ICE
TRUSTED IT PARTNER

ICE’S DATA BREACH CASE STUDIES

Snowflake

The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever

A cyberattack targeting Snowflake's cloud storage clients could become one of the largest data breaches in history. Recently, Snowflake disclosed that malicious hackers had been trying to breach customer accounts using stolen login credentials. Similar attacks on Ticketmaster and Santander have been connected to these incidents.

Since Snowflake initially reported a "limited number" of customer accounts being accessed, cybercriminals have since publicly declared selling data stolen from two other prominent firms, claiming it originated from Snowflake accounts. Concurrently, TechCrunch disclosed that hundreds of Snowflake customer passwords have surfaced online, posing a risk for cybercriminals to exploit.

Amid the claims, uncertainty lingers regarding the extent and magnitude of the attempted attack on Snowflake customers, the identity of the attackers, and the operation of a malicious tool dubbed “rapeflake.” This situation emphasizes the increasing prevalence of infostealer malware in recent years and underscores the importance for third-party software providers and companies to enable multifactor authentication to diminish the risk of account compromise.

SNOWBALLING

A significant portion of the Snowflake controversy has unfolded on the well-known cybercrime platform BreachForums. While the FBI took down the forum in mid-May, a new iteration swiftly emerged. The group behind it, identified as the hacker collective ShinyHunters, boasted about selling 560 million records from Ticketmaster and 30 million from Santander. Both companies acknowledged data breaches, with Ticketmaster explicitly linking its incident to Snowflake, whereas Santander reported unauthorized access to a database "managed by a third-party provider." However, neither company has disclosed the scale of the breaches.

Recently, an account on BreachForums under the alias Sp1d3r highlighted two additional companies allegedly connected to the Snowflake event: the automotive giant Advance Auto Parts, supposedly with 380 million customer records, and the financial services firm LendingTree along with its subsidiary QuoteWizard, with purported data on 190 million individuals.

Some of the email addresses for Advance Auto Parts staff and customers in the hacker's sample data seem legitimate; emails sent by WIRED to those addresses were successfully delivered. BleepingComputer confirmed the authenticity of customer data from Advance Auto Parts.

“We are aware of reports that Advance may be involved in a security incident related to Snowflake,” Darryl Carr, a spokesperson from the company, tells WIRED. “We are investigating the matter and do not have further information to share at this time. We have not experienced any impact to our operations or systems.”

LendingTree and Advance Auto Parts have not yet submitted breach notifications to the Securities and Exchange Commission as of the current moment. Snowflake has previously identified both companies as its customers.

A LendingTree representative confirmed to WIRED that the company utilizes Snowflake for its business operations. The spokesperson stated that the company was informed that its QuoteWizard subsidiary might have been affected by the incident. An internal investigation by LendingTree is currently underway. The spokesperson reassured that at present, there seems to be no compromise in consumer financial account details or information pertaining to LendingTree.

Snowflake has acknowledged that certain accounts were targeted and has since provided additional details regarding the incident. Brad Jones, Snowflake’s chief information security officer, explained in a blog post that threat actors utilized login credentials from accounts that had either been "purchased or obtained through infostealing malware." This malicious software is crafted to extract usernames and passwords from compromised devices. The incident seems to have been a "targeted campaign aimed at users relying on single-factor authentication," according to Jones.

In his post, Jones mentioned that Snowflake, along with cybersecurity firms CrowdStrike and Mandiant—hired to investigate the matter—did not uncover any proof indicating that the breach resulted from "compromised credentials of current or former Snowflake staff." Nevertheless, it was discovered that demo accounts of a former employee had been accessed; fortunately, these accounts did not contain sensitive information.

When asked about possible data breaches in certain companies, a representative from Snowflake cited Jones' statement: "We have not found any evidence indicating that this activity resulted from a vulnerability, misconfiguration, or breach in Snowflake's platform." In a subsequent statement, the company further clarified their definition of a breach: "Any instances of our customers' accounts being accessed due to leaked credentials are not attributable to Snowflake," as stated by a spokesperson.

The US Cybersecurity and Infrastructure Security Agency has raised an alert concerning the Snowflake incident. Additionally, Australia's Cyber Security Center has confirmed "successful compromises of multiple companies leveraging Snowflake environments."

UNCLEAR ORIGINS

Limited information exists about the Sp1d3r account advertising data on BreachForums. It remains unclear whether ShinyHunters sourced the data they were selling from an alternate origin or obtained it directly from victims' Snowflake accounts. Initially, details of a Ticketmaster and Santander breach surfaced on a different cybercrime forum through a novel user named SpidermanData.

The Sp1d3r account shared on BreachForums that 2 terabytes of purported LendingTree and QuoteWizard data were up for sale at $2 million. Additionally, 3 TB of data reportedly from Advance Auto Parts was priced at $1.5 million.. “The price set by the threat actor appears extremely high for a typical listing posted to BreachForums,” says Chris Morgan, a senior cyber-threat intelligence analyst at security firm ReliaQuest.

Morgan questions the legitimacy of Sp1d3r, noting a potential link to the teenage hacking group Scattered Spider. He highlights that the threat actor's profile picture originates from an article mentioning the group, raising uncertainty about any deliberate connection between them.

Though the precise origin of the purported data breaches remains uncertain, the event underscores the intricate interdependence among companies that depend on offerings from

third-party providers. “I think a lot of this is just a recognition of how interdependent these services now are and how hard it is to control the security posture of third parties,” security researcher Tory Hunt told WIRED when the incidents first emerged.

In response to the attacks, Snowflake has advised all customers to ensure they implement multifactor authentication on all accounts and permit traffic solely from authorized users or locations. Companies affected should also reset their Snowflake login details. The utilization of multifactor authentication significantly minimizes the risk of online account breaches. According to a recent TechCrunch report, there have been instances of "hundreds of alleged Snowflake customer credentials" being compromised by infostealing malware from devices of individuals who accessed Snowflake accounts.

Amid the surge in remote work due to the Covid-19 pandemic, there has been a notable uptick in infostealer malware usage. Ian Gray, VP of Intelligence at Flashpoint, notes that the popularity of infostealers is on the rise due to their high demand and relative ease of creation. Hackers are observed to duplicate or alter existing infostealers, offering them for as little as $10 to obtain login details, cookies, files, and more from a single compromised device.

"This malware can be distributed through various methods targeting critical information such as browser data (cookies and credentials), credit card details, and cryptocurrency wallets,"
Gray explains. "Hackers may search through logs to obtain enterprise credentials and illicitly access accounts."

Protecting your business from becoming the next news headline!

ICE Consulting has served as a Managed Cybersecurity Provider for more than 26 years.
Our expertise lies in enhancing businesses' security stance and delivering a range of cybersecurity services including:

1. Security Operation as a Service (24x7 real time cyber threat monitoring and response services)
2. Incident Response Planning
3. Security & Network Vulnerability Scans
4. Penetration Testing
5. Cybersecurity Training

As data breaches reach record levels and show no signs of slowing down, it's crucial for every business to regularly evaluate its security stance for weaknesses. We offer this service at no charge to businesses. Reach out today to discover more about this process.

AICPA SOC 2 CERTIFIED

ICE Consulting, Inc
Managed Cybersecurity Provider

ICE
TRUSTED IT PARTNER

888-423-4801

info@iceconsulting.com

www.iceconsulting.com