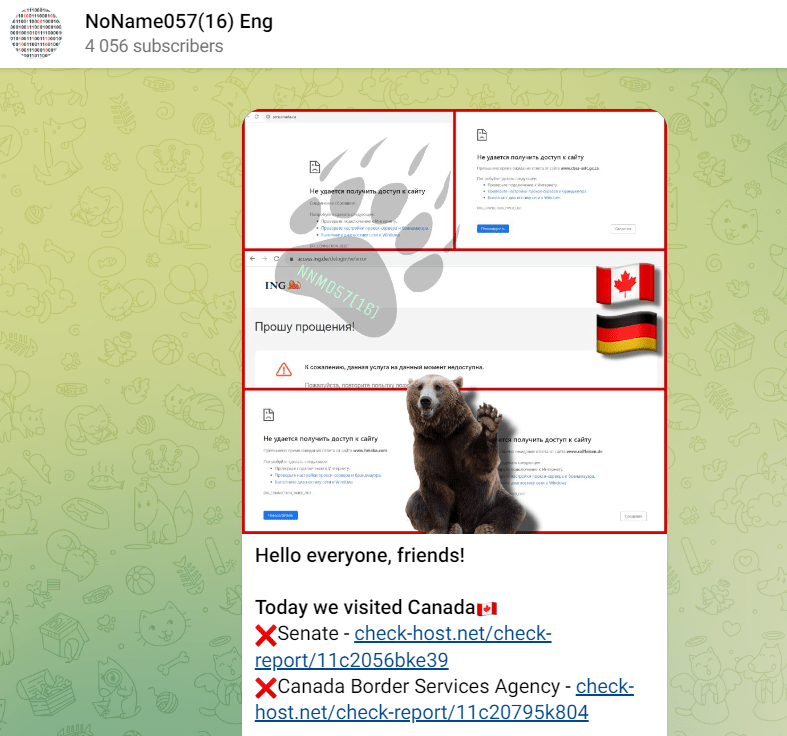
A DDOS attack was launched against Canadian airports by the pro-Russian hacker group NoName, resulting in severe disruptions.



It is believed that the pro-Russian hacking collective NoName was behind the cyberattack that shut down the border checkpoints at various Canadian airports.

Operations at a number of Canadian airports were significantly hampered last week by a significant DDoS cyber-attack, which was probably launched by the pro-Russian hacker organization NoName, according to Recorded Future News.

After a few hours, the Canada Border Services Agency (CBSA) was able to stop the onslaught.

The check-in kiosks and electronic gates at airports were affected by the hack, according to the Canada Border Services Agency (CBSA).

At border checkpoints across the nation, the cyberattack resulted in delays in the processing of arrivals of more than an hour.

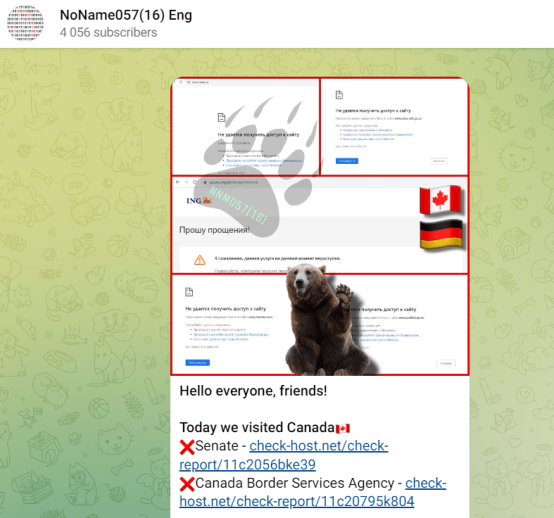
The Canada Border Services Agency (CBSA) formally acknowledged on Tuesday that a distributed denial of service (DDoS) attack is to blame for "connectivity issues that affected kiosks and electronic gates at airports." La Presse, a Canadian news organization, reported this.

"However, according to its Telegram profile, the Russian-speaking cyber gang NoName057 specifically targeted the government agency. "We are assessing the situation and conducting an investigation closely with our partners. No personal information has been released as a result of these attacks because the CBSA's first priority is the protection of Canadians and visitors, according to Maria Ladouceur, a spokesperson for the agency.

The Canada Border Services Agency (CBSA) confirmed that the attack impacted check-in kiosks and electronic gates at airports.

The cyber-attack caused delays in the processing of arrivals for more than an hour at border checkpoints across the country.

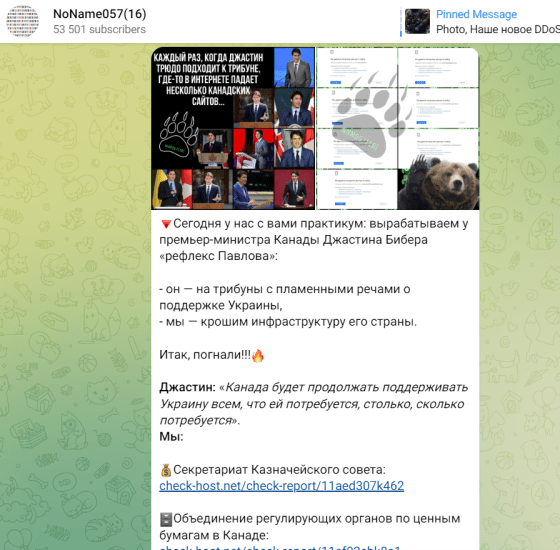
“The Canada Border Services Agency (CBSA) finally confirmed on Tuesday that “connectivity issues that affected kiosks and electronic gates at airports” are the result of a distributed denial of service (DDoS) attack.” [*reported*](https://www.lapresse.ca/actualites/national/2023-09-19/agence-des-services-frontaliers/la-panne-dans-les-aeroports-provenait-bien-d-une-attaque-informatique.php) the Canadian media outlet La Presse.



NoName asserts that the DDoS campaign is the group's response to the assistance Canada has provided to Ukraine.

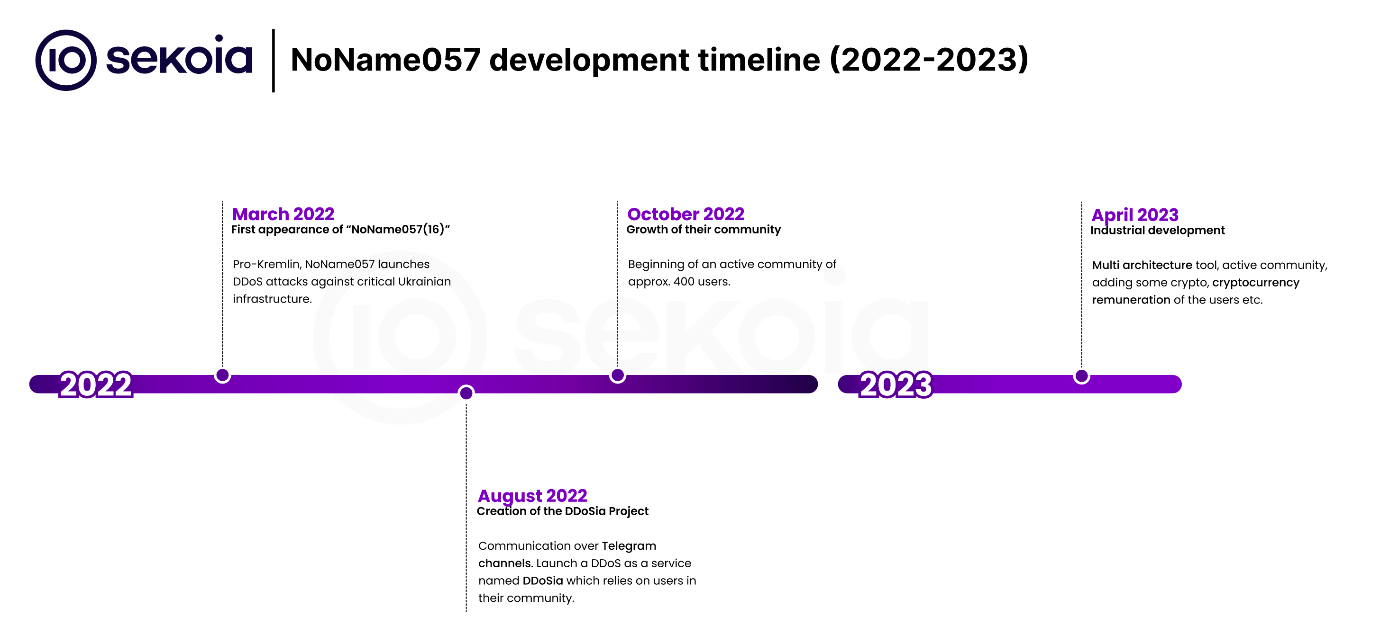
A distributed denial of service attack that is aimed against several Canadian industries was described in an advisory provided by the Canadian Centre for Cyber Security.

"Since 13 September 2023, the Cyber Centre has been aware of and responding to reports of several distributed denial of service (DDoS) campaigns targeting multiple levels within the Government of Canada, as well as the financial and transportation sectors." scans the warning. "This Alert is being published to increase awareness of these campaigns, to highlight the potential impact on government services, and to provide guidance for organizations that may be the target of malicious activity," the alert reads.

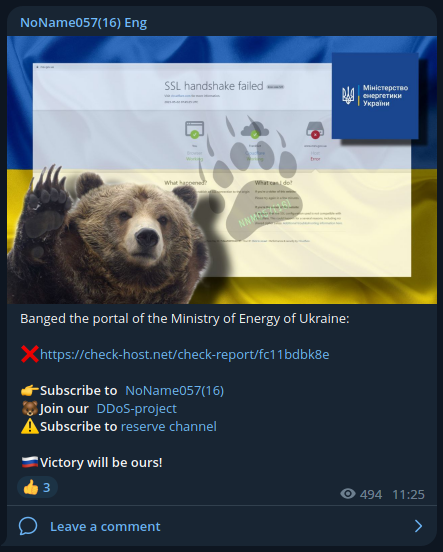


The pro-Russian hacktivist nationalist organization NoName057(16) developed and used the Distributed Denial of Service (DDoS) attack toolset against nations who opposed the Russian invasion of Ukraine.

Early in 2022, the DDoSia project was introduced on Telegram. As of June 2023, the main Telegram channel for the NoName057(16) primary group had more than 45,000 subscribers, while the channels for the DDoSia project had more than 10,000. Administrators added the option to pay in cryptocurrency for individuals who declare a genuine TON wallet based on their involvement in the DDoS attacks, and also issued instructions for potential volunteers who wish to take part in projects.



<https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/>



NoName057(16), a pro-Kremlin hacktivist collective, particularly targets NATO nations such the Eastern Flank (Lithuania, Poland, Czech Republic, and Latvia) and the Ukrainian government. This is most likely due to the fact that those nations are the most outspoken in their public comments opposing Russia and in favor of Ukraine, as well as in their provision of military support and capabilities.

France, the United Kingdom, Italy, Canada, and other EU nations are among the secondary DDoSia targets. This is likely because these nations have supported Ukraine politically, militarily, and economically since the crisis began.