

Moscow police detain suspected DataSuckers hackers linked to breaches in Ukraine and Russia

By Daryna Antoniuk

Published: 2026-10-16 · Archived: 2026-10-30 02:00:43 UTC

Russian authorities have reportedly detained three suspected members of the DataSuckers hacking group following a [cyberattack](#) on a popular restaurant chain that exposed vast amounts of customer information.

A Moscow court on Wednesday [placed](#) 19-year-old Denis Fridman under house arrest until December 8 in connection with the Dodo Pizza breach, which reportedly involved the theft of records related to hundreds of millions of orders placed over 15 years. He faces charges connected to the illegal handling of computer information containing personal data.

Fridman is one of four alleged members of DataSuckers, a financially motivated hacking group that has claimed responsibility for recent attacks on major businesses in Russia and Ukraine. Two other suspects have been detained while a fourth remains at large, according to Russian newspaper [Kommersant](#) and Telegram news outlet [Baza](#). The suspects reportedly include citizens of Russia, Kazakhstan and Belarus.

According to Baza, police identified the suspected hackers after Fridman accidentally exposed his IP address while accessing data stolen from Dodo Pizza, allowing authorities to trace him to his home in the Russian city of Barnaul.

The attack reportedly began when the hackers discovered Dodo Pizza's corporate credentials exposed on GitHub. Using those credentials, the attackers allegedly gained access to interconnected company systems, including cloud storage and databases, as well as stored passwords.

Kommersant reported that the stolen database was offered for sale on the dark web and that the hackers received \$100,000 for the archive, with the money transferred to a shared cryptocurrency wallet. The wallet's password was reportedly changed after Fridman's arrest.

Recorded Future News could not independently verify the circumstances that led Russian law enforcement to the suspects.

Dodo Pizza, a Russian fast-food chain operating approximately 1,500 restaurants across 28 countries, previously [acknowledged](#) that attackers may have accessed customer information, including names, addresses, phone numbers, email addresses, dates of birth and order details.

Attacks across Russia and Ukraine

DataSuckers has emerged in recent months, claiming responsibility for attacks on major businesses in Russia and Ukraine.

In September, the group claimed responsibility for breaching Russian tour operator Tez Tour, saying it had spent about two weeks inside the company's systems and obtained large amounts of customer information.

The hackers also defaced the company's website. Tez Tour [acknowledged](#) the disruption but disputed claims that customer data had been compromised, saying it had isolated its internal systems before the attackers could access them.

Fridman allegedly participated in that attack, according to Kommersant. The newspaper reported that he had previously targeted Ukrainian websites before joining DataSuckers.

Earlier this month, the group [claimed responsibility](#) for an attack on ATB, Ukraine's largest grocery store chain, demanding \$400,000 and threatening to publish data it claimed to have stolen from millions of customers.

The hackers placed an extortion message and a countdown timer on the retailer's website, which subsequently became unavailable. ATB denied that customer information had been compromised and said it had temporarily taken some online services offline for technical maintenance.

DataSuckers claimed to have obtained records belonging to 7.9 million ATB customers, including names, contact information, addresses and password hashes, as well as employee passport information and more than 11 million order records. Those claims have not been independently verified.

The group describes itself as financially motivated rather than politically aligned. It primarily communicates in Russian and uses a public Telegram channel to announce attacks, publish details of alleged intrusions and invite victims, journalists and law enforcement agencies to contact its members.

In a message posted last weekend, DataSuckers said it was continuing operations but would reduce its public activity.

"We're operating as usual, but you'll be seeing less public activity from us," the group said. "For now, we're focused on specific targets and working on them."

The group has not published any further messages on its Telegram channel since that statement.



Know what matters.

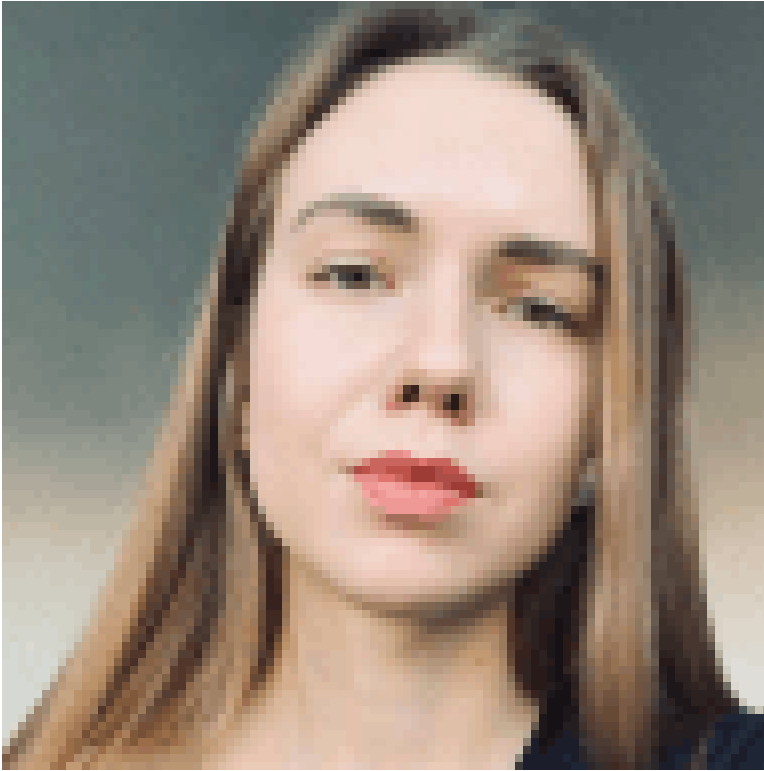
Act first.

Get started



No previous article

No new articles



[Daryna Antoniuk](#)

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.

Source: <https://therecord.media/russia-datasuckers-hackers-arrested>