Pivoting From PayTool: Tracking Various Frauds and E-Crime Targeting Canada

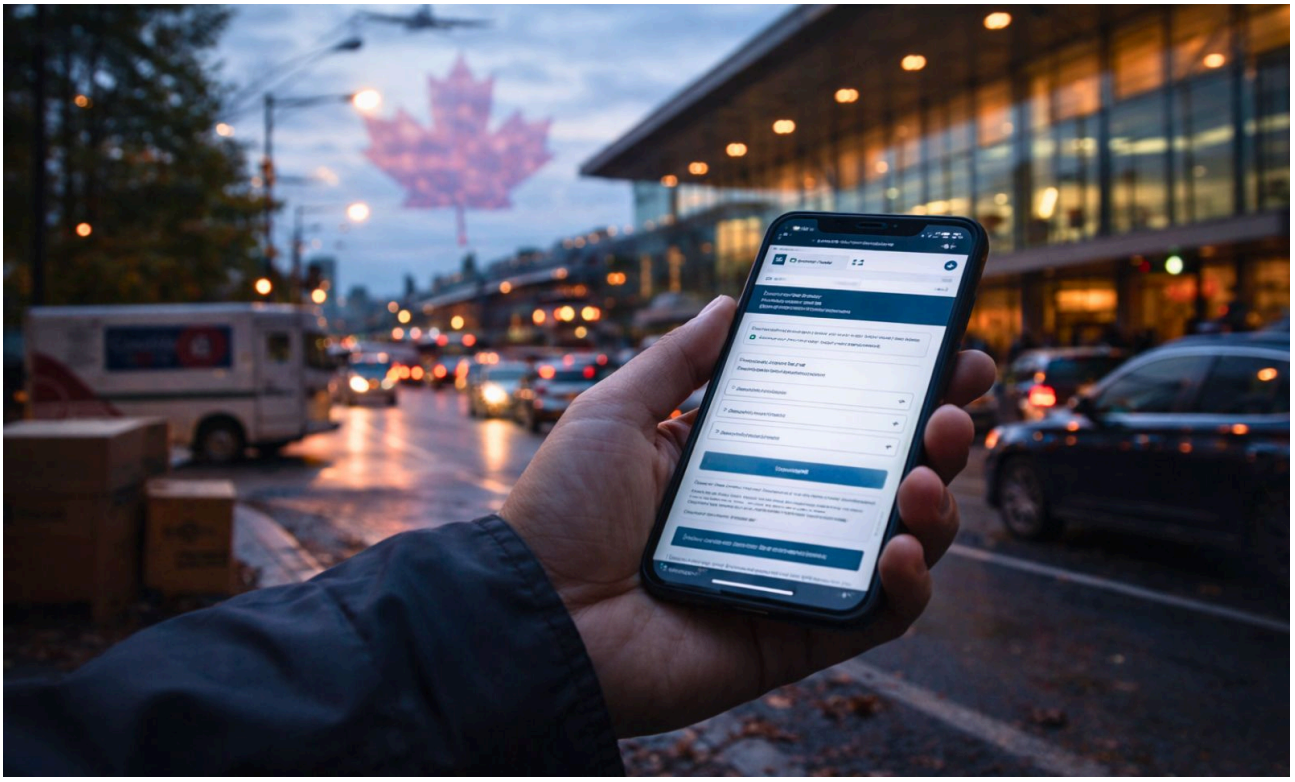
By Jainam Shah

Published: 2026-01-28 · Archived: 2026-04-02 12:25:31 UTC

Back

CloudSEK’s latest investigation exposes a rapidly evolving fraud ecosystem targeting Canadians through highly convincing impersonation of government services and trusted national brands. From fake traffic fines and tax refunds to airline bookings and parcel delivery alerts, attackers are scaling operations using shared infrastructure and phishing-as-a-service models. The report reveals how urgency and institutional trust are weaponized—and what organizations must do to stay ahead.

January 27, 2026



Executive Summary

As Canadian citizens increasingly rely on digital services for transportation, taxation, parcel delivery, and travel, threat actors continue to exploit this dependency by deploying highly convincing impersonation campaigns that mimic trusted government bodies and national brands. CloudSEK discovered multiple interconnected fraud clusters that abuse traffic ticket enforcement themes, tax refund narratives, airline booking portals, and postal delivery alerts to harvest personal and financial information at scale.

A significant portion of the activity is aligned with the "PayTool" phishing ecosystem, a known fraud framework that specializes in traffic violation and fine payment scams targeting Canadians through SMS-based social engineering.

In parallel, additional infrastructure was observed impersonating Canada Revenue Agency (CRA), Air Canada, and Canada Post, indicating a broader fraud operation that reuses common design patterns. Furthermore, the investigation uncovered threat actors actively commercializing these campaigns on underground forums by selling specialized phishing kits designed to mimic official government services and banking portals.

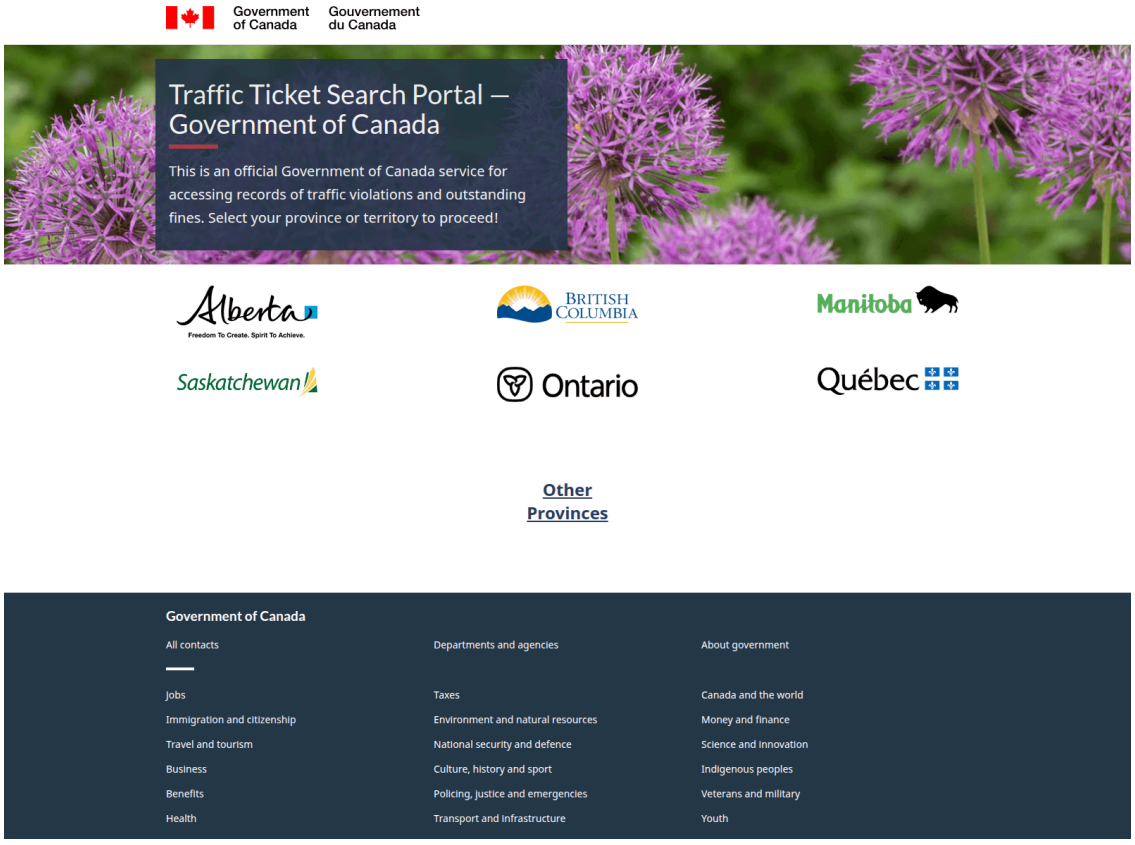
Modus Operandi

Victims are primarily seen lured using sms messages and malicious advertisements. Messages utilize high pressure tactics alleging unpaid fines, delivery failures, or booking errors to impersonate authoritative bodies like

PayBC, CRA, Canada Post, and Air Canada. The use of URL shorteners or typosquatted domains adds a layer of perceived legitimacy.

Upon clicking, victims are not immediately asked for data. Instead, they are taken through a “fake validation” phase. This stage typically requests inputs such as ticket numbers, booking references, or account identifiers. However, these fields accept virtually any value and perform no real verification. Their sole purpose is to create an illusion of authenticity and to psychologically prime the victim by making the interaction appear official and procedural.

After this trust-building step, the site transitions to a fraudulent payment gateway. These pages closely mimic legitimate payment processors but in reality, they are engineered to harvest personally identifiable information (PII) and financial data.



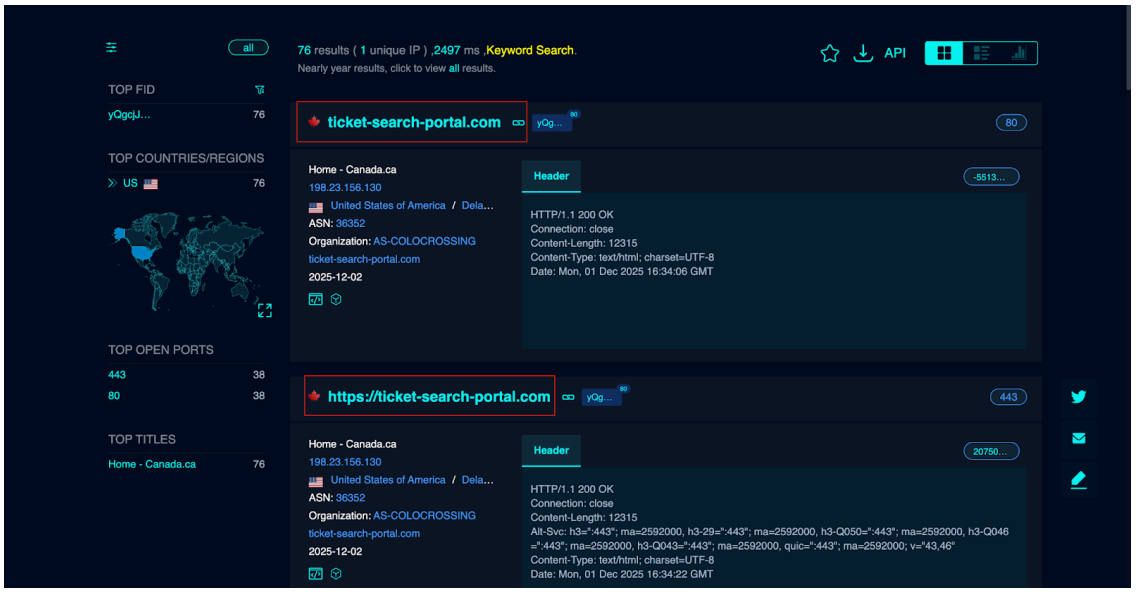
Fake webpage impersonating Traffic Ticket Search Portal

Analysis of Observed Infrastructure and Campaigns

The core theme observed across multiple clusters in this campaign is the impersonation of Canadian government traffic enforcement and fine payment services. This activity strongly aligns with the previously documented “PayTool” ecosystem, which focuses on provincial traffic fines and parking violations, while also expanding into a broader federal-style “**Traffic Ticket Search Portal**” model that aggregates multiple provinces under a single interface.

Unlike simple single-page phishing sites, this infrastructure is designed to simulate a centralized government service. Victims are presented with what appears to be an official “Government of Canada” portal where they can select their province (Alberta, British Columbia, Ontario, Quebec, Manitoba, Saskatchewan, etc.) to search for outstanding traffic violations. This mirrors how legitimate Canadian federal services provide entry points to provincial systems, significantly strengthening the illusion of authenticity.

On analysis we found over 70 websites which were resolving to ip address 198[.]23[.]156[.]130 impersonating the legitimate *canada.ca* The inclusion of provincial logos and a “Traffic Ticket Search Portal – Government of Canada” banner establishes institutional trust before any data is requested.



Results showing multiple Canada.ca impersonating “Traffic Ticket Search Portal” domains hosted on shared infrastructure

From an operational perspective, this structure serves three major purposes:

- **Trust Centralization:** By positioning the page as a federal-level service, attackers reduce suspicion. Victims are conditioned to believe they are interacting with a legitimate nationwide government platform rather than a standalone site.
- **Scalability Across Provinces:** A single template can be reused for multiple provinces, allowing threat actors to rapidly deploy localized scams without rebuilding infrastructure for each region.

This workflow mirrors legitimate provincial traffic enforcement portals such as PayBC and ServiceOntario, making it consistent with known PayTool attack patterns.

Domain Pattern Observations

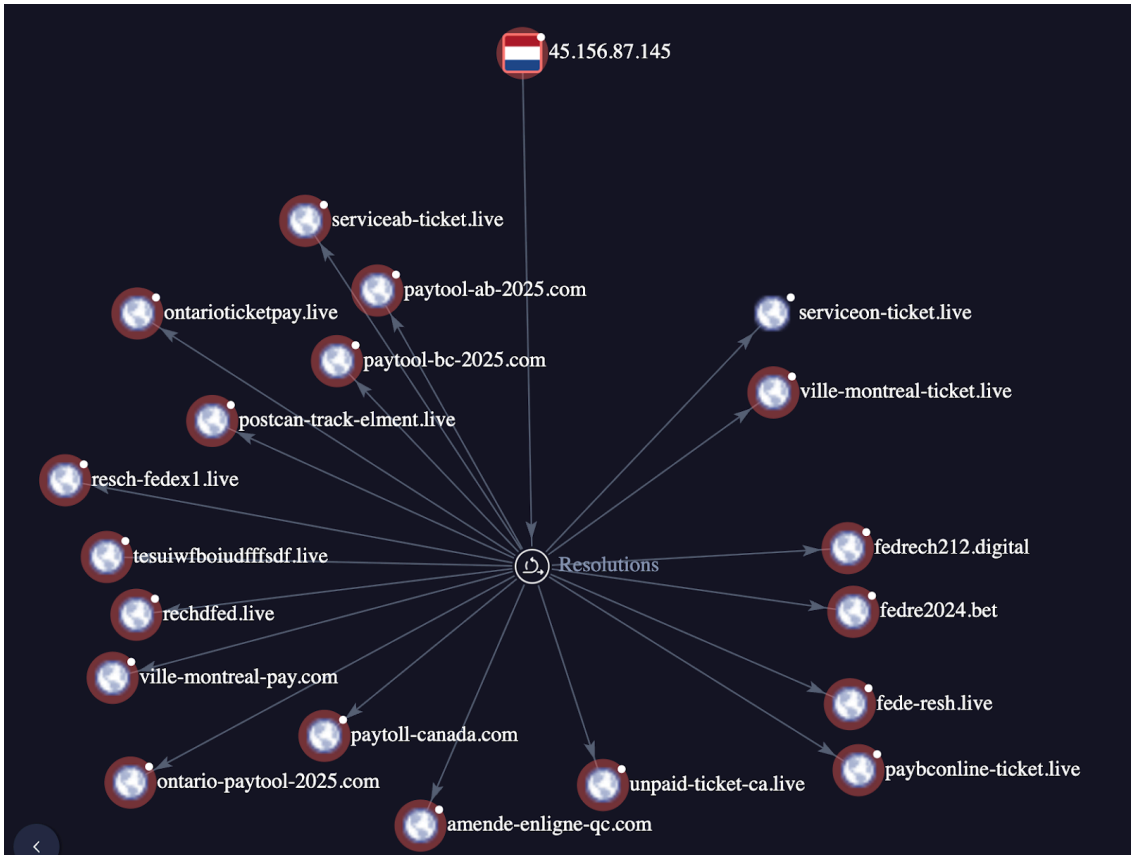
The domains associated with this cluster exhibit highly systematic naming conventions centered around:

- *“ticket”*
- *“traffic”*
- *“portal”*
- *“search”*
- *“violation”*
- *“infraction”*
- *“offence”*
- *“citation”*

These naming patterns indicate automation and bulk generation rather than organic domain creation. The repetition of terms reinforces the legitimacy narrative by matching keywords users expect when dealing with official traffic violation services.

Key IP Relations:

- *45[.]156[.]87[.]145*
- *45[.]156[.]87[.]131*
- *45[.]156[.]87[.]143*
- *45[.]156[.]87[.]213*



The central node 45.156.87.145 exhibit a high-density relationship with multiple provincial phishing domains

The infrastructure allows for simultaneous targeting across different jurisdictions using the same hosting provider. Based on domain relation data, we discovered multiple phishing domains of different provinces:

- **British Columbia (PayBC)**: paytool-bc-2025[.]com, bc-infraction[.]com, paybc-portal[.]live
- **Ontario (ServiceOntario):** ontarioticketpay[.]live, ontario-paytool-2025[.]com, serviceon-ticket[.]live
- **Quebec/Montreal:** ville-montreal-pay[.]com, amende-enligne-qc[.]com, a25pont-laval[.]com (Toll bridge impersonation)

Beyond the direct government impersonations, the relation data for 162[.]243[.]100[.]252 and the 45.156.87.x subnet exposes a "long tail" of generic infraction domains, such as parking-portal[.]live and overdueticketinfraction[.]info.

This indicates that the PayTool threat actor maintains a pool of generic, fallback domains. When specific provincial domains (like paybc-portal) are inevitably flagged or blacklisted by browser vendors, the actor can immediately rotate traffic to these generic "infraction" sites to maintain campaign continuity.

Canada Post Parcel & Redelivery Phishing

Further analysis of the infrastructure revealed a subset of domains mimicking Canada Post. While these specific domains were inactive during the investigation, passive DNS data and reputation signals strongly suggest a campaign focused on parcel delivery scams.

The naming conventions heavily utilize keywords associated with "failed delivery" narratives:

- redeliver
- handling
- parcel
- canpost / capost

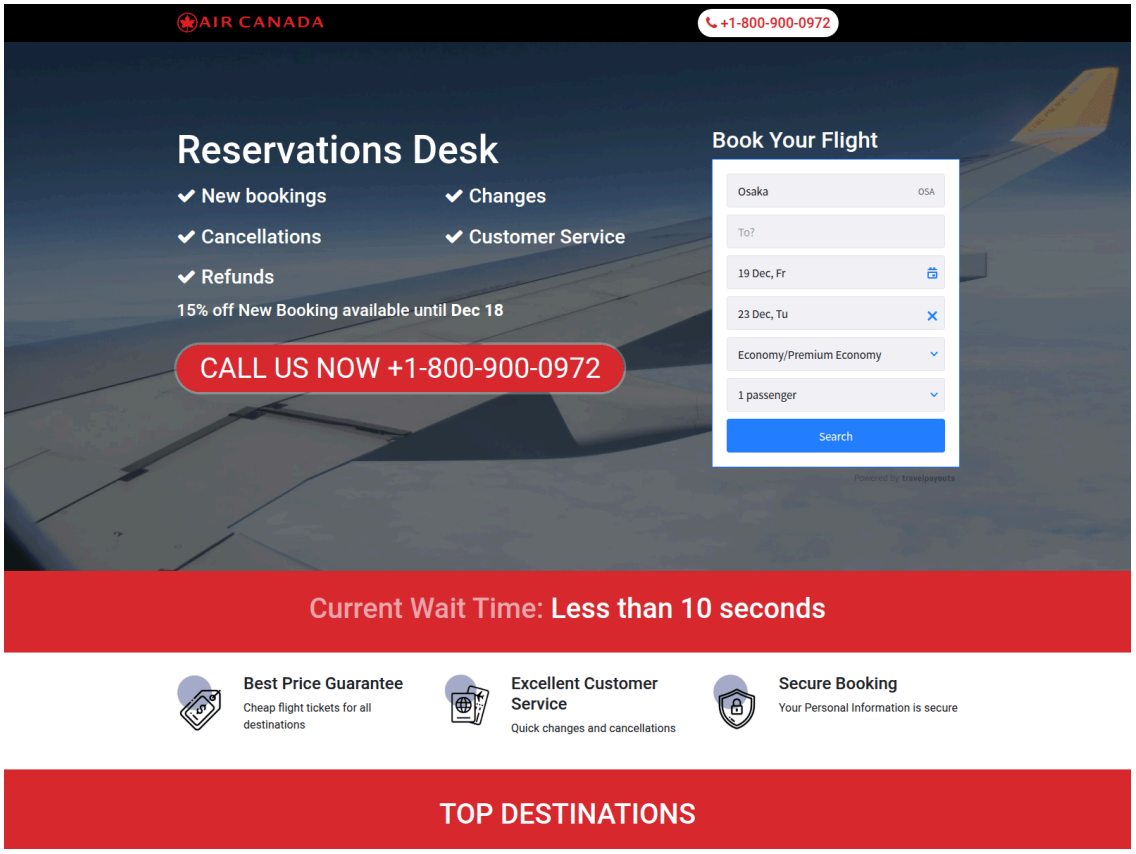
Although the domains were offline, their clustering around the same hosting provider aligns with the broader "PayTool" and ticket-fraud infrastructure. This indicates a consistent pattern of brand trust exploitation using disposable domains to cast a wide net for victims.

Air Canada Impersonation & Typosquatting

A distinct branch of this campaign targets the travel sector through Air Canada impersonation. Unlike the ticket and postal scams, which rely heavily on SMS (Smishing), this cluster appears driven by **SEO poisoning and typosquatting.**

Observed domain patterns include:

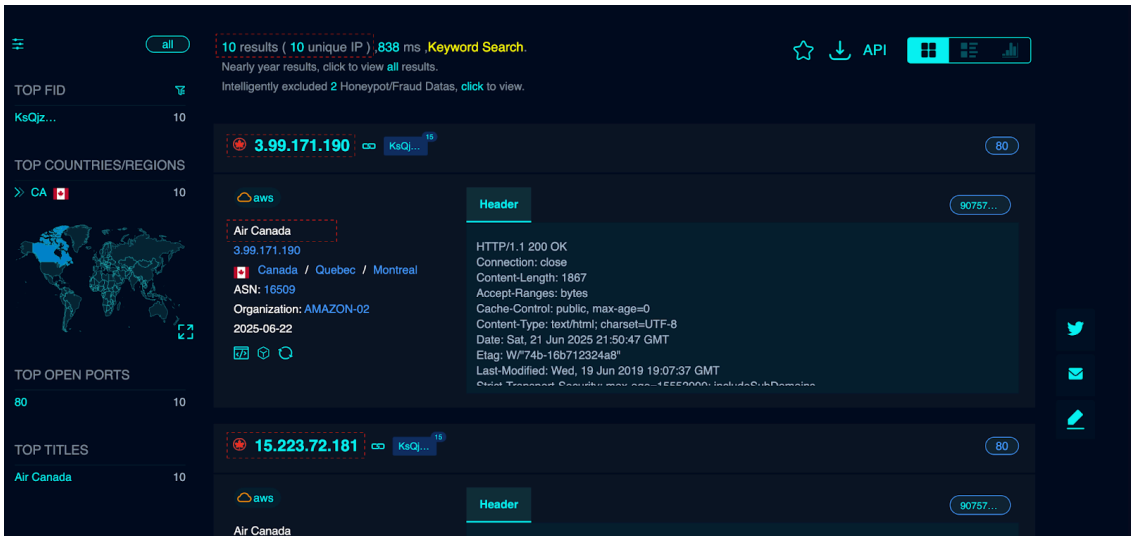
- aircanda-booking[.]com (Character Omission)
- air-canaada-booking[.]com (Character Duplication)
- airscanada-booking[.]com (Character Substitution)



Screenshot of the impersonated Air Canada landing page

The objective is to intercept users who mistype the legitimate domain or click malicious search engine ads. Furthermore, FOFA queries identified multiple servers hosting these domains using:

- Identical Favicon Hashes matching the official Air Canada website.
- Replicated Page Titles.



FOFA search results showing the cluster of Air Canada clones

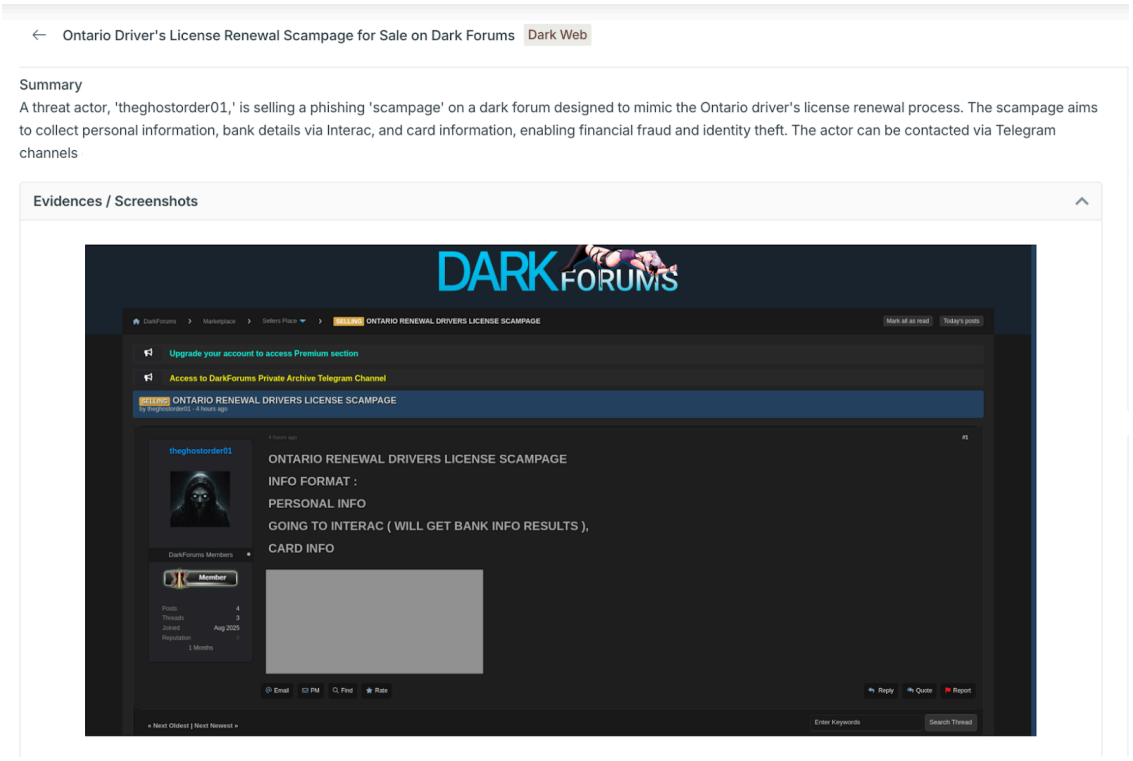
This confirms the deliberate cloning of legitimate branding assets rather than superficial imitation. The attackers likely leverage airline fraud because:

- Users expect to enter payment details for bookings.
- Modification and baggage fees provide a natural pretext for charges.
- Travel deadlines lower victim skepticism.

This expansion demonstrates that the threat actors are not limited to government service impersonation; they are effectively diversifying their targets to exploit commercial sectors where financial urgency is common.

Relationship With Underground Forums Activity

Intelligence gathered from various dark web cybercrime forums confirms that the proliferation of these localized campaigns is being driven by a "Phishing-as-a-Service" (PhaaS) model. Our analysis identified a threat actor operating under the alias 'theghostorder01', actively selling a specialized phishing kit designed to mimic the Ontario Driver's License Renewal process on multiple dark web forums.

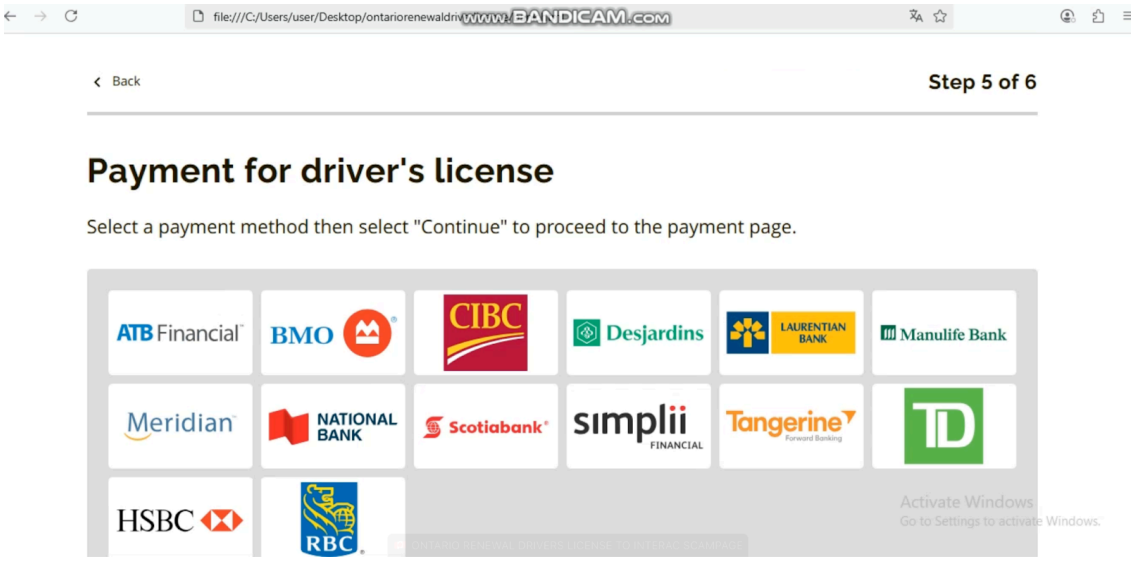


Threat actor listing the Ontario scam page on DarkForums, source: GTI CloudSEK

The advertisement highlights the kit's capability to harvest high-value data points, including:

- Personal Information (PII): Full name, address, and license details.
- Banking Credentials: Specifically targeting Interac e-Transfer logins to facilitate immediate account takeovers.

- Payment Data: Credit card numbers and CVV codes.



Screenshot shared by threat actor impersonating the ontario driver license page, claiming it has 14 bank pages involved.

The actor facilitates sales and support via different telegram channels. To validate these claims, one of our sources engaged with the threat actor. During the interaction, the seller was unable to demonstrate any server-side data handling or hosted infrastructure. Also when questioned about how victim data would be captured and delivered, the actor provided vague responses, stating that results would be sent via email or messaging platforms.

While the handling of the exfiltrated data is the responsibility of the buyer in most cases, the barrier of setting up the backend infrastructure has lowered significantly. Threat actors can now use Gen AI tools to rapidly script backend logic to process victim data. Additionally instead of a complex server-side database the victim data can be fetched via API and pushed directly to the bots and messaging platforms in real-time, a functionality that requires minimal technical skill to implement.

Threat Actor Profiling	
Active since	2024
Reputation	0
Current Status	ACTIVE
History	The threat actor has been active for at least two years and operates under the same username across multiple underground forums. Recent leaks revealed the email *theghostorder01@gmail.com*. The activity mainly advertising and selling custom phishing (“scampage”) source code targeting banks, cryptocurrency platforms, webmail providers, government services, and e-commerce brands majorly targeting UK, Canada, Australia and United States.

Threat Actor Profiling	
Rating	Medium
Payment Methods	USDT (TRC-20), Bitcoin (BTC)
Crypto Assets (USDT)	TWNCawkk3NbPZsY6mdnog8Sn7rS2vue95d
Crypto Assets (Bitcoin)	bc1qvhxkqujf347apsgy65ffykste0jy6txhgejhm048ukrys7cm6d3q2v4ze7

Impact & Risk Assessment

- Mass Data Compromise: Large-scale compromise of PII and financial data, including credit card details and Interac e-Transfer credentials, enabling account takeovers and direct financial fraud.
- Erosion of Public Trust: Increased victim trust erosion in legitimate Canadian government and national brand services (CRA, Canada Post, Air Canada, PayBC, ServiceOntario).
- Sector Diversification: Expanded attack surface through diversification into multiple sectors (government services, postal delivery, and airlines), which increases overall fraud exposure.
- Reputational Risk: Potential regulatory and reputational risk for organizations whose brands and infrastructure are abused in these high-fidelity phishing campaigns.

Mitigation

- Enforce proactive domain monitoring for typosquatting and keyword-based domains (e.g., ticket, portal, infraction, booking, parcel) and initiate rapid takedown procedures.
- Implement DNS and web gateway controls to block newly registered domains, suspicious TLDs (.live, .info), and known PayTool-related IP ranges.
- Strengthen public awareness campaigns emphasizing that Canadian government agencies and airlines do not request payments or sensitive data via SMS links.
- Deploy threat intelligence-driven detections to identify shared hosting patterns, favicon hashes, and page title reuse across phishing infrastructure.
- Encourage users to access services only through official bookmarked portals (e.g., canada.ca, PayBC, ServiceOntario, aircanada.com) rather than through links in messages or ads.

Conclusion

This investigation highlights a significant evolution in phishing campaigns targeting the Canadian demographic. Moving beyond generic "tax refund" lures, threat actors are now leveraging highly localized and context-aware

themes ranging from PayBC speeding fines and ServiceOntario renewals to Air Canada booking modifications.

The discovery of phishing kit developers on the dark web confirms that this is a commoditized operation, ensuring a steady supply of fresh domains and updated templates.

As these attacks rely heavily on urgency (unpaid fines) and trust (government branding), organizations and users must remain vigilant against domains utilizing irregular TLDs (e.g., .live, .info) and verify links directly through official provincial portals.

Domain	Registrar	Creation Date	Updated Date	Expiration Date
justice-ticket-portal[.]com	MAT BAO CORPORATION	2025-12-14	2025-12-14	2026-12-14
paybc-portal[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-07-19	2025-07-19	2026-07-19
bc-account[.]com	PDR Ltd. d/b/a PublicDomainRegistry.com	2024-05-20	2024-05-20	2025-05-20
paytool-bc-2025[.]com	Hosting Concepts B.V. d/b/a Registrar.eu	2025-07-14	2025-07-24	2026-07-14
paybconline-ticket[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-06-29	2025-11-24	2026-06-29
bc-infraction[.]com	NICENIC INTERNATIONAL GROUP CO., LIMITED	2025-10-19	2025-10-27	2026-10-19
vancouver-infraction[.]com	NICENIC INTERNATIONAL GROUP CO., LIMITED	2025-10-20	2025-10-22	2026-10-20
ontarioticketpay[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-07-09	2025-11-24	2026-07-09
ontario-paytool-2025[.]com	Hosting Concepts B.V. d/b/a Registrar.eu	2025-07-09	2025-07-27	2026-07-09
serviceon-ticket[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-06-29	2025-07-04	2026-06-29
overdueticketinfraction[.]info	NameSilo, LLC	2025-08-07	2025-10-21	2026-08-07
ville-montreal-pay[.]com	Hosting Concepts B.V. d/b/a Registrar.eu	2025-07-06	2025-07-24	2026-07-06

Domain	Registrar	Creation Date	Updated Date	Expiration Date
amende-enligne-qc[.]com	Hosting Concepts B.V. d/b/a Registrar.eu	2025-07-05	2025-07-24	2026-07-05
ville-montreal-ticket[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-06-22	2025-11-24	2026-06-22
a25pont-laval[.]com	NICENIC INTERNATIONAL GROUP CO., LIMITED	2025-10-21	2025-10-24	2026-10-21
paytool-ab-2025[.]com	Hosting Concepts B.V. d/b/a Registrar.eu	2025-07-14	2025-07-24	2026-07-14
serviceab-ticket[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-06-29	2025-07-11	2026-06-29
ab-speed[.]com	NICENIC INTERNATIONAL GROUP CO., LIMITED	2025-10-16	2025-10-20	2026-10-16
abmarketworks[.]com	DYNADOT LLC	2003-05-18	2025-06-27	2026-05-18
outel[.]abmarketworks[.]com	Dynadot Inc	2003-05-18	2025-06-27	2026-05-18
parking-portal[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-07-09	2025-07-14	2026-07-09
unpaid-ticket-ca[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-06-26	2025-11-24	2026-06-26
parking-fines[.]com	OwnRegistrar, Inc.	2025-12-16	2025-12-20	2026-12-16
speedfines[.]com	OwnRegistrar, Inc.	2025-12-08	2025-12-15	2026-12-08
paytoll-canada[.]com	TUCOWS DOMAINS, INC.	2025-07-03	2025-07-09	2026-07-03
quickplate-check[.]com	OwnRegistrar, Inc.	2025-06-29	2025-06-29	2026-06-29
ticket-search-portal[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29

Domain	Registrar	Creation Date	Updated Date	Expiration Date
search-ticket-portal[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-search-violation[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-search-violations[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-portal-search[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
search-portal-ticket[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-portal-infractions[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-portal-infraction[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-portal-violations[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
ticket-portal-violation[.]com	MAT BAO CORPORATION	2025-11-29	2025-12-09	2026-11-29
my-traffic-ticket-portal[.]com	Global Domain Group LLC	2025-09-23	2025-12-12	2026-09-23
my-traffic-tickets-portal[.]com	Global Domain Group LLC	2025-10-22	2025-10-30	2026-10-22
my-traffics-citations[.]com	Dominet (HK) Limited	2025-10-28	2025-11-04	2026-10-28
my-traffics-citation[.]com	Dominet (HK) Limited	2025-10-28	2025-11-04	2026-10-28
my-traffic-citations[.]com	Dominet (HK) Limited	2025-10-28	2025-11-04	2026-10-28
my-traffic-citation[.]com	Dominet (HK) Limited	2025-10-28	2025-11-04	2026-10-28

Domain	Registrar	Creation Date	Updated Date	Expiration Date
my-traffic-violations[.]com	Global Domain Group LLC	2025-10-23	2025-10-30	2026-10-23
my-traffic-violation[.]com	Dominet (HK) Limited	2025-10-22	2025-11-02	2026-10-22
my-traffic-offence[.]com	Global Domain Group LLC	2025-10-24	2025-10-30	2026-10-24
postcan-track-elment[.]live	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-06-18	2025-11-24	2026-06-18
handlingpostecan1[.]com	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-07-24	2025-09-07	2026-07-24
www[.]handlingpostecan1[.]com	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-07-24	2025-09-07	2026-07-24
redeliverparcel[.]info	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-09-18	2025-09-27	2026-09-18
capost[.]redeliverparcel[.]info	-	2025-09-18	2025-09-18	2025-09-16
handlingxpress[.]info	PDR Ltd. d/b/a PublicDomainRegistry.com	2025-09-13	2025-09-18	2026-09-13
capost[.]handlingxpress[.]info	-	2025-09-13	2025-09-13	2026-09-13
handlingparcel[.]info	NameSilo, LLC	2025-09-07	2025-10-21	2026-09-07
canpost[.]handlingparcel[.]info	-	2025-09-07	2025-09-07	2026-09-07
aircanda-booking[.]com	NAMECHEAP INC	2025-08-06	2025-08-06	2026-08-06
air-canaada-booking[.]com	NAMECHEAP INC	2025-11-03	2025-11-04	2026-11-03
airscanada-booking[.]com	NAMECHEAP INC	2025-11-03	2025-11-04	2026-11-03

IP Addresses

45.156.87.145

45.156.87.131

45.156.87.143

45.156.87.213

198.23.156.130

162.243.100.252

192.109.138.183

209.141.50.110

3.99.171.190

15.223.72.181

35.183.85.238

3.97.15.116

35.183.132.238

35.182.194.55

3.96.139.96

15.156.206.92

3.97.9.55

99.79.60.130

References:

- *Intelligence source and information reliability - Wikipedia
- #Traffic Light Protocol - Wikipedia
- https://flare.io/learn/resources/blog/paytool-targets-canadians-traffic-scams/

Related Blogs

Predict Cyber Threats against your organization
