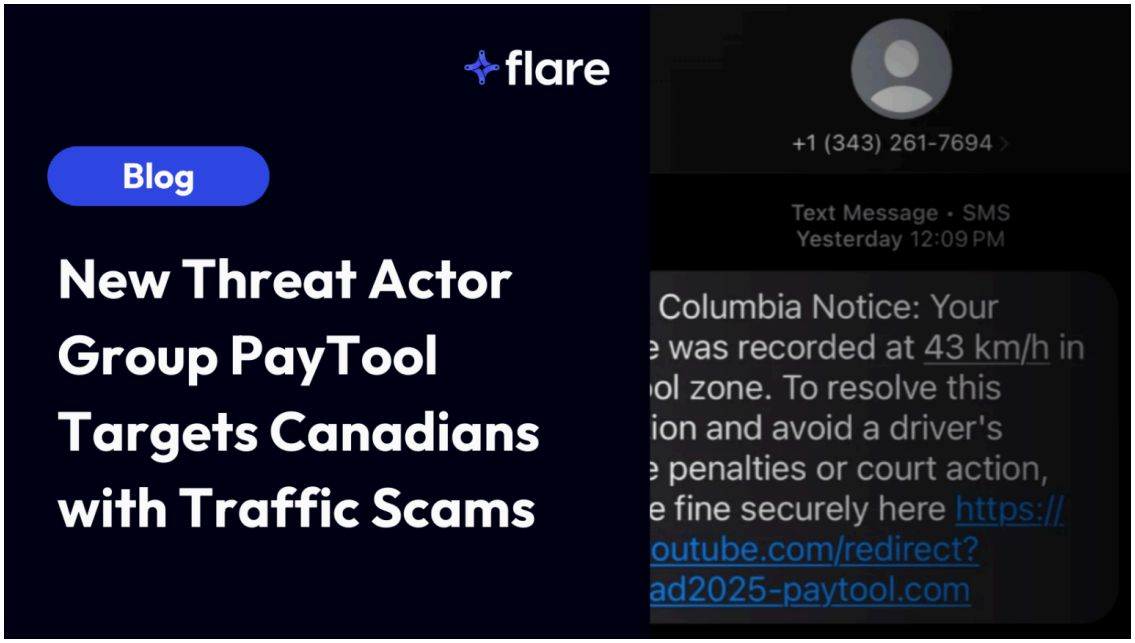
New Threat Actor Group PayTool Targets Canadians with Traffic Scams

By Research Team

Published: 2026-01-09 · Archived: 2026-04-02 11:13:35 UTC



By Adrian Cheek, Senior Cybercrime Researcher

Receiving a text message which informs you of a missed toll fee or parking fine seems to be a daily occurrence. These scams, which are mostly run by Chinese speaking threat actors, are easy to ignore for Canadians when the text references a US state, but the scams are becoming more accurate in their locations and showing provinces.

“Traffic scams,” the collective name we give to toll and parking scams, are a form of “smishing” (SMS phishing) in which the threat actors send text messages impersonating legitimate government agencies or private firms, such as the 407 ETR, claiming you have an unpaid balance and trick users into providing personal and financial information.

Flare Research recently began tracking a threat actor group, “PayTool,” that is specifically targeting Canadians. The group operates using different tactics we often see referenced by Chinese speaking threat actors targeting the United States.

We suspect we may be the first cybercrime researchers to identify PayTool, and it’s more likely that we may be the first to identify all victims from this scam. We are closely following this group as they continue to push out new scam domains.

Key Takeaways of Our Analysis of Canadian Victims of PayTool

- The scams have become more believable over the last few months
- Since we've been tracking websites associated with PayTool in the last 12 months, the frequency of newly registered websites has increased since July (also tied to an increase in scam text messages publicly reported)
- We have identified over 900 potential victims from this specific campaign, and additional victims from earlier campaigns believed to be run by PayTool

How Traffic Scams Work

Below are a couple of examples of how PayTool's traffic scams operate (there may be different versions of the same process):

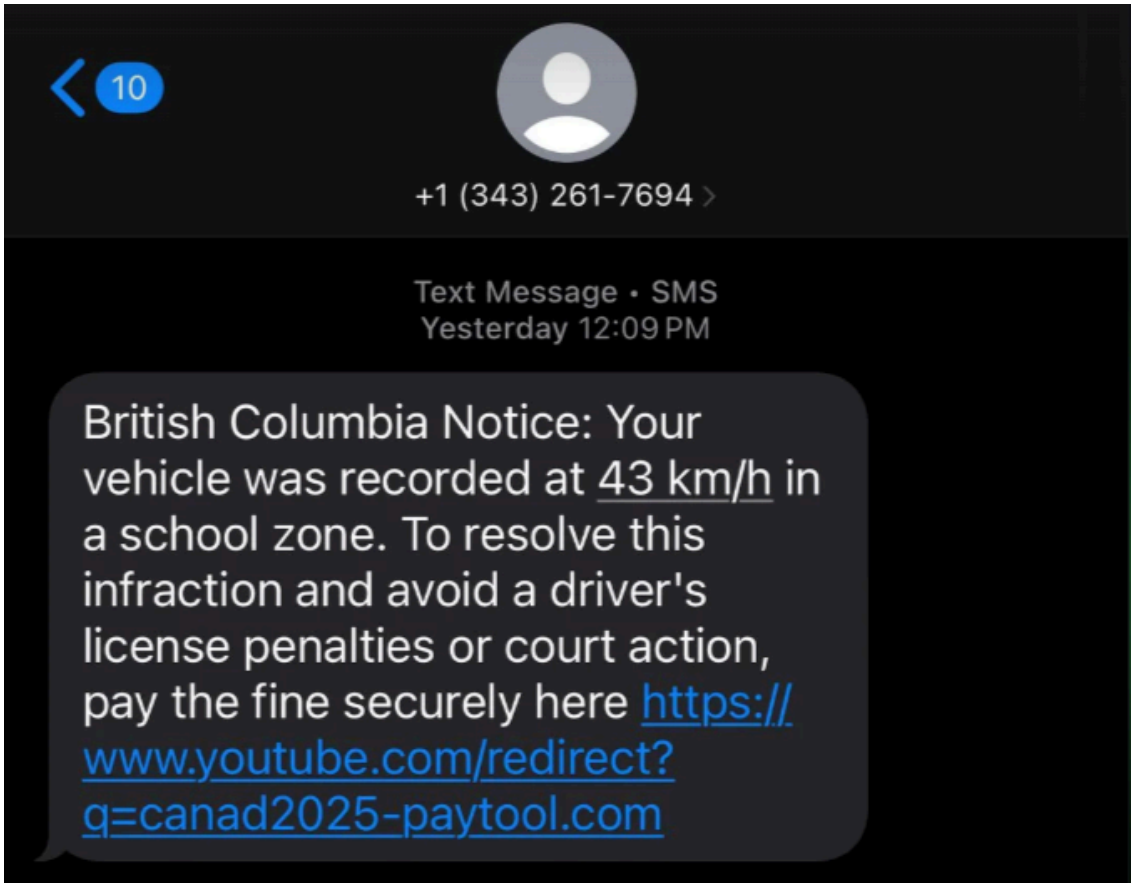
- **Unsolicited message**: Users receive an unexpected text message from a Canadian phone number claiming an "unpaid parking fine" or "toll evasion notice" for a specific, small, amount (e.g., $6.97).
- **Urgency and threatening language**: The message will typically threaten late fees, license suspension, or legal action if payment isn't made immediately.
- **Malicious link:** A hyperlink to a fake website is included in the text. This site is meticulously designed to look like the official parties payment portal, using similar logos and URLs (e.g., 4o7etr[.]com instead of 407etr[.]com).
- **Personal information theft:** When the link is clicked and an attempt is made to pay the fake fine, the user is prompted to enter sensitive data, such as a credit card number, bank account details, driver's license number, or other personal information.

This information is then used to purchase goods and services elsewhere which the actors can then convert to a currency of their choice.

What is the PayTool Group?

The scam begins with an unsolicited text. In the example below, the phone number used is an Ontario area code. However, the message claims to be a notice from British Columbia regarding speeding in a school zone.

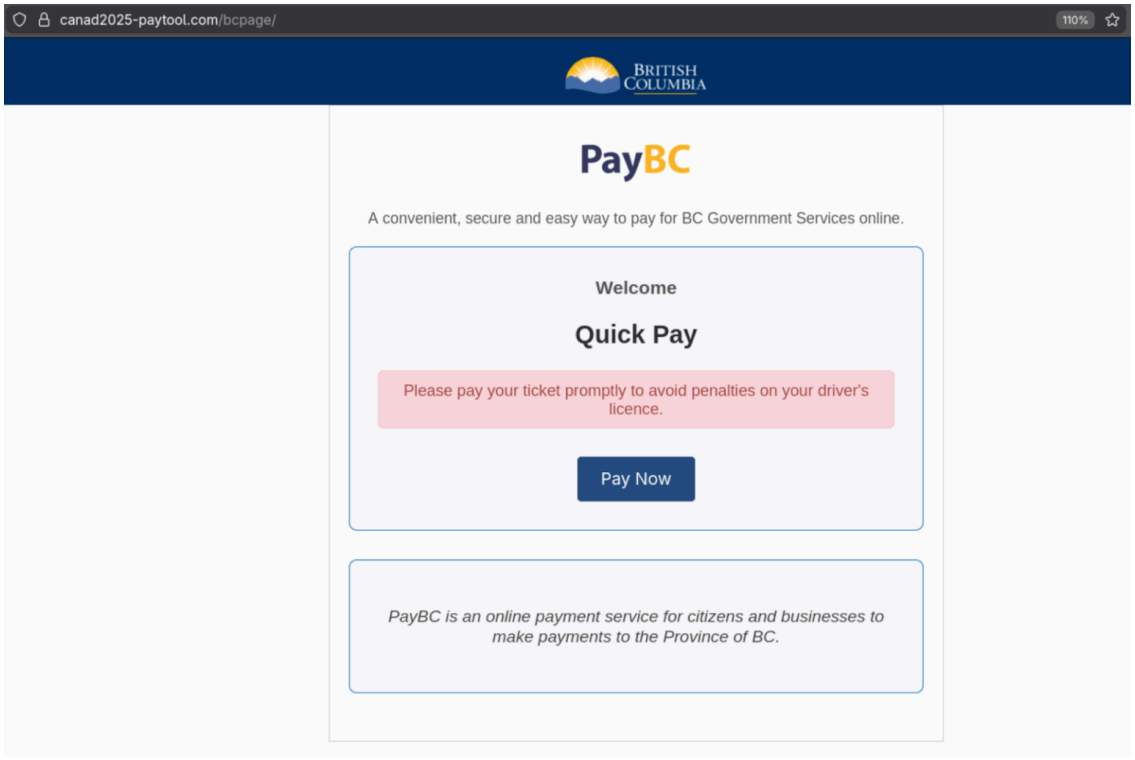
Open source reporting suggests that some recipients of the messages were from provinces outside of the alleged offense, indicating that targeting in this instance was not location based.



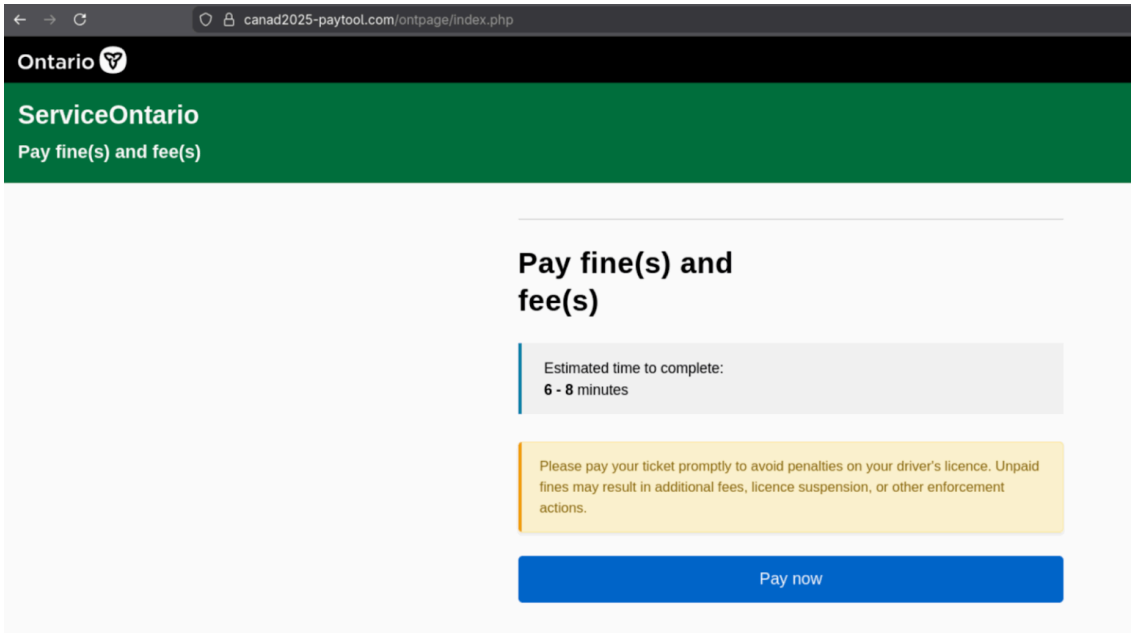
Text message that claims to be a notice about a speeding infraction

The message openly threatens legal action if payment is not made, which implies some form of urgency is required. Messages with identical wording have been collected from locations in Prince Edward Island and Ontario. Unlike other scam notifications Flare tracks, this message provides a hyperlink that clearly redirects to YouTube, then a social media platform, and finally to a payment page.

The payment pages are designed to look genuine and contain the relevant provincial branding with the URL being the only indicator that this is not a legitimate service. Each page contains a button which then allows for credit card details to be added.



Example of the BC PayTool page



Example of the Ontario PayTool page

Our analysis of the phone numbers used in the text messages reveal area codes from Ottawa, Toronto, and Northeastern Ontario which is a strong indicator that the threat actor group behind this scam is based in Canada or has knowledge of or access to Canadian technology, such as eSIMs or physical SIM cards.

When we compared this information to the same type of scam conducted in the United States, Flare observed a much wider spread of area codes, even branching out into multiple country codes, such as the Caribbean which uses a +1 country code, but would appear to be from the US at first glance. The phone numbers and area codes

also varied depending on the type of scam the group is operating and the availability of SIMs and software to cycle through cell phone numbers.

We're currently tracking 37 websites that have been associated with this threat actor group in the previous 12 months. Of some significance, the frequency of newly registered websites has increased since July, which ties to an increase in text messages being observed and publicly reported. The websites are registered using smaller, less popular domain registrars, often based in Europe and only remain operational during the timeframe of each campaign.

As part of our intelligence gathering, we have identified over 900 potential victims from this specific campaign and additional victims associated with earlier campaigns believed to run by the same group.

ICBC, The Insurance Corporation of British Columbia, responded to a recent post in a public forum regarding a text message a user received stating that

"We never contact customers via text about driving infractions or outstanding debt and do not ask for payment via an e-transfer link in a text message. If you receive a suspicious message, please delete it—it's a scam."

Continuing to Monitor PayTool

We're closely monitoring PayTool at Flare Research as their traffic scams appear to be increasing and pushing out new domains for scamming. We advise security teams to incorporate traffic scams into employee cybersecurity training.

Tracking Scams with Flare

The Flare Threat Exposure Management solution empowers organizations to proactively detect, prioritize, and mitigate the types of exposures commonly exploited by threat actors. Our platform automatically scans the clear & dark web and prominent threat actor communities 24/7 to discover unknown events, prioritize risks, and deliver actionable intelligence you can use instantly to improve security.

Flare integrates into your security program in 30 minutes and often replaces several SaaS and open source tools. See what external threats are exposed for your organization by signing up for our free trial.
