TLP:WHITE

Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

# BULLETIN SUR LES CYBERMENACES

## Le rançongiciel moderne et son évolution

**18 SEPTEMBRE 2020**





TLP:WHITE

Canada

# À PROPOS DU PRÉSENT DOCUMENT

## PUBLIC CIBLE

Le présent bulletin sur les cybermenaces est destiné à la collectivité de la cybersécurité. Tout en étant assujettie 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, prière de consulter la page Web https://www.first.org/tlp/

## COORDONNÉES

Pour toute question ou tout problème relatif au présent document, écrivez au Centre canadien pour la cybersécurité à contact@cyber.gc.ca.

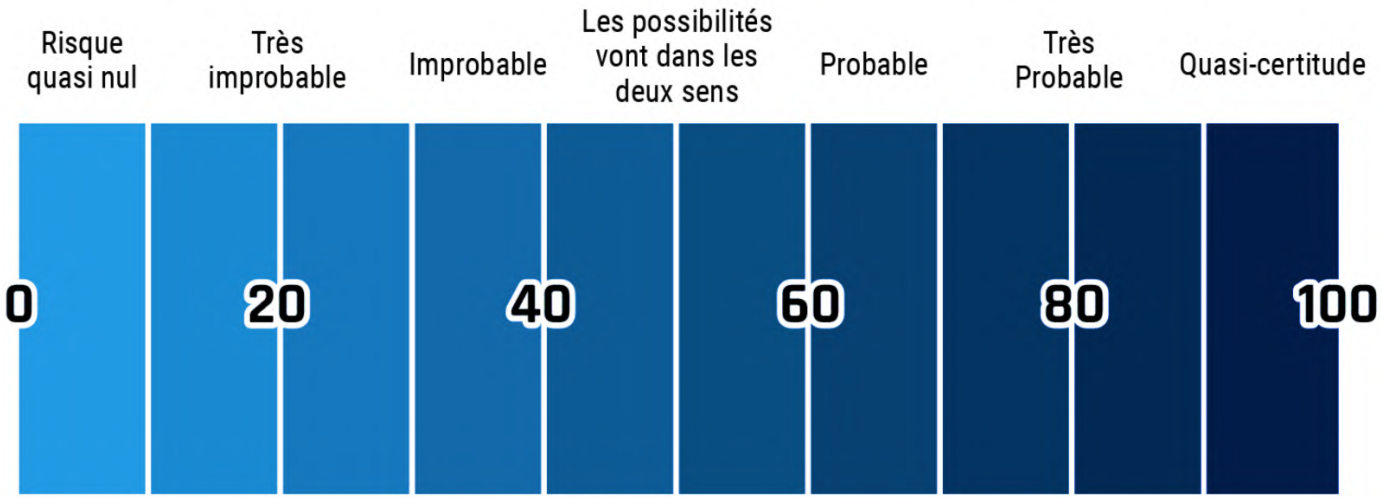
## MÉTHODOLOGIE ET FONDEMENT DE L'ÉVALUATION

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 Centre canadien 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. Dans le cadre du volet de renseignement étranger du mandat du CST, 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 tenu de toujours protéger ses sources et méthodes classifiées, il s'efforce de justifier le plus possible ses jugements.

Les principaux jugements 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 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 13 août 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

- Le Canada se classe souvent parmi les principaux pays touchés par les rançongiciels, bien que les comparaisons internationales soient limitées par les lacunes dans les données et l'asymétrie des méthodologies. De plus, le Centre pour la cybersécurité estime qu'il est presque certain qu'une majorité d'attaques de rançongiciels contre des victimes canadiennes ne sont pas signalées aux autorités.
- Au cours des deux dernières années, les campagnes de rançongiciels ont touché des centaines d'entreprises canadiennes et de fournisseurs d'infrastructures essentielles, y compris de nombreux hôpitaux et services de police, ainsi que des administrations municipales, provinciales et territoriales.
- Le Centre pour la cybersécurité estime qu'il est presque certain que les rançongiciels dirigés contre le Canada au cours des 12 prochains mois continueront de cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles, ainsi que les organisations de toutes tailles. De nombreuses victimes canadiennes continueront d'accepter les demandes de rançon en raison des graves conséquences économiques et potentiellement destructrices du refus de paiement.
- Il y a tout lieu de croire que les cybercriminels continueront d'intensifier l'exploitation de rançongiciels et qu'ils tenteront de forcer les victimes à verser des sommes plus importantes en menaçant de divulguer ou de vendre leurs données en ligne.
- Les rançongiciels modernes dépendent de plusieurs technologies (p. ex. les cryptomonnaies) et de services disponibles sur les marchés criminels en ligne, et sans eux, nous estimons avec quasi-certitude que les rançongiciels seraient prohibitifs pour les cybercriminels.
- Le succès des rançongiciels modernes dépend des lieux où les lois et l'application de la loi contre la cybercriminalité sont laxistes ou inexistantes. Nous estimons qu'il serait beaucoup plus difficile pour les cybercriminels d'exploiter des rançongiciels s'ils ne pouvaient trouver de lieux leur permettant de mener leurs activités en toute impunité.
- Nous estimons qu'il est probable que les auteurs de cybermenaces de plusieurs États utiliseront des rançongiciels pour brouiller les origines ou les intentions de leurs cyberopérations. De plus, de nombreux États entretiennent presque certainement des liens avec des cybercriminels qui utilisent des rançongiciels. Dans certains cas, les cybercriminels fournissent de l'aide aux services de renseignement, ce qui leur permet de mener leurs activités à l'abri des forces de l'ordre.

## INTRODUCTION

Le rançongiciel est une forme de maliciel qui utilise le chiffrement pour perturber des systèmes de technologie de l'information (TI), habituellement pour entraver les fonctions organisationnelles qui dépendent d'un accès sans entrave aux données. Ces tâches peuvent être essentielles à la sécurité humaine ou à la continuité des activités, et une fois celles-ci perturbées, les auteurs de menaces extorquent à leurs victimes un paiement pour déchiffrer les données. En 2019, des cybercriminels auraient tenté d'extorquer environ 25 milliards de dollars canadiens à des victimes partout dans le monde en utilisant des rançongiciels[i]. Ce montant s'ajoute aux coûts liés aux temps d'arrêt, à la corruption de données, au vol de données et à d'autres dépenses.

En 2019, les campagnes de rançongiciels ont touché des centaines d'entreprises canadiennes et de fournisseurs d'infrastructures essentielles, y compris plusieurs hôpitaux et services de police, ainsi que des administrations municipales, provinciales et territoriales. Bien que les comparaisons internationales soient limitées par les lacunes dans les données et

l'asymétrie des méthodologies, le Canada se classe souvent parmi les principaux pays touchés par les rançongiciels. Par exemple, en 2019, les soumissions du Canada au service ID Ransomware — un portail en ligne qui fournit de l'information et des outils de déchiffrement, lorsqu'ils sont disponibles, aux victimes de rançongiciels — étaient étroitement comparables, par habitant, aux chiffres des soumissions d'autres pays ciblés, comme l'Australie, l'Italie, l'Allemagne et la France[ii]. Nous estimons que le niveau élevé de ciblage du Canada est probablement attribuable à une combinaison du niveau élevé d'utilisation d'Internet pour des services bancaires et d'autres services, de la richesse relativement élevée des entreprises et des particuliers canadiens, et de la facilité avec laquelle des Canadiens se résignent à payer des rançons pour retrouver leurs données.

L'exploitation des rançongiciels évolue continuellement, et la tendance la plus récente est de cibler des organisations d'importance stratégique, comme celles qui s'occupent des infrastructures essentielles, de la défense nationale ou des technologies liées à la sécurité nationale.

## PRINCIPAUX EXPLOITANTS DE RANÇONGICIELS ET LEURS VARIANTES

| | |
|---|---|
| **CRYPTO LOCKER** | Il s'agit d'un rançongiciel créé en 2013 par le cybercriminel russe Evgeniy Bogachev. Il est considéré comme la première variante moderne de rançongiciel, distribué par le maliciel GameOverZeus et les exploitants comprenaient des membres de Bogachev et d'Evil Corp. |
| **EVIL CORP** | Evil Corp est un groupe de cybercriminels organisés basé en Russie. Il est responsable du maliciel Dridex et des multiples campagnes de rançongiciels menées depuis 2015. En décembre 2019, les membres d'Evil Corp ont été inculpés et sanctionnés par les États-Unis pour leurs activités cybercriminelles continues et pour avoir aidé un service de renseignement russe. |
| **FIN6** | FIN6 est un groupe de cybercriminels organisés, probablement russophone, qui aurait été lié à de multiples infections à Ryuk et à Megacortex depuis 2018, mais actif depuis 2015. |
| **MAZE** | Il s'agit d'une variante de rançongiciel dont les exploitants sont connus pour divulguer des données concernant les victimes lorsqu'elles refusent de payer. Actif depuis au moins novembre 2019. |
| **MEGA CORTEX** | Il s'agit d'une variante de rançongiciel découverte en 2019 qui ciblait les processus des systèmes de contrôle industriels; elle est apparemment liée aux opérations Trickbot et FIN6. |
| **RYUK** | Il s'agit d'une variante de rançongiciel connue pour cibler les grandes entreprises, les hôpitaux et les infrastructures essentielles et qui demande des rançons extrêmement élevées. Actif depuis août 2018. Ryuk est affilié à plusieurs cybercriminels russophones, dont les exploitants de Trickbot. |
| **SAMSAM** | Il s'agit d'une variante de rançongiciel utilisée par des cybercriminels iraniens qui a compromis plusieurs municipalités, hôpitaux, universités et entreprises au Canada, aux États-Unis, au Royaume-Uni et dans d'autres pays, principalement en 2015-2018. |
| **SODINOKIBI** | Il s'agit d'une variante de rançongiciel et les développeurs russophones embauchent d'autres cybercriminels pour distribuer et déployer leur rançongiciel. |
| **TRICKBOT** | Il s'agit d'un cheval de Troie du système bancaire utilisé pour voler des données financières et des justificatifs d'identité bancaire en ligne. Trickbot est affilié à plusieurs cybercriminels russophones et il est l'un des principaux distributeurs du rançongiciel Ryuk. |

## BREF HISTORIQUE DES RANÇONGICIELS

### *De la preuve de concept à l'automatisation*

Bien que la preuve de concept des rançongiciels soit apparue dès 1989, la première campagne moderne est généralement attribuée au rançongiciel CryptoLocker, administré par le cybercriminel russe Evgeniy Bogachev et ses associés en 2013. Bogachev a utilisé CryptoLocker pour exploiter encore davantage les victimes de son autre création, le tristement célèbre maliciel GameOverZeus. De septembre 2013 à mai 2014, selon les rapports du FBI, CryptoLocker a infecté près de 500 000 victimes et permis d'engranger jusqu'à 27 millions de dollars canadiens[iii].

De 2014 à 2016, le modèle de rançongiciels CryptoLocker — généralement des courriels avec des pièces jointes malveillantes distribuées au moyen de campagnes de diffusion — a proliféré, en particulier au sein de la communauté de la cybercriminalité russophone, composée de nombreux anciens associés de Bogachev. Ces campagnes précoces de rançongiciels exigeaient généralement de 500 $ à 3 000 $ CA par rançon et misaient sur l'échelle de diffusion parce que relativement peu de victimes finiraient par payer. Les auteurs de menaces se sont rendu compte que les coûts de main-d'œuvre requis pour parvenir à des compromis et extorquer des paiements de la part de chaque victime étaient trop élevés et se sont tournés vers des processus automatisés pour réduire les coûts et accroître les profits. Les rançongiciels ont évolué et sont devenus en grande partie automatisés, et cloisonnent les victimes dans un processus d'extorsion et de paiement. Les auteurs de menaces ont également intégré d'autres techniques pour augmenter les chances de paiement. Par exemple, ils ont mis en place un service de clavardage en direct 24 heures sur 24, 7 jours sur 7 et offrent de déchiffrer un ou plusieurs fichiers gratuitement pour garantir que le déchiffrement est possible. Ils ont pu ainsi procurer aux victimes hésitantes l'éclairage et l'assurance dont elles avaient besoin pour payer.

### *Des campagnes dispersées à la recherche de cibles de grande valeur*

Les rançongiciels ont évolué au fur et à mesure que les auteurs de menaces ont délaissé les campagnes automatisées diffuses de rançongiciels au profit du ciblage manuel de grandes organisations. Bien que les coûts de ces opérations aient été plus élevés, les auteurs de menaces ont appris que les grandes organisations étaient plus disposées à verser des rançons beaucoup plus élevées pour se remettre des perturbations le plus rapidement possible. En décembre 2015, des cybercriminels iraniens ont commencé à cibler des hôpitaux, des municipalités et des institutions publiques du Canada, du Royaume-Uni et des États-Unis au moyen d'un rançongiciel connu sous le nom de SamSam, qui a extorqué plus de 7,8 millions de dollars canadiens à plus de 200 victimes en novembre 2018, y compris l'Université de Calgary[iv]. SamSam est devenu un modèle pour les campagnes de rançongiciels ciblées d'aujourd'hui. Aussi connues sous le nom de « Big Game Hunting », les attaques ciblées de rançongiciels ont touché des milliers de fournisseurs de soins de santé et d'autres fournisseurs d'infrastructures essentielles, des gouvernements et de grandes entreprises. En mars 2019, une entreprise d'aluminium norvégienne a fermé ses installations de production en raison d'une attaque ciblée de rançongiciels qui a causé des dommages de près de 100 millions de dollars canadiens[v].

Aujourd'hui, les cybercriminels qui réussissent dans le créneau des rançongiciels sont en mesure de développer et d'adapter rapidement leurs logiciels malveillants pour tirer parti des contextes mondiaux, nationaux ou régionaux en évolution, et des changements qui en découlent dans les vulnérabilités de certaines organisations. En mars 2020, pendant la pandémie de COVID-19, une campagne de rançongiciels a frappé 11 hôpitaux américains; le même groupe avait ciblé trois hôpitaux canadiens et une administration municipale canadienne à l'automne 2019[vi].

## LES FACTEURS HABILITANTS DES RANÇONGICIELS MODERNES

Les rançongiciels modernes dépendent de plusieurs technologies (p. ex. les cryptomonnaies) et de services disponibles sur les marchés criminels en ligne, et sans eux, nous estimons avec quasi-certitude que les rançongiciels seraient prohibitifs pour les cybercriminels. Les rançongiciels ont suivi l'évolution de secteurs légitimes de l'économie, comme le secteur financier, pour profiter de la chute des coûts de stockage de données et informatiques, de l'augmentation de la bande passante et de la connectivité, et de la création d'une économie de services fondée sur Internet. Cependant, contrairement aux secteurs légitimes, les rançongiciels modernes sont tributaires des cryptomonnaies et des services de blanchiment de cryptomonnaies, et des territoires où les lois et l'application de la loi contre la cybercriminalité sont laxistes ou inexistantes.

### *Croissance effrénée des données et des systèmes connectés à Internet*

Dans les dernières décennies, la tendance en informatique a été une augmentation importante de la connectivité Internet, de la puissance de calcul et de la capacité de stockage des données, et ce, à des coûts qui ne cessent de diminuer. Cette croissance s'est accompagnée de la création d'une quantité toujours plus grande de données personnelles et exclusives, ainsi que de la connexion à Internet de systèmes de TI de plus en plus importants pour les entreprises, les universités, les industries et les gouvernements. Le monde analogique d'autrefois est désormais numérique et connecté pour inclure les avatars en ligne, le magasinage, les services bancaires, les communications d'entreprise, les systèmes de contrôle industriels et plus encore, en ligne. Par conséquent, dans les années 2010, les données et les systèmes qui pouvaient être retenus en rançon sont devenus abondants, vulnérables aux rançongiciels et de plus en plus importants pour les organisations et les personnes qui n'étaient pas préparées à faire face à une perte de données.

### *La cryptomonnaie et le système de paiement*

L'avènement de cryptomonnaies comme le bitcoin a créé une infrastructure financière transnationale qui facilite les paiements anonymes, rapides et de n'importe où dans le monde. Les transactions en cryptomonnaie sont *immuables* (c.-à-d. qu'elles ne peuvent pas être révoquées) et *vérifiables* (c.-à-d. que les transactions sont toujours publiques et peuvent être confirmées automatiquement). Il s'agit de fonctions essentielles qui font en sorte que les paiements de rançon ne peuvent pas être révoquées une fois que les fichiers de la victime sont déchiffrés. De 2011 à 2013, le bitcoin a pris de l'importance dans plusieurs marchés en ligne où s'échangent des biens illégaux, et les cybercriminels ont adopté le bitcoin comme forme standard de paiement de rançon vers 2013.

Avant les cryptomonnaies et les services de blanchiment connexes, les cybercriminels comptaient presque entièrement sur l'argent traditionnel et des mécanismes de blanchiment tels que le virement de l'argent volé vers des comptes intermédiaires dans le pays victime et le recours à des criminels ou des résidents locaux utilisés à leur insu pour transférer rapidement les fonds vers des banques étrangères ou des systèmes de paiement en ligne mal réglementés. Ces intermédiaires pouvaient facturer jusqu'à 60 % de la valeur de la transaction. En comparaison, les transactions de cryptomonnaie coûtent habituellement moins de 5 % de la valeur de la transaction.

### *Communications anonymes et sécurisées avec les victimes*

Jusqu'à ce que les applications de communication sécurisées et le Web invisible (c.-à-d. les réseaux Internet accessibles seulement par l'entremise d'un logiciel d'anonymisation spécialisé) deviennent fiables et facilement accessibles aux cybercriminels et aux victimes potentielles, la plupart des cybercriminels n'avaient pas la capacité de communiquer de façon sécuritaire avec leurs victimes pour faciliter le processus de versement de rançon. Les applications de communications

sécurisées et les réseaux du Web invisible offrent aux cybercriminels un endroit où ils peuvent puiser dans Internet dont ils ont besoin pour mener à bien leurs activités criminelles.

### *Spécialisation du marché de la cybercriminalité*

La cybercriminalité mondiale prospère grâce à la spécialisation du marché. Par exemple, un cybercriminel peut être un excellent développeur de logiciels, mais il n'a pas les compétences de piratage nécessaires pour cibler et compromettre les victimes. Les marchés de la cybercriminalité offrent aux cybercriminels un accès à d'autres cybercriminels qui se spécialisent dans la maîtrise des compétences qui leur manquent, comme les campagnes de pourriels, l'hébergement de sites Web malveillants ou l'exploitation de réseaux zombies de victimes dont les données ont déjà été compromises. Compte tenu de cette spécialisation, il n'est pas rare qu'une victime de rançongiciel soit compromise par de multiples éléments de maliciels qui sont délibérément conçus pour exécuter une ou plusieurs des étapes requises pour qu'une opération de rançongiciel soit couronnée de succès. Étant donné qu'un rançongiciel rend un système inopérant, il s'agit presque toujours du dernier maliciel d'une chaîne d'infections. Bon nombre des campagnes de fraude bancaire et de rançongiciels les plus percutantes, comme Trickbot et Ryuk, impliquent plusieurs groupes cybercriminels spécialisés travaillant de concert selon divers arrangements financiers et de service pour identifier des victimes lucratives et en tirer le maximum de valeur.

### *Protection contre les forces de l'ordre*

Il serait beaucoup plus difficile pour les cybercriminels de se procurer des rançongiciels s'ils ne pouvaient pas compter sur des endroits où les structures juridiques ou les régimes d'application de la loi tolèrent la cybercriminalité. Par exemple, de nombreuses variantes de rançongiciels ne s'exécutent pas sur des systèmes dont les paramètres de langue ou d'emplacement prennent en charge le russe ou une autre langue proche. Il y a tout lieu de croire qu'il en est ainsi pour éviter d'attirer l'attention des organismes d'application de la loi en Russie, qui tolèrent les activités cybercriminelles motivées par des intérêts financiers, pour autant qu'elles ne visent pas des victimes au pays et, dans une mesure moindre, des alliés régionaux.

## NOUVELLES TENDANCES : RANÇONGICIELS EN 2020-2021

Nous estimons qu'en 2021, les rançongiciels seront très probablement caractérisés par de nouvelles méthodes d'intensification des campagnes et contraindront à des paiements plus importants de la part des victimes. Nous nous attendons de façon quasi certaine à ce que les cybercriminels bénéficient d'une plus grande spécialisation au sein du marché criminel et qu'ils concluent des ententes de service et financières pour faciliter leurs activités. En outre, nous estimons que les cybercriminels continueront presque certainement de cibler les infrastructures essentielles et l'industrie lourde en raison des attentes de paiements de rançon plus élevés et plus rapides, quelles que soient les conséquences potentiellement destructrices de ces activités.

### *Adoption de tactiques plus sophistiquées*

Pour identifier et compromettre des cibles de grande valeur, de nombreux exploitants de rançongiciels adoptent des tactiques sophistiquées plus couramment associées à des groupes parrainés par un État qu'aux cybercriminels. Par exemple, le Centre pour la cybersécurité a récemment observé que certains exploitants de rançongiciels profitent des vulnérabilités en matière de cybersécurité divulguées publiquement à une vitesse presque égale à celle des auteurs de cybermenaces parrainés par un État[vii].

### *Augmentation de la valeur des demandes de rançons*

À mesure que les campagnes de rançongiciels sont devenues mieux à même d'identifier et de compromettre des cibles de grande valeur, la valeur des demandes de rançon a augmenté. Les chercheurs estiment que la demande moyenne de rançon a augmenté de 33 % depuis le quatrième trimestre de 2019 pour atteindre 111 605 $ CA au premier trimestre de 2020 en raison de l'incidence des opérations ciblées de rançongiciels[viii]. La demande moyenne de rançons a bondi à 257 756 $ CA en décembre 2019, et nous estimons qu'il est très probable qu'elle dépasse ce montant en un mois ou plus en 2020[ix].

À l'extrémité du spectre se trouvent des rançons de plusieurs millions de dollars, qui sont de plus en plus fréquentes. En octobre 2019, une compagnie d'assurance canadienne a payé 1,3 million de dollars canadiens pour récupérer 20 serveurs et 1 000 postes de travail[x]. En avril 2020, les cybercriminels ont demandé 15 millions de dollars canadiens en rançon au géant portugais de l'énergie, Energias de Portugal (EDP)[xi].

### *Cibler les fournisseurs de services gérés pour atteindre leurs clients*

Nous estimons qu'il est très probable que les campagnes de rançongiciels ciblent de plus en plus les fournisseurs de services gérés (FSG), c'est-à-dire les entreprises qui hébergent et gèrent les TI de leurs clients, dans le but de cibler leurs clients en aval comme moyen de mettre à l'échelle de façon efficace les campagnes futures de rançongiciels ciblés. Depuis au moins 2019, les exploitants de rançongiciels ont compromis des FSG et utilisé un logiciel de gestion à distance pour installer automatiquement des charges de virus du rançongiciel sur plusieurs réseaux clients en même temps[xii]. En août 2019, les sociétés affiliées à Sodinokibi ont compromis TSM Consulting, un FSG basé au Texas, pour infecter 22 municipalités américaines et exiger une rançon de plus de 3 M$ CA[xiii].

### *Tactiques novatrices pour forcer le paiement*

Nous estimons qu'un nombre croissant d'exploitants de rançongiciels divulgueront des données sur leurs victimes pour punir le refus de paiement. Les attaques ciblées de rançongiciels permettent souvent aux cybercriminels d'accéder à des secrets commerciaux, à de la propriété intellectuelle et à des bases de données sensibles sur les employés et les clients. Depuis novembre 2019, les exploitants du rançongiciel Maze exigent une rançon pour le déchiffrement des données stockées localement ainsi que la destruction des copies exfiltrées. Les victimes qui ne veulent pas payer ont vu leurs données divulguées ou vendues en ligne. Maze est également connu pour publier des données sur les victimes pendant les négociations afin de prouver qu'il les a en main et probablement exercer des pressions pour obtenir le paiement par l'entremise des médias. En date d'août 2020, au moins 16 campagnes de rançongiciels avaient mis à exécution leurs menaces de fuite de données des victimes[xiv].

### *Perturbation des systèmes de contrôle industriels*

Dans les dernières années, les rançongiciels ont de plus en plus touché les systèmes de contrôle industriels (SCI) responsables du contrôle et de la surveillance de l'équipement matériel utilisé par l'industrie lourde et les fournisseurs d'infrastructures essentielles. Nous estimons avec une quasi-certitude que les exploitants de rançongiciels sont devenus habiles dans la propagation des rançongiciels par les réseaux de TI d'entreprise au point où les environnements des SCI adjacents sont de plus en plus vulnérables aux perturbations. Par exemple, en février 2020, des rançongiciels ont contaminé une installation de compression de gaz naturel aux États-Unis, en traversant des réseaux avec accès à Internet pour se rendre jusqu'à des actifs du SCI utilisés pour surveiller l'exploitation des pipelines[xv].

Dans certains cas, les victimes ont choisi de désactiver leurs procédés industriels par mesure de précaution pendant un incident important impliquant un rançongiciel. Par exemple, en mars 2019, Norsk Hydro, une aluminerie norvégienne, a été contaminé par un rançongiciel qui a perturbé ses données logistiques et de production au point de provoquer l'arrêt du SCI et d'entraîner le retour aux opérations manuelles[xvi].

Il y a tout lieu de croire qu'au moins sept variantes de rançongiciel semblent cibler les environnements de SCI. Depuis janvier 2019, ces familles de rançongiciels contiennent des instructions pour interrompre plusieurs processus de SCI (et dans un cas, plus d'une centaine)[xvii]. Les répercussions de ces attaques varient selon les circonstances particulières des processus du SCI et la réaction du personnel sur place[xviii].

## COMMENT LES ÉTATS UTILISENT LE RANÇONGICIEL ET EN BÉNÉFICIENT

Nous estimons qu'il est probable que les auteurs de cybermenaces de plusieurs États utiliseront des rançongiciels pour brouiller les origines ou les intentions de leurs cyberopérations. De plus, de nombreux États entretiennent presque certainement des liens avec des cybercriminels qui utilisent des rançongiciels. Dans certains cas, les cybercriminels fournissent de l'aide aux services de renseignement, ce qui leur permet de mener leurs activités à l'abri des forces de l'ordre.

### *Le rançongiciel comme arme*

La République populaire démocratique de Corée (RPDC) a été responsable[xix] de l'introduction du rançongiciel WannaCry dans le cyberespace le 12 mai 2017, qui a infecté plus de 200 000 ordinateurs dans plus de 150 pays, dont ceux du National Health Service du Royaume-Uni[xx].

Le 27 juin 2017, des auteurs de cybermenaces ont lancé des cyberattaques destructrices déguisées en rançongiciels contre l'Ukraine, qui ont rapidement proliféré à l'échelle mondiale. L'infrastructure publique et privée de l'Ukraine, y compris les banques, les transports et d'autres infrastructures essentielles, a été gravement perturbée. Surnommées NotPetya, ces attaques ont causé plus de 10 milliards de dollars canadiens de dommages à l'échelle mondiale. Le géant pharmaceutique Merck aurait subi des pertes de plus d'un milliard de dollars canadiens et la société de transport danoise A.P. Møller-Maersk aurait perdu 390 millions de dollars canadiens[xxi]. Le Canada a déterminé que des auteurs de cybermenaces russes avaient mis au point le rançongiciel NotPetya[xxii]. L'Australie[xxiii], la Nouvelle-Zélande[xxiv], le Royaume-Uni[xxv] et les États-Unis[xxvi] ont déterminé que la Russie était directement responsable de l'attaque de juin 2017.

### *Le rançongiciel comme écran de fumée pour les activités cybercriminelles parrainées par l'État*

En février 2016, des cybercriminels parrainés par la Corée du Nord auraient acheté et installé des rançongiciels sur les réseaux de la Far Eastern International Bank établie à Taïwan[xxvii]. Les chercheurs en cybersécurité qui ont par la suite analysé des échantillons du maliciel ont déterminé que les données chiffrées n'étaient pas récupérables. Selon leur analyse, l'aspect rançon du maliciel était presque certainement une ruse, et que le véritable objectif était de détruire des preuves et d'empêcher une enquête sur des allégations selon lesquelles des cybercriminels liés à la RPDC auraient volé de l'argent au moyen de transferts SWIFT frauduleux[xxviii].

### *Liens de l'État avec les exploitants de rançongiciels*

Le 5 décembre 2019, le département du Trésor américain a sanctionné le groupe Evil Corp, qui avait organisé des activités de cybercriminalité pour, entre autres, recueillir des renseignements et mener des cyberopérations pour le compte des services de renseignement russes depuis au moins 2017[xxix].

Plusieurs sources de l'industrie associent Evil Corp et ses associés criminels à de multiples variantes de rançongiciel très médiatisées, communément appelées Locky, BitPaymer, DoppelPaymer et, plus récemment, WastedLocker. Depuis avril 2020, WastedLocker a compromis de nombreuses cibles de grande valeur au Canada, au Royaume-Uni et aux États-Unis, touchant principalement les grandes entreprises de fabrication et de technologie. En juillet 2020, Garmin, une entreprise américaine axée sur la technologie GPS, aurait apparemment versé des millions de dollars en rançon aux exploitants de WastedLocker pour récupérer ses données et interrompre la perturbation de ses services[xxx].

## ACTIVITÉ DE RANÇONGICIELS CONTRE LE CANADA

Nous nous attendons avec une quasi-certitude à ce que les rançongiciels dirigés contre le Canada au cours des 12 prochains mois continuent de cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles, ainsi que les organisations de toutes tailles. De plus, de nombreuses victimes canadiennes accéderont presque certainement aux demandes de rançon en raison des graves conséquences économiques et potentiellement destructrices du refus de paiement.

- En 2019, des rançongiciels ont compromis plusieurs administrations municipales, provinciales et territoriales canadiennes, y compris la Ville de Woodstock, en Ontario, qui a subi des dommages de plus de 660 000 $ CA après avoir refusé de payer ses attaquants[xxxi].
- En décembre 2019, Bird Construction, une entreprise de construction établie à Toronto qui a obtenu 48 contrats avec le ministère de la Défense nationale du Canada depuis 2006, a été contaminé par le rançongiciel Maze[xxxii].
- En avril 2020, la Société d'énergie des Territoires du Nord-Ouest a été compromise par des rançongiciels et ses services intégrés ont été interrompus[xxxiii].

Depuis la fin de 2019, plusieurs entreprises canadiennes et un gouvernement provincial ont vu leurs données divulguées publiquement par des exploitants de rançongiciels après avoir refusé de payer une rançon. Les exploitants du rançongiciel Maze qui ont compromis Bird Construction auraient prétendument publié en ligne les données volées à l'entreprise après que cette dernière eut refusé de payer une rançon. En juin 2020, les données d'un consortium d'entreprises agricoles canadiennes ont été mises aux enchères sur le site Web du groupe de rançongiciels Sodinokibi.

Bien que les services publics et les fournisseurs de soins de santé soient souvent les plus touchés de façon visible, nous estimons avec une quasi-certitude que la majorité des attaques de rançongiciel à impact élevé contre le Canada touchent les moyennes ou grandes organisations du secteur privé et ne sont pas signalées aux autorités. Tout au long de 2019-2020, le Centre pour la cybersécurité a pris connaissance de centaines de victimes canadiennes dans un large éventail de secteurs commerciaux, ainsi que de plusieurs municipalités, services de police et fournisseurs de services d'éducation qui ont été compromis par la variante du rançongiciel Ryuk. En date du premier trimestre de 2020, la rançon moyenne mondiale exigée par Ryuk est estimée à 1,7 million de dollars canadiens[xxxiv].

[i] « Report : The Cost of Ransomware in 2020. A Country by Country Analysis », Emsisoft Malware Lab, 11 février 2020
[ii] « Report: The Cost of Ransomware in 2020. A Country by Country Analysis », Emsisoft Malware Lab, 11 février 2020
[iii] « U.S. Leads Multi-National Action Against Gameover Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator », US Department of Justice, Office of Public Affairs, 2 juin 2014
[iv] « Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals... », US Department of Justice Office of Public Affairs, 28 novembre 2018
[v] « Hackers hit Norsk Hydro with Ransomware. The Company Responded with Transparency » Microsoft, 16 décembre 2019
[vi] « Ryuk Keeps Targeting Hospitals During the Pandemic », Bleepingcomputer, 26 mars 2020
[vii] Par exemple, l'exploitation active de multiples passerelles et vulnérabilités RPV découvertes en 2019 et 2020. Voir : « Exploitation active d'une vulnérabilité touchant F5 BIG-IP », Centre canadien pour la cybersécurité, 5 juillet 2020; « Exploitation active de vulnérabilités dans Citrix », Centre canadien pour la cybersécurité, 17 janvier 2020; « Exploitation active de vulnérabilités dans les réseaux privés virtuels (RPV) », Centre canadien pour la cybersécurité, 17 septembre 2019
[viii] « Q1 2020 Ransomware Marketplace Report » Coveware. 29 avril 2020
[ix] « Ransomware Attacks Grow, Crippling Cities and Businesses », The New York Times, 9 février 2020
[x] « Canadian insurance company lost nearly US$1M in ransomware attack », CTV News, 30 janvier 2020
[xi] « RagnarLocker Ransomware Hits EDP Energy Giant, Asks for 10M » Bleepingcomputer, 14 avril 2020
[xii] « Ransomware Gang Hacks MSPs to Deploy Ransomware on Customer Systems » ZDNet, 20 juin 2019
[xiii] « Managed Service Providers are Ransomware Hacker's New Gold Mine », Houston Chronicle, 16 septembre 2019
[xiv] « List of Ransomware that Leaks victims' stolen files if not paid », Bleepingcomputer, 26 mai 2020 (mise à jour)
[xv] « Alert (AA20-049A): Ransomware Impacting Pipeline Operations », US DHS/CISA Alert, 18 février 2020
[xvi] « Ransomware Against the Machine: How Adversaries Are Learning to Disrupt Industrial Production by Targeting IT and OT », FireEye, 24 février 2020
[xvii] « Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families », FireEye, 15 juillet 2020
[xviii] « EKANS Ransomware and ICS Operations » DRAGOS, 3 février 2020
[xix] « Déclaration du CST concernant la source du maliciel WannaCry », Centre de la sécurité des télécommunications du Canada, 19 décembre 2017
[xx] « Investigation: WannaCry cyber attack and the NHS », Report by the Comptroller and Auditor General, Department of Health, National Audit Office, HC 414 SESSION 2017–2019, 25 avril 2018
[xxi] « The Untold Story of NotPetya, the Most Devastating Cyberattack in History », WIRED, 22 août 2018
[xxii] « Déclaration du CST concernant l'affaire du maliciel NotPetya », Centre de la sécurité des télécommunications du Canada, 18 février 2018
[xxiii] « Australian Government attribution of the 'NotPetya' cyber incident to Russia », Statement by Minister for Law Enforcement and Cyber Security Angus Taylor, 16 février 2018
[xxiv] « New Zealand joins international condemnation of NotPetya cyber-attack », Government Communications Security Bureau, 16 février 2018
[xxv] « Russian military 'almost certainly' responsible for destructive 2017 cyber attack », UK National Cyber Security Centre, 16 février 2018
[xxvi] « *In June 2017, the Russian military launched the most destructive and costly cyber-attack in history* », See: « Statement from the Press Secretary of the White House on NotPetya », The White House, 15 février 2018
[xxvii] « North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist » Bleepingcomputer, 17 octobre 2017
[xxviii] « North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist », Bleepingcomputer, 17 octobre 2017
[xxix] « Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware », US Department of the Treasury Press Release, 5 décembre 2019
[xxx] « Garmin Pays Up to Evil Corp After Ransomware Attack – Reports » ThreatPost, 3 août 2020
[xxxi] « Cyber attack costs Woodstock more than 660k Report », Woodstock Sentinel-Review, 9 décembre 2019
[xxxii] « Ransomware attack on construction company raises questions about federal contracts » CBC News, 26 janvier 2020
[xxxiii] « NTPC confirms cyber attack from unknown source on Thursday, RCMP investigating » CBC News, 30 avril 2020
[xxxiv] « Ransomware payments up 33% as Maze and Sodinokibi Proliferate in Q1 2020 », Coverware, 29 avril 2020