US indicts Snowflake hackers who extorted $2.5 million from 3 victims

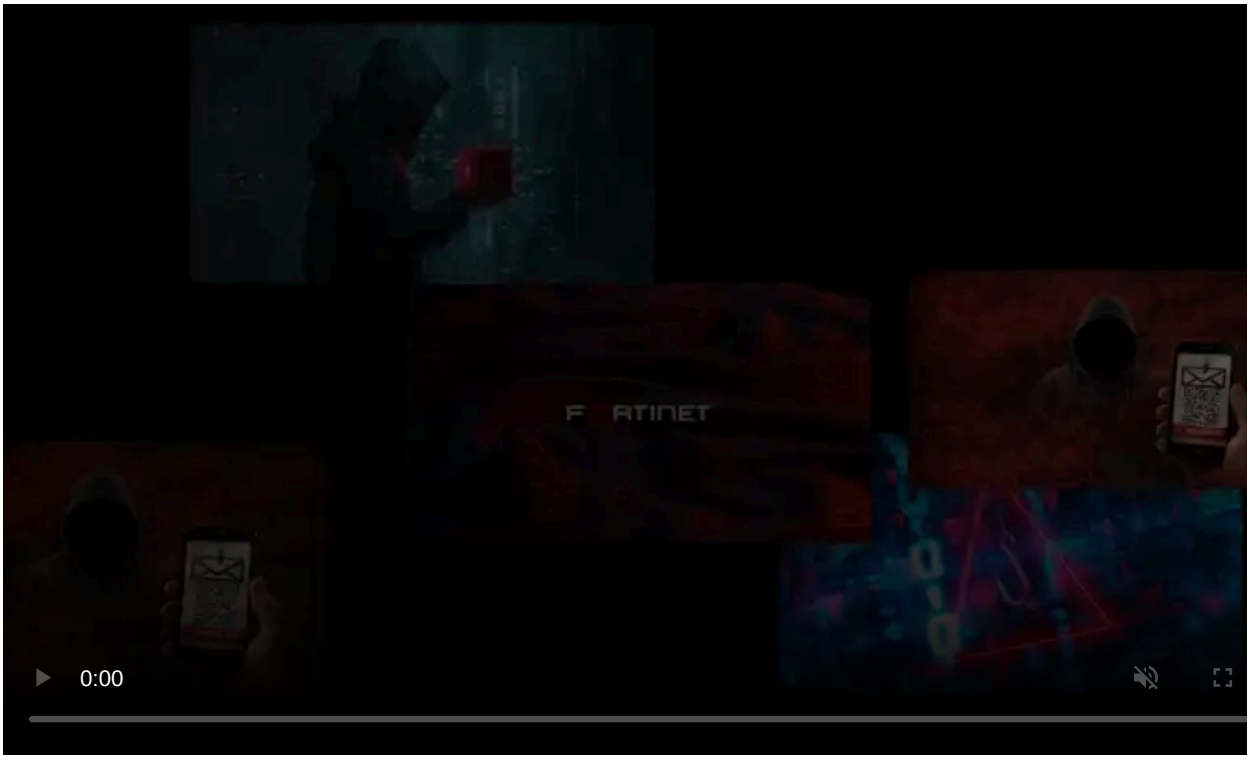
By Bill Toulas

Published: 2024-11-13 · Archived: 2026-04-05 20:35:53 UTC

The U.S. Department of Justice has unsealed the indictment against two suspected Snowflake hackers, who breached more than 165 organizations using the services of the Snowflake cloud storage company.

Connor Riley Moucka and John Erin Binns are accused of using credentials, obtained with the help of info-stealing malware, to hijack Snowflake accounts that were not protected by multi-factor authentication

Moucka and Binns exfiltrated terabytes of data from various companies and demanded ransom payments in exchange for deleting the stolen information.


0:00

According to the indictment, the two hackers stole "approximately 50 billion customer call and text records" from a "major telecommunications" company in the U.S.

One company fitting the profile that suffered a major data breach in the same timeframe as described in the indictment is AT&T.

AT&T disclosed in July that call logs of 109 million customers were exposed during the incident and that the data was accessed from an online database on the company's Snowflake account.

As per the indictment, Moucka and Binns received around mid-May a ransom payment from the telco provider in the form of cryptocurrency.

They tried to hide the source and destination of the funds through "a complex series of cryptocurrency transactions," which included converting the payments into Monero cryptocurrency.

With some victims, the attackers engaged in double extortion, where they tried to get a new ransom payment from a breached company that had already paid the initial demand.

The court document notes that the two hackers and their co-conspirators extorted three victims for at least 36 Bitcoins, or $2.5 million at transaction time.

Apart from AT&T, data breaches linked to Snowflake attacks affected hundreds of millions of individuals, customers of Ticketmaster, Santander, Pure Storage, Advance Auto Parts, Los Angeles Unified, QuoteWizard/LendingTree, and Neiman Marcus.

To make a profit with the data stolen from victims that did not pay the ransom, the hackers advertised it to potential buyers on multiple hacking forums.

Moucka (aka “Waifu” and “Judische”) was arrested in late October 2024 in Canada at the request of the United States, who suspected the man of having masterminded the data theft operation that impacted over 165 organizations.

The other hacker was arrested in Turkey this year in May and his name is John Erin Binns (aka “irdev” and “j_irdev1337”), who in 2021 claimed the major attack on T-Mobile and mocked the company's security in interviews to the media.

The two now face multiple counts for various cybercrime charges, including wire fraud, securities fraud, conspiracy to commit fraud, unauthorized access and breach of computer systems, data theft, and privacy violations.

If convicted, the two could face significant prison sentences, as the announced charges carry from 5 to up to 25 years of imprisonment each, and a total of 60 years.

Additionally, the two will have their assets and proceeds seized by the government, including bank accounts, vehicles, real estate, and any other valuables obtained as a result of the alleged offenses.

Source: https://www.bleepingcomputer.com/news/security/us-indicts-snowflake-hackers-who-extorted-25-million-from-3-victims/