Report on the Snowflake Data Breach Incident

Kirk Turner

Department of Cybersecurity, Old Dominion University

CS462: Cybersecurity Fundamentals

Professor Susan Zehra

November 23, 2025

In these past few decades, technology has advanced at an accelerated rate, with new breakthroughs being introduced to the world sooner than the last. Although new forms of technology can heighten efficiency and provide security for businesses and consumers alike, they also open the door for new vulnerabilities to be identified and exploited by malicious actors. Therefore, it's safe to say that a positive correlation can be labeled onto technology and cyberattacks, wherein as technology continues to be built upon and released to the public, new vulnerabilities and methods of attacking that take advantage of these new forms of technology will also be introduced to the world. One such example of a cyberattack that occurred recently is the Snowflake data breach that took place in April of 2024. The intent of this attack was one of stealing personal user data to sell on hacker forums while also attempting to extort money from the victims of this incident. This paper will cover how this attack took place, what the attacker was targeting, the impact this attack held on society, and the overall resolution after this attack occurred.

To begin, let's discuss what Snowflake is in order to understand how this attack was able to succeed. Snowflake is a cloud-based data platform that is developed upon Amazon Web Services, Microsoft Azure, and Google Cloud infrastructure (Naryan, 2024). It is used by customers to store, analyze, and share large sets of data across several independent layers for storage, computing, and managing resources (Google, 2024). The Snowflake software service is one where users must input login credentials each time they need to access their data stored within the Snowflake database. This factor is the root of this cyber incident as the security protocols surrounding the digital Snowflake environment were not originally breached by the attacker, rather login credentials were gathered by the attacker on the user end, and then used to gain access to users' personal Snowflake databases. The attacker collected various user credentials through the use of a malware technology known as an infostealer (Cloud Security, 2025).

An infostealer is a malicious software that collects data from an infected device and transmits it back to the attacker. This type of malware is commonly transmitted to a device through malicious attachments sent to a user typically in the form of a spam message or fake email (Info Stealers, 2023). Once the malware has been installed onto the device, it can utilize a range of methods to gather data, such as keylogging to record the keystrokes of a user, accessing the users saved passwords within the system and cookies, using malicious scripts to alter a web page in order to collect additional information, etc (Info Stealers, 2023). For types of malware that gather user data, it's critical to preemptively identify them before any credentials can be captured, otherwise user accounts and any associated information will most likely become compromised and require deactivation.

Once the credentials had been gathered by the attacker who conducted the Snowflake breach, they began sifting through the databases associated with the compromised accounts in order to find any data of high value. After locating any valuable data, the attacker could then exfiltrate the information and post it for sale online or extort the original owner of the stolen information for money. This incident can be associated to several vulnerabilities that the attacker was able to take advantage of: a portion of the stolen credentials were unupdated or reused by the user, many of the compromised accounts had not utilized multi-factor authentication (MFA) which made accessing the accounts much easier for the attacker, a lack of user awareness when it came to accessing the malicious links of the infostealer, and the impacted accounts did not utilize network allow lists which would have only allowed access to a user account if they attempt to access it from a certain location (Google, 2024).

These vulnerabilities certainly contributed to the success of this attack because the attacker was able to identify them with ease and exploit them to gain access to the confidential data that was stolen. Factors that would have helped to address these vulnerabilities and mitigate this incident altogether could include several policies and procedures on the end users' side of things. First, a thorough credential policy could have been implemented by the

companies associated with the compromised accounts. This policy would need to define the complexity requirements of user passwords in order to ensure that they are suitable passwords that are not easily cracked or obtained by attackers. Also, the credential policy should include a portion detailing how often a user's password credentials should be changed or updated; according to an article posted by McAfee (2024), cybersecurity experts state that for a password to be considered secure, it should be updated at least every three months. A section of this policy should require that all users must utilize multi-factor authentication as an extra security layer for user accounts. In the case of this cyber attack, the attacker was able to access accounts with only the login credentials, however, if the customer accounts had MFA enabled, the attacker would need to bypass an additional authentication step in order to gain access to the Snowflake accounts. Further, employee training procedures should be a regular exercise in the workplace in order to ensure that employees are aware of social engineering tactics that are commonly used by threat actors. These procedures could include random social engineering attacks sent to employees by an administrator to test their thought process and actions, training employees to be skeptical of any messages or emails they aren't expecting, and define where an employee should report any suspicious activity or content they encounter (SecurityMetrics, n.d.). Altogether, approximately 165 organizations had been potentially exposed to a data breach associated with this attack on Snowflake databases (Google, 2024). If the proper security measures had been implemented within each of these companies, then a large portion of this attack could have been mitigated as the attacker would have been less likely to gain the login credentials.

This data breach incurred serious impacts on today's society. Due to the increasing volume of cyber attacks that take place in the modern digital landscape, this significant attack only further fueled the public anxiety associated with malicious cyber incidents. According to an article posted by True Security Company (2025), this attack resulted in billions of records being leaked from multiple organizations who had accounts with Snowflake. Some of the more well

known organizations who suffered from this attack include AT&T, TicketMaster, and Sandtander. When large companies incur serious financial and reputational losses from cyber attacks like this one, it sends a message that if large corporations such as these can be victims to these kinds of attacks, then it's possible that anyone could find themself in the position of the victims of this attack. Additionally, the public trust placed in the companies that were targeted by this attack had certainly faltered in the aftermath of this attack. People began to question the methods of data privacy and protection used by these victim companies since their data was so easily obtained and leaked by the attacker. This can cause a change in how consumers interact with these organizations and affect the overall volume of business opportunities that is normal for these companies.

In summary, this attack was one of critical implications as there were over one hundred victim companies that took serious economic and reputational tolls. Although Snowflake databases were the desired targets in this scenario, attacks like these are relatively common in the present-day online environment. If anything, this attack highlights how anyone can be at risk of data breaches and extortion when the proper vulnerabilities are taken advantage of. Just by adding simple security measures, such as strong password creation and management, utilizing multi-factor authentication, and constantly practicing responsible cyber hygiene tactics like remaining aware of suspicious links or messages, then a person or entity significantly decreases the risk that they will suffer from a targeted cyber attack similar to the 2024 Snowflake data breach.

References:

Cloud Data Exfiltration & Data extortion: Overview and analysis of the ticketmaster and santander incidents. True Security Company. (2025, October 13). https://truesecco.com/en/cloud-data-exfiltration-data-extortion-overview-and-analysis-of-the-ticketmaster-and-santander-incidents/

Cloud Security Alliance. (2025, May 7). *Unpacking the 2024 Snowflake data breach*. Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2025/05/07/unpacking-the-2024-snowflake-data-breach#

Google. (2024, June 10). *UNC5537 targets snowflake customer instances for data theft and extortion* . Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

Info stealers. (2023, October 30). Malwarebytes. https://www.malwarebytes.com/blog/threats/info-stealers

McAfee. (2024). *How often should you change your passwords?*. McAfee. https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/

Narayan, P. (2024, March 21). *What is the snowflake data platform?* . SnapLogic. https://www.snaplogic.com/blog/snowflake-data-platform

SecurityMetrics. (n.d.). *Social engineering training: what your employees should know*. SecurityMetrics. https://www.securitymetrics.com/blog/social-engineering-training-what-your-employees-should-know