BRANDEFENSE COUNTRY REPORT · CANADA 2026

Brandefense : rapport 2026 sur le paysage des cybermenaces au Canada

Extorsion, vol d'identité et ingénierie sociale des services d'assistance dans une économie infonuagique

Odin by Brandefense

Période de recherche: 1er janvier-18 novembre 2026

Version 1.0 · Public Research Edition · TLP:CLEAR · 21 novembre 2026

107 sur 250

organisations avaient un identifiant mis en vente le jour de la vérification

12 124-12 656

publications liées à la criminalité recensées parmi les 43 549 publications étiquetées lues

3

intrusions hacktivistes dans des systèmes de commande canadiens, cités par le Centre pour la cybersécurité (octobre 2025)

13 sur 22

banques émettrices de cartes avec un identifiant mis en vente en cours, premier élément à trier

TABLE DES MATIÈRES

Table des matières

Translated with AI

Cette édition a été traduite avec l'aide de l'intelligence artificielle à partir de l'original anglais; la version anglaise fait foi.

01	Sommaire exécutif	04
	Carte du rapport	08
02	Le contexte numérique et le contexte des menaces au Canada	09
03	Exposition nationale : 250 grandes organisations	13
04	Ce que nous observons sur le web clandestin	22
05	Exemples de ciblage par secteur	39
06	Hacktivisme, DDoS et technologie opérationnelle	46
07	Acteurs de la menace	50
08	L'économie de la fraude	66
09	Analyse approfondie : banques et finance	73
10	Réglementation et réponse nationale	76
11	Perspectives	80
12	Plan d'action	84
A	Annexe A. Méthode	92
B	Annexe B. Registre des preuves	95
C	Annexe C. Sources	96
D	Annexe D. Glossaire	101
	À propos de ce rapport	103

Conseil d'administration et direction	01 03 12
RSSI et responsables de la sécurité	03 06 07 09 10 12
SOC et renseignement sur les menaces	04 06 07 08 12 A B
Fraude et protection de la clientèle	04 05 08 09
Communications et affaires juridiques	06 10 12

À propos de cette édition

Préparé par Odin by Brandefense à partir des données de Brandefense Blackhole, Ransompedia et Atlas. Analyse et premières versions par des agents d'IA (Anthropic Claude); constatations revues par les analystes de Brandefense avant la publication. Résumé de la méthode à l'annexe A.

CHAPITRE 01

Sommaire exécutif

01

CE CHAPITRE RÉPOND À LA QUESTION

Que s'est-il passé en 2026, qu'est-ce qui compte le plus pour les organisations canadiennes et que doivent décider les dirigeants en premier?

4

décisions pour les dirigeants, chacune appuyée par des données des chapitres

Quatre décisions pour les dirigeants 06

L'année en chiffres 07

CHAPITRE 01

Sommaire exécutif

EN BREF

En 2026, la menace pour les organisations canadiennes était l'extorsion de données et le vol fondé sur l'identité. Ransompedia compte 386 inscriptions canadiennes acceptées, près du Royaume-Uni. L'hameçonnage vocal a causé plusieurs atteintes signalées dans des cabinets d'avocats; d'autres incidents confirmés touchaient des comptes détournés ou des données infonuagiques, sans voie d'accès initiale établie. Sur 250 grandes organisations, 107 avaient un identifiant mis en vente lors de la vérification. Ordre d'action : verrouiller les réinitialisations au service d'assistance, valider chaque mise en vente, puis retirer les systèmes de commande d'Internet.

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

Ce rapport combine trois sources de données propres à Brandefense et des informations publiques vérifiées. **Brandefense Blackhole** a fourni 696 200 publications étiquetées comme concernant le Canada. Nous en avons lu un échantillon qui comprend la plupart des publications de forum étiquetées. Blackhole a aussi fourni des données d'appareils infectés et d'identifiants pour 250 organisations sélectionnées, et des données de cartes apparues en clair dans des publications. **Ransompedia** a fourni les inscriptions sur les sites de fuite de rançongiciels pour le Canada et trois pays de comparaison. Les cotes d'exposition **Atlas** ont été calculées pour les 250 organisations. Ces populations sont distinctes et ne sont jamais additionnées.

1. L'extorsion de données est stable et proche du niveau britannique. Ransompedia compte 386 inscriptions acceptées visant des organisations canadiennes et datées du 1er janvier au 18 novembre 2026, contre 406 pour toute l'année 2025, un rythme annuel semblable ou légèrement supérieur [S6]. Le Royaume-Uni en comptait 377 et l'Australie 169 sur la même période. Qilin (48), The Gentlemen (34) et Akira (33) arrivaient en tête. Les inscriptions sont des revendications, non des atteintes confirmées. Les entreprises de fabrication, de construction et de services-conseils sont les plus souvent nommées (chapitre 7).

2. L'hameçonnage vocal a causé plusieurs atteintes signalées dans des cabinets d'avocats. Le 28 octobre, le Centre canadien pour la cybersécurité a mis en garde contre une campagne d'hameçonnage vocal visant les services d'assistance d'organisations canadiennes. Cette campagne contourne l'AMF classique au moyen d'un relais en temps réel et vole des données SaaS [S15]. Selon le Globe and Mail, quatre grands cabinets d'avocats de Toronto ont subi une atteinte de cette façon en octobre [S16]. Loblaw, Telus Digital, Canada Life et la plateforme d'apprentissage Canvas ont aussi confirmé des incidents en 2026 touchant des comptes ou des données infonuagiques [S22][S23][S24][S25]. Ces divulgations confirment l'utilisation abusive de comptes ou l'exposition de données infonuagiques, sans établir l'accès initial.

3. 107 des 250 organisations avaient un identifiant mis en vente lors de la vérification. Selon les cotes Atlas, la note globale des 250 organisations est de 59 sur 100 (0 = aucun risque observé, 100 = le plus élevé). Une mise en vente indique à un défenseur de chercher un compte actif; elle ne dit pas combien de comptes ni à qui ils appartiennent. Presque toutes les organisations présentent des associations à des appareils infectés et à des identifiants historiques. Ces chiffres sont cumulatifs et doivent être validés; ils n'établissent pas une atteinte [S3] [S4].

4. Des hacktivistes et d'autres attaquants ont atteint des systèmes de commande exposés. Le Centre pour la cybersécurité a signalé qu'en octobre 2025, un acteur prorusse avait manipulé des vannes d'un réseau d'eau municipal. Il a aussi signalé que d'autres acteurs avaient interagi avec une jauge de carburant d'aéroport et un silo à grains [S17]. Il a décrit une situation qui se détériore. En juillet 2026, une petite municipalité du Québec a signalé une attaque contre sa station d'eau potable. Citant les experts en sécurité de la MRC, elle l'a attribuée à un groupe organisé basé en Russie [S21]. Notre propre collecte ne contenait presque aucune liste de cibles hacktivistes visant le Canada en 2026.

5. Un vaste marché clandestin fait le commerce d'identités et de comptes canadiens. Sur les 43 549 publications étiquetées Canada que nous avons lues, 12 124-12 656 étaient liées à la criminalité (annexe A.2). Elles concernent surtout la fraude par carte (carding), le commerce de comptes, les offres de données, les services d'identité et l'hameçonnage. Des vendeurs de forums ont annoncé des données de clients attribuées à deux entreprises de télécommunications nationales, à un assureur vie et à un hôpital de l'Ontario. Seule l'offre visant l'assureur peut être rattachée à un incident confirmé. Les pertes liées à la fraude signalées au Centre antifraude du Canada ont dépassé 704 millions de dollars canadiens en 2025 [S13].

Quatre décisions pour les dirigeants

1. **Verrouiller les réinitialisations par le service d'assistance.** Exiger une vérification par rappel à un numéro connu avant toute réinitialisation de mot de passe ou d'AMF. Faire passer les utilisateurs à distance et privilégiés à une AMF résistante à l'hameçonnage. Ce contrôle vise la voie d'hameçonnage vocal à l'origine des atteintes signalées dans des cabinets d'avocats (§7.3).
2. **Traiter chaque mise en vente d'identifiant en cours comme un déclencheur d'incident, non une statistique.** Acheminer chaque mise en vente en cours liée à vos domaines vers l'équipe responsable des identités et consigner une décision dans un délai de 5 jours ouvrables. Organiser dès le jour 1 la surveillance des mises en vente d'identifiants et des appareils infectés, par une équipe interne ou un fournisseur (§12.1).
3. **Retirer les systèmes de commande d'Internet.** Placer tout accès à distance aux commandes d'eau, d'énergie, de bâtiments ou industrielles derrière un serveur de rebond avec AMF. Vérifier le processus physique avant de commenter toute revendication (§6.4).
4. **Se préparer à l'extorsion et à plusieurs organismes de réglementation à la fois.** Répéter un scénario d'extorsion par vol de données avec les délais de déclaration de chaque organisme de réglementation qui vous concerne. Inclure la Loi sur la protection des cybersystèmes essentiels une fois votre organisation désignée (chapitre 10).

L'année en chiffres

386

Inscriptions de rançongiciels acceptées par Ransompedia pour le Canada, datées du 1er janv. au 18 nov. 2026 (406 en 2025)

CE QUE CE N'EST PAS

Pas des atteintes confirmées; les cas non inscrits et non publiés sont invisibles

696 200

Publications de Blackhole étiquetées comme concernant le Canada, 1er janv.-18 nov. 2026

CE QUE CE N'EST PAS

Pas un nombre d'attaques; janvier et février sont dominés par des annonces de robots en turc

12 124-12 656

Publications liées à la criminalité directement recensées parmi les 43 549 publications étiquetées lues (12 124 strictement pertinentes plus 532 limites; annexe A.2)

CE QUE CE N'EST PAS

Pas un recensement complet de l'étiquette ni des incidents uniques; la projection graphique de 93 500-99 400 est une fourchette modélisée non reproductible

250

Grandes organisations publiques et privées évaluées selon la méthode Atlas

CE QUE CE N'EST PAS

Pas un échantillon aléatoire; pas une estimation de prévalence nationale

644 465

Appareils infectés associés à ces 250 domaines (32 833 classés « employé »); cumulatif

CE QUE CE N'EST PAS

Pas seulement 2026, pas des personnes uniques, pas des infections actuelles vérifiées

39,7 millions

Enregistrements historiques d'identifiants pour les mêmes domaines (bases de données d'atteintes, journaux de vol d'informations, listes combinées); cumulatif

CE QUE CE N'EST PAS

Pas des comptes uniques ni des mots de passe actifs; les totaux des télécoms sont surtout des boîtes aux lettres de clients

107 sur 250

Organisations ayant un identifiant mis en vente au moment de la vérification

CE QUE CE N'EST PAS

Pas un nombre de comptes ni d'atteintes confirmées

374

Cartes de paiement distinctes associées au Canada vues en clair dans les publications lues (279 attribuées à un émetteur canadien nommé)

CE QUE CE N'EST PAS

Pas un montant de pertes liées à la fraude; portée étroite (§8.5)

69 %

des 250 organisations appliquent DMARC (173)

CE QUE CE N'EST PAS

Pas une mesure du succès de l'hameçonnage ni de la sécurité de la livraison

704 millions CAD

Pertes liées à la fraude signalées au Centre antifraude du Canada en 2025 [S13]

CE QUE CE N'EST PAS

Pas la fraude totale; le centre estime que seulement 5-10 % des fraudes sont signalées [S79]

Carte du rapport

Douze chapitres, cinq parcours de lecture. Commencez par la ligne qui correspond à votre rôle; chaque chapitre s'ouvre sur la question à laquelle il répond, et les chapitres 2-12 se terminent par trois points à retenir.

Conseil d'administration et direction	Que s'est-il passé, quel est notre degré d'exposition et que devons-nous décider?	01 03 12
RSSI et responsables de la sécurité	Quelles expositions sont les nôtres, quels acteurs comptent et quels contrôles passent en premier?	03 06 07 09 10 12
SOC et renseignement sur les menaces	Qu'ont publié les acteurs, quels sont leurs liens et quelles techniques ont-ils utilisées?	04 06 07 08 12 A B
Fraude et protection de la clientèle	Comment les identités, les comptes et les cartes de Canadiens sont-ils échangés, et où les banques le constatent-elles?	04 05 08 09
Communications et affaires juridiques	Comment parler des revendications non vérifiées, et quelles obligations de déclaration s'appliquent?	06 10 12

01 Sommaire
Ce qui s'est passé en 2026 et ce que les dirigeants doivent décider en premier

02 Contexte
Quelles caractéristiques du Canada et quels chiffres officiels encadrent l'année

03 Exposition nationale
Degré d'exposition de 250 grandes organisations, avec la cote Atlas nationale

04 Web clandestin
Ce que les criminels publient sur le Canada une fois le pourriel retiré

05 Secteurs
Quels secteurs sont nommés et quelle réponse chacun exige

06 Hacktivisme et TO
Ce qui a été revendiqué, ce que les autorités ont signalé, comment se préparer

07 Acteurs de la menace
Qui sont les acteurs, quels sont leurs liens, ce que disent les rapports

08 Économie de la fraude
Comment les identités et les comptes sont convertis en argent

09 Secteur bancaire
Où se situe l'exposition visible des banques

10 Réglementation
Ce qui a changé en 2026 et quelles obligations s'appliquent

11 Perspectives
Ce qu'il faut prévoir et ce qui changerait le plan

12 Plan d'action
Qui fait quoi en 90 jours

CHAPITRE 02

Le contexte numérique et le contexte des menaces au Canada

CE CHAPITRE RÉPOND À LA QUESTION

Quelles caractéristiques du Canada façonnent les menaces décrites dans ce rapport, et que disent déjà les chiffres officiels?

95,2 %

taux de pénétration d'Internet, avec 42,8 millions de connexions cellulaires

2.1 Une population connectée et dépendante du nuage 10

2.2 Ce que dit l'évaluation nationale 10

2.3 Chiffres officiels de l'année 11

2.4 Événements ayant suscité des avertissements officiels en 2026 12

2.5 Un État fédéral aux responsabilités partagées 12

CHAPITRE 02

Le contexte numérique et le contexte des menaces au Canada

EN BREF

Le Canada est une grande économie très connectée dont les données sont réparties entre des systèmes fédéraux, provinciaux et privés. Le rançongiciel est la principale menace cybercriminelle pour les infrastructures essentielles, et des acteurs étatiques mènent de l'espionnage et du prépositionnement (obtenir un accès maintenant pour perturber plus tard). Les pertes de fraude signalées au centre national antifraude ont dépassé 700 millions CAD en 2025. Prévoyez le rançongiciel, l'espionnage étatique et la fraude, et signalez les incidents tôt : les chiffres officiels en dépendent.

2.1 Une population connectée et dépendante du nuage

Le Canada comptait environ 40,5 millions d'habitants et 38,6 millions d'internautes en octobre 2026, soit un taux de pénétration de 95,2 %. Il comptait 42,8 millions de connexions cellulaires (106 % de la population) et 34,7 millions d'identités d'utilisateurs de médias sociaux [S9]. L'anglais porte l'essentiel des publications criminelles pertinentes que nous avons lues pour le Canada; l'étiquette brute est gonflée par des pourriels en turc et en chinois (chapitre 4). Le français y est rare; la fraude en français visant les francophones du Canada, au Québec et ailleurs, est donc probablement sous-représentée dans nos observations. La plupart des échanges clandestins liés au Canada passent par des canaux Telegram et forums anglophones qui servent aussi les États-Unis, le Royaume-Uni et l'Australie.

2.2 Ce que dit l'évaluation nationale

Le Centre canadien pour la cybersécurité (le Centre pour la cybersécurité) a établi le cadre dans son Évaluation des cybermenaces nationales 2025-2026 [S10]. Voici ses principales évaluations, telles que le Centre pour la cybersécurité les formule :

- **Le rançongiciel** est la principale menace cybercriminelle pour les infrastructures essentielles du Canada, selon l'évaluation, et la cybercriminalité en tant que service le rend peu coûteux à exploiter.
- **La République populaire de Chine** a le programme cybernétique étatique le plus sophistiqué et le plus actif contre le Canada, selon l'évaluation.
- **La Russie**, selon l'évaluation du Centre pour la cybersécurité, cherche à affronter et à déstabiliser le Canada, et des acteurs non étatiques prorusses ciblent des organisations canadiennes.
- **L'Iran** emploie les cyberactivités pour contraindre et harceler, et le Centre pour la cybersécurité juge qu'il a probablement accès à certains réseaux canadiens.
- **L'Inde** mène probablement du cyberespionnage contre les réseaux du gouvernement du Canada, selon la même évaluation.

- **La Corée du Nord** présente une menace cybercriminelle persistante et bien dotée pour les personnes et les organisations au Canada, sans menace stratégique comparable à la Chine ou à la Russie, selon l'évaluation.

Nous présentons ces éléments comme les évaluations du Centre pour la cybersécurité. Ils ne constituent pas une attribution propre à ce rapport, et les données des chapitres suivants sont surtout de nature criminelle, non liées à des États.

2.3 Chiffres officiels de l'année

Les chiffres officiels montrent l'ampleur de l'activité signalée. Ils utilisent des unités et des périodes différentes; il ne faut donc ni les additionner ni les comparer comme une tendance.

Source	Chiffre	Période et unité
Rapport annuel du Centre de la sécurité des télécommunications (CST)	3 216 cyberincidents ayant fait l'objet d'une intervention : 1 528 fédéraux et 1 688 visant d'autres entités canadiennes [S11]	Exercice avril 2025-mars 2026
Perspectives de la menace des rançongiciels du Centre pour la cybersécurité	Les incidents de rançongiciel connus du Centre pour la cybersécurité ont augmenté en moyenne de 26 % par année de 2021 à 2024; aucun chiffre brut [S12]	Années civiles, incidents connus seulement
Enquête auprès des entreprises de Statistique Canada	16 % des entreprises canadiennes sondées ont déclaré un cyberincident ayant eu des répercussions en 2025 (stable par rapport à 2023); parmi les entreprises touchées, la part des rançongiciels est passée de 13 % en 2023 à 8 % en 2025 [S80]	Années civiles 2023 et 2025; entreprises de 10 employés ou plus de la plupart des secteurs, hors administration publique
Centre antifraude du Canada	Plus de 704 millions de dollars canadiens perdus en 2025, selon plus de 112 000 signalements; on estime que seulement 5-10 % des fraudes sont signalées [S13] [S79]	Année civile 2025, pertes signalées
Commissariat à la protection de la vie privée du Canada	Près de 700 déclarations d'atteinte provenant d'entreprises, touchant plus de 20 millions de Canadiens, et environ 450 provenant d'institutions fédérales [S14]	Exercice 2025-2026

Le rapport du CST recense aussi 67 avis de pré-rançongiciel transmis à des organisations canadiennes en 2025-2026 [S11]. Les Perspectives de la menace des rançongiciels en indiquaient 336 pour 2024-2025 [S12]. Les deux documents n'expliquent pas l'écart; nous ne l'interprétons donc pas comme une baisse des rançongiciels.

2.4 Événements ayant suscité des avertissements officiels en 2026

Trois événements ont suscité des avertissements officiels de cyberactivité hostile contre le Canada en 2026.

- **L'anniversaire de l'invasion de l'Ukraine par la Russie.** Le 19 février, le CST a indiqué que des acteurs prorusses avaient ciblé des réseaux gouvernementaux, militaires, privés et d'infrastructures essentielles au Canada. Il a exhorté les organisations à s'attendre à des perturbations [S20].
- **Les frappes américaines et israéliennes contre l'Iran du 28 février.** Le 1er mars, le Centre pour la cybersécurité a évalué que des hacktivistes pro-iraniens considéreraient probablement le Canada comme une cible de perturbations peu sophistiquées. Il a aussi évalué que des acteurs étatiques iraniens espionnent probablement des militants et des journalistes au Canada [S18].
- **La Coupe du monde de la FIFA.** Le tournoi s'est déroulé du 11 juin au 19 juillet et comprenait des matchs à Toronto et à Vancouver. Le Centre pour la cybersécurité a jugé que le tournoi serait presque certainement ciblé par des criminels et par des acteurs étatiques et non étatiques [S19].

2.5 Un État fédéral aux responsabilités partagées

La gouvernance de la cybersécurité au Canada est partagée. Le CST et son Centre pour la cybersécurité dirigent la défense technique et l'intervention en cas d'incident à l'échelle fédérale. La Gendarmerie royale du Canada (GRC) et son Centre national de coordination en cybercriminalité dirigent l'application de la loi fédérale contre la cybercriminalité, aux côtés des polices provinciales et municipales. Les atteintes à la vie privée sont déclarées au commissaire fédéral à la protection de la vie privée, aux commissaires provinciaux ou à la Commission d'accès à l'information du Québec, selon l'organisation.

En 2026, le Parlement a adopté le projet de loi C-8, qui crée la Loi sur la protection des cybersystèmes essentiels (LPCE) pour les services vitaux sous réglementation fédérale (chapitre 10). Au Québec, la page gouvernementale du ministère de la Cybersécurité et du Numérique indiquait en novembre 2026 que son contenu Web serait regroupé avec celui du Secrétariat du Conseil du trésor [S53]. Le chapitre 10 présente ce qui a changé pour les organisations.

POINTS À RETENIR

01

Le Centre pour la cybersécurité place le rançongiciel au premier rang des menaces cybercriminelles pour les infrastructures essentielles et évalue cinq programmes cybernétiques étatiques : Chine, Russie, Iran, Inde et Corée du Nord.

02

Les chiffres officiels utilisent des unités différentes : lisez chacun séparément, non comme une tendance.

03

Des événements internationaux de 2026 ont suscité des avertissements officiels de perturbations hacktivistes contre le Canada.

CHAPITRE 03

Exposition nationale : 250 grandes organisations

03

CE CHAPITRE RÉPOND À LA QUESTION

Quelle est l'exposition des 250 grandes organisations publiques et privées du Canada, notées comme Brandefense Atlas note un client, et quel signal un défenseur doit-il traiter en premier?

107 sur 250

organisations avaient un identifiant mis en vente le jour de la vérification

3.1 Fiche de l'univers 14

3.2 Cote Atlas nationale et mises en vente en cours par secteur 15

3.3 Appareils et identifiants 17

3.4 Mises en vente d'identifiants en cours 19

3.5 Domaines sosies, documents exposés et mentions 19

3.6 Hygiène du courriel et du Web 20

CHAPITRE 03

Exposition nationale : 250 grandes organisations

EN BREF

Nous avons évalué 250 grandes organisations canadiennes avec les cotes d'exposition de Brandefense Atlas. Presque toutes ont des appareils infectés et des enregistrements historiques d'identifiants associés à leurs domaines. De plus, 107 avaient un identifiant mis en vente lors de notre vérification. Au total, 173 sur 250 appliquent DMARC, mais seulement 27 publient une délégation DNSSEC. Traitez d'abord les mises en vente en cours, puis les appareils d'employés.

3.1 Fiche de l'univers

Élément	Définition
Population	250 organisations : 60 organismes publics (fédéraux, provinciaux, territoriaux et municipaux), 33 en banque et finance, 22 organisations du commerce électronique et de détail, 22 universités et conseils scolaires, 20 en énergie et services publics, 16 en transport, 13 en santé, 13 en médias et divertissement, 13 en fabrication et industrie, 12 en télécommunications, 11 en assurance, 9 en technologie et services de TI, 6 en hôtellerie. 124 du secteur public ou sociétés d'État, 126 privées
Sélection	Raisonnée : organismes fédéraux, provinciaux et municipaux, banques sous réglementation fédérale et grandes coopératives de crédit, sociétés d'État et chefs de file du marché par leur taille ou leur rôle systémique. Pas de classement selon le chiffre d'affaires; aucun classement publié des 250 premières organisations canadiennes n'a été utilisé
Unité	Un domaine principal par organisation, tiré de son site Web officiel. Les 250 domaines se résolvent dans le DNS (21 novembre 2026); les vérifications Web ont été possibles pour 184. L'appartenance des domaines a été attribuée à partir de la connaissance publique du site officiel de chaque organisation, sans confirmation indépendante
Mesures	Appareils infectés et appareils d'employés, enregistrements de bases de données d'atteintes, de journaux de vol d'informations et de listes combinées, mentions dans les clavardages et forums du web clandestin, domaines sosies, documents exposés et mises en vente en cours sur les marchés d'identifiants, à partir des mêmes données qu'Atlas; plus des vérifications publiques du DNS, du TLS et des en-têtes HTTP

Élément	Définition
Date	Chiffres lus le 21 novembre 2026. Les chiffres d'appareils, d'identifiants et de mises en vente comprennent tous les enregistrements détenus à cette date, quelle que soit la date de capture (cumulatifs, pas seulement 2026). Les mentions couvrent la dernière année; les domaines sosies couvrent ceux observés récemment
Chevauchement	Les décomptes peuvent se chevaucher entre les sources, les organisations et les personnes. Une personne peut figurer dans plusieurs sources; un appareil peut contenir des identifiants de plusieurs organisations
Non représentatif	Les résultats décrivent cette liste. Ce ne sont pas des taux de prévalence nationaux

3.2 Cote Atlas nationale et mises en vente en cours par secteur

Atlas attribue à chaque organisation une cote de 0 (aucun risque observé) à 100. La note globale nationale des 250 organisations est de 59 sur 100; les cotes par secteur ou par groupe ne sont pas publiées ici.

Comment lire les cotes Atlas.

Terme	Signification
Note globale	Le chiffre Atlas national des 250 organisations
Mise en vente en cours	Identifiant lié au domaine en vente au moment de la vérification
Historique de mises en vente	Mises en vente antérieures sur les marchés d'identifiants consignées avant la vérification actuelle (106 sur 250; en énergie et services publics, 4 des 5 domaines ayant une mise en vente en cours avaient aussi une inscription antérieure, et 1 était inscrit pour la première fois)

Les appareils et les identifiants sont quasi universels; les mises en vente en cours varient selon le secteur

Part des organisations de chaque secteur présentant le signal. Les annonces actuelles d'identifiants sont en corail.

	Appareils infectés	Appareils d'employés	Identifiants enregistrés	Mise en vente en cours	Historique de mises en vente	Domaines ensosies (30 jours)	Documents exposés
Commerce électronique et de détail (22)	95 %	95 %	100 %	77 %	77 %	91 %	95 %
Télécommunications (12)	92 %	83 %	100 %	67 %	67 %	83 %	83 %
Éducation (22)	100 %	100 %	100 %	64 %	64 %	95 %	100 %
Médias et divertissement (13)	100 %	92 %	100 %	62 %	62 %	92 %	100 %
Transport et logistique (16)	100 %	75 %	100 %	56 %	56 %	81 %	88 %
Technologie et services de TI (9)	100 %	89 %	100 %	56 %	56 %	100 %	67 %
Banque et finance (33)	100 %	91 %	100 %	42 %	42 %	94 %	94 %
Assurance (11)	91 %	73 %	100 %	36 %	36 %	100 %	82 %
Gouvernement (60)	85 %	65 %	97 %	33 %	33 %	95 %	78 %
Hôtellerie et tourisme (6)	83 %	67 %	100 %	33 %	33 %	83 %	67 %
Énergie et services publics (20)	95 %	85 %	100 %	25 %	20 %	85 %	75 %
Fabrication et industrie (13)	100 %	100 %	100 %	8 %	8 %	85 %	100 %
Santé (13)	100 %	85 %	100 %	0 %	0 %	77 %	77 %

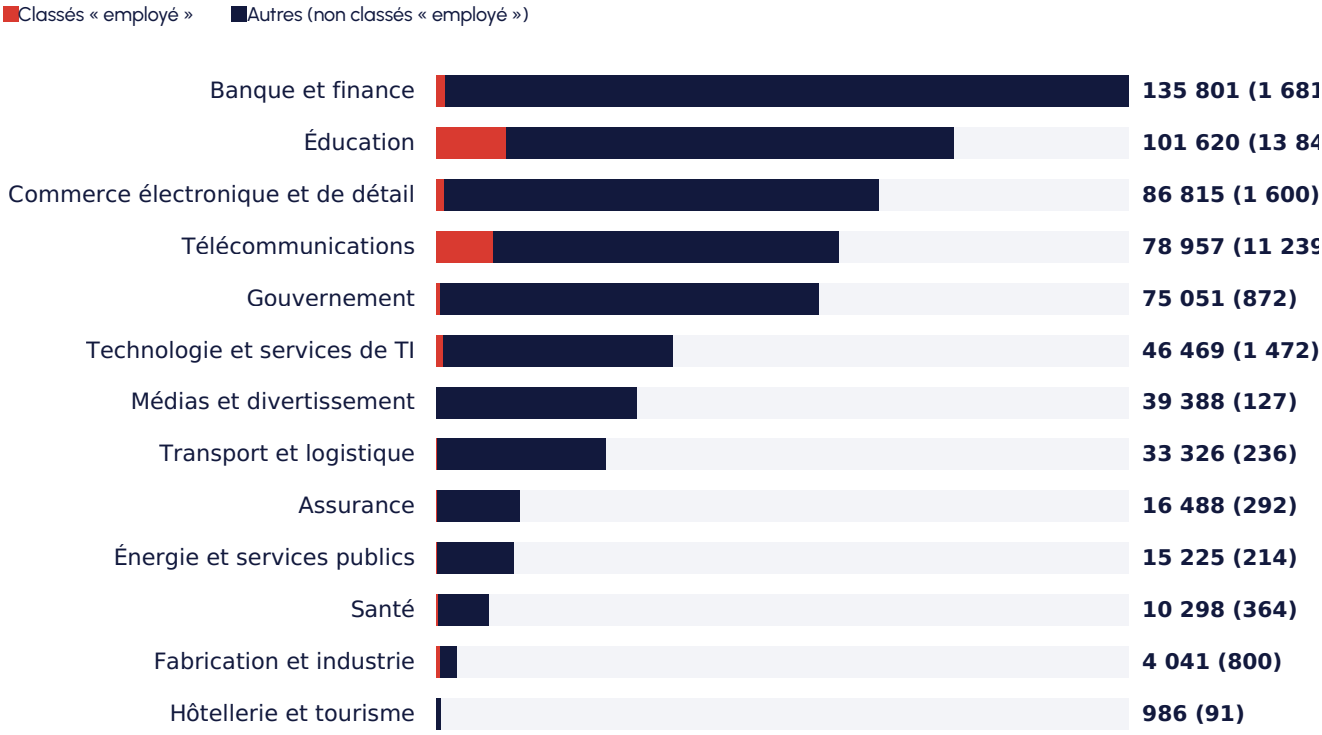
Source : associations Brandefense Blackhole et cotes Atlas de 250 organisations, lues le 21 novembre 2026 [S3][S4]. Les enregistrements sont cumulatifs, et non propres à 2026.

Secteur	Org.	Org. ayant une mise en vente d'identifiant en cours
Commerce électronique et de détail	22	17
Télécommunications	12	8
Éducation	22	14
Médias et divertissement	13	8
Transport et logistique	16	9
Technologie et services de TI	9	5
Banque et finance	33	14
Assurance	11	4
Gouvernement	60	20
Hôtellerie et tourisme	6	2
Énergie et services publics	20	5
Fabrication et industrie	13	1
Santé	13	0
Les 250	**250**	**107**

Lecture du tableau. Les mises en vente en cours varient fortement selon le secteur, d'aucune sur 13 organismes de santé à 17 sur 22 organisations du commerce électronique et de détail (§3.4).

3.3 Appareils et identifiants

La banque, l'éducation et le commerce de détail comptent le plus d'associations à des appareils infectés; les télécommunications et l'éducation détiennent la plupart des appareils classés « employé »



Source : associations Brandefense Blackhole et cotes Atlas de 250 organisations, lues le 21 novembre 2026 [S3][S4]. Les enregistrements sont cumulatifs, et non propres à 2026.

Secteur	Org. ayant des appareils infectés	Appareils (employés)	Enregistrements d'identifiants	Part des deux plus grandes org.
Banque et finance	33 sur 33	135 801 (1 681)	1 739 108	48 %
Éducation	22 sur 22	101 620 (13 845)	10 597 903	20 %
Commerce électronique et de détail	21 sur 22	86 815 (1 600)	369 019	34 %
Télécommunications	11 sur 12	78 957 (11 239)	22 565 617	88 %
Gouvernement	51 sur 60	75 051 (872)	1 460 082	33 %
Technologie et services de TI	9 sur 9	46 469 (1 472)	950 842	87 %

Secteur	Org. ayant des appareils infectés	Appareils (employés)	Enregistrements d'identifiants	Part des deux plus grandes org.
Médias et divertissement	13 sur 13	39 388 (127)	223 053	52 %
Transport et logistique	16 sur 16	33 326 (236)	186 576	42 %
Assurance	10 sur 11	16 488 (292)	327 945	74 %
Énergie et services publics	19 sur 20	15 225 (214)	389 689	30 %
Santé	13 sur 13	10 298 (364)	379 484	68 %
Fabrication et industrie	13 sur 13	4 041 (800)	424 683	44 %
Hôtellerie et tourisme	5 sur 6	986 (91)	77 835	94 %
Total	**236 sur 250**	**644 465 (32 833)**	**39 691 836**	**50 %**

Les enregistrements d'identifiants se répartissent en 14 991 506 enregistrements de bases de données d'atteintes, 1 451 109 lignes de journaux de vol d'informations et 23 249 221 entrées de listes combinées. Ces trois sources totalisent 39 691 836 enregistrements correspondant aux domaines (une connexion par ligne, sans dédoublonnage). Séparément, les 644 465 appareils infectés contiennent plus de 3,9 millions de connexions capturées pour les 250 domaines évalués et pour des sites tiers. Ce chiffre côté appareils se situe hors des 39 691 836 enregistrements, mais recoupe les 1 451 109 lignes de journaux lorsque la connexion vise l'un des 250 domaines.

Ce que cela signifie.

- **Les identifiants des télécoms sont surtout des boîtes aux lettres de clients.** Les domaines de certains fournisseurs servent aussi d'adresses de courriel grand public. Les 22,6 millions d'enregistrements d'identifiants des télécoms appartiennent donc en grande partie à des clients, non au personnel. Un seul domaine de télécommunications en compte 15,2 millions.
- **La banque porte la charge des appareils, surtout hors de la classification « employé ».** Au total, 134 120 des 135 801 appareils associés aux banques ne sont pas classés « employé ». Leurs journaux de vol d'informations contiennent une connexion au site de la banque. Il s'agit selon toute vraisemblance des ordinateurs des clients eux-mêmes, bien que leur propriété ne soit pas établie. Ces associations sont un signal de fraude et de détournement de compte; elles n'établissent pas à elles seules une intrusion dans la banque.
- **Les universités ont le plus important problème d'appareils d'employés.** L'éducation compte 13 845 appareils classés « employé », soit 42 % du total de notre liste. Le personnel et les étudiants partagent les domaines; « employé » peut donc inclure ici des étudiants. Le risque est la réutilisation d'identifiants vers des systèmes de recherche, de finance et du gouvernement.
- **L'organisation médiane n'est pas petite.** L'organisation médiane compte 534 appareils infectés et environ 11 800 enregistrements d'identifiants. L'importante main-d'œuvre canadienne, dépendante du nuage, se traduit par du volume dans tous les secteurs.

3.4 Mises en vente d'identifiants en cours

Au moment de la vérification, 107 des 250 organisations avaient au moins un identifiant lié à leur domaine mis en vente sur un marché d'identifiants surveillé. Dans la carte thermique sectorielle, l'historique de mises en vente compte les inscriptions antérieures consignées avant la vérification actuelle (106 sur 250). En énergie et services publics, 4 domaines avaient une inscription antérieure et 1 des 5 domaines actuellement inscrits l'était pour la première fois.

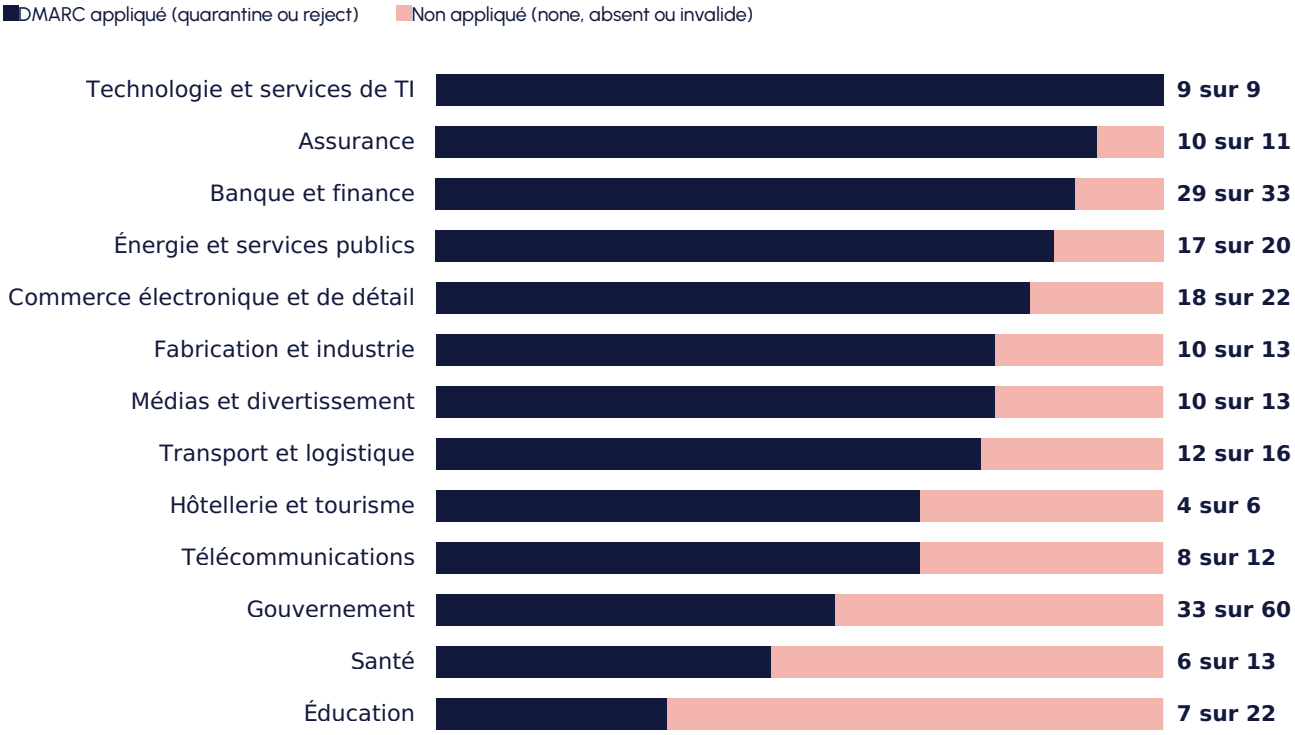
Une mise en vente en cours est le signal de marché le plus direct qu'un identifiant lié au domaine est offert. Savoir si cet identifiant fonctionne encore est précisément ce que la validation doit établir. La mise en vente n'indique ni le nombre de comptes ni leurs titulaires. Elle n'indique pas non plus si le compte est actif, protégé par l'authentification multifacteur ou déjà réinitialisé. La décision qu'elle appuie est « valider le compte maintenant », non « déclarer une atteinte ».

3.5 Domaines sosies, documents exposés et mentions

- **Domaines sosies :** 227 organisations avaient au moins un domaine sosie observé récemment (62 948 au total). Les chiffres sont plus bruités pour les marques au nom générique ou très courant. Les domaines sosies sont des candidats, non des sites d'hameçonnage confirmés.
- **Documents exposés :** 215 organisations ont au moins un document exposé qui mentionne leur domaine (3 913 au total).
- **Mentions :** 111 organisations ont été mentionnées dans des sources de clavardage clandestin au cours de la dernière année, et 116 dans des sources du web clandestin (onion). Les chiffres de mentions mesurent la visibilité, non l'hostilité.

3.6 Hygiène du courriel et du Web

La technologie, l'assurance et la banque appliquent surtout DMARC; les universités et les organismes de santé, surtout pas



Source : vérifications Brandefense des DNS publics, du TLS et des pages d'accueil de 250 domaines, 21 novembre 2026 [S5].

Résultats de courriel, de DNS et Web [S5] :

Contrôle	Résultat (sur 250, sauf indication contraire)	Lecture
DMARC reject	122	Le courriel usurpant le domaine devrait être refusé
DMARC quarantine	51	Le courriel usurpant le domaine devrait aller dans les pourriels
DMARC p=none ou absent	77 (69 none, 8 absents)	Aucune application; l'usurpation du domaine est plus facile
SPF se terminant par -all / ~all / ?all / redirect / aucun	127 / 95 / 7 / 9 / 12	12 domaines ne publient aucune politique SPF
Enregistrement DKIM trouvé	212	L'absence ne prouve pas l'absence de DKIM

Contrôle	Résultat (sur 250, sauf indication contraire)	Lecture
Enregistrement DS observé (délégation DNSSEC)	27	Aucun enregistrement DS observé pour 223 domaines; un enregistrement DS seul ne prouve pas une chaîne de confiance valide
Certificat TLS invalide	5 sur 240 vérifiés	Certificats expirés, non concordants ou non fiables
HSTS sur la page d'accueil	150 sur 184 accessibles	La plupart des sites accessibles imposent HTTPS aux visiteurs qui reviennent
Fournisseur de courriel	135 Microsoft 365, 8 Google, 6 sans MX	Les autres exploitent leur propre service de courriel ou un autre service hébergé

La technologie et la finance mènent, les universités et la santé tirent de l'arrière. Les 9 entreprises de technologie, 10 des 11 assureurs et 29 des 33 organisations de banque et de finance appliquent DMARC. Les universités et conseils scolaires (7 sur 22) et les organismes de santé (6 sur 13) l'appliquent le moins, et seulement 33 des 60 organismes gouvernementaux le font. Les valeurs de l'indice d'hygiène par secteur (annexe A.5; 0-100, une valeur élevée signifie plus faible) sont les plus élevées pour l'éducation (47) et la santé (46). Elles sont les plus basses pour la technologie (12) et l'assurance (18).

Concentration sur Microsoft 365. Au total, 135 des 250 domaines principaux acheminent leur courriel par Microsoft 365. Cette concentration compte pour le schéma de vol par le service d'assistance et le SaaS décrit au chapitre 7. Dans ce schéma, les attaquants ont pris des données dans des locataires infonuagiques après qu'un membre du personnel eut remis un identifiant.

POINTS À RETENIR

01

Les associations à des appareils et à des identifiants sont quasi universelles dans la liste; elles appellent une validation, non l'alarme.

02

Une mise en vente d'identifiant en cours est le premier élément à trier : 107 sur 250 en avaient une.

03

L'application de DMARC est courante (173 sur 250), mais les universités, les organismes de santé et de nombreux domaines gouvernementaux tirent de l'arrière, et DNSSEC est rare.

CHAPITRE 04

Ce que nous observons sur le web clandestin

CE CHAPITRE RÉPOND À LA QUESTION

Une fois le pourriel retiré, que publient réellement les criminels au sujet du Canada, et quelles offres comptent pour les défenseurs?

12 124-12 656

publications liées à la criminalité recensées parmi les 43 549 publications étiquetées lues

4.1 Fiche de l'univers 23
4.2 Plateformes, langues et volume 24
4.3 Familles criminelles après nettoyage 26
4.4 Grands ensembles de données canadiens en vente 28
4.5 Offres visant le gouvernement et offres d'accès 32
4.6 Études de cas 34
4.7 Ce qu'apportent les forums 38

CHAPITRE 04

Ce que nous observons sur le web clandestin

EN BREF

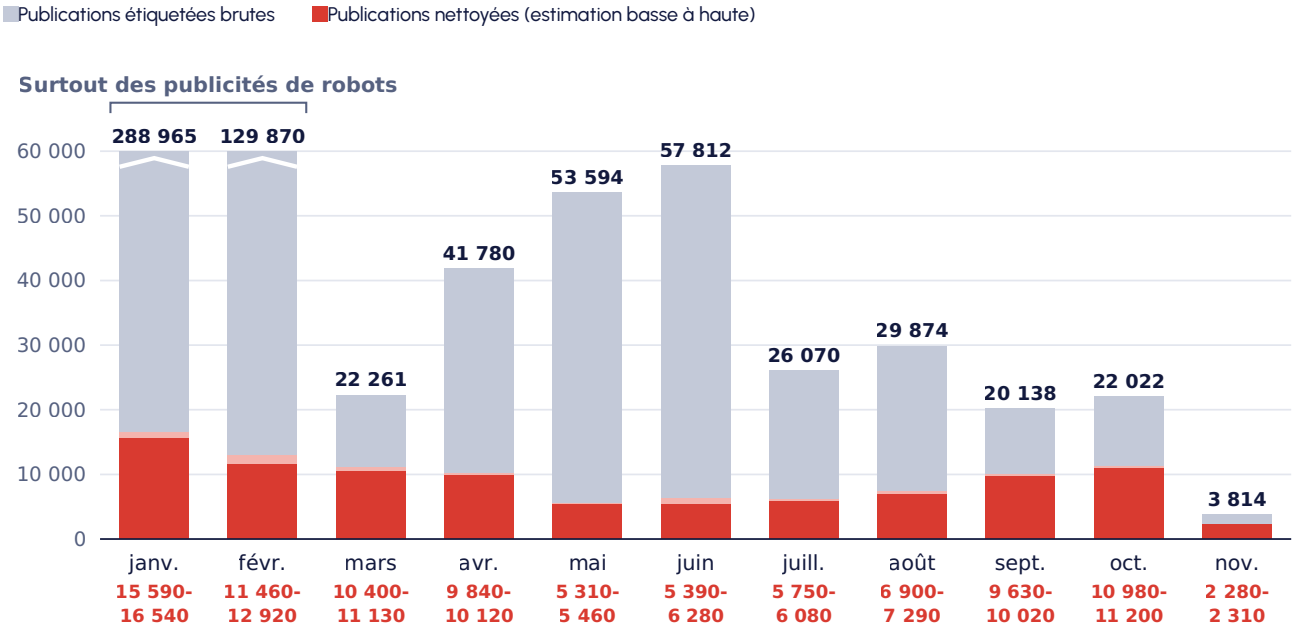
Le trafic clandestin étiqueté Canada est surtout du pourriel sous drapeau canadien : robots en turc, paris en chinois, listes de RPV en persan. Parmi les 43 549 publications étiquetées lues, 12 124-12 656 concernaient la criminalité : fraude par carte, comptes bancaires, offres de données, services d'identité et hameçonnage. Les forums portent les revendications précises visant des télécommunicateurs, un assureur et un hôpital. Appuyez-vous sur les décomptes directement lus plutôt que sur le volume brut, et triez chaque revendication selon sa provenance avant de commenter.

4.1 Fiche de l'univers

Élément	Définition
Source	Brandefense Blackhole : canaux et groupes Telegram, un ensemble de forums de cybercriminalité, des sites de collage et Discord, collectés en continu
Définition du pays	Une étiquette de pays (« cette publication porte sur le Canada, le cible ou le mentionne »)
Période	Date de publication du 1er janvier au 18 novembre 2026 (novembre partiel). La date de collecte n'est jamais utilisée
Ensemble étiqueté	696 200 publications dénombrées [S1]
Publications lues	43 549 publications étiquetées et 1 438 des 1 449 publications de forum étiquetées, plus d'autres publications sur des marques et des lieux canadiens
Total des publications lues	60 595 publications distinctes
Publications pertinentes lues	12 124-12 656 parmi les 43 549 publications étiquetées lues (12 124 strictement pertinentes plus 532 limites); les graphiques c01-c02 tracent aussi une fourchette modélisée indicative de 93 500-99 400 (somme mensuelle de 93 530-99 350; annexe A.2)
Non établi	Qu'une publication étiquetée cible le Canada, qu'une revendication soit vraie, ou que deux publications concernent le même fichier

4.2 Plateformes, langues et volume

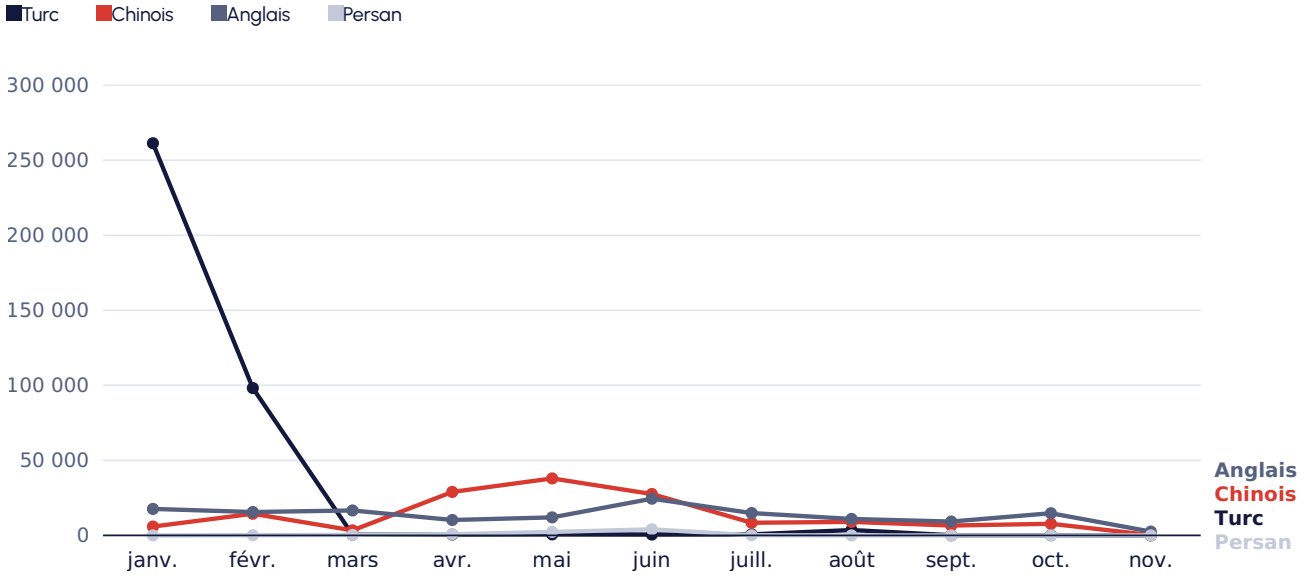
Les pourriels de robots et de paris gonflent janvier et février; la fourchette mensuelle modélisée est d'environ 5 300-16 500 publications par mois complet



Source : Brandefense Blackhole, publications étiquetées comme concernant le Canada, publications datées du 1er janvier au 18 novembre 2026, novembre partiel [S1]. Les chiffres nettoyés sont une borne supérieure.

Mesure	Valeur
Part de Telegram dans les publications étiquetées	99,75 % (694 484)
Publications de forum	1 449
Discord et sites de collage	214, 53
Publications brutes par mois	288 965 en janvier et 129 870 en février; 3 814-57 812 les autres mois
Publications étiquetées par langue (une publication peut en porter plusieurs)	turc 366 561; chinois 149 976; anglais 148 881; russe 25 679; persan 7 678; espagnol 2 766; français 320

Les publications en turc et en chinois dominent l'étiquette brute; après nettoyage, l'anglais porte l'essentiel du poids



Telegram porte 99,75 % des publications étiquetées. Les étiquettes de langue peuvent se chevaucher. Source : Brandefense Blackhole, publications étiquetées comme concernant le Canada, publications datées du 1er janvier au 18 novembre 2026, novembre partiel [S1]. Les chiffres nettoyés sont une borne supérieure.

Le pic de janvier-février n'est pas une vague d'attaques. Les publications en turc représentent 261 356 des publications étiquetées de janvier et 98 182 de celles de février. Dans les publications lues, il s'agit surtout de publicités répétées pour des robots de messagerie automatisée qui arborent des drapeaux de pays, dont celui du Canada. Les publications en chinois culminent d'avril à juin. Elles proviennent surtout de canaux de paris nommés d'après un jeu de loterie lié aux tirages du keno canadien. Les publications en persan culminent en mai et en juin; ce sont surtout des listes gratuites de configurations RPV.

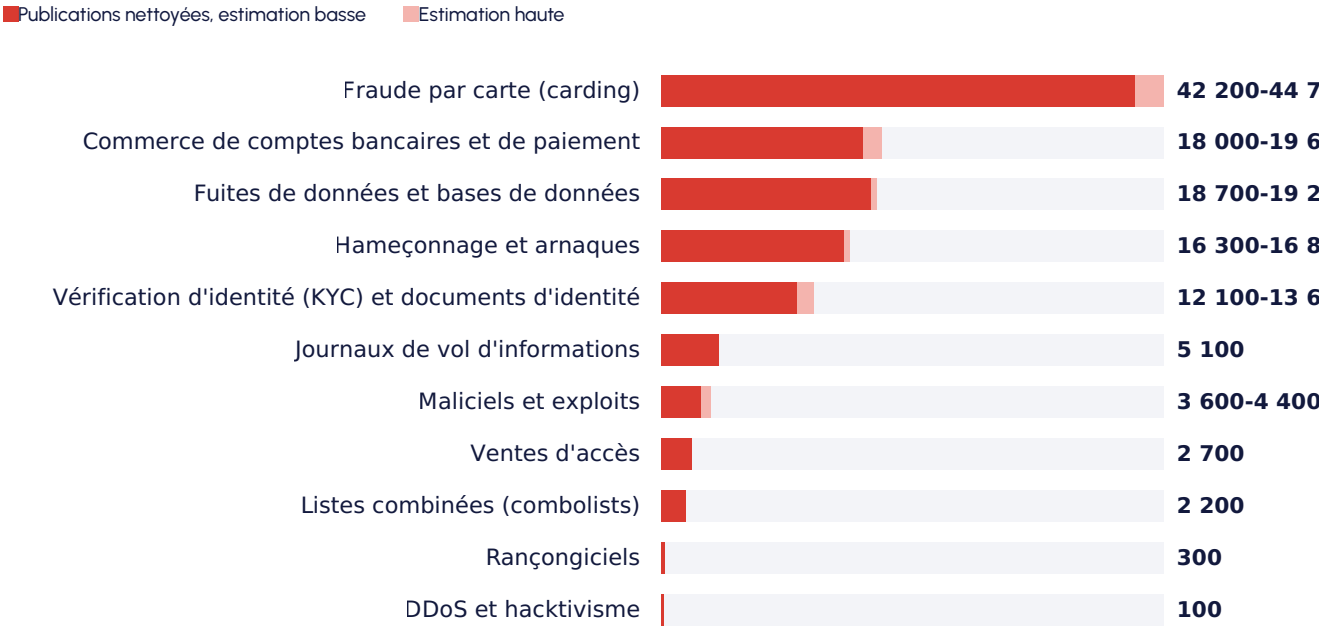
L'anglais porte la criminalité. Sur les 43 549 publications étiquetées lues, 17 579 étaient en anglais, et 9 096 d'entre elles étaient pertinentes. Seules 188 des 7 543 publications en turc l'étaient. Les publications criminelles en français étaient rares (26 après nettoyage). La fraude en français visant les francophones du Canada, au Québec et ailleurs, est donc probablement sous-représentée.

Le volume de collecte varie au fil de l'année. Le volume étiqueté de la Türkiye passe de 528 914 en mai à 107 910 en juillet, et les autres pays comparés varient aussi fortement d'un mois à l'autre. Nous ne lisons pas les variations mensuelles du volume canadien comme des tendances de la menace.

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

4.3 Familles criminelles après nettoyage

La fraude par carte mène les publications pertinentes lues; suivent le commerce de comptes, les offres de données, les services d'identité et l'hameçonnage



Source : Brandefense Blackhole, publications étiquetées comme concernant le Canada, publications datées du 1er janvier au 18 novembre 2026, novembre partiel [S1]. Les chiffres nettoyés sont une borne supérieure.

Le tableau ci-dessous présente d'abord les publications criminelles directement comptées parmi les 43 549 publications lues. Il indique aussi la fourchette modélisée indicative sur l'ensemble de l'étiquette tracée au graphique c02, non reproductible à partir des totaux publics (annexe A.2). Les familles se chevauchent : il ne faut donc pas les additionner.

Famille	Publications nettoyées lues	Fourchette modélisée sur l'étiquette (indicative)	Contenu
Fraude par carte (carding)	5 461	42 200-44 700	Résultats de vérificateurs de cartes, mises à jour de boutiques de cartes, listes de BIN « non-VBV » (cartes sans la vérification Visa des paiements en ligne), acheteurs à la recherche de cartes canadiennes
Commerce de comptes bancaires et de paiement	3 185	18 000-19 600	Offres d'achat, de location ou de vente de comptes bancaires, de technofinance et de virement électronique; « drops » (mules)

Famille	Publications nettoyées lues	Fourchette modélisée sur l'étiquette (indicative)	Contenu
Fuites de données et bases de données	3 153	18 700-19 200	Listes de consommateurs, de clients et d'entreprises; revendications visant des télécommunicateurs, des assureurs et des hôpitaux; services de recherche
Hameçonnage et arnaques	1 543	16 300-16 800	Pages d'hameçonnage bancaires et de télécommunications, leurres par texto, trousses « scampage »
Vérification d'identité (KYC) et documents d'identité	1 772	12 100-13 600	Numérisations de permis de conduire et de passeports avec égoportraits, guides de contournement de la vérification
Journaux de vol d'informations	580	5 100	Ventes de journaux et « bank logs » avec soldes
Maliciels et exploits	627	3 600-4 400	Ventes d'outils et discussions d'exploits, surtout mondiales
Ventes d'accès	589	2 700	Bureau à distance, RPV et accès d'entreprise, souvent multipays
Listes combinées (combolists)	273	2 200	Listes de courriels et de mots de passe étiquetées par pays
Rançongiciels	72	300	Relais de revendications de sites de fuite; le chapitre 7 emploie plutôt Ransompedia
DDoS et hacktivisme	25	100	Marginal dans l'étiquette; voir le chapitre 6

Beaucoup de publications nettoyées lues sont des listes multipays où le Canada n'est qu'un drapeau parmi des dizaines. Traitez tant les décomptes lus que les fourchettes modélisées comme des bornes supérieures de la criminalité propre au Canada.

Prix annoncés. Dans les publications nettoyées qui indiquent un prix, le prix demandé médian était de 120 USD pour les comptes bancaires et de paiement. Il était de 80 USD pour les services de vérification d'identité (KYC) et de documents. Les offres d'accès avaient une médiane de 140 USD et celles de journaux de vol d'informations, de 180 USD (chapitre 8). Ce sont des prix demandés, et non des ventes conclues.

4.4 Grands ensembles de données canadiens en vente

Les revendications canadiennes les plus précises apparaissent sur les forums [S2]. Aucune n'a été vérifiée de façon indépendante, et nous n'avons obtenu aucun fichier.

Date	Ensemble de données revendiqué	Volume et prix revendiqués	Lieu	Publication
9 janv.	Données d'annuaire « Canada residential »	Environ 10 millions d'enregistrements; une republication était titrée « [FAKE] »	Deux forums de fuites	B07
23 janv.	Liste de contacts d'une communauté de la diaspora (selon le vendeur)	115 000 lignes	Forum de fuites	B08
21 mars	Données clients attribuées à un télécommunicateur national et à sa sous-marque mobile	10,9 millions de lignes, 300 000 USD	Forum de fuites	B01
25 avr.	Données clients attribuées à un deuxième télécommunicateur national	1,8 million de lignes, 100 000 USD	Forum de fuites	B02
29 avr.	Enregistrements attribués au CRM infonuagique d'un assureur vie	« 5,6 M+ », téléchargement gratuit	Trois forums, avril-juillet	B03
8 mai	Données attribuées au site Web d'un organisme de réglementation financière	« 127 M+ » enregistrements	Forum de fuites	B15
14 nov.	Dossiers de patients attribués à un hôpital ontarien	1,9 million de dossiers d'identité	Forum de fuites	B13

Ce que cela indique aux défenseurs. De grands ensembles de données canadiens sont souvent annoncés, et les tailles revendiquées varient beaucoup. Certaines revendications sont incohérentes en elles-mêmes : les 127 millions d'enregistrements « d'organisme de réglementation financière » contiennent des codes de médicaments et des montants de subventions. Une seule coïncide avec un incident confirmé : l'offre visant l'assureur, publiée neuf jours après la divulgation de l'assureur lui-même (cas B). Les champs récurrents sont le nom, l'adresse, le téléphone, le courriel et la date de naissance, parfois avec le numéro d'assurance sociale. Les organisations qui vérifient leurs clients par ces champs devraient présumer qu'ils ne sont pas secrets.

Les publications telles qu'elles sont apparues, caviardées :

Fiche de preuve B01 — 21 mars 2026

Murad | Forum de fuites de données | Forum | Anglais

ORIGINAL

SELLING [national telecom] & [mobile sub-brand] Database
[national telecom] is [...] well known telecom provider. The data is 10.9 million lines, directly from [national telecom] mobile and their subsidiary [mobile sub-brand], Below I have provided some samples. [link removed]
[...] Price: $300,000
We deal strictly through GARANT [contact removed]

TRADUCTION

VENTE : base de données de [télécommunicateur national] et de [sous-marque mobile]
[télécommunicateur national] est [...] un fournisseur de télécommunications bien connu. Les données comptent 10,9 millions de lignes, provenant directement de [télécommunicateur national] mobile et de sa filiale [sous-marque mobile]. Ci-dessous, j'ai fourni quelques échantillons. [lien retiré]
[...] Prix : 300 000 $
Nous traitons uniquement par GARANT [contact retiré]

Ce que nous pouvons établir
L'offre, la taille revendiquée (10,9 millions de lignes), le prix demandé et la condition de dépôt fiduciaire (escrow).

Ce qui n'est pas établi
Que les données proviennent de l'opérateur, leur ancienneté ou une quelconque vente.

Fiche de preuve B02 — 25 avr. 2026

Murad | Forum de fuites de données | Forum | Anglais

ORIGINAL

[national telecom], [mobile brand] Database
[national telecom] is one of canadas most well known telecom providers, The data is 1.8 million lines directly from their internal network [...] Price: $100,000
Prices are negotiable
We deal strictly through GARANT [contact removed]

TRADUCTION

[télécommunicateur national], base de données de [marque mobile]
[télécommunicateur national] est l'un des fournisseurs de télécommunications les plus connus au Canada. Les données comptent 1,8 million de lignes provenant directement de leur réseau interne [...] Prix : 100 000 $
Les prix sont négociables
Nous traitons uniquement par GARANT [contact retiré]

Ce que nous pouvons établir
Une deuxième offre visant un opérateur, publiée par le même pseudonyme, avec le même contact et la même formulation de dépôt fiduciaire, cinq semaines après B01.

Ce qui n'est pas établi
L'accès au réseau interne de l'opérateur, l'origine ou l'ancienneté des données.

Fiche de preuve B03 — 29 avr. 2026

GlitchX | Forum de fuites de données | Forum | Anglais

ORIGINAL

DATABASE [life insurer]
The [life insurer] ([domain removed]) Over 5.6M Salesforce records containing PII have been compromised.
5.6M+ Records
Download
Hidden Content [...]

TRADUCTION

BASE DE DONNÉES [assureur vie]
Le [assureur vie] ([domaine retiré]) Plus de 5,6 M d'enregistrements Salesforce contenant des renseignements personnels ont été compromis.
Plus de 5,6 M d'enregistrements
Télécharger
Contenu masqué [...]

Ce que nous pouvons établir
Une inscription en téléchargement gratuit citant 5,6 millions d'enregistrements, publiée neuf jours après que l'assureur a divulgué un accès non autorisé ; republiée sur deux autres forums en mai et en juillet.

Ce qui n'est pas établi
Que le fichier corresponde aux systèmes de l'assureur, ni le nombre de personnes touchées.

Fiche de preuve B13 — 14 nov. 2026

scarlettgroup | Forum de fuites de données | Forum | Anglais

ORIGINAL

DATABASE [CA] [Ontario hospital] | [domain removed]
Hello Breach Forums Community, We have breached [Ontario hospital] and are releasing its Full DB, Enjoy! [...]
Compromised data: patient records - patient identity records (1,927,708) - patient accounts (2,014,226) - contacts (126,003) [...]

TRADUCTION

BASE DE DONNÉES [CA] [hôpital ontarien] | [domaine retiré]
Bonjour à la communauté Breach Forums, nous avons piraté [hôpital ontarien] et publions sa base de données complète. Profitez-en. [...] Données compromises : dossiers de patients - fiches d'identité de patients
(1 927 708) - comptes de patients (2 014 226) - contacts (126 003) [...]

Ce que nous pouvons établir
Une revendication de fuite avec des nombres d'enregistrements, quatre jours avant notre date limite ; le groupe figure aussi dans des inscriptions de sites de fuite.

Ce qui n'est pas établi
Aucune confirmation de l'hôpital ou des autorités au 18 novembre.

Fiche de preuve B07 — 9 janv. 2026

phoenix_leads | Forum de fuites de données | Forum | Anglais

ORIGINAL

Canada Residential Data | 2025 | 10 Million
Description: 2025's Canada Residential Phone database (short form version). Approx 10million records.
Sample: Name Address City Province PostalCode Phone
[personal data removed]

TRADUCTION

Données résidentielles du Canada | 2025 | 10 millions
Description : base de données téléphonique résidentielle du Canada de 2025 (version abrégée). Environ 10 millions d'enregistrements.
Échantillon : Nom Adresse Ville Province CodePostal Téléphone [données personnelles retirées]

Ce que nous pouvons établir
Une offre de type annuaire résidentiel ; une republication sur un deuxième forum le même jour était intitulée « [FAKE] ».

Ce qui n'est pas établi
La source, la fraîcheur ou l'unicité ; l'étiquette « fake » reflète l'avis d'un autre utilisateur, non une constatation.

Fiche de preuve B08 — 23 janv. 2026

hulky | Forum de fuites de données | Forum | Anglais

ORIGINAL

Database: [diaspora community] in Canada
Number of rows: 115K unique
Containing: [name in original script], english_name, phone, state, postal, city, address
[personal data removed]

TRADUCTION

Base de données : [communauté de la diaspora] au Canada
Nombre de lignes : 115K uniques
Contenu : [nom en écriture d'origine], english_name, téléphone, état, code postal, ville, adresse
[données personnelles retirées]

Ce que nous pouvons établir
Une liste de contacts d'une communauté de la diaspora au Canada, selon la description du vendeur ; en février, un acheteur distinct cherchait des données semblables sur des résidents du Canada et des États-Unis désignés selon leur origine.

Ce qui n'est pas établi
La source, l'exactitude ou la finalité de l'une ou l'autre publication.

Fiche de preuve B15 — 8 mai 2026

MDGhost | Forum de fuites de données | Forum | Anglais

ORIGINAL

127M [financial regulator's site] leak + login access 8 may 2026
Hi everyone, we successfully hacked [site removed] security by taking at least more than 127M user data [...] -Records: 127M+ -Data: Anti-Counterfeit Code, Health Department, Drug/Product, [...] Subsidy Value [...]

TRADUCTION

Fuite de 127M [site d'un organisme de réglementation financière] + accès de connexion 8 mai 2026
Bonjour à tous, nous avons réussi à percer la sécurité de [site retiré] en prenant au moins plus de 127M de données d'utilisateurs [...] -Enregistrements : plus de 127M -Données : code anticontrefaçon, ministère de la Santé, médicament/produit, [...] valeur de subvention [...]

Ce que nous pouvons établir
Une revendication dont les champs (codes de médicaments, ministère de la Santé, subventions) ne correspondent pas au site d'un organisme de réglementation financière.

Ce qui n'est pas établi
Aucun lien entre les données et le site nommé.

4.5 Offres visant le gouvernement et offres d'accès

Date	Publication observée	Notre lecture	Publication
17 mars	Une demande d'accès à des boîtes de courriel du gouvernement fédéral, qui nomme six domaines fédéraux	Signal de demande, et non preuve d'accès	B05
13 mai	Accès web au bureau à distance et au PGI (ERP) d'un distributeur alimentaire québécois au chiffre d'affaires de « 100 M$+ »	Une offre d'accès initial typique; la voie d'accès correspond à des passerelles de bureau à distance exposées	B06
9 nov.	« Accès administrateur complet » à un locataire CRM infonuagique exploité par un fournisseur tiers et contenant les coordonnées des participants d'un tribunal fédéral	Non vérifié; si l'offre est authentique, l'exposition se situe chez un fournisseur, et non dans les systèmes du tribunal	B04

Fiche de preuve B05 — 17 mars 2026

Anonymous poster | Groupe Telegram | Telegram | Anglais

ORIGINAL

anyone have .gc.ca email access [list of six federal domains] ??

TRADUCTION

quelqu'un a un accès à des courriels .gc.ca [liste de six domaines fédéraux] ??

Ce que nous pouvons établir
Une demande d'accès à des boîtes de courriel du gouvernement fédéral, nommant six domaines fédéraux.

Ce qui n'est pas établi
Que quiconque ait fourni un tel accès.

Fiche de preuve B06 — 13 mai 2026

XOverStm | Forum de fuites de données | Forum | Anglais

ORIGINAL

[SELLING] RDWeb + ERP Access | Canadian Food Giant | $100M+ Revenue
Target Industry: Major Food Distribution & Logistics. Region: Quebec, Canada. [...] Access Type: RDWeb (Remote Desktop Web Access). [...] Internal Domain: Local Active Directory access (.local domain). Privileges: User-level access with lateral movement potential. [...]

TRADUCTION

[VENTE] Accès RDWeb + ERP | Géant alimentaire canadien | Revenus de plus de 100 M$
Secteur ciblé : grande distribution alimentaire et logistique.
Région : Québec, Canada. [...] Type d'accès : RDWeb (accès Web au Bureau à distance). [...] Domaine interne : accès à l'Active Directory local (domaine .local). Privilèges : accès de niveau utilisateur avec possibilité de déplacement latéral. [...]

Ce que nous pouvons établir
Une offre d'accès décrivant un accès Web au bureau à distance et une visibilité sur l'ERP d'un distributeur alimentaire du Québec.

Ce qui n'est pas établi
L'identité de la victime, le fonctionnement de l'accès ou une quelconque vente.

Fiche de preuve B04 — 9 nov. 2026

DataJava | Forum de fuites de données | Forum | Anglais

ORIGINAL

[count removed] [Canada] [federal tribunal site removed] - full admin access (Salesforce) + member/contact
[...] Tenant: [third-party service provider]
Access: full admin account in Salesforce [product removed]
[...] Contact records for [participant roles removed] [...]

TRADUCTION

[nombre retiré] [Canada] [site de tribunal fédéral retiré] - accès administrateur complet (Salesforce) + membres/contacts
[...] Locataire : [fournisseur de services tiers]
Accès : compte administrateur complet dans Salesforce [produit retiré]
[...] Fiches de contact des [rôles des participants retirés] [...]

Ce que nous pouvons établir
Une revendication d'accès administrateur à un locataire de CRM infonuagique exploité par un fournisseur tiers et contenant les coordonnées des participants d'un tribunal fédéral.

Ce qui n'est pas établi
Que cet accès existe ou ait existé, que les propres systèmes du tribunal aient été atteints, ni aucune confirmation officielle.

4.6 Études de cas

Chaque cas suit la même structure : revendication, chronologie, ce que nous pouvons établir, autres hypothèses, limites et réponse proportionnée.

CAS A

A

Un même alias met en vente deux bases de données de télécommunicateurs nationaux (B01, B02)

Télécommunications

Revendication non vérifiée

REVENDICATION	Le 21 mars, l'alias Murad a mis en vente 10,9 millions de lignes qui proviendraient « directement » d'un télécommunicateur national et de sa sous-marque mobile, pour 300 000 USD. Le 25 avril, le même alias a mis en vente 1,8 million de lignes qui proviendraient « directement » du « réseau interne » d'un deuxième télécommunicateur national, pour 100 000 USD.
CE QUE NOUS POUVONS ÉTABLIR	Un même alias, avec un même contact et la même formulation d'entiercement, a publié les deux offres sur deux forums à cinq semaines d'intervalle. C'est un élément concret commun : les deux publications sont donc liées à un seul personnage.

CE QUE NOUS NE POUVONS PAS ÉTABLIR	Que l'un ou l'autre ensemble provienne du réseau de l'entreprise, son âge, ou s'ils ont été vendus. Un fichier plus ancien, attribué au deuxième télécommunicateur, a été republié sur un autre forum en avril. Nous n'avons pu rattacher les offres de mars et d'avril (B01, B02) à aucun des incidents de télécommunications confirmés dans ce rapport, et ce rapport n'indique pas quels opérateurs ces offres désignent.
AUTRES HYPOTHÈSES	Des fuites anciennes reconditionnées; des données prises chez un revendeur, chez un partenaire de facturation ou dans une liste de marketing; une intrusion réelle.
RÉPONSE	Les télécommunicateurs devraient comparer tout échantillon avec leurs schémas et avec les fichiers anciens connus avant de commenter. Les numéros de téléphone et les adresses des clients devraient être considérés comme connus des fraudeurs. Les contrôles d'échange de SIM et de transfert de numéro comptent donc plus que le secret de ces champs.

En définitive

Un persona, deux jeux de données d'opérateurs : comparez les échantillons aux schémas et aux fuites antérieures avant tout commentaire, et renforcez entre-temps les contrôles contre l'échange de carte SIM.

CAS B

B L'incident confirmé d'un assureur et une revendication de 5,6 millions d'enregistrements

Incident confirmé ; volume non vérifié

Fiche de preuve B03 | 29 avr. 2026 | Forum de fuites de données | Assurance

REVENDICATION	Le 29 avril, un auteur sur un forum a mis en vente « plus de 5,6 M d'enregistrements Salesforce » attribués à un assureur vie, en téléchargement gratuit. La publication a été republiée sur deux autres forums en mai et en juillet.
CHRONOLOGIE	Canada Life a déclaré le 20 avril qu'un compte d'employé avait servi à un accès non autorisé à certaines applications, touchant « une petite proportion » de clients [S24]. Un groupe d'extorsion de données a revendiqué l'assureur le 19 avril, selon un outil de suivi public [S7].
CE QUE NOUS POUVONS ÉTABLIR	L'assureur a confirmé un incident. Le nombre d'enregistrements de la publication est le chiffre de son auteur; nous n'avons pas obtenu le fichier.
AUTRES HYPOTHÈSES	Un extrait authentique des données de l'incident; un nombre gonflé; un ensemble de données sans lien, renommé pour profiter de l'actualité.

En définitive

L'assureur a confirmé un incident ; le chiffre de 5,6 millions est celui de l'auteur de la publication. Comparez tout échantillon à la portée de l'incident avant de vous exprimer.

Point	Revendication de l'auteur sur le forum	Version de l'entreprise	Couverture médiatique
Ce qui s'est passé	Enregistrements tirés d'un CRM infonuagique	Accès non autorisé à certaines applications au moyen d'un compte d'employé [S24]	Des milliers de personnes seraient touchées [S24]
Volume	« 5,6 M+ » enregistrements	Une petite proportion de clients [S24]	Pas chiffré à 5,6 millions
Données	« PII »	Non précisées dans la déclaration que nous avons lue	Non précisées

- **Réponse.** Toute organisation dans une situation semblable devrait comparer l'échantillon publié avec la portée de l'incident avant tout commentaire public. Les clients avisés devraient s'attendre à un hameçonnage de suivi qui cite l'incident.

CAS C

C

Le locataire infonuagique d'un fournisseur présenté comme une atteinte visant un tribunal fédéral

Revendication non vérifiée

Fiche de preuve B04 | 9 nov. 2026 | Forum de fuites de données | Gouvernement (fournisseur)

REVENDICATION

Le 9 novembre, un auteur sur un forum a mis en vente un « accès administrateur complet » à un locataire de CRM infonuagique exploité par un fournisseur tiers. Selon l'auteur, ce locataire contenait plus de 100 000 fiches de contact de participants d'un tribunal fédéral.

CE QUE NOUS POUVONS ÉTABLIR

L'offre, la liste de champs revendiquée et le locataire nommé. Nous n'avons trouvé aucune déclaration officielle à ce sujet à notre date limite.

AUTRES HYPOTHÈSES

Un accès périmé ou partiel; un locataire mal décrit; une compromission réelle du fournisseur.

RÉPONSE

Les organismes publics devraient dresser la liste des fournisseurs qui détiennent leurs données de dossiers dans des plateformes CRM infonuagiques. Ils devraient confirmer que ces locataires appliquent une AMF résistante à l'hameçonnage et la journalisation, et examiner les connexions récentes des administrateurs.

En définitive

Si elle est authentique, l'exposition se situe dans le locataire infonuagique d'un fournisseur : dressez la liste de ceux qui détiennent vos données de dossiers et vérifiez leurs connexions administrateur.

CAS D

D

Une offre d'accès chez un distributeur alimentaire québécois

Fiche de preuve B06 | 13 mai 2026 | Forum de fuites de données | Distribution alimentaire

Offre d'accès (une publication)

REVENDICATION	Le 13 mai, un vendeur sur un forum a mis en vente un accès web au bureau à distance et une visibilité « Full ERP ». L'entreprise visée serait une distributrice alimentaire québécoise au chiffre d'affaires de « 100 M$+ ». L'offre comprenait un accès au domaine de niveau utilisateur.
CE QUE NOUS POUVONS ÉTABLIR	L'offre et sa description. Les publications ne nomment pas l'entreprise.
POURQUOI C'EST IMPORTANT	Ce type d'offre d'accès est une première étape courante avant un rançongiciel, qui, au Canada, nomme le plus souvent des entreprises de fabrication, de construction et de services-conseils (chapitre 7).
RÉPONSE	Placez les passerelles web de bureau à distance derrière une AMF résistante à l'hameçonnage et déclenchez une alerte sur les nouvelles connexions provenant de réseaux d'hébergement. Examinez aussi l'exposition dans les journaux de vol d'informations du personnel qui dispose d'un accès à distance (chapitre 3).

En définitive

Les défenseurs devraient protéger les passerelles Web de bureau à distance par une AMF résistante à l'hameçonnage.

CAS E

E

Une revendication de fuite visant un hôpital quatre jours avant la date limite

Fiche de preuve B13 | 14 nov. 2026 | Forum de fuites de données | Santé

Revendication non vérifiée

REVENDICATION	Le 14 novembre, un groupe se faisant appeler scarlettgroup a affirmé avoir pénétré les systèmes d'un hôpital ontarien et a publié des nombres d'enregistrements, dont environ 1,9 million de dossiers d'identité de patients.
CE QUE NOUS POUVONS ÉTABLIR	La revendication et ses chiffres. Ni l'hôpital ni les autorités n'avaient confirmé d'incident au 18 novembre dans les sources que nous avons vérifiées.
AUTRES HYPOTHÈSES	Des données prises chez un fournisseur ou dans un ancien système; des chiffres gonflés; une intrusion réelle.

RÉPONSE

Pour les hôpitaux, la première étape consiste à comparer l'échantillon publié avec les systèmes de patients actuels et anciens, et avec les fournisseurs qui détiennent des extraits. Préparez un avis aux patients au cas où un échantillon serait vérifié.

En définitive

Comparez l'échantillon publié aux systèmes actuels, aux anciens systèmes et à ceux des fournisseurs ; préparez un avis aux patients au cas où la revendication serait vérifiée.

4.7 Ce qu'apportent les forums

Les forums ne comptaient que 1 449 publications étiquetées, mais ils regroupent presque toutes les revendications visant des organisations nommées. Ils portent aussi des demandes d'acheteurs. En janvier, un acheteur cherchait des données d'entreprises canadiennes « de services » de 2025-2026 seulement; en avril, un utilisateur demandait une base de données d'une grande institution financière canadienne. De petits téléversements automatisés de fichiers d'identifiants pour des pages de connexion canadiennes de loterie, de transport aérien et de télécommunications sont apparus de mai à août. Ces fichiers de 5 à 100 lignes chacun évoquent des extraits de journaux de vol d'informations tirés des appareils des utilisateurs plutôt qu'une atteinte aux sites.

POINTS À RETENIR

01

Le volume brut est surtout du pourriel sous drapeau; appuyez-vous sur les 12 124-12 656 publications pertinentes directement lues, et traitez les fourchettes modélisées comme des bornes supérieures indicatives.

02

Les offres sur les forums nommaient deux télécommunicateurs nationaux, un assureur vie et un hôpital; seule l'offre visant l'assureur peut être rattachée à un incident confirmé.

03

Les offres d'accès et une demande de boîtes de courriel fédérales sont des signaux de demande; vérifiez d'abord les passerelles d'accès à distance et les locataires des fournisseurs.

CHAPITRE 05

Exemples de ciblage par secteur

05

CE CHAPITRE RÉPOND À LA QUESTION

Quels secteurs canadiens sont nommés dans les publications criminelles, les revendications d'extorsion et les rapports officiels, et quelle première réponse chacun exige-t-il?

10

secteurs avec une activité observée ou signalée, du gouvernement au commerce de détail

CHAPITRE 05

Exemples de ciblage par secteur

EN BREF

Tous les grands secteurs canadiens apparaissent dans les données de 2026, mais sous des formes différentes. Les banques et les télécommunicateurs sont surtout nommés comme infrastructure de fraude. Les assureurs, les détaillants et les cabinets professionnels apparaissent comme victimes de vol de données. Les hôpitaux, les écoles et les universités sont des cibles d'extorsion; les réseaux d'eau, des cibles de manipulation. Les exemples de publications sont des revendications; les rapports officiels et d'entreprises sont indiqués comme tels. Commencez par la première réponse du secteur.

Les victimes sont décrites par leur rôle, selon la politique de l'annexe A.9, sauf si un incident a été confirmé et largement rapporté. Les exemples proviennent des publications Blackhole, de Ransompedia et des sources publiques de l'annexe A.8.

Gouvernement

Demande d'accès | revendication visant un fournisseur | prise de contrôle de compte | communication non autorisée (enquête en cours)

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Demande d'accès à des boîtes de courriel fédérales (mars; B05); accès administrateur revendiqué au locataire CRM d'un fournisseur contenant les coordonnées d'un tribunal fédéral (nov.; B04); prises de contrôle de comptes de l'Agence du revenu du Canada depuis 2020 (commissaire à la protection de la vie privée [S26]); la liste électorale provinciale, environ 2,9 millions de personnes, publiée sans autorisation sur le site Web d'un tiers (avr.; commissaire provincial à la protection de la vie privée [S31])

CE QUE CELA SIGNIFIE

Les prises de contrôle d'identité et les fournisseurs sont les principales voies d'accès; les données des citoyens se diffusent au-delà de l'organisme qui les a recueillies

PREMIÈRE RÉPONSE

Imposer une AMF résistante à l'hameçonnage pour les comptes des citoyens et du personnel; inventorier les fournisseurs qui détiennent des données de dossiers

Banques et finance

Commerce de comptes | fraude à la vérification d'identité (KYC) | fraude par carte | atteinte aux données

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Comptes vieillis de neuf banques et entreprises de technofinance nommées mis en vente (B10); guides de contournement de la vérification d'identité (KYC) à distance (B11); résultats de vérificateurs de cartes nommant 10 émetteurs (§8.5); un organisme canadien du secteur financier a signalé une atteinte de 2025 touchant environ 750 000 investisseurs (janv. [S64])

CE QUE CELA SIGNIFIE

Les publications sont dominées par les outils de fraude; les comptes mules et l'intégration des clients sont les points d'exposition

PREMIÈRE RÉPONSE

Resserrer l'intégration à distance; déclencher une alerte sur les refus des vérificateurs visant vos plages de BIN (chapitre 9)

Assurance

Incident confirmé | revendication de données | revendication d'extorsion

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Un assureur vie a confirmé un accès non autorisé au moyen d'un compte d'employé (avr.; Canada Life [S24]); une revendication de 5,6 millions d'enregistrements a suivi (B03); une revendication d'extorsion visant la branche de gestion de patrimoine d'un autre assureur (non vérifiée [S7])

CE QUE CELA SIGNIFIE

Un compte d'employé détourné et des données SaaS; accès initial non divulgué

PREMIÈRE RÉPONSE

Examiner les alertes d'exportation massive des SaaS et les règles de réinitialisation du service d'assistance

Télécommunications

Revendications de données | hameçonnage | incidents confirmés

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Revendications : deux bases de données de télécommunicateurs nationaux mises en vente par un même alias (B01, B02); une trousse d'hameçonnage visant un télécommunicateur québécois et demandant le numéro d'assurance sociale (B14). Incidents confirmés, distincts : Telus Digital a confirmé un accès non autorisé (mars [S23]); un fournisseur canadien de télécommunications a confirmé le vol de coordonnées de clients entreprises dans un système de préproduction (17 nov. [S33])

CE QUE CELA SIGNIFIE

Les télécommunicateurs sont à la fois des cibles d'atteintes et une infrastructure de fraude (SIM, transfert de numéro)

PREMIÈRE RÉPONSE

Valider les ensembles revendiqués au regard des schémas; resserrer les contrôles de transfert de numéro et d'échange de SIM

Services professionnels et juridiques

Hameçonnage vocal | incidents confirmés

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Quatre grands cabinets d'avocats de Toronto ont subi une intrusion par hameçonnage vocal visant le service d'assistance (oct. [S16]); KPMG Canada a confirmé un accès à des documents fiscaux de clients (nov. [S34])

CE QUE CELA SIGNIFIE

Les dossiers des clients sont la cible; le service d'assistance est la porte d'entrée

PREMIÈRE RÉPONSE

Vérification par rappel pour chaque réinitialisation d'AMF ou de mot de passe; alerte sur les téléchargements massifs

Commerce de détail et marques grand public

Incident confirmé | fuite de données | annonce d'accès à des comptes

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Loblaw a confirmé l'accès aux données de comptes clients, environ 2 millions de personnes touchées (commissaire à la protection de la vie privée [S22]); Canada Goose a affirmé qu'un ensemble de données de commandes divulgué par ShinyHunters était historique et ne provenait pas de ses propres systèmes (févr. [S54]); accès annoncé à des comptes de fidélité (B16; non vérifié)

CE QUE CELA SIGNIFIE

Les comptes de fidélité et de commerce électronique contiennent des données personnelles et de paiement

PREMIÈRE RÉPONSE

Surveiller le bourrage d'identifiants; imposer l'AMF pour les comptes de fidélité

Santé

Rançongiciel | revendication de données

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Rançongiciel sur les systèmes des installations du plus grand hôpital du Manitoba (août [S27]); revendication de fuite visant un hôpital ontarien (nov.; B13); Ransompedia recense 25 revendications canadiennes étiquetées « santé »

CE QUE CELA SIGNIFIE

Extorsion visant les systèmes cliniques et les systèmes du bâtiment; données des patients

PREMIÈRE RÉPONSE

Segmenter les systèmes de gestion technique du bâtiment; répéter l'avis aux patients

Éducation

Atteinte SaaS | rançongiciel | espionnage

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Atteinte à la plateforme d'apprentissage Canvas touchant des universités canadiennes (mai [S25]); des universités de Calgary, de Winnipeg et de Toronto et un district scolaire de la Colombie-Britannique ont confirmé un vol de données (juin-nov. [S28][S62][S63][S68]); campagne d'exploits Roundcube ciblant des universités canadiennes; compromission au Canada non établie (recherche d'un fournisseur [S36])

CE QUE CELA SIGNIFIE

Les universités détiennent des données de recherche et des données personnelles, et exploitent une messagerie Web exposée

PREMIÈRE RÉPONSE

Corriger la messagerie Web; imposer l'AMF au personnel et aux étudiants; examiner les locataires SaaS

Énergie et services publics

Manipulation de la TO | prise de contrôle de compte

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Manipulation hacktiviste d'un réseau d'eau municipal (oct. 2025, Centre pour la cybersécurité [S17]); une station d'eau potable québécoise attaquée (juil. [S21]); plus de 2 500 connexions inhabituelles au portail client d'Hydro-Québec, avec des mots de passe réutilisés d'autres sites (prise de contrôle de comptes clients; oct. [S32])

CE QUE CELA SIGNIFIE

Systèmes de commande et portails clients exposés

PREMIÈRE RÉPONSE

Retirer les systèmes de commande d'Internet; AMF pour les portails clients

Transport

Annonce d'accès à des comptes | revendication d'extorsion | compromission d'un fournisseur

EXEMPLE D'ACTIVITÉ OBSERVÉE OU SIGNALÉE

Accès annoncé à des comptes de grands voyageurs avec soldes indiqués (B16; validité non vérifiée); une revendication d'extorsion visant une compagnie aérienne canadienne (sept., non vérifiée [S7]); systèmes de sonorisation de trois aéroports détournés par l'intermédiaire d'un fournisseur infonuagique (oct. 2025 [S57])

CE QUE CELA SIGNIFIE

Fraude aux programmes de fidélité et systèmes des fournisseurs

PREMIÈRE RÉPONSE

Surveiller les connexions inhabituelles aux comptes de fidélité; examiner les fournisseurs ayant accès aux systèmes aéroportuaires

Lecture transversale. Les incidents confirmés en 2026 se concentrent dans les secteurs qui détiennent de grands ensembles de données clients dans des plateformes infonuagiques : commerce de détail, télécommunications, assurance, services professionnels et éducation. Les publications clandestines se concentrent dans la banque et les télécommunications, mais surtout comme outils de fraude contre les clients. Ce rapport ne mesure pas les préjudices.

Pourquoi la fabrication, la construction et le conseil sont traités au chapitre 7. Le tableau ci-dessus regroupe les 10 secteurs où les données de 2026 comprenaient des offres précises sur des forums, des divulgations confirmées ou des études de cas officielles. La fabrication (42 inscriptions acceptées dans Ransompedia), la construction (36) et le conseil (30) arrivent en tête des revendications de sites de fuite au §7.2 [S6]. Cela concorde avec l'évaluation du Centre pour la cybersécurité sur le ciblage opportuniste d'entreprises sensibles aux interruptions [S12]. Comme ces données consistent en des revendications agrégées plutôt qu'en des divulgations confirmées, la réponse figure sous le durcissement des accès à distance (cas D) et la reprise après rançongiciel (§7.2, chapitre 12).

POINTS À RETENIR

01

Les atteintes confirmées en 2026 se concentrent là où les données clients résident dans le nuage : détail, télécommunications, assurance, droit et éducation.

02

Les banques et les télécommunicateurs apparaissent surtout comme infrastructure de fraude : comptes vieillis, contournement KYC, fraude par échange de carte SIM et trousses d'hameçonnage.

03

Les réseaux d'eau et d'autres systèmes de commande exposés subissent des manipulations; vérifiez d'abord toute revendication au regard du procédé physique.

CHAPITRE 06

Hacktivisme, DDoS et technologie opérationnelle

06

CE CHAPITRE RÉPOND À LA QUESTION

Qui a revendiqué des perturbations contre le Canada en 2026, qu'ont confirmé les autorités, et pourquoi la technologie opérationnelle compte-t-elle davantage que les pannes de sites Web?

3

intrusions hacktivistes dans des systèmes de commande canadiens, cités par le Centre pour la cybersécurité (octobre 2025)

6.1 Chronologie 47

6.2 Systèmes de commande : les cas publiés par le Centre pour la cybersécurité 48

6.3 Sites Web, aéroports et revendications 49

6.4 Leçons pour les défenseurs 49

CHAPITRE 06

Hacktivisme, DDoS et technologie opérationnelle

EN BREF

En 2026, les meilleures preuves hacktivistes au Canada étaient des rapports officiels d'altérations de systèmes de commande exposés, non des DDoS. Le Centre pour la cybersécurité, qui juge la situation en détérioration, signale des acteurs prorusses et pro-Hamas sur un réseau d'eau, une jauge de carburant d'aéroport et un silo à grains en octobre 2025. En juillet 2026, une municipalité québécoise, citant des experts régionaux, a attribué l'attaque de sa station d'eau à un groupe basé en Russie. Retirez les systèmes de commande d'Internet et désignez d'avance un porte-parole.

6.1 Chronologie

15 oct. 2025	**Centre pour la cybersécurité** Octobre 2025 : acteurs prorusses et pro-Hamas dans un réseau d'eau, une jauge de carburant d'aéroport et un silo (signalé le 28 juillet 2026)
20 oct. 2025	**Centre pour la cybersécurité** Octobre 2025 : messages politiques diffusés sur la sonorisation de trois aéroports par l'entremise d'un fournisseur infonuagique (signalé en 2026)
19 févr. 2026	**CST** Des acteurs prorusses ont ciblé des réseaux au Canada; prévoir des DDoS et des défigurations autour de l'anniversaire de l'invasion
1er mars 2026	**Centre pour la cybersécurité** Selon le Centre, des hacktivistes pro-iraniens considéreront probablement le Canada comme une cible après les frappes du 28 février contre l'Iran
2 mars 2026	**Flux de défigurations** Cinq relais signalent des fichiers texte déposés le 28 février sur des hôtes Web provinciaux d'approvisionnement; non vérifié
29 mai 2026	**Centre pour la cybersécurité** Bulletin sur la Coupe du monde : le tournoi sera presque certainement ciblé par des criminels, des acteurs non étatiques et des acteurs étatiques
23 juill. 2026	**Municipalité, selon Le Soleil** Station d'eau potable du Bas-Saint-Laurent attaquée à 07:30; un employé est intervenu; selon la municipalité, citant la MRC, attaque d'un groupe organisé basé en Russie
28 juill. 2026	**Centre pour la cybersécurité** Bulletin : ciblage continu de systèmes de commande exposés au Canada; aucun incident à fort impact, mais la situation se détériore

4 sept. 2026	**Centre pour la cybersécurité** Appel à une vigilance accrue contre les DDoS et les défigurations dans un contexte de tensions mondiales et d'événements très médiatisés
8 sept. 2026	**Centre pour la cybersécurité** Campagne mondiale appuyée par l'IA contre des automates programmables exposés à Internet; ciblage observé au Canada; non attribuée

Les marqueurs corail sont des déclarations officielles; les marqueurs à contour sont des relais de tiers. Les deux éléments d'octobre 2025 précèdent la période de recherche. Nous les incluons parce que les bulletins de 2026 reposent sur eux. Les dates des éléments d'octobre sont approximatives à l'intérieur du mois.

6.2 Systèmes de commande : les cas publiés par le Centre pour la cybersécurité

Les éléments de preuve hacktivistes les plus importants pour le Canada en 2026 sont officiels; ils ne proviennent pas des canaux des acteurs. Le 28 juillet, le Centre pour la cybersécurité a publié un bulletin sur l'activité non étatique visant la technologie opérationnelle (TO) canadienne, soit les systèmes qui pilotent des processus physiques [S17]. Il y décrivait trois incidents d'octobre 2025 :

Cible	Acteur tel que décrit	Ce qui s'est passé	Impact déclaré
Réseau d'eau municipal	Acteur prorusse	Vannes de pression d'eau manipulées	Impact mineur sur le service
Système de jaugeage des réservoirs de carburant d'un aéroport	Acteur pro-Hamas	Accès au système	Consultation seulement
Silo de séchage de grains	Acteur prorusse	Réglages de température et d'humidité modifiés	Aucun dommage signalé

Le Centre pour la cybersécurité a indiqué que le Canada avait évité jusqu'ici un incident de TO à fort impact, mais il a qualifié la situation de « en détérioration » [S17]. Il a évalué que cette activité s'intensifie très probablement autour des annonces de politiques et des grands événements. Selon lui, la majeure partie de cette activité est presque certainement indépendante des États.

Le 8 septembre, le Centre pour la cybersécurité a ajouté un avis sur une campagne mondiale qui emploie des scripts générés par l'IA pour perturber des automates programmables exposés à Internet. Il a observé du ciblage au Canada et n'a pas attribué la campagne [S56].

Une station d'eau québécoise en juillet. Une petite municipalité du Bas-Saint-Laurent a signalé que sa station d'eau potable avait été attaquée à 07:30 le 23 juillet. Un employé est intervenu peu après 08:00. La municipalité, citant les experts en sécurité de la MRC, a attribué l'attaque à un groupe organisé basé en Russie. Elle a affirmé que la sécurité publique n'avait jamais été menacée [S21]. Nous rapportons cette attribution comme étant la leur, et non la nôtre; nous n'avons trouvé aucun rapport technique sur ce cas.

6.3 Sites Web, aéroports et revendications

L'évaluation du secteur de l'aviation publiée le 19 octobre par le Centre pour la cybersécurité cite la compromission d'un fournisseur infonuagique en octobre 2025. Elle a permis à des acteurs de diffuser des messages politiques sur les systèmes de sonorisation de trois aéroports canadiens [S57]. Ce cas montre comment un service tiers peut porter le message politique d'un acteur externe jusque dans un site essentiel par l'intermédiaire d'un fournisseur plutôt que, selon l'évaluation, par le réseau de l'aéroport lui-même.

Dans nos propres données, les revendications hacktivistes visant des cibles canadiennes sont presque absentes. Les publications que nous avons lues ne contenaient aucune liste de cibles DDoS de 2026 nommant des organisations canadiennes. Elles contenaient cinq relais de flux de défigurations signalant des fichiers texte déposés le 28 février sur des hôtes Web provinciaux d'approvisionnement, que nous n'avons pas pu vérifier. Cela contraste avec les avertissements officiels de février, de mars et de septembre [S18][S20][S58].

Deux explications sont possibles : les cibles canadiennes figurent dans des canaux que nous ne collectons pas, ou les acteurs ont choisi d'autres pays en 2026. Nos données ne permettent pas de les départager.

6.4 Leçons pour les défenseurs

1. **Retirez les systèmes de commande d'Internet.** Le Centre pour la cybersécurité relie ces cas à des acteurs qui recherchent des systèmes de commande exposés à Internet [S17]. Placez l'accès à distance derrière un RPV ou un hôte de rebond doté d'une AMF résistante à l'hameçonnage, et changez les mots de passe par défaut.
2. **Considérez la mesure physique comme la vérité.** Si un hacktiviste affirme contrôler une pompe ou une vanne, vérifiez le processus physique et le journal local avant tout commentaire public.
3. **Surveillez les fournisseurs, pas seulement votre propre réseau.** Le cas des aéroports est passé par un fournisseur infonuagique. Demandez à vos fournisseurs de services comment ils détecteraient et signaleraient l'usage abusif de systèmes qui diffusent vers vos sites.
4. **Convenez d'avance du message public.** Décidez à l'avance qui confirme l'état du service, et dans quels délais, si un hacktiviste publie une revendication au sujet de votre organisation.

POINTS À RETENIR

01

Les trois cas de TO d'octobre 2025 publiés par le Centre pour la cybersécurité, et non les revendications de DDoS, sont les éléments hacktivistes les plus importants pour le Canada.

02

Une municipalité québécoise a attribué une attaque de juillet contre sa station d'eau à un groupe basé en Russie, citant les experts de sa MRC; cette attribution est la leur, et non la nôtre.

03

Notre collecte ne contenait presque aucune liste de cibles hacktivistes de 2026 pour le Canada; c'est une lacune, et non une preuve de calme.

CHAPITRE 07

Acteurs de la menace

07

CE CHAPITRE RÉPOND À LA QUESTION

Qui est derrière l'activité, comment les acteurs sont-ils liés, et que disent les rapports publics sur chacun d'eux?

386

inscriptions acceptées sur des sites de fuite de rançongiciels pour le Canada, 1er janvier-18 novembre 2026

7.1 Liens entre les acteurs 51

7.2 Rançongiciels et extorsion 52

7.3 Vol de données axé sur l'identité : le schéma du service d'assistance et du SaaS 55

7.4 Espionnage lié à des États 60

7.5 Personas criminels observés dans Blackhole 63

7.6 Mesures d'application de la loi contre des acteurs opérant au Canada ou depuis le Canada 64

CHAPITRE 07

Acteurs de la menace

EN BREF

Les groupes d'extorsion sont les acteurs les plus visibles : Ransompedia compte 386 inscriptions canadiennes acceptées en 2026, près du Royaume-Uni. L'hameçonnage vocal, par de faux appels au personnel, a causé plusieurs atteintes signalées dans des cabinets d'avocats; d'autres divulgations confirment l'usage abusif de comptes, sans établir l'accès initial. Des rapports officiels et de fournisseurs signalent des acteurs liés à des États, surtout contre la recherche, les universités et la société civile. Renforcez d'abord le service d'assistance et la récupération d'identité, puis exercez-vous à un cas d'extorsion.

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

Chaque profil distingue le **comportement observé**, **la revendication de l'acteur lui-même**, **ce qui reste non résolu** et **ce que cela signifie pour les organisations**. Le niveau de confiance s'applique à une proposition précise, et non à l'acteur dans son ensemble.

7.1 Liens entre les acteurs

La carte ne relie des acteurs que lorsqu'une source contient des éléments de preuve, et chaque lien en précise la nature : publication de l'acteur lui-même, déclaration officielle, rapport public ou notre propre observation. Un lien est une association, et non la preuve d'un opérateur commun. Aucun élément ne relie entre eux les marques d'extorsion, les personas et les acteurs liés à des États présentés ici, sauf là où un lien est tracé.



7.2 Rançongiciels et extorsion

Le Canada comptait 386 inscriptions de rançongiciels acceptées en 2026, près du Royaume-Uni et plus du double de l'Australie

Canada

386

Inscriptions acceptées, 1er janv.-18 nov. 2026

2025	Toutes dates
406	1449

Groupes en 2026

Qilin, The Gentlemen, Akira, Clop, Play, INC Ransom, DragonForce, N0n

États-Unis

4532

Inscriptions acceptées, 1er janv.-18 nov. 2026

2025	Toutes dates
3996	15475

Groupes en 2026

Qilin, Akira, INC Ransom, The Gentlemen, Play, DragonForce, N0n, Settra

Royaume-Uni

377

Inscriptions acceptées, 1er janv.-18 nov. 2026

2025	Toutes dates
288	1420

Groupes en 2026

Qilin, The Gentlemen, DragonForce, Clop, 0apt, Akira, INC Ransom, SafePay

Australie

169

Inscriptions acceptées, 1er janv.-18 nov. 2026

2025	Toutes dates
129	619

Groupes en 2026

Qilin, The Gentlemen, Clop, Storm, INC Ransom, Kairos, SafePay, DragonForce

Source : inscriptions acceptées de Brandefense Ransompedia, toutes dates confondues, jusqu'au 18 novembre 2026 [S6]; ransomware.live comme contre-vérification [S7].

Ransompedia, la base de données de Brandefense sur les rançongiciels, contient 386 inscriptions acceptées sur des sites de fuite nommant des organisations canadiennes et datées du 1er janvier au 18 novembre 2026 [S6]. En comparaison, on en compte 406 pour toute l'année 2025, 377 pour le Royaume-Uni et 169 pour l'Australie pendant la même période de 2026. Les États-Unis en comptaient 4 532. Les chiffres mensuels canadiens ont varié de 23 (mars) à 45 (mai).

Groupe	Inscriptions canadiennes 2026	Part des 386
Qilin	48	12,4 %
The Gentlemen	34	8,8 %
Akira	33	8,5 %
Clop	24	6,2 %

Groupe	Inscriptions canadiennes 2026	Part des 386
Play	20	5,2 %
INC Ransom	15	3,9 %
DragonForce	15	3,9 %
Autres groupes	197	51,0 %

Les principaux secteurs dans les inscriptions étaient la fabrication (42), la construction (36), le conseil (30), la santé (25), la technologie (22), l'éducation (21) et la finance (19). Il s'agit d'étiquettes sectorielles associées à des revendications, et une même victime peut être inscrite plus d'une fois.

Microsoft a signalé en septembre que Storm-2570 avait mené des intrusions au Canada [S39]. Il s'agit d'un affilié de rançongiciel que Microsoft suit et qui travaille avec plusieurs marques de rançongiciels, dont Qilin et DragonForce.

Ce qu'est une inscription. Une inscription est l'affirmation d'un criminel selon laquelle il a attaqué une organisation ou lui a volé des données. Ce n'est pas une atteinte confirmée, et son étiquette de pays peut être erronée; Ransompedia ne compte que les inscriptions acceptées [S6]. Un outil de suivi public répertorie des revendications visant plusieurs grandes marques canadiennes en 2026. Elles visent une compagnie aérienne, la branche de gestion de patrimoine d'un assureur et une société de logiciels. Nous n'avons trouvé aucune déclaration de ces entreprises ou des autorités confirmant un incident. Nous les décrivons donc uniquement comme des revendications non vérifiées [S7].

Lorsque la déclaration d'une organisation concorde avec une revendication. Pour plusieurs organismes publics, l'organisation a confirmé un incident, puis un groupe d'extorsion l'a inscrite [S6]. C'est le cas du plus grand hôpital du Manitoba. En août, son exploitant, Shared Health, a signalé un rançongiciel touchant des systèmes des installations [S27].

Un district scolaire de la Colombie-Britannique a confirmé une attaque par rançongiciel en septembre, puis le vol de données d'élèves, de parents et de membres du personnel en octobre [S28]. Des universités de Calgary, de Winnipeg et de Toronto ont confirmé des vols de données entre juin et novembre [S62][S63][S68].

Ce que cela signifie. Sur les sites de fuite, la pression d'extorsion reste constante en 2025 et 2026. Selon Statistique Canada, la part des entreprises touchées déclarant un rançongiciel est passée de 13 % en 2023 à 8 % en 2025, avec une prévalence globale stable à 16 % [S80]. L'enquête sonde les entreprises canadiennes de 10 employés ou plus de la plupart des secteurs, hors administration publique, alors que Ransompedia compte les revendications publiques d'extorsion. Présumez un vol de données en plus du chiffrement : un test de restauration valide la reprise, non la confidentialité des fichiers.

Qilin

Agenda

Rançongiciel et extorsion de données | Motivation financière

VU DANS LES SOURCES PUBLIQUES

janv.-nov.

48 inscriptions canadiennes acceptées sur des sites de fuite, le plus grand nombre parmi tous les groupes (Ransompedia)

sept.

Nommé par Microsoft parmi les marques qu'un affilié de rançongiciel a déployées lors d'intrusions qui touchaient aussi le Canada

sept.-nov.

Les inscriptions d'un district scolaire de la Colombie-Britannique et d'une université de Toronto ont suivi des incidents confirmés par ces établissements

CIBLES REVENDIQUÉES

Entreprises, écoles, universités et organismes publics

VU DANS LES SOURCES PUBLIQUES

[S6] Ransompedia : 48 des 386 inscriptions canadiennes acceptées en 2026 ; aussi le premier groupe pour les États-Unis, le Royaume-Uni et l'Australie sur la même période

[S39] Microsoft : Storm-2570, un affilié travaillant avec Qilin et d'autres marques, a mené des intrusions au Canada

NOTRE ÉVALUATION

La marque d'extorsion la plus active contre le Canada en 2026, selon le nombre d'inscriptions. Une inscription est une revendication. Plusieurs correspondaient à des incidents confirmés par les victimes, la plupart non.

DEGRÉ DE CONFIANCE

Élevée quant à l'inscription de victimes canadiennes ; intrusions individuelles non vérifiées, sauf confirmation par la victime

The Gentlemen

Rançongiciel et extorsion de données | Motivation financière

VU DANS LES SOURCES PUBLIQUES

janv.-nov.

34 inscriptions canadiennes acceptées (Ransompedia)

sept.

Un outil de suivi public montre une revendication visant une compagnie aérienne canadienne ; aucune confirmation trouvée

CIBLES REVENDIQUÉES

Entreprises de tous les secteurs, dont une compagnie aérienne canadienne revendiquée

VU DANS LES SOURCES PUBLIQUES

[S6] Ransompedia : deuxième pour le Canada, le Royaume-Uni et l'Australie, et quatrième pour les États-Unis, en 2026

[S7] Outil de suivi public : revendication visant une compagnie aérienne canadienne en septembre, non confirmée par l'entreprise ni par les autorités dans les sources que nous avons vérifiées

NOTRE ÉVALUATION

Une marque à volume élevé dont la plus importante revendication canadienne n'était pas confirmée à notre date limite. Ses revendications doivent déclencher une validation et ne pas être traitées comme des faits.

DEGRÉ DE CONFIANCE

Élevée quant à l'inscription de victimes canadiennes ; revendication visant la compagnie aérienne non vérifiée

7.3 Vol de données axé sur l'identité : le schéma du service d'assistance et du SaaS

L'hameçonnage vocal a causé plusieurs atteintes signalées dans des cabinets d'avocats en 2026. D'autres divulgations confirment l'utilisation abusive de comptes ou l'exposition de données infonuagiques sans établir l'accès initial. Certaines atteintes sont passées par le logiciel de fournisseurs (plus bas).

Opérateurs d'hameçonnage vocal visant les services d'assistance

Non nommés par le Centre pour la cybersécurité

Vol de données et extorsion (ingénierie sociale) | Motivation financière, selon le Centre pour la cybersécurité

VU DANS LES SOURCES PUBLIQUES

janv.

Première observation d'une infrastructure nommant des organisations canadiennes, selon le Centre pour la cybersécurité

juill.

Hausse du ciblage des cabinets financiers et juridiques

19-31 oct.

Quatre grands cabinets d'avocats de Toronto atteints au moyen de faux appels de soutien informatique, selon les médias

28 oct.

Alerte AL26-028 du Centre pour la cybersécurité

CIBLES

Cabinets juridiques et financiers ; locataires Microsoft 365 et autres locataires SaaS

VU DANS LES SOURCES PUBLIQUES

[S15] Centre pour la cybersécurité : les appelants se font passer pour le soutien informatique, relaient la connexion en temps réel et contournent ainsi l'AMF classique. Ils prennent ensuite les données SaaS et peuvent envoyer des demandes d'extorsion après le vol de données

[S16] The Globe and Mail : quatre grands cabinets d'avocats de Toronto atteints au moyen de faux appels de soutien informatique ; le journal relie l'alerte à ces atteintes

[S40] Google Threat Intelligence, cité dans les notes de bas de page de l'alerte : UNC6671 cible les services financiers et les environnements infonuagiques d'entreprise ; le rapport de Google lui-même ne mentionne pas le Canada

NOTRE ÉVALUATION

La campagne que les médias ont reliée aux atteintes confirmées de 2026 dans des cabinets d'avocats. Le Centre pour la cybersécurité ne précise pas qui la mène. Les rapports de Google cités dans ses notes sont une piste, pas une attribution.

DEGRÉ DE CONFIANCE

Élevée quant au ciblage d'entreprises canadiennes par la campagne (source officielle) ; identité des opérateurs non établie

Le 28 octobre, le Centre pour la cybersécurité a publié l'alerte AL26-028 sur une campagne d'hameçonnage vocal visant le service d'assistance d'organisations canadiennes [S15]. Les appelants se faisaient passer pour le soutien informatique interne. Ils dirigeaient le personnel vers une page de connexion qui relayait les vrais identifiants en temps réel, ce qui contournait l'AMF classique (non résistante à l'hameçonnage). Les acteurs ont ensuite pris des données dans Microsoft 365 et d'autres plateformes de logiciel-service (SaaS). Selon l'alerte, ils peuvent envoyer des demandes d'extorsion après le vol de données. Ses notes citent les recherches de Google sur la même activité [S40].

Selon l'alerte, le Centre pour la cybersécurité observait depuis janvier une infrastructure nommant des organisations canadiennes. Le ciblage des cabinets financiers et juridiques a augmenté à partir de juillet, et l'activité d'octobre était centrée sur les cabinets d'avocats.

Les étapes décrites dans l'alerte correspondent aux techniques ci-dessous. Cette correspondance est la nôtre; l'alerte du Centre pour la cybersécurité est la source de chaque étape [S15].

TECHNIQUES CORRESPONDANT AUX ÉTAPES DÉCRITES DANS L'ALERTE, PAR TACTIQUE

Accès initial	Contournement des défenses	Accès aux identifiants	Persistance	Collecte	Impact
T1566.004 Hameçonnage ciblé vocal : appels se faisant passer pour le soutien informatique interne	T1656 Usurpation de l'identité du personnel informatique	T1557 Page de connexion d'adversaire au milieu (adversary-in-the-middle) relayant la véritable connexion	T1078.004 Comptes infonuagiques valides	T1530 Données provenant du stockage infonuagique (Microsoft 365 et SaaS, consultées par l'API Microsoft Graph ; canal d'exfiltration externe non précisé dans l'alerte)	T1657 Vol financier : demandes d'extorsion
		T1111 Interception de l'authentification multifacteur (relais en temps réel de l'AMF classique)			

Correspondance établie par Odin entre les étapes que décrit le Centre pour la cybersécurité dans l'alerte AL26-028 et les techniques MITRE ATT&CK ; la correspondance est la nôtre, pas celle du Centre pour la cybersécurité. L'alerte indique que l'API Microsoft Graph a servi à consulter et à exfiltrer des données Microsoft 365 sans préciser la destination externe ; aucune technique distincte de canal d'exfiltration n'est donc associée. [S15]

The Globe and Mail a rapporté que quatre grands cabinets d'avocats de Toronto avaient subi une atteinte de cette façon entre le 19 et le 31 octobre [S16]. Chaque cabinet a confirmé un incident. Le journal a relié l'alerte du Centre pour la cybersécurité à ces atteintes; l'alerte elle-même ne nomme aucune victime.

ShinyHunters

Vol de données et extorsion | Motivation financière

VU DANS LES SOURCES PUBLIQUES

févr.

Fuite d'un jeu de données de commandes d'une marque canadienne de vêtements d'extérieur ; l'entreprise a affirmé qu'il s'agissait de données historiques ne provenant pas de ses propres systèmes

mars

Revendication du vol de jusqu'à 1 Po chez Telus Digital ; l'entreprise a confirmé un accès non autorisé limité

avr.

Inscription d'un assureur vie canadien sur son site de fuite, selon un outil de suivi public

mai

Revendication de l'atteinte à la plateforme d'apprentissage Canvas qui a touché des universités canadiennes

CIBLES REVENDIQUÉES

Marques grand public, impartition en télécommunications, assurance et plateformes éducatives

VU DANS LES SOURCES PUBLIQUES

[S54] BleepingComputer : plus de 600 000 fiches de commande divulguées ; l'entreprise a affirmé que ses propres systèmes ne montraient aucune atteinte

[S23] BleepingComputer : Telus Digital a confirmé une atteinte après que le groupe a revendiqué environ 1 Po

[S25] Global News : des universités canadiennes touchées par l'atteinte à Canvas revendiquée par le groupe

NOTRE ÉVALUATION

La marque d'extorsion de données le plus souvent liée à des incidents canadiens confirmés en 2026. Les volumes qu'elle revendique dépassent régulièrement ce que les victimes confirment.

DEGRÉ DE CONFIANCE

Élevée quant à la revendication de ces victimes ; volumes revendiqués non vérifiés

D'autres incidents confirmés en 2026 touchaient des comptes ou des données infonuagiques; la voie d'accès n'est connue que pour certains. Chacun est un incident distinct; nous ne les attribuons pas à un seul acteur.

Quand	Organisation	Ce qui a été confirmé	Voie d'accès connue?	Source
Février-mars	Loblaw (détaillant en alimentation et en pharmacie)	Un groupe de pirates a accédé aux données de comptes clients; environ 2 millions de Canadiens touchés	Non	Commissaire à la protection de la vie privée [S22]
Mars	Telus Digital (branche expérience client de Telus)	Accès non autorisé à un nombre limité de systèmes; ShinyHunters revendique un vol beaucoup plus important	Non	Déclaration de l'entreprise [S23]
Avril	Canada Life (assureur vie)	Accès non autorisé à certaines applications au moyen d'un compte d'employé	Compte d'employé utilisé; mécanisme de compromission initiale non divulgué	Déclaration de l'entreprise [S24]
Début mai	Instructure (plateforme d'apprentissage Canvas)	Activité non autorisée touchant les plateformes de cours d'universités canadiennes; ShinyHunters l'a revendiquée	Non	Universités et fournisseur [S25]
Octobre-novembre (signalé les 18 et 19 novembre)	Hydro-Québec (service public d'électricité)	Prise de contrôle de comptes clients, et non atteinte aux systèmes de l'entreprise : plus de 2 500 connexions inhabituelles au portail client (20 octobre), et l'entreprise a affirmé que ses systèmes n'avaient pas été compromis; AMF par code envoyé par courriel étendue à tous les clients le 5 novembre	Oui : mots de passe réutilisés d'autres sites, selon l'entreprise	Déclaration de l'entreprise, telle que rapportée [S32]
Novembre	KPMG Canada (services professionnels)	Accès à certains documents fiscaux de clients; méthode non divulguée	Non	Déclaration de l'entreprise [S34]
17 novembre (signalé le 20 novembre)	Un fournisseur canadien de télécommunications	Un attaquant, selon l'entreprise, a pris des données de contact de clients d'affaires dans un système de préproduction	Non précisée; les données se trouvaient dans un système de préproduction	Déclaration de l'entreprise, telle que rapportée [S33]

Nous n'avons pu rattacher les offres de mars et d'avril (B01, B02) à aucun des incidents de télécommunications confirmés dans ce rapport, et ce rapport n'indique pas quels opérateurs ces offres désignent.

Plusieurs atteintes de l'année sont passées par des fournisseurs. En septembre, le commissaire à la protection de la vie privée a ouvert une enquête sur une atteinte chez IDScan.net. Ce service de numérisation de pièces d'identité est utilisé par des bars et des entreprises d'hôtellerie; l'atteinte touchait des numérisations de permis de conduire et d'autres pièces d'identité [S30]. En octobre, il en a ouvert une sur Navigate360, le fournisseur de la plateforme de signalement utilisée par les programmes Échec au crime partout au Canada [S29].

Les tribunaux de l'Ontario ont divulgué en septembre que la plateforme d'un fournisseur de gestion des dossiers avait servi à obtenir des dossiers judiciaires. Le fournisseur a indiqué que des renseignements scellés pourraient avoir été touchés [S65]. Le commissaire a aussi publié en 2026 des suivis sur deux atteintes de 2025. Chez WestJet, un contournement de l'AMF par ingénierie sociale a touché plus de 5 millions de clients et d'employés; chez Nova Scotia Power, plus de 900 000 personnes ont été touchées [S60][S61].

Deux fournisseurs du secteur de la santé figurent aussi dans les divulgations de 2026. Un hôpital pour enfants de Toronto a indiqué en août que des données d'employés et de candidats avaient été exposées par une faille dans une application tierce [S76]. Des reportages de mars ont montré qu'une attaque de 2025 contre un fournisseur de matériel médical du réseau ontarien de soins à domicile était un rançongiciel [S77].

Ce que cela signifie. Pour les organisations canadiennes, le service d'assistance, le fournisseur d'identité et les locataires SaaS constituent désormais la porte d'entrée. L'AMF résistante à l'hameçonnage, la vérification par rappel pour les réinitialisations de mots de passe et d'AMF, et les alertes sur les téléchargements massifs dans le SaaS sont les mesures qui correspondent à ces cas.

7.4 Espionnage lié à des États

L'activité liée à des États a atteint le Canada surtout par l'entremise des recherches de fournisseurs et des avis conjoints officiels. Nous présentons chaque attribution exactement comme sa source la formule.

UNC6508

Espionnage lié à un État (selon l'attribution du fournisseur) | « lien avec la RPC » (traduction), selon Google Threat Intelligence

VU DANS LES SOURCES PUBLIQUES

juin

Google signale des organisations aux États-Unis et au Canada trouvées compromises par le maliciel INFINITERED sur des serveurs de données de recherche REDCap

CIBLES

Organisations médicales et de recherche exploitant des serveurs de données de recherche

VU DANS LES SOURCES PUBLIQUES

[S35] Google Threat Intelligence : une campagne attribuée à UNC6508, un acteur de la menace ayant un lien avec la RPC ; plusieurs organisations aux États-Unis et au Canada trouvées compromises

NOTRE ÉVALUATION

Le seul rapport de fournisseur de 2026 que nous avons trouvé qui affirme que des organisations canadiennes ont été compromises par un acteur lié à un État. Les victimes et les données prises ne sont pas publiées.

DEGRÉ DE CONFIANCE

Attribution telle qu'énoncée par le fournisseur ; victimes canadiennes non nommées

Source et date	Acteur tel que nommé	Élément canadien	Formulation de l'attribution
Google Threat Intelligence, 15 juin [S35]	UNC6508	Organisations aux États-Unis et au Canada où le maliciel INFINITERED a été trouvé sur des serveurs de données de recherche REDCap	« un acteur de la menace lié à la République populaire de Chine (RPC) » (traduction)
Proofpoint, 7 juillet [S36]	UNK_MassTraction	Serveurs de messagerie Roundcube d'universités américaines et canadiennes visés par des exploits depuis mai 2026; compromission de serveurs canadiens non précisée	« probablement un acteur d'espionnage aligné sur la Chine » (traduction)
Unit 42, 12 novembre [S37]	CL-STA-1238	Un organisme canadien de défense des droits de la personne parmi les cibles; compromission non précisée	« une campagne de collecte de renseignement liée à la Chine » (traduction), avec une « confiance modérée »
Centre pour la cybersécurité avec des partenaires, 2 avril et 22 juillet [S69][S70]	Acteurs parrainés par l'État russe	Campagnes mondiales visant des routeurs et la messagerie Web Zimbra; aucune victime canadienne mentionnée	Tel qu'indiqué par les agences
Centre pour la cybersécurité, 1er mars [S18]	Acteurs étatiques iraniens	Espionnage probable de militants, de journalistes et de défenseurs des droits de la personne au Canada	Évaluation du Centre pour la cybersécurité

Référence de correctifs. Les failles Roundcube sont à l'origine de la campagne contre les universités. En février, Unit 42 a relié les trois failles de produits de périphérie à de l'activité dans plusieurs pays, dont le Canada, sans nommer d'acteur [S66][S67]. Ivanti a publié des correctifs provisoires avant le correctif permanent.

CVE	Produit	Versions touchées / corrigées	Liste des vulnérabilités exploitées connues de la CISA	Source
CVE-2024-42009	Messagerie Web Roundcube	Corrigée dans 1.5.8 et 1.6.8	Exploitée connue (NVD)	[S55]
CVE-2025-49113	Messagerie Web Roundcube	Corrigée dans 1.5.10 et 1.6.11	Exploitée connue (NVD)	[S55]
CVE-2026-1731	BeyondTrust Remote Support et Privileged Remote Access	Remote Support avant 25.3.2; Privileged Remote Access avant 25.1	Ajoutée le 13 février 2026	[S55][S66]
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM)	Jusqu'à 12.7.0.0; correctif permanent 12.8.0.0	Ajoutée le 29 janvier 2026	[S55][S67]
CVE-2026-1340	Ivanti Endpoint Manager Mobile (EPMM)	Jusqu'à 12.7.0.0; correctif permanent 12.8.0.0	Ajoutée le 8 avril 2026	[S55][S67]

Non résolu. Quelles organisations canadiennes ont été touchées dans la campagne visant les serveurs de recherche, si un serveur universitaire canadien a subi une intrusion lors de la campagne Roundcube, et ce qui a été pris. **Signification.** Les universités, les instituts de recherche et les organismes de la société civile sont les cibles canadiennes les plus souvent nommées dans les recherches de fournisseurs de 2026. Les serveurs de messagerie Web et de données de recherche exposés à Internet méritent la même rigueur de correctifs que les pare-feu de périmètre.

Réseaux gouvernementaux hors du noyau fédéral. Le CST évalue dans son rapport annuel 2024-2025 que les réseaux des gouvernements provinciaux, territoriaux, municipaux et autochtones sont des cibles de valeur pour le cyberespionnage étatique [S81]. Cette évaluation permanente est plus large que les rapports de fournisseurs de 2026 ci-dessus. Ceux-ci documentaient des intrusions sur des serveurs de recherche [S35] et le ciblage d'universités ou de la société civile [S36][S37], sans confirmer publiquement d'atteinte d'espionnage provinciale ou territoriale en 2026. Les organismes publics infranationaux devraient néanmoins appliquer la même rigueur de correctifs périphériques et de contrôles d'identité.

7.5 Personas criminels observés dans Blackhole

Murad

Persona de vendeur de données | Motivation financière

VU DANS LES SOURCES PUBLIQUES

21 mars

Met en vente 10,9 millions de lignes attribuées à un télécommunicateur national et à sa sous-marque pour 300 000 USD (B01)

25 avr.

Met en vente 1,8 million de lignes attribuées à un deuxième télécommunicateur national pour 100 000 USD (B02)

CIBLES REVENDIQUÉES

Données de clients de télécommunicateurs nationaux

DANS LEURS PROPRES MOTS

"The data is 10.9 million lines, directly from [national telecom] mobile" B01

VU DANS LES SOURCES PUBLIQUES

Aucune source publique fiable trouvée

NOTRE ÉVALUATION

Aucune source publique fiable n'a été trouvée. Un même persona relie deux offres de télécommunications à prix élevé par un contact et une formulation communs. L'origine d'aucun des deux jeux de données n'est établie. Nous n'avons pu rattacher ces offres à aucun des incidents de télécommunications confirmés dans ce rapport.

DEGRÉ DE CONFIANCE

Élevée quant à la publication des deux offres par un même persona ; origine des données non vérifiée

Pseudonymes seulement; aucun contact, lien ou identité réelle. Ces personas ont publié des offres propres au Canada sur des forums en 2026 (chapitre 4).

Persona ou marque	Rôle observé en 2026	Revendication propre	Non résolu
phoenix_leads	Auteur, sur un forum, d'un jeu de données « Canada residential » (janvier, avril)	Environ 10 millions d'enregistrements	Origine; un forum a qualifié une republication de « fausse »
CC-GuRu	Auteur, sur un forum, de grandes listes canadiennes de consommateurs et d'entreprises (avril)	40 millions de consommateurs; 400 000 entreprises	Origine, ancienneté, doublons avec d'autres listes
Maxi_Leaks	Auteur récurrent de listes « Canada » de courriels et de mots de passe (avril)	68 000-186 000 lignes chacune	Fraîcheur; répétition éventuelle des lignes
Sophia01	Auteur, sur un forum, de la base de données d'un site de rencontres (octobre)	23 Go avec mots de passe et témoins	Toute vérification

7.6 Mesures d'application de la loi contre des acteurs opérant au Canada ou depuis le Canada

Plusieurs mesures de 2026 visent des acteurs opérant au Canada ou depuis le Canada, ou une infrastructure utilisée contre des Canadiens.

- **Opération Endgame.** En juin, la Gendarmerie royale du Canada (GRC) s'est jointe à une action internationale contre le réseau de maliciels SocGholish, qu'elle a décrit comme lié au groupe cybercriminel russe Evil Corp. Elle a affirmé que le réseau avait frappé des infrastructures essentielles, des établissements d'enseignement et des gouvernements canadiens. Elle a ajouté que toutes les entités canadiennes touchées avaient été avisées [S41].
- **Maple Disruption 2.0.** Du 2 au 6 novembre, la GRC et le Centre antifraude du Canada ont dirigé plus de 50 partenaires dans 10 987 actions de perturbation contre des fraudeurs. Ils ont récupéré environ 1,06 million CAD [S42].
- **Arrestation liée à un réseau de zombies DDoS.** En mai, des policiers des États-Unis et du Canada ont porté des accusations contre un Ottawais de 23 ans soupçonné d'administrer le réseau de zombies DDoS Kimwolf [S78].
- **Arrestations liées à un « SMS blaster ».** En avril, le Service de police de Toronto a porté des accusations contre trois personnes pour avoir utilisé un « SMS blaster » mobile. L'appareil servait à envoyer des textos frauduleux; selon la police, des dizaines de milliers d'appareils s'y sont connectés. La police a parlé d'une première au Canada [S43].

POINTS À RETENIR

01

Le Canada a compté 386 inscriptions de rançongiciels acceptées en 2026, près du Royaume-Uni; les inscriptions sont des revendications, et non des atteintes confirmées.

02

L'hameçonnage vocal a causé plusieurs atteintes signalées dans des cabinets d'avocats; d'autres divulgations, comme le compte d'employé détourné d'un assureur, n'établissent pas l'accès initial. Hydro-Québec a aussi subi des connexions à des comptes clients avec des mots de passe réutilisés.

03

Les recherches de fournisseurs ont nommé des universités, des serveurs de recherche et un organisme de défense des droits de la personne comme cibles canadiennes d'espionnage lié à des États.

CHAPITRE 08

L'économie de la fraude

CE CHAPITRE RÉPOND À LA QUESTION

Comment les criminels transforment-ils les identités et les comptes canadiens en argent, et combien demandent-ils pour ce faire?

704 M CAD

pertes liées à la fraude signalées au Centre antifraude du Canada en 2025

8.1 Ce que disent les chiffres officiels 67

8.2 Commerce de comptes bancaires et de comptes de paiement 68

8.3 Identité, vérification d'identité (KYC), initiés revendiqués et vérification au comptoir 68

8.4 Trousses d'hameçonnage et comptes de fidélité 70

8.5 Données de cartes dans les publications : une vue restreinte 71

8.6 Les prix en contexte 72

CHAPITRE 08

L'économie de la fraude

EN BREF

La fraude au Canada repose sur l'identité. Des canaux clandestins vendent des comptes bancaires « vieillis », des initiés revendiqués et des guides contre les vérifications d'identité à distance. D'autres offrent une vérification en personne aux comptoirs pour des « drops » (titulaires de comptes mules). Des trousses d'hameçonnage imitent des banques et des télécoms. Les pertes signalées ont dépassé 704 millions CAD en 2025, surtout par fraude à l'investissement. Confirmez les changements de paiement par un autre canal; présumez que nom, adresse et date de naissance sont connus.

8.1 Ce que disent les chiffres officiels

Le Centre antifraude du Canada (CAFC) a reçu plus de 112 000 signalements de fraude en 2025, pour des pertes déclarées de plus de 704 millions CAD [S13]. Les pertes déclarées depuis 2022 dépassent 2,4 milliards CAD [S79]. Le centre estime que seulement 5-10 % des fraudes sont signalées; les chiffres réels sont donc plus élevés [S79].

Type de fraude (2025)	Pertes déclarées	Signalements
Investissement	351 millions CAD	4 409
Harponnage	67,9 millions CAD	813
Relation sentimentale	63,3 millions CAD	Non indiqué sur la page
Emploi	50,6 millions CAD	Non indiqué sur la page
Extorsion	23 millions CAD	2 767

La fraude d'identité a été le type le plus signalé, avec 8 403 signalements [S13]. Les pertes déclarées au CAFC ont dépassé 188 millions CAD au premier trimestre de 2026 [S71].

Le rapport spécial du commissaire à la protection de la vie privée sur l'Agence du revenu du Canada a recensé plus de 42 000 atteintes individuelles à des comptes de contribuables depuis 2020. Elles comportaient un accès non autorisé aux renseignements des contribuables ou leur modification, à des fins de demandes de prestations frauduleuses [S26]. C'est le même schéma de prise de contrôle d'identité que les publications clandestines de ce chapitre vendent comme un service.

8.2 Commerce de comptes bancaires et de comptes de paiement

Le commerce de comptes bancaires est la deuxième famille criminelle de notre échantillon lu, avec 3 185 publications nettoyées lues (fourchette modélisée sur l'étiquette de 18 000-19 600; chapitre 4). Les publications typiques vendent des comptes « vieillis » dans des banques et des sociétés de technologie financière canadiennes, avec cartes de débit et accès en ligne. D'autres recrutent des « drops » qui ouvrent des comptes pour d'autres (B10). Le virement électronique est le moyen de paiement le plus souvent nommé, avec les plateformes d'échange de cryptomonnaies. Les publications montrent des offres; elles ne montrent pas que de tels comptes ont été ouverts ou utilisés dans une banque évaluée.

Fiche de preuve B10 13 mai 2026

Calciumpound Canal Telegram Telegram Anglais

ORIGINAL

Selling [list of nine Canadian banks and fintechs] Accounts
(Creation open ups with physical debit incl.)
-FRESH OPEN UPS AVAILABLE IF NEEDED. [...] (debit+online access+creation info) {Aged over 30 days} [...]

TRADUCTION

Vente de comptes [liste de neuf banques et entreprises de technologie financière canadiennes]
(Comptes ouverts par création, carte de débit physique incluse)
-NOUVEAUX COMPTES DISPONIBLES AU BESOIN. [...] (débit + accès en ligne + renseignements de création) {Âgés de plus de 30 jours} [...]

Ce que nous pouvons établir
Une offre de comptes bancaires vieillis, ouverts avec des identités fabriquées ou empruntées, avec cartes de débit et accès en ligne.

Ce qui n'est pas établi
Que des comptes aient été ouverts dans l'une des banques nommées, ou utilisés à des fins de fraude.

8.3 Identité, vérification d'identité (KYC), initiés revendiqués et vérification au comptoir

Les publications sur la vérification d'identité (KYC) et les documents (1 772 publications nettoyées lues; fourchette modélisée sur l'étiquette de 12 100-13 600) offrent des numérisations de permis de conduire et de passeports avec égoportraits. Elles offrent aussi des guides payants pour réussir depuis l'étranger la vérification d'identité à distance d'une société de technologie financière canadienne (B11). Elles proposent enfin des « créations » : des identités synthétiques ou empruntées pour ouvrir des comptes.

Certains menus de services de fraude prétendent disposer d'initiés chez une entreprise de livraison, une banque et un fournisseur de services mobiles (B09). D'autres vendent une vérification d'identité en personne à un comptoir de service pour des « drops » (B12). Nous ne pouvons établir l'existence d'aucun initié revendiqué. Les offres montrent tout de même où les criminels situent les points faibles : la vérification en personne, la réexpédition du courrier et les services d'assistance des fournisseurs mobiles.

Fiche de preuve B11 — 5 mai 2026

bigbosskyc1 | Groupe Telegram | Telegram | Anglais

ORIGINAL

[fintech card] PROCEDURE FOR PASSPORT HOLDERS:
ALL COUNTRIES ACCEPTED [...] RATE 50$ [...] Connect vpn to canada first [...] register a new account using a fresh email [...] FOR NUMBERS USE ANY OF THESE SITES: [list removed] [...] go to [app] to complete kyc

TRADUCTION

PROCÉDURE [carte de technologie financière] POUR LES TITULAIRES DE PASSEPORT :
TOUS LES PAYS ACCEPTÉS [...] TARIF 50 $ [...] Connectez d'abord le RPV au Canada [...] créez un nouveau compte avec une adresse courriel neuve [...] POUR LES NUMÉROS, UTILISEZ L'UN DE CES SITES : [liste retirée] [...] allez dans [application] pour terminer la vérification d'identité (KYC)

Ce que nous pouvons établir
Un guide payant pour réussir depuis l'étranger la vérification d'identité à distance d'une entreprise canadienne de technologie financière, à l'aide d'un RPV (VPN) et de numéros de téléphone temporaires.

Ce qui n'est pas établi
Que la méthode fonctionne aujourd'hui.

Fiche de preuve B09 — 1er janv. 2026

Fraud-services vendor | Canal Telegram | Telegram | Anglais

ORIGINAL

MENU [...] - Fullz to BTC [...] - Creation Service [...] creations are used for opening bank accounts, loans, credit cards, and more. [...] Inside Worker(s) Available: - [delivery company] Insider - [bank] Bank Insider - [mobile carrier] Mobile Insider - Car Dealership Insider

TRADUCTION

MENU [...] - Fullz contre BTC [...] - Service de création [...] les créations servent à ouvrir des comptes bancaires, obtenir des prêts, des cartes de crédit, et plus encore. [...] Initié(s) disponible(s) : - Initié chez [entreprise de livraison] - Initié à la banque [banque] - Initié chez [opérateur mobile] Mobile - Initié chez un concessionnaire automobile

Ce que nous pouvons établir
Un menu de services de fraude annonçant des identités synthétiques et des initiés revendiqués chez une entreprise de livraison, une banque et un opérateur mobile.

Ce qui n'est pas établi
Qu'un initié existe ou soit employé par ces organisations.

Fiche de preuve B12 — 14 sept. 2026

Fraud-services vendor | Groupe Telegram | Telegram | Anglais

ORIGINAL

Service(s): [...] - [delivery company] Verif: This service consists of me verifying your drops/nips identity via [delivery company] [code type removed] that you provide. [...] - Creation Service [...]

TRADUCTION

Service(s) : [...] - Vérif [entreprise de livraison] : ce service consiste à vérifier l'identité de vos drops/nips au moyen du [type de code retiré] de [entreprise de livraison] que vous fournissez. [...] - Service de création [...]

Ce que nous pouvons établir
Un service pour réussir la vérification d'identité en personne à un comptoir de service pour des « drops », les personnes dont les comptes reçoivent les produits de la fraude.

Ce qui n'est pas établi
Que le service fonctionne ou ait été utilisé.

8.4 Trousses d'hameçonnage et comptes de fidélité

Les publications d'hameçonnage (1 543 publications nettoyées lues; fourchette modélisée sur l'étiquette de 16 300-16 800) comprennent des pages sur mesure qui imitent des banques et des entreprises de télécommunications canadiennes. Une trousse imitant une entreprise de télécommunications québécoise demande le numéro d'assurance sociale de la victime en plus des données de carte (B14). Une boutique annonçait l'accès à des comptes de fidélité de compagnies aériennes et d'hôtels avec soldes de points indiqués; la validité, la provenance et toute vente conclue ne sont pas vérifiées (B16).

Fiche de preuve B14 — 16 juin 2026

theghostorder01 | Forum de fraude | Forum | Anglais

ORIGINAL

[SELL] [regional telecom] CUSTOM SCAMPAGE FEATURES GET FULL INFO FORMAT PERSONAL INFO : FULLNAME, ADDRESS, CITY, POSTALCODE, PROVINCE, PHONE, EMAIL, DOB, SIN CARD INFO : NAME ON CARD, CARD NO, EXP, CVV RESULTS COME TO TELE , EMAIL , TXT [...]

TRADUCTION

[VENTE] PAGE D'ARNAQUE PERSONNALISÉE [télécommunicateur régional]
FONCTIONNALITÉS : OBTENTION DE TOUTES LES INFOS, FORMAT RENSEIGNEMENTS PERSONNELS : NOM COMPLET, ADRESSE, VILLE, CODE POSTAL, PROVINCE, TÉLÉPHONE, COURRIEL, DATE DE NAISSANCE, NAS INFOS DE CARTE : NOM SUR LA CARTE, NO DE CARTE, EXP., CVV RÉSULTATS ENVOYÉS PAR TELE, COURRIEL, TEXTO [...]

Ce que nous pouvons établir
Une trousse d'hameçonnage imitant une marque de télécommunications québécoise, qui demande aux victimes leur numéro d'assurance sociale et les données de leur carte.

Ce qui n'est pas établi
Si la trousse a été déployée, ni contre combien de personnes.

Fiche de preuve B16 — 17 mars 2026

Loyalty-account shop | Canal Telegram | Telegram | Anglais

ORIGINAL

Account available
[European airline] 320k
[Canadian airline] 200k
[hotel chain] 350k [...]
Full access
Escrow

TRADUCTION

Comptes disponibles
[compagnie aérienne européenne] 320k
[compagnie aérienne canadienne] 200k
[chaîne hôtelière] 350k [...]
Accès complet
Dépôt fiduciaire (escrow)

Ce que nous pouvons établir
Une annonce affirmant donner accès à des comptes de fidélité de compagnies aériennes et d'hôtels avec soldes de points indiqués, y compris le programme d'une compagnie aérienne canadienne.

Ce qui n'est pas établi
La validité des comptes, la provenance de l'accès et la conclusion de toute vente.

Les rapports officiels concordent avec ces schémas :

Date	Signalé par	Ce qui s'est passé
2026 (page datée du 24 avr.)	Centre pour la cybersécurité avec la GRC	Hameçonnage par texto sophistiqué se faisant passer pour des banques et d'autres organisations de confiance, ciblant activement les utilisateurs mobiles partout au Canada [S59]

Date	Signalé par	Ce qui s'est passé
Avril	Microsoft	Un acteur à motivation financière que Microsoft appelle Storm-2755 a utilisé de fausses pages de connexion Microsoft 365 pour voler des jetons de session et tenter de rediriger les dépôts de salaire d'employés canadiens; Microsoft documente au moins un versement de paie redirigé [S38]
23 avril	Service de police de Toronto	Trois personnes accusées d'avoir utilisé un « SMS blaster » mobile pour envoyer des textos frauduleux dans la région de Toronto; selon la police, des dizaines de milliers d'appareils s'y sont connectés [S43]
Octobre-novembre (signalé les 18 et 19 novembre)	Hydro-Québec	Prise de contrôle de comptes clients : plus de 2 500 connexions inhabituelles au portail client (20 octobre), au moyen de mots de passe réutilisés d'autres sites, selon l'entreprise; celle-ci a affirmé que ses systèmes n'avaient pas été compromis et a étendu l'AMF par code envoyé par courriel à tous les clients le 5 novembre [S32]
2-6 novembre	GRC et CAFC	Maple Disruption 2.0 : 10 987 actions de perturbation contre des fraudeurs et des cybercriminels [S42]

8.5 Données de cartes dans les publications : une vue restreinte

PORTÉE DES CHIFFRES DES FICHES

Les chiffres sur les cartes présentés dans ce rapport ne portent que sur les cartes de paiement apparues en clair dans les publications du web clandestin que nous avons lues pour ce rapport. Brandefense détecte les cartes volées par de nombreuses autres méthodes, que ce rapport ne couvre pas. Ces chiffres ne mesurent ni le vol de cartes ni les pertes liées à la fraude au Canada.

Dans cette portée restreinte, 374 cartes distinctes associées au Canada sont apparues en clair dans les publications que nous avons lues. Parmi elles, 279 étaient attribuées à l'un de 10 émetteurs canadiens nommés, et les 95 autres étaient étiquetées seulement comme canadiennes. La moitié d'entre elles (190) figuraient dans des résultats de vérificateurs de cartes, et 147 des 374 figuraient dans des publications de janvier [S8]. Le signal utile pour les émetteurs est le schéma de vérification : des lots de cartes testés au moyen de petites autorisations auprès de passerelles marchandes (chapitre 9).

8.6 Les prix en contexte

Produit (publications nettoyées)	Prix demandé médian	Fourchette
Compte bancaire ou de paiement	120 USD	50-220 USD
Service de KYC ou de documents	80 USD	30-200 USD
Offre d'accès	140 USD	90-500 USD
Offre de journaux de vol d'informations	180 USD	80-833 USD
Offre de données	20 USD	10-58 USD
Outil ou page d'hameçonnage	8 USD	3,5-50 USD

Les prix sont des prix demandés, tirés de la minorité de publications qui en indiquent un; ils ne mesurent ni la valeur marchande ni les ventes conclues. La fourchette correspond à la moitié centrale des prix indiqués (du 25e au 75e centile), et non à l'étendue complète. Les deux jeux de données de télécommunications du chapitre 4 étaient affichés à 100 000 et à 300 000 USD, bien au-delà de ces fourchettes.

POINTS À RETENIR

01

Les pertes liées à la fraude signalées ont dépassé 704 millions CAD en 2025; le centre estime que seulement 5-10 % des fraudes sont signalées [S79].

02

Les services clandestins ciblent les vérifications d'identité : comptes vieillis, initiés revendiqués, vérification au comptoir et guides de contournement de la KYC à distance.

03

Les chiffres sur les cartes ne portent que sur les cartes vues en clair dans les publications que nous avons lues (§8.5).

CHAPITRE 09

Analyse approfondie : banques et finance

09

CE CHAPITRE RÉPOND À LA QUESTION

Où se situe l'exposition visible des banques canadiennes : dans la banque, chez son personnel ou chez ses clients?

13 sur 22

banques émettrices de cartes avec un identifiant mis en vente en cours, premier élément à trier

CHAPITRE 09

Analyse approfondie : banques et finance

EN BREF

L'exposition visible se situe surtout côté clients : 116 660 appareils non classés « employé » (selon toute vraisemblance ceux des clients), la vérification de cartes et la revente de comptes. Côté banque et personnel : mises en vente en cours chez 13 émetteurs sur 22 et 817 appareils classés « employé ». Trois émetteurs concentrent les signaux liés aux cartes. Triez d'abord chaque mise en vente, validez les appareils des employés et surveillez les refus de vérification sur vos plages BIN (préfixe de carte de l'émetteur).

Ce chapitre porte sur les 22 banques et fintechs émettrices de cartes parmi les 33 organisations du secteur bancaire et financier du chapitre 3. Les 11 autres sont des organismes de réglementation, des réseaux de paiement, des prêteurs d'État et des sociétés d'investissement. C'est pourquoi les 116 660 appareils non classés « employé » diffèrent ici des 134 120 du chapitre 3, et les 817 appareils d'employés des 1 681. Données agrégées seulement; aucune banque n'est nommée.

13 sur 22

émetteurs avec un identifiant mis en vente en cours (13 des 14 organisations du secteur ayant une mise en vente en cours)

14 sur 33

organisations bancaires et financières ayant un identifiant mis en vente en cours

22 sur 22

émetteurs avec des associations d'appareils non classés « employé » (116 660; propriété et infection actuelle non vérifiées)

19 sur 22

émetteurs avec des appareils classés « employé » (817 au total)

29 sur 33

organisations bancaires et financières qui appliquent DMARC

9 sur 22

émetteurs de notre liste dont des cartes figurent en clair dans les publications lues (278 des 374 cartes; une autre nomme un émetteur hors de ces 22; portée restreinte, §8.5)

Les trois premiers émetteurs représentent 77 % des 278 cartes attribuées à des émetteurs de notre liste et 47 % des associations d'appareils non classés « employé ».

Ce que cela signifie pour les banques.

1. **Les mises en vente en cours passent en premier.** 13 émetteurs sur 22 en avaient une le jour de la vérification. Appliquez la règle de décision en 5 jours ouvrables du §12.1.

2. **L'exposition des employés est faible mais réelle.** Les 817 appareils classés « employé » répartis chez 19 émetteurs forment le sous-ensemble pertinent pour une intrusion. Après les mises en vente en cours, ils méritent une validation prioritaire, avant le total bien plus élevé d'appareils non classés « employé ».
3. **Les associations d'appareils non classés « employé » constituent l'exposition la plus large.** Les 116 660 associations d'appareils chez les 22 émetteurs ne sont pas classées « employé ». Selon toute vraisemblance, il s'agit des appareils des clients. La propriété, l'infection actuelle et la validité d'une session ou d'un mot de passe stockés ne sont pas vérifiées. Les équipes antifraude devraient utiliser des signaux de risque liés à l'appareil et à la session à la connexion et lors des changements de bénéficiaire, et pas seulement la vérification du mot de passe.
4. **La vérification de cartes est un signe précurseur détectable.** Les robots vérificateurs testent les cartes par de petites autorisations ou des tentatives d'ajout de carte sur des passerelles de commerçants. Les émetteurs peuvent détecter des grappes de tentatives refusées de faible montant sur leurs plages BIN et repérer les cartes visées. Ils peuvent ensuite vérifier leurs signaux d'autorisation et de fraude, puis réémettre, selon leur politique, les cartes dont le risque est confirmé.
5. **Les comptes mules et l'ouverture de comptes constituent le risque en aval.** Des publications de revente de comptes proposent des comptes vieillis dans des banques et fintechs canadiennes nommées. Elles proposent aussi des guides pour réussir les vérifications d'identité à distance (chapitre 8). Elles ne montrent pas que des comptes ont été ouverts ou utilisés dans les banques évaluées. Les contrôles d'ouverture de compte devraient partir du principe que le nom, la date de naissance et l'adresse sont connus des criminels.
6. **Des initiés sont annoncés.** Des menus de fraude affirment disposer d'initiés dans des banques (B09). Nous ne pouvons vérifier aucune de ces affirmations. Des revues d'accès pour le personnel qui peut consulter ou modifier les données des clients constituent toutefois une réponse proportionnée. Une affaire judiciaire de 2026 visait un ancien membre du personnel d'une succursale, qui a ouvert des comptes frauduleux et consulté les données bancaires d'une personnalité publique [S75].

POINTS À RETENIR

01

Les identifiants mis en vente en cours chez 13 émetteurs sur 22 passent en premier, puis les 817 appareils classés « employé ». L'ensemble plus large d'appareils non classés « employé » doit aussi être validé.

02

Les organisations bancaires et financières appliquent largement DMARC (29 sur 33).

03

Les refus de vérification de cartes sur vos plages BIN et l'activité des comptes vieillis sont des signes précurseurs détectables.

CHAPITRE 10

Réglementation et réponse nationale

10

CE CHAPITRE RÉPOND À LA QUESTION

Qu'est-ce qui a changé dans les règles canadiennes de cybersécurité en 2026, et que doit avoir en place une organisation avant l'entrée en vigueur des nouvelles obligations?

72 h

le délai de déclaration d'incident le plus long que permet la Loi sur la protection des cybersystèmes essentiels

10.1 Lois et règles en vigueur ou en préparation 77

10.2 Institutions fédérales et provinciales 78

10.3 Quel régime s'applique à vous? 78

CHAPITRE 10

Réglementation et réponse nationale

EN BREF

2026 a apporté la première loi fédérale canadienne de cybersécurité visant les systèmes essentiels : le projet de loi C-8 a reçu la sanction royale le 15 juin. Ses obligations pour les exploitants désignés des télécommunications, de l'énergie, de la finance et des transports seront mises en place par règlement. Les déclarations d'incident seront dues dans un délai d'au plus 72 heures. Les obligations de déclaration en matière de vie privée s'appliquent déjà. Déterminez quels régimes vous visent et désignez dès maintenant la personne qui déclare les incidents.

10.1 Lois et règles en vigueur ou en préparation

Mesure	Ce que nous avons pu vérifier	Statut et mise en garde
Projet de loi C-8 : Loi sur la protection des cybersystèmes essentiels (LPCE) et modifications de la Loi sur les télécommunications	Adopté par la Chambre des communes le 26 mars et par le Sénat le 4 juin 2026; sanction royale le 15 juin 2026 (L.C. 2026, ch. 9) [S44]. Les exploitants désignés de six services essentiels doivent déclarer un incident de cybersécurité au CST dans un délai fixé par règlement, qui ne peut dépasser 72 heures (article 17). Les sanctions administratives maximales sont de 500 000 CAD pour une personne physique et de 15 millions CAD dans les autres cas (article 91) [S44]	Les pouvoirs de sécurité prévus par la Loi sur les télécommunications ont pris effet immédiatement; la LPCE sera mise en place par étapes, et le gouvernement n'a donné aucune date [S45]
Services essentiels visés par la LPCE	Télécommunications; pipelines et lignes électriques interprovinciaux ou internationaux; énergie nucléaire; transports sous réglementation fédérale; services bancaires; systèmes de compensation et de règlement [S44]	La désignation des exploitants est fixée par règlement
Loi fédérale sur la protection des renseignements personnels dans le secteur privé (LPRPDE)	Les organisations doivent déclarer au commissaire à la protection de la vie privée toute atteinte aux mesures de sécurité « dès que possible » lorsqu'elle présente un risque réel de préjudice grave (article 10.1) [S47]	En vigueur; amendes pour infraction jusqu'à 10 000 ou 100 000 CAD (article 28) [S47]
Projet de loi C-36 : Loi sur la protection de la vie privée et des données des consommateurs	Première lecture le 15 juin 2026; débat de deuxième lecture non encore entamé au 21 novembre [S48]	Ce n'est pas une loi. Dans sa version actuelle, sanctions pouvant atteindre 10 millions CAD ou 3 % des recettes globales brutes, selon le montant le plus élevé, et amendes pour infraction jusqu'à 25 millions CAD ou 5 % [S48]

Mesure	Ce que nous avons pu vérifier	Statut et mise en garde
Loi 25 du Québec (secteur privé)	Une entreprise doit aviser avec diligence la Commission d'accès à l'information et les personnes concernées lorsqu'un incident de confidentialité présente un risque de préjudice sérieux [S46]	En vigueur. Sanctions administratives pécuniaires jusqu'à 10 millions CAD ou 2 % du chiffre d'affaires mondial. Amendes pénales pour une entreprise de 15 000 CAD jusqu'à 25 millions CAD ou 4 %, selon le montant le plus élevé, doublées en cas de récidive [S46]
Secteur public de l'Ontario (projet de loi 194)	La Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public a reçu la sanction royale le 25 novembre 2024 (L.O. 2024, chap. 24) [S49]	Impose des obligations de cybersécurité aux entités du secteur public ontarien; vérifiez quels règlements s'appliquent à vous
Institutions financières sous réglementation fédérale (BSIF)	La ligne directrice B-13 sur la gestion des risques liés aux technologies et au cyberrisque s'applique depuis le 1er janvier 2024 [S51]. Le préavis du BSIF sur la déclaration des incidents demande aux institutions de déclarer un incident technologique ou de cybersécurité dans les 24 heures, ou plus tôt si possible [S50]	En vigueur
Fournisseurs de services de paiement (Loi sur les activités associées aux paiements de détail)	Cadres de gestion des risques et de protection des fonds exigés depuis le 8 septembre 2025, sous la supervision de la Banque du Canada [S52]	En vigueur
Fournisseurs du secteur de la défense	Le niveau 1 du Programme canadien de certification en cybersécurité s'applique à certains contrats de défense à compter de l'été 2026 [S72]	Premier de trois niveaux

10.2 Institutions fédérales et provinciales

- **Québec.** En novembre 2026, la page gouvernementale du ministère de la Cybersécurité et du Numérique indiquait que son contenu Web serait regroupé avec celui du Secrétariat du Conseil du trésor [S53]. Les organisations qui lui font rapport devraient confirmer leurs points de contact.
- **Stratégie nationale antifraude.** En mars, le ministère fédéral des Finances a lancé des consultations sur une première stratégie nationale antifraude. La consultation porte notamment sur un cadre qui pourrait imposer de nouvelles obligations aux banques, aux entreprises de télécommunications et aux plateformes en ligne [S73].
- **Infrastructures essentielles.** En avril, le Centre pour la cybersécurité a lancé une initiative pour aider les exploitants d'infrastructures essentielles à se préparer aux cybermenaces graves [S74].

10.3 Quel régime s'applique à vous?

Le tableau applique les textes ci-dessus à cinq cas courants. Il constitue un point de départ, pas un avis juridique.

Organisation	Principales obligations en cybersécurité et en matière d'atteintes	Action immédiate
Banque ou assureur sous réglementation fédérale	B-13 du BSIF et déclaration des incidents en 24 heures; déclaration des atteintes selon la LPRPDE; LPCE en cas de désignation (services bancaires, compensation et règlement)	Vérifier que les déclarations au BSIF, en matière de vie privée et, à l'avenir, au CST proviennent d'un même dossier d'incident
Exploitant de télécommunications	Pouvoirs de sécurité de la Loi sur les télécommunications en vigueur; LPCE en cas de désignation; LPRPDE	Se préparer aux décrets pris en vertu de la loi modifiée; désigner un contact pour les déclarations au CST
Exploitant de pipeline, de ligne électrique, d'installation nucléaire ou de transport fédéral	LPCE en cas de désignation; LPRPDE pour les renseignements personnels	Mettre en place dès maintenant une procédure de déclaration en 72 heures, avant que les règlements fixent le délai
Entreprise privée au Québec	Registre des incidents et avis prévus par la Loi 25; LPRPDE lorsqu'elle s'applique	Tenir à jour le registre des incidents; répéter un avis à la CAI
Entité du secteur public ontarien	Obligations du projet de loi 194; loi provinciale sur la protection de la vie privée	Confirmer quels règlements s'appliquent et qui fait les déclarations

Ce que les RSSI devraient faire dès maintenant. Déterminez lesquels de ces régimes visent votre organisation. Désignez la personne qui déclarerait un incident à chaque organisme de réglementation, et assurez-vous qu'un même dossier d'incident peut les alimenter tous. Conservez des preuves datées des contrôles que vous mettez en place, car les règlements de la LPCE restent à venir. Cette section ne constitue pas un avis juridique.

POINTS À RETENIR

01

Le projet de loi C-8 est devenu loi le 15 juin 2026; les déclarations d'incident prévues par la nouvelle loi seront dues dans un délai d'au plus 72 heures.

02

Les obligations relatives aux atteintes à la vie privée s'appliquent déjà au fédéral et au Québec, où les amendes pénales atteignent 25 millions CAD ou 4 % du chiffre d'affaires mondial.

03

Bâtissez un dossier d'incident unique qui peut alimenter le CST, le BSIF et les organismes de protection de la vie privée; les règlements continuent d'arriver.

CHAPITRE 11

Perspectives

11

CE CHAPITRE RÉPOND À LA QUESTION

À quoi les organisations canadiennes doivent-elles se préparer ensuite, et quelles données changeraient ce plan?

5

jugements clés, chacun assorti d'un signal à surveiller

11.1 Jugements clés 81

11.2 Ce qui changerait l'évaluation 82

11.3 Scénarios conditionnels 82

CHAPITRE 11

Perspectives

EN BREF

Préparez-vous aux mêmes types de données probantes, pas à une nouvelle menace. Prévoyez des rançongiciels et une extorsion de données stables. Le vol axé sur l'identité passe par les services d'assistance et le SaaS. Le marché de la fraude d'identité est vaste, et des hacktivistes visent les systèmes de commande exposés. Selon des fournisseurs, l'espionnage lié à des États contre la recherche et les universités se poursuit. Faute de série comparable pour la plupart de ces éléments, changez le plan quand les signaux ci-dessous changent, pas selon un calendrier.

11.1 Jugements clés

Jugement	Confiance	Fondement et limite
Les rançongiciels et l'extorsion de données resteront la menace criminelle la plus visible pour les organisations canadiennes	Élevée	Inscriptions observées : 386 inscriptions retenues en 2026 contre 406 en 2025; les inscriptions sont des revendications, et les cas non publiés sont invisibles; signal : inscriptions canadiennes acceptées par mois
L'hameçonnage vocal visant les services d'assistance et le vol de données SaaS resteront une voie d'accès majeure vers des atteintes confirmées	Moyenne	L'alerte du Centre pour la cybersécurité et plusieurs atteintes confirmées en 2026; les auteurs ne sont pas tous les mêmes; signal : alertes du Centre et divulgations d'entreprises mentionnant des réinitialisations par le service d'assistance
L'exposition des identités dans la liste des 250 organisations est assez répandue pour traiter les signaux d'identifiants et d'appareils comme un tri de routine	Élevée pour la liste	Décomptes du chapitre 3; il ne s'agit pas d'une prévalence nationale; signal : part des mises en vente en cours validées comme actives
Si les systèmes de commande restent accessibles depuis Internet, prévoir d'autres revendications de manipulation par des hacktivistes dans des installations d'eau, de services publics et industrielles	Moyenne (hypothèse de planification)	Trois cas officiels en octobre 2025 et un cas municipal en juillet 2026; petit échantillon; signal : bulletins du Centre pour la cybersécurité
Si les systèmes de recherche, les webmails et les systèmes en périphérie restent sans correctif, prévoir des tentatives d'espionnage liées à des États contre les universités et les organismes de recherche	Moyenne (hypothèse de planification)	Trois rapports de fournisseurs de 2026 nommant des universités canadiennes, des serveurs de recherche ou un organisme de défense des droits de la personne; signal : avis des fournisseurs

11.2 Ce qui changerait l'évaluation

Interprétation actuelle	Données qui la changeraient	Décision touchée
Les inscriptions canadiennes sont stables tout au long de l'année	Une hausse mensuelle soutenue des inscriptions canadiennes retenues, ou une vaste campagne d'un seul groupe	Augmenter la fréquence des tests de restauration; revoir les accès des fournisseurs
Les offres de jeux de données visant des entreprises de télécommunications, des assureurs et des hôpitaux ne sont pas vérifiées	Un échantillon correspondant au schéma d'un système précis, ou une confirmation officielle	Déclencher les mesures d'avis et de protection des clients pour ce jeu de données
L'hameçonnage vocal visant les services d'assistance se concentre dans les secteurs juridique et financier	Un rapport du Centre pour la cybersécurité ou d'une entreprise signalant la même méthode dans un autre secteur	Étendre la vérification par rappel et les alertes de téléchargement SaaS à ce secteur
Les incidents de TO attribués à des hacktivistes ont eu jusqu'ici un impact mineur	Un rapport officiel faisant état d'une panne prolongée ou d'un événement de sécurité dans un système de commande canadien	Financer la segmentation de la TO et les contrôles d'accès à distance avant d'autres projets
Un identifiant mis en vente en cours signifie « à valider », pas « compromis »	La validation montre des comptes actifs sans AMF parmi les identifiants mis en vente	Passer à la réponse aux incidents et imposer l'AMF à la population touchée

11.3 Scénarios conditionnels

- **Si** un événement international ou une déclaration de politique canadienne attire une attention hostile, **alors** prévoir des attaques DDoS et des revendications de manipulation de systèmes de commande par des hacktivistes (hypothèse de planification). **Signal :** bulletins du Centre pour la cybersécurité et listes de cibles des acteurs. **Décision :** vérifier qu'aucun système de commande n'est accessible depuis Internet et activer la ligne de communication convenue à l'avance.
- **Si** une nouvelle vulnérabilité critique touchant un système en périphérie ou un webmail est divulguée, **alors** prévoir des tentatives d'exploitation criminelles et liées à des États. **Signal :** avis des fournisseurs et alertes du Centre pour la cybersécurité. **Décision :** appliquer le correctif et le vérifier dans votre délai pour les systèmes exposés à Internet, puis rechercher des interpréteurs de commandes Web (web shells).
- **Si** votre service d'assistance reçoit des demandes inhabituelles de réinitialisation de l'AMF, **alors** prévoir une tentative d'hameçonnage vocal. **Signal :** demandes de réinitialisation provenant de nouveaux numéros ou en dehors des heures normales. **Décision :** appliquer la vérification par rappel et examiner les téléchargements SaaS récents.

POINTS À RETENIR

01

Préparez-vous à des types de données probantes, pas à une nouvelle menace : extorsion, vol axé sur l'identité, fraude d'identité et systèmes de commande exposés.

02

Chaque jugement est assorti d'un signal; changez le plan quand le signal change.

03

Il n'existe pas encore de série chronologique comparable pour dire si la plupart de ces menaces augmentent.

CHAPITRE 12

Plan d'action

12

CE CHAPITRE RÉPOND À LA QUESTION

Que doit faire chaque équipe au cours des 90 prochains jours, et comment le conseil d'administration saura-t-il que c'est fait?

20

actions assorties d'un responsable et d'une preuve d'achèvement

12.1 30/60/90 jours 85

12.2 Par rôle 89

12.3 Comment Brandefense peut aider 89

CHAPITRE 12

Plan d'action

EN BREF

Confirmez d'abord que vous recevez les alertes d'identifiants mis en vente et d'appareils infectés. Verrouillez ensuite le service d'assistance et la récupération d'identité, voie connue de plusieurs atteintes confirmées de 2026. Validez les mises en vente et les appareils des employés, fermez l'accès à distance et les systèmes de commande exposés, puis faites un exercice de simulation d'extorsion et de déclarations réglementaires. Le conseil d'administration s'appuie sur la preuve d'achèvement de chaque ligne et le tableau de bord ci-dessous; présentez-les d'ici le jour 90.

12.1 30/60/90 jours

Il s'agit d'une séquence, pas d'une période d'attente. Une menace importante en cours devrait entrer immédiatement dans votre processus de gestion des incidents.

1Jours 1-30

Confirmer que vous recevez les alertes d'identifiants mis en vente et d'appareils infectés pour vos domaines principaux. Sinon, les mettre en place et noter comme bloquées les lignes ci-dessous sur les mises en vente et les appareils jusqu'à l'arrivée des alertes

RESPONSABLE

RSSI et renseignement sur les menaces

PREUVE D'ACHÈVEMENT

Source des alertes nommée; première alerte reçue

Exiger une vérification par rappel à un numéro connu avant toute réinitialisation de mot de passe ou d'AMF par le service d'assistance, y compris pour les appels qui prétendent venir des TI internes (§7.3)

RESPONSABLE

Service d'assistance et équipe identité

PREUVE D'ACHÈVEMENT

Procédure approuvée; un appel d'hameçonnage vocal simulé intercepté

Pour chaque identifiant mis en vente en cours lié à vos domaines, valider le compte et l'état de son AMF dans un délai de 5 jours ouvrables

RESPONSABLE

Équipe identité

PREUVE D'ACHÈVEMENT

Chaque mise en vente a une décision datée : réinitialisé, déjà corrigé ou ne nous concerne pas

Valider les associations d'appareils classés « employé »; révoquer les sessions et les jetons actifs

RESPONSABLE

Équipes identité et postes de travail

PREUVE D'ACHÈVEMENT

Liste des appareils rapprochée de l'inventaire des actifs; révocations consignées

Placer dès maintenant les passerelles Web de bureau à distance, les RPV et les webmails derrière l'AMF, et commencer l'AMF résistante à l'hameçonnage pour les utilisateurs privilégiés. Corriger les systèmes en périphérie exposés à Internet dès qu'une alerte du Centre pour la cybersécurité nomme un produit que vous utilisez

RESPONSABLE
Infrastructure

PREUVE D'ACHÈVEMENT
Nouveau test externe réussi; exceptions datées

Désigner la personne qui déclare les incidents à chaque organisme de réglementation (le CST une fois désigné, le BSIF, le commissaire à la protection de la vie privée, la CAI). Convenir d'un dossier d'incident unique (§10.3)

RESPONSABLE
RSSI et service juridique

PREUVE D'ACHÈVEMENT
Carte des déclarations d'une page, approuvée

2 Jours 31-60

Créer des alertes sur les téléchargements massifs et les nouvelles applications API dans Microsoft 365 et les autres locataires SaaS

RESPONSABLE
SOC et responsables SaaS

PREUVE D'ACHÈVEMENT
Alerte active et testée

Faire passer d'abord les utilisateurs privilégiés et à distance, puis les autres, à une AMF résistante à l'hameçonnage (clés de sécurité FIDO2, clés d'accès ou connexion par certificat)

RESPONSABLE
Équipe identité

PREUVE D'ACHÈVEMENT
Couverture consignée par groupe d'utilisateurs

Retirer les systèmes de commande de toute exposition directe à Internet; placer l'accès à distance derrière un hôte de rebond avec AMF; changer les mots de passe par défaut (§6.4)

RESPONSABLE
TO et ingénierie

PREUVE D'ACHÈVEMENT
La vérification de l'exposition externe ne montre aucune interface de commande; journal d'accès à distance examiné

Là où DMARC est à p=none, absent ou invalide, inventorier les expéditeurs et passer graduellement à l'application

RESPONSABLE
Messagerie

PREUVE D'ACHÈVEMENT
Expéditeurs alignés; p=quarantine avec une voie de retour arrière

Tester les processus de récupération de compte, d'échange de carte SIM et de changement de bénéficiaire face à un attaquant qui connaît le nom, l'adresse, le téléphone et la date de naissance

RESPONSABLE
Fraude et opérations clients

PREUVE D'ACHÈVEMENT
Faiblesses consignées et corrigées, nouveau test réussi

Exiger une confirmation hors bande pour les changements d'instructions de paiement et de dépôt de paie (§8.4)

RESPONSABLE
Finances et RH

PREUVE D'ACHÈVEMENT
Procédure approuvée; une demande simulée interceptée

Banques : créer des alertes sur les grappes de refus de vérification de cartes sur vos plages BIN et sur les nouveaux destinataires de virements électroniques pour les comptes vieillis

RESPONSABLE
Fraude

PREUVE D'ACHÈVEMENT
Alerte active; premier examen consigné

Dresser la liste des fournisseurs qui détiennent vos données de clients ou de dossiers sur des plateformes infonuagiques; confirmer leurs conditions d'AMF, de journalisation et d'avis d'atteinte

RESPONSABLE
Approvisionnement et risque lié aux tiers

PREUVE D'ACHÈVEMENT
Liste des fournisseurs avec confirmations datées

Effectuer un test de restauration chronométré d'un système critique

RESPONSABLE
Infrastructure

PREUVE D'ACHÈVEMENT
Temps de restauration consigné par rapport à l'objectif de temps de reprise (RTO : la plus longue interruption que permet votre plan de continuité des activités)

3Jours 61-90

Signer le DNS des domaines principaux lorsque votre registraire le permet; corriger les certificats TLS invalides et ajouter HSTS

RESPONSABLE
Équipes réseau et Web

PREUVE D'ACHÈVEMENT
La validation DNSSEC réussit depuis un résolveur externe; les vérifications de certificats sont réussies

Mener un exercice sur table sur l'extorsion de données : fichiers volés publiés, aucun chiffrement, délais réglementaires en cours

RESPONSABLE
RSSI, communications, service juridique

PREUVE D'ACHÈVEMENT
Journal des décisions et minutage, y compris l'échéance de chaque organisme de réglementation

Préparer des avis aux clients et aux patients pour une revendication de fuite non vérifiée, en séparant la revendication, le fait vérifié et l'action

RESPONSABLE

Communications et protection de la vie privée

PREUVE D'ACHÈVEMENT

Modèles approuvés

Examiner les comptes de fidélité et de portail client pour détecter le bourrage d'identifiants; offrir ou exiger l'AMF

RESPONSABLE

Équipes numérique et fraude

PREUVE D'ACHÈVEMENT

Taux de prise de contrôle mesuré avant et après

Présenter le tableau de bord par rapport aux cibles (ci-dessous)

RESPONSABLE

RSSI au conseil d'administration

PREUVE D'ACHÈVEMENT

Document au conseil indiquant les lacunes restantes et leurs responsables

Cibles du tableau de bord. Ce sont des valeurs par défaut suggérées; fixez les vôtres lorsque votre politique diffère.

Mesure	Cible
Réinitialisations par le service d'assistance avec vérification par rappel	100 % d'ici le jour 30
Mises en vente en cours ayant une décision dans un délai de 5 jours ouvrables	100 % d'ici le jour 90
Appareils classés « employé » rapprochés de l'inventaire des actifs	100 % d'ici le jour 90
Passerelles d'accès à distance et webmails derrière une AMF résistante à l'hameçonnage	100 %, ou un plan daté, d'ici le jour 90
Systèmes de commande accessibles depuis Internet	Zéro, ou un plan daté, d'ici le jour 90
Domaines principaux avec DMARC à quarantine ou reject	100 %, ou un plan daté, d'ici le jour 90
Changements de paiement et de paie confirmés hors bande	100 % d'ici le jour 90
Test de restauration dans le RTO	Réussi, ou une correction datée, d'ici le jour 90

12.2 Par rôle

Rôle	Première décision
Conseil d'administration	Demander comment le service d'assistance vérifie l'identité d'un appelant avant de réinitialiser l'AMF. Demander aussi les chiffres sur les mises en vente en cours et les appareils des employés, avec une date de validation pour chacun
RSSI	Mettre en place la surveillance des mises en vente et des appareils, puis financer l'AMF résistante à l'hameçonnage pour les utilisateurs à distance et privilégiés
SOC	Ajouter des détections pour les connexions juste après une réinitialisation par le service d'assistance, les téléchargements SaaS massifs, les nouvelles applications OAuth et les connexions depuis des réseaux d'hébergement
Fraude	Utiliser le risque lié à l'appareil et à la session à la connexion et lors des changements de bénéficiaire et de paie; surveiller les refus de vérification de cartes et l'activité des comptes vieillis
Communications et service juridique	Préparer des déclarations pour les revendications de fuite non vérifiées et une carte des déclarations pour chaque organisme de réglementation applicable

POINTS À RETENIR

01

Au cours des 30 premiers jours, confirmez la surveillance et imposez la vérification par rappel pour chaque réinitialisation par le service d'assistance.

02

D'ici le jour 60, étendez l'AMF résistante à l'hameçonnage, créez des alertes sur les téléchargements SaaS massifs et retirez les systèmes de commande d'Internet.

03

D'ici le jour 90, répétez un scénario d'extorsion de données avec les échéances réglementaires et présentez le tableau de bord au conseil d'administration.

12.3 Comment Brandefense peut aider

Brandefense combine le renseignement sur les cybermenaces (Cyber Threat Intelligence), la protection contre les risques numériques (Digital Risk Protection) et la gestion de la surface d'attaque externe (External Attack Surface Management). L'analyse de ce rapport a utilisé les mêmes données et la même notation que la plateforme applique aux organisations surveillées. Il s'agit des associations d'appareils infectés et d'identifiants, des identifiants mis en vente en cours, des domaines semblables, des documents exposés et des mentions sur le web clandestin. Cette analyse ne promet pas que chaque revendication peut être vérifiée ni qu'un enregistrement historique reste utilisable.

Présentez vos domaines, vos marques et vos priorités de sécurité lors d'une démonstration de 30-45 minutes avec les équipes Ventes et Avant-vente. L'équipe peut montrer comment la surveillance de la plateforme relie les signaux externes aux actifs que vous gérez. Un membre de l'équipe Brandefense ou un partenaire de votre région fera le suivi.

Demander une démonstration

ANNEXES

Annexes

A–D

CE CHAPITRE RÉPOND À LA QUESTION

Annexe A. Méthode · Annexe B. Registre des preuves · Annexe C. Sources · Annexe D. Glossaire

81
sources

Annexe A. Méthode 92
Annexe B. Registre des preuves 95
Annexe C. Sources 96
Annexe D. Glossaire 101

Annexe A. Méthode

Les pays de comparaison ont été choisis à titre d'exemples uniquement pour apporter du contexte ; leur sélection n'implique ni classement ni appréciation politique.

A.1 Période, sources et priorité

La période de recherche va du 1er janvier au 18 novembre 2026, selon la date de publication des messages et non leur date de collecte. Nos propres données passent en premier. Il s'agit de Brandefense Blackhole (publications du web clandestin et des messageries, associations d'appareils infectés et d'identifiants de connexion, données de cartes dans les publications). S'y ajoutent Ransompedia (inscriptions sur les sites de fuite de rançongiciels) et les cotes d'exposition Brandefense Atlas.

Les sources externes fournissent le contexte et ne sont citées qu'après lecture du passage qui les appuie. Les données ont été extraites le 21 novembre 2026. Les sources S1-S8 sont des données propres à Brandefense ou un outil de suivi public utilisé comme contre-vérification. Les entrées externes de l'annexe C indiquent l'URL complète (ou la racine du site de l'éditeur lorsque l'URL de l'article est retenue selon l'annexe A.9) et la date de vérification.

A.2 Publications Blackhole

Élément	Valeur
Publications portant l'étiquette de pays Canada	696 200 dénombrées
Publications étiquetées lues	43 549, un échantillon sur l'ensemble de l'année
Publications de forum portant l'étiquette	1 449 dénombrées; 1 438 lues
Autres publications lues	Publications sur des marques et des lieux canadiens
Publications pertinentes parmi les publications lues (mesure principale)	12 124-12 656 (12 124 strictement pertinentes plus 532 publications limites)
Fourchette modélisée sur l'étiquette aux graphiques c01-c02 (indicative)	93 500-99 400 (arrondie de la somme mensuelle de 93 530-99 350)

Les publications pertinentes sont celles liées à la criminalité; le pourriel est exclu. Ce rapport retient comme mesure principale les 12 124-12 656 publications pertinentes directement lues parmi les 43 549 publications étiquetées lues. Les publications de forum ont été lues presque intégralement (1 438 sur 1 449, soit 99,2 %). Celles de Telegram, Discord et des sites de collage ont été échantillonnées sur les 11 mois (42 111 sur 694 751, soit 6,1 %). L'échantillon couvrait 17 579 des 148 881 publications en anglais (11,8 %, dont 9 096 pertinentes) et 7 543 des 366 561 en turc (2,1 %, dont 188 pertinentes).

Les graphiques c01 et c02 tracent aussi une projection indicative totalisant 93 530-99 350 sur les 11 lignes mensuelles du graphique c01 (arrondie à 93 500-99 400). Ces lignes correspondent à des parts de pertinence effectives de 5,4 %-5,7 % en janvier et de 8,8 %-9,9 % en février. Elles sont de 9,9 %-10,2 % en mai, de 9,3 %-10,9 % en

juin et de 22,1 %-60,6 % en mars-avril et juillet-novembre. Les tailles d'échantillon mensuelles et les pondérations internes par strate sont retenues, et l'échantillonnage était raisonné. Cette projection de 93 500-99 400 n'est donc pas reproductible à partir des totaux publics et ne sert pas de mesure principale.

Le volume de collecte influe sur chaque tendance de ce rapport. Le volume étiqueté des pays de comparaison varie aussi fortement d'un mois à l'autre. Nous ne lisons donc pas les variations mensuelles canadiennes, ni les variations de la composition des familles criminelles, comme des tendances de la menace.

A.3 Les 250 organisations

La sélection, la vérification et les limites sont présentées au §3.1. Pour chaque domaine principal, nous avons lu les signaux d'exposition qu'Atlas emploie pour ses cotes. Il s'agit des appareils infectés, des appareils d'employés, des enregistrements d'identifiants de connexion et des mentions sur les messageries et le web clandestins. S'y ajoutent les nouveaux domaines sosies, les documents qui mentionnent le domaine et les mises en vente d'identifiants en cours. Nous lisons aussi les mises en vente antérieures (« historique de mises en vente », consignées avant la vérification actuelle). Les données ont été lues le 21 novembre 2026.

A.4 Cotes Atlas

Chaque organisation a reçu une cote d'exposition Atlas fondée sur ces signaux, et les 250 organisations, une note globale nationale. Une mise en vente d'identifiants en cours doit être traitée comme une raison de valider les comptes, et non comme la preuve d'une atteinte. Le décompte des domaines sosies est plus bruité pour les marques au nom générique ou très courant.

A.5 Vérifications DNS, TLS et Web

Les résultats portent sur les paramètres publiés de messagerie, SPF, DMARC, DKIM, DNSSEC et CAA, les certificats TLS et les en-têtes de la page d'accueil de chaque domaine principal. Les politiques DMARC absentes, invalides ou de surveillance seulement (p=none) sont comptées comme une absence d'application. Tous les résultats sont passifs.

Les valeurs de l'indice d'hygiène résument ces résultats de courriel, de DNS, de TLS et d'en-têtes par secteur, sur une échelle de 0-100; une valeur plus élevée signifie une hygiène plus faible. Il s'agit d'un indice analytique d'Odin, et non d'une cote, qui ne fait pas partie d'Atlas.

A.6 Données de cartes dans les publications

Portée : uniquement les cartes de paiement apparues en clair dans les publications du web clandestin lues pour ce rapport. Brandefense détecte les cartes volées par de nombreuses autres méthodes, qui n'entrent pas dans le cadre de ce rapport. Ces chiffres ne mesurent ni le vol de cartes ni les pertes liées à la fraude.

A.7 Rançongiciels

Nous avons utilisé les inscriptions acceptées de Ransompedia pour le Canada, les États-Unis, le Royaume-Uni et l'Australie, toutes dates confondues, datées selon leur publication. Un outil de suivi public et des publications Blackhole relayées servent uniquement de contre-vérification.

A.8 Couverture des incidents

La couverture des incidents combine les publications Blackhole sur les 250 organisations et sur des fuites, des accès ou des exploits précis avec les comptes rendus publics, en anglais et en français.

Les sources publiques comprennent le Centre canadien pour la cybersécurité et les communiqués du CST, de la GRC, du Centre antifraude du Canada, de Sécurité publique Canada et du BSIF.

Elles comprennent aussi les commissaires fédéral et provinciaux à la protection de la vie privée, les gouvernements provinciaux, les services de police et les municipalités. S'y ajoutent les médias nationaux de langue anglaise et de langue française, ainsi que la recherche des fournisseurs.

Limites de couverture restantes. Notre vue demeure partielle :

- Les sites de fuite de rançongiciels sur Tor ne sont couverts que par Ransompedia.
- La couverture de Telegram est partielle; une publication propre au Canada peut donc nous échapper.
- Les forums fermés ou accessibles sur invitation seulement, les groupes Telegram privés et les ventes conclues par messages directs échappent à notre collecte.
- Plusieurs sites de nouvelles de langue française et certaines pages officielles n'ont pas pu être récupérés aux fins de vérification; leurs articles ne sont donc pas utilisés.
- Les incidents que les organisations gèrent sans les divulguer restent invisibles.

L'absence d'un incident dans ce rapport ne signifie pas qu'il n'a pas eu lieu.

A.9 Confiance et limites

Un niveau de confiance élevé s'applique à une mesure reproductible, et non à l'affirmation sous-jacente d'un criminel. Un niveau moyen indique une interprétation appuyée par un élément clair, avec des limites énoncées. La mention « non vérifié » signifie non établi de façon indépendante; ce n'est ni une preuve de fabrication ni une preuve d'atteinte. Les organisations victimes sont décrites par leur rôle. Une organisation n'est nommée que si elle-même ou une autorité a confirmé l'incident, et que l'incident a été largement rapporté.

Les alias des acteurs sont imprimés; les liens, contacts, indicateurs et données personnelles sont retenus. La provenance complète est conservée dans un registre interne des preuves.

Annexe B. Registre des preuves

Chaque publication citée dans ce rapport figure sous forme de fiche de publication caviardée dans le chapitre indiqué. Les extraits sont courts et les omissions sont marquées [...]. Les identifiants, contacts, liens et organisations victimes sont remplacés par des libellés entre crochets, selon la politique décrite en A.9. Les dates de publication ne sont pas des dates d'intrusion. Les identifiants des publications, les liens et le texte intégral sont conservés dans un registre interne des preuves.

Fiche	Publiée le	Lieu	Alias affiché	Langue	Présentée au
B01	2026-03-21	Forum de fuites de données	Murad	Anglais	§4.4
B02	2026-04-25	Forum de fuites de données	Murad	Anglais	§4.4
B03	2026-04-29	Forum de fuites de données	GlitchX	Anglais	§4.4
B04	2026-11-09	Forum de fuites de données	DataJava	Anglais	§4.5
B05	2026-03-17	Groupe Telegram	Auteur anonyme	Anglais	§4.5
B06	2026-05-13	Forum de fuites de données	XOverStm	Anglais	§4.5
B07	2026-01-09	Forum de fuites de données	phoenix_leads	Anglais	§4.4
B08	2026-01-23	Forum de fuites de données	hulky	Anglais	§4.4
B09	2026-01-01	Canal Telegram	Vendeur de services de fraude	Anglais	§8.3
B10	2026-05-13	Canal Telegram	Calciumpound	Anglais	§8.2
B11	2026-05-05	Groupe Telegram	bigbosskyc1	Anglais	§8.3
B12	2026-09-14	Groupe Telegram	Vendeur de services de fraude	Anglais	§8.3
B13	2026-11-14	Forum de fuites de données	scarlettgroup	Anglais	§4.4
B14	2026-06-16	Forum de fraude	theghostorder01	Anglais	§8.4
B15	2026-05-08	Forum de fuites de données	MDGhost	Anglais	§4.4
B16	2026-03-17	Canal Telegram	Boutique de comptes de fidélité	Anglais	§8.4

Annexe C. Sources

S1: Corpus de publications Brandefense Blackhole, étiquette de pays Canada et publications sur des marques et des lieux canadiens, publications datées du 1er janvier au 18 novembre 2026, extrait le 21 novembre 2026.

S2: Publications de forums et de marchés Brandefense Blackhole citées dans les études de cas, du 1er janvier au 18 novembre 2026.

S3: Associations Brandefense Blackhole d'appareils infectés, de bases de données issues d'atteintes, de journaux de vol d'informations et de listes combinées (combolists) pour 250 domaines, lues le 21 novembre 2026.

S4: Cotes d'exposition Brandefense Atlas des 250 domaines, 21 novembre 2026, y compris les mises en vente d'identifiants, les domaines sosies, les documents exposés et les statistiques de mentions.

S5: Vérifications Brandefense des DNS publics, du TLS et des pages d'accueil des 250 domaines, 21 novembre 2026.

S6: Brandefense Ransompedia, inscriptions acceptées pour le Canada, les États-Unis, le Royaume-Uni et l'Australie, toutes dates confondues, extraites le 21 novembre 2026.

S7: ransomware.live, victimes par pays pour le Canada, consulté le 21 novembre 2026 (contre-vérification seulement). https://www.ransomware.live/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S8: Brandefense Blackhole, cartes associées au Canada vues en clair dans des publications du web clandestin, 21 novembre 2026.

S9: DataReportal (Kepios), Digital 2027: Canada, 4 novembre 2026 (données d'octobre 2026). https://datareportal.com/reports/digital-2027-canada. Vérifié le 21 novembre 2026.

S10: Centre canadien pour la cybersécurité, National Cyber Threat Assessment 2025-2026. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026. Vérifié le 21 novembre 2026.

S11: Centre de la sécurité des télécommunications, Annual Report 2025-2026, 29 juin 2026. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2025-2026. Vérifié le 21 novembre 2026.

S12: Centre canadien pour la cybersécurité, Ransomware Threat Outlook 2025-2027. https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027. Vérifié le 21 novembre 2026.

S13: Centre antifraude du Canada, "Fraud Prevention Month 2026" (principales fraudes de 2025). https://antifraudcentre-centreantifraude.ca/features-vedette/2026/02/month-prevention-mois-eng.htm. Vérifié le 21 novembre 2026.

S14: Commissariat à la protection de la vie privée du Canada, communiqué sur le rapport annuel, 4 juin 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260604/. Vérifié le 21 novembre 2026.

S15: Centre canadien pour la cybersécurité, "AL26-028 Ongoing Help Desk Voice Phishing Campaign Targeting Canadian Organizations", 28 octobre 2026. https://www.cyber.gc.ca/en/alerts-advisories/al26-028-ongoing-help-desk-voice-phishing-campaign-targeting-canadian-organizations. Vérifié le 21 novembre 2026.

S16: The Globe and Mail, reportages sur des atteintes visant des cabinets d'avocats de Toronto, 29-31 octobre 2026. https://www.theglobeandmail.com/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S17: Centre canadien pour la cybersécurité, "Cyber threat bulletin: Non-state activity targeting Canadian operational technology", 28 juillet 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-non-state-activity-targeting-canadian-operational-technology. Vérifié le 21 novembre 2026.

S18: Centre canadien pour la cybersécurité, "Cyber threat bulletin: Iranian Cyber Threat Response to US/Israel strikes, February 2026", 1er mars 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026. Vérifié le 21 novembre 2026.

S19: Centre canadien pour la cybersécurité, "Cyber threat bulletin: FIFA World Cup 2026", 29 mai 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-fifa-world-cup-2026tm. Vérifié le 21 novembre 2026.

S20: Centre de la sécurité des télécommunications, appel à renforcer les défenses au quatrième anniversaire de l'invasion de l'Ukraine par la Russie, 19 février 2026. https://www.cyber.gc.ca/en/news-events/cse-calls-canadian-organizations-critical-infrastructure-providers-strengthen-defences-fourth-anniversary-russias-invasion-ukraine. Vérifié le 21 novembre 2026.

S21: Le Soleil, "Une cyberattaque russe frappe une station d'eau potable au Bas-Saint-Laurent", 31 juillet 2026. https://www.lesoleil.com/actualites/actualites-locales/est-du-quebec/2026/07/31/une-cyberattaque-russe-frappe-une-station-deau-potable-au-bas-saint-laurent-ZZSATQTBFJABDJNBCL7PAJZMIE/. Vérifié le 21 novembre 2026.

S22: Commissariat à la protection de la vie privée du Canada, "Loblaw commits to strengthening security measures following privacy breach", 26 octobre 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_261026/. Vérifié le 21 novembre 2026.

S23: BleepingComputer, "Telus Digital confirms breach after hacker claims 1 petabyte data theft", mars 2026. https://www.bleepingcomputer.com/news/security/telus-digital-confirms-breach-after-hacker-claims-1-petabyte-data-theft/. Vérifié le 21 novembre 2026.

S24: CTV News, "Cybersecurity incident at Canada Life reportedly impacts thousands", avril 2026. https://www.ctvnews.ca/canada/article/cybersecurity-incident-at-canada-life-reportedly-impacts-thousands/. Vérifié le 21 novembre 2026.

S25: Global News, reportages sur l'atteinte visant Canvas dans des universités canadiennes, mai 2026. https://globalnews.ca/news/11840444/canadian-universities-data-leak/. Vérifié le 21 novembre 2026.

S26: Commissariat à la protection de la vie privée du Canada, rapport spécial sur des atteintes à l'Agence du revenu du Canada, 7 mai 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260507/. Vérifié le 21 novembre 2026.

S27: CTV News, "Ransomware attack hits facility systems at Manitoba's largest hospital", août 2026. https://www.ctvnews.ca/winnipeg/article/ransomware-attack-hits-facility-systems-at-manitobas-largest-hospital/. Vérifié le 21 novembre 2026.

S28: CTV News, reportages sur une cyberattaque visant un district scolaire de la Colombie-Britannique, septembre-octobre 2026. https://www.ctvnews.ca/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S29: Commissariat à la protection de la vie privée du Canada, "Privacy Commissioner of Canada to investigate data breach involving Crime Stoppers", 27 octobre 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_261027/. Vérifié le 21 novembre 2026.

S30: Commissariat à la protection de la vie privée du Canada, enquête sur une atteinte aux données impliquant des renseignements d'identification volés, 21 septembre 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260921/. Vérifié le 21 novembre 2026.

S31: Office of the Information and Privacy Commissioner of Alberta, déclaration sur la distribution non autorisée de la liste électorale, 2026. https://oipc.ab.ca/information-and-privacy-commissioner-of-alberta-issues-statement-regarding-unauthorized-distribution-of-list-of-electors/. Vérifié le 21 novembre 2026.

S32: MTL Blog, "Hydro-Québec cyber scare: Over 1.5 million Quebecers are asked to change their passwords now", 19 novembre 2026, citant un porte-parole d'Hydro-Québec. https://www.mtlblog.com/hydro-quebec-cyber-password-hack. Voir aussi CTV News, "Nearly 2 million Hydro-Québec customers urged to change their passwords", 18 novembre 2026. https://www.ctvnews.ca/montreal/article/nearly-2-million-hydro-quebec-customers-urged-to-change-their-passwords/. Vérifié le 21 novembre 2026.

S33: BleepingComputer, reportage sur la déclaration d'un fournisseur canadien de télécommunications concernant le vol de données de clients entreprises, 20 novembre 2026. https://www.bleepingcomputer.com/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S34: The Globe and Mail, "KPMG Canada data breach", 18 novembre 2026. https://www.theglobeandmail.com/business/technology/article-kpmg-canada-data-breach-client-files-cyber-attack-november-18/. Vérifié le 21 novembre 2026.

S35: Google Threat Intelligence Group, "PRC targets US medical research", 15 juin 2026. https://cloud.google.com/blog/topics/threat-intelligence/prc-targets-us-medical-research. Vérifié le 21 novembre 2026.

S36: Proofpoint, "One email closer to the edge: UNK_MassTraction", 7 juillet 2026. https://www.proofpoint.com/us/blog/threat-insight/one-email-closer-edge-unkmasstraction-physics-exploitation. Vérifié le 21 novembre 2026.

S37: Palo Alto Networks Unit 42, cadre Cairn et attaques autonomes par IA, 12 novembre 2026. https://unit42.paloaltonetworks.com/cairn-framework-ai-autonomous-attacks/. Vérifié le 21 novembre 2026.

S38: Microsoft Threat Intelligence, "Investigating Storm-2755: payroll pirate attacks targeting Canadian employees", 9 avril 2026. https://www.microsoft.com/en-us/security/blog/2026/04/09/investigating-storm-2755-payroll-pirate-attacks-targeting-canadian-employees/. Vérifié le 21 novembre 2026.

S39: Microsoft Threat Intelligence, "Beyond ransomware: tracking Storm-2570", 24 septembre 2026. https://www.microsoft.com/en-us/security/blog/2026/09/24/beyond-ransomware-tracking-storm-2570-consistent-tradecraft-across-deployments/. Vérifié le 21 novembre 2026.

S40: Google Threat Intelligence Group, "UNC6671 targets financial services and enterprise cloud environments", 2026. https://cloud.google.com/blog/topics/threat-intelligence/unc6671-targets-financial-services-and-enterprise-cloud-environments. Vérifié le 21 novembre 2026.

S41: GRC, "Operation Endgame: RCMP join international partners in crackdown of Russian cybercriminal network", 18 juin 2026. https://rcmp.ca/en/news/2026/06/4354276. Vérifié le 21 novembre 2026.

S42: GRC, "Maple Disruption 2.0", novembre 2026. https://rcmp.ca/en/news/2026/11/4358530. Vérifié le 21 novembre 2026.

S43: Global News, arrestations liées à des simulateurs de station cellulaire (SMS blasters) par le Service de police de Toronto, 23 avril 2026. https://globalnews.ca/news/11813885/toronto-police-arrest-cyber-attack/. Vérifié le 21 novembre 2026.

S44: Parlement du Canada, LEGISinfo, projet de loi C-8 (45e législature, 1re session), et texte de la sanction royale. https://www.parl.ca/legisinfo/en/bill/45-1/c-8 et https://www.parl.ca/DocumentViewer/en/45-1/bill/C-8/royal-assent. Vérifié le 21 novembre 2026.

S45: Sécurité publique Canada, "Government of Canada Strengthens Cyber Security and Critical Infrastructure with Royal Assent of Bill C-8", 16 juin 2026. https://www.canada.ca/en/public-safety-canada/news/2026/06/government-of-canada-strengthens-cyber-security-and-critical-infrastructure-with-royal-assent-of-bill-c8.html. Vérifié le 21 novembre 2026.

S46: Commission d'accès à l'information du Québec, pages sur les incidents de confidentialité et sur les sanctions et poursuites visant les entreprises. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises et https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/sanctions-entreprises-poursuites. Vérifié le 21 novembre 2026.

S47: Justice Canada, Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), texte intégral. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html. Vérifié le 21 novembre 2026.

S48: Parlement du Canada, LEGISinfo, projet de loi C-36 (45e législature, 1re session), et texte de première lecture. https://www.parl.ca/legisinfo/en/bill/45-1/c-36 et https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading. Vérifié le 21 novembre 2026.

S49: Gouvernement de l'Ontario, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (S.O. 2024, c. 24). https://www.ontario.ca/laws/statute/24s24. Vérifié le 21 novembre 2026.

S50: BSIF, avis Technology and Cyber Security Incident Reporting. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-security-incident-reporting. Vérifié le 21 novembre 2026.

S51: BSIF, version définitive de la ligne directrice B-13 Technology and Cyber Risk Management (lettre, 13 juillet 2022; en vigueur le 1er janvier 2024). https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfi-releases-final-guideline-b-13-technology-cyber-risk-management-letter-2022. Voir aussi le communiqué du BSIF, "OSFI releases new guideline for technology and cyber risk, balancing innovation with risk management", 13 juillet 2022. https://www.osfi-bsif.gc.ca/en/news/osfi-releases-new-guideline-technology-cyber-risk-balancing-innovation-risk-management. Vérifié le 21 novembre 2026.

S52: Banque du Canada, supervision des paiements de détail. https://www.bankofcanada.ca/core-functions/retail-payments-supervision/. Vérifié le 21 novembre 2026.

S53: Gouvernement du Québec, page du Ministère de la Cybersécurité et du Numérique. https://www.quebec.ca/gouvernement/ministere/cybersecurite-numerique. Vérifié le 21 novembre 2026.

S54: BleepingComputer, "Canada Goose investigating as hackers leak 600K customer records", février 2026. https://www.bleepingcomputer.com/news/security/canada-goose-investigating-as-hackers-leak-600k-customer-records/. Vérifié le 21 novembre 2026.

S55: NIST National Vulnerability Database, fiches de CVE-2024-42009, CVE-2025-49113, CVE-2026-1731, CVE-2026-1281 et CVE-2026-1340. https://nvd.nist.gov/vuln/detail/CVE-2024-42009, https://nvd.nist.gov/vuln/detail/CVE-2025-49113, https://nvd.nist.gov/vuln/detail/CVE-2026-1731, https://nvd.nist.gov/vuln/detail/CVE-2026-1281 et https://nvd.nist.gov/vuln/detail/CVE-2026-1340. Correctifs provisoires et version corrigée prévue (12.8.0.0) d'Ivanti, selon le CERT-EU, Security Advisory 2026-001, 30 janvier 2026. https://cert.europa.eu/publications/security-advisories/2026-001/. Vérifié le 21 novembre 2026.

S56: Centre canadien pour la cybersécurité, "Cyber threat actors use artificial intelligence in an active global campaign to disrupt internet-exposed programmable logic controllers", 8 septembre 2026. https://www.cyber.gc.ca/en/news-events/cyber-threat-actors-use-artificial-intelligence-active-global-campaign-disrupt-internet-exposed-programmable-logic-controllers. Vérifié le 21 novembre 2026.

S57: Centre canadien pour la cybersécurité, "The cyber threat to aviation", 19 octobre 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-aviation. Vérifié le 21 novembre 2026.

S58: Centre canadien pour la cybersécurité, "The Cyber Centre urges heightened vigilance amid global tensions and high-profile events", 4 septembre 2026. https://www.cyber.gc.ca/en/news-events/cyber-centre-urges-heightened-vigilance-amid-global-tensions-high-profile-events. Vérifié le 21 novembre 2026.

S59: Centre canadien pour la cybersécurité, "Cyber Centre warns of sophisticated smishing activity targeting Canadians", 2026 (page datée du 24 avril 2026). https://www.cyber.gc.ca/en/news-events/cyber-centre-warns-sophisticated-smishing-activity-targeting-canadians. Vérifié le 21 novembre 2026.

S60: Commissariat à la protection de la vie privée du Canada, "WestJet commits to improving security measures following a data breach", 14 juillet 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260714/. Vérifié le 21 novembre 2026.

S61: Commissariat à la protection de la vie privée du Canada, "Nova Scotia Power commits to strengthening security measures", 25 mars 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260325/. Vérifié le 21 novembre 2026.

S62: CTV News, reportages sur une cyberattaque visant une université de Calgary, juin-juillet 2026. https://www.ctvnews.ca/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S63: CTV News, reportages sur un vol de données dans une université de Toronto, novembre 2026. https://www.ctvnews.ca/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S64: BNN Bloomberg (The Canadian Press), reportage sur la mise à jour d'un organisme canadien du secteur financier concernant une atteinte, 14 janvier 2026. https://www.bnnbloomberg.ca/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S65: CTV News, "Confidential and sealed files may have been accessed in cybersecurity incident that hit Ontario's courts", septembre 2026. https://www.ctvnews.ca/toronto/article/confidential-and-sealed-files-may-have-been-accessed-in-cybersecurity-incident-that-hit-ontarios-courts/. Vérifié le 21 novembre 2026.

S66: Palo Alto Networks Unit 42, activité liée à BeyondTrust CVE-2026-1731, février 2026. https://unit42.paloaltonetworks.com/beyondtrust-cve-2026-1731/. Vérifié le 21 novembre 2026.

S67: Palo Alto Networks Unit 42, activité liée à Ivanti EPMM CVE-2026-1281 et CVE-2026-1340, février 2026. https://unit42.paloaltonetworks.com/ivanti-cve-2026-1281-cve-2026-1340/. Vérifié le 21 novembre 2026.

S68: CTV News, reportages sur une cyberattaque visant une université de Winnipeg, octobre 2026. https://www.ctvnews.ca/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S69: Centre canadien pour la cybersécurité et ses partenaires, "Joint advisory on Russian GRU exploiting vulnerable routers to steal sensitive information", 2 avril 2026. https://www.cyber.gc.ca/en/news-events/joint-advisory-russian-gru-exploiting-vulnerable-routers-steal-sensitive-information. Vérifié le 21 novembre 2026.

S70: Centre canadien pour la cybersécurité et ses partenaires, "Joint cyber security advisory on Russian state-sponsored phishing campaign targeting Zimbra webmail", 22 juillet 2026 (page datée du 23 juillet 2026). https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-russian-state-sponsored-phishing-campaign-targeting-zimbra-webmail. Vérifié le 21 novembre 2026.

S71: Centre antifraude du Canada, "Canadian Anti-Fraud Centre supported Operation FRONTIER+III", 4 juin 2026. https://antifraudcentre-centreantifraude.ca/news-nouvelles/2026/2026-06-04-eng.htm. Vérifié le 21 novembre 2026.

S72: Services publics et Approvisionnement Canada, "Government of Canada introduces Level 1 of Canadian Program for Cyber Security Certification", 14 avril 2026. https://www.canada.ca/en/public-services-procurement/news/2026/04/government-of-canada-introduces-level-1-of-canadian-program-for-cyber-security-certification.html. Vérifié le 21 novembre 2026.

S73: Ministère des Finances Canada, "Government of Canada launches consultations on first ever National Anti-Fraud Strategy", mars 2026. https://www.canada.ca/en/department-finance/news/2026/03/government-of-canada-launches-consultations-on-first-ever-national-anti-fraud-strategy.html. Vérifié le 21 novembre 2026.

S74: Centre de la sécurité des télécommunications, "Cyber Centre launches new initiative to help Canada's critical infrastructure prepare for severe cyber threats", 17 avril 2026. https://www.canada.ca/en/communications-security/news/2026/04/cyber-centre-launches-new-initiative-to-help-canadas-critical-infrastructure-prepare-for-severe-cyber-threats.html. Vérifié le 21 novembre 2026.

S75: CP24 (The Canadian Press), reportage sur l'audience de détermination de la peine d'un ancien employé de banque, 18 novembre 2026 (plaidoyer de culpabilité en août 2026). https://www.cp24.com/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S76: BleepingComputer, reportage sur une atteinte aux données d'un hôpital pour enfants de Toronto, août 2026. https://www.bleepingcomputer.com/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S77: Global News, reportage sur l'attaque par rançongiciel de 2025 contre un fournisseur de soins à domicile, mars 2026. https://globalnews.ca/ (URL de l'article retenue). Vérifié le 21 novembre 2026.

S78: BleepingComputer, "US and Canada arrest and charge suspected Kimwolf botnet admin", mai 2026. https://www.bleepingcomputer.com/news/security/us-and-canada-arrest-and-charge-suspected-kimwolf-botnet-admin/. Vérifié le 21 novembre 2026.

S79: Centre antifraude du Canada et Bureau de la concurrence, "Fraud Prevention Month to bring hidden crime into the spotlight", 6 mars 2026. https://antifraudcentre-centreantifraude.ca/news-nouvelles/2026/2026-03-06-eng.htm. Vérifié le 21 novembre 2026.

S80: Statistique Canada, "Impact of cybercrime on Canadian businesses, 2025", 21 octobre 2026. https://www150.statcan.gc.ca/n1/daily-quotidien/261021/dq261021b-eng.htm. Voir aussi Statistique Canada, "StatCan Plus weekly review: October 19 to 23, 2026", 23 octobre 2026. https://www.statcan.gc.ca/o1/en/plus/9368-weekly-review-october-19-23-2026. Vérifié le 23 novembre 2026.

S81: Centre de la sécurité des télécommunications, Annual Report 2024-2025, 27 juin 2025. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2024-2025. Vérifié le 23 novembre 2026.

Annexe D. Glossaire

- **Blackhole :** source de données de Brandefense sur la cybercriminalité, qui couvre les publications, les appareils infectés, les identifiants de connexion et les données de cartes.
- **Ransompedia :** base de données de Brandefense sur les rançongiciels; les inscriptions consignent des revendications criminelles.
- **Atlas :** notation de l'exposition externe de Brandefense; les notes vont de 0 (rien d'observé) à 100.
- **Appareil infecté :** appareil dont le journal de vol d'informations contient une connexion au domaine de l'organisation; « employé » est une classification de Brandefense, et non un emploi vérifié.
- **Mise en vente d'identifiants :** identifiant de connexion lié au domaine et offert sur un marché surveillé au moment de la vérification. Dans la carte thermique sectorielle, l'historique de mises en vente compte les inscriptions antérieures consignées avant la vérification actuelle.
- **Liste combinée (combolist) :** liste de paires identifiant-mot de passe compilées à partir de diverses sources; leur ancienneté et leur validité varient.
- **Journal de vol d'informations (stealer log) :** données saisies sur un appareil par un maliciel voleur d'informations.
- **Robot vérificateur (checker bot) :** robot qui teste des cartes volées auprès de passerelles de paiement et affiche le résultat.
- **Fiche de publication :** reproduction caviardée d'une publication du web clandestin, avec le lieu, la date, l'alias, la langue, et ce qu'elle établit ou n'établit pas.
- **Hameçonnage vocal (vishing) :** appel téléphonique dans lequel l'appelant se fait passer pour une personne de confiance, comme le soutien informatique, afin d'obtenir un accès.
- **SaaS :** logiciel-service, comme Microsoft 365 ou un CRM hébergé, où les données d'une organisation se trouvent dans le nuage du fournisseur.
- **« Drops » et comptes mules :** personnes, et comptes ouverts à leur nom, utilisés pour recevoir et transférer les produits de la fraude.
- **Creation :** terme du milieu criminel désignant une identité synthétique ou empruntée qui sert à ouvrir des comptes.
- **Vérification d'identité (KYC) :** contrôles d'identité « connaître son client » (know your customer) effectués par les banques, les plateformes d'échange et d'autres services.
- **AiTM (adversary-in-the-middle) :** page d'hameçonnage qui relaie une vraie connexion et saisit les mots de passe, les codes à usage unique et le témoin de session.
- **AMF résistante à l'hameçonnage :** connexion liée au vrai site (clés de sécurité FIDO2, clés d'accès ou certificats), qu'une page relais ne peut donc pas réutiliser.
- **AMF (authentification multifacteur) :** connexion qui exige un second facteur en plus du mot de passe.
- **TO / PLC :** technologie opérationnelle, et automates programmables (PLC) qui commandent des processus physiques.
- **BIN :** préfixe du numéro de carte propre à l'émetteur (bank identification number).

- **DMARC / SPF / DKIM :** normes d'authentification du courriel; DMARC indique aux destinataires quoi faire du courrier qui échoue.
- **DNSSEC et enregistrement DS :** signatures qui permettent aux résolveurs de vérifier les réponses DNS, et enregistrement de la zone parente qui relie un domaine à ses clés.
- **HSTS :** en-tête Web qui indique aux navigateurs d'utiliser uniquement HTTPS.
- **p=none :** politique DMARC qui se limite à la surveillance et ne demande pas aux destinataires de rejeter ou de mettre en quarantaine.
- **Note globale :** le chiffre Atlas national des 250 organisations, sur l'échelle Atlas de 0 à 100 (0 = aucun risque observé, 100 = le plus élevé).
- **Indice d'hygiène :** indice analytique d'Odin résumant par secteur des résultats de courriel, de DNS, de TLS et d'en-têtes; 0-100, une valeur plus élevée signifie plus faible; pas une cote.
- **Exploitant désigné :** en vertu de la Loi sur la protection des cybersystèmes essentiels, exploitant d'un service vital désigné par règlement, qui assume alors les obligations prévues par la loi.
- **RTO :** objectif de délai de reprise (recovery time objective), soit la plus longue interruption qu'un plan de continuité des activités admet.
- **SMS blaster :** fausse antenne cellulaire portative qui envoie des textos aux téléphones à proximité.

À propos de ce rapport

Préparé par Odin by Brandefense. La version 1.0 a été achevée le 21 novembre 2026.

Date limite de la recherche : 18 novembre 2026 (période des données primaires). Les comptes rendus publics ont été lus jusqu'au 21 novembre 2026. Les éléments publiés après la date limite ne sont inclus que s'ils décrivent des événements antérieurs à celle-ci, et ils sont signalés. Le rapport privilégie les données propres à Brandefense et distingue les revendications criminelles des incidents établis de façon indépendante. Il ne prétend pas recenser de façon complète la cybercriminalité qui touche le Canada. Les recommandations décrivent ce que les organisations pourraient faire; elles n'affirment pas qu'une organisation les a mises en œuvre ou non.

Ceci est l'édition en français canadien, traduite à l'aide de l'IA à partir de l'édition anglaise. L'édition anglaise prévaut en cas de divergence.

© 2026 Brandefense. Tous droits réservés.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS

4.7 / 5

COVERAGE

3 pillars

CTI, DRPS, EASM

MONITORING

24 / 7

Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO