Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:00:25 UTC

Other threat group: UNC5537

Names	UNC5537 *(Mandiant)*	
Country	Canada	
Motivation	Financial gain	
First seen	2024	
Description	(Mandiant) Through the course of our incident response engagements and threat intelligence collections, Mandiant has identified a threat campaign targeting Snowflake customer database instances with the intent of data theft and extortion. Snowflake is a multi-cloud data warehousing platform used to store and analyze large amounts of structured and unstructured data. Mandiant tracks this cluster of activity as UNC5537, a financially motivated threat actor suspected to have stolen a significant volume of records from Snowflake customer environments. UNC5537 is systematically compromising Snowflake customer instances using stolen customer credentials, advertising victim data for sale on cybercrime forums, and attempting to extort many of the victims. Mandiant's investigation has not found any evidence to suggest that unauthorized access to Snowflake customer accounts stemmed from a breach of Snowflake's enterprise environment. Instead, every incident Mandiant responded to associated with this campaign was traced back to compromised customer credentials.	
Observed		
Tools used		
Counter operations	Nov 2024	Canadian Suspect Arrested Over Snowflake Customer Breach and Extortion Attacks <https://thehackernews.com/2024/11/canadian-suspect-arrested-over.html>
	Nov 2024	US indicts Snowflake hackers who extorted $2.5 million from 3 victims <https://www.bleepingcomputer.com/news/security/us-indicts-snowflake-hackers-who-extorted-25-million-from-3-victims/>

Information	<https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion> <https://www.bleepingcomputer.com/news/security/pure-storage-confirms-data-breach-after-snowflake-account-hack/> <https://krebsonsecurity.com/2025/02/u-s-soldier-charged-in-att-hack-searched-can-hacking-be-treason/>
Playbook	<https://services.google.com/fh/files/misc/snowflake-threat-hunting-guide.pdf>

Last change to this card: 02 March 2025

Download this actor card in PDF or JSON format
