Pure Storage confirms data breach after Snowflake account hack

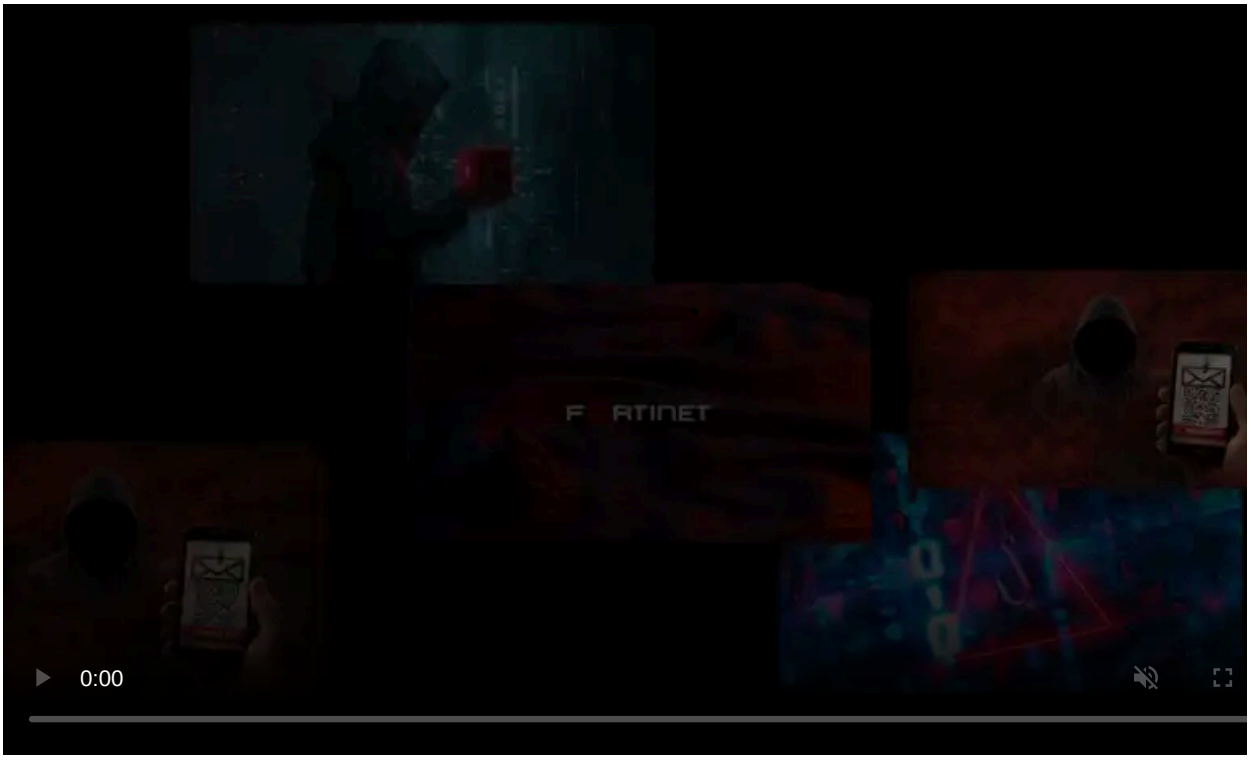
By Sergiu Gatlan

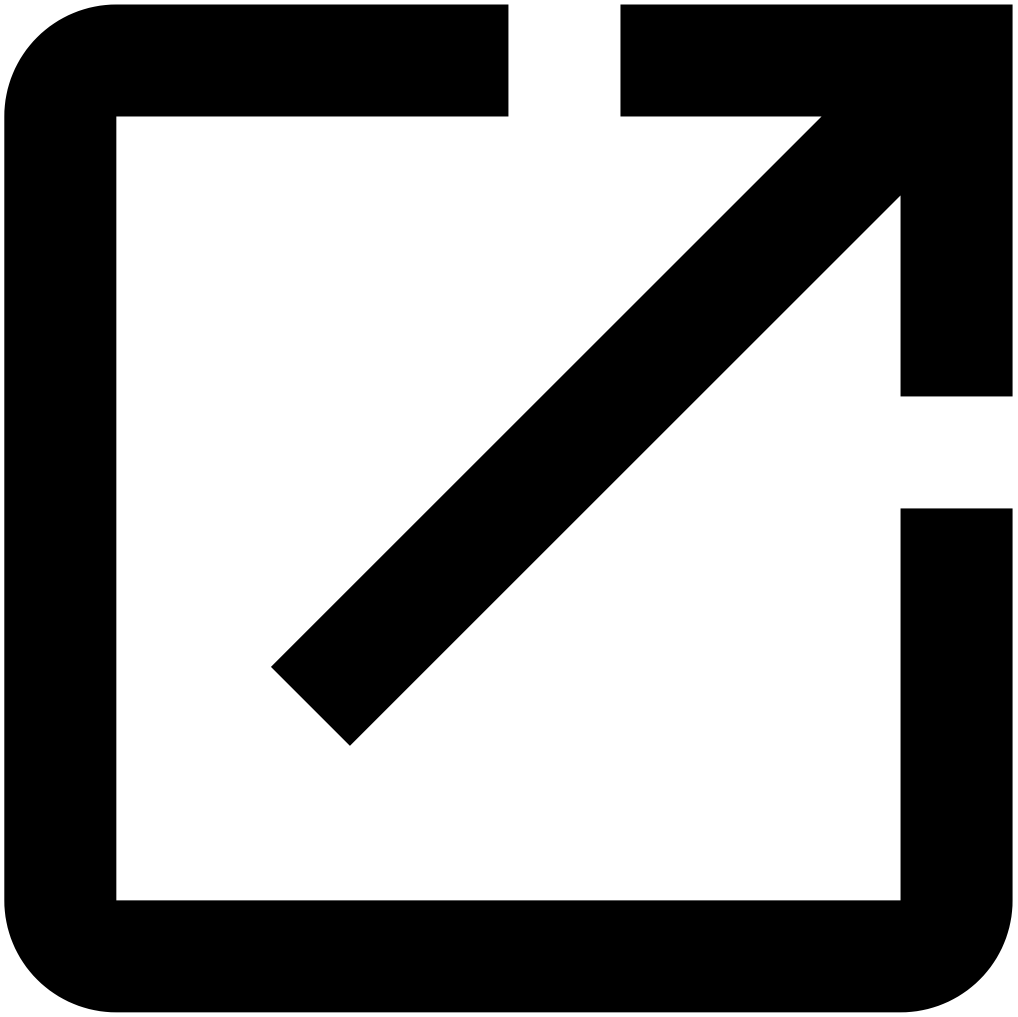
Published: 2024-06-11 · Archived: 2026-04-05 21:51:39 UTC

Pure Storage, a leading provider of cloud storage systems and services, confirmed on Monday that attackers breached its Snowflake workspace and gained access to what the company describes as telemetry information.

While the exposed information also included customer names, usernames, and email addresses, it did not contain credentials for array access or any other data stored on customer systems.

"Following a thorough investigation, Pure Storage has confirmed and addressed a security incident involving a third party that had temporarily gained unauthorized access to a single Snowflake data analytics workspace," the storage company said.


F RTINET
0:00



"The workspace contained telemetry information that Pure uses to provide proactive customer support services. That information includes company names, LDAP usernames, email addresses, and the Purity software release version number."

Pure took measures to prevent further unauthorized access to its Snowflake workspace and has yet to find evidence of malicious activity on other parts of its customer infrastructure.

"We are currently in contact with customers who similarly have not detected unusual activity targeting their Pure systems," the company added.

More than 11,000 customers use Pure Storage's data storage platform, including high-profile companies and organizations like Meta, Ford, JP Morgan, NASA, NTT, AutoNation, Equinix, and Comcast.

At least 165 orgs likely impacted by Snowflake attacks

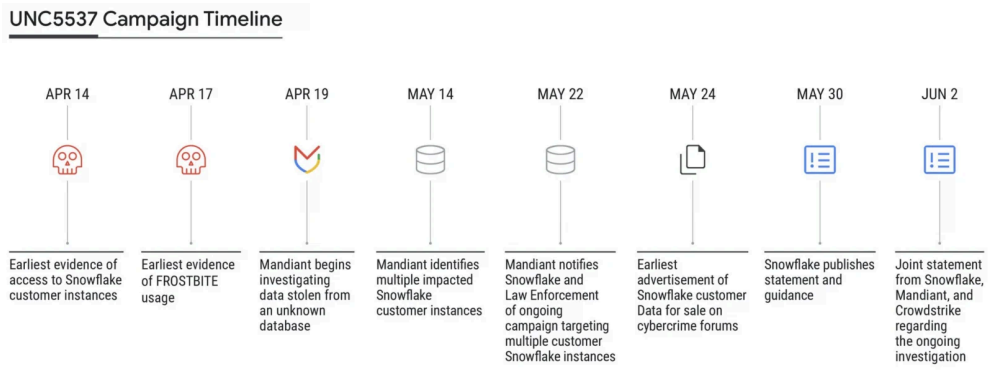
In a joint advisory with Mandiant and CrowdStrike, Snowflake revealed that attackers use stolen customer credentials to target accounts lacking multi-factor authentication protection.

Mandiant also linked the Snowflake attacks to a financially motivated threat actor tracked as UNC5537 since May 2024.

The malicious actor gains access to Snowflake customer accounts using customer credentials stolen in historical infostealer malware infections dating back to 2020, targeting hundreds of organizations worldwide and extorting victims for financial gain.

"The impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password," Mandiant said.

"Credentials identified in infostealer malware output were still valid, in some cases years after they were stolen, and had not been rotated or updated. The impacted Snowflake customer instances did not have network allow lists in place to only allow access from trusted locations."



UNC5537 Snowflake attack timeline (Mandiant)

So far, the cybersecurity company has identified hundreds of customer Snowflake credentials exposed in Vidar, RisePro, Redline, Racoon Stealer, Lumm, and Metastealer infostealer malware attacks.

Snowflake and Mandiant have already notified around 165 organizations potentially exposed to these ongoing attacks.

While Mandiant has not disclosed much information about UNC5537, BleepingComputer has learned that they are part of a larger community of threat actors who frequently visit the same websites, Telegram and Discord servers, where they regularly collaborate on attacks.

Recent breaches at Santander, Ticketmaster, and QuoteWizard/LendingTree have also been linked to these ongoing Snowflake attacks. Ticketmaster's parent company, Live Nation, confirmed that a data breach affected the ticketing firmafter its Snowflake account was compromised on May 20.

A threat actor is now selling 3TB of data from automotive aftermarket parts provider Advance Auto Parts, allegedly including 380 million customer profiles and 44 million Loyalty / Gas card numbers (with customer details), stolen after the company's Snowflake account was breached.

Source: https://www.bleepingcomputer.com/news/security/pure-storage-confirms-data-breach-after-snowflake-account-hack/