Canadian Suspect Arrested Over Snowflake Customer Breach and Extortion Attacks

By The Hacker News

Published: 2024-11-05 · Archived: 2026-04-05 21:29:32 UTC

Canadian law enforcement authorities have arrested an individual who is suspected to have conducted a series of hacks stemming from the breach of cloud data warehousing platform Snowflake earlier this year.

The individual in question, Alexander "Connor" Moucka (aka Judische and Waifu), was apprehended on October 30, 2024, on the basis of a provisional arrest warrant, following a request by the U.S.

The development was first reported by Bloomberg and corroborated by 404 Media. The exact nature of the charges against Moucka is currently not known.

In June 2024, Snowflake disclosed that a "limited number" of its customers were targeted as part of a targeted campaign. Later, Google-owned Mandiant attributed it to a financially motivated threat group called UNC5537.

"UNC5537 comprises members based in North America, and collaborates with an additional member in Turkey," the company assessed with moderate confidence at the time, adding approximately 165 organizations were impacted.

Some of the targeted companies included major corporations such as Advance Auto Parts, AT&T, LendingTree, Neiman Marcus, Santander, and Ticketmaster (Live Nation).

In some of the incidents, the threat actor(s) attempted to extort the companies by threatening to sell the stolen data on criminal forums if they didn't pay up. AT&T reportedly paid the hackers $370,000 to delete the stolen data, according to WIRED.

The attacks worked by leveraging stolen customer credentials obtained via prior stealer malware infections to obtain initial access. The investigation also found that the initial compromise of infostealer malware occurred on contractor systems that were used for downloading games and pirated software.

Reports published by Krebs On Security and 404 Media in September 2024 revealed that Judische is likely based in Canada and has connections to a broader cybercrime ecosystem called the Com, which is known to engage in physical and digital attacks, sometimes resorting to violence, to gain access to accounts and steal funds from rivals.

Judische is also believed to have collaborated with another hacker called John Binns, who was arrested in Turkey in May 2024.

Update

The U.S. Department of Justice has unsealed an indictment accusing Connor Riley Moucka and John Erin Binns of using credentials obtained via information stealers to breach at least 10 Snowflake customers and exfiltrate sensitive data in exchange for ransom payments.

This included "approximately 50 billion customer call and text records" from a "major telecommunications" company in the U.S., court documents said, likely referencing AT&T. The defendants have also been alleged to conceal the money trail by routing the funds through "a complex series of cryptocurrency transactions."

In all, the two hackers are estimated to have extorted three victims for at least 36 bitcoins, valued at roughly $2.5 million at the time of the payment. They also attempted to sell the stolen data, harvested using a tool dubbed Rapeflake, on cybercriminal forums for millions of dollars.

"Through this scheme, the co-conspirators gained unlawful access to billions of sensitive customer records, including individuals' non-content call and text history records, banking and other financial information, payroll records, Drug Enforcement Agency ('DEA') registration numbers, driver's license numbers, passport numbers, Social Security numbers, and other personally identifiable information," it said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2024/11/canadian-suspect-arrested-over.html