Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

BULLETIN SUR LES CYBERMENACES : La menace des rançongiciels en 2021

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.

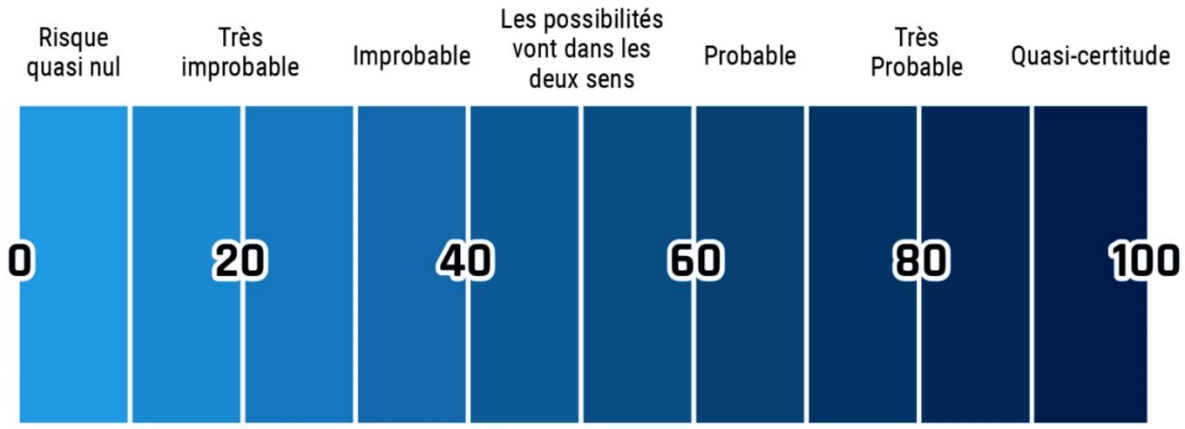
MÉTHODOLOGIE ET FONDEMENT DE L'ÉVALUATION

Les principaux 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. 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. 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 que nous soyons toujours tenus de protéger les sources et méthodes classifiées, nous fournirons au lecteur, dans la mesure du possible, les justifications qui ont motivé nos jugements.

Les jugements 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. On emploiera des termes tels que « nous estimons que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « probable » et « très probable » pour exprimer les probabilités.

Le présent document est basé sur des renseignements disponibles en date du 16 novembre 2021.

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.



LA MENACE DES RANÇONGICIELS EN 2021

L'année 2021 a été marquée par une série d'attaques par rançongiciel très médiatisées partout dans le monde. L'attaque ayant touché Colonial Pipeline aux États-Unis en a initié plusieurs aux attaques par rançongiciel et aux répercussions qu'elles peuvent avoir sur la vie de millions de personnes. Pendant cinq jours en mai dernier, cette attaque par rançongiciel a entraîné la fermeture de l'un des plus gros pipelines des États-Unis et provoqué une flambée des prix et une pénurie d'essence pour des millions d'Américains. Elle reflète certaines des principales tendances en 2021, qui a été marquée par des attaques par rançongiciel audacieuses et sophistiquées de plus en plus fréquentes et, pour les cybercriminels, très lucratives. L'ampleur et la portée des activités des opérateurs de rançongiciels posent des risques à la fois pour la sécurité et l'économie du Canada et de ses alliés.

En termes simples, un rançongiciel est un type de maliciel qui chiffre les fichiers sur un appareil. L'auteur de menace exige par la suite une rançon en échange du déchiffrement. Les rançongiciels ne sont pas un problème récent. Observées dès 1989, les attaques par rançongiciel sont devenues l'un des cybercrimes les plus courants au fil des 15 dernières années.

L'année dernière, le Centre pour la cybersécurité a publié une évaluation intitulée *Bulletin sur les cybermenaces : Le rançongiciel moderne et son évolution* dans laquelle il a fait état de l'évolution des tactiques et de l'ampleur des activités liées aux rançongiciels et présenté des prévisions selon lesquelles les attaques deviendraient de plus en plus sophistiquées et viseraient davantage des cibles de haut niveau, ce qui ferait augmenter les rançons demandées.

Malheureusement, ces prévisions se sont concrétisées. Lors de la première moitié de 2021, les attaques par rançongiciel ont augmenté de 151 % à l'échelle mondiale comparativement à la première moitié de 2020. Cette année, les rançons et les paiements ont également atteint des niveaux jamais vus[1]. Au Canada, le coût moyen estimé d'une violation de données, une catégorie de compromission qui inclut notamment les rançongiciels, s'élève à 6,35 M$ CA[2].

Le Centre pour la cybersécurité est au courant de 235 incidents liés à des rançongiciels ayant touché des victimes canadiennes du 1er janvier au 16 novembre 2021. Plus de la moitié de ces victimes étaient des fournisseurs d'infrastructures essentielles. Il importe toutefois de noter que la majorité des événements liés à des rançongiciels ne sont pas signalés. Une fois qu'elles ont été ciblées, les victimes de rançongiciels sont souvent attaquées à de multiples reprises[3]. Le Centre pour la cybersécurité continue d'observer régulièrement des campagnes d'attaques par rançongiciel qui produisent d'importantes répercussions pouvant paralyser les entreprises et les fournisseurs d'infrastructures essentielles.

Une attaque par rançongiciel est susceptible d'être dévastatrice et d'entraîner de graves répercussions financières. Les opérateurs de rançongiciels utilisent de plus en plus la tactique consistant à rendre publiques les données d'une victime si celle-ci ne paye pas la rançon[4]. En mai 2021, des renseignements sur 520 patients du Health Service Executive de l'Irlande ont été publiés en ligne à la suite d'une attaque par le rançongiciel Conti[5]. Les violations de données sont coûteuses, tant sur le plan financier que pour la réputation.

Tout au long de 2021, plusieurs hauts responsables canadiens, y compris le ministre de la Sécurité publique, la chef du CST et le dirigeant principal du Centre pour la cybersécurité, ont déclaré publiquement que les rançongiciels constituaient la plus grande menace pour la cybersécurité des Canadiens et des entreprises canadiennes[6]. En avril 2021, le Ransomware Task Force, une initiative internationale dirigée par l'Institute for Security and Technology des États-Unis en partenariat avec 60 experts en cybersécurité de l'industrie, du gouvernement, d'organismes d'application de la loi et de la société civile — y compris le Groupe national de coordination contre la cybercriminalité de la Gendarmerie royale du (GRC)— a renforcé la nécessité de déployer des efforts collectifs pour atténuer la menace des rançongiciels[7]. Le 13 octobre 2021, le Canada a participé à des réunions animées par le National Security Council de la Maison-Blanche dans le cadre de la Counter-Ransomware Initiative.

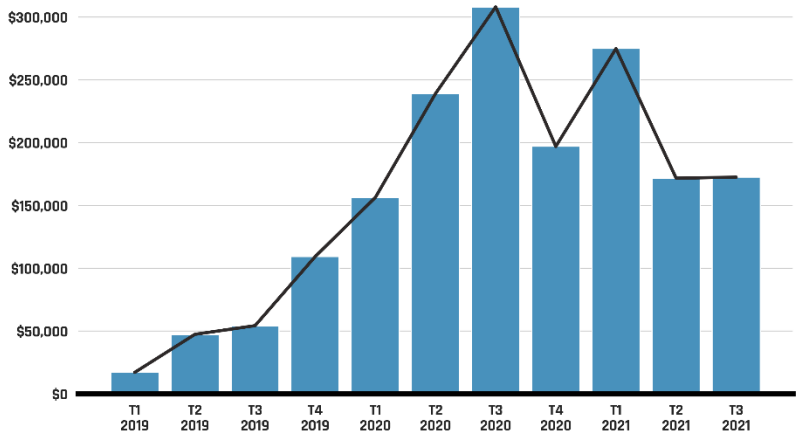
Le présent bulletin sur les cybermenaces renseigne les Canadiens sur la menace des rançongiciels au Canada et établit nos prévisions quant à l'évolution attendue de cette menace au cours de la prochaine année.

TENDANCES EN COURS D'ÉVOLUTION

Rançongiciel comme service

L'ampleur et les répercussions accrues des attaques par rançongiciel de 2019 à 2021 sont attribuables en grande partie à la croissance du modèle opérationnel du « rançongiciel comme service » (RaaS pour *Ransomware-as-a-Service*), dans le cadre duquel des développeurs vendent ou louent des rançongiciels à d'autres cybercriminels. Ces stratagèmes d'affiliation permettent à des attaquants habiles de lancer des campagnes de distribution de rançongiciels, alors que le développeur du rançongiciel en question reçoit un pourcentage de la rançon payée par chaque victime.

Figure 1 - Montant moyen des rançons payées par trimestre



Le montant des rançons connues, qui avait augmenté rapidement de 2019 à 2020, semble s'être stabilisé à environ 200 000 $ en 2021, une légère baisse par rapport aux sommes de 2020 (voir la figure 1)[8]. En revanche, à l'échelle mondiale en 2021, le coût total moyen des activités de reprise à la suite d'une attaque par rançongiciel (c'est-à-dire le coût de la rançon payée et/ou du rétablissement du réseau compromis) a plus que doublé, en passant de 970 722 $ CA en 2020 à 2,3 M$ CA en 2021[9]. **Nous estimons que le marché des rançons a probablement atteint un point d'équilibre : les auteurs de menace arrivent de mieux en mieux à adapter leurs demandes aux montants que leurs victimes sont sujettes à payer compte tenu de l'augmentation des coûts de reprise et du risque de subir une atteinte à la réputation si leurs données étaient divulguées.** De nombreux groupes d'opérateurs de rançongiciels sophistiqués continuent de demander aux grandes entreprises et aux fournisseurs d'infrastructures essentielles des sommes de plus en plus exorbitantes. La rançon la plus élevée jamais payée – 48,4 M$ CA – a d'ailleurs été versée en 2021[10].

Activités fortement ciblées

Le 2 juillet 2021, le groupe Sodinokibi (également connu sous le nom de « REvil »), un groupe de cybercriminels qui parlent russe et qui exploitent le rançongiciel du même nom, a tiré profit d'une vulnérabilité liée à Kaseya VSA, un logiciel de gestion de réseau, pour compromettre de 800 à 1500 organisations en aval. Le rançongiciel a été déployé sur les réseaux des victimes compromises par le biais d'une mise à jour logicielle falsifiée et malveillante[11]. **À notre avis, il est probable que les opérateurs de rançongiciels continuent de cibler les chaînes d'approvisionnement de logiciels afin de maximiser le nombre de victimes potentielles et les profits.** Nous avons également constaté que certains cybercriminels ont abandonné les campagnes automatisées génériques et arbitraires pour se tourner vers des attaques plus ciblées qui nécessitent l'intervention active d'un pirate.

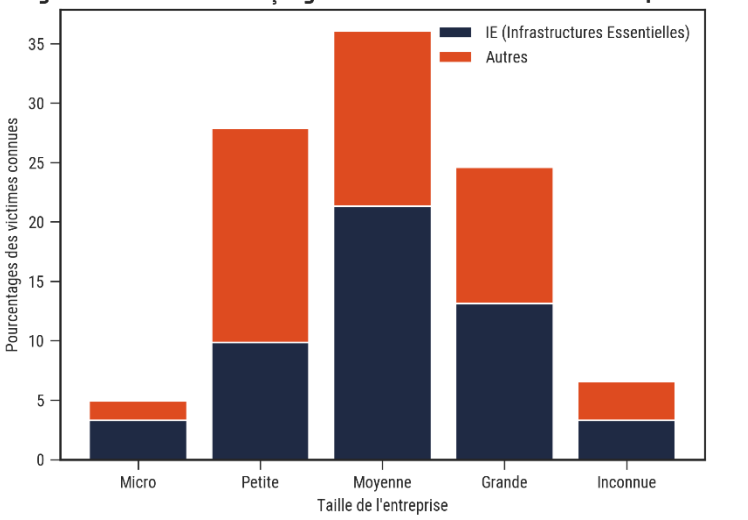
Comme dans d'autres crimes à motivation financière, les opérateurs de rançongiciels cherchent à maximiser leurs profits. Bien que les attaques contre de grandes cibles mieux défendues exigent plus de temps et d'expertise, les grandes organisations continuent d'être ciblées, car elles sont mieux en mesure de payer des rançons élevées, ce qui en fait des cibles lucratives pour les opérateurs de rançongiciels habiles. Comme l'a affirmé la chef du CST en mai 2021, « Les infrastructures essentielles et les grandes entreprises sont les cibles les plus lucratives des rançongiciels, car elles sont moins en mesure de tolérer une perturbation de leurs activités et peuvent compter sur d'importantes ressources financières »[12].

Du 1er janvier au 30 juin 2021, plus de la moitié des victimes canadiennes touchées par une attaque par rançongiciel faisaient partie d'un secteur d'infrastructures essentielles, comme les secteurs de l'énergie et de la santé et le secteur manufacturier. Dans le contexte de la pandémie de COVID-19, des organisations comme les hôpitaux, les gouvernements et les universités étaient plus conscientes des risques associés à la perte de l'accès à leurs réseaux et se résignaient souvent à payer la rançon. Les cybercriminels en ont profité pour demander des rançons beaucoup plus fortes.

Nous estimons que les opérateurs de rançongiciels continueront presque certainement de cibler de grandes organisations possédant des biens de technologie opérationnelle (TO), y compris des organisations au Canada, dans le but de tenter d'obtenir des rançons, de voler de la propriété intellectuelle et des informations commerciales exclusives, et de mettre la main sur les renseignements personnels de clients. Même si la cyberactivité touche le réseau de technologie de l'information (TI) du propriétaire d'un bien de TO, la TO pourrait elle aussi être mise hors service[13]. Par exemple, en mai 2021, Colonial Pipeline, qui exploite l'un des plus grands pipelines de produits raffinés aux États-Unis, a été victime d'un incident attribué à Darkside, un groupe de cybercriminels basé en Russie qui offre des services

RaaS. Bien que l'incident n'aurait touché que les systèmes de TI, il a nui aux activités de l'entreprise, ce qui a engendré une hausse record des prix, des achats dictés par la panique et une pénurie d'essence[14].

Figure 2 - Victimes de rançongiciels connues selon les sites de « punition »



Tirer profit de la pandémie de COVID-19

Les groupes d'opérateurs de rançongiciels ciblent également de plus en plus les services médicaux d'urgence et les organismes d'application de la loi, qui peinent à gérer la pandémie de COVID-19. Par exemple, le 14 juin 2021, l'hôpital Humber River, en Ontario, a dû arrêter ses systèmes de TI afin de prévenir une attaque par rançongiciel. Le personnel n'avait donc plus accès aux dossiers électroniques des patients ni aux résultats de tests de diagnostic, ce qui a rallongé le temps d'attente au service des urgences. De plus, l'hôpital a dû annuler divers services de clinique et rediriger des ambulances à d'autres hôpitaux[15].

Comme l'indique la figure 2, d'après des blogues de « punition » (*name and shame*) liés à des rançongiciels (des sites Web où les cybercriminels divulguent les données des victimes qui ont refusé de payer la rançon), près des deux tiers des victimes canadiennes touchées par ce type de rançongiciel du 1er janvier au 30 juin 2021 étaient de petites et moyennes organisations. Depuis mars 2020, près du quart des petites entreprises canadiennes – un grand nombre desquelles ont dû utiliser davantage des plateformes en ligne durant la pandémie de COVID-19 – ont été victimes d'un cyberincident malveillant[16]. **Nous estimons que ce nombre est probablement plus élevé que les incidents signalés.**

CATALYSEURS DE RANÇONGICIELS

Les rançons sont demandées en cryptomonnaies, car celles-ci sont très accessibles et difficiles à retracer. Au cours des six premiers mois de 2021, les rançons payées en cryptomonnaie à la suite d'attaques par rançongiciel s'élevaient à 590 M$ US, une augmentation par rapport aux 416 M$ US signalés pour l'ensemble de 2020[17]. Bien que le bitcoin ait longtemps été le mode de paiement de choix et continue de prédominer dans les demandes de rançon, **nous estimons qu'il est très probable que les cybercriminels demanderont de plus en plus les rançons en cryptomonnaies anonymes, comme le Monero, pour masquer davantage leur identité et leurs activités dans le but de déjouer les organismes d'application de la loi.**

Les cryptomonnaies anonymes comme le Monero permettent aux cybercriminels de contourner plus facilement certains outils et mécanismes de suivi pris en charge par la chaîne de blocs du bitcoin et d'autres cryptomonnaies populaires. En mars 2021, une attaque par rançongiciel ayant ciblé le fabricant d'ordinateurs Acer, basé à Taïwan, a donné lieu à la demande de rançon la plus élevée jamais connue : 50 millions de dollars US en Monero[18]. Sodinokibi a retiré l'option de paiement en bitcoins et exige exclusivement des paiements en Monero[19]. Les opérateurs de rançongiciels utilisent également les cryptomonnaies pour payer les fournisseurs tiers desquels ils dépendent pour mener leurs attaques, notamment les services de tests d'intrusion, les vendeurs d'exploits et les fournisseurs d'hébergement à toute épreuve.

Les attaquants qui utilisent des rançongiciels investissent la majorité des fonds qu'ils extorquent à leurs victimes dans les bourses d'échange de cryptomonnaies conventionnelles, les bourses d'échange à haut risque (dont les normes de conformité sont faibles ou absentes) et des mélangeurs (des services qui permettent aux utilisateurs de mêler leurs monnaies à celles d'autres utilisateurs) afin de blanchir et d'encaisser leurs revenus.

De plus, la vente commerciale de cyberoutils, à laquelle s'ajoute un bassin mondial de talents, a fait augmenter le nombre d'auteurs de cybermenace et donné lieu à des attaques plus sophistiquées. Par exemple, des auteurs de cybermenace se sont approprié Cobalt Strike, un outil commercial servant à tester la sécurité réseau, dans le but de faciliter des activités cybercriminelles sophistiquées et, très probablement, des campagnes de cyberespionnage parrainées par des États. L'utilisation de Cobalt Strike à des fins malveillantes a augmenté de 161 % de 2019 à 2020 et continue de représenter une menace importante en 2021[20]. Des opérateurs de rançongiciels et leurs collaborateurs continuent de recruter des programmeurs sur des sites Web de travail à la pige, y compris des candidats d'expérience qui connaissent bien les outils utilisés par des testeurs d'intrusion légitimes, comme Cobalt Strike[21]. Les marchés en ligne servant à la vente d'outils et de services illicites ont également permis aux cybercriminels de mener des activités plus complexes et sophistiquées.

LIEN ENTRE ÉTATS ET RANÇONGICIELS

Nous estimons toujours qu'il est probable que des auteurs de cybermenace parrainés par des États continueront d'utiliser des rançongiciels pour brouiller les origines ou les intentions de leurs cyberopérations. Il y a plusieurs exemples de ce type d'activité. En 2019, des individus responsables d'activités de cybermenace parrainées par la Chine ont été accusés d'avoir mené des activités à motivations explicitement financières, notamment au moyen de rançongiciels[22]. Selon un rapport de tierce partie de l'industrie, de la fin juillet 2020 au début septembre 2020, le Corps des Gardiens de la révolution islamique (CGRI) de l'Iran a mené une campagne d'attaques par rançongiciel parrainée par l'État par l'intermédiaire d'une entreprise de sous-traitance iranienne, en imitant les tactiques, techniques et procédures (TTP) de groupes d'opérateurs de rançongiciels à motivations financières dans le but d'éviter que la campagne lui soit attribuée et de maintenir le déni plausible[23].

Nous estimons qu'il est presque certain que les services de renseignement et les organismes d'application de la loi russes entretiennent des relations avec des cybercriminels, soit en s'associant à ceux-ci, soit en les recrutant, et leur permettent de mener leurs activités avec une impunité quasi totale, à condition qu'ils dirigent leurs attaques sur des cibles à l'extérieur de la Russie et de l'ancienne Union soviétique. Par conséquent, un grand nombre des variants de rançongiciels les plus sophistiqués et prolifiques sont opérés par des cybercriminels basés en Russie. En 2019, le département de la Justice des États-Unis a porté des accusations contre Maksim Yakubets, dirigeant du groupe cybercriminel EvilCorp basé en Russie, pour avoir contribué directement aux cyberefforts malveillants de la Fédération de Russie[24]. En avril 2021, le département du Trésor des États-Unis a déclaré que le Service fédéral de sécurité (FSB) de la Russie appuie et mobilise des cybercriminels, y compris EvilCorp, ce qui permet à ceux-ci de lancer des attaques par rançongiciel perturbatrices[25].

À la suite du sommet entre les États-Unis et la Russie en juin 2021, les groupes cybercriminels DarkSide et Sodinokibi — qui étaient responsables d'une série d'attaques par rançongiciel contre Colonial Pipeline, JBS USA et Kaseya — ont mis leur infrastructure hors service et cessé leurs activités. Toutefois, en septembre 2021, les groupes BlackMatter — successeur de plusieurs groupes d'opérateurs de rançongiciels, y compris DarkSide — et Sodinokibi avaient refait surface et repris leurs activités malveillantes. Or, Sodinokibi a été mis hors service en octobre 2021 lorsque ses serveurs ont été compromis dans le cadre d'une opération menée par plusieurs pays et dirigée par les États-Unis[26]. Le groupe BlackMatter avait d'abord affirmé qu'il ne permettrait pas que son rançongiciel soit déployé contre des infrastructures essentielles, mais il est revenu sur cette promesse depuis[27].

PRÉVISIONS

Malgré l'accalmie temporaire à la suite de mesures internationales, nous estimons que les attaques par rançongiciel continueront de poser une menace pour la sécurité nationale et la prospérité économique du Canada et de ses alliés en 2022, car il s'agit d'activités lucratives pour les cybercriminels. Pour atténuer les risques accrus, il faudra déployer des efforts concertés à l'échelle nationale pour améliorer la cybersécurité et adopter des pratiques exemplaires visant à renforcer les systèmes essentiels, de même que prendre des mesures coordonnées à l'échelle internationale afin de miner l'infrastructure et les tactiques des criminels.

Par exemple, le 27 janvier 2021, une coalition mondiale d'organismes d'application de la loi des États-Unis, du Canada, du Royaume-Uni, des Pays-Bas, de l'Allemagne, de la France, de la Lituanie et d'Ukraine, en collaboration avec des chercheurs en sécurité du secteur privé, a perturbé l'infrastructure d'Emotet – un réseau zombie utilisé par les cybercriminels pour déployer des rançongiciels – et s'est emparée des serveurs de commande et de contrôle de ce dernier. Au moins deux des membres du groupe de cybercriminels ont également été arrêtés en Ukraine[28]. Le même jour, le département de la Justice des États-Unis a porté des accusations contre un ressortissant canadien associé à des attaques par le rançongiciel NetWalker[29].

Nous estimons que les opérateurs de rançongiciels cibleront probablement des victimes de plus en plus importantes, y compris des infrastructures essentielles. La réponse collective visant à contrer l'épidémie d'attaques par rançongiciel consiste notamment à limiter la mesure dans laquelle les cybercriminels peuvent se réfugier dans des pays où ils sont à l'abri des conséquences, comme la Russie[30]. De nombreux opérateurs de rançongiciels et leurs collaborateurs se trouvent dans des pays où les lois et l'application de la loi contre la cybercriminalité sont laxistes ou inexistantes et ils continuent de cibler le Canada, les États-Unis et d'autres alliés. Par exemple, à la suite de l'attaque par rançongiciel lancée en juin 2021 par Sodinokibi contre JBS USA, la plus grande compagnie de conditionnement de la viande du monde, un porte-parole du groupe de cybercriminels basé en Russie a déclaré que Sodinokibi ne s'empêcherait pas de lancer d'autres attaques contre les États-Unis[31]. Un mois plus tard, le 2 juillet 2021, Sodinokibi a compromis la chaîne d'approvisionnement liée à Kaseya VSA dans le cadre de l'attaque par rançongiciel la plus importante de l'histoire.

Les cybercriminels continuent presque certainement d'avoir recours aux monnaies électroniques pour faciliter leurs opérations de rançongiciels. Dans le cadre des efforts internationaux visant à contrer les rançongiciels, on renforce également la surveillance et la réglementation des bourses de cryptomonnaies qui ne signalent pas les transactions suspectes, en mettant l'accent sur les services de

mélangeurs qui dissimulent les transactions criminelles dans le trafic local[32]. Par exemple, en septembre 2021, le département du Trésor des États-Unis a imposé des sanctions à la plateforme d'échange virtuelle de cryptomonnaie Suex pour son rôle dans la facilitation des paiements liés aux rançongiciels[33]. Les mesures visant à entraver les activités des opérateurs de rançongiciels s'apparenteraient à celles employées par les institutions financières depuis plusieurs années pour lutter contre le blanchiment d'argent, le trafic de stupéfiants et le financement du terrorisme, notamment l'établissement et l'adoption de politiques sur la « règle de la connaissance du client » et la présentation de rapports sur les activités suspectes[34].

Alors que le Canada et la communauté internationale poursuivent les efforts visant à perturber les éléments qui encouragent les cybercriminels à lancer des attaques par rançongiciel et qui leur permettent d'extorquer de l'argent à leurs victimes, la menace que posent les rançongiciels continuera fort probablement de s'accroître et d'évoluer de manière à entraîner des répercussions considérables sur les organisations et les infrastructures essentielles du Canada et de ses partenaires internationaux.

L'ampleur, la fréquence et le degré de sophistication des attaques par rançongiciel continueront presque certainement de s'accroître, mais il est possible de prévenir la grande majorité de ces attaques en prenant des mesures de cybersécurité de base. À titre d'autorité technique nationale en matière de cybersécurité au Canada, le Centre pour la cybersécurité met en place d'importantes ressources qui permettent aux Canadiens et aux organisations canadiennes d'atténuer la menace des rançongiciels. Consultez notre page Web sur les rançongiciels ou communiquez avec le Centre pour la cybersécurité à contact@cyber.gc.ca pour en savoir plus.

---

[1] *Ransomware Volumes Hit Record Highs as 2021 Wears On*, Threatpost, 3 août 2021. https://threatpost.com/ransomware-volumes-record-highs-2021/168327/

[2] *Rapport 2021 sur le coût d'une violation de données*, IBM, le 28 juillet 2021. https://www.ibm.com/fr-fr/security/data-breach

[3] *The Hiscox Cyber Readiness Report 2021*, Hiscox, avril 2021. https://www.hiscox.co.uk/cyberreadiness

[4] *Another Ransomware Will Now Publish Victims' Data If Not Paid*, Bleeping Computer, 12 décembre 2019. https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid

[5] *HSE Confirms Data of 520 Patients Published Online*, The Irish Times, 28 mai 2021. https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136

[6] Bill Blair, ministre de la Sécurité publique, Five Country Ministerial Statement Regarding the Threat of Ransomware, 8 avril 2021; *Enhancing Cybersecurity Readiness in an Era of Digital Disruption: A Discussion with Shelly Bruce, Chief, Communications Security Establishment*, 18 mai 2021; Scott Jones, ancien dirigeant principal du Centre canadien pour la cybersécurité, Comité permanent des opérations gouvernementales et des prévisions budgétaires, 31 mai 2021.

[7] *Combatting Ransomware*, Ransomware Task Force, 29 avril 2021. https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

[8] *Ransomware Recovery Blog*, Coveware, consulté le 9 novembre 2021. https://www.coveware.com/blog

[9] *The State of Ransomware 2021*, Sophos, 27 avril 2021. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

[10] *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, Bloomberg, 20 mai 2021. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[11] *Updated Kaseya Ransomware Attack FAQ: What We Know Now*, ZDNet, 23 juillet 2021. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

[12] « Améliorer la préparation à la cybersécurité à l'ère des perturbations numériques : une discussion avec Shelly Bruce, chef du Centre de la sécurité des télécommunications », 18 mai 2021.

[13] *Ransomware Against the Machine: How Adversaries Are Learning to Disrupt Industrial Production by Targeting IT and OT*, FireEye, 24 février 2020. https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html

[14] Krauss, C., N. Chokshi et D.E. Sanger. *Gas Pipeline Hack Leads to Panic Buying in the Southeast*, New York Times, 11 mai 2021. https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html

[15] *Cyberattack leads to computer system failure at Humber River Hospital, impacting patient care*, Toronto Star, 15 juin 2021. https://www.thestar.com/news/gta/2021/06/15/computer-system-failure-at-humber-river-hospital-impacts-patient-care.html

[16] *Small Businesses were Forced Online Because of the Pandemic — Now a Quarter Say They've Experienced a Cyber Attack*, Toronto Star, 4 février 2021. https://www.thestar.com/business/2021/02/04/small-businesses-pivoting-online-because-of-covid-19-are-vulnerable-to-cyber-attacks-cfib-report.html
[17] *U.S. Treasury Puts Crypto Industry on Notice over Rising Ransomware Attacks*, Reuters, 15 octobre 2021. https://www.reuters.com/business/finance/us-treasury-warns-crypto-industry-preventing-sanctions-violations-2021-10-15/
[18] *Computer Giant Acer Hit by $50 Million Ransomware Attack*, Bleeping Computer, 19 mars 2021. https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/
[19] *Monero Emerges as Crypto of Choice for Cybercriminals*, Financial Times, 22 juin 2021. https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6
[20] *Cobalt Strike: Favorite Tool from APT to Crimeware*, Proofpoint, 29 juin 2021. https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware
[21] *Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work*, Krebs on Security, 8 octobre 2020. https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/
[22] *Justice Department Charges Five Chinese Members of APT41 over Cyberattacks on US Companies*, TechCrunch, 16 septembre 2020. https://techcrunch.com/2020/09/16/justice-department-charges-apt41-chinese-hackers/
[23] *A Second Iranian State-sponsored Ransomware Operation "Project Signal" Emerges*, Flashpoint, 30 avril 2021.
[24] *Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses*, département de la Justice des États-Unis, 5 décembre 2019. https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens
[25] *Treasury Sanctions Russia with Sweeping New Sanctions Authority*, département du Trésor des États-Unis, 15 avril 2021. https://home.treasury.gov/news/press-releases/jy0127
[26] *Governments Turn Tables on Ransomware Gang REvil by Pushing it Offline*, Reuters, 21 octobre 2021. https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.
[27] *BlackMatter Strikes Iowa Farmers Cooperative, Demands $5.9M Ransom*, Threatpost, 21 septembre 2021. https://threatpost.com/blackmatter-strikes-iowa-farmers-cooperative-demands-5-9m-ransom/174846/
[28] *Cops Disrupt Emotet, the Internet's "Most Dangerous Malware"*, Wired, 27 janvier 2021. https://www.wired.com/story/emotet-botnet-takedown/
[29] *Canadian man charged in U.S. with NetWalker ransomware attacks*, Toronto Star, 27 janvier 2021. https://www.thestar.com/news/canada/2021/01/27/canadian-man-charged-in-us-with-netwalker-ransomware-attacks.html
[30] *How the Kremlin provides a safe harbor for ransomware*, Associated Press, 6 avril 2021. https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999
[31] *REvil Ransomware Gang Spill Details on US Attacks*, Threatpost, 4 juin 2021. https://threatpost.com/revil-spill-details-us-attacks/166669/
[32] *The Ransomware Problem Is a Bitcoin Problem*, Lawfare, 27 mai 2021. https://www.lawfareblog.com/ransomware-problem-bitcoin-problem
[33] *Treasury Takes Robust Actions to Counter Ransomware*, département du Trésor des États-Unis, 21 septembre 2021. https://home.treasury.gov/news/press-releases/jy0364
[34] *How A New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back*, NPR, 8 juin 2021. https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac

CAT. D96-78/2021F-PDF
ISBN 978-0-660-41161-3

Centre de la sécurité des télécommunications Communications Security Establishment

Canada