D96-138/2025F-PDF
ISBN 978-0-660-97647-1

VUE D'ENSEMBLE DES MENACES PAR RANÇONGICIEL DE 2025 À 2027

UNE ÉVALUATION DE L'ÉVOLUTION DES MENACES PAR RANÇONGICIEL AU CANADA

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Canada

Centre de la sécurité des télécommunications Canada
1929, chemin Ogilvie
Ottawa (Ontario) K1J 8K6
cse-cst.gc.ca

D96-138/2025F-PDF
ISBN 978-0-660-97647-1

Table des matières

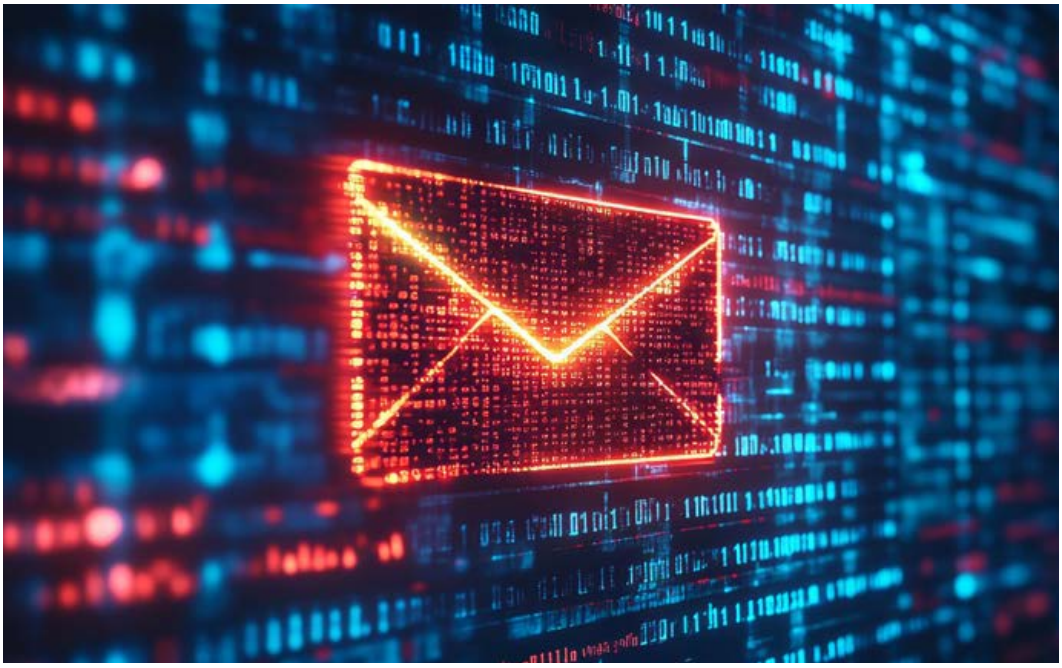
Sommaire

La présente évaluation actualise l'Évaluation des menaces de base : Cybercriminalité, publiée en 2023 par le Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Elle a pour but de faire le point sur les menaces par rançongiciel au Canada et d'informer les organisations canadiennes au sujet de l'historique des rançongiciels, des tendances émergentes et prévisionnelles et des répercussions des rançongiciels sur le Canada et les organisations canadiennes. Elle réfutera également des mythes courants et des idées fausses concernant les pratiques exemplaires en cybersécurité et l'intervention en cas de cyberincident. Le présent rapport vise les organisations canadiennes de toutes tailles, y compris les entités du secteur public et des infrastructures essentielles, mais toutes les Canadiennes et tous les Canadiens peuvent en apprendre plus sur l'écosystème de rançongiciel.

Dans la présente évaluation, un rançongiciel désigne généralement un type de maliciel qui empêche une utilisatrice ou un utilisateur légitime d'accéder à un système ou à des données jusqu'à ce qu'il ait payé une rançon. Toutefois, le Centre pour la cybersécurité reconnaît que les rançongiciels ont évolué et que certains incidents se traduisent plutôt par le vol de données et l'extorsion.

Les rançongiciels sont apparus comme une méthode informelle de cybercriminalité utilisant le chiffrement de base et l'extorsion. Dans les dernières décennies, ils se sont rapidement transformés en écosystème sophistiqué dans lequel les auteurs de menace communiquent et procèdent à des paiements par l'entremise du cyberespace sans frontière difficile d'accès sur le Web clandestin.

On estime que les auteurs de menace qui mènent des attaques par rançongiciel contre des organisations canadiennes sont presque certainement opportunistes et motivés par l'appât du gain. Toutes les organisations canadiennes, peu importe leur taille ou leur secteur, sont à risque d'être la cible d'un rançongiciel. En plus d'avoir des répercussions sur l'infrastructure, les données, la chaîne d'approvisionnement et les activités de l'organisation, une attaque par rançongiciel peut avoir des conséquences sur les moyens de subsistance des Canadiennes et Canadiens si elle interrompt des services essentiels dont ils dépendent.



Méthodologie et fondement de l'évaluation

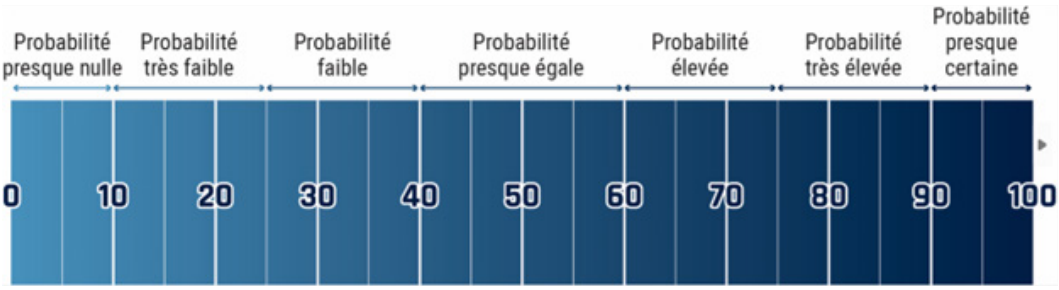
Les principaux jugements dans cette évaluation reposent sur des rapports provenant de diverses sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise en matière de cybersécurité du Centre pour la cybersécurité. Le rôle que joue le Centre pour la cybersécurité dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans un contexte de cybermenace, ce qui a contribué à la présente évaluation. Grâce au volet du mandat du Centre de la sécurité des télécommunications Canada (CST) touchant le renseignement étranger, il a aussi accès à de l'information précieuse sur le comportement des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité doive toujours protéger les sources et les méthodes classifiées, il présente autant que possible les justifications qui ont motivé les conclusions du présent rapport.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploie les termes « on estime que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « probablement » et « très probablement » pour exprimer les probabilités.

Les évaluations et les analyses contenues dans le présent rapport sont fondées sur les renseignements disponibles en date du **4 septembre 2025**.

Lexique des estimations

Le graphique 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 avis antérieurs et des méthodes qui accroissent la précision des estimations.



À propos du Centre canadien pour la cybersécurité

Le Centre pour la cybersécurité est l'autorité technique et opérationnelle en matière de cybersécurité du Canada. Relevant du CST, il est la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité pour la population et les organisations canadiennes. Le Centre pour la cybersécurité travaille étroitement avec les ministères du gouvernement du Canada, les secteurs des infrastructures essentielles, les entreprises canadiennes et les partenaires internationaux pour se préparer et réagir aux cyberévénements, pour en atténuer les conséquences et pour s'en remettre. Il cherche à nouer le dialogue avec des entités externes et favorise les partenariats pour construire un cyberespace canadien fort et résilient. Conformément à la Stratégie nationale de cybersécurité, le Centre pour la cybersécurité représente une approche plus collaborative à la cybersécurité au Canada. Le Centre pour la cybersécurité aide à relever le niveau de la cybersécurité au Canada afin que les Canadiennes et Canadiens puissent vivre et travailler en ligne en toute confiance et sécurité.

Message du dirigeant principal du Centre pour la cybersécurité

Dans une période où les entreprises canadiennes, les infrastructures essentielles et les systèmes du gouvernement continuent d'être la cible des cybercriminelles et cybercriminels, l'éducation sur les menaces est plus importante que jamais. À titre d'autorité nationale du Canada en matière de cybersécurité, le Centre pour la cybersécurité est déterminé à aider les Canadiennes et les Canadiens à comprendre les menaces numériques qui touchent notre économie, nos institutions et notre quotidien, à s'y préparer, à s'en protéger et à intervenir en cas d'incident.

Parmi ces menaces, les rançongiciels se démarquent comme étant l'un des défis les plus perturbants, coûteux et soutenus auxquelles les organisations canadiennes de toutes tailles sont confrontées. C'est pourquoi ce rapport, Vue d'ensemble des menaces par rançongiciel de 2025 à 2027, présente un aperçu axé vers l'avenir de l'environnement de menaces anticipé dans les deux prochaines années. L'analyse se fonde sur les signalements de partout au Canada et dans le monde, sur le renseignement classifié des partenaires étrangers et sur des données du secteur privé. Combinées, ces perspectives permettent au Centre pour la cybersécurité de déterminer les outils, les tactiques et les procédures des exploitants du cybercrime les plus prolifiques, de même que les tendances et les évolutions qui définiront les prochaines menaces.

Comme vous le découvrirez dans ce rapport, les rançongiciels sont lucratifs. En dépit de certaines tendances préoccupantes, le public canadien peut se fier sur le Centre pour la cybersécurité pour répondre à ces menaces au même rythme qu'elles évoluent et pour développer de nouveaux outils de protection des réseaux et des systèmes canadiens.

L'objectif est clair : outiller les décisionnaires en leur donnant les informations nécessaires pour gérer les risques, renforcer la résilience du Canada et préserver la confiance du public canadien envers les systèmes numériques. Pour ce faire, seule la collaboration pourra faire obstacle aux rançongiciels et assurer la sécurité et la résilience du Canada dans le cyberespace en constante évolution.

Cordialement,

Rajiv Gupta
Dirigeant principal, Centre canadien pour la cybersécurité

Principaux avis

- La menace de rançongiciel au Canada continue de croître et d'évoluer rapidement. Les auteurs de menace tirent parti de diverses tactiques sophistiquées pour mener à bien leurs activités cybercriminelles. On estime que les auteurs d'attaques par rançongiciel contre des cibles canadiennes sont presque certainement opportunistes et motivés par l'appât du gain. Il y a un risque presque certain que les organisations, et les personnes, au Canada soient la cible d'un rançongiciel, donc elles doivent accroître leur cyberrésilience en conséquence.
- Les auteurs d'attaque par rançongiciel font preuve d'adaptabilité face aux changements de l'environnement numérique et ils continueront très probablement à utiliser les avancées de l'intelligence artificielle (IA) et de la cryptomonnaie pour développer de nouvelles tactiques d'extorsion lucratives.
- Selon nos observations, l'adoption de pratiques exemplaires en cybersécurité, comme la mise à jour régulière des logiciels, l'activation de l'authentification multifacteur (AMF), les sauvegardes et la prudence face aux tentatives d'hameçonnage, aide le public canadien et les organisations canadiennes à renforcer leur préparation pour se protéger des cybermenaces de base. Les pratiques de cybersécurité ne sont pas qu'un autre facteur optionnel d'une entreprise. Elles sont intégrales à la protection des activités et des données essentielles et à la protection de la population canadienne qui se fie aux services des organisations responsables de ces données.
- Pour comprendre l'écosystème de rançongiciel et en atténuer les répercussions, il faut faire preuve de diligence et de coopération entre les organismes d'application de la loi, les organismes fédéraux, les organisations du secteur privé et le public canadien. On considère que les auteurs de menace menant des attaques par rançongiciel demeureront une menace importante pour le Canada dans les deux prochaines années.

1/ L'ÉCOSYSTÈME DE MENACE

Entre les années 1990 et 2020, le cybercrime a connu des changements importants dans la manière dont les auteurs de menace et les Canadiennes et Canadiens interagissent entre eux. Comprendre l'évolution des rançongiciels montre comment les cybercriminelles et cybercriminels tirent avantage des avancées technologiques et comment les changements à l'écosystème augmentent la prévalence et l'omniprésence des cybermenaces. On peut également relever de l'histoire des indicateurs de tendances futures.

L'évolution des rançongiciels

→ **1989 :** Le professeur de Harvard, **Joseph L. Popp** a envoyé 20 000 disquettes infectées par un maliciel à des chercheuses et chercheurs sur le SIDA de 90 pays, afin de chiffrer les noms de fichiers au moyen du chiffrement symétrique. Les victimes avaient pour instruction d'envoyer un chèque pouvant aller jusqu'à 378 $ à une boîte postale au Panama pour recevoir une disquette de déchiffrement qui leur rendrait accès à leurs systèmes. D'après certaines informations, les seules personnes à avoir payé la rançon étaient les responsables de l'enquête. Joseph L. Popp a été arrêté et a été accusé de chantage. C'est la première occurrence attestée d'une attaque par rançongiciel. À la suite de l'arrestation de l'auteur, les incidents liés à des rançongiciels sont toutefois demeurés assez peu courants, jusqu'à l'adoption massive de l'Internet au cours du 21e siècle[1].

→ **2009 :** L'apparition du **Bitcoin** en 2009, première cryptomonnaie décentralisée, et la soudaine popularité des cryptomonnaies non conventionnelles dans les années suivantes, ont donné aux cybercriminelles et cybercriminels des capacités accrues pour traiter les paiements et blanchir l'argent obtenu lors d'activités illégales en ligne. En donnant aux auteurs de menace les moyens de traiter des fonds de façon intraçable, le Bitcoin a fait en sorte que les rançongiciels deviennent une industrie rentable[2].

→ **2012 :** C'est le déploiement du rançongiciel **Reveton**, un maliciel qui s'installe dans le réseau de la victime lorsque celle-ci clique sur un site Web compromis. Le rançongiciel se fait passer pour des organismes d'application de la loi qui ont pris le contrôle de l'appareil en raison des prétendues activités criminelles en ligne de l'utilisatrice ou de l'utilisateur. On menaçait les victimes de peines d'emprisonnement et leur ordonnait de payer une rançon au moyen de cartes de débit prépayées. Selon des rapports de source ouverte, les exploitants de Reveton ont vendu le maliciel à des tiers, ce qui a fait en sorte d'augmenter le nombre de victimes. C'était le premier cas signalé de rançongiciel-service (RaaS pour *Ransomware-as-a-Service*)[3].

→ **2013 :** Le rançongiciel **CryptoLocker** a d'abord infecté des ordinateurs Windows en septembre 2013 au moyen de pièces jointes malveillantes dans des courriels d'hameçonnage et des pourriels comme principale méthode de livraison. CryptoLocker était l'une des premières variantes de rançongiciel à utiliser un chiffrement sophistiqué. Lorsqu'un appareil était chiffré, une note de rançon apparaissait pour ordonner à la victime de payer un montant afin de récupérer l'accès à ses fichiers. La cryptomonnaie faisait partie des options de paiement. Le Federal Bureau of Investigation (FBI) signalait que, dans les deux premiers mois d'activité, le groupe avait accumulé plus de 27 millions de dollars américains en rançons. CryptoLocker était distribué par l'entremise du réseau zombie GameOver Zeus, attribué à un cybercriminel russe. En juin 2014, on annonçait qu'un regroupement multinational d'organismes d'application de la loi avait réussi à démanteler le réseau zombie de GameOver Zeus et avait saisi les serveurs de CryptoLocker[4].

→ **2015 :** Le groupe à l'origine du rançongiciel **SamSam** est apparu comme le premier à mener régulièrement des attaques ciblées contre les infrastructures essentielles et les grandes organisations, dont les entités gouvernementales et les organismes de santé au Canada et aux États-Unis. Ce comportement, maintenant bien connu comme la chasse au « gros gibier », vise les infrastructures essentielles et d'autres organisations sensibles qui sont perçues comme ayant de meilleures chances de payer de grosses sommes en rançon pour éviter l'interruption de services critiques ou protéger les informations sensibles. En 2018, deux Iraniens avaient été accusés par la justice fédérale aux États-Unis d'avoir déployé le rançongiciel SamSam chez plus de 200 victimes et d'avoir entraîné des pertes de 30 millions de dollars américains[5].

→ **2017 :** L'attaque **WannaCry** qui est survenue en mai 2017 a été identifiée comme l'incident mondial de grande envergure lié à un rançongiciel s'étant propagé le plus rapidement à cette époque. Une fois qu'un appareil a été infecté, WannaCry, qui exploitait une vulnérabilité Microsoft, s'est propagé rapidement par l'entremise de réseaux en infectant d'autres machines vulnérables, et ce, sans interaction humaine. Même si Microsoft avait corrigé la vulnérabilité plusieurs mois avant l'incident, les utilisatrices et utilisateurs qui n'avaient pas apporté les correctifs demeuraient vulnérables à l'attaque. En une seule journée, l'attaque a vu l'infection de 230 000 ordinateurs dans 150 pays, ce qui a mis les rançongiciels sous le feu des projecteurs du monde entier comme jamais auparavant[6].

→ **2019 :** Après qu'une entreprise de sécurité américaine n'a pas payé la rançon demandée par le groupe **Maze** dans les délais, celui-ci a publié environ 700 Mo de données volées à l'entreprise sur son site de fuite de données pour accroître la pression pour qu'elle paie la rançon demandée. Il s'agissait de la première occurrence de publication des données de la victime par un groupe d'exploitation de rançongiciels et de l'utilisation de méthodes de double extorsion. Le fait que les auteurs de menace publient les informations d'entreprise sensibles a rendu désuètes les sauvegardes comme seule tactique d'atténuation efficace[7].

→ **Années 2020 :** Les obstacles techniques à l'entrée de cybercriminelles et cybercriminels disparaissent en raison de la popularité des RaaS et de l'apparition de modèles d'affaires basés sur les affiliés à qui on accorde une licence d'utilisation du maliciel et qui distribuent les profits. La montée des courtières et courtiers d'accès initial a également amélioré l'efficacité des groupes d'exploitation de rançongiciels actifs. En vendant l'accès réseau aux auteurs de menace, ces courtières et courtiers réduisent le temps nécessaire pour commettre une attaque. La propagation des plateformes de communications sécurisées et des marchés et forums sur le Web clandestin a accru la capacité des auteurs de menace de vendre activement leurs services, de réseauter avec les cybercriminelles et cybercriminels et de prendre contact avec les victimes[8].

Le contexte moderne des rançongiciels

La réalité moderne veut que les rançongiciels soient des écosystèmes de menace très sophistiqués, connectés entre eux et en constante évolution. Comprendre les tendances actuelles et émergentes dans ce contexte peut aider les Canadiennes et Canadiens à reconnaître les risques et à mieux s'y préparer.

Attaques par rançongiciel à tactiques d'extorsion multiple

Tandis que les organisations canadiennes élargissent et améliorent la résilience de leurs mesures de cybersécurité de base, les cybercriminelles et cybercriminels continuent de chercher des manières de modifier et d'adapter leur savoir-faire pour mieux extorquer de l'argent à leurs victimes partout dans leur chaîne d'approvisionnement. On estime que la transition des méthodes à tactiques d'extorsion unique à des méthodes à tactiques d'extorsion multiples s'explique par la sophistication accrue des cybercriminelles et cybercriminels et par leur motivation à accroître les répercussions de leurs attaques et la possibilité que les victimes paient la rançon.

Selon des rapports de source ouverte, les possibles stratégies d'extorsion multiple correspondent notamment à des attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) et à la demande de rançon auprès des entités tierces associées à une organisation, comme ses fournisseurs, ses partenaires, ses clients[9]. En plus de pertes financières et de fuites de données sensibles, les attaques à tactiques d'extorsion multiple peuvent nuire à la réputation d'une organisation en raison des interruptions de service ou de victimisation répétée des victimes.

Attaques par exfiltration de données seulement

Si la plupart des groupes d'exploitation de rançongiciels continueront probablement à utiliser le chiffrement dans le cadre de leurs attaques, on estime que la tendance voulant que les auteurs de menace adoptent la pratique d'exfiltrer les données seulement est un changement de comportement notable. En novembre 2024, le groupe d'exploitation de rançongiciels Hunter International se concentrait principalement sur les attaques par exfiltration de données seulement et l'extorsion[10]. En janvier 2025, Hunters International a fort probablement changé d'image pour devenir World Leaks, un groupe d'extorsion qui fournit son outil adapté d'exfiltration de données à ses affiliés pour que ceux-ci les utilisent contre leurs victimes[11]. Des rapports de source ouverte attribuent la tendance croissante des attaques par exfiltration de données seulement à leur rapidité et à leur simplicité de déploiement et d'exécution, comparativement aux attaques par chiffrement[12].

Changements dans la démographie des victimes

Les infrastructures essentielles et les grandes entreprises demeurent des cibles attrayantes pour les auteurs de rançongiciel. Toutefois, selon de récentes évolutions dans la démographie des victimes, on estime qu'aucune organisation n'est à l'abri des cyberincidents. Les entreprises ayant moins de ressources en cybersécurité peuvent être confrontées à plus de défis lorsque vient le temps d'intervenir à la suite d'une attaque sophistiquée par rançongiciel.

Les auteurs de menace tireront souvent avantage de points d'accès initial, comme des logiciels non corrigés, des justificatifs d'identité compromis, l'hameçonnage ou le protocole de bureau à distance (ou remote desk protocol). Les entités ayant de faibles capacités d'investissement dans leurs infrastructures de technologies de l'information (TI) ou dans la formation en cybersécurité de leur personnel peuvent donc se trouver en situation vulnérable[13].

Les répercussions d'un rançongiciel, notamment les périodes d'indisponibilité, les retards dans la chaîne d'approvisionnement, la réduction de la confiance des consommatrices et consommateurs et les coûts de reprise, peuvent avoir d'importances conséquences sur les petites et moyennes entreprises et pourraient être un facteur décisif de leur viabilité commerciale[14]. Les organisations ayant moins de spécialistes internes en cybersécurité ont aussi souvent recours à des fournisseurs de services gérés (FSG) pour gérer leurs services de TI et de gestion de l'information. Étant donné leurs réseaux de clients élargis et leur accès à des informations sensibles, les FSG représentent donc une cible attrayante[15].

Intelligence artificielle

Au fur et à mesure que l'IA devient plus sophistiquée et plus intégrée qu'elle ne l'est déjà dans les organisations canadiennes, on considère que les cybercriminelles et cybercriminels adopteront des capacités alimentées par l'IA pour cibler des victimes et réduire davantage les obstacles techniques à l'entrée de rançongiciel dans l'écosystème. Les auteurs de menace tirent avantage des améliorations en IA générative, en particulier les grands modèles de langage, à différentes étapes des attaques par rançongiciel, notamment les suivantes :

- Développement de maliciels
- Génération d'hypertrucages
- Automatisation des négociations avec les victimes
- Recherche sur les vulnérabilités
- Mise en œuvre de stratégies de piratage psychologique

Ce faisant, les cybercriminelles et cybercriminels sont moins restreints par le manque de compétences et de ressources[16].

Cryptomonnaie et finances décentralisées

On estime que les auteurs de rançongiciel continueront à tirer parti de la cryptomonnaie en raison de l'anonymat qu'elle propose en comparaison avec les biens financiers courants. Les pressions accrues sur les plans de la réglementation et des mesures d'application de la loi visant les crimes financiers en ligne incitent davantage les auteurs de menace à trouver des façons de dissimuler leurs transactions[17].

La cryptomonnaie permet aux profits des cybercrimes de traverser les frontières, a pour effet d'accroître la portée des activités illégales des auteurs de menace et représente un défi dans le cadre des enquêtes des organismes d'application de la loi. En 2023, le Centre d'analyse des opérations et déclarations financières du Canada a affirmé que le mouvement des recettes découlant de la fraude et des attaques par rançongiciel est la méthode de blanchiment d'argent la plus répandue liée aux monnaies virtuelles[18].

Actifs virtuels

Cryptomonnaies

Les cryptomonnaies sont des jetons numériques qui se basent sur des techniques de cryptographie pour transférer de façon pseudo-anonyme des fonds par l'entremise d'un registre public (chaîne de blocs) qui enregistre les transactions entre les adresses de portefeuille de cryptomonnaie. Les cybercriminelles et cybercriminels utilisent souvent les cryptomonnaies comme Bitcoins (BTC) pour faire des transactions illégales[19].

Monnaies privées

Les monnaies privées sont un type de cryptomonnaie qui offrent un meilleur anonymat, étant donné qu'elles fonctionnent sur leur propre chaîne de blocs afin de masquer l'identité des utilisatrices et utilisateurs et les historiques de transaction. Il s'agit par exemple des monnaies Monero (XMR), Zcash (ZEC) et Dash (DASH)[20].

Techniques de blanchiment et d'obscurcissement

Saut de chaîne

Le saut de chaîne (ou chain hopping), c'est le transfert de fonds d'une chaîne de blocs à une autre pour masquer l'origine illégale des fonds[21].

Mixeurs

Les mixeurs sont des services qui brisent les liens entre l'adresse d'origine et l'adresse de destination des fonds de cryptomonnaie afin de masquer leur origine illégale[22].

Influence géopolitique sur les rançongiciels

Les conflits géopolitiques se transposent de plus en plus dans l'environnement numérique tandis que plus en plus de gouvernements prennent part à des cybercrimes, dont des rançongiciels, comme moyen non traditionnel de représailles contre leurs adversaires ou comme de contournement des sanctions internationales. Le niveau de mobilisation des cybercriminelles et cybercriminels varie selon l'État : certains États donnent des ressources et des protections directement aux cybercriminelles et cybercriminels, et d'autres tolèrent en silence les cybercrimes, pourvu que ces activités correspondent à leurs intérêts politiques et ne fassent pas de victimes dans leur pays[23].

En 2022, pendant l'invasion de l'Ukraine par la Russie, le groupe d'exploitation de rançongiciels Conti a menacé publiquement de s'en prendre aux pays occidentaux qui lançaient des cyberattaques contre les infrastructures essentielles russes[24]. Selon des rapports de source ouverte, dans le contexte du conflit en court au Moyen-Orient, un groupe d'exploitation de rançongiciels ayant des liens avec la République islamique d'Iran a commencé à proposer des gains accrus aux auteurs de menace qui menaient des cyberattaques contre les adversaires de l'Iran[25].

Le Centre pour la cybersécurité continue de surveiller l'influence du contexte géopolitique sur le cybercrime et le degré de participation des auteurs parrainés par des États qui mobilisent les cybercriminelles et cybercriminels afin d'atteindre les objectifs stratégiques de leur pays.

2/ LES RANÇONGICIELS AU CANADA

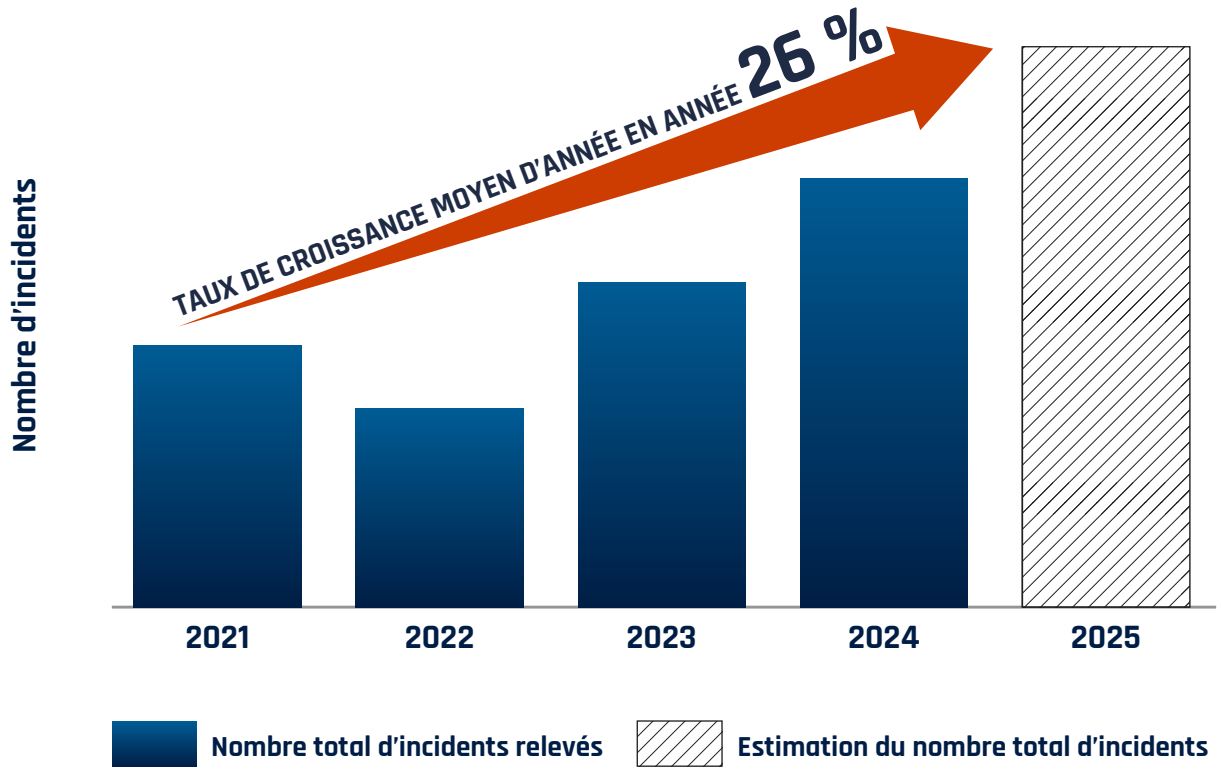
La majorité des principaux groupes d'exploitation de rançongiciels qui s'en prennent au Canada sont presque certainement opportunistes et motivés par le gain. On estime que les principales et principaux membres de ces groupes sont très probablement russophones et qu'ils mènent leurs activités à partir de la Communauté des États indépendants (CEI), bien que leurs affiliés proviennent de partout dans le monde.

Comme l'Évaluation des cybermenaces nationales 2025-2026 du Centre pour la cybersécurité l'explique, les mesures d'application de la loi et les événements géopolitiques peuvent faire fluctuer les activités de cybercriminalité. Toutefois, selon nos observations, le nombre d'incidents liés à des rançongiciels augmente au Canada et continuera d'augmenter chaque année dans la plupart des secteurs.

Les paiements demandés par les rançongiciels ont également varié au cours des quatre dernières années, possiblement en raison de paiements moins élevés et moins fréquents par les victimes en parallèle avec l'augmentation du nombre de victimes canadiennes. Même si la plupart des auteurs de rançongiciel motivés par le gain sont opportunistes, les infrastructures essentielles canadiennes demeureront probablement des cibles attrayantes, étant donné que ces organisations sont plus enclines à payer les rançons demandées pour limiter les interruptions.

Le Centre pour la cybersécurité a constaté une augmentation du nombre d'incidents liés à des rançongiciels en 2024 comparativement à 2023. On considère qu'il est très probable que les RaaS ont éliminé les obstacles techniques à l'entrée des auteurs de menace dans l'écosystème des rançongiciels et ont permis la prolifération des tactiques, techniques et procédures (TTP) sophistiquées sont utilisées contre le public canadien et les organisations canadiennes. Étant donné que les incidents ne sont pas tous signalés, on estime que le nombre d'incidents liés à un rançongiciel et de paiements est presque certainement plus élevé que les statistiques présentées ci-dessous.

Figure 1 : Croissance depuis 2021 du nombre d'incidents liés à des rançongiciels au Canada connus du Centre pour la cybersécurité



En 2024, les trois principales menaces par rançongiciel au Canada étaient :

- **Akira :** Apparu en avril 2013, le groupe Akira exploite des RaaS et est fort probablement lié au groupe d'exploitation de rançongiciels Conti, maintenant dissous[26]. Le groupe exploite deux variantes de rançongiciels. Il exfiltre les données des victimes avant de chiffrer leurs appareils et de se servir des données pour mener une double extorsion[27]. Le secteur manufacturier et celui des télécommunications ont notamment été touchés par Akira, au Canada et ailleurs dans le monde[28].
- **Play :** Apparu en juin 2022, Play est un groupe d'exploitation de rançongiciels fermé qui a adopté le modèle de RaaS en novembre 2023. Le groupe exploite une variante de rançongiciel du même nom et emploie un modèle de double extorsion[29]. Le rançongiciel Play a été utilisé pour s'en prendre à des organisations du secteur de l'information et des technologies et celui des services professionnels, au Canada et ailleurs dans le monde[30].
- **Medusa :** Medusa est un groupe d'exploitation de RaaS qui est apparu en juin 2021. Le groupe exploite une variante de rançongiciel du même nom et emploie un modèle de double extorsion. Le rançongiciel Medusa a été utilisé pour s'en prendre à des organisations des infrastructures essentielles et de l'information et des technologies, au Canada et ailleurs dans le monde[31].

Les rançongiciels peuvent avoir d'importantes répercussions sur les activités d'une organisation et la sécurité de leurs informations sensibles. Ils peuvent également nuire à sa réputation. Tous ces aspects peuvent avoir une incidence sur la concurrentialité de l'organisation dans son secteur et dans l'ensemble de l'économie canadienne[32].

Enquête canadienne sur la cybersécurité et le cybercrime

Statistique Canada mène l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC) pour le compte de Sécurité publique Canada. Cette enquête recueille des renseignements sur les répercussions financières et opérationnelles de la cybercriminalité sur les entreprises canadiennes. Elle recueille également des renseignements sur la disposition des entreprises canadiennes à mettre en œuvre des mesures de cybersécurité proactives et à gérer les incidents de sécurité. Les données les plus récentes de l'ECCC, publiées en octobre 2024, utilisent des renseignements recueillis en 2023 auprès d'un échantillon de plus de 12 000 organisations canadiennes. L'enquête fournit des renseignements clés sur la prévalence et les répercussions des cyberincidents, y compris les attaques par rançongiciel, ainsi que sur l'évolution des postures et des procédures de sécurité au sein des entreprises canadiennes[33].

Chez les entreprises ayant signalé des incidents de cybersécurité, **13 %** d'entre elles ont dit que les **rançongiciels** ont servi de mode d'attaque, ce qui représente une hausse de 2 % depuis l'ECCC de 2021.

À la suite d'une augmentation de 200 millions de dollars canadiens entre 2019 et 2021, les coûts totaux de reprise associés aux incidents de cybersécurité en 2023 **ont doublé** pour s'établir à **1,2 milliard de dollars canadiens**.

Environ **22 % des entreprises** ont signalé qu'une formation formelle a été offerte aux travailleuses et travailleurs n'œuvrant pas dans le domaine des TI pour les aider à développer et à améliorer leurs compétences en matière de cybersécurité.

Une **baisse de 11 %** a été observée dans les organisations qui emploient des **travailleuses et travailleurs en cybersécurité**, principalement en raison du recours à des consultantes et consultants indépendants en cybersécurité et à des FSG.

3/ EXEMPLES DE CYBERINCIDENTS

Partout au Canada, les organisations doivent de plus en plus tenir compte du contexte des cybermenaces en constante évolution. Les rançongiciels peuvent gravement miner les fonctions opérationnelles, la gestion de la chaîne d'approvisionnement et la confiance de la clientèle lorsque des cybercriminelles et cybercriminels perturbent les opérations, ou volent ou divulguent de l'information sensible.

On estime que les auteurs d'attaques par rançongiciel continueront de cibler le Canada et les organisations canadiennes au cours des deux prochaines années. L'examen d'études de cas publiques sur des incidents liés à des rançongiciels peut permettre de contextualiser les répercussions sur les fonctions opérationnelles et les collectivités tributaires des services de ces organisations. En comprenant les répercussions réelles des rançongiciels, les Canadiennes et Canadiens peuvent reconnaître la gravité du problème et en quoi ces répercussions peuvent les toucher et toucher leurs entreprises et leurs collectivités.

Secteur public

Premier exemple

Une entité canadienne du secteur public a déclaré avoir été victime d'une brèche de cybersécurité. La brèche a causé des pannes techniques généralisées, ce qui a fait en sorte que les services de l'entité n'étaient pas disponibles pendant plusieurs mois. Plutôt que de payer la rançon, l'entité a choisi de reconstruire ses systèmes.

L'entité, après avoir décelé une activité suspecte pour la première fois, a fait appel à son équipe d'intervention en cas d'incident, à des consultantes et consultants en sécurité, aux forces policières et à des conseillères et conseillers juridiques afin de maîtriser la situation et de mener une enquête.

Une évaluation des répercussions a révélé que les auteurs de menace avaient initialement accédé au réseau, mais qu'ils étaient restés inactifs pendant plusieurs mois avant d'exfiltrer des données. Les données volées comprenaient des renseignements concernant des membres du personnel et leurs personnes à charge. Elles comprenaient également des renseignements personnels, médicaux et financiers concernant la clientèle, des entrepreneures et entrepreneurs, des parties prenantes, des bénévoles et des candidates et candidats.

Second exemple

Un organisme du secteur public canadien a été la cible d'une attaque par rançongiciel qui a considérablement perturbé ses opérations.

Dans l'espace de quelques jours, l'organisme a maîtrisé la situation et a rétabli la plupart de ses services à partir des sauvegardes de système. Il a affirmé qu'aucune rançon n'avait été payée et que, à la suite d'une analyse criminalistique, rien n'indiquait que les auteurs de menace avaient récupéré des renseignements sensibles ou personnels.

Malgré le rétablissement de quelques services, certains systèmes sont demeurés inutilisables pendant plusieurs mois après l'incident. Les coûts de rétablissement et de reconstruction ont été estimés à des millions de dollars.

Secteur privé

Deux entreprises de logistique canadiennes ont été victimes d'une atteinte à la protection des renseignements personnels de leurs clientèles.

Les entreprises ont signalé l'attaque aux parties susceptibles d'être touchées, ainsi qu'aux autorités fédérales compétentes et au Commissariat à la protection de la vie privée du Canada (le Commissariat). Le Commissariat a immédiatement lancé une enquête afin d'évaluer l'efficacité des mesures de précaution mises en place pour protéger les renseignements sensibles.

Un groupe d'exploitation de rançongiciels a revendiqué la responsabilité de l'attaque et aurait volé un nombre important de documents.

Secteur de la vente au détail

Un important détaillant canadien de produits de santé a signalé une attaque par rançongiciel qui l'a forcé à cesser ses activités pendant plusieurs jours alors qu'il reconstruisait ses systèmes.

Le détaillant a refusé de payer la rançon et a déployé des contre-mesures pour empêcher que ses réseaux soient davantage compromis. Il a fait appel à des spécialistes externes et à des organismes d'application de la loi pour maîtriser la situation et rétablir ses systèmes. Il a déclaré que l'attaque par rançongiciel avait compromis des données liées à ses services des ressources humaines et des finances, ainsi que certains renseignements sur le personnel.

Secteur de l'éducation

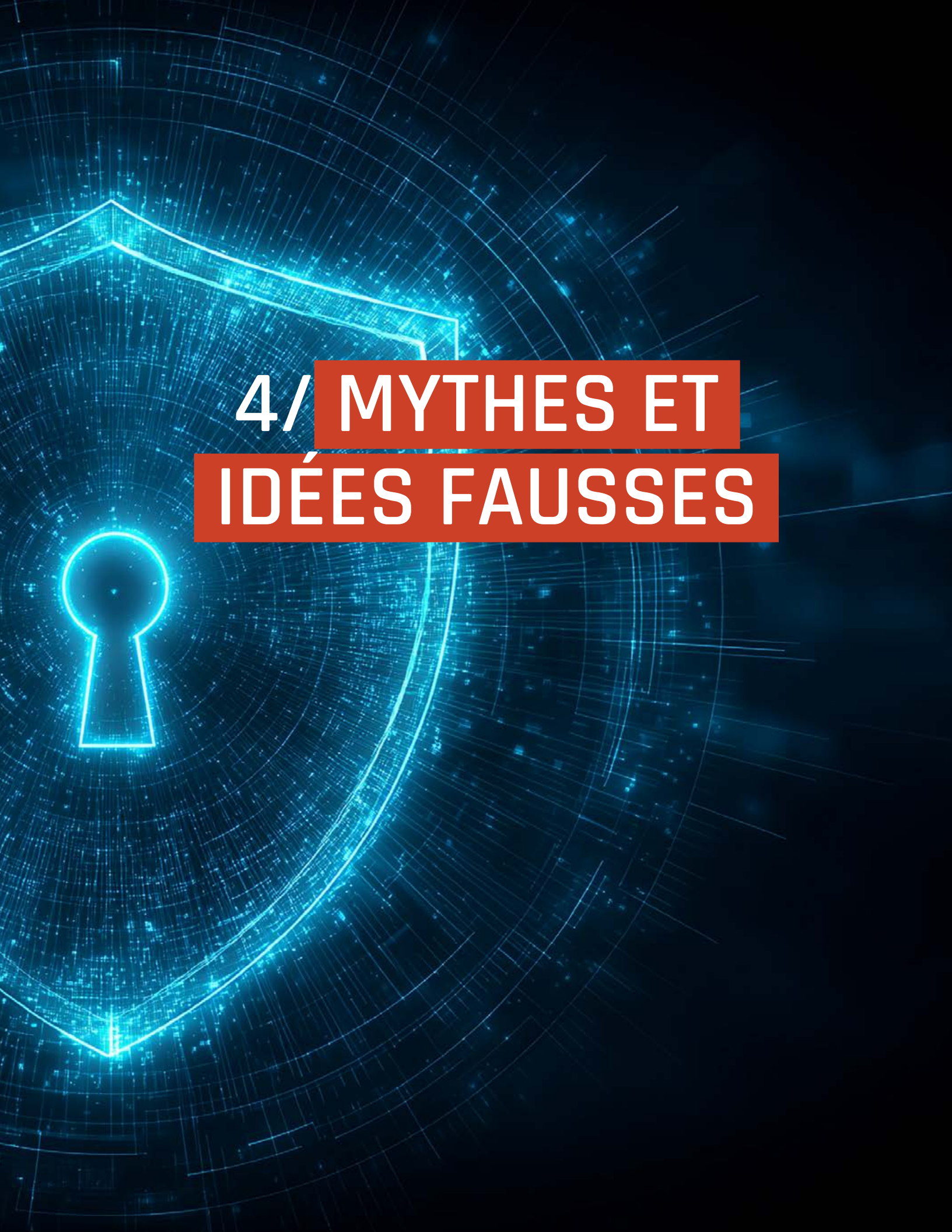
Une organisation de technologie éducative a annoncé qu'un auteur de menace avait utilisé des justificatifs d'identité compromis pour accéder à des données sensibles. Les bases de données concernées contenaient les renseignements de plusieurs millions de personnes.

L'organisation a signalé l'incident aux autorités policières compétentes et a décidé de payer la rançon. Malgré la garantie de l'auteur de menace que les renseignements volés seraient supprimés, il a été annoncé que l'auteur de menace continuait à communiquer avec les victimes dans le but de leur extorquer de l'argent au moyen des mêmes données utilisées lors du premier incident.

Secteur de l'énergie

Une entité canadienne du secteur de l'énergie a confirmé avoir été victime d'une attaque par rançongiciel qui a entraîné la fuite de renseignements personnels et bancaires sensibles d'un grand nombre de clientes et clients actuels et anciens. L'entité a avisé les clientes et clients touchés et leur a offert des services de surveillance du crédit et de protection de l'identité sans frais.

L'entité a confirmé ne pas avoir payé la rançon et a mis en application ses protocoles d'intervention en cas d'incident, en collaborant avec des spécialistes en cybersécurité pour évaluer les répercussions de l'attaque et reconstruire et rétablir les systèmes touchés.



4/ MYTHES ET IDÉES FAUSSES

L'une des mesures essentielles que les Canadiennes et Canadiens peuvent prendre pour renforcer leur résilience aux cyberattaques consiste à déboulonner les idées fausses et les croyances courantes. Il s'agit notamment pour eux de mieux comprendre la proximité des menaces et le caractère délicat de leurs renseignements personnels ou commerciaux, et de prendre d'importantes mesures d'intervention en cas d'incident.

« Notre organisation est trop petite pour être une cible. »

On estime que toute organisation canadienne, petite ou grande, peut être vulnérable aux cybermenaces et aux répercussions des rançongiciels. Bien que certains groupes d'exploitation de rançongiciels maintiennent un « code moral » autoproclamé selon lequel ils s'abstiennent de cibler certaines organisations (par exemple, les hôpitaux, les organismes de bienfaisance, les organismes gouvernementaux et les institutions religieuses), d'autres cibleront n'importe quelle organisation[34].

Les groupes dotés de moyens techniques plus sophistiqués et disposant de ressources adéquates peuvent faire des recherches proactives sur les entreprises afin de repérer celles qui sont les plus susceptibles de payer des demandes de rançon. Entre-temps, d'autres auteurs de menace priorisent l'augmentation du nombre de publications de sites de fuite de données, peu importe la taille des organisations victimes, afin de renforcer leur réputation.

Les petites entreprises font souvent appel à des FSG pour gérer une partie de leurs opérations, ou elles intègrent des parties de leurs chaînes d'approvisionnement à plusieurs autres entités. Ces entreprises peuvent être davantage exposées à des menaces si les tierces parties sont victimes de compromissions.

Ressources

- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises
- Cyberactivité malveillante ciblant les fournisseurs de services gérés en technologie de l'information

« Nous n'avons pas besoin de tous ces outils et règles de cybersécurité. »

En fermant ses fenêtres, en verrouillant ses portes et en allumant son système de sécurité avant de quitter son domicile, on peut fort probablement atténuer les risques potentiels.

De même, la mise en œuvre de pratiques de cybersécurité de base peut réduire considérablement le risque d'attaques par rançongiciel. La formation et l'éducation de routine du personnel favorisent la diligence personnelle et renforcent la sensibilisation à la cybersécurité. Cela peut grandement contribuer à prévenir l'entrée de rançongiciels par des moyens courants, notamment :

- des sites Web mystifiés
- des messages d'hameçonnage
- des justificatifs d'ouverture de session compromis

Signaler du contenu suspect, prendre le temps de réfléchir de manière critique et valider les adresses URL et les adresses de courriel sont des mesures simples que les gens peuvent prendre pour prévenir les attaques par maliciel[35]. Voici d'autres mesures que les particuliers et les organisations peuvent prendre pour se protéger contre les rançongiciels :

- des sauvegardes régulières
- des mises à jour automatiques
- des outils de sécurité

Ressources

- Protéger votre organisation contre les maliciels
- Sauvegarder et récupérer vos données
- Élaborer un plan d'intervention en cas d'incident
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF)
- Pratiques exemplaires de création de phrases de passe et de mots de passe
- Conseils de sécurité sur les gestionnaires de mots de passe
- Pratiques exemplaires en matière de cybersécurité à intégrer dans votre organisation

« Payer la rançon, c'est la plus simple façon de récupérer nos données. »

Rien ne garantit que les auteurs de menace déverrouilleront les systèmes ou retourneront les données volées si les organisations victimes d'une attaque par rançongiciel paient la rançon demandée. Les auteurs de menace peuvent copier les données et s'en servir pour victimiser à nouveau une organisation ou sa clientèle afin d'obtenir plus d'argent[36].

La cyberassurance comme mesure de protection proactive contre les rançongiciels peut encourager les organisations à aligner leurs postures de cybersécurité sur les normes des polices d'assurance. Toutefois, si les documents de police d'assurance ne sont pas adéquatement protégés sur le site Web ou dans les systèmes d'une organisation, des auteurs d'attaques par rançongiciel dotés de moyens sophistiqués pourraient obtenir des renseignements sur les montants de la couverture et les exploiter lors de négociations de rançon pour maximiser leur paiement[37].

« Je n'exploite pas d'entreprise, alors pourquoi devrais-je me soucier des rançongiciels? »

Dans le contexte numérique actuel, il est fort probable que d'innombrables organisations recueillent et stockent des renseignements sensibles. Si ces entreprises subissent une attaque par rançongiciel, des données personnelles pourraient être indirectement compromises. Une attaque par rançongiciel peut avoir des répercussions sur les Canadiennes et Canadiens, peu importe leur emploi ou la diligence avec laquelle ils utilisent les données. Lorsque des cyberattaques perturbent des organisations fournissant des services essentiels, elles peuvent gravement limiter l'accès du public aux produits pharmaceutiques, au transport, aux services Internet et à d'autres ressources critiques.

« Je m'en fiche si mes données sont accessibles – les gens peuvent les avoir. »

De plus en plus, les organisations doivent traiter d'immenses quantités de données personnelles provenant de clientes et clients canadiens, comme des renseignements financiers sensibles, des coordonnées et des dossiers de santé. À la suite d'une attaque par rançongiciel, les auteurs de menace vendent souvent les données compromises sur le Web clandestin. Une fois compromises, les données demeureront très probablement dans cet écosystème. Cette situation accroît la vulnérabilité aux menaces, comme les campagnes de courriels d'hameçonnage ciblées, qui peuvent ensuite causer un préjudice à la clientèle, à la famille et aux proches[38].

Les propriétaires d'entreprise devraient se soucier de la sécurité de leurs données, car la compromission de leurs renseignements (comme la propriété intellectuelle) peut porter une atteinte directe à leur réputation, à leur sécurité financière et à leur compétitivité sur le marché.

Signaler un incident lié à un rançongiciel

Si vous ou votre organisation êtes victime d'une attaque par rançongiciel, nous vous conseillons de le signaler à vos autorités locales, au Centre antifraude du Canada et au Centre pour la cybersécurité (dans Mon cyberportail ou par courriel à l'adresse contact@cyber.gc.ca).

Le fait de signaler des cyberattaques aux autorités compétentes permet à celles-ci d'enquêter adéquatement sur les attaques et de repérer la source de la compromission afin de protéger votre organisation et d'autres organisations contre de futurs incidents.

Pour comprendre le contexte des rançongiciels au Canada, il faut comprendre la taille et la nature des auteurs de menace. En signalant les cyberattaques, vous contribuez à faire du Canada un pays plus sûr et plus intelligent.

Perspective

On estime que les rançongiciels demeureront une menace importante pour le Canada et qu'ils susciteront énormément d'attention de la part des Canadiennes et Canadiens au cours des prochaines années. Plus les organisations s'intègrent au contexte numérique, augmentant les possibilités d'exploitation par des auteurs de menace, plus leur infrastructure et leurs données sensibles continueront fort probablement d'être compromises par des rançongiciels.

Les auteurs de cybermenace ont développé leurs TTP, notamment les tactiques d'extorsion et les caractéristiques démographiques des victimes, et continueront de le faire, afin d'accroître l'incidence de leurs attaques et leurs possibilités de récolter une récompense financière. Cela dit, il y a de nombreuses mesures que les organisations canadiennes peuvent prendre pour se protéger contre ces menaces. Les organisations canadiennes qui cherchent à protéger leurs systèmes et leur information doivent impérativement tenir compte de la cybersécurité dans tout ce qu'elles font. Il s'agit notamment de mettre en œuvre des pratiques fondamentales en matière de cybersécurité, comme l'application de correctifs à la technologie opérationnelle, l'activation des mises à jour automatiques et de l'authentification multifacteur, et la promotion du développement sécurisé. Il leur conviendrait également de tirer parti des outils à leur disposition, comme l'outil de détection et d'analyse des maliciels Assemblyline, mis au point par le Centre pour la cybersécurité, afin d'assurer une surveillance continue de leurs réseaux et de demeurer vigilantes face aux menaces en constante évolution.

Une collaboration soutenue entre les organismes nationaux d'application de la loi, le secteur privé et les alliés internationaux s'avérera nécessaire pour faire davantage connaître l'écosystème des menaces et coordonner les mesures proactives et adaptées appropriées afin de limiter les répercussions mondiales et de prévenir la propagation de rançongiciels.

Le Centre pour la cybersécurité travaille jour et nuit à détecter les rançongiciels et d'autres cybermenaces semblables, et à se défendre contre ceux-ci. L'une des façons d'y parvenir est de fournir des notifications de signes avant-coureurs d'une attaque par rançongiciel pour avertir les victimes potentielles pendant la phase initiale d'un incident lié à un rançongiciel. Au moyen de ces notifications, les responsables de la cyberdéfense peuvent repérer et arrêter les attaques par rançongiciel avant que des données soient compromises. Au cours de l'exercice 2024 à 2025, 336 notifications de signes avant-coureurs d'une attaque par rançongiciel ont été envoyées à plus de 300 organisations canadiennes, ce qui s'est traduit par des économies allant jusqu'à 18 millions de dollars canadiens.

Pour obtenir de plus amples renseignements sur la façon dont le public canadien et les organisations canadiennes peuvent se protéger contre la menace des rançongiciels et renforcer leur cyberrésilience globale, nous les encourageons à consulter les Objectifs relatifs à l'état de préparation en matière de cybersécurité, le Guide sur les rançongiciels et d'autres conseils en matière de cybersécurité sur le site Web du Centre pour la cybersécurité.

Glossaire

Intelligence artificielle (IA) : Un sous-champ de l'informatique qui développe des programmes informatiques intelligents capables de donner l'impression d'une intelligence humaine (par exemple, résoudre des problèmes, tirer des leçons, comprendre une langue, interpréter des scènes visuelles).

Chasse au « gros gibier » : Pratique consistant à viser les infrastructures essentielles et d'autres organisations sensibles qui sont perçues comme ayant de meilleures chances de payer de grosses sommes en rançon pour éviter l'interruption de services critiques ou protéger les informations sensibles.

Réseau de zombies : Réseau d'ordinateurs forcés d'exécuter ensemble la commande d'un utilisateur distant non autorisé. Ce réseau d'ordinateurs compromis sert à attaquer d'autres systèmes.

Communauté des États indépendants (CEI) : Organisation régionale établie en 1991 et composée de neuf États appartenant anciennement à l'Union soviétique, à savoir l'Arménie, l'Azerbaïdjan, le Bélarus, le Kazakhstan, le Kirghizistan, la Moldova, la Russie, le Tadjikistan et l'Ouzbékistan.

Cryptomonnaies : Actifs virtuels qui utilisent la cryptographie pour protéger et confirmer leur propriété. Les cryptomonnaies se divisent en unités, comme « bitcoin » et « ether ». Les transactions connexes sont généralement enregistrées dans leurs chaînes de blocs respectives. Les « jetons » représentent une certaine valeur de « monnaie » et peuvent servir à acheter certains biens et services. Les cryptomonnaies sont échangées sur un système pair à pair et ne sont pas gérées par une autorité centrale, comme une banque, un gouvernement ou un pays.

Cyberassurance : Produit spécialisé destiné à aider les entreprises à gérer les pertes causées par des menaces liées aux réseaux informatiques, comme les atteintes à la protection des données et la cyberextorsion. La cyberassurance peut couvrir les conséquences d'un éventail de cyberévénements, dont les atteintes à la protection des données confidentielles, la cyberextorsion et les perturbations technologiques.

Web clandestin : Segment non indexé d'Internet qui n'est accessible qu'au moyen de logiciels spécialisés ou de mandataires réseau. En raison de sa nature axée sur l'anonymat et la confidentialité, le Web clandestin facilite un écosystème complexe de cybercriminalité et de commerce de biens et de services illicites.

Décrypteur : Outil spécialisé conçu pour aider les entreprises à récupérer des fichiers chiffrés sans avoir à payer des auteurs pour obtenir des clés de déchiffrement[39].

Sites de fuite de données : Sites Web où des auteurs de menace par rançongiciel publient des données volées auprès d'entreprises qui refusent de payer la rançon. Ces sites peuvent contenir des renseignements de nature délicate, comme les justificatifs d'ouverture de session, la propriété intellectuelle et des données personnelles et financières. Elles exposent les organisations victimes à des risques de brèches de sécurité, de vol d'identité, de fraude financière, d'atteinte à la réputation et de conséquences juridiques[40].

Hypertrucages : Contenu qui a été manipulé par des moyens numériques dans le but de tromper les gens. Il peut s'agir d'images, de contenu audio ou de vidéos générés artificiellement.

Déni de service distribué (DDoS pour *Distributed Denial of Service*) : Cyberattaque au cours de laquelle les auteurs de menace cherchent à perturber l'accès à un système, à un service, à un site Web ou à une application en réseau ou à empêcher les utilisatrices et utilisateurs légitimes d'y accéder.

Double extorsion : Lorsque des auteurs d'attaques par rançongiciel exfiltrent des fichiers avant de les chiffrer et menacent de divulguer publiquement des renseignements sensibles si la rançon n'est pas payée.

Chiffrement : Opération par laquelle on transforme une information d'une forme vers une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.

Exfiltration : Transfert non autorisé de données d'un réseau, d'un système ou d'un appareil[41].

IA générative : Catégorie de modèles d'IA qui imitent la structure et les caractéristiques des données d'entrée pour générer du contenu synthétique. Il peut s'agir d'images, de contenu audio, de textes et d'autres contenus numériques[42].

Courtiers d'accès initial : Auteurs de menace qui vendent l'accès à des réseaux internes[43].

Grands modèles de langage (GML) : Réseaux de neurones artificiels que l'on entraîne au moyen de jeux de données linguistiques très volumineux en faisant appel à un apprentissage autosupervisé ou semi-supervisé. Par le passé, les grands modèles de langage généraient le texte en prédisant le mot suivant, mais ils peuvent maintenant utiliser les phrases entières fournies par les utilisatrices et utilisateurs dans des invites ou générer des documents entiers sur un sujet donné. L'entraînement basé sur des jeux de données exceptionnellement grands permet au modèle d'apprendre des structures linguistiques sophistiquées ainsi que les biais ou les inexactitudes que l'on trouve dans ces données.

Maliciel : Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement de la ou du propriétaire. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.

Fournisseurs de services gérés (FSG) : Entreprises qui offrent une gamme de services de gestion et de technologie de l'information. Il s'agit de l'infrastructure physique, virtuelle ou infonuagique, ainsi que des fournisseurs qui gèrent des données stockées principalement dans un environnement virtuel.

Authentification multifacteur (AMF) : Mécanisme pouvant ajouter une couche de sécurité supplémentaire aux appareils et aux comptes. L'authentification multifacteur exige une vérification supplémentaire (comme un numéro d'identification personnel [NIP] ou une empreinte digitale) pour accéder aux appareils ou aux comptes. L'authentification à deux facteurs est un type d'authentification multifacteur.

Hameçonnage : Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle auprès d'une personne, d'un groupe ou d'une organisation en usurpant ou en imitant une certaine marque généralement bien connue, habituellement dans le but d'obtenir des gains financiers. Les hameçonneuses et hameçonneurs incitent les utilisatrices et utilisateurs à fournir leurs renseignements personnels sensibles, comme des numéros de carte de crédit ou des données bancaires en ligne, afin de s'en servir pour commettre des actes frauduleux.

Rançongiciel : Type de maliciel qui empêche une utilisatrice ou un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'une rançon soit versée.

Rançongiciel-service (RaaS pour *Ransomware-as-a-Service*) : Noyau de développeuses et développeurs qui vend ou loue sa variante de rançongiciel à d'autres auteurs de menace, qu'on appelle affiliés. Les développeuses et développeurs aident les affiliés à déployer leur rançongiciel en échange d'un paiement forfaitaire unique, de frais d'abonnement ou d'une part des profits, ou des trois.

Piratage psychologique : Pratique qui consiste à obtenir des renseignements confidentiels en manipulant des utilisatrices et utilisateurs légitimes. Une ou un pirate psychologique incitera les gens à révéler de l'information sensible au téléphone ou en ligne. L'hameçonnage est un type de piratage psychologique.

Cryptographie symétrique : Recours à une clé cryptographique pour effectuer une opération cryptographique et son opération inverse (par exemple, chiffrer et déchiffrer, créer un code d'authentification de message et vérifier le code).

Tactiques, techniques et procédures (TTP) : Comportement d'un auteur de menace. Une tactique est la description la plus générale de ce comportement, tandis que les techniques sont une description plus détaillée du comportement dans le contexte d'une tactique, et les procédures, une description encore plus détaillée dans le contexte d'une technique[44].

Vulnérabilité : Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les actifs ou les activités d'une organisation.

Notes de fin de texte

1 BAKER, Kurt. « History of Ransomware » (en anglais seulement), CrowdStrike, 9 octobre 2022; KnowBe4. « AIDS Trojan or PC Cyborg Ransomware » (en anglais seulement); ESTES, Ryan. « Dr. Joseph L Popp Jr and The First-Ever Ransomware – The AIDS Trojan » (en anglais seulement), WatchGuard, 18 février 2025; WADDELL, Kaveh. « The Computer Virus That Haunted Early AIDS Researchers » (en anglais seulement), The Atlantic, 10 mai 2016.

2 Europol. « Cryptocurrencies: Tracing the evolution of criminal finances » (en anglais seulement), 26 janvier 2022; Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Le rançongiciel moderne et son évolution », 30 novembre 2020; BAKER, Kurt. « History of Ransomware » (en anglais seulement), CrowdStrike, 9 octobre 2022.

3 Arctic Wolf. « The History of Ransomware » (en anglais seulement), 5 juin 2024; FBI. « New Internet Scam » (en anglais seulement), 9 août 2012; TRAYNOR, Orlaith, « From Reveton to Maze: Tracing the Evolution of Ransomware » (en anglais seulement), CyberAngel, 27 août 2020.

4 FBI. « GameOver Zeus Botnet Disrupted » (en anglais seulement), 2 juin 2014; KOSINSKI, Matthew. « Qu'est-ce qu'un ransomware? », IBM, 4 juin 2024; United States Department of Justice. « U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator » (en anglais seulement), 2 juin 2014; Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Le rançongiciel moderne et son évolution », 30 novembre 2020; FBI. « Ransomware on the Rise » (en anglais seulement), 20 janvier 2015; BELCIC, Ivan. « Qu'est-ce que CryptoLocker et comment le supprimer ? », Avast, 27 février 2020.

5 Symantec. « SamSam: Targeted Ransomware Attacks Continue » (en anglais seulement), 30 octobre 2018; United States Department of Justice. « Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses » (en anglais seulement), 28 novembre 2018; Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Le rançongiciel moderne et son évolution », 30 novembre 2020; CrowdStrike. « Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware » (en anglais seulement), 14 novembre 2018.

6 DRAKE, Veronica. « The History and Evolution of Ransomware Attacks » (en anglais seulement), Flashpoint, 29 juillet 2022; ZUGEC, Martin. « The Origin of Ransomware – Exploring the evolution of one of cybersecurity's most prolific threats » (en anglais seulement), Bitdefender, 23 mai 2022; GREGORY, Jennifer. IBM. « Wannacry: how the widespread ransomware changed cybersecurity » (en anglais seulement), 30 octobre 2020.

7 DRAKE, Veronica. « The History and Evolution of Ransomware Attacks » (en anglais seulement), Flashpoint, 29 juillet 2022; ABRAMS, Lawrence. « Allied Universal Breached by Maze Ransomware, Stolen Data Leaked » (en anglais seulement), Bleeping Computer, 21 novembre 2019.

8 Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Le rançongiciel moderne et son évolution », 30 novembre 2020; Arctic Wolf. « The History of Ransomware » (en anglais seulement), 5 juin 2024.

9 Check Point. « What is Triple Extortion Ransomware? » (en anglais seulement); POIREAULT, Kevin. « Ransomware Trends: The Rise of Multi-Extortion Tactics » (en anglais seulement), Infosecurity Europe, 11 février 2025; Palo Alto Networks. « What is Multi-Extortion Ransomware? » (en anglais seulement).

10 ZOHDY, Mahmoud, et al., « The beginning of the end: the story of Hunters International » (en anglais seulement), Group-IB, 2 avril 2025.

11 ZOHDY, Mahmoud, et al., « The beginning of the end: the story of Hunters International » (en anglais seulement), Group-IB, 2 avril 2025.

12 LMG Security. « Online Extortion Is the New Ransomware: Why Hackers Just Want Your Data » (en anglais seulement), 10 juillet 2025; Help Net Security. « Ransomware attacks are getting smarter, harder to stop » (en anglais seulement), 28 avril 2025; MNCASTER, Phil. « Only a Fifth of Ransomware Attacks Now Encrypt Data » (en anglais seulement), Infosecurity Magazine, 25 février 2025.

13 MACCOLL, Jamie, et al. « Ransomware: Victim Insights on Harms to Individuals, Organisations and Society » (en anglais seulement), Royal United Services Institute, 16 janvier 2024.

14 DOHADWALA, Aliasgar. « The Ransomware Epidemic: Why SMEs Are the New Primary Target » (en anglais seulement), Forbes, 27 février 2025.

15 Centre canadien pour la cybersécurité. « Cyberactivité malveillante ciblant les fournisseurs de services gérés en technologie de l'information », 20 décembre 2018.

16 STANHAM, Lucia. « AI-Powered Cyberattacks » (en anglais seulement), CrowdStrike, 16 janvier 2025; TOLOGONOV, Jambul, et John FOKKER. « Analysis of Black Basta Ransomware Chat Leaks » (en anglais seulement), 18 mars 2025; Check Point Research. « FunkSec – Alleged Top Ransomware Group Powered by AI » (en anglais seulement), 10 janvier 2025.

17 TRM Blog. « Démasquer Embargo Rançonlogiciel: une plongée en profondeur dans les TTP et les liens BlackCat du groupe », TRM, 8 août 2025; TRM Blog. « Rançonlogiciel en 2024 : dernières tendances, menaces croissantes et réponse du gouvernement », TRM, 10 octobre 2024.

18 BRONSKILL, Jim. « Criminal use of cryptocurrency to keep growing, Canada's Fintrac warns » (en anglais seulement), Global News, 4 décembre 2023.

19 Chainalysis. « 2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized » (en anglais seulement), 15 janvier 2025; SIGALOS, MacKenzie. « Why some cyber criminals are ditching bitcoin for a cryptocurrency called monero » (en anglais seulement), CNBC, 14 juin 2021; Gendarmerie royale du Canada. « Une experte démystifie les biens numériques », 20 octobre 2020.

20 Chainalysis. « Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies » (en anglais seulement), 18 avril 2023; Europol. « Cryptocurrency: Tracing the Evolution of Criminal Finances » (en anglais seulement), 26 janvier 2022.

21 TRM Blog, « TRM Phoenix Solves Crypto Investigators' 'Chain-Hopping' Problem » (en anglais seulement), TRM, 24 août 2022.

22 Europol. « Cryptocurrency: Tracing the Evolution of Criminal Finances » (en anglais seulement), 26 janvier 2022.

23 Spambrella. « Geopolitical Influences on Ransomware: Trends and Risks » (en anglais seulement).

24 Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie », 14 juillet 2022.

25 ANTONIUK, Daryna. « Iranian ransomware group offers bigger payouts for attacks on Israel, US », The Record, 8 juillet 2025.

26 ANTONIUK, Daryna. « Akira ransomware compromised at least 63 victims since March, report says » (en anglais seulement), The Record, 26 juillet 2023.

27 CAMPBELL, Steven, Akshay SUTHAR, Connor BELFIORE. « Conti and Akira: Chained Together » (en anglais seulement), 26 juillet 2023.

28 ARGHIRE, Ionut. « Akira Ransomware Drops 30 Victims on Leak Site in One Day » (en anglais seulement), 19 novembre 2024; DEMBOSKI, Morgan. « Akira, again: The ransomware that keeps on taking » (en anglais seulement) Sophos, 21 décembre 2023.

29 ARGHIRE, Ionut. « FBI Aware of 900 Organizations Hit by Play Ransomware » (en anglais seulement), Security Week, 5 juin 2025.

30 MATEO, Cj Arsley, Darrel Tristan VIRTUSIO, Sarah Pearl CAMILING, Andrei ALIMBOYAO, Nathaniel MORALES, Jacob SANTOS, Earl John BARENG. « Play Ransomware Group's New Linux Variant Targets ESXi, Shows Ties With Prolific Puma » (en anglais seulement), Trend Micro, 19 juillet 2024.

31 COKER, James. « Medusa Ransomware Claims 40+ Victims in 2025, Confirmed Healthcare Attacks » (en anglais seulement), Inforsecurity Magazine, 7 mars 2025; GRIEG, Jonathan. « CISA: More than 300 critical infrastructure orgs attacked by Medusa ransomware » (en anglais seulement), The Record, 12 mars 2025.

32 Centre canadien pour la cybersécurité. « Introduction à l'environnement de cybermenaces », 28 octobre 2022.

33 Statistique Canada. « Enquête canadienne sur la cybersécurité et le cybercrime », 18 octobre 2024.

34 National Cyber Security Centre. « Ransomware, extortion and the cyber crime ecosystem » (en anglais seulement), 11 septembre 2023.

35 Gouvernement du Canada. « Protégez votre entreprise contre les rançongiciels », Pensez cybersécurité, 14 janvier 2025.

36 Centre canadien pour la cybersécurité. « Rançongiciels : comment les prévenir et s'en remettre, 18 avril 2024.

37 NEUBERGER, Anne. « The ransomware battle is shifting – so should our response » (en anglais seulement), Financial Times, 4 octobre 2024; Marsh. « Ransomware: A persistent challenge in cyber insurance claims » (en anglais seulement), 11 juin 2024.

38 AALDERS, Celina. « Canada's cybersecurity head offers rare insight into Nova Scotia Power breach » (en anglais seulement), 14 juin 2025.

39 ROBB, Brenda. « Understanding Ransomware Decryptors and How They Can Be Used » (en anglais seulement), 24 juillet 2025.

40 Group-IB. « Dedicated Leak Sites (DLS): Here's what you should know (en anglais seulement).

41 National Institute of Standards and Technology. « Security and Privacy Controls for Information Systems and Organizations » (en anglais seulement).

42 National Institute of Standards and Technology. « Computer Security Resource Center Glossary » (en anglais seulement).

43 TATAR, Sule. « Initial Access Brokers » (en anglais seulement), Arctic Wolf.

44 National Institute of Standards and Technology. « Computer Security Resource Center Glossary » (en anglais seulement).