Threat Intelligence Report

Emerging Threat: Unauthorized Access to Snowflake Customer Accounts Lacking Multi-Factor Authentication

Snowflake, a cloud-based data storage and analytics company, has reportedly observed an increase in cyber threat activity targeting customer accounts. Though investigation is ongoing, Snowflake believes threat actors are leveraging already-stolen customer credentials, likely obtained through previous breaches or infostealer malware infections, to access Snowflake environments lacking multi-factor authentication (MFA).

In May 2024, FTI Cybersecurity responded to suspicious activity within client Snowflake environments and identified unauthorized access and possible data exfiltration in alignment with recent open source reporting. Specifically, FTI Cybersecurity observed threat actors using compromised accounts for initial access, followed by enumeration and potential exfiltration of Snowflake tables containing business-sensitive or otherwise valuable information related to customers and vendors.

THREAT ACTIVITY

Threat actors have been observed utilizing stolen customer credentials to access Snowflake environments, focusing primarily on those lacking MFA. FTI Cybersecurity investigations have corroborated these observations, shedding additional light on threat actor behavior inside the compromised Snowflake environments.

- In a since-deleted report, threat researchers from Hudson Rock, a cybercrime intelligence company, claimed cybercriminal group ShinyHunters obtained Snowflake customer credentials via a compromised Snowflake employee. Though threat actors did in fact obtain credentials to access demo accounts belonging to a former Snowflake employee, Snowflake has stated the demo accounts were not connected to Snowflake production nor corporate systems and therefore did not contain sensitive customer data.
- According to Snowflake communications, Snowflake is investigating unauthorized access attempts against their customers. In the course of their investigation, Snowflake observed malicious traffic originating from remote devices identifying themselves as “rapeflake” and “DBeaver_DBeaverUltimate.”[1] Initial third-party reporting suggested “rapeflake” was a custom attack tool deployed by the threat actors.
- FTI Cybersecurity investigations have identified threat actors using compromised developer accounts to access Snowflake environments. Leveraging the accounts’ widespread permissions, the threat actors enumerated all database schema tables within the Snowflake environment to identify those containing sensitive or otherwise valuable data.
- FTI Cybersecurity observed the threat actors running targeted SQL queries to return sensitive data from the relevant tables, once identified.

THREAT ASSESSMENT

FTI Cybersecurity assesses threat actors will continue unauthorized access attempts using harvested or stolen Snowflake credentials, likely in an effort to gain access to sensitive data and extort victim entities for profit.

RECOMMENDED ACTION

- Reset and rotate Snowflake credentials.
- Enable and enforce multi-factor authentication on all accounts.
- Configure Network Policy Rules to block non-authorized users and traffic from untrusted locations.
- Query Snowflake logs for traffic originating from suspected IP addresses and disable the accounts for any affiliated users, if deemed suspicious.
- Conduct a thorough dark web assessment to identify any leaked or stolen employee credentials that could be used to access Snowflake environments.

[1] See this Snowflake community post for an updated list of IP addresses under investigation.

SOURCES

Sources include open-source information from public and private industry reporting.

- CISA: Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access
- Snowflake Forums: Detecting and Preventing Unauthorized User Access
- Snowflake Knowledge Base Articles: Detecting and Preventing Unauthorized User Access: Instructions

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

AMERICAS

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI CONSULTING