions immédiates, les organisations victimes de rançongiciels peuvent également se heurter à des brèches de donnée, une menace employée par de nombreux opérateurs de rançongiciels pour forcer leurs victimes à payer. Depuis novembre 2019, le Centre pour la cybersécurité a observé plusieurs cas d'exfiltration et de fuite de données découlant du refus de certaines victimes de payer une rançon. Cette menace est grave et bien réelle pour les fournisseurs de soins de santé de première ligne qui possèdent des renseignements personnels sensibles sur la santé. La divulgation de ceux-ci aurait des effets négatifs sur leur réputation ainsi que des conséquences juridiques importantes.

Propriété intellectuelle et chaînes d'approvisionnement

Selon nos estimations, les services de renseignement étrangers continueront presque certainement d'utiliser leurs cybercapacités pour recueillir du renseignement sur la recherche médicale et la propriété intellectuelle liées à la COVID-19. Étant donné le degré inattendu de propagation et de sévérité du virus, on peut supposer que les gouvernements estiment qu'ils ne disposent pas de l'information adéquate pour mettre en place des mesures d'intervention efficaces sur le plan de la santé publique et de l'économie en vue de lutter contre la pandémie de COVID-19. C'est pourquoi on a presque certainement confié aux services de renseignement étrangers le mandat d'obtenir du renseignement concernant la pandémie de COVID-19. Il est

également probable que les cybercriminels associés aux gouvernements touchés ciblent le secteur de la santé pour appuyer les efforts de collecte de renseignement menés par les organismes de renseignement officiels. La propriété intellectuelle, notamment en ce qui concerne le développement de vaccins et de traitements, le dépistage de la COVID-19 et les dispositifs médicaux comme les respirateurs ou l'équipement de protection individuelle (EPI), apporterait presque certainement des avantages sur le plan de la santé publique, de l'économie et de la sécurité nationale. Par exemple, la propriété intellectuelle volée pourrait permettre à un pays d'accélérer la vaccination à grande échelle et ainsi augmenter sa croissance économique, ce qui favoriserait la stabilité à l'échelle nationale et lui vaudrait des éloges à l'échelle internationale.

Le Centre pour la cybersécurité est au courant d'activités de cybermenaces ciblant le Canada, ce qui est presque certainement attribuable à sa réputation de chef de file mondial dans le secteur de la santé et de la biotechnologie. Plusieurs entreprises et universités de recherche du Canada sont des cibles attrayantes, car elles dirigent les efforts menés à l'échelle mondiale pour mettre au point des tests de dépistage de la COVID-19, des traitements et des vaccins.

À la mi-avril 2020, les systèmes d'une société biopharmaceutique canadienne ont été compromis par un auteur de cybermenaces étranger qui cherchait presque certainement à voler sa propriété intellectuelle. Des auteurs de menaces parrainés par un État ont également ciblé des entreprises médicales et des universités de recherche en Corée du Sud[19], en Chine[20], aux États-Unis[21] et au Royaume-Uni[22]. Le 13 mai 2020, le Federal Bureau of Investigation (FBI) et la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis ont publié un avis dans lequel ils avertissaient les organismes de soins de santé, les entreprises pharmaceutiques et les organisations de recherche qui contribuent aux mesures d'intervention liées à la pandémie de COVID-19 qu'ils sont des cibles de choix pour les auteurs de cybermenaces parrainés par un État[23].

Compromission de superordinateurs

Des cybercriminels ont pris le contrôle de superordinateurs à plusieurs endroits en Europe pour miner de la cryptomonnaie. Un certain nombre de ces superordinateurs étaient utilisés dans le cadre de la recherche sur la COVID-19, notamment la modélisation de la propagation du virus et le soutien du développement de traitements et de vaccins. Il a fallu mettre les systèmes hors ligne pour les réparer, ce qui a interrompu les efforts de recherche[18].

Des sociétés pharmaceutiques, des entreprises qui vendent de l'équipement médical et des organisations de recherche médicale ont également été victimes d'attaques par rançongiciel. Comme les fournisseurs de soins de santé de première ligne, ces organisations sont des cibles attrayantes pour les cybercriminels, car leur travail est tout aussi critique et qu'elles sont en mesure de payer la rançon. En mars et avril 2020, des attaques par rançongiciel ont touché de telles organisations au Canada[24], aux États-Unis[25], au Royaume-Uni[26], en Belgique[27] et en Allemagne[28].

Influence et fraude en ligne

Nous estimons que les campagnes d'influence en ligne continueront presque certainement de répandre des mensonges et de susciter de plus en plus de scepticisme à l'égard des statistiques et des déclarations officielles concernant la pandémie de COVID-19. Selon nos estimations, le Canada ne constitue pas une cible prioritaire des activités d'influence en ligne, mais la situation pourrait changer rapidement, tout particulièrement en réponse aux tensions politiques accrues avec certains États. De plus, les États-Unis[29], le Royaume-Uni[30] et d'autres pays font l'objet de campagnes d'influence en ligne, et leurs écosystèmes d'information sont étroitement liés à celui du Canada. Des organismes canadiens de l'application de la loi mènent actuellement des enquêtes sur des liens possibles entre des attaques lancées sur des tours de téléphonie cellulaire au Canada et une théorie du complot selon laquelle la COVID-19 serait liée à la technologie 5G, théorie qui a mené à des attaques sur des tours cellulaires partout dans le monde[31]. En avril 2020, une campagne de désinformation a ciblé un groupement tactique de l'OTAN

dirigé par le Canada en Lettonie. Dans le cadre de cette campagne, on affirmait faussement que l'un des contingents était aux prises avec « un nombre élevé » de cas de COVID-19[32]. Cette activité visait presque certainement à accroître l'hostilité entre la population de la Lettonie et les forces dirigées par le Canada stationnées dans ce pays.

Les campagnes d'influence en ligne visent normalement à apaiser les auditoires nationaux mécontents de l'intervention de leur pays à l'égard de la pandémie ou à cibler les auditoires étrangers dans le but d'émousser et de contrer les critiques internationales. Il peut s'agir de propager des faussetés et de l'information faussée ou d'orienter le discours sur les médias sociaux de manière à dépeindre les gouvernements rivaux comme étant peu fiables ou parfaitement inaptes à gérer la pandémie de COVID-19. Selon un rapport publié en avril 2020 par EUvsDisinfo, un projet de l'Union européenne visant à analyser la désinformation, les activités d'influence en ligne comportent notamment la propagation de théories selon lesquelles la COVID-19 serait un canular, des propos qui contredisent les conseils officiels de l'OMS et de l'information erronée sur des traitements possibles[33]. L'objectif immédiat de ce type d'influence en ligne est de semer la confusion et la colère, de susciter la méfiance et le doute, et de nuire à la capacité des pays ciblés à gérer la pandémie. Par ailleurs, les personnes qui croient ces messages malveillants risquent de mettre leur santé et celle des autres en péril.

Les cybercriminels se sont également servis de la pandémie de COVID-19 pour annoncer la vente de fournitures médicales contrefaites[34] et demander frauduleusement des dons[35]. Le Centre antifraude du Canada a publié un avertissement dressant la liste des arnaques liées à la COVID-19, y compris des offres frauduleuses de tests de dépistage rapides de la COVID-19, de produits contrefaits qui traiteraient ou préviendraient présumément la maladie, et de fausses annonces en ligne offrant des produits de nettoyage en forte demande[36]. Le FBI a signalé plusieurs cas d'organismes gouvernementaux ayant transféré des fonds à des vendeurs frauduleux dans le but d'acheter de l'EPI, de l'équipement médical ou d'autres fournitures médicales[37]. En une semaine, INTERPOL a saisi plus de 34 000 masques contrefaits de qualité inférieure ainsi que d'autres faux produits, comme un « vaporisateur anti-coronavirus » et des « produits médicinaux contre le coronavirus », un grand nombre desquels étaient vendus en ligne[38].

La fraude a des répercussions financières immédiates sur les victimes de ces arnaques, en plus de détourner des fonds destinés aux efforts de lutte légitimes contre la COVID-19. Dans plusieurs cas, les victimes n'ont jamais reçu le produit acheté, mais dans d'autres, la distribution de produits contrefaits de qualité inférieure met en péril les efforts déployés par le secteur de la santé pour protéger son personnel et le public contre la COVID-19[39]. Nous estimons que les efforts d'intervention déployés dans le cadre de la pandémie continueront d'être minés par des activités de fraude en ligne liées à la COVID-19 en raison du détournement de ressources et de la distribution de produits contrefaits de qualité inférieure.

RESSOURCES UTILES

Pour obtenir de plus amples renseignements sur les mesures d'atténuation des cybermenaces, y compris celles visant les télétravailleurs et les leurres liées à la COVID-19, nous vous recommandons de consulter les pages Web suivantes :

- Cybermenaces pesant sur les organismes de santé canadiens (https://cyber.gc.ca/fr/avis/cybermenaces-pesant-sur-les-organismes-de-sante-canadiens)
- Avis et conseils en matière de cybersécurité à l'intention des organismes de recherche et de développement durant la pandémie de la COVID 19 (https://cyber.gc.ca/fr/orientation/avis-et-conseils-en-matiere-de-cybersecurite-lintention-des-organismes-de-recherche-et)
- Bouclier canadien – Le Centre pour la cybersécurité fournit du renseignement sur les menaces afin de protéger les Canadiens pendant la pandémie de COVID-19 (https://cyber.gc.ca/fr/bouclier-canadien-le-centre-pour-la-cybersecurite-fournit-du-renseignement-sur-les-menaces-afin-de)
- La COVID-19 et les sites web malveillants (https://cyber.gc.ca/fr/orientation/la-covid-19-et-les-sites-web-malveillants-itsap00103)
- Pratiques exemplaires en cybersécurité (https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-cybersecurite)
- Reconnaître les courriels malveillants (https://cyber.gc.ca/fr/orientation/reconnaitre-les-courriels-malveillants-itsap00100)
- La cybersécurité en mode télétravail (https://cyber.gc.ca/fr/la-cybersecurite-en-mode-teletravail)
- Conseils de cybersécurité pour le télétravail (https://cyber.gc.ca/fr/orientation/conseils-de-cybersecurite-pour-le-teletravail-itsap10116)
- Vidéoconférence (https://cyber.gc.ca/fr/orientation/videoconference-itsap10216)
- Facteurs à considérer pour l'utilisation de produits et services de vidéoconférence (https://cyber.gc.ca/fr/avis/facteurs-considerer-pour-lutilisation-de-produits-et-services-de-videoconference)
- Conseils de sécurité pour les organisations dont les employés travaillent à distance (https://cyber.gc.ca/fr/orientation/problemes-de-securite-lies-au-teletravail-itsap10016)
- Les réseaux privés virtuels (https://cyber.gc.ca/fr/orientation/les-reseaux-prives-virtuels-itsap80101)
- Exploitation active de vulnérabilités dans les réseaux privés virtuels (RPV) (https://cyber.gc.ca/fr/avis/exploitation-active-de-vulnerabilites-dans-les-reseaux-prives-virtuels-rpv)
- Comment reconnaître l'information trompeuse en ligne et ce qu'il faut faire pour y remédier (https://www.pensezcybersecurite.gc.ca/cnt/blg/pst-20181023-fr.aspx)
- Rançongiciels : comment les prévenir et s'en remettre (https://cyber.gc.ca/fr/orientation/rancongiciels-comment-les-prevenir-et-sen-remettre-itsap00099)
- Protéger l'organisme contre les maliciels (https://cyber.gc.ca/fr/orientation/proteger-lorganisme-contre-les-maliciels-itsap00057)
- Sécurité de l'internet des objets pour les petites et moyennes organisations (https://cyber.gc.ca/fr/orientation/securite-de-linternet-des-objets-pour-les-petites-et-moyennes-organisations-itsap00012)

[1] BRAGDON, Bob. « Pandemic impact report: Security leaders weigh in », *CSO,* le 1er avril 2020. [https://www.csoonline.com/article/3535195/pandemic-impact-report-security-leaders-weigh-in.html/]
[2] MICROSOFT. « Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do », *Microsoft*, le 1er avril 2020. [https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/]
[3] CENTRE CANADIEN POUR LA CYBERSÉCURITÉ. « Active Exploitation of Citrix Vulnerabilities », *Centre canadien pour la cybersécurité*, le 17 janvier 2020. [https://cyber.gc.ca/en/alerts/active-exploitation-citrix-vulnerabilities]; CENTRE CANADIEN POUR LA CYBERSÉCURITÉ. « Exploitation active de vulnérabilités dans les réseaux privés virtuels (RPV) », *Centre canadien pour la cybersécurité*, le 17 septembre 2019. [https://cyber.gc.ca/fr/avis/exploitation-active-de-vulnerabilites-dans-les-reseaux-prives-virtuels-rpv]
[4] Voir la publication précédente du CCC intitulée *Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les activités de cybermenace* (CCCS-SCTA20200427) pour prendre connaissance de l'évaluation des répercussions globales de la pandémie sur la cybersécurité. https://cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-incidence-de-la-covid-19-sur-les-activites-de.
[5] CENTRE CANADIEN POUR LA CYBERSÉCURITÉ. « Cybermenaces pesant sur les organismes de santé canadiens », *Centre canadien pour la cybersécurité*, le 20 mars 2020. [https://www.cyber.gc.ca/fr/avis/cybermenaces-pesant-sur-les-organismes-de-sante-canadiens]
[6] McCABE, Adrian, Vicky RAY et Juan CORTES. « Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns », *Palo Alto Networks, Unit 42*, le 14 avril 2020. [https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
[7] SATTER, Raphael, Jack STUBBS, and Christopher BING. « Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike », *Reuters*, le 23 mars 2020. [https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN]
[8] POLICE NÉERLANDAISE. « La police arrête un suspect pour une attaque DDoS sur MijnOverheid.nl », (Traduit de la langue d'origine). *Police néerlandaise,* le 10 abril 2020. [https://www.politie.nl/nieuws/2020/april/10/03-politie-houdt-verdachte-aan-voor-ddos-aanval-op-mijnoverheid.nl.html]
[9] UNIT 42. « 2020 Unit 42 IoT Threat Report », *Palo Alto Networks, Unit 42*, le 10 mars 2020. [https://unit42.paloaltonetworks.com/iot-threat-report-2020/]
[10] WHITTACKER, Zack. « Hackers publish ExecuPharm internal data after ransomware attack », *Tech Crunch*, le 27 avril 2020. [https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/]; ABRAMS, Lawrence. « Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic », *Bleeping Computer*, le 26 mars 2020. [https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/]
[11] ILASCU, Ionut. « COVID-19 Testing Center Hit by Cyberattack », *Bleeping Computer*, le 14 mars 2020. [https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/]
[12] TRUTA, Filip. « Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak », *Security Boulevard*, le 19 mars 2020. [https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/]
[13] INSIKT GROUP. « Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide », *Recorded Future, Insikt Group*, le 12 mars 2020. [https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf]
[14] KREBS, Brian. « Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware », *Krebs on Security*, le 6 mai 2020. [https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/]
[15] ABRAMS, Lawrence. « Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic », *Bleeping Computer*, le 26 mars 2020. [https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/]
[16] SECURITY MAGAZINE. « Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak », *Security Magazine*, le 17 mars 2020. [https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak]
[17] THOMPSON, Brandon. « IT incident under investigation at Parkview Medical Center », *Fox21 News* le 24 abril 2020. [https://www.fox21news.com/top-stories/it-incident-under-investigation-at-parkview-medical-center/]
[18] BBC. « Europe's supercomputers hijacked by attackers for cryptomining », *BBC*, le 18 mai 2020. [https://www.bbc.com/news/technology-52709660]; MUNCASTER, Phil. « Crypto-Miners Take Out Supercomputers Working on #COVID-19 », *Infosecurity Magazine*, le 18 mai 2020. [https://www.infosecurity-magazine.com/news/cryptominers-out-supercomputers/]
[19] SHIN, Eun-byeol. « Tentative de piratage dans une entreprise nationale de kits de diagnostic corona… technologie presque en fuite », (Traduit de la langue d'origine) *Hankook Ilbo*, le 31 mars 2020. [https://www.hankookilbo.com/News/Read/202003311798732396?did=NA&dtype=&dtypecode=&prnewsid=]
[20] DOFFMAN, Zak. « Chinese 'Frontline' COVID-19 Research Firm Reported Hacked: Data Now on Dark Web », *Forbes*, le 26 avril 2020. [https://www.forbes.com/sites/zakdoffman/2020/04/26/chinese-covid-19-detection-firm-just-got-hacked-data-for-sale-on-dark-web-new-report/#5b9db7395dec]

[21] WINDER, Davey. « FBI Says Foreign States Hacked Into U.S. COVID-19 Research Centers: Report », *Forbes*, le 17 avril 2020. [https://www.forbes.com/sites/daveywinder/2020/04/17/fbi-says-foreign-states-hacked-into-us-covid-19-research-centers-report/#4dbde9573c29]; CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY et NATIONAL CYBER SECURITY CENTRE. « APT Groups Target Healthcare and Essential Services », *Cybersecurity and Infrastructure Security Agency*, le 5 mai 2020. [https://www.us-cert.gov/ncas/alerts/AA20126A]; STUBBS, Jack. « Exclusive: Iran-linked Hackers Recently Targeted Coronavirus Drugmaker Gilead – sources », *Reuters*, le 8 mai 2020. [https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV]

[22] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY et NATIONAL CYBER SECURITY CENTRE. « APT Groups Target Healthcare and Essential Services », *Cybersecurity and Infrastructure Security Agency*, le 5 mai 2020. [https://www.us-cert.gov/ncas/alerts/AA20126A]

[23] FEDERAL BUREAU OF INVESTIGATION. « FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations », *Federal Bureau of Investigation*, le 13 mai 2020. [https://www.fbi.gov/news/pressrel/press-releases/fbi-and-cisa-warn-against-chinese-targeting-of-covid-19-research-organizations]

[24] McCABE, Adrian, Vicky RAY et Juan CORTES. « Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns », *Palo Alto Networks, Unit 42*, le 14 avril 2020. [https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/]

[25] U.S. SECURITIES AND EXCHANGE COMMISSION. « Form 8-K 10x Genomics, Inc.: Current report, item 7.01 », *U.S. Securities and Exchange Commission*, le 1er avril 2020. [https://sec.report/Document/0001193125-20-094606/]; WHITTACKER, Zack. « Hackers publish ExecuPharm internal data after ransomware attack », *Tech Crunch*, le 27 avril 2020. [https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/]

[26] BARTH, Bradley. « Maze ransomware attackers extort vaccine testing facility », *SC Media*, le 23 mars 2020. [https://www.scmagazine.com/home/security-news/ransomware/maze-ransomware-attackers-extort-vaccine-testing-facility/]

[27] ILASCU, Ionut. « Russian-Speaking Hackers Attack Pharma, Manufacturing Companies in Europe », *Bleeping Computer*, le 27 mars 2020. [https://www.bleepingcomputer.com/news/security/russian-speaking-hackers-attack-pharma-manufacturing-companies-in-europe/]

[28] KREBS, Brian. « Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware », *Krebs on Security*, le 6 mai 2020. [https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/]; ILASCU, Ionut. « Russian-Speaking Hackers Attack Pharma, Manufacturing Companies in Europe », *Bleeping Computer*, le 27 mars 2020. [https://www.bleepingcomputer.com/news/security/russian-speaking-hackers-attack-pharma-manufacturing-companies-in-europe/]

[29] SCOTT, Mark. « Chinese diplomacy ramps up social media offensive in COVID-19 info war », *Politico*, le 29 avril 2020. [https://www.politico.eu/article/china-disinformation-covid19-coronavirus/]

[30] BBC. « Coronavirus : Fake news crackdown by UK government », *BBC News*, le 30 mars 2020. [https://www.bbc.com/news/technology-52086284]

[31] BELLEMARE, Andrea, Jason HO et Katie NICHOLSON. « Quebec Police Investigating Possible Link Between Cell Tower Fires and 5G Coronavirus Conspiracy Theories », *CBC News*, le 8 mai 2020. [https://www.cbc.ca/news/canada/coronavirus-conspiracy-theory-5g-fires-quebec-1.5560570]

[32] BREWSTER, Murray. « Canadian-led NATO Battlegroup in Latvia Targeted by Pandemic Disinformation Campaign », *CBC News*, le 24 mai 2020. [https://www.cbc.ca/news/politics/nato-latvia-battle-group-pandemic-covid-coronavirus-disinformation-russia-1.5581248]

[33] EUvsDisinfo. « 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 / coronavirus (mise à jour 2 - 22 avril) » *EUvsDisinfo*, le 24 avril 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-coronavirus-mise-a-jour-2-22-avril/

[34] FEDERAL BUREAU OF INVESTIGATION. « FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic », *Federal Bureau of Investigation*, le 13 avril 2020. [https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic]

[35] CENTRE ANTIFRAUDE DU CANADA. « Fraude liée à la COVID-19 », *Centre antifraude du Canada*, le 9 avril 2020. [https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-fra.htm]; TOWNSEND, Mark. « Fraudsters exploiting COVID-19 fears have scammed £1.6m », *The Guardian*, le 4 avril 2020. [https://www.theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m]

[36] CENTRE ANTIFRAUDE DU CANADA. « Fraude liée à la COVID-19 », *Centre antifraude du Canada*, le 9 avril 2020. [https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-fra.htm]

[37] FEDERAL BUREAU OF INVESTIGATION. « FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic », *Federal Bureau of Investigation*, le 13 avril 2020. [https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic]

[38] DE SOUZA, Tristan. « COVID-19 Critical Infrastructure Cyber Threat Brief », *Cyjax*, le 4 mai 2020. [https://www.cyjax.com/download/covid-19-critical-infrastructure-cyber-threat-brief/]
[39] DE SOUZA, Tristan. « COVID-19 Critical Infrastructure Cyber Threat Brief », *Cyjax*, le 4 mai 2020. [https://www.cyjax.com/download/covid-19-critical-infrastructure-cyber-threat-brief/]