Neiman Marcus confirms data breach after Snowflake account hack

By **Lawrence Abrams**

June 25, 2024 10:43 AM 0

Luxury retailer Neiman Marcus confirmed it suffered a data breach after hackers attempted to sell the company's database stolen in recent Snowflake data theft attacks.

In a data breach notification filed with the Office of the Maine Attorney General, the company says that the breach impacted 64,472 people.

"In May 2024, we learned that, between April and May 2024, an unauthorized third party gained access to a database platform used by Neiman Marcus Group. Based on our investigation, the unauthorized third party obtained certain personal information stored in the database platform," warns Neiman Marcus in a data breach notification.

"The types of personal information affected varied by individual, and included information such as name, contact information, date of birth, and Neiman Marcus or

Bergdorf Goodman gift card number(s) (without gift card PINs)."

Neiman Marcus said they disabled access to the database platform when the breach was detected, investigated with cybersecurity experts, and notified law enforcement.

While gift card numbers for Neiman Marcus and Bergdorf Goodman were exposed in the breach, the data did not include PINs, so the gift cards should still be valid.

In a statement to BleepingComputer, Neiman Marcus confirmed that the data was stolen from their Snowflake account.

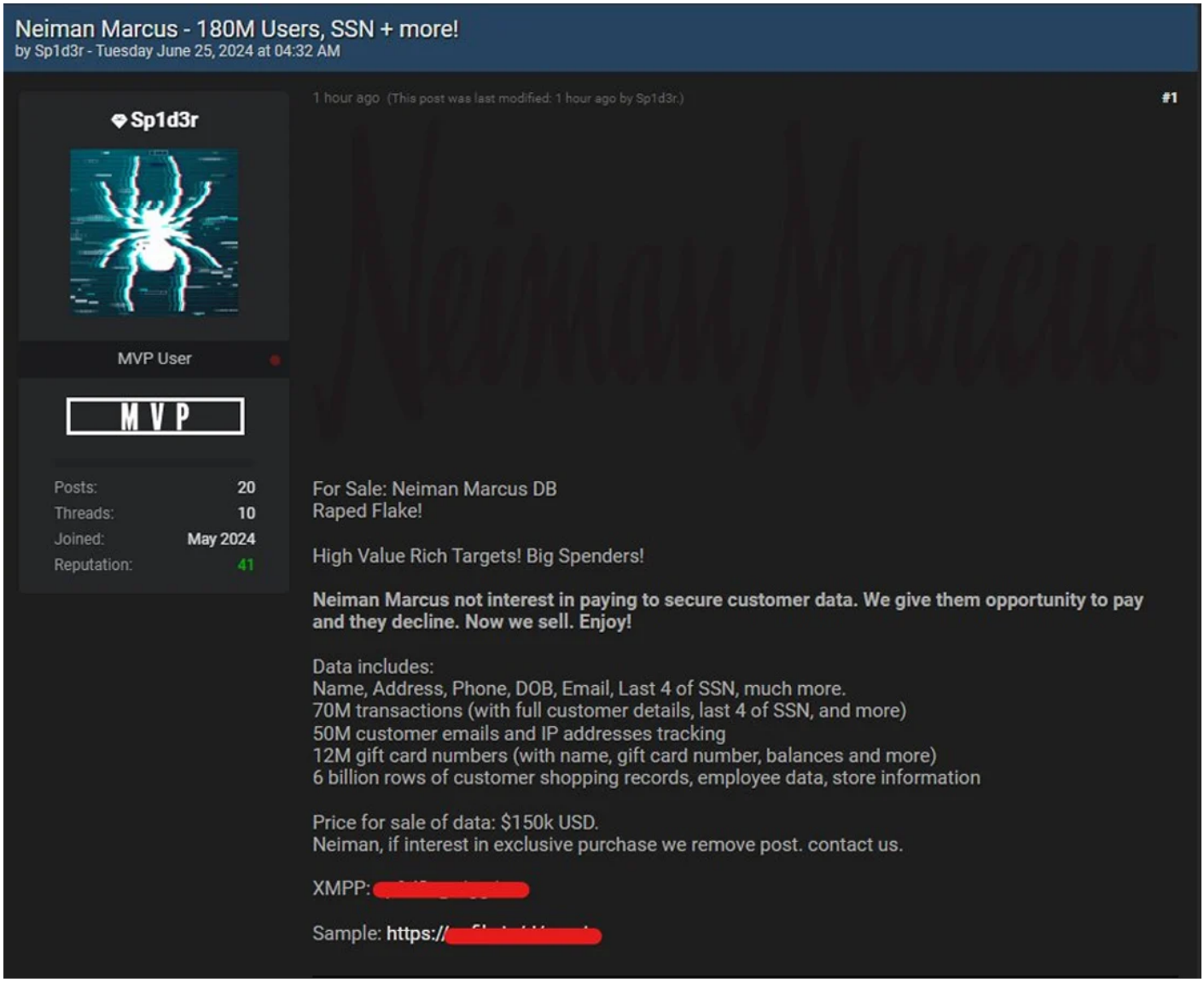
"Neiman Marcus Group (NMG) recently learned that an unauthorized party gained access to a cloud database platform used by NMG that is provided by a third party, Snowflake," the Neiman Marcus Group told BleepingComputer.

Linked to Snowflake data theft attacks

The data breach notifications come after a threat actor named "Sp1d3r" put Neiman Marcus' data up for sale on a hacking forum for $150,000, as first shared by HackManac.

This threat actor is behind the sale of data for numerous companies breached in the recent Snowflake data theft attacks.

While the threat actor did not mention Snowflake in the post, they included "Raped Flake,", which is in reference to a custom tool of the same name the threat actors created to steal data from the database platform.



Neiman Marcus data for sale on a hacking forum

Source: HacManac

According to the threat actor, the stolen data included what Neiman Marcus shared, plus the last four digits of social security numbers, customer transactions, customer emails, shopping records, employee data, and millions of gift card numbers.

The threat actor claims to have attempted to extort the company before the forum posting, stating that the company refused to pay an extortion demand.

However, soon after the post was made on the forum, it was subsequently taken down along with the data sample, indicating that the company may have begun negotiating with the threat actors.

165 orgs likely impacted by Snowflake attacks

A joint investigation by SnowFlake, Mandiant, and CrowdStrike revealed that a threat actor, tracked as UNC5537, used stolen customer credentials to target at least 165

organizations that had not configured multi-factor authentication protection on their accounts.

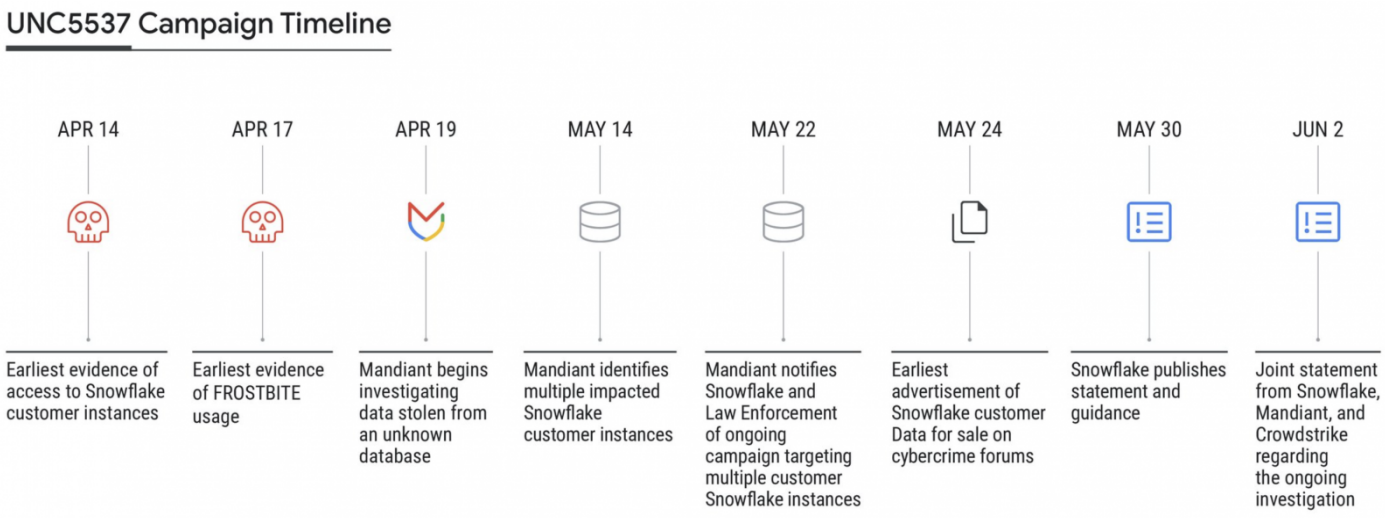
Mandiant also linked the Snowflake attacks to a financially motivated threat actor tracked as UNC5537 since May 2024. This threat actor is known for breaching organizations, stealing data, and attempting to extort companies into paying a ransom for the data not to be published or leaked to other threat actors.

While Mandiant has not publicly disclosed much information about UNC5537, BleepingComputer has learned they are part of a community of threat actors who frequently visit the same websites, Telegram and Discord servers.

To breach Snowflake accounts, the threat actor used credentials stolen by information-stealing malware infections dating back to 2020.

"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

Source: Mandiant

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

Recent breaches linked to these attacks include Santander, Ticketmaster, QuoteWizard/LendingTree, Advance Auto Parts, Los Angeles Unified, and Pure Storage.

DATA BREACH | GIFT CARDS | HACKING FORUM | NEIMAN MARCUS | PERSONAL INFORMATION | SNOWFLAKE

LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE

NEXT ARTICLE