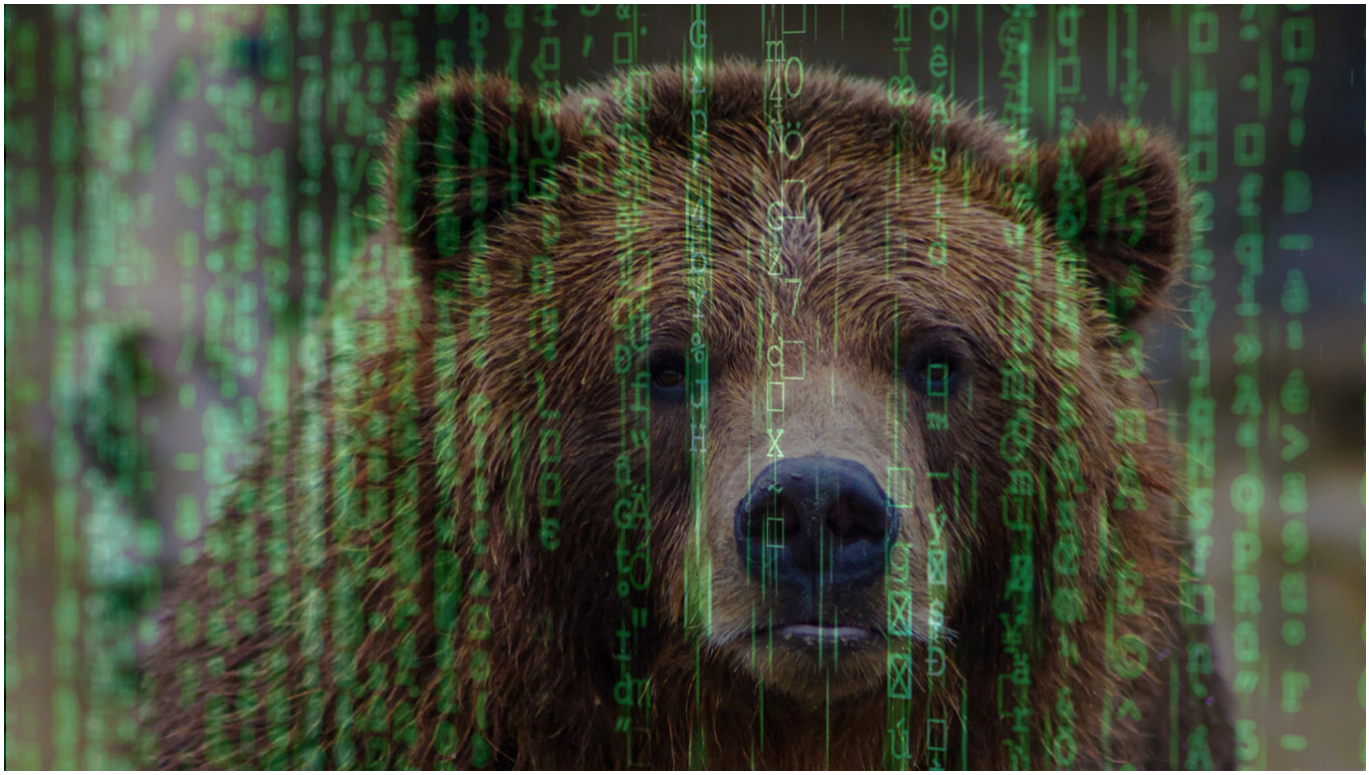
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Pro-Russian Hacker Group Gamifies Cyberattacks on Europe With Crypto Rewards – Investigation

April 29, 2026



Markus Spiske, becca / unsplash

A pro-Russian hacker group accused by European authorities of carrying out cyberattacks against governments, banks and infrastructure across the West has turned participation in cybercrime into what it calls a "patriotic online game," recruiting volunteers through Telegram and rewarding them with cryptocurrency.

The group, NoName057(16), has claimed responsibility for waves of distributed denial-of-service (DDoS) attacks on public institutions and private companies across Europe since Russia's full-scale invasion of Ukraine in 2022. Western intelligence agencies and Europol say the hackers function as part of Russia's broader hybrid war against countries supporting Kyiv.

An investigation by the Poland-based news outlet Vot Tak, conducted with cybersecurity experts from RKS.Global, found that the group's activity has not diminished despite a major Europol-led crackdown in July 2025 known as Operation Eastwood.

Instead, the number of attack commands sent to its network of infected devices increased in the months afterward.

The findings underscore how difficult it is for law enforcement to dismantle decentralized cyber groups that rely on ideology, small financial incentives and thousands of ordinary users turning their own devices into attack tools.

One of the group's most visible campaigns came during Denmark's municipal elections in November 2025. Fearing disruptions, local authorities installed backup generators, printed paper voter lists and bought camping lanterns for polling stations in case of outages.

The precautions followed waves of cyberattacks that temporarily disrupted Danish government websites, political parties, municipal administrations, police services, railway operators and a defense company.

Responsibility was claimed by NoName057(16), which had warned in a private channel days earlier that Denmark would be its next target.

The hackers said Denmark was targeted because politicians had increased support for Ukraine during the election campaign.

The attacks were limited to DDoS operations, in which massive volumes of artificial traffic are directed at websites until they become overloaded and stop responding. Such attacks rarely cause permanent damage, but they can disrupt services for hours or days and create significant public alarm.

Most Danish websites were quickly restored and the elections were not disrupted. Still, Denmark's military intelligence service later confirmed NoName057(16) was responsible.

"The Russian state uses the group as a tool of its hybrid war against the West," the intelligence service said. "The goal is to create instability in targeted countries and punish those that support Ukraine."

NoName057(16) first appeared in March 2022, weeks after Russia launched its full-scale invasion of Ukraine.

Initially focused on Ukrainian media and government websites, it later expanded across Europe and beyond, targeting countries that support Kyiv, including the U.S., Canada, Israel and Taiwan.

Its manifesto closely mirrors Kremlin narratives, accusing the West of "russophobia," censorship and support for what it calls "Ukrainian terrorists." The group frames its attacks as retaliation against anti-Russian policies and defense of "traditional values."

In 2026, its campaigns were tied to events including the Milan-Cortina Winter Olympics, new Western military aid packages for Ukraine and the escalation of conflict between Israel and Iran. During the Israeli-Iranian confrontation, the hackers attacked Israeli websites and described their actions as solidarity with Iran, echoing Russian state messaging.

The group's operations rely on software called DDoSia, which experts say is simple enough for

non-specialists to install.

RKS.Global researchers downloaded and analyzed the program for Vot Tak. Available for Windows, Linux, macOS and Android, it can be installed on phones, computers and even routers.

Once installed, the software effectively turns the device into a participant in cybercrime.

Users do not choose targets themselves. NoName057(16) administrators send attack configurations from rented control servers, specifying which domains or IP addresses should be hit. After receiving those instructions, the infected device automatically begins generating traffic against the selected targets.

To join, users contact administrators through a Telegram bot, receive an access key and server address, enter the data into the program and press "Start." From then on, the process is largely automatic.

According to RKS.Global, a single infected device can generate hundreds of thousands or even millions of requests per day. When combined across thousands of devices, the traffic creates serious DDoS threats.

The simplicity of the system has helped NoName057(16) recruit widely.

The group runs a closed Telegram support chat called DDoSia Project, where participants receive technical help, instructions and access to a reward system based on an internal currency called dCoin.

Participants earn dCoins depending on the number of "successful" requests sent during attacks. The more traffic their devices generate, the more they are paid.

For example, 500,000 successful requests per day can earn 50 dCoin. One dCoin is worth 2 rubles, or about 2.4 U.S. cents, and can be converted into the TON cryptocurrency and later into cash.

Users can increase earnings by installing the software on multiple devices or recruiting others through referral links. The system also includes military-style ranks such as private, sergeant and colonel, with the highest level called "General Dosi."

Telegram advertisements promote the project as both easy money and patriotic duty.

Messages reviewed by Vot Tak promised users they could "carry out DDoS attacks and earn money," "learn hacking in 15 minutes" or "help Russia on the information front and get rewarded." They do not mention that DDoS attacks are criminal offenses, including under Russian law.

European authorities launched Operation Eastwood in July 2025 in a coordinated attempt to dismantle NoName057(16) involving 12 countries and coordinated by Europol.

Authorities seized more than 100 servers, carried out 24 searches, issued seven arrest warrants and questioned 13 individuals. Three suspects were arrested in France, Spain and

Poland.

Five Russian citizens were added to Europol's most wanted list. More than 1,000 suspected supporters, including Telegram administrators, also received warnings about criminal liability.

While authorities said they had dismantled the group's infrastructure, data analyzed by Vot Tak and RKS.Global showed the attacks resumed within days and overall activity increased.

The group sent an average of about 6,300 attack commands per month before Eastwood, compared to an average of 7,708 afterward.

In the eight months before the operation, researchers recorded 56,231 attack commands. In the eight months after, from July 2025 to March 2026, they counted 61,666.

From late October 2025 to mid-March 2026, NoName057(16) claimed 1,530 successful operations, about 300 per month.

Related article: Russian Hackers 'Targeting Messaging Apps,' Dutch Spy Agency Says

Vot Tak verified that at least some of those attacks were genuine, with targeted websites temporarily inaccessible. Several affected companies and local administrations also confirmed experiencing DDoS disruptions.

Government websites accounted for nearly one-third of identified targets, according to RKS.Global. Financial institutions, transport and logistics companies, municipalities and telecom operators were also frequent victims.

Germany became one of the group's main targets after Operation Eastwood, with hackers openly describing attacks there as revenge for the crackdown.

Poland was also repeatedly targeted, including ministries, city governments, transport systems, defense contractors and industrial facilities.

Poland's Digital Affairs Ministry told Vot Tak that the real damage remained limited and said such groups often exaggerate their success online to appear more effective than they are.

Europol identifies 39-year-old Mikhail Burlakov and 36-year-old Maxim Lupin as the main coordinators of NoName057(16), accusing them of developing and maintaining DDoSia and paying for the servers used by the network.

Both men are believed to live in Moscow and both hold senior positions at the state-run Center for the Study and Network Monitoring of the Youth Environment (CISM), according to leaked records reviewed by Vot Tak.

Officially, CISM monitors harmful online content such as cyberbullying and criminal subcultures. But Vot Tak previously reported that one of its functions was compiling denunciations against Russians for online comments.

Lupin serves as CISM's general director, while Burlakov is his deputy.

Both men denied involvement.

Burlakov said European authorities had "dragged random people into completely unclear criminal cases" and blamed what he called Western bias and russophobia.

A Telegram account linked to Lupin's phone number also denied knowledge of NoName057(16), calling Europol's accusations "some kind of mistake."

Dismantling groups like NoName057(16) is difficult because they are run by professionals who know how to hide infrastructure, mask IP addresses and quickly restore operations if key members remain free, cybersecurity expert Leonid Yuldashev told Vot Tak.

Still, he said police actions like Operation Eastwood are not meaningless, as they can expose infrastructure, identify devices, provide access to internal communications and disrupt finances.

"It also had symbolic value," Yuldashev said. "It clearly showed the group that it is being targeted."

He said the most effective long-term defense is broader use of DDoS protection systems that filter malicious traffic before it reaches target servers.

Around 80% of websites already have some level of protection, he said, and the remaining 20% remain highly vulnerable.

"That is still a very large number," Yuldashev said. "Attackers can find such resources automatically."

Original url:
https://www.themoscowtimes.com/2026/04/29/pro-russian-hacker-group-gamifies-cyberattacks-on-europe-with-crypto-rewards-investigation-a92634