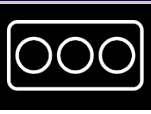
Active Threat Impersonating the Government of Alberta to Scam the Public

June 16, 2025

TLP:CLEAR



Source: Publicly Reported Incidents

Overview:

CyberAlberta Threat Intelligence has received multiple reports of a malicious domain impersonating the Government of Alberta, claiming to offer Canada Carbon Rebate (CCR) payments to illicit personally identifiable information (PII) from members of the public.

The threat actor is using this scam in an attempt to gather alberta.ca usernames, social security numbers, and mother's maiden names. These details are almost certainly later leveraged in attempts to commit fraud. This scam has been observed being delivered on Facebook but could be leveraging other social media platforms also.

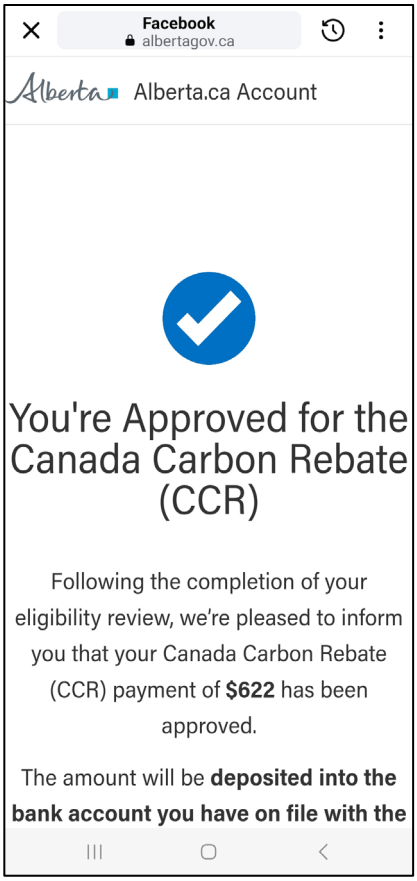


Figure 1 - Screenshot of the CCR scam observed on Facebook.

Threat Actor Infrastructure

The malicious domain used to host this scam **`albertagov[.]ca`** was recently created on June 3rd and currently resolves to IP address **`47.239.216[.]183`** owned by Alibaba US Technology (AS45102) and based in Hong Kong. Both the domain and IP address have low to no reports of previous malicious activity on open-source repositories.

The IP address also hosts the following Alberta-themed domains which are/were likely used for the same fraudulent style activity advertising fake CCR payments:

- **`myalbertaccr[.]ca`**
- **`ccr-alberta[.]info`**

Recommendations:

- Users are strongly encouraged to be aware of this scam and others like it, to not engage with them, and to report any observations of future similar scams to the owners of the platform it is found on.
- If any users have engaged with this scam and have submitted the requested PII, they should:
  - Sign in to their alberta.ca account and reset their password immediately.

  - Notify the alberta.ca contact centre.
  - Report the incident to the Canadian Anti-Fraud Centre (CAFC).
  - Contact their banks only if they have reason to believe their financial information has also been compromised.
- If users can no longer access their alberta.ca accounts using their passwords, it could be a sign of account takeover. In this case, it is once again strongly advised to contact alberta.ca by using their urgent issues hotline (844) 643-2789.
- Network defenders are advised to block the indicators of compromise (IOCs) listed below, review logs for signs of user impact related to this scam, and engage with affected users to ascertain the context of the activity and enhance awareness.

Indicators of Compromise

Indicator	Further Detail
`47.239.216[.]183`	Alibaba US Technology (AS45102)
`albertagov[.]ca`	Reported domain
`affordabilityactionplan.albertagov[.]ca`	Subdomain of reported domain
`myalbertaccr[.]ca`	Same IP
`ccr-alberta[.]info`	Same IP