# Pro-Russian hackers disrupt Dutch municipal services amid NATO summit



On Monday, a cyberattack disrupted NotuBiz, the service used by various Dutch municipalities and provinces to publish official documents. This impact rendered council and provincial document pages difficult to access across multiple regions, including the provinces of South Holland and Overijssel, as well as municipalities such as The Hague, Den Bosch, and Delft. The timing was particularly notable, coinciding with The Hague’s hosting of the annual NATO summit—a period when authorities had already warned of potential cyber threats targeting government infrastructure.

The pro-Russian hacker group NoName05716 took responsibility for the attack via their Telegram channel, continuing their pattern of targeting countries supporting Ukraine. This claim, however, has not been officially verified by government sources. NotuBiz reported a significant surge in network traffic aimed at their systems, leading to disruptions. Although their firewall blocked much of this traffic and prevented a complete outage, the attack nonetheless caused extensive delays and practical difficulties for users attempting to access official documents.

This event reflects a broader trend of cyberattacks orchestrated by Russia-aligned hacktivist groups against Dutch public and private entities. The Dutch National Cyber Security Center (NCSC) confirmed a wave of large-scale distributed denial of service (DDoS) attacks targeting multiple organizations both within the Netherlands and across Europe. These attacks are seen as retaliatory measures in response to the Netherlands’ military support for Ukraine, which includes financial aid amounting to several billion euros.

NoName05716, a loosely organized pro-Russian group, is known for frequent DDoS attacks on government websites, media outlets, and companies deemed adversaries of Russia. Their tactic involves overwhelming targeted servers with excessive traffic, impairing accessibility without stealing data or damaging critical infrastructure. Cybersecurity experts estimate that the group targets five to fifteen websites daily, amplifying the disruptive effect across multiple sectors.

The assault on NotuBiz follows previous high-profile attacks by NoName05716 in the Netherlands, including a notable DDoS attack on the North Sea Port website earlier this year and an incident affecting the public transport chip card system website. Although these attacks hamper digital services temporarily, physical operations typically continue without interruption.

These recurring cyber incidents underscore the vulnerabilities inherent in digital government and public service infrastructure, emphasizing the need for robust defensive measures. While firewalls and mitigation efforts can reduce the severity of such attacks, the inconvenience to citizens and potential risks to sensitive systems remain a critical concern for Dutch authorities amid escalating geopolitical tensions.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.techzine.eu/news/security/132434/pro-russian-hacker-group-claims-attack-on-dutch-government-websites/), [[2]](https://www.techzine.eu/news/security/132434/pro-russian-hacker-group-claims-attack-on-dutch-government-websites/), [[4]](https://www.themoscowtimes.com/2025/04/29/pro-russian-hackers-take-down-local-government-websites-in-netherlands-a88911)
* Paragraph 2 – [[1]](https://www.techzine.eu/news/security/132434/pro-russian-hacker-group-claims-attack-on-dutch-government-websites/), [[3]](https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/), [[4]](https://www.themoscowtimes.com/2025/04/29/pro-russian-hackers-take-down-local-government-websites-in-netherlands-a88911)
* Paragraph 3 – [[3]](https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/), [[4]](https://www.themoscowtimes.com/2025/04/29/pro-russian-hackers-take-down-local-government-websites-in-netherlands-a88911), [[5]](https://www.radware.com/cyberpedia/ddos-attacks/noname057%2816%29/)
* Paragraph 4 – [[4]](https://www.themoscowtimes.com/2025/04/29/pro-russian-hackers-take-down-local-government-websites-in-netherlands-a88911), [[5]](https://www.radware.com/cyberpedia/ddos-attacks/noname057%2816%29/), [[6]](https://www.nltimes.nl/2023/06/20/zeeland-port-website-hit-ddos-attack-possibly-russian-hackers), [[7]](https://www.nltimes.nl/2023/11/04/russian-hackers-attack-public-transport-chip-card-website-temporarily-inaccessible)
* Paragraph 5 – [[1]](https://www.techzine.eu/news/security/132434/pro-russian-hacker-group-claims-attack-on-dutch-government-websites/), [[3]](https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/), [[7]](https://www.nltimes.nl/2023/11/04/russian-hackers-attack-public-transport-chip-card-website-temporarily-inaccessible)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techzine.eu/news/security/132434/pro-russian-hacker-group-claims-attack-on-dutch-government-websites/> - Please view link - unable to able to access data
2. <https://www.techzine.eu/news/security/132434/pro-russian-hacker-group-claims-attack-on-dutch-government-websites/> - A cyberattack disrupted the service used by municipalities and provinces to publish official documents on Monday. Pages containing council and provincial documents became difficult to access due to the attack on NotuBiz. The timing of the disruption is striking. The Hague is hosting the annual NATO summit this week. In the run-up to the summit, authorities had already warned of possible cyberattacks. The pro-Russian hacker group NoName05716 claimed responsibility for the attack via its Telegram channel. This group frequently attacks websites in countries that support Ukraine. However, the claim has not yet been verified by official sources.
3. <https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/> - Russia-aligned hacktivists persistently target key public and private organizations in the Netherlands with distributed denial of service (DDoS) attacks, causing access problems and service disruptions. The situation was acknowledged via a statement by the country's National Cyber Security Center (NCSC), part of the Dutch Ministry of Justice. 'This week, several Dutch organizations have been targeted by large-scale DDoS attacks,' reads the NCSC announcement. 'The DDoS attacks are directed at both Dutch and other European organizations. Within the Netherlands, both public and private entities are being attacked.' The NCSC noted that the attacks were claimed by the hacktivist group named NoName057(16) on the threat actor's Telegram channel.
4. <https://www.themoscowtimes.com/2025/04/29/pro-russian-hackers-take-down-local-government-websites-in-netherlands-a88911> - A group of pro-Russian hackers took down the websites of several Dutch municipalities and provinces on Monday in retaliation for the Netherlands’ military assistance to Ukraine. At least 19 websites were affected by the coordinated distributed denial of service (DDoS) attacks, which overload websites and applications with targeted requests to knock them offline, the Algemeen Dabbled newspaper reported. The hacker group NoName, which previously claimed credit for DDoS attacks across Europe, the U.S. and Ukraine, said it picked the latest target as the Netherlands because it had sent Ukraine 6 billion euros in military assistance. 'It's time to visit the Netherlands again and remind you how the help of the Kyiv regime ends,' NoName wrote on Telegram Monday. Cybersecurity experts say NoName hackers target between five and 15 websites per day for a greater impact of DDoS attacks, which frustrate users but otherwise do not steal information or compromise critical infrastructure, according to the NL Times.
5. <https://www.radware.com/cyberpedia/ddos-attacks/noname057%2816%29/> - NoName057(16) is a pro-Russian hacker group that is known for its cyberattacks on Ukrainian, American, and European websites of government agencies, media, and private companies. It is regarded as an unorganized and free pro-Russian activist group seeking to attract attention in Western countries. NoName057(16) operates using Telegram channels where they claim responsibility for their attacks, mock targets, make threats, and share educational content.
6. <https://www.nltimes.nl/2023/06/20/zeeland-port-website-hit-ddos-attack-possibly-russian-hackers> - A DDoS attack took down the North Sea Port website, the company that operates the ports of Vlissingen and Terneuzen in Zeeland, and the Gent port in Belgium. The website was inaccessible for several hours, starting at 8:30 a.m. on Tuesday. By early afternoon, the attack had been repelled, and the site was up and running again. Work in the port continued as usual, those systems were not affected. North Sea Port confirmed the attack. Russian hackers claimed responsibility, but the port authority would not comment on that, saying they were not in a position to provide information about the attackers. Cybersecurity firm FalconFeeds.io said the site may have been attacked by NoName05716, a relatively unknown hacker group. These hacktivists regularly carry out digital attacks on those they consider to be opponents of Russia.
7. <https://www.nltimes.nl/2023/11/04/russian-hackers-attack-public-transport-chip-card-website-temporarily-inaccessible> - The website of public transport chip card (OV chip card) company Translink is unavailable on Saturday due to a DDoS attack (Distributed Denial of Service), according to a spokesperson for the public transport chip card company. In the attack, the computer systems are bombarded with data traffic until they can no longer cope and collapse. 'There is a DDoS attack, which means that the website is temporarily inaccessible. There was an initial attack yesterday, which we were able to fend off with appropriate measures,' said the spokesperson. However, travelers can check in and out as usual using their chip cards. Translink hopes that the problem will be resolved in the course of the afternoon. The attack was claimed by the pro-Russian hacktivist group NoName05716, which attacks Dutch organizations in retaliation for supporting Ukraine in the war with Russia. It is not the first time that Dutch companies or institutions have been attacked by the Russian hacker group. In the spring of this year, the Dutch government website and the website of the Dutch court system, Rechtspraak.nl, were subject to cyberattacks.