BRANDEFENSE COUNTRY REPORT · CANADA 2026

Brandefense Canada Cyber Threat Landscape Report 2026

Extortion, identity theft and help-desk social engineering in a cloud-dependent economy

Odin by Brandefense
Research window: 1 January–18 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · 21 November 2026

107 of 250
organisations had a credential listed for sale on the day of the check

12,124–12,656
crime-relevant posts directly identified in the 43,549 tagged posts read

3
hacktivist intrusions into Canadian control systems cited by the Cyber Centre (October 2025)

13 of 22
card-issuing banks with a current credential listing, the first item to triage

CONTENTS

Contents

01	Executive summary	04
	Report map	08
02	Canada's digital and threat context	09
03	National exposure: 250 leading organisations	13
04	What we see on the dark web	21
05	Targeting examples by sector	35
06	Hacktivism, DDoS and operational technology	42
07	Threat actors	46
08	The fraud economy	59
09	Banking and finance deep dive	65
10	Regulatory and national response	68
11	Outlook	72
12	Action plan	75
A	Appendix A. Method	82
B	Appendix B. Evidence register	85
C	Appendix C. Sources	86
D	Appendix D. Glossary	91
	About this report	93

Board and executives	01 03 12
CISO and security leads	03 06 07 09 10 12
SOC and threat intelligence	04 06 07 08 12 A B
Fraud and customer protection	04 05 08 09
Communications and legal	06 10 12

About this edition

Prepared by Odin by Brandefense from Brandefense Blackhole, Ransompedia and Atlas data. Analysis and first drafts by AI agents (Anthropic Claude); findings reviewed by Brandefense analysts before release. Method summary in Appendix A.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What happened in 2026, what matters most for Canadian organisations, and what should leaders decide first?

4

decisions for leaders, each tied to evidence in the chapters

Four decisions for leaders 06

The year in numbers 06

CHAPTER 01

Executive summary

IN SHORT

For Canadian organisations, the threat in 2026 was data extortion and identity-led theft. Ransompedia holds 386 accepted Canadian ransomware listings, close to the United Kingdom. Voice phishing caused several reported law-firm breaches; other confirmed incidents involved misused accounts or cloud data without an established initial route. Of the 250 leading organisations we assessed, 107 had a credential listed for sale when we checked. Act in this order: lock down help-desk resets, validate every current listing, then take control systems off the internet.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 696,200 posts tagged as concerning Canada, of which we read a sample that includes most tagged forum posts. It also supplied infected-device and credential records for 250 selected organisations, and card material that appeared in clear text in posts. **Ransompedia** supplied ransomware leak-site listings for Canada and three comparators. **Atlas** exposure ratings were computed for the 250 organisations. These are separate populations and are never added together.

1. Data extortion is steady and close to UK levels. Ransompedia holds 386 accepted listings naming Canadian organisations and dated 1 January-18 November 2026, against 406 for the whole of 2025, a similar or slightly higher annual pace [S6]. The United Kingdom had 377 and Australia 169 in the same window. Qilin (48), The Gentlemen (34) and Akira (33) led. Listings are claims, not confirmed breaches, and manufacturing, construction and consulting firms are named most often (Chapter 7).

2. Voice phishing caused several reported law-firm breaches. On 28 October the Cyber Centre warned of a help-desk voice-phishing campaign against Canadian organisations that bypasses conventional MFA through a real-time relay and steals SaaS data [S15]. The Globe and Mail reported that four large Toronto law firms were breached in this way in October [S16]. Loblaw, Telus Digital, Canada Life and the Canvas learning platform also confirmed 2026 incidents involving accounts or cloud data [S22][S23][S24][S25]. These disclosures confirm account misuse or cloud-data exposure without establishing initial access.

3. 107 of 250 organisations had a credential listed for sale when checked. Using Atlas ratings, the 250-organisation headline is 59 out of 100 (0 = no risk observed, 100 = highest). A listing tells a defender to look for an active account; it does not say how many accounts or whose. Almost every organisation carries infected-device and historical credential associations. These counts are cumulative and require validation; they do not establish a breach [S3][S4].

4. Hacktivists and other attackers have reached exposed control systems. The Cyber Centre reported that in October 2025 a pro-Russia actor manipulated valves at a municipal water system, and that other actors interacted with an airport fuel gauge and a grain silo [S17]. It called the picture deteriorating. In July 2026 a small Quebec municipality reported an attack on its drinking-water station, which the municipality, citing the regional county's security experts, attributed to an organised Russia-based group [S21]. Our own collection held almost no 2026 hacktivist target lists for Canada.

5. A large underground market trades Canadian identities and accounts. In the 43,549 Canada-tagged posts we read, 12,124-12,656 were crime-relevant (Appendix A.2), led by carding, account trading, data offers, identity services and phishing. Forum sellers advertised customer datasets attributed to two national telecoms, a life insurer and an Ontario hospital; only the insurer's offer can be tied to a confirmed incident. Fraud losses reported to the Canadian Anti-Fraud Centre passed 704 million CAD in 2025 [S13].

Four decisions for leaders

1. **Lock down help-desk resets.** Require call-back verification to a known number before any password or MFA reset, and move remote and privileged users to phishing-resistant MFA. It addresses the voice-phishing route behind the reported law-firm breaches (§7.3).
2. **Treat current credential listings as an incident trigger, not a statistic.** Route every current listing tied to your domains to the identity team and record a disposition within 5 working days. Arrange monitoring of credential listings and infected devices from day 1, through an internal team or a provider (§12.1).
3. **Take control systems off the internet.** Put any remote access to water, energy, building or industrial controls behind a jump host with MFA, and check the physical process before commenting on any claim (§6.4).
4. **Prepare for extortion and for several regulators at once.** Rehearse a data-theft extortion case with the reporting deadlines of each regulator that applies to you, including the Critical Cyber Systems Protection Act once you are designated (Chapter 10).

The year in numbers

386

Ransompedia accepted ransomware listings for Canada dated 1 Jan-18 Nov 2026 (406 in 2025)

WHAT IT IS NOT

Not confirmed breaches; unlisted and unpublished cases are invisible

696,200

Blackhole posts tagged as concerning Canada, 1 Jan-18 Nov 2026

WHAT IT IS NOT

Not a count of attacks; January and February are dominated by Turkish-language bot adverts

12,124-12,656

crime-relevant posts directly identified in the 43,549 tagged posts we read (12,124 strictly relevant plus 532 borderline; Appendix A.2)

WHAT IT IS NOT

Not a full-tag census or unique incidents; the 93,500-99,400 chart projection is a non-reproducible model range

250

leading public and private organisations assessed with Atlas methodology

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

644,465

infected devices associated with those 250 domains (32,833 classified as employee devices); cumulative

WHAT IT IS NOT

Not 2026-only, not unique people, not verified current infections

39.7 million

historical credential records for the same domains (breach databases, stealer logs, combolists); cumulative

WHAT IT IS NOT

Not unique accounts or active passwords; telecom totals are mostly customers' mailboxes

107 of 250

organisations with a credential listed for sale at the time of the check

WHAT IT IS NOT

Not a count of accounts or of confirmed breaches

374

distinct Canada-associated payment cards seen in clear text in the posts we read (279 attributed to a named Canadian issuer)

WHAT IT IS NOT

Not a fraud-loss figure; narrow scope (§8.5)

69%

of the 250 organisations enforcing DMARC (173)

WHAT IT IS NOT

Not a measure of phishing success or delivery security

704 million CAD

fraud losses reported to the Canadian Anti-Fraud Centre in 2025 [S13]

WHAT IT IS NOT

Not total fraud; the centre thinks only 5-10% is reported [S79]

Report map

Twelve chapters, five reader paths. Start with the row that matches your role; each chapter opens with the question it answers, and chapters 2-12 close with three takeaways.

Board and executives	What happened, how exposed are we, and what should we decide?	01 03 12
CISO and security leads	Which exposures are ours, which actors matter, and which controls come first?	03 06 07 09 10 12
SOC and threat intelligence	What did the actors post, how are they connected, and which techniques did they use?	04 06 07 08 12 A B
Fraud and customer protection	How are Canadian identities, accounts and cards traded, and where do banks see it?	04 05 08 09
Communications and legal	How do we speak about unverified claims, and which reporting duties apply?	06 10 12

01 Executive summary
What happened in 2026 and what leaders should decide first

02 Context
Which features of Canada and which official figures frame the year

03 National exposure
How exposed 250 leading organisations are, with the national Atlas rating

04 Dark web
What criminals post about Canada once spam is removed

05 Sectors
Which sectors are named and what response each needs

06 Hacktivism and OT
What was claimed, what officials reported, how to prepare

07 Threat actors
Who the actors are, how they connect, what reporting says

08 Fraud economy
How identities and accounts are turned into money

09 Banking
Where banks' visible exposure sits

10 Regulation
What changed in 2026 and which duties apply

11 Outlook
What to plan for and what would change the plan

12 Action plan
Who does what in 90 days

CHAPTER 02

Canada's digital and threat context

02

THIS CHAPTER ANSWERS

Which features of Canada shape the threats in this report, and what do the official figures already say?

95.2%

internet penetration, with 42.8 million cellular connections

2.1 A connected, cloud-dependent population 10

2.2 What the national assessment says 10

2.3 Official counts for the year 11

2.4 Events that prompted official warnings in 2026 11

2.5 A federal state with split responsibilities 12

CHAPTER 02

Canada's digital and threat context

IN SHORT

Canada is a large, highly connected economy whose data is spread across federal, provincial and private systems. The official picture for 2026 is consistent. Ransomware is the top cybercrime threat to critical infrastructure, and state actors pursue espionage and pre-positioning (gaining access now to disrupt later). Fraud losses reported to the national fraud centre passed 700 million CAD in 2025. Plan for ransomware, state espionage and fraud, and report incidents early: official counts depend on it.

2.1 A connected, cloud-dependent population

Canada had about 40.5 million people and 38.6 million internet users in October 2026, a penetration of 95.2%. It had 42.8 million cellular connections (106% of the population) and 34.7 million social-media user identities [S9]. English carries most of the crime-relevant posts we read for Canada; the raw tag is inflated by Turkish- and Chinese-language spam (Chapter 4). French appears rarely in those posts, so French-language fraud aimed at French-speaking Canadians, in Quebec and elsewhere, is likely under-represented in what we see. Most Canada-relevant underground trading happens in English-language Telegram channels and forums that also serve the United States, the United Kingdom and Australia.

2.2 What the national assessment says

The Canadian Centre for Cyber Security (the Cyber Centre) set the frame in its National Cyber Threat Assessment 2025-2026 [S10]. Its main assessments, as the Cyber Centre states them:

- **Ransomware** is the top cybercrime threat to Canada's critical infrastructure, according to the assessment, and cybercrime-as-a-service keeps it cheap to run.
- **The People's Republic of China** has the most sophisticated and active state cyber programme against Canada, according to the assessment.
- **Russia**, in the Cyber Centre's assessment, seeks to confront and destabilise Canada, and pro-Russia non-state actors target Canadian organisations.
- **Iran** uses cyber activity to coerce and harass, and the Cyber Centre judges that it likely has access to some Canadian networks.
- **India** likely conducts cyber espionage against Government of Canada networks, according to the same assessment.
- **North Korea** presents a persistent and well-resourced cybercrime threat to people and organisations in Canada, though not a strategic threat on a par with China or Russia, in the assessment's judgement.

We report these as the Cyber Centre's assessments. They are not this report's own attribution, and the evidence in later chapters is mostly criminal, not state-linked.

2.3 Official counts for the year

Official figures show the scale of reported activity. They use different units and periods, so they should not be added or compared as a trend.

Source	Figure	Period and unit
Communications Security Establishment (CSE) annual report	3,216 cyber incidents responded to: 1,528 federal and 1,688 other Canadian entities [S11]	Fiscal year April 2025-March 2026
Cyber Centre Ransomware Threat Outlook	Ransomware incidents known to the Cyber Centre rose by an average of 26% a year from 2021 to 2024; no raw counts [S12]	Calendar years, known incidents only
Statistics Canada business survey	16% of surveyed Canadian businesses reported an impactful cyber incident in 2025 (unchanged from 2023); among impacted businesses, the ransomware share fell from 13% in 2023 to 8% in 2025 [S80]	Calendar years 2023 and 2025; enterprises with 10 or more employees across most sectors, excluding public administration
Canadian Anti-Fraud Centre	Over 704 million CAD lost in 2025 from over 112,000 reports; only 5-10% of frauds are thought to be reported [S13][S79]	Calendar year 2025, reported losses
Office of the Privacy Commissioner of Canada	Almost 700 breach reports from businesses affecting over 20 million Canadians, and about 450 from federal institutions [S14]	Fiscal year 2025-2026

The CSE report also counts 67 pre-ransomware notifications to Canadian organisations in 2025-2026 [S11]. The Ransomware Threat Outlook gave 336 for 2024-2025 [S12]. The two documents do not explain the difference, so we do not read it as a fall in ransomware.

2.4 Events that prompted official warnings in 2026

Three events prompted official warnings of hostile cyber activity against Canada in 2026.

- **The anniversary of Russia's invasion of Ukraine.** On 19 February CSE said pro-Russia actors had targeted government, military, private and critical-infrastructure networks in Canada, and urged organisations to expect disruption [S20].
- **The US and Israeli strikes on Iran of 28 February.** On 1 March the Cyber Centre assessed that pro-Iran hacktivists would likely view Canada as a target for low-sophistication disruption. It also assessed that Iranian state actors likely spy on activists and journalists in Canada [S18].

- **The FIFA World Cup.** The tournament ran from 11 June to 19 July and included matches in Toronto and Vancouver. The Cyber Centre judged that the tournament would almost certainly be targeted by criminals and by state and non-state actors [S19].

2.5 A federal state with split responsibilities

Cyber governance in Canada is shared. CSE and its Cyber Centre lead technical defence and incident response at the federal level. The RCMP and its National Cybercrime Coordination Centre lead federal cybercrime enforcement, with provincial and municipal police alongside. Privacy breaches go to the federal Privacy Commissioner, to provincial commissioners, or to Quebec's Commission d'accès à l'information, depending on the organisation.

In 2026 Parliament passed Bill C-8, which creates the Critical Cyber Systems Protection Act for federally regulated vital services (Chapter 10). In Quebec, the government's page for the Ministère de la Cybersécurité et du Numérique said in November 2026 that its web content would be grouped with that of the Treasury Board secretariat [S53]. Chapter 10 sets out what changed for organisations.

KEY TAKEAWAYS

01

The Cyber Centre ranks ransomware first among cybercrime threats to critical infrastructure and assesses five state cyber programmes: China, Russia, Iran, India and North Korea.

02

Official counts use different units; read each one on its own, not as a trend.

03

International events in 2026 drew official warnings of hacktivist disruption against Canada.

CHAPTER 03

National exposure: 250 leading organisations

03

THIS CHAPTER ANSWERS

How exposed are Canada's 250 leading public and private organisations when they are scored the way Brandefense Atlas scores a customer, and which signal should a defender triage first?

107 of 250

organisations had a credential listed for sale on the day of the check

3.1 Universe card 14
3.2 National Atlas rating and current listings by sector 15
3.3 Devices and credentials 17
3.4 Current credential listings 18
3.5 Lookalike domains, exposed documents and mentions 19
3.6 Email and web hygiene 19

CHAPTER 03

National exposure: 250 leading organisations

IN SHORT

We assessed 250 leading Canadian organisations with Brandefense Atlas exposure ratings. Almost all have infected devices and historical credential records associated with their domains, and 107 had a credential listed for sale when we checked. 173 of 250 enforce DMARC, but only 27 publish DNSSEC delegation. Triage current listings first, then employee devices.

3.1 Universe card

Item	Definition
Population	250 organisations: 60 government bodies (federal, provincial, territorial and municipal), 33 banking and finance, 22 e-commerce and retail organisations, 22 universities and school boards, 20 energy and utilities, 16 transport, 13 healthcare, 13 media and entertainment, 13 manufacturing and industry, 12 telecom, 11 insurance, 9 technology and IT services, 6 hospitality. 124 public-sector or Crown-owned, 126 private
Selection	Purposive: federal, provincial and municipal bodies, federally regulated banks and large credit unions, Crown corporations and market leaders by size or systemic role. Not ranked by revenue; no published Canadian top-250 ranking was used
Unit	One primary domain per organisation, taken from its official website. All 250 resolve in DNS (21 November 2026); web checks were possible for 184. Domain ownership was assigned from public knowledge of each organisation's official site, not independently confirmed
Measurements	Infected devices and employee devices, breach-database, stealer-log and combolist records, dark-web chat and forum mentions, lookalike domains, exposed documents and current credential-market listings, using the same data Atlas uses; plus public DNS, TLS and HTTP header checks
Date	Counts read 21 November 2026. Device, credential and listing counts are all records held on that date, regardless of capture date (cumulative, not 2026-only). Mention counts cover the past year; lookalike counts cover recently observed domains
Overlap	Counts can overlap across sources, organisations and people. One person can appear in several sources; one device can hold logins for several organisations
Not representative	Results describe this list. They are not national prevalence rates

3.2 National Atlas rating and current listings by sector

Atlas rates each organisation from 0 (no risk observed) to 100. The national headline for the 250 organisations is 59 out of 100; ratings by sector or group are not published here.

How to read Atlas ratings.

Term	Meaning
Headline	The national Atlas figure for the 250 organisations
Current listing	A credential tied to the domain on sale at the time of the check
Sale history	Prior credential-market listings recorded before the current check (106 of 250; in energy and utilities, 4 of the 5 currently listed domains also had a prior listing, while 1 was listed for the first time)

Devices and credentials are near-universal; current listings vary by sector

Share of organisations in each sector with the signal. Current credential listings are shown in coral.

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
E-commerce and retail (22)	95%	95%	100%	77%	77%	91%	95%
Telecom (12)	92%	83%	100%	67%	67%	83%	83%
Education (22)	100%	100%	100%	64%	64%	95%	100%
Media and entertainment (13)	100%	92%	100%	62%	62%	92%	100%
Transport and logistics (16)	100%	75%	100%	56%	56%	81%	88%
Technology and IT services (9)	100%	89%	100%	56%	56%	100%	67%
Banking and finance (33)	100%	91%	100%	42%	42%	94%	94%
Insurance (11)	91%	73%	100%	36%	36%	100%	82%
Government (60)	85%	65%	97%	33%	33%	95%	78%
Hospitality and tourism (6)	83%	67%	100%	33%	33%	83%	67%
Energy and utilities (20)	95%	85%	100%	25%	20%	85%	75%
Manufacturing and industry (13)	100%	100%	100%	8%	8%	85%	100%
Healthcare (13)	100%	85%	100%	0%	0%	77%	77%

Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

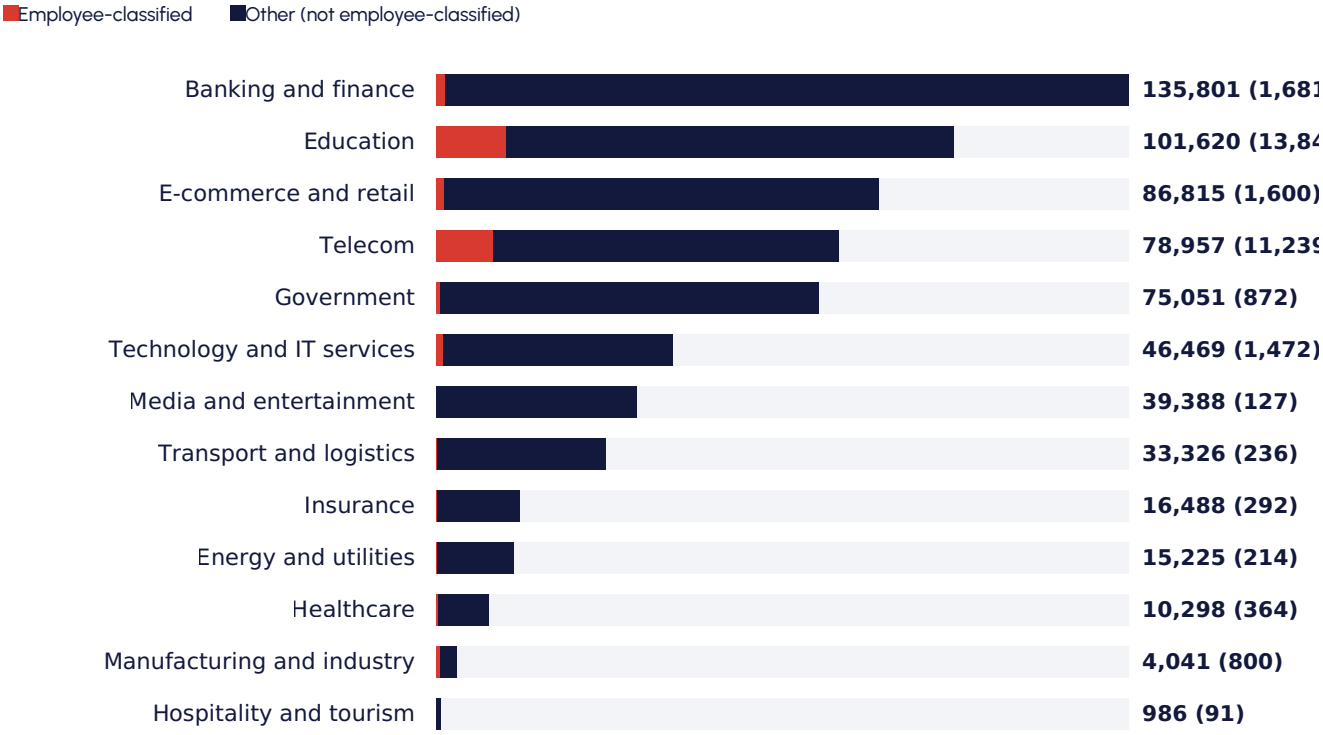
Sector	Orgs	Orgs with a current credential listing
E-commerce and retail	22	17

Sector	Orgs	Orgs with a current credential listing
Telecom	12	8
Education	22	14
Media and entertainment	13	8
Transport and logistics	16	9
Technology and IT services	9	5
Banking and finance	33	14
Insurance	11	4
Government	60	20
Hospitality and tourism	6	2
Energy and utilities	20	5
Manufacturing and industry	13	1
Healthcare	13	0
All 250	**250**	**107**

Reading the table. Current listings vary widely by sector, from none of 13 healthcare bodies to 17 of 22 e-commerce and retail organisations (§3.4).

3.3 Devices and credentials

Banking, education and retail carry the most infected-device associations; telecom and education hold most employee-classified devices



Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share held by two largest orgs
Banking and finance	33 of 33	135,801 (1,681)	1,739,108	48%
Education	22 of 22	101,620 (13,845)	10,597,903	20%
E-commerce and retail	21 of 22	86,815 (1,600)	369,019	34%
Telecom	11 of 12	78,957 (11,239)	22,565,617	88%
Government	51 of 60	75,051 (872)	1,460,082	33%
Technology and IT services	9 of 9	46,469 (1,472)	950,842	87%
Media and entertainment	13 of 13	39,388 (127)	223,053	52%
Transport and logistics	16 of 16	33,326 (236)	186,576	42%

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share held by two largest orgs
Insurance	10 of 11	16,488 (292)	327,945	74%
Energy and utilities	19 of 20	15,225 (214)	389,689	30%
Healthcare	13 of 13	10,298 (364)	379,484	68%
Manufacturing and industry	13 of 13	4,041 (800)	424,683	44%
Hospitality and tourism	5 of 6	986 (91)	77,835	94%
All	**236 of 250**	**644,465 (32,833)**	**39,691,836**	**50%**

The 39,691,836 domain-matched credential records are the sum of 14,991,506 breach-database records, 1,451,109 stealer-log lines and 23,249,221 combolist entries (one login record per line, not deduplicated across sources). Separately, the 644,465 infected devices hold more than 3.9 million captured login pairs across all services on those machines, covering both the 250 assessed domains and third-party sites. That device-side figure sits outside the 39,691,836 domain-record total, but overlaps with the 1,451,109 stealer-log lines where a captured login matches one of the 250 primary domains.

What this means.

- **Telecom credential counts are mostly customers' mailboxes.** Some carriers' domains also serve as consumer email addresses, so the 22.6 million telecom credential records largely belong to customers, not staff. One telecom domain alone carries 15.2 million.
- **Banking carries the device load, mostly outside the employee classification.** 134,120 of 135,801 bank-associated devices are not employee-classified. Their stealer logs include a login to the bank's site, so they are most plausibly customers' own computers, though ownership is not established. These associations are a fraud and account-hijacking signal and do not by themselves establish an intrusion into the bank.
- **Universities hold the largest employee-device problem.** Education has 13,845 employee-classified devices, 42% of the total in our list. Staff and students share domains, so "employee" here may include students; the risk is credential reuse into research, finance and government systems.
- **The median organisation is not small.** The median organisation has 534 infected devices and about 11,800 credential records. Canada's large, cloud-dependent workforce shows up as volume in every sector.

3.4 Current credential listings

107 of 250 organisations had at least one credential tied to their domain listed on a monitored credential market at the time of the check. In the sector heatmap, "sale history" counts prior listings recorded before the current check (106 of 250). In energy and utilities, 4 domains had a prior listing and 1 of the 5 currently listed domains was a first-time listing.

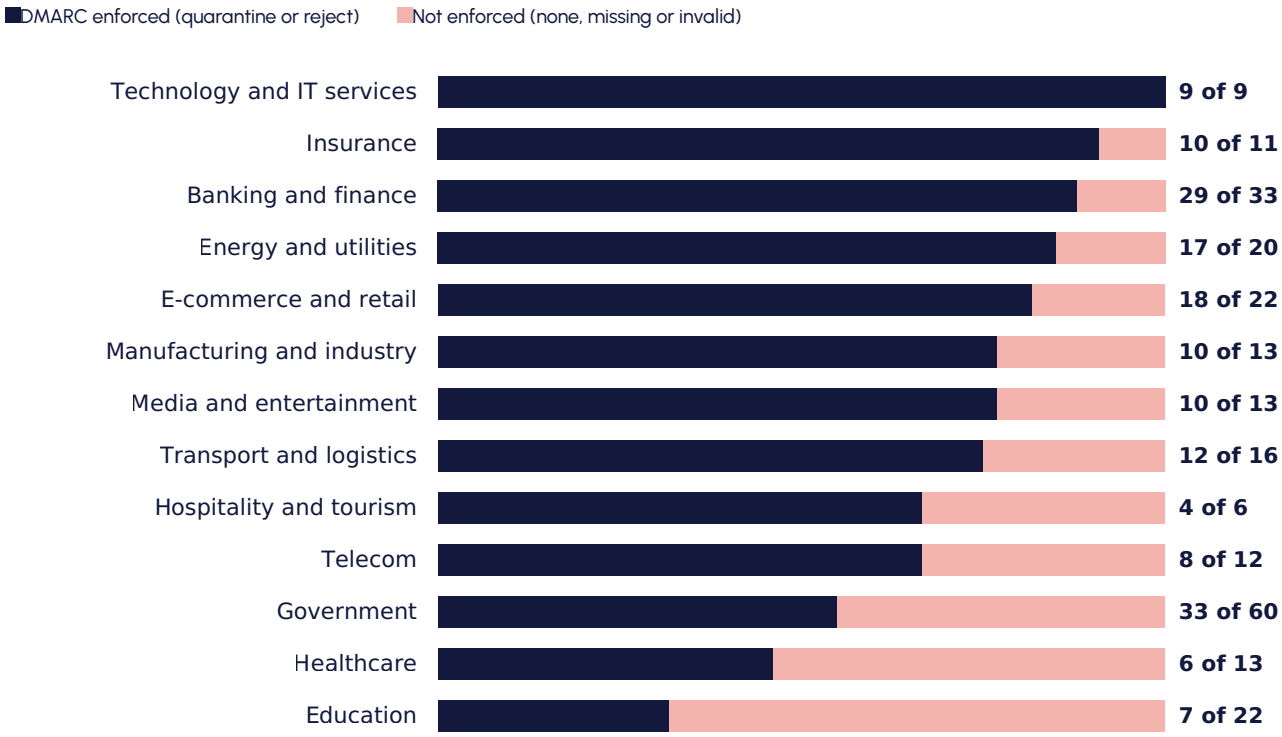
A current listing is the most direct market signal that a login tied to the domain is on offer. Whether that login still works is exactly what validation must establish. The listing does not say how many accounts, whose accounts, or whether the account is active, protected by multi-factor authentication, or already reset. The decision it supports is "validate the account now", not "declare a breach".

3.5 Lookalike domains, exposed documents and mentions

- **Lookalikes:** 227 organisations had at least one recently observed lookalike domain (62,948 in total). Counts are noisier for brands with generic or very common names. Lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 215 organisations have at least one exposed document that references their domain (3,913 in total).
- **Mentions:** 111 organisations were mentioned in dark-chat sources in the past year and 116 in dark-web (onion) sources. Mention counts measure visibility, not hostility.

3.6 Email and web hygiene

Technology, insurance and banking mostly enforce DMARC; universities and health bodies mostly do not



Source: Brandefense public DNS, TLS and homepage checks of 250 domains, 21 November 2026 [S5].

Email, DNS and web results [S5]:

Control	Result (of 250 unless stated)	Reading
DMARC reject	122	Spoofed mail from the domain should be refused
DMARC quarantine	51	Spoofed mail should go to spam
DMARC p=none or missing	77 (69 none, 8 missing)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / redirect / none	127 / 95 / 7 / 9 / 12	12 domains publish no SPF policy
DKIM record found	212	Absence is not proof of no DKIM
DS record observed (DNSSEC delegation)	27	No DS record observed for 223 domains; a DS record alone does not prove a valid chain of trust
TLS certificate invalid	5 of 240 checked	Expired, mismatched or untrusted certificates
HSTS on homepage	150 of 184 reachable	Most reachable sites force HTTPS for returning visitors
Mail provider	135 Microsoft 365, 8 Google, 6 no MX	The rest run their own or other hosted mail

Technology and finance lead, universities and health lag. All 9 technology firms, 10 of 11 insurers and 29 of 33 banking and finance organisations enforce DMARC. Universities and school boards (7 of 22) and healthcare bodies (6 of 13) enforce least, and only 33 of 60 government bodies do. Hygiene index values by sector (Appendix A.5; 0–100, higher means weaker) are highest for education (47) and healthcare (46) and lowest for technology (12) and insurance (18).

Microsoft 365 concentration. 135 of the 250 primary domains route mail through Microsoft 365. That concentration matters for the help-desk and SaaS theft pattern in Chapter 7, in which attackers took data from cloud tenants after a staff member handed over a login.

KEY TAKEAWAYS

01

Device and credential associations are near-universal in the list; they call for validation, not alarm.

02

A current credential listing is the first item to triage: 107 of 250 had one.

03

DMARC enforcement is common (173 of 250), but universities, health bodies and many government domains lag, and DNSSEC is rare.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do criminals actually post about Canada once spam is removed, and which offers matter to defenders?

12,124-12,656

crime-relevant posts directly identified in the 43,549 tagged posts read

4.1 Universe card 22
4.2 Platforms, languages and volume 23
4.3 Crime families after cleaning 25
4.4 Large Canadian datasets on offer 26
4.5 Government and access offers 29
4.6 Case studies 30
4.7 What the forums add 34

CHAPTER 04

What we see on the dark web

IN SHORT

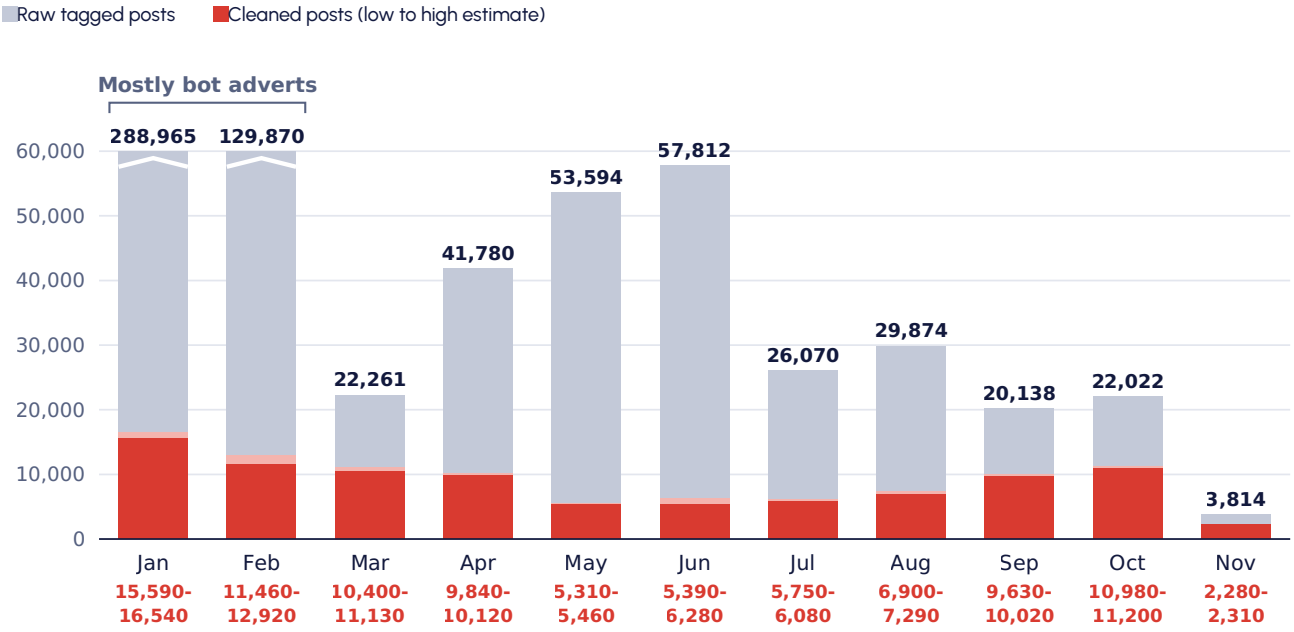
Most Canada-tagged underground traffic is spam that carries a Canadian flag: Turkish-language bot adverts, Chinese-language betting channels and Persian VPN lists. In the 43,549 tagged posts we read, 12,124-12,656 were crime-relevant, led by carding, bank-account trading, data offers, identity services and phishing. Forums carry the most specific claims, including large telecom, insurer and hospital datasets. Rely on the directly read counts rather than raw tag volume, and triage each claim by provenance before comment.

4.1 Universe card

Item	Definition
Source	Brandefense Blackhole: Telegram channels and groups, a set of cybercrime forums, paste sites and Discord, collected continuously
Country definition	A country tag ("this post is about, targets or mentions Canada")
Window	Post time 1 January-18 November 2026 (November partial). Collection time is never used
Tagged set	696,200 posts counted [S1]
Posts read	43,549 tagged posts and 1,438 of the 1,449 tagged forum posts, plus other posts about Canadian brands and places
Combined posts read	60,595 distinct posts
Relevant posts read	12,124-12,656 in the 43,549 tagged posts read (12,124 strictly relevant plus 532 borderline); Charts c01-c02 also plot an indicative model range of 93,500-99,400 (monthly sum 93,530-99,350; Appendix A.2)
Not established	That a tagged post targets Canada, that a claim is true, or that two posts concern the same file

4.2 Platforms, languages and volume

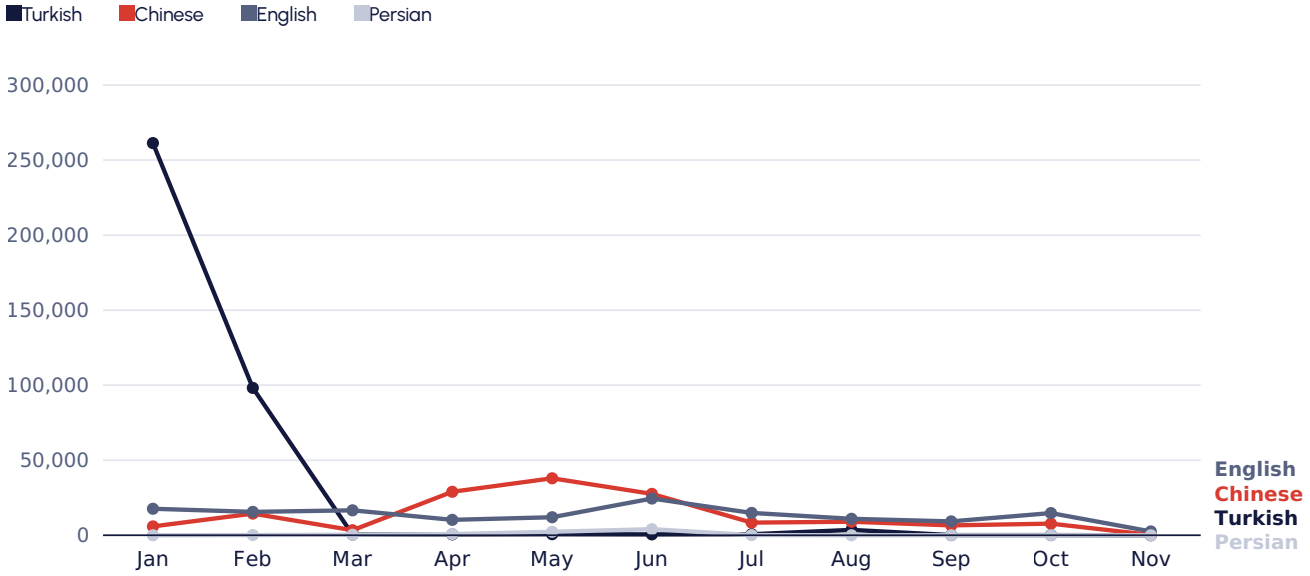
Bot and betting spam inflate January and February; the modelled monthly relevant range is about 5,300-16,500 posts in full months



Source: Brandefense Blackhole, posts tagged as concerning Canada, post dates 1 January-18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Measure	Value
Telegram share of tagged posts	99.75% (694,484)
Forum posts	1,449
Discord and paste sites	214, 53
Raw posts per month	288,965 in January and 129,870 in February; 3,814-57,812 in other months
Tagged posts by language (a post can carry more than one)	Turkish 366,561; Chinese 149,976; English 148,881; Russian 25,679; Persian 7,678; Spanish 2,766; French 320

Turkish and Chinese posts dominate the raw tag; after cleaning, English carries most of the weight



Telegram carries 99.75% of tagged posts. Language labels can overlap. Source: Brandefense Blackhole, posts tagged as concerning Canada, post dates 1 January–18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

The January-February spike is not an attack wave. Turkish-language posts make up 261,356 of January's tagged posts and 98,182 of February's. In the posts we read, they are mostly repeated advertisements for automated messaging bots that carry country flags, including Canada's. Chinese-language posts peak from April to June. They come mostly from betting channels named after a lottery game linked to Canadian keno draws. Persian posts peak in May and June and are mostly free VPN configuration lists.

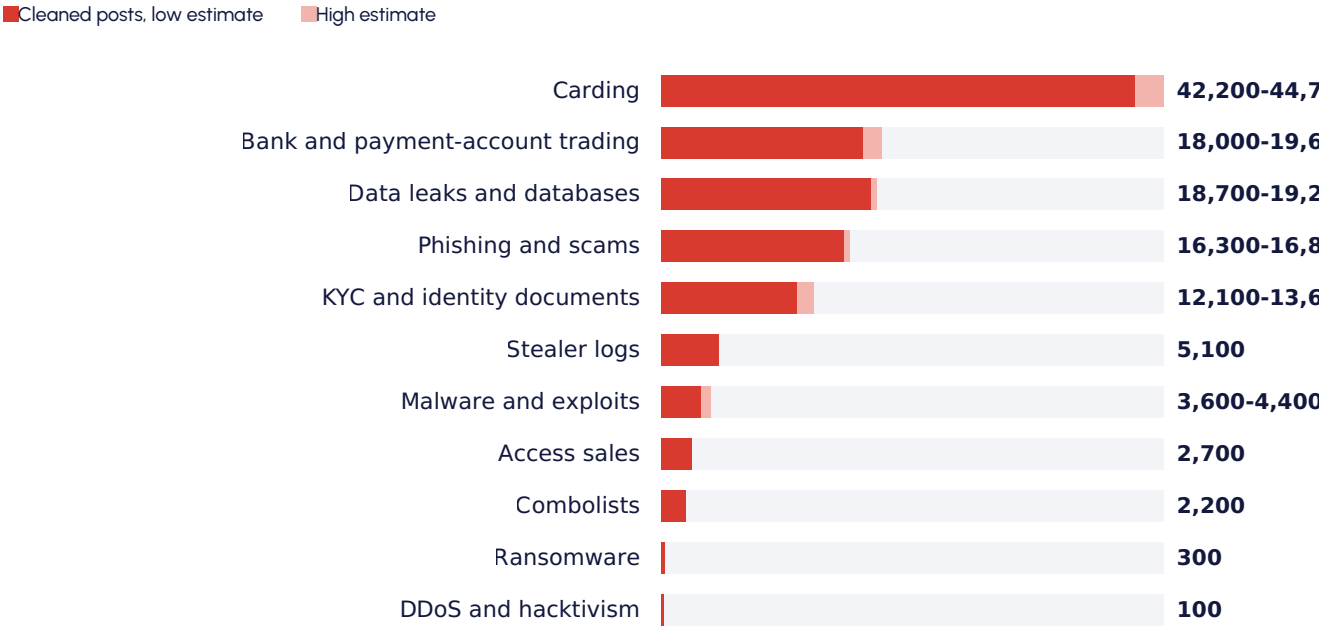
English carries the crime. Of the 43,549 tagged posts we read, 17,579 were in English and 9,096 of those were relevant. Only 188 of 7,543 Turkish posts were. French-language crime posts were rare (26 after cleaning), so French-language fraud aimed at French-speaking Canadians, in Quebec and elsewhere, is probably under-represented.

Collection volume changes across the year. Türkiye's tagged volume falls from 528,914 in May to 107,910 in July, and the other compared countries also move sharply between months. We do not read month-to-month changes in Canadian volume as threat trends.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

4.3 Crime families after cleaning

Carding leads the crime-relevant posts we read; account trading, data offers, identity services and phishing follow



Source: Brandefense Blackhole, posts tagged as concerning Canada, post dates 1 January–18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

The table below leads with the crime-relevant posts directly counted in the 43,549 posts we read. It also lists the indicative full-tag model range plotted in Chart c02, which is not reproducible from public totals (Appendix A.2). Families overlap, so rows must not be added.

Family	Cleaned posts read	Modelled full-tag range (indicative)	What it contains
Carding	5,461	42,200–44,700	Card-checker outputs, card-shop updates, "non-VBV" BIN lists (cards without the Visa online-payment check), buyers seeking Canadian cards
Bank and payment-account trading	3,185	18,000–19,600	Offers to buy, rent or sell bank, fintech and e-transfer accounts; "drops"
Data leaks and databases	3,153	18,700–19,200	Consumer, customer and business lists; telecom, insurer and hospital claims; lookup services
Phishing and scams	1,543	16,300–16,800	Bank and telecom phishing pages, SMS lures, "scam-page" kits

Family	Cleaned posts read	Modelled full-tag range (indicative)	What it contains
KYC and identity documents	1,772	12,100–13,600	Driver's licence and passport scans with selfies, verification bypass guides
Stealer logs	580	5,100	Log sales and "bank logs" with balances
Malware and exploits	627	3,600–4,400	Tool sales and exploit discussion, mostly global
Access sales	589	2,700	Remote desktop, VPN and corporate access, often multi-country
Combolists	273	2,200	Country-labelled email-and-password lists
Ransomware	72	300	Relays of leak-site claims; Chapter 7 uses Ransompedia instead
DDoS and hacktivism	25	100	Small within the tag; see Chapter 6

Many cleaned posts we read are multi-country lists in which Canada is one flag among dozens. Treat both the read counts and the modelled ranges as upper bounds for Canada-specific crime.

Prices quoted. In cleaned posts that state a price, the median asking price was 120 USD for bank and payment accounts and 80 USD for KYC and document services. Access offers had a median of 140 USD and stealer-log offers 180 USD (Chapter 8). These are asking prices, not completed sales.

4.4 Large Canadian datasets on offer

The most specific Canadian claims appear on forums [S2]. None was independently verified, and we did not obtain any file.

Date	Claimed dataset	Claimed volume and price	Venue	Post
9 Jan	"Canada residential" directory data	About 10 million records; a repost was titled "[FAKE]"	Two breach forums	B07
23 Jan	Contact list of one diaspora community (seller's description)	115,000 rows	Breach forum	B08

Date	Claimed dataset	Claimed volume and price	Venue	Post
21 Mar	Customer data attributed to a national telecom and its mobile sub-brand	10.9 million lines, 300,000 USD	Breach forum	B01
25 Apr	Customer data attributed to a second national telecom	1.8 million lines, 100,000 USD	Breach forum	B02
29 Apr	Records attributed to a life insurer's cloud CRM	"5.6M+", free download	Three forums, April–July	B03
8 May	Data attributed to a financial regulator's website	"127M+" records	Breach forum	B15
14 Nov	Patient records attributed to an Ontario hospital	1.9 million identity records	Breach forum	B13

What this tells defenders. Large Canadian datasets are advertised often, and claimed sizes vary widely. Some claims are internally inconsistent: the 127 million "financial regulator" records list drug codes and subsidy values. One coincides with a confirmed incident: the insurer offer, posted nine days after the insurer's own disclosure (Case B). The fields that recur are name, address, phone, email and date of birth, sometimes with social insurance numbers. Organisations that verify customers by those fields should assume they are not secret.

The posts as they appeared, redacted:

Evidence card B01 — 21 Mar 2026

Murad · Breach forum · Forum · English

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]

Held
The offer, the claimed size (10.9 million lines), the asking price and the escrow condition.

Not established
That the data came from the carrier, its age, or any sale.

Evidence card B02 — 25 Apr 2026

Murad · Breach forum · Forum · English

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]

Held
A second carrier offer by the same alias, with the same contact and the same escrow wording, five weeks after B01.

Not established
Access to the carrier's internal network, the data's origin or age.

Evidence card B03 — 29 Apr 2026

GlitchX | Breach forum | Forum | English

ORIGINAL

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

Held
A free-download listing citing 5.6 million records, posted nine days after the insurer disclosed unauthorised access; re-posted on two other forums in May and July.

Not established
That the file matches the insurer's systems, or the number of people affected.

Evidence card B13 — 14 Nov 2026

scarlettgroup | Breach forum | Forum | English

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) [...]

Held
A leak claim with record counts, four days before our cut-off; the group also appears in leak-site listings.

Not established
Any confirmation by the hospital or the authorities by 18 November.

Evidence card B07 — 9 Jan 2026

phoenix_leads | Breach forum | Forum | English

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]

Held
A residential directory-style offer; a repost on a second forum the same day was titled "[FAKE]".

Not established
Source, freshness or uniqueness; the label "fake" is another user's view, not a finding.

Evidence card B08 — 23 Jan 2026

hulky | Breach forum | Forum | English

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]

Held
A contact list of one diaspora community in Canada, as the seller describes it; a separate buyer in February sought similar data on residents of Canada and the US described by origin.

Not established
Source, accuracy or purpose of either post.

Evidence card B15 — 8 May 2026

MDGhost | Breach forum | Forum | English

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 [...]

Held
A claim whose fields (drug codes, health department, subsidies) do not match a financial regulator's site.

Not established
Any link between the data and the site named.

4.5 Government and access offers

Date	Observed post	Our reading	Post
17 Mar	A request for access to federal government mailboxes, naming six federal domains	Demand signal, not evidence of access	B05
13 May	Remote-desktop web and ERP access at a Quebec food distributor with "$100M+" revenue	A typical initial-access offer; the access route matches exposed remote-desktop gateways	B06
9 Nov	"Full admin access" to a cloud CRM tenant run by a third-party provider and holding a federal tribunal's participant contacts	Unverified; if genuine, the exposure sits at a supplier, not in the tribunal's own systems	B04

Evidence card B05 17 Mar 2026

Anonymous poster | Telegram group | Telegram | English

ORIGINAL

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

Held
Demand for access to federal government mailboxes, naming six federal domains.

Not established
That anyone supplied such access.

Evidence card B06 13 May 2026

XOverStm | Breach forum | Forum | English

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. [...]

Held
An access offer describing remote-desktop web access and ERP visibility at a Quebec food distributor.

Not established
The victim's identity, whether the access worked, or any sale.

Evidence card B04 9 Nov 2026

DataJava | Breach forum | Forum | English

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] [...]

Held
A claim of administrator access to a cloud CRM tenant run by a third-party provider and holding a federal tribunal's participant contacts.

Not established
That access exists or existed, that the tribunal's own systems were entered, or any official confirmation.

4.6 Case studies

Each case follows the same structure: claim, chronology, what we can establish, alternatives, limits and a proportionate response.

CASE A

A ■ One alias offers two national telecom databases (B01, B02)

Telecom

Claim unverified

CLAIM	On 21 March the alias Murad offered 10.9 million lines said to come "directly from" a national telecom and its mobile sub-brand, for 300,000 USD. On 25 April the same alias offered 1.8 million lines said to come "directly from" the "internal network" of a second national telecom, for 100,000 USD.
WHAT WE CAN ESTABLISH	That one alias, with one contact and the same escrow wording, posted both offers on two forums five weeks apart. That is a shared concrete element, so the two posts are linked to one persona.
WHAT WE CANNOT ESTABLISH	That either dataset came from the carrier's network, its age, or whether they were sold. An older file attributed to the second carrier was re-shared on another forum in April. We could not tie the March and April forum offers (B01, B02) to either confirmed telecom incident in this report, and this report does not say which carriers those offers name.
ALTERNATIVES	Repackaged older leaks; data taken from a reseller, a billing partner or a marketing list; a genuine intrusion.
RESPONSE	Carriers should compare any sample with their schemas and with known older files before comment. Customers' phone numbers and addresses should be treated as known to fraudsters, so SIM-swap and port-out checks matter more than secrecy of those fields.

Bottom line

One persona, two carrier datasets: compare samples with schemas and older leaks before comment, and harden SIM-swap checks meanwhile.

CASE B

B ■ An insurer's confirmed incident and a 5.6 million-record claim

Evidence card B03 | 29 Apr 2026 | Breach forum | Insurance

Incident confirmed; volume unverified

CLAIM	On 29 April a forum poster offered "Over 5.6M Salesforce records" attributed to a life insurer, as a free download. The post was re-shared on two other forums in May and July.

CHRONOLOGY	Canada Life said on 20 April that an employee account had been used for unauthorised access to certain applications, affecting "a small proportion" of customers [S24]. A data-extortion group claimed the insurer on 19 April, according to a public tracker [S7].
WHAT WE CAN ESTABLISH	The insurer confirmed an incident. The forum post's record count is the poster's own figure; we did not obtain the file.
ALTERNATIVES	A genuine extract of the incident data; an inflated count; an unrelated dataset relabelled to ride the news.

Bottom line

The insurer confirmed an incident; the 5.6 million figure is the poster's. Match any sample to the incident scope before speaking.

Point	Forum poster's claim	Company's account	Press reporting
What happened	Records taken from a cloud CRM	Unauthorised access to certain applications through an employee account [S24]	Thousands reportedly affected [S24]
Volume	"5.6M+" records	A small proportion of customers [S24]	Not stated as 5.6 million
Data	"PII"	Not detailed in the statement we read	Not detailed

- **Response.** For any organisation in a similar position, compare the posted sample with the incident scope before public comment. Customers who are notified should expect follow-up phishing that cites the incident.

CASE C

C

A supplier's cloud tenant offered as a federal tribunal breach

Claim unverified

Evidence card B04 | 9 Nov 2026 | Breach forum | Government (supplier)

CLAIM	On 9 November a forum poster offered "full admin access" to a cloud CRM tenant run by a third-party provider. The poster said it held over 100,000 participant contact records for a federal tribunal.
WHAT WE CAN ESTABLISH	The offer, the claimed field list and the named tenant. We found no official statement about it by our cut-off.
ALTERNATIVES	Stale or partial access; a misdescribed tenant; a genuine supplier compromise.

RESPONSE	Public bodies should list which suppliers hold their case data in cloud CRM platforms, confirm that those tenants enforce phishing-resistant MFA and logging, and review recent administrator sign-ins.

Bottom line

If genuine, the exposure is at a supplier's cloud tenant: list who holds your case data and check their admin sign-ins.

D

CASE D

An access offer at a Quebec food distributor

Evidence card B06 | 13 May 2026 | Breach forum | Food distribution

Access offer (one post)

CLAIM	On 13 May a forum seller offered remote-desktop web access and "Full ERP" visibility at a Quebec food-distribution firm with "$100M+" revenue, with user-level domain access.
WHAT WE CAN ESTABLISH	The offer and its description. The posts do not name the firm.
WHY IT MATTERS	Access offers like this are a common first step before ransomware, which in Canada most often names manufacturing, construction and consulting firms (Chapter 7).
RESPONSE	Put remote-desktop web gateways behind phishing-resistant MFA, alert on new sign-ins from hosting networks, and review stealer-log exposure for staff with remote access (Chapter 3).

Bottom line

Defenders should protect remote-desktop web gateways with phishing-resistant MFA.

E

CASE E

A hospital leak claim four days before the cut-off

Evidence card B13 | 14 Nov 2026 | Breach forum | Healthcare

Claim unverified

CLAIM	On 14 November a group calling itself scarlettgroup claimed to have breached an Ontario hospital and posted record counts, including about 1.9 million patient identity records.
WHAT WE CAN ESTABLISH	The claim and its counts. Neither the hospital nor the authorities had confirmed an incident by 18 November in the sources we checked.
ALTERNATIVES	Data taken from a supplier or an older system; inflated counts; a genuine intrusion.

RESPONSE	For hospitals, the first step is to compare the posted sample with current and legacy patient systems and with suppliers that hold extracts. Prepare a patient notice in case a sample is verified.

Bottom line

Compare the posted sample with current, legacy and supplier systems; prepare a patient notice in case it is verified.

4.7 What the forums add

Forums carried only 1,449 tagged posts, but they hold almost all the named-organisation claims. They also hold buyer requests: in January a buyer sought "service-based" Canadian company data from 2025-2026 only, and in April a user asked for a database from a large Canadian financial institution. Small automated uploads of credential files for Canadian lottery, airline and telecom login pages appeared from May to August. Those files held from 5 to 100 lines each, which points to stealer-log extracts from users' own devices rather than a breach of the sites.

KEY TAKEAWAYS

01

Raw volume is mostly flag-carrying spam; rely on the 12,124-12,656 relevant posts we directly read, and treat modelled full-tag ranges as indicative upper bounds.

02

Forum offers named two national telecoms, a life insurer and a hospital; only the insurer's offer can be tied to a confirmed incident.

03

Access offers and a request for federal mailboxes are demand signals; check remote-access gateways and supplier tenants first.

CHAPTER 05

Targeting examples by sector

05

THIS CHAPTER ANSWERS

Which Canadian sectors are named in criminal posts, extortion claims and official reports, and what first response does each need?

10

sectors with observed or reported activity, from government to retail

CHAPTER 05

Targeting examples by sector

IN SHORT

Every major Canadian sector appears in 2026 evidence, but in different forms. Banks and telecoms are named mostly as fraud infrastructure; insurers, retailers and professional firms as data-theft victims; hospitals, schools and universities as extortion targets; and water systems as tampering targets. Post examples are claims; official and company reports are marked as such. Start with the sector's first response.

Victims are described by role under the policy in Appendix A.9, unless an incident was confirmed and widely reported. Examples are drawn from Blackhole posts, Ransompedia and the public reporting in Appendix A.8.

Government

Access demand | supplier claim | account takeover | unauthorised release (under investigation)

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Request for federal mailbox access (Mar; B05); claimed admin access to a supplier's CRM tenant holding a federal tribunal's contacts (Nov; B04); Canada Revenue Agency account takeovers since 2020 (Privacy Commissioner [S26]); the province's list of electors, about 2.9 million people, posted on a third party's website without authorisation (Apr; provincial privacy commissioner [S31])

WHAT IT MEANS

Identity takeover and suppliers are the main routes; citizen data spreads beyond the body that collected it

FIRST RESPONSE

Enforce phishing-resistant MFA on citizen and staff accounts; inventory suppliers that hold case data

Banking and finance

Account trading | KYC fraud | carding | data breach

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Aged accounts at nine named banks and fintechs for sale (B10); remote-KYC bypass guides (B11); card-checker output naming 10 issuers (§8.5); a Canadian financial-industry body reported a 2025 breach affecting about 750,000 investors (Jan [S64])

WHAT IT MEANS

Posts are dominated by fraud tooling; mule accounts and onboarding are the exposure

FIRST RESPONSE

Tighten remote onboarding; alert on checker declines on your BIN ranges (Chapter 9)

Insurance

Confirmed incident | data claim | extortion claim

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

A life insurer confirmed unauthorised access through an employee account (Apr; Canada Life [S24]); a 5.6 million-record claim followed (B03); an extortion claim against another insurer's wealth arm (unverified [S7])

WHAT IT MEANS

A misused employee account and SaaS data; initial access not disclosed

FIRST RESPONSE

Review SaaS bulk-export alerts and help-desk reset rules

Telecom

Data claims | phishing | confirmed incidents

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Claims: two national carrier databases offered by one alias (B01, B02); a Quebec telecom phishing kit asking for social insurance numbers (B14). Confirmed, separate incidents: Telus Digital confirmed unauthorised access (Mar [S23]); a Canadian telecom provider confirmed theft of enterprise customer contact data from a pre-production system (17 Nov [S33])

WHAT IT MEANS

Telecoms are both breach targets and fraud infrastructure (SIM, number porting)

FIRST RESPONSE

Validate claimed datasets against schemas; tighten port-out and SIM-swap checks

Professional and legal services

Vishing | confirmed incidents

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Four large Toronto law firms breached through help-desk voice phishing (Oct [S16]); KPMG Canada confirmed access to client tax documents (Nov [S34])

WHAT IT MEANS

Client files are the target; the help desk is the door

FIRST RESPONSE

Call-back verification for every MFA or password reset; alert on mass downloads

Retail and consumer brands

Confirmed incident | data leak | account-access advert

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Loblaw confirmed customer account data accessed, about 2 million affected (Privacy Commissioner [S22]); Canada Goose said an order dataset leaked by ShinyHunters was historical and not from its own systems (Feb [S54]); advertised access to loyalty accounts (B16; unverified)

WHAT IT MEANS

Loyalty and e-commerce accounts carry personal and payment data

FIRST RESPONSE

Monitor credential stuffing; force MFA for loyalty accounts

Healthcare

Ransomware | data claim

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Ransomware on Manitoba's largest hospital's facility systems (Aug [S27]); a leak claim against an Ontario hospital (Nov; B13); Ransompedia lists 25 health-labelled Canadian claims

WHAT IT MEANS

Extortion against clinical and building systems; patient data

FIRST RESPONSE

Segment building-management systems; rehearse patient notification

Education

SaaS breach | ransomware | espionage

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Canvas learning-platform breach affecting Canadian universities (May [S25]); universities in Calgary, Winnipeg and Toronto and a British Columbia school district confirmed data theft (Jun-Nov [S28][S62][S63][S68]); Roundcube exploit campaign targeting Canadian universities; Canadian compromise not established (vendor research [S36])

WHAT IT MEANS

Universities hold research and personal data and run exposed webmail

FIRST RESPONSE

Patch webmail; enforce MFA for staff and students; review SaaS tenants

Energy and utilities

OT tampering | account takeover

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Hacktivist tampering with a municipal water system (Oct 2025, Cyber Centre [S17]); a Quebec drinking-water station attacked (Jul [S21]); more than 2,500 unusual logins to Hydro-Québec's customer portal, with passwords reused from other sites (customer-account takeover; Oct [S32])

WHAT IT MEANS

Exposed control systems and customer portals

FIRST RESPONSE

Remove control systems from the internet; MFA for customer portals

Transport

Account-access advert | extortion claim | supplier compromise

EXAMPLE OF OBSERVED OR REPORTED ACTIVITY

Advertised access to frequent-flyer accounts with stated balances (B16; validity unverified); an extortion claim against a Canadian airline (Sep, unverified [S7]); public-address systems at three airports misused through a cloud provider (Oct 2025 [S57])

WHAT IT MEANS

Loyalty fraud and supplier systems

FIRST RESPONSE

Monitor loyalty accounts for unusual logins; review suppliers with access to airport systems

Reading across sectors. Confirmed 2026 incidents cluster in sectors that hold large customer datasets in cloud platforms: retail, telecom, insurance, professional services and education. The underground posts cluster in banking and telecom, but mostly as tools for fraud against customers. This report does not measure harm.

Why manufacturing, construction and consulting are covered in Chapter 7. The table above groups the 10 sectors where 2026 evidence included specific forum offers, confirmed disclosures or official case studies. Manufacturing (42 accepted Ransompedia listings), construction (36) and consulting (30) lead the leak-site claims in §7.2 [S6], matching the Cyber Centre's assessment that ransomware actors opportunistically target downtime-sensitive and supply-chain firms [S12]. Because their 2026 evidence sits in aggregate leak-site claims rather than confirmed public disclosures, their response is set out under remote-access hardening (Case D) and ransomware recovery (§7.2, Chapter 12).

KEY TAKEAWAYS

01

Confirmed 2026 breaches cluster where customer data sits in cloud platforms: retail, telecom, insurance, law and education.

02

Banks and telecoms appear mostly as fraud infrastructure: aged accounts, KYC bypass, SIM and phishing kits.

03

Water systems and other exposed control systems face tampering; verify any claim with the physical process first.

CHAPTER 06

Hacktivism, DDoS and operational technology

06

THIS CHAPTER ANSWERS

Who claimed disruption against Canada in 2026, what did officials confirm, and why does operational technology matter more than website outages?

3

hacktivist intrusions into Canadian control systems cited by the Cyber Centre (October 2025)

6.1 Timeline 43

6.2 Control systems: the cases the Cyber Centre published 44

6.3 Websites, airports and claims 44

6.4 Lessons for defenders 45

CHAPTER 06

Hacktivism, DDoS and operational technology

IN SHORT

In 2026, the strongest hacktivist evidence for Canada was not DDoS claims but official reports of tampering with exposed control systems. The Cyber Centre reported that in October 2025 pro-Russia and pro-Hamas actors interacted with a water system, an airport fuel gauge and a grain silo, and called the picture deteriorating. In July 2026 a small Quebec municipality reported an attack on its drinking-water station and, citing regional experts, attributed it to an organised Russia-based group. Take control systems off the internet, and pre-agree who speaks when a claim appears.

6.1 Timeline

15 Oct 2025	**Cyber Centre** October 2025: pro-Russia and pro-Hamas actors interacted with a municipal water system, an airport fuel gauge and a grain silo (reported 28 July 2026)
20 Oct 2025	**Cyber Centre** October 2025: a cloud-provider compromise let actors broadcast political messages on public-address systems at three Canadian airports (reported 2026)
19 Feb 2026	**CSE** Pro-Russia actors targeted government, military, private and critical-infrastructure networks in Canada; expect DDoS and defacement around the invasion anniversary
1 Mar 2026	**Cyber Centre** Pro-Iran hacktivists will likely view Canada as a target after the 28 February strikes on Iran
2 Mar 2026	**Defacement feed** Five relays list text files placed on provincial procurement web hosts on 28 February; unverified
29 May 2026	**Cyber Centre** World Cup bulletin: the tournament will almost certainly be targeted by criminals, non-state and state actors
23 Jul 2026	**Municipality, as reported by Le Soleil** A drinking-water station in Bas-Saint-Laurent attacked at 07:30; an employee intervened; the municipality, citing regional experts, attributed it to an organised Russia-based group
28 Jul 2026	**Cyber Centre** Bulletin: non-state actors keep targeting internet-exposed control systems in Canada; no high-impact incident yet, but the picture is deteriorating
4 Sep 2026	**Cyber Centre** Calls for heightened vigilance against DDoS and defacement amid global tensions and high-profile events

8 Sep 2026 **Cyber Centre**
AI-enabled global campaign against internet-exposed programmable logic controllers; targeting in Canada observed; not attributed

Coral markers are official statements, outlined markers are third-party relays. The two October 2025 items come before the research window; we include them because the 2026 bulletins rest on them. Dates of the October items are approximate within the month.

6.2 Control systems: the cases the Cyber Centre published

The most important hacktivist evidence for Canada in 2026 is official, not from actor channels. On 28 July the Cyber Centre published a bulletin on non-state activity against Canadian operational technology (OT), the systems that run physical processes [S17]. It described three incidents from October 2025:

Target	Actor as described	What happened	Impact stated
Municipal water system	Pro-Russia actor	Water-pressure valves manipulated	Minor service impact
Airport fuel-tank gauging system	Pro-Hamas actor	System accessed	View only
Grain-drying silo	Pro-Russia actor	Temperature and humidity settings changed	No damage reported

The Cyber Centre said that Canada had avoided a high-impact OT incident so far, but called the picture "deteriorating" [S17]. It assessed that this activity very likely increases around policy announcements and major events, and that most of it is almost certainly independent of states.

On 8 September the Cyber Centre added an advisory on a global campaign that uses AI-generated scripts to disrupt internet-exposed programmable logic controllers. It observed targeting in Canada and did not attribute the campaign [S56].

A Quebec water station in July. A small municipality in the Bas-Saint-Laurent region reported that its drinking-water station was attacked at 07:30 on 23 July. An employee intervened soon after 08:00. The municipality, citing the regional county's security experts, attributed the attack to an organised Russia-based group, and said public safety was never at risk [S21]. We report the attribution as theirs, not ours; we found no technical report on the case.

6.3 Websites, airports and claims

The Cyber Centre's aviation assessment of 19 October cites the October 2025 compromise of a cloud provider. It let actors broadcast political messages on public-address systems at three Canadian airports [S57]. The case shows how a third-party service can carry an outside actor's political message into a critical site through a supplier rather than, as far as the assessment states, through the airport's own network.

In our own data, hacktivist claims against Canadian targets are close to absent. The posts we read held no 2026 DDoS target list naming Canadian organisations. They held five defacement-feed relays of text files placed on provincial procurement web hosts on 28 February, which we could not verify. This contrasts with the official warnings of February, March and September [S18][S20][S58]. Two explanations fit: Canadian targets appear in channels we do not collect, or the actors chose other countries in 2026. Our data cannot separate them.

6.4 Lessons for defenders

1. **Take control systems off the internet.** The Cyber Centre ties these cases to actors scanning for internet-exposed control systems [S17]. Put remote access behind a VPN or a jump host with phishing-resistant MFA, and change default passwords.
2. **Treat a physical reading as the truth.** If a hacktivist claims control of a pump or valve, check the physical process and the local log before any public comment.
3. **Watch the providers, not only your own network.** The airport case ran through a cloud provider. Ask service providers how they would detect and report misuse of systems that broadcast to your sites.
4. **Pre-agree the public line.** Decide in advance who confirms service status, and how quickly, if a hacktivist posts a claim about your organisation.

KEY TAKEAWAYS

01

The Cyber Centre's three October 2025 OT cases, not DDoS claims, are the most important hacktivist evidence for Canada.

02

A Quebec municipality attributed a July attack on its water station to a Russia-based group, citing its regional county's experts; the attribution is theirs, not ours.

03

Our collection held almost no 2026 hacktivist target lists for Canada; that is a gap, not proof of calm.

CHAPTER 07

Threat actors

07

THIS CHAPTER ANSWERS

Who is behind the activity, how are the actors connected, and what does public reporting say about each of them?

386

accepted ransomware leak-site listings for Canada, 1 January–18 November 2026

7.1 How the actors connect 47

7.2 Ransomware and extortion 48

7.3 Identity-led data theft: the help-desk and SaaS pattern 51

7.4 State-linked espionage 55

7.5 Criminal personas seen in Blackhole 57

7.6 Enforcement against actors operating in or from Canada 58

CHAPTER 07

Threat actors

IN SHORT

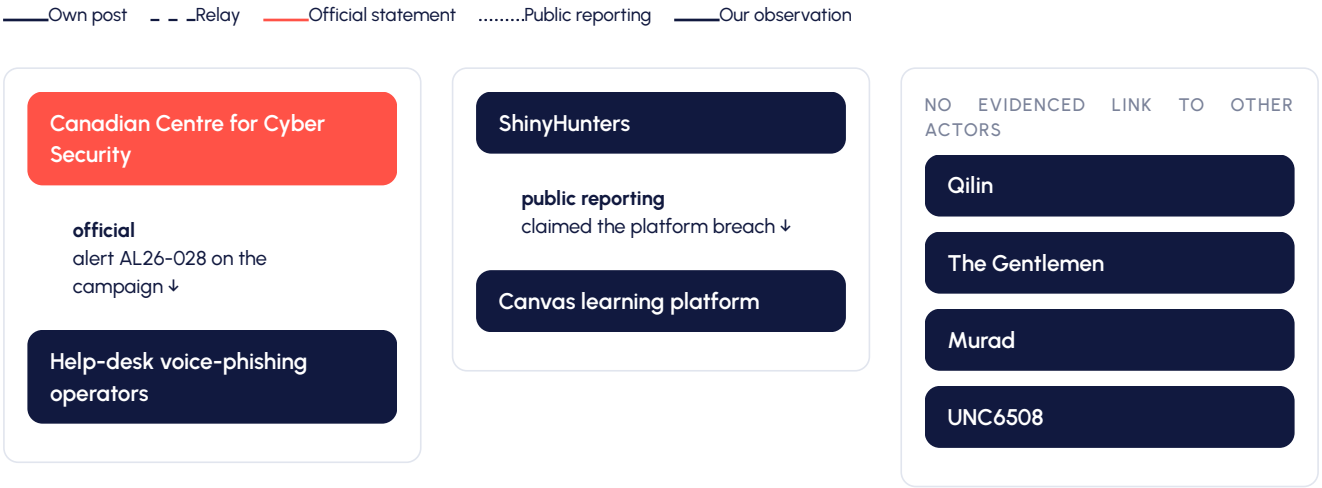
Extortion groups are the most visible actors against Canada: Ransompedia holds 386 accepted Canadian listings in 2026, about as many as for the United Kingdom. Voice phishing caused several reported law-firm breaches, with callers talking staff into handing over access; other disclosures confirm account misuse or cloud-data exposure without establishing initial access. State-linked actors appear in vendor and official reporting, mostly against research, universities and civil society. Harden the help desk and identity recovery first, then rehearse your response to extortion.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Each profile separates **observed behaviour**, **the actor's own claim**, **what remains unresolved** and **what it means for organisations**. Confidence applies to a specific proposition, not to the actor as a whole.

7.1 How the actors connect

The map links actors only where a source holds evidence, and each line says what kind: the actor's own post, an official statement, public reporting or our own observation. A line is an association, not proof of a common operator. No evidence links the profiled extortion brands, personas and state-linked actors to each other, except where a line is drawn.



7.2 Ransomware and extortion

Canada had 386 accepted ransomware listings in 2026, close to the United Kingdom and more than twice Australia

Canada

386

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
406	1449

Groups in 2026

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

United States

4532

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
3996	15475

Groups in 2026

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

United Kingdom

377

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
288	1420

Groups in 2026

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

Australia

169

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
129	619

Groups in 2026

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

Source: Brandefense Ransompedia accepted listings, all dates, to 18 November 2026 [S6]; ransomware.live as a cross-check [S7].

Ransompedia, Brandefense's ransomware database, holds 386 accepted leak-site listings naming Canadian organisations and dated 1 January-18 November 2026 [S6]. That compares with 406 for the whole of 2025, 377 for the United Kingdom and 169 for Australia in the same 2026 window. The United States had 4,532. Monthly Canadian counts ranged from 23 (March) to 45 (May).

Group	Canadian listings 2026	Share of 386
Qilin	48	12.4%
The Gentlemen	34	8.8%
Akira	33	8.5%
Clop	24	6.2%
Play	20	5.2%

Group	Canadian listings 2026	Share of 386
INC Ransom	15	3.9%
DragonForce	15	3.9%
Other groups	197	51.0%

The leading sectors in the listings were manufacturing (42), construction (36), consulting (30), health (25), technology (22), education (21) and finance (19). These are sector labels on claims, and one victim can be listed more than once.

Microsoft reported in September that Storm-2570, a ransomware affiliate it tracks working with several ransomware brands including Qilin and DragonForce, had intrusions in Canada [S39].

What a listing is. A listing is a criminal's claim that it attacked or stole data from an organisation. It is not a confirmed breach, and its country label can be wrong; Ransompedia counts accepted listings only [S6]. A public tracker lists claims for several large Canadian brands in 2026, including an airline, an insurer's wealth arm and a software company. We found no statement by those companies or the authorities confirming an incident, so we describe them only as unverified claims [S7].

Where an organisation's own statement matches a claim. For several public bodies, the organisation confirmed an incident and an extortion group later listed it [S6]. Examples include Manitoba's largest hospital, whose operator Shared Health reported ransomware on facility systems in August [S27]. A British Columbia school district confirmed a ransomware attack in September and the theft of student, parent and staff data in October [S28]. Universities in Calgary, Winnipeg and Toronto confirmed data theft between June and November [S62][S63][S68].

What it means. On leak sites, Canadian extortion pressure is steady across 2025 and 2026. By contrast, Statistics Canada's business survey found that the ransomware share among impacted businesses fell from 13% in 2023 to 8% in 2025, while overall incident prevalence stayed at 16% [S80]. Those two measures cover different periods and populations: the survey samples Canadian enterprises with 10 or more employees across most sectors, excluding public administration, whereas Ransompedia counts public extortion claims. Planning should assume data theft as well as encryption: a restore test shows that recovery works, not that stolen files stay private.

Qilin

Agenda

Ransomware and data extortion | Financially motivated

SEEN IN PUBLIC REPORTING

Jan-Nov

48 accepted Canadian leak-site listings, the most of any group (Ransompedia)

CLAIMED TARGETS

Companies, schools, universities and public bodies

Sep

Named by Microsoft as one of the brands a ransomware affiliate deployed in intrusions that included Canada

Sep-Nov

Listings of a British Columbia school district and a Toronto university followed incidents the institutions confirmed

SEEN IN PUBLIC REPORTING

[S6] Ransompedia: 48 of 386 accepted Canadian listings in 2026; also the leading group for the US, the UK and Australia in the same window

[S39] Microsoft: Storm-2570, an affiliate working with Qilin and other brands, had intrusions in Canada

OUR ASSESSMENT

The most active extortion brand against Canada in 2026 by listings. A listing is a claim; several matched incidents the victims confirmed, most did not.

CONFIDENCE

High that it listed Canadian victims; individual intrusions unverified unless the victim confirmed

The Gentlemen

Ransomware and data extortion | Financially motivated

SEEN IN PUBLIC REPORTING

Jan-Nov

34 accepted Canadian listings (Ransompedia)

Sep

A public tracker shows a claim against a Canadian airline; no confirmation found

CLAIMED TARGETS

Companies across sectors, including a claimed Canadian airline

SEEN IN PUBLIC REPORTING

[S6] Ransompedia: second for Canada, the UK and Australia, and fourth for the US, in 2026

[S7] Public tracker: claim against a Canadian airline in September, unconfirmed by the company or the authorities in the sources we checked

OUR ASSESSMENT

A high-volume brand whose largest Canadian claim was not confirmed by our cut-off. Treat its claims as triggers for validation, not as facts.

CONFIDENCE

High that it listed Canadian victims; the airline claim unverified

7.3 Identity-led data theft: the help-desk and SaaS pattern

Voice phishing caused several reported law-firm breaches in 2026. Other disclosures confirm account misuse or cloud-data exposure without establishing initial access, and some breaches ran through suppliers' software (below).

Help-desk voice-phishing operators

Not named by the Cyber Centre

Data theft and extortion (social engineering) | Financially motivated, according to the Cyber Centre

SEEN IN PUBLIC REPORTING

Jan

Infrastructure naming Canadian organisations first seen, according to the Cyber Centre

Jul

Targeting of finance and legal firms rises

19-31 Oct

Four large Toronto law firms breached through fake IT-support calls, according to press reporting

28 Oct

Cyber Centre alert AL26-028

TARGETS

Legal and financial firms; Microsoft 365 and other SaaS tenants

SEEN IN PUBLIC REPORTING

[S15] Cyber Centre: callers pose as IT support and relay the login in real time, bypassing conventional MFA; they take SaaS data and may send extortion demands after data theft

[S16] The Globe and Mail: four large Toronto law firms breached through fake IT-support calls; the paper links the alert to these breaches

[S40] Google Threat Intelligence, cited in the alert's footnotes: UNC6671 targets financial services and enterprise cloud environments; the Google report itself does not mention Canada

OUR ASSESSMENT

The campaign the press linked to the confirmed 2026 law-firm breaches. Who runs it is not stated by the Cyber Centre; the Google reports in its footnotes are a lead, not an attribution.

CONFIDENCE
High that the campaign targeted Canadian firms (official); operator identity unresolved

On 28 October the Cyber Centre published alert AL26-028 on a help-desk voice-phishing campaign against Canadian organisations [S15]. Callers posed as internal IT support and steered staff to a sign-in page that relayed the real login in real time, bypassing conventional (non-phishing-resistant) MFA. The actors then took data from Microsoft 365 and other software-as-a-service (SaaS) platforms, and the alert says they may send extortion demands after data theft. Its footnotes cite Google's research on the same activity [S40]. The alert says the Cyber Centre had seen infrastructure naming Canadian organisations since January. Targeting of finance and legal firms rose from July, and October activity centred on legal firms.

The steps the alert describes map onto the techniques below. The mapping is ours; the Cyber Centre's alert is the source for each step [S15].

TECHNIQUES MAPPED TO THE STEPS THE ALERT DESCRIBES, BY TACTIC

Initial access	Defence evasion	Credential access	Persistence	Collection	Impact
T1566.004 Spearphishing voice: calls posing as internal IT support	T1656 Impersonation of IT staff	T1557 Adversary-in-the-middle sign-in page relaying the real login	T1078.004 Valid cloud accounts	T1530 Data from cloud storage (Microsoft 365 and SaaS, accessed via the Microsoft Graph API; external exfiltration channel not specified in the alert)	T1657 Financial theft: extortion demands
		T1111 Multi-factor authentication interception (real-time relay of conventional MFA)			

Odin's mapping of the steps the Cyber Centre describes in alert AL26-028 to MITRE ATT&CK techniques; the mapping is ours, not the Cyber Centre's. The alert states that the Microsoft Graph API was used to access and exfiltrate Microsoft 365 data but does not specify the external destination, so no separate exfiltration-channel technique is mapped. [S15]

The Globe and Mail reported that four large Toronto law firms were breached in this way between 19 and 31 October [S16]. Each firm confirmed an incident. The newspaper linked the Cyber Centre's alert to these breaches; the alert itself names no victim.

ShinyHunters

Data theft and extortion | Financially motivated

SEEN IN PUBLIC REPORTING

Feb

Leaked an order dataset of a Canadian outerwear brand; the company said it was historical and not from its own systems

Mar

Claimed a theft of up to 1 PB from Telus Digital; the company confirmed limited unauthorised access

Apr

Listed a Canadian life insurer on its leak site, according to a public tracker

May

Claimed the Canvas learning-platform breach that affected Canadian universities

CLAIMED TARGETS

Consumer brands, telecom outsourcing, insurance and education platforms

SEEN IN PUBLIC REPORTING

[S54] BleepingComputer: over 600,000 order records leaked; the company said its own systems showed no breach

[S23] BleepingComputer: Telus Digital confirmed a breach after the group claimed about 1 PB

[S25] Global News: Canadian universities affected by the Canvas breach the group claimed

OUR ASSESSMENT

The data-extortion brand most often tied to confirmed Canadian incidents in 2026. Its volume claims are routinely larger than what victims confirm.

CONFIDENCE

High that it claimed these victims; claimed volumes unverified

Other confirmed 2026 incidents involved accounts or cloud data; the route is disclosed for only some of them. Each is a separate incident; we do not attribute them to one actor.

When	Organisation	What was confirmed	Route disclosed?	Source
February-March	Loblaw (grocery and pharmacy retailer)	A hacking group accessed customer account data; about 2 million Canadians affected	No	Privacy Commissioner [S22]
March	Telus Digital (customer-experience arm of Telus)	Unauthorised access to a limited number of systems; ShinyHunters claims a far larger theft	No	Company statement [S23]
April	Canada Life (life insurer)	Unauthorised access to some applications through an employee account	Employee account used; initial compromise mechanism undisclosed	Company statement [S24]
Early May	Instructure (Canvas learning platform)	Unauthorised activity affecting Canadian universities' course platforms; ShinyHunters claimed it	No	Universities and vendor [S25]
October-November (reported 18-19 November)	Hydro-Québec (electric utility)	Customer-account takeover, not a breach of the utility's systems: more than 2,500 unusual logins to the customer portal (20 October), and the utility said its systems were not breached; email-code MFA extended to all customers on 5 November	Yes: passwords reused from other sites, according to the utility	Company statement, as reported [S32]
November	KPMG Canada (professional services)	Some client tax documents accessed; method not disclosed	No	Company statement [S34]
17 November (reported 20 November)	A Canadian telecom provider	An attacker, according to the company, took enterprise customer contact data from a pre-production system	Not stated; the data sat in a pre-production system	Company statement, as reported [S33]

We could not tie the March and April forum offers ([B01], [B02]) to either confirmed telecom incident in this report, and this report does not say which carriers those offers name.

Suppliers carried several of the year's breaches. In September the Privacy Commissioner opened an investigation into a breach at IDScan.net, an identity-scanning service used by bars and hospitality businesses, involving scans of driver's licences and other ID [S30]. In October it opened one into Navigate360, the vendor of the tip platform

used by Crime Stoppers programmes across Canada [S29]. Ontario's courts disclosed in September that a case-management supplier's platform had been used to obtain court files; the supplier said sealed information may have been affected [S65].

Two health suppliers also figured in 2026 disclosures. A Toronto children's hospital said in August that staff and job-applicant data were exposed through a flaw in a third-party application [S76]. Press reporting in March showed that a 2025 attack on a medical-supply vendor to Ontario's home-care system was ransomware [S77]. The Commissioner also published 2026 follow-ups on two 2025 breaches: WestJet, where a social-engineering MFA bypass affected over 5 million customers and employees, and Nova Scotia Power, with over 900,000 affected [S60][S61].

What it means. For Canadian organisations, the help desk, the identity provider and SaaS tenants are now the front door. Phishing-resistant MFA, call-back verification for password and MFA resets, and alerting on bulk SaaS downloads are the controls that match these cases.

7.4 State-linked espionage

State-linked activity reached Canada mainly through vendor research and official joint advisories. We present each attribution exactly as its source states it.

UNC6508

State-linked espionage (as attributed by the vendor) | "PRC-nexus", according to Google Threat Intelligence

SEEN IN PUBLIC REPORTING

Jun
Google reports organisations in the US and Canada found compromised with INFINITERED malware on REDCap research-data servers

TARGETS

Medical and research organisations running research-data servers

SEEN IN PUBLIC REPORTING

[S35] Google Threat Intelligence: a campaign attributed to UNC6508, a PRC-nexus threat actor; multiple organisations across the US and Canada found compromised

OUR ASSESSMENT

The only 2026 vendor report we found that states Canadian organisations were compromised by a state-linked actor. Victims and data taken are not published.

CONFIDENCE
Attribution as stated by the vendor; Canadian victims unnamed

Source and date	Actor as named	Canadian element	Attribution wording
Google Threat Intelligence, 15 June [S35]	UNC6508	Organisations in the US and Canada found with INFINITERED malware on REDCap research-data servers	"a People's Republic of China (PRC)-nexus threat actor"
Proofpoint, 7 July [S36]	UNK_MassTraction	Roundcube mail servers at US and Canadian universities targeted with exploits since May 2026; compromise of Canadian servers not stated	"likely a China-aligned espionage" actor
Unit 42, 12 November [S37]	CL-STA-1238	A Canadian human-rights body among the targets; compromise not stated	"a China-nexus intelligence collection campaign", with "moderate confidence"
Cyber Centre with partners, 2 April and 22 July [S69][S70]	Russian state-sponsored actors	Global router and Zimbra webmail campaigns; no Canadian victims stated	As stated by the agencies
Cyber Centre, 1 March [S18]	Iranian state actors	Likely spying on activists, journalists and human-rights advocates in Canada	Cyber Centre assessment

Patch reference. The Roundcube flaws are behind the university campaign. In February Unit 42 linked the three edge-product flaws to activity in several countries including Canada, without naming an actor [S66][S67]. Ivanti issued interim patches before the permanent fix.

CVE	Product	Affected / fixed	CISA known-exploited	Source
CVE-2024-42009	Roundcube webmail	Fixed in 1.5.8 and 1.6.8	Known exploited (NVD)	[S55]
CVE-2025-49113	Roundcube webmail	Fixed in 1.5.10 and 1.6.11	Known exploited (NVD)	[S55]
CVE-2026-1731	BeyondTrust Remote Support and Privileged Remote Access	Remote Support before 25.3.2; Privileged Remote Access before 25.1	Added 13 February 2026	[S55][S66]
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM)	Through 12.7.0.0; permanent fix 12.8.0.0	Added 29 January 2026	[S55][S67]
CVE-2026-1340	Ivanti Endpoint Manager Mobile (EPMM)	Through 12.7.0.0; permanent fix 12.8.0.0	Added 8 April 2026	[S55][S67]

Unresolved. Which Canadian organisations were affected in the research-server campaign, whether any Canadian university server was breached in the Roundcube campaign, and what was taken. **Meaning.** Universities, research institutes and civil-society bodies are the Canadian targets most often named in 2026 vendor research. Webmail and research-data servers exposed to the internet deserve the same patch discipline as perimeter firewalls.

Government networks beyond the federal core. CSE assesses in its 2024-2025 annual report that provincial, territorial, municipal and Indigenous government networks are valuable targets for state-sponsored cyber espionage [S81]. That standing assessment is broader than the 2026 vendor reports above, which documented research-server intrusions [S35] and university or civil-society targeting [S36][S37], without publicly confirming a 2026 provincial or territorial espionage breach. Sub-national public bodies should still apply the same perimeter-patching and identity controls.

7.5 Criminal personas seen in Blackhole

Murad

Data-seller persona | Financially motivated

SEEN IN PUBLIC REPORTING

21 Mar
Offers 10.9 million lines attributed to a national telecom and its sub-brand for 300,000 USD (B01)

25 Apr
Offers 1.8 million lines attributed to a second national telecom for 100,000 USD (B02)

CLAIMED TARGETS

National telecom customer data

IN THEIR WORDS

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

SEEN IN PUBLIC REPORTING

No reputable public reporting found

OUR ASSESSMENT

No reputable public reporting was found. One persona links two high-priced telecom offers through a shared contact and wording. Neither dataset's origin is established. We could not tie these offers to either confirmed telecom incident in this report.

CONFIDENCE
High that one persona posted both; data origin unverified

Aliases only; no contacts, links or real identities. These personas posted Canada-specific offers on forums in 2026 (Chapter 4).

Persona or brand	Observed role in 2026	Own claim	Unresolved
phoenix_leads	Forum poster of a "Canada residential" dataset (January, April)	About 10 million records	Origin; one forum labelled a repost "fake"
CC-GuRu	Forum poster of large Canadian consumer and business lists (April)	40 million consumers; 400,000 businesses	Origin, age, duplication with other lists
Maxi_Leaks	Recurring poster of "Canada" email-and-password lists (April)	68,000-186,000 lines each	Freshness; whether lines repeat
Sophia01	Forum poster of a match-making site's database (October)	23 GB with passwords and cookies	Any verification

7.6 Enforcement against actors operating in or from Canada

Several 2026 actions concern actors operating in or from Canada, or infrastructure used against Canadians.

- **Operation Endgame.** In June the RCMP joined international action against the SocGholish malware network, which it described as linked to the Russian cybercriminal group Evil Corp. It said the network had hit Canadian critical infrastructure, education and government, and that all affected Canadian entities were notified [S41].
- **Maple Disruption 2.0.** From 2 to 6 November the RCMP and the Canadian Anti-Fraud Centre led over 50 partners in 10,987 disruptive actions against fraudsters and recovered about 1.06 million CAD [S42].
- **DDoS botnet arrest.** In May police in the United States and Canada charged a 23-year-old Ottawa man suspected of administering the Kimwolf DDoS botnet [S78].
- **SMS blaster arrests.** In April Toronto Police charged three people with using a mobile "SMS blaster" to send fraudulent texts, to which tens of thousands of devices connected, according to police. Police called it a first in Canada [S43].

KEY TAKEAWAYS

01

Canada carried 386 accepted ransomware listings in 2026, close to the United Kingdom; listings are claims, not confirmed breaches.

02

Voice phishing caused several reported law-firm breaches; other disclosures, such as an insurer's misused employee account, do not establish initial access; Hydro-Québec also saw customer-account logins with reused passwords.

03

Vendor research named universities, research servers and a human-rights body as Canadian targets of state-linked espionage.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How do criminals turn Canadian identities and accounts into money, and what do they charge for it?

704M CAD

fraud losses reported to the Canadian Anti-Fraud Centre in 2025

8.1 What the official figures say 60
8.2 Bank and payment-account trading 60
8.3 Identity, KYC, insiders and counter verification 61
8.4 Phishing kits and loyalty accounts 62
8.5 Card material in posts: a narrow view 63
8.6 Prices in context 64

CHAPTER 08

The fraud economy

IN SHORT

Canada's fraud economy runs on identity. Underground channels sell aged bank accounts, insiders, in-person verification at service counters for "drops" (mule account holders) and guides to beat remote identity checks, while phishing kits imitate Canadian banks and telecoms. Reported fraud losses passed 704 million CAD in 2025, with investment fraud the largest single type. Confirm payment changes out of band, and assume name, address and birth date are known to criminals.

8.1 What the official figures say

The Canadian Anti-Fraud Centre (CAFC) received over 112,000 fraud reports in 2025, with over 704 million CAD in reported losses [S13]. Losses reported since 2022 exceed 2.4 billion CAD [S79]. The centre estimates that only 5-10% of frauds are reported, so the true figures are higher [S79].

Fraud type (2025)	Reported losses	Reports
Investment	351 million CAD	4,409
Spear phishing	67.9 million CAD	813
Relationship	63.3 million CAD	Not stated on the page
Job	50.6 million CAD	Not stated on the page
Extortion	23 million CAD	2,767

Identity fraud was the most reported type, with 8,403 reports [S13]. Losses reported to the CAFC passed 188 million CAD in the first quarter of 2026 [S71].

The Privacy Commissioner's special report on the Canada Revenue Agency counted more than 42,000 individual breaches of taxpayer accounts since 2020. They involved unauthorised access to or changes of taxpayer information, used for fraudulent benefit requests [S26]. That is the same identity-takeover pattern that the underground posts in this chapter sell as a service.

8.2 Bank and payment-account trading

Bank-account trading is the second-largest crime family in our read sample, with 3,185 cleaned posts read (modelled full-tag range 18,000-19,600; Chapter 4). Typical posts sell "aged" accounts at Canadian banks and fintechs with debit cards and online access, or recruit "drops" who open accounts for others (B10). E-transfer is the payment rail most often named, alongside crypto exchanges. The posts show offers; they do not show that such accounts were opened or used at any assessed bank.

Evidence card B10 13 May 2026

Calciumpound Telegram channel Telegram English

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} [...]

Held
An offer of aged bank accounts opened with fabricated or borrowed identities, with debit cards and online access.

Not established
That accounts were opened at any named bank, or used for fraud.

8.3 Identity, KYC, insiders and counter verification

KYC and document posts (1,772 cleaned posts read; modelled full-tag range 12,100-13,600) offer driver's licence and passport scans with selfies. They also offer paid guides to pass a Canadian fintech's remote identity check from abroad (B11), and "creations": synthetic or borrowed identities for opening accounts. Some fraud-services menus advertise insiders at a delivery company, a bank and a mobile carrier (B09). Others sell in-person identity verification at a service counter for drops (B12). We cannot establish that any claimed insider exists. The offers still show where criminals think the weak points are: in-person verification, mail redirection and carrier support desks.

Evidence card B11 5 May 2026

bigbosskyc1 Telegram group Telegram English

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

Held
A paid how-to for passing a Canadian fintech's remote identity check from abroad, using a VPN and temporary phone numbers.

Not established
That the method works today.

Evidence card B09 1 Jan 2026

Fraud-services vendor | Telegram channel | Telegram | English

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

Held
A fraud-services menu advertising synthetic identities and claimed insiders at a delivery company, a bank and a mobile carrier.

Not established
That any insider exists or is employed by those organisations.

Evidence card B12 14 Sep 2026

Fraud-services vendor | Telegram group | Telegram | English

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 [...]

Held
A service to pass in-person identity verification at a service counter for "drops", the people whose accounts receive fraud proceeds.

Not established
That the service works or was used.

8.4 Phishing kits and loyalty accounts

Phishing posts (1,543 cleaned posts read; modelled full-tag range 16,300-16,800) include custom pages that imitate Canadian banks and telecoms. One kit imitating a Quebec telecom asks for the victim's social insurance number as well as card details (B14). One shop advertised access to airline and hotel loyalty accounts with stated points balances; validity, provenance and any completed sale are unverified (B16).

Evidence card B14 16 Jun 2026

theghostorder01 | Fraud forum | Forum | English

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 [...]

Held
A phishing kit imitating a Quebec telecom brand that asks victims for their social insurance number and card details.

Not established
Whether the kit was deployed, or against how many people.

Evidence card B16 17 Mar 2026

Loyalty-account shop | Telegram channel | Telegram | English

ORIGINAL

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

Held
An advertisement claiming access to airline and hotel loyalty accounts with stated points balances, including a Canadian airline's programme.

Not established
Whether the accounts are valid, where the access came from, or whether any sale took place.

Official reporting matches these patterns:

Date	Reported by	What happened
2026 (page dated 24 Apr)	Cyber Centre with the RCMP	Sophisticated SMS phishing impersonating banks and other trusted organisations, actively targeting mobile users across Canada [S59]
April	Microsoft	A financially motivated actor it calls Storm-2755 used fake Microsoft 365 sign-in pages to steal session tokens and attempt to redirect Canadian employees' salary deposits; Microsoft documents at least one redirected payroll payment [S38]
23 April	Toronto Police	Three people charged for using a mobile "SMS blaster" to send fraudulent texts in the Toronto area; tens of thousands of devices connected to it, according to police [S43]
October-November (reported 18-19 November)	Hydro-Québec	Customer-account takeover: more than 2,500 unusual logins to the customer portal (20 October), using passwords reused from other sites, according to the utility; it said its systems were not breached and extended email-code MFA to all customers on 5 November [S32]
2-6 November	RCMP and CAFC	Maple Disruption 2.0: 10,987 disruptive actions against fraudsters and cybercriminals [S42]

8.5 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

The card figures in this report cover only payment cards that appeared in clear text inside the dark-web posts we read for this report. Brandefense detects stolen cards through many other methods, which this report does not cover. These figures are not a measure of card theft or fraud loss in Canada.

Within that narrow scope, 374 distinct Canada-associated cards appeared in clear text in the posts we read: 279 attributed to one of 10 named Canadian issuers and the other 95 labelled only as Canadian. Half of them (190) appeared in card-checker output, and 147 of the 374 appeared in January posts [S8]. The useful signal for issuers is the checker pattern: batches of cards tested with small authorisations against merchant gateways (Chapter 9).

8.6 Prices in context

Product (cleaned posts)	Median asking price	Spread
Bank or payment account	120 USD	50-220 USD
KYC or document service	80 USD	30-200 USD
Access offer	140 USD	90-500 USD
Stealer-log offer	180 USD	80-833 USD
Data offer	20 USD	10-58 USD
Phishing tool or page	8 USD	3.5-50 USD

Prices are asking prices from a minority of posts that quote one; they do not measure market value or completed sales. Spread is the middle half of the quoted prices (25th to 75th percentile), not the full range. The two telecom datasets in Chapter 4 were priced at 100,000 and 300,000 USD, far outside these ranges.

KEY TAKEAWAYS

01

Reported fraud losses passed 704 million CAD in 2025; the centre thinks only 5-10% of fraud is reported [S79].

02

Underground services target identity checks: aged accounts, insiders, counter verification and remote-KYC bypass guides.

03

Card figures cover only cards seen in clear text in the posts we read (§8.5).

CHAPTER 09

Banking and finance deep dive

09

THIS CHAPTER ANSWERS

Where does the visible exposure of Canadian banks sit: in the bank, at its staff, or at its customers?

13 of 22

card-issuing banks with a current credential listing, the first item to triage

CHAPTER 09

Banking and finance deep dive

IN SHORT

Most visible exposure sits on the customer side: 116,660 non-employee device associations (most plausibly customers' devices), card-checker activity and account-trading channels. The bank- and staff-side signals are current listings at 13 of 22 issuers and 817 employee-classified devices. Three issuers carry most of the card signals. Triage each current listing first, then validate employee devices, and monitor checker declines on your BIN ranges (a BIN is the issuer's card-number prefix).

This chapter covers the 22 card-issuing banks and fintechs among the 33 banking-and-finance organisations in Chapter 3; the other 11 are regulators, payment networks, Crown lenders and investment firms. That is why 116,660 non-employee devices here differs from 134,120 there, and 817 employee devices from 1,681. Aggregates only; individual banks are not named.

13 of 22

issuers with a current credential listing (13 of the sector's 14 organisations with current listings)

14 of 33

banking and finance organisations with a current credential listing

22 of 22

issuers with non-employee device associations (116,660; ownership and current infection unverified)

19 of 22

issuers with employee-classified devices (817 in total)

29 of 33

banking and finance organisations enforcing DMARC

9 of 22

issuers on our list with cards in clear text in the posts we read (278 of the 374 cards; one more names an issuer outside the 22; narrow scope, §8.5)

The top three issuers account for 77% of the 278 cards attributed to issuers on our list and 47% of the non-employee device associations.

What it means for banks.

1. **Current listings come first.** 13 of 22 issuers had one on the day of the check; apply the 5-working-day disposition rule in §12.1.

2. **Employee exposure is small but real.** 817 employee-classified devices across 19 issuers are the intrusion-relevant subset. After current listings, these deserve priority validation over the much larger non-employee total.
3. **Non-employee device associations are the larger exposure.** 116,660 device associations across all 22 issuers are not employee-classified, and most plausibly they are customers' devices. Ownership, current infection and whether any stored session or password still works are unverified. Fraud teams should use device and session risk signals at login and at payee changes, not only password checks.
4. **Card checking is a detectable precursor.** Checker bots test cards with small authorisations or card-add attempts on merchant gateways. Issuers can detect clusters of declined low-value attempts on their BIN ranges, identify the cards involved, check their authorisation and fraud signals, and reissue the cards confirmed at risk under issuer policy.
5. **Mule accounts and onboarding are the downstream risk.** Account-trading posts sell aged accounts at named Canadian banks and fintechs and guides to pass remote identity checks (Chapter 8). They do not show that accounts were opened or used at the assessed banks. Onboarding controls should assume that name, birth date and address are known to criminals.
6. **Insiders are advertised.** Fraud menus claim bank insiders (B09). We cannot verify any claim, but access reviews for staff who can view or change customer data are a proportionate response. A 2026 court case involved a former branch employee who opened fraudulent accounts and viewed a public figure's banking data [S75].

KEY TAKEAWAYS

01

Current credential listings at 13 of 22 issuers come first, then the 817 employee-classified devices; the larger non-employee set also needs validation.

02

Banking and finance organisations enforce DMARC widely (29 of 33).

03

Card-checker declines on your BIN ranges and aged-account activity are detectable precursors.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

What changed in Canada's cyber rules in 2026, and what should an organisation have in place before the new duties apply?

72 h

the longest incident-reporting period the Critical Cyber Systems Protection Act allows

10.1 Laws and rules in force or in progress 69

10.2 Federal and provincial institutions 70

10.3 Which regime applies to you? 70

CHAPTER 10

Regulatory and national response

IN SHORT

2026 brought Canada's first federal cyber-security law for critical systems: Bill C-8 received royal assent on 15 June. Its duties for designated operators in telecom, energy, finance and transport will be phased in by regulation, with incident reports due within a period of at most 72 hours. Privacy reporting duties already apply. Map which regimes cover you, and name the person who reports incidents now.

10.1 Laws and rules in force or in progress

Measure	What we could verify	Status and caution
Bill C-8: Critical Cyber Systems Protection Act (CCSPA) and Telecommunications Act amendments	Passed the House of Commons on 26 March and the Senate on 4 June 2026; royal assent on 15 June 2026 (S.C. 2026, c. 9) [S44]. Designated operators in six vital services must report a cyber incident to CSE within a period set by regulation "not to exceed 72 hours" (section 17). Maximum administrative penalties are 500,000 CAD for an individual and 15 million CAD in other cases (section 91) [S44]	The Telecommunications Act security powers took effect at once; the CCSPA will be phased in, and the government gave no dates [S45]
Vital services under the CCSPA	Telecommunications; interprovincial or international pipelines and power lines; nuclear energy; federally regulated transportation; banking; clearing and settlement systems [S44]	Which operators are designated is set by regulation
Federal private-sector privacy law (PIPEDA)	Organisations must report a breach of security safeguards to the Privacy Commissioner "as soon as feasible" where it creates a real risk of significant harm (section 10.1) [S47]	In force; fines for offences up to 10,000 or 100,000 CAD (section 28) [S47]
Bill C-36: Protecting Privacy and Consumer Data Act	First reading on 15 June 2026; awaiting second-reading debate as of 21 November [S48]	Not law. As drafted, penalties up to the greater of 10 million CAD or 3% of gross global revenue, and fines for offences up to 25 million CAD or 5% [S48]
Quebec Law 25 (private sector)	An enterprise must promptly notify the Commission d'accès à l'information and the people affected when a confidentiality incident presents a risk of serious harm [S46]	In force. Administrative monetary penalties up to 10 million CAD or 2% of worldwide turnover; penal fines for an enterprise from 15,000 CAD up to the greater of 25 million CAD or 4%, doubled for a repeat offence [S46]

Measure	What we could verify	Status and caution
Ontario public sector (Bill 194)	The Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 received royal assent on 25 November 2024 (S.O. 2024, c. 24) [S49]	Sets cyber-security duties for Ontario public-sector entities; check which regulations apply to you
Federally regulated financial institutions (OSFI)	Guideline B-13 on technology and cyber risk management has applied since 1 January 2024 [S51]. OSFI's incident reporting advisory asks institutions to report a technology or cyber incident within 24 hours, or sooner if possible [S50]	In force
Payment service providers (Retail Payment Activities Act)	Risk-management and safeguarding frameworks required since 8 September 2025, supervised by the Bank of Canada [S52]	In force
Defence suppliers	Level 1 of the Canadian Program for Cyber Security Certification applies to select defence contracts from summer 2026 [S72]	First of three levels

10.2 Federal and provincial institutions

- **Quebec.** In November 2026 the government's page for the Ministère de la Cybersécurité et du Numérique said that its web content would be grouped with that of the Treasury Board secretariat [S53]. Organisations that report to it should confirm their contact points.
- **National anti-fraud strategy.** In March the federal Finance department opened consultations on a first national anti-fraud strategy, including a proposed framework that would introduce obligations for banks, telecoms and online platforms [S73].
- **Critical infrastructure.** In April the Cyber Centre launched an initiative to help critical-infrastructure operators prepare for severe cyber threats [S74].

10.3 Which regime applies to you?

The table reads the texts above for five common cases. It is a starting point, not legal advice.

Organisation	Main cyber and breach duties	Action now
Federally regulated bank or insurer	OSFI B-13 and 24-hour incident reporting; PIPEDA breach reporting; CCSPA if designated (banking, clearing and settlement)	Check that the OSFI, privacy and future CSE reports come from one incident record
Telecom operator	Telecommunications Act security powers in force; CCSPA if designated; PIPEDA	Prepare for orders under the amended act; name a CSE reporting contact
Pipeline, power line, nuclear or federal transport operator	CCSPA if designated; PIPEDA for personal data	Build a 72-hour reporting path now, before the regulations set the period
Private business in Quebec	Law 25 incident register and notification; PIPEDA where it applies	Keep the incident register current; rehearse a CAI notification
Ontario public-sector entity	Bill 194 duties; provincial privacy law	Confirm which regulations apply and who reports

What CISOs should do now. Map which of these regimes covers your organisation. Name the person who would report an incident to each regulator, and make sure one incident record can feed all of them. Keep dated evidence of the controls you implement, because CCSPA regulations are still to come. This section is not legal advice.

KEY TAKEAWAYS

01

Bill C-8 became law on 15 June 2026; incident reports under the new act will be due within a period of at most 72 hours.

02

Privacy breach duties already apply federally and in Quebec, where penal fines reach 25 million CAD or 4% of worldwide turnover.

03

Build one incident record that can feed CSE, OSFI and privacy regulators; regulations are still arriving.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

What should Canadian organisations plan for next, and what evidence would change that plan?

5

key judgements, each with a signal to watch

11.1 Key judgements 73

11.2 What would change the assessment 74

11.3 Conditional scenarios 74

CHAPTER 11

Outlook

IN SHORT

Plan for the same evidence types, not a new threat: steady ransomware and data extortion, identity-led theft through help desks and SaaS, a large identity-fraud market, and hacktivist interest in exposed control systems. State-linked espionage against research and universities continues in vendor reporting. We have no comparable time series for most of these, so change the plan when the signals below change, not on a calendar.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Ransomware and data extortion will remain the most visible criminal threat to Canadian organisations	High	Observed listings: 386 accepted listings in 2026 against 406 in 2025; listings are claims, and unpublished cases are invisible; signal: monthly accepted Canadian listings
Help-desk voice phishing and SaaS data theft will remain a leading route to confirmed breaches	Medium	The Cyber Centre's alert and several confirmed 2026 breaches; the actors behind them are not all the same; signal: Cyber Centre alerts and company disclosures naming help-desk resets
Identity exposure in the 250-organisation list is widespread enough to treat credential and device signals as routine triage	High for the list	Chapter 3 counts; not national prevalence; signal: share of current listings validated as active
If control systems stay reachable from the internet, plan for further hacktivist tampering claims at water, utility and industrial sites	Medium (planning assumption)	Three official October 2025 cases and a July 2026 municipal case; small sample; signal: Cyber Centre bulletins
If research, webmail and edge systems stay unpatched, plan for state-linked espionage attempts against universities and research bodies	Medium (planning assumption)	Three 2026 vendor reports naming Canadian universities, research servers or a human-rights body; signal: vendor advisories

11.2 What would change the assessment

Current interpretation	Evidence that would change it	Decision affected
Canadian listings are steady through the year	A sustained monthly rise in accepted Canadian listings, or a large campaign by one group	Raise restore-test frequency; review supplier access
Telecom, insurer and hospital dataset offers are unverified	A sample matched to a specific system's schema, or an official confirmation	Trigger notification and customer-protection actions for that dataset
Help-desk vishing is concentrated in legal and finance	A Cyber Centre or company report of the same method in another sector	Extend call-back verification and SaaS download alerting to that sector
Hacktivist OT incidents have had minor impact so far	An official report of a sustained outage or a safety event at a Canadian control system	Fund OT segmentation and remote-access controls ahead of other projects
Current credential listings mean "validate", not "breached"	Validation shows active accounts without MFA among listed credentials	Escalate to incident response and enforce MFA for the affected population

11.3 Conditional scenarios

- **If** an international event or a Canadian policy statement draws hostile attention, **then** plan for hacktivist DDoS and control-system tampering claims (a planning assumption); **signal:** Cyber Centre bulletins and actor target lists. **Decision:** check that no control system is reachable from the internet, and activate the pre-agreed communication line.
- **If** a new critical edge or webmail vulnerability is disclosed, **then** plan for criminal and state-linked exploitation attempts; **signal:** vendor advisories and Cyber Centre alerts. **Decision:** patch and verify within your deadline for internet-facing systems, then hunt for web shells.
- **If** your help desk receives unusual MFA-reset requests, **then** plan for a voice-phishing attempt; **signal:** reset requests from new numbers or outside hours. **Decision:** apply call-back verification and review recent SaaS downloads.

KEY TAKEAWAYS

01

Plan for evidence types, not a new threat: extortion, identity-led theft, identity fraud and exposed control systems.

02

Each judgement has a signal; change the plan when the signal changes.

03

No comparable time series exists yet to say whether most of these are growing.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should each team do in the next 90 days, and how will the board know it was done?

20

actions with an owner and completion evidence

12.1 30/60/90 days 76

12.2 By role 79

12.3 How Brandefense can help 80

CHAPTER 12

Action plan

IN SHORT

Start by confirming you receive credential-listing and infected-device alerts, then lock down the help desk and identity recovery, the disclosed route behind several of 2026's confirmed breaches. Then validate listings and employee devices, close remote-access and control-system exposure, and rehearse your response to extortion and regulator reporting. The board knows the work is done from each row's completion evidence and the scorecard below; report both by day 90.

12.1 30/60/90 days

This is a sequence, not a waiting period. A current material threat should enter your incident process immediately.

1Days 1-30

Confirm that you receive credential-listing and infected-device alerts for your primary domains; if not, arrange them, and record the listing and device rows below as blocked until alerts arrive

OWNER

CISO and threat intelligence

COMPLETION EVIDENCE

Alert source named; first alert received

Require call-back verification to a known number before any password or MFA reset by the help desk, including calls that claim to come from internal IT (§7.3)

OWNER

Service desk and identity team

COMPLETION EVIDENCE

Procedure signed off; one simulated vishing call caught

For every current credential listing tied to your domains, validate the account and its MFA status within 5 working days

OWNER

Identity team

COMPLETION EVIDENCE

Each listing has a disposition: reset, already remediated, or not ours, with a date

Validate employee-classified device associations; revoke sessions and tokens where active

OWNER

Identity and endpoint teams

COMPLETION EVIDENCE

Device list reconciled with asset inventory; revocations logged

Put remote-desktop web gateways, VPNs and webmail behind MFA now and start phishing-resistant MFA for privileged users; patch internet-facing edge systems whenever a Cyber Centre alert names a product you run

OWNER	COMPLETION EVIDENCE
Infrastructure	External re-test passes; exceptions dated

Name the person who reports incidents to each regulator (CSE once designated, OSFI, the Privacy Commissioner, the CAI) and agree one incident record (§10.3)

OWNER	COMPLETION EVIDENCE
CISO and legal	A one-page reporting map, approved

2Days 31-60

Alert on bulk downloads and new API applications in Microsoft 365 and other SaaS tenants

OWNER	COMPLETION EVIDENCE
SOC and SaaS owners	Alert live and tested

Move privileged and remote users first, then others, to phishing-resistant MFA (FIDO2 security keys, passkeys or certificate-based sign-in)

OWNER	COMPLETION EVIDENCE
Identity team	Coverage recorded per user group

Remove control systems from direct internet exposure; put remote access behind a jump host with MFA; change default passwords (§6.4)

OWNER	COMPLETION EVIDENCE
OT and engineering	External exposure check shows no control interface; remote-access log reviewed

Where DMARC is p=none, missing or invalid, inventory senders and stage enforcement

OWNER	COMPLETION EVIDENCE
Messaging	Aligned senders; p=quarantine with a rollback route

Test account-recovery, SIM-swap and payee-change processes against an attacker who knows name, address, phone and birth date

OWNER	COMPLETION EVIDENCE
Fraud and customer operations	Weaknesses recorded and fixed, retest passed

Require out-of-band confirmation for payment-instruction and payroll-deposit changes (§8.4)

OWNER
Finance and HR

COMPLETION EVIDENCE
Procedure signed off; one simulated request caught

Banks: alert on clustered card-checker declines on your BIN ranges, and on new e-transfer recipients for aged accounts

OWNER
Fraud

COMPLETION EVIDENCE
Alert live; first review recorded

List suppliers that hold your customer or case data in cloud platforms; confirm their MFA, logging and breach notice terms

OWNER
Procurement and third-party risk

COMPLETION EVIDENCE
Supplier list with dated confirmations

Run a timed restore test of one crown-jewel system

OWNER
Infrastructure

COMPLETION EVIDENCE
Restore time recorded against the recovery time objective (RTO: the longest outage your business-continuity plan allows)

3Days 61-90

Sign DNS for primary domains where your registrar supports it; fix invalid TLS certificates and add HSTS

OWNER
Network and web teams

COMPLETION EVIDENCE
DNSSEC validation succeeds from an external resolver; certificate checks pass

Run a tabletop on data extortion: stolen files published, no encryption, regulator clocks running

OWNER
CISO, communications, legal

COMPLETION EVIDENCE
Decision log and timings, including each regulator's deadline

Prepare customer and patient notices for an unverified leak claim, separating claim, verified fact and action

OWNER
Communications and privacy

COMPLETION EVIDENCE
Approved templates

Review loyalty and customer-portal accounts for credential stuffing; offer or require MFA

OWNER
Digital and fraud teams

COMPLETION EVIDENCE
Takeover rate measured before and after

Report the scorecard against targets (below)

OWNER	COMPLETION EVIDENCE
CISO to board	Board paper with remaining gaps and owners

Scorecard targets. These are suggested defaults; set your own where policy differs.

Measure	Target
Help-desk resets with call-back verification	100% by day 30
Current listings with a disposition within 5 working days	100% by day 90
Employee-classified devices reconciled with the asset inventory	100% by day 90
Remote-access gateways and webmail behind phishing-resistant MFA	100%, or a dated plan, by day 90
Control systems reachable from the internet	Zero, or a dated plan, by day 90
Primary domains with DMARC at quarantine or reject	100%, or a dated plan, by day 90
Payment and payroll changes confirmed out of band	100% by day 90
Restore test within RTO	Passed, or a dated fix, by day 90

12.2 By role

Role	First decision
Board	Ask how the help desk verifies a caller before resetting MFA, and for the current-listing and employee-device numbers with a date by which each is validated
CISO	Put listing and device monitoring in place, then fund phishing-resistant MFA for remote and privileged users
SOC	Add detections for sign-ins right after a help-desk reset, bulk SaaS downloads, new OAuth applications and sign-ins from hosting networks
Fraud	Use device and session risk at login, payee and payroll changes; watch checker declines and aged-account activity
Communications and legal	Prepare statements for unverified leak claims and a reporting map for every regulator that applies

KEY TAKEAWAYS

01

In the first 30 days, confirm monitoring and put call-back verification on every help-desk reset.

02

By day 60, extend phishing-resistant MFA, alert on SaaS bulk downloads and remove control systems from the internet.

03

By day 90, rehearse data extortion with regulator deadlines and report the scorecard to the board.

12.3 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The analysis in this report used the same data and scoring that the platform applies to monitored organisations: infected-device and credential associations, current credential-market listings, lookalike domains, exposed documents and dark-web mentions. It does not promise that every claim can be verified or that a historical record remains usable.

Bring your domains, brands and security priorities to a 30-45 minute demo with Sales and Presales. The team can show how platform monitoring relates external signals to the assets you manage. A Brandefense team member or a partner in your region will follow up.

Request a demo

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Method · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

81
sources

Appendix A. Method 82
Appendix B. Evidence register 85
Appendix C. Sources 86
Appendix D. Glossary 91

Appendix A. Method

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Window, sources and priority

The research window is 1 January-18 November 2026 by the date a post was published, not the date it was collected. Own data comes first: Brandefense Blackhole (dark-web and messaging posts, infected-device and credential associations, card material in posts), Ransompedia (ransomware leak-site listings) and Brandefense Atlas exposure ratings. External sources give context and are cited only after the supporting passage was read. Data were extracted on 21 November 2026. Sources S1-S8 are Brandefense's own data or a public tracker used as a cross-check. External entries in Appendix C give the full URL (or the publisher's site root where the article URL is withheld under Appendix A.9) and the date verified.

A.2 Blackhole posts

Item	Value
Posts with the Canada country tag	696,200 counted
Tagged posts read	43,549, a sample across the year
Forum posts with the tag	1,449 counted; 1,438 read
Other posts read	Posts about Canadian brands and places
Relevant posts in the posts read (headline measure)	12,124-12,656 (12,124 strictly relevant plus 532 borderline posts)
Modelled full-tag range in Charts c01-c02 (indicative only)	93,500-99,400 (rounded from the monthly sum of 93,530-99,350)

Relevant posts are crime-relevant posts; spam and other non-crime content are not counted. This report uses the directly read count of 12,124-12,656 relevant posts in the 43,549 tagged posts read as its headline measure. Forum posts were read almost in full (1,438 of 1,449, or 99.2%), while Telegram, Discord and paste posts were sampled across all 11 months (42,111 of 694,751, or 6.1%). Across the year, the read sample covered 17,579 of 148,881 English tagged posts (11.8%, of which 9,096 were relevant) and 7,543 of 366,561 Turkish tagged posts (2.1%, of which 188 were relevant).

Charts c01 and c02 also plot an indicative full-tag projection summing to 93,530-99,350 across the 11 monthly rows of Chart c01 (rounded to 93,500-99,400). Those monthly rows correspond to effective relevance shares of 5.4%-5.7% in January, 8.8%-9.9% in February, 9.9%-10.2% in May and 9.3%-10.9% in June, and 22.1%-60.6% in March-April and July-November. Because monthly sample sizes and internal stratum weights are withheld and sampling was purposive, the 93,500-99,400 projection cannot be reproduced from public totals and is not a headline finding.

Collection volume shapes every trend in this report. Tagged volume for the comparison countries also moves sharply between months, so we do not read Canadian month-to-month changes, or changes in the mix of crime families, as threat trends.

A.3 The 250 organisations

Selection, verification and limits are in §3.1. For each primary domain we read the exposure signals that Atlas uses for its ratings. They are infected devices, employee devices, credential records, dark-chat and dark-web mentions, new lookalike domains, documents that reference the domain, current credential-market listings, and prior credential-market listings ("sale history", recorded before the current check). Data were read on 21 November 2026.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating from these signals, and the 250 organisations a national headline rating. Treat a current credential-market listing as a reason to validate accounts, not as proof of a breach. Lookalike-domain counts are noisier for brands with generic or very common names.

A.5 DNS, TLS and web checks

Results cover published mail, SPF, DMARC, DKIM, DNSSEC and CAA settings, TLS certificates and homepage headers for each primary domain. Missing, invalid and monitoring-only (p=none) DMARC policies count as no enforcement. All results are passive.

Hygiene index values summarise these email, DNS, TLS and header results by sector on a scale of 0-100; a higher value means weaker hygiene. They are an Odin analytical index, not a rating, and not part of Atlas.

A.6 Card material in posts

Scope: only payment cards that appeared in clear text in the dark-web posts read for this report. Brandefense detects stolen cards through many other methods, which are outside this report. These figures do not measure card theft or fraud loss.

A.7 Ransomware

We used Ransompedia accepted listings for Canada, the United States, the United Kingdom and Australia, all dates, dated by publication. A public tracker and relayed Blackhole posts are used only as cross-checks.

A.8 Incident coverage

Incident coverage combines Blackhole posts about the 250 organisations and about specific data-leak, access or exploit events with public reporting for the window in English and French.

Public sources include the Canadian Centre for Cyber Security and releases of CSE, the RCMP, the Canadian Anti-Fraud Centre, Public Safety and OSFI. They also include the federal and provincial privacy commissioners, provincial governments, police and municipalities, national English- and French-language press, and vendor research.

Remaining coverage limits. Our view is still partial:

- Tor ransomware leak sites are covered only through Ransompedia.
- Telegram coverage is partial, so a single Canada-specific post can be missed.
- Closed and invite-only forums, private Telegram groups and sales arranged in direct messages are outside our collection.
- Several French-language news sites and some official pages could not be retrieved for checking, so their articles are not used.
- Incidents that organisations handle without disclosure stay invisible.

That an incident is absent from this report does not mean it did not happen.

A.9 Confidence and boundaries

High confidence applies to a reproducible measurement, not to a criminal's underlying assertion. Medium indicates an interpretation with a clear supporting line and stated limits. "Unverified" means not independently established; it is neither proof of fabrication nor proof of a breach. Victim organisations are described by role; an organisation is named only where it or an authority confirmed the incident and the incident was widely reported. Actor aliases are printed; links, contacts, indicators and personal data are withheld. Full provenance is held in an internal evidence register.

Appendix B. Evidence register

Every post quoted in this report appears as a redacted post card in the chapter shown. Excerpts are short; omissions are marked [...]; identifiers, contacts, links and victim organisations are replaced with labels in brackets, under the policy in A.9. Posting dates are not intrusion dates. Post identifiers, links and full text are held in an internal evidence register.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-03-21	Breach forum	Murad	English	§4.4
B02	2026-04-25	Breach forum	Murad	English	§4.4
B03	2026-04-29	Breach forum	GlitchX	English	§4.4
B04	2026-11-09	Breach forum	DataJava	English	§4.5
B05	2026-03-17	Telegram group	Anonymous poster	English	§4.5
B06	2026-05-13	Breach forum	XOverStm	English	§4.5
B07	2026-01-09	Breach forum	phoenix_leads	English	§4.4
B08	2026-01-23	Breach forum	hulky	English	§4.4
B09	2026-01-01	Telegram channel	Fraud-services vendor	English	§8.3
B10	2026-05-13	Telegram channel	Calciumpound	English	§8.2
B11	2026-05-05	Telegram group	bigbosskyc1	English	§8.3
B12	2026-09-14	Telegram group	Fraud-services vendor	English	§8.3
B13	2026-11-14	Breach forum	scarlettgroup	English	§4.4
B14	2026-06-16	Fraud forum	theghostorder01	English	§8.4
B15	2026-05-08	Breach forum	MDGhost	English	§4.4
B16	2026-03-17	Telegram channel	Loyalty-account shop	English	§8.4

Appendix C. Sources

S1: Brandefense Blackhole post corpus, Canada country tag and posts about Canadian brands and places, post dates 1 January–18 November 2026, extracted 21 November 2026.

S2: Brandefense Blackhole forum and market posts cited in the case studies, 1 January–18 November 2026.

S3: Brandefense Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, read 21 November 2026.

S4: Brandefense Atlas exposure ratings for the 250 domains, 21 November 2026, including credential-market listings, lookalike domains, exposed documents and mention statistics.

S5: Brandefense public DNS, TLS and homepage checks of the 250 domains, 21 November 2026.

S6: Brandefense Ransompedia, accepted listings for Canada, the United States, the United Kingdom and Australia, all dates, extracted 21 November 2026.

S7: ransomware.live, country victims for Canada, accessed 21 November 2026 (cross-check only). https://www.ransomware.live/ (article URL withheld). Verified on 21 November 2026.

S8: Brandefense Blackhole, Canada-associated cards seen in clear text in dark-web posts, 21 November 2026.

S9: DataReportal (Kepios), Digital 2027: Canada, 4 November 2026 (data for October 2026). https://datareportal.com/reports/digital-2027-canada. Verified on 21 November 2026.

S10: Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025–2026. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026. Verified on 21 November 2026.

S11: Communications Security Establishment, Annual Report 2025–2026, 29 June 2026. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2025-2026. Verified on 21 November 2026.

S12: Canadian Centre for Cyber Security, Ransomware Threat Outlook 2025–2027. https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027. Verified on 21 November 2026.

S13: Canadian Anti-Fraud Centre, "Fraud Prevention Month 2026" (top frauds of 2025). https://antifraudcentre-centreantifraude.ca/features-vedette/2026/02/month-prevention-mois-eng.htm. Verified on 21 November 2026.

S14: Office of the Privacy Commissioner of Canada, annual report news release, 4 June 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260604/. Verified on 21 November 2026.

S15: Canadian Centre for Cyber Security, "AL26-028 Ongoing Help Desk Voice Phishing Campaign Targeting Canadian Organizations", 28 October 2026. https://www.cyber.gc.ca/en/alerts-advisories/al26-028-ongoing-help-desk-voice-phishing-campaign-targeting-canadian-organizations. Verified on 21 November 2026.

S16: The Globe and Mail, reporting on breaches at Toronto law firms, 29–31 October 2026. https://www.theglobeandmail.com/ (article URL withheld). Verified on 21 November 2026.

S17: Canadian Centre for Cyber Security, "Cyber threat bulletin: Non-state activity targeting Canadian operational technology", 28 July 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-non-state-activity-targeting-canadian-operational-technology. Verified on 21 November 2026.

S18: Canadian Centre for Cyber Security, "Cyber threat bulletin: Iranian Cyber Threat Response to US/Israel strikes, February 2026", 1 March 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026. Verified on 21 November 2026.

S19: Canadian Centre for Cyber Security, "Cyber threat bulletin: FIFA World Cup 2026", 29 May 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-fifa-world-cup-2026tm. Verified on 21 November 2026.

S20: Communications Security Establishment, call to strengthen defences on the fourth anniversary of Russia's invasion of Ukraine, 19 February 2026. https://www.cyber.gc.ca/en/news-events/cse-calls-canadian-organizations-critical-infrastructure-providers-strengthen-defences-fourth-anniversary-russias-invasion-ukraine. Verified on 21 November 2026.

S21: Le Soleil, "Une cyberattaque russe frappe une station d'eau potable au Bas-Saint-Laurent", 31 July 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/. Verified on 21 November 2026.

S22: Office of the Privacy Commissioner of Canada, "Loblaw commits to strengthening security measures following privacy breach", 26 October 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_261026/. Verified on 21 November 2026.

S23: BleepingComputer, "Telus Digital confirms breach after hacker claims 1 petabyte data theft", March 2026. https://www.bleepingcomputer.com/news/security/telus-digital-confirms-breach-after-hacker-claims-1-petabyte-data-theft/. Verified on 21 November 2026.

S24: CTV News, "Cybersecurity incident at Canada Life reportedly impacts thousands", April 2026. https://www.ctvnews.ca/canada/article/cybersecurity-incident-at-canada-life-reportedly-impacts-thousands/. Verified on 21 November 2026.

S25: Global News, reporting on the Canvas breach at Canadian universities, May 2026. https://globalnews.ca/news/11840444/canadian-universities-data-leak/. Verified on 21 November 2026.

S26: Office of the Privacy Commissioner of Canada, special report on breaches at the Canada Revenue Agency, 7 May 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260507/. Verified on 21 November 2026.

S27: CTV News, "Ransomware attack hits facility systems at Manitoba's largest hospital", August 2026. https://www.ctvnews.ca/winnipeg/article/ransomware-attack-hits-facility-systems-at-manitobas-largest-hospital/. Verified on 21 November 2026.

S28: CTV News, reporting on a British Columbia school district cyberattack, September–October 2026. https://www.ctvnews.ca/ (article URL withheld). Verified on 21 November 2026.

S29: Office of the Privacy Commissioner of Canada, "Privacy Commissioner of Canada to investigate data breach involving Crime Stoppers", 27 October 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_261027/. Verified on 21 November 2026.

S30: Office of the Privacy Commissioner of Canada, investigation into a data breach involving stolen identification details, 21 September 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260921/. Verified on 21 November 2026.

S31: Office of the Information and Privacy Commissioner of Alberta, statement on the unauthorized distribution of the list of electors, 2026. https://oipc.ab.ca/information-and-privacy-commissioner-of-alberta-issues-statement-regarding-unauthorized-distribution-of-list-of-electors/. Verified on 21 November 2026.

S32: MTL Blog, "Hydro-Québec cyber scare: Over 1.5 million Quebecers are asked to change their passwords now", 19 November 2026, quoting a Hydro-Québec spokesperson. https://www.mtlblog.com/hydro-quebec-cyber-password-hack. Also CTV News, "Nearly 2 million Hydro-Québec customers urged to change their passwords", 18 November 2026. https://www.ctvnews.ca/montreal/article/nearly-2-million-hydro-quebec-customers-urged-to-change-their-passwords/. Verified on 21 November 2026.

S33: BleepingComputer, reporting on a Canadian telecom provider's statement on stolen enterprise customer data, 20 November 2026. https://www.bleepingcomputer.com/ (article URL withheld). Verified on 21 November 2026.

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

S35: Google Threat Intelligence Group, "PRC targets US medical research", 15 June 2026. https://cloud.google.com/blog/topics/threat-intelligence/prc-targets-us-medical-research. Verified on 21 November 2026.

S36: Proofpoint, "One email closer to the edge: UNK_MassTraction", 7 July 2026. https://www.proofpoint.com/us/blog/threat-insight/one-email-closer-edge-unkmasstraction-physics-exploitation. Verified on 21 November 2026.

S37: Palo Alto Networks Unit 42, Cairn framework and autonomous AI attacks, 12 November 2026. https://unit42.paloaltonetworks.com/cairn-framework-ai-autonomous-attacks/. Verified on 21 November 2026.

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

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

S41: RCMP, "Operation Endgame: RCMP join international partners in crackdown of Russian cybercriminal network", 18 June 2026. https://rcmp.ca/en/news/2026/06/4354276. Verified on 21 November 2026.

S42: RCMP, "Maple Disruption 2.0", November 2026. https://rcmp.ca/en/news/2026/11/4358530. Verified on 21 November 2026.

S43: Global News, Toronto Police SMS blaster arrests, 23 April 2026. https://globalnews.ca/news/11813885/toronto-police-arrest-cyber-attack/. Verified on 21 November 2026.

S44: Parliament of Canada, LEGISinfo, Bill C-8 (45th Parliament, 1st session), and the royal assent text. https://www.parl.ca/legisinfo/en/bill/45-1/c-8 and https://www.parl.ca/DocumentViewer/en/45-1/bill/C-8/royal-assent. Verified on 21 November 2026.

S45: Public Safety Canada, "Government of Canada Strengthens Cyber Security and Critical Infrastructure with Royal Assent of Bill C-8", 16 June 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. Verified on 21 November 2026.

S46: Commission d'accès à l'information du Québec, pages on confidentiality incidents and on sanctions and prosecutions for enterprises. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises and https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/sanctions-entreprises-poursuites. Verified on 21 November 2026.

S47: Justice Canada, Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), full text. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html. Verified on 21 November 2026.

S48: Parliament of Canada, LEGISinfo, Bill C-36 (45th Parliament, 1st session), and first-reading text. https://www.parl.ca/legisinfo/en/bill/45-1/c-36 and https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading. Verified on 21 November 2026.

S49: Government of 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. Verified on 21 November 2026.

S50: OSFI, Technology and Cyber Security Incident Reporting advisory. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-security-incident-reporting. Verified on 21 November 2026.

S51: OSFI, final Guideline B-13 Technology and Cyber Risk Management (letter, 13 July 2022; effective 1 January 2024). https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfi-releases-final-guideline-b-13-technology-cyber-risk-management-letter-2022. Also OSFI news release, "OSFI releases new guideline for technology and cyber risk, balancing innovation with risk management", 13 July 2022. https://www.osfi-bsif.gc.ca/en/news/osfi-releases-new-guideline-technology-cyber-risk-balancing-innovation-risk-management. Verified on 21 November 2026.

S52: Bank of Canada, retail payments supervision. https://www.bankofcanada.ca/core-functions/retail-payments-supervision/. Verified on 21 November 2026.

S53: Gouvernement du Québec, page of the Ministère de la Cybersécurité et du Numérique. https://www.quebec.ca/gouvernement/ministere/cybersecurite-numerique. Verified on 21 November 2026.

S54: BleepingComputer, "Canada Goose investigating as hackers leak 600K customer records", February 2026. https://www.bleepingcomputer.com/news/security/canada-goose-investigating-as-hackers-leak-600k-customer-records/. Verified on 21 November 2026.

S55: NIST National Vulnerability Database, records for CVE-2024-42009, CVE-2025-49113, CVE-2026-1731, CVE-2026-1281 and 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 and https://nvd.nist.gov/vuln/detail/CVE-2026-1340. Ivanti's interim patches and planned fixed release (12.8.0.0) as relayed by CERT-EU, Security Advisory 2026-001, 30 January 2026. https://cert.europa.eu/publications/security-advisories/2026-001/. Verified on 21 November 2026.

S56: Canadian Centre for Cyber Security, "Cyber threat actors use artificial intelligence in an active global campaign to disrupt internet-exposed programmable logic controllers", 8 September 2026. https://www.cyber.gc.ca/en/news-events/cyber-threat-actors-use-artificial-intelligence-active-global-campaign-disrupt-internet-exposed-programmable-logic-controllers. Verified on 21 November 2026.

S57: Canadian Centre for Cyber Security, "The cyber threat to aviation", 19 October 2026. https://www.cyber.gc.ca/en/guidance/cyber-threat-aviation. Verified on 21 November 2026.

S58: Canadian Centre for Cyber Security, "The Cyber Centre urges heightened vigilance amid global tensions and high-profile events", 4 September 2026. https://www.cyber.gc.ca/en/news-events/cyber-centre-urges-heightened-vigilance-amid-global-tensions-high-profile-events. Verified on 21 November 2026.

S59: Canadian Centre for Cyber Security, "Cyber Centre warns of sophisticated smishing activity targeting Canadians", 2026 (page dated 24 April 2026). https://www.cyber.gc.ca/en/news-events/cyber-centre-warns-sophisticated-smishing-activity-targeting-canadians. Verified on 21 November 2026.

S60: Office of the Privacy Commissioner of Canada, "WestJet commits to improving security measures following a data breach", 14 July 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260714/. Verified on 21 November 2026.

S61: Office of the Privacy Commissioner of Canada, "Nova Scotia Power commits to strengthening security measures", 25 March 2026. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260325/. Verified on 21 November 2026.

S62: CTV News, reporting on a Calgary university cyberattack, June–July 2026. https://www.ctvnews.ca/ (article URL withheld). Verified on 21 November 2026.

S63: CTV News, reporting on a Toronto university data theft, November 2026. https://www.ctvnews.ca/ (article URL withheld). Verified on 21 November 2026.

S64: BNN Bloomberg (The Canadian Press), reporting on a Canadian financial-industry body's breach update, 14 January 2026. https://www.bnnbloomberg.ca/ (article URL withheld). Verified on 21 November 2026.

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

S66: Palo Alto Networks Unit 42, BeyondTrust CVE-2026-1731 activity, February 2026. https://unit42.paloaltonetworks.com/beyondtrust-cve-2026-1731/. Verified on 21 November 2026.

S67: Palo Alto Networks Unit 42, Ivanti EPMM CVE-2026-1281 and CVE-2026-1340 activity, February 2026. https://unit42.paloaltonetworks.com/ivanti-cve-2026-1281-cve-2026-1340/. Verified on 21 November 2026.

S68: CTV News, reporting on a Winnipeg university cyberattack, October 2026. https://www.ctvnews.ca/ (article URL withheld). Verified on 21 November 2026.

S69: Canadian Centre for Cyber Security and partners, "Joint advisory on Russian GRU exploiting vulnerable routers to steal sensitive information", 2 April 2026. https://www.cyber.gc.ca/en/news-events/joint-advisory-russian-gru-exploiting-vulnerable-routers-steal-sensitive-information. Verified on 21 November 2026.

S70: Canadian Centre for Cyber Security and partners, "Joint cyber security advisory on Russian state-sponsored phishing campaign targeting Zimbra webmail", 22 July 2026 (page dated 23 July 2026). https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-russian-state-sponsored-phishing-campaign-targeting-zimbra-webmail. Verified on 21 November 2026.

S71: Canadian Anti-Fraud Centre, "Canadian Anti-Fraud Centre supported Operation FRONTIER+III", 4 June 2026. https://antifraudcentre-centreantifraude.ca/news-nouvelles/2026/2026-06-04-eng.htm. Verified on 21 November 2026.

S72: Public Services and Procurement Canada, "Government of Canada introduces Level 1 of Canadian Program for Cyber Security Certification", 14 April 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. Verified on 21 November 2026.

S73: Department of Finance Canada, "Government of Canada launches consultations on first ever National Anti-Fraud Strategy", March 2026. https://www.canada.ca/en/department-finance/news/2026/03/government-of-canada-launches-consultations-on-first-ever-national-anti-fraud-strategy.html. Verified on 21 November 2026.

S74: Communications Security Establishment, "Cyber Centre launches new initiative to help Canada's critical infrastructure prepare for severe cyber threats", 17 April 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. Verified on 21 November 2026.

S75: CP24 (The Canadian Press), reporting on the sentencing hearing of a former bank employee, 18 November 2026 (guilty plea August 2026). https://www.cp24.com/ (article URL withheld). Verified on 21 November 2026.

S76: BleepingComputer, reporting on a Toronto children's hospital data breach, August 2026. https://www.bleepingcomputer.com/ (article URL withheld). Verified on 21 November 2026.

S77: Global News, reporting on a home-care supplier's 2025 ransomware attack, March 2026. https://globalnews.ca/ (article URL withheld). Verified on 21 November 2026.

S78: BleepingComputer, "US and Canada arrest and charge suspected Kimwolf botnet admin", May 2026. https://www.bleepingcomputer.com/news/security/us-and-canada-arrest-and-charge-suspected-kimwolf-botnet-admin/. Verified on 21 November 2026.

S79: Canadian Anti-Fraud Centre and Competition Bureau, "Fraud Prevention Month to bring hidden crime into the spotlight", 6 March 2026. https://antifraudcentre-centreantifraude.ca/news-nouvelles/2026/2026-03-06-eng.htm. Verified on 21 November 2026.

S80: Statistics Canada, "Impact of cybercrime on Canadian businesses, 2025", 21 October 2026. https://www150.statcan.gc.ca/n1/daily-quotidien/261021/dq261021b-eng.htm. Also Statistics Canada, "StatCan Plus weekly review: October 19 to 23, 2026", 23 October 2026. https://www.statcan.gc.ca/o1/en/plus/9368-weekly-review-october-19-23-2026. Verified on 23 November 2026.

S81: Communications Security Establishment, Annual Report 2024-2025, 27 June 2025. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2024-2025. Verified on 23 November 2026.

Appendix D. Glossary

- **Blackhole:** Brandefense's cybercrime data source covering posts, infected devices, credentials and card material.
- **Ransompedia:** Brandefense's ransomware database; listings record criminal claims.
- **Atlas:** Brandefense's external exposure scoring; scores run from 0 (nothing observed) to 100.
- **Infected device:** a device whose stealer log contains a login to the organisation's domain; "employee" is a Brandefense classification, not verified employment.
- **Credential-market listing:** a credential tied to the domain offered on a monitored market at the time of the check. In the sector heatmap, "sale history" counts prior listings recorded before the current check.
- **Combolist:** a list of login and password pairs assembled from various sources; age and validity vary.
- **Stealer log:** data captured by information-stealing malware from a device.
- **Checker bot:** a bot that tests stolen cards against payment gateways and prints the result.
- **Post card:** a redacted reproduction of one dark-web post, with venue, date, alias, language and what it does and does not establish.
- **Voice phishing (vishing):** a phone call in which the caller poses as a trusted person, such as IT support, to obtain access.
- **SaaS:** software as a service, such as Microsoft 365 or a hosted CRM, where an organisation's data sits in the provider's cloud.
- **Drops and mule accounts:** people, and accounts opened in their names, used to receive and move fraud proceeds.
- **Creation:** underground term for a synthetic or borrowed identity used to open accounts.
- **KYC:** "know your customer" identity checks at banks, exchanges and other services.
- **AiTM (adversary-in-the-middle):** a phishing page that relays a real login and captures passwords, one-time codes and the session cookie.
- **Phishing-resistant MFA:** sign-in tied to the real site (FIDO2 security keys, passkeys or certificates), so a relay page cannot reuse it.
- **MFA (multi-factor authentication):** a sign-in that needs a second factor beyond the password.
- **OT / PLC:** operational technology, and the programmable logic controllers that run physical processes.
- **BIN:** the issuer's card-number prefix (bank identification number).
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC and DS record:** signatures that let resolvers verify DNS answers, and the parent-zone record that links a domain to its keys.
- **HSTS:** a web header telling browsers to use HTTPS only.
- **p=none:** a DMARC policy that only monitors and does not ask receivers to reject or quarantine.

- **Headline score:** the national Atlas figure for the 250 organisations, on the Atlas 0-100 scale (0 = no risk observed, 100 = highest).
- **Hygiene index:** Odin analytical index values summarising email, DNS, TLS and header results by sector; 0-100, higher means weaker; not a rating.
- **Designated operator:** under the Critical Cyber Systems Protection Act, an operator in a vital service named by regulation, which then carries the act's duties.
- **RTO:** recovery time objective, the longest outage a business-continuity plan allows.
- **SMS blaster:** a portable fake cell tower that pushes text messages to nearby phones.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 21 November 2026.

Research cut-off: 18 November 2026 (primary data window). Public reporting was read through 21 November 2026; items published after the cut-off are included only where they describe events before it, and are marked. The report prioritises Brandefense's own data, keeps criminal claims separate from independently established incidents and does not claim a complete census of cybercrime affecting Canada. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. A Canadian French edition accompanies this report.

© 2026 Brandefense. All rights reserved.

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