Published on *The National Law Review* https://natlawreview.com

Update on Snowflake Cyber Threat

Article By:

Linn F. Freedman

On June 2, 2024, cloud service provider Snowflake reported increased cyber threat activity targeting some of its customer's accounts. Snowflake recommended that customers review unusual activity to detect and prevent unauthorized user access.

The Cybersecurity and Infrastructure Agency (CISA) then sent an alert on June 3, 2024, recommending that Snowflake customers "hunt for malicious activity, report positive findings to CISA, and review the Snowflake notice" on steps to take.

On June 10, 2024, Mandiant provided additional information about the incident. If you are a Snowflake user, the Mandiant Alert is a mandatory read. According to Mandiant, it identified a campaign by threat actor UNC5537, targeting "Snowflake database instances with the intent of data theft and extortion." The threat actor is suspected of having stolen records from Snowflake customers using stolen customer credentials and subsequently advertised the sale of customer data attempting to extort Snowflake customers. Mandiant has not found any evidence of a breach of Snowflake's environment, but instead, the incidents stemmed from stolen customer credentials to access Snowflake's system, in one instance, using infostealer malware. The credentials used by the threat actor were "available from historical infostealer infections, some of which data as far back as 2020."

The three factors that allowed a successful compromise included:

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

2. Credentials identified in infostealer malware output were still valid, in some cases years after they were stolen, and had not been rotated or updated.

3. The impacted Snowflake customer instances did not have network allow lists in place to only allow access from trusted locations.

Snowflake users may wish to confirm that these three factors are not applicable to them, and if so, take measures to address them.

According to Mandiant, it and Snowflake have notified 165 "potentially exposed organizations," and

Snowflake is working with customers to mitigate a potential compromise.

Google/Mandiant provided a helpful threat intelligence collection of indicators of compromise, which is worth a scan.

National Law Review, Volume XIV, Number 166