Rapid Response Mechanism Canada | Open Data Analysis Report
Mécanisme de réponse rapide du Canada | Rapport d'analyse des données 2023-09-15

Probable PRC "Spamouflage" Campaign Targets Dozens of Canadian MPs in Disinformation Campaign, as well as Chinese-language Commentator in Vancouver

Key Findings

- A probable PRC "Spamouflage" campaign has targeted dozens of Canadian parliamentarians on Twitter, Facebook and YouTube. Targets include the Prime Minister, the leader of the opposition, several members of Cabinet, and dozens of backbench MPs from across the political spectrum and spanning multiple geographic regions of Canada.
- The campaign primarily targets the Prime Minister but accuses dozens of the MPs of criminal and ethical violations, including "political corruption", sexual scandals" involving minors, and "bribery of voters during an election". The social media posts attribute these allegations to a well-known critic of the Chinese Community Party (CCP) in Canada and popular Chinese-language vlogger (i.e. video blogger) – Mr. Xin Liu.
- In addition to the Facebook and Twitter (X) posts, Mr. Liu purportedly appears in a series of three YouTube videos, amplified by a known bot network, showing Mr. Liu making these allegations.
- These videos are likely "deep fakes" (i.e. AI-generated impersonation videos). This constitutes the first time, which has been tracked by RRM Canada, that a spamouflage campaign has employed "deep fake" AI technology.
- The bot network engaged in circulating these allegations and videos was most recently involved in circulating disinformation claiming the Hawaiian wildfires were started by a US "weather weapon", and disinformation on the Fukushima water release.

Report

- On September 5, 2023, Rapid Response Mechanism Canada (RRM) received a notice from its counterparts [redacted] that a bot network connected to the People's Republic of China (PRC) was targeting dozens of Canadian parliamentarians on Twitter, Facebook, and YouTube. Targets included the Prime Minister, the Leader of the Opposition, several members of Cabinet, and backbencher MPs across the political spectrum and spanning multiple geographic regions of Canada.
- Beginning in early August 2023 and accelerating in scale over the September long-weekend, the bot network left thousands of comments in English and French on the Facebook and Twitter accounts of MPs, claiming a CCP-critic in Canada, Mr. Xin Liu, had accused the various MPs of criminal and ethical violations, including "political corruption", "sexual scandals" involving minors, and "bribed voters during an election."
- These bot accounts also circulated a set of three YouTube videos of Mr. Liu making particularly strong allegations, and suggesting the Canadian Prime Minister "has a strong inclination towards lust, and is extremely corrupt." These videos were not posted on Mr. Liu's official YouTube channel nor posted on his official account on Twitter (X).
- RRM Canada, CSE (based on a preliminary assessment), and [redacted] believe it is likely that these videos are "deep fakes" (i.e. AI-generated impersonation videos). This would constitute the first time that RRM Canada is aware of a specific spamouflage campaign employing "deep fakes".

- Mr. Liu is a Vancouver-based video commentator who participated in China's 1989 Democracy movement. He maintains a popular video blog on YouTube (162K subscribers) and a large following on Twitter (299.3K followers). He frequently criticizes the governance practices of Chinese Communist Party (CCP) General Secretary Xi Jinping. However, RRM Canada has found no posts or videos on Mr. Liu's official YouTube or Twitter channels of him criticizing Canadian politicians.
- The same bot networks involved in this campaign were engaged in last month's disinformation campaign claiming that the Hawaiian wildfires were caused by a secret US "weather weapon"[1], and according to contacts at the Microsoft Threat Analysis Center, they tracked the same bot network spreading disinformation regarding the Fukushima water release in August.
- RRM Canada assesses the goal of the operation is likely two-fold. First, it likely seeks to discredit and denigrate the targeted MPs through seemingly organic posts, alleging sexual or financial impropriety, by posting waves of social media posts and videos that call into question the political and ethical standards of the MPs (smearing them reputationally), using a popular Chinese-speaking figure in Canada. Second, it likely seeks to silence Mr. Liu's criticism of the CCP by, getting MPs to distance themselves from him and discouraging wider online communities from engaging with him.
- [redacted] assess that the unusual network activity is "Spamouflage" -- a bot network likely controlled by the PRC's law enforcement entity, the Ministry of Public Security (MPS). Facebook parent company Meta also attributes Spamouflage tactics and techniques to the MPS.
- [redacted] findings through its own data collection, and came to the same conclusion that the operation is indeed Spamouflage, and "points to the MPS." RRM Canada has also conducted a review, validating the data samples provided by [redacted] and concurs with [redacted] that the operation is likely Spamouflage, suggesting MPS involvement.

Implications

RRM Canada assesses the impact of the operation on Canadian parliamentarians is likely low. Spamouflage bot networks produce a mass of posts, but often receive little non-bot public engagement. According to the social media metrics provided by both Facebook and Twitter, most Spamouflage posts received between "zero" and "five" views or impressions. This means an exceedingly low number of Canadians – or even in some cases zero users – will have viewed the content.

The [redacted] identified 21 MPs that were targeted in the campaign, including the Prime Minister, the leader of the Official Opposition, one Cabinet minister, and several MPs from across the political spectrum. RRM Canada independently validated [redacted] findings, and found an additional 25 MPs, several additional members of Cabinet, as well as [redacted] RRM Canada is continuing to search for other targets of the operation.

The impact on Mr. Liu, however, is likely very high. Over the past month, Mr. Liu has likely received hundreds of thousands of alerts from Facebook, Twitter, and YouTube with false claims that he has libeled dozens of cabinet members, members of the opposition, and backbencher MPs from all political

[1] Sanger, David E., and Steven Lee Myers, "China Sows Disinformation About Hawaii Fires Using New Techniques", *The New York Times*, https://www.nytimes.com/2023/09/11/us/politics/china-disinformation-ai.html

parties. In targeting and intimidating a known critic of the PRC in Canada, RRM Canada believes this spamouflage operation could be a manifestation of transnational repression.

The use of sophisticated “deep fake” technology in a spamouflage campaign is also significant, suggesting a new tactic by the MPS, and the likelihood that spamouflage could become more persuasive to a wider audience.

Background

“Spamouflage” should be considered a tactic or technique, not an entity. It is a network of new or hijacked social media accounts that posts and amplifies propaganda messages across multiple social media platforms – including Facebook, Twitter, Instagram, YouTube, Medium, Reddit, TikTok, and LinkedIn. The word is a portmanteau of “spam” and “camouflage”, intended to portray the covert and hidden attempts to spread spam-like content and propaganda among more benign, human-interest-style content. Spamouflage networks are largely contained within their own echo chambers of fake users, and rarely garner organic social media engagement from real users.

On August 29, 2023, Meta released its standard quarterly Adversarial Threat Report, which featured a significant section detailing the company’s efforts to take down accounts linked to Spamouflage operations. The company affirmed that Spamouflage activity is linked to PRC law enforcement entities.[2]

Earlier this year, the US Department of Justice announced charges against 34 MPS officers for creating fake online personas to harass critics and disseminate PRC-friendly propaganda and messages.[3] Nimmo noted that the company had also identified the activity outlined in the indictment, and attributed it to “Spamouflage”.[4]

RRM Canada has also reported on previous Spamouflage activity in Canada.[5] In August 2022, RRM Canada confirmed Mandiant’s findings that a PRC-linked bot network had attempted to discredit the opening of a rare earths drill site at Alces Lake in Northern Saskatchewan.[6] The bot network created personas of Canadian Facebook and Twitter users and feigned concern for the environmental and health impacts related to the drill site. In that instance, RRM Canada assessed the impact of the operation was low and that very few Canadian social media users will have seen the Spamouflage posts in question.

[2] Rosen, Guy. Aug. 29, 2023. "Raising Online Defenses Through Transparency and Collaboration." *FB Newsroom*. https://about.fb.com/news/2023/08/raising-online-defenses/

[3] Office of Public Affairs, US DOJ. Apr. 17, 2023. "40 Officers of China’s National Police Charged in Transnational Repression Schemes Targeting U.S. Residents." *US DOJ*. https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us

[4] Martin, Alexander. Aug. 29, 2023. “Chinese law enforcement linked to largest covert influence operation ever discovered.” *The Record*. https://therecord.media/spamouflage-china-accused-largest-covert-influence-operation-meta

[5] See IOL/RRM Canada Aug. 5, 2022 report “Analysis of PRC Influence Operation Directed at Saskatchewan Rare Earth Drill Site.” Available on request.

[6] Mandiant Threat Intelligence. Jun. 28, 2022. “Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance.” Mandiant. https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies