Man Arrested for Snowflake Hacking Spree Faces US Extradition

Matt Burgess, Andy Greenberg ⋮ 6-7 minutes ⋮ 11/5/2024

For much of this summer, a mysterious group of hackers carried out a landmark spree of major data breaches, all targeting customers of the cloud data storage company Snowflake. Now one alleged hacker—whom experts believe to be the ringleader of that group—has been arrested in Canada, and he may be on his way to a US court.

On Monday, Bloomberg and 404 Media reported that a Canadian man named Alexander Moucka, who also goes by the name Connor Moucka, was detained at the end of October on a provisional arrest warrant. Moucka then appeared in a court hearing today, November 5, as part of extradition proceedings, 404 Media first reported.

Under the hacker handles Waifu and Judische, Moucka is believed to be a notorious figure in the cybercriminal underground, says Allison Nixon, a security researcher and the chief research officer at security firm Unit 221B, who has long tracked his online activity. She alludes to Moucka’s alleged hacking activity going back years prior to the Snowflake breaches. “I was waiting for this one,” says Nixon. “Waifu was the leader of a group who was responsible for many major intrusions over the last half decade.”

Suspicious activity linked to Snowflake customer accounts was first spotted in April, according to a June report by Google-owned security company Mandiant, which was employed by Snowflake to jointly investigate the hacking. The first unknown victim’s Snowflake systems had been accessed using login details that were previously taken by infostealer malware, the report says. Over the next couple of chaotic months more than 165 Snowflake customers, according to Mandiant’s report, potentially had data they stored in Snowflake’s systems exposed or stolen. Hundreds of millions of records from AT&T, Santander, Ticketmaster owner Live Nation Entertainment, and more were accessed in the hacking spree.

Mandiant’s report in June said that the majority of the compromised Snowflake accounts did not have multifactor authentication turned on, and credentials gathered from infostealer logs—some dating back to 2020—were used to access them. Since the breaches, Snowflake has updated its systems to require multifactor authentication to be turned on by default.

A spokesperson for Snowflake tells WIRED it has no comment on the arrest. Ian McLeod, a spokesperson for Canada’s Department of Justice, says Moucka was arrested following a request by the United States. “As extradition requests are considered confidential state-to-state communications, we cannot comment further on this case,” McLeod says.

The cybersecurity firm Mandiant, a subsidiary of Google that has investigated the Snowflake breaches, referred to the hacker behind them as UNC5537, and the company's threat intelligence analyst Austin Larsen describes him in a statement to WIRED as “one of the most consequential threat actors of 2024.”

“The operation, which left organizations reeling from significant data loss and extortion attempts, highlighted the alarming scale of harm a single individual can cause using off-the-shelf tools,” Larsen adds.

While the hacker behind the Waifu and Judische handles has been linked to a Canadian identity for several months, they are believed to not be the only person linked to the Snowflake incidents. As WIRED reported in July, American hacker John Binns was allegedly involved in the Snowflake-related AT&T breach, which saw the company pay out more than $300,000 to have millions of stolen customer records deleted. (Binns was previously arrested in Turkey after the US indicted him for a 2021 breach of T-Mobile). Unit 221B’s Nixon says she’s aware of other members of the cybercriminal gang who remain at large.

According to Nixon, Waifu, now alleged to be Moucka, emerged from a cybercriminal community known as “the Com,” an underground network of young hackers and trolls active on platforms like Telegram and Discord and responsible for hacking and other digital crimes including ransomware, SIM swapping, cryptocurrency theft, sextortion, and harassment. The ransomware group known as Scattered Spider, which is responsible for highly disruptive extortion attacks against victims including MGM Entertainment and Caesars Entertainment, is among several criminal subgroups linked to the Com. “These are people who treat criminal statutes like a checklist,” says Nixon.

“I know that he’s been in the Com for a very long time, closer to a decade. He clearly spent his former teenage years being part of this culture,” Nixon says of Moucka, whom she says is now in his 20s. “When people grow up in the Com, this is how they turn out.”

As Nixon tracked Waifu and his associates over the past year, she says that he at one point made an operational security or “opsec” slipup that may have led law enforcement to his identity—though she declined to say what that mistake was or exactly when it occurred. Waifu subsequently tried to cover up this accidental reveal with false leads and misinformation posted to Telegram, what he described as “well poison.” But Nixon says law enforcement has nonetheless been aware of Moucka’s identity since at least early July. “If you make an opsec mistake, it’s done. You can’t bury it under a lot of bullshit you post later,” says Nixon. “All it’s accomplished is to show that he knew that what he was doing was wrong.”

While Moucka’s arrest is far from the end of the Com, Nixon says she sees it as a potentially important move in responding to the chaos that the larger criminal network has inflicted. Waifu, she says, was an example of a larger principle she’s observed in the cybercriminal world, that a small minority of criminals are often responsible for the majority of harms.

“This particular case is significant because they’ve picked up one of that tiny minority that causes disproportionate harm,” she says. “That’s why this is a good start. We need to arrest more of these disproportionately harmful actors.”

Updated 3:55 pm EST, November 5, 2024: Added a statement from Mandiant.