Cylance confirms data breach linked to 'third-party' platform

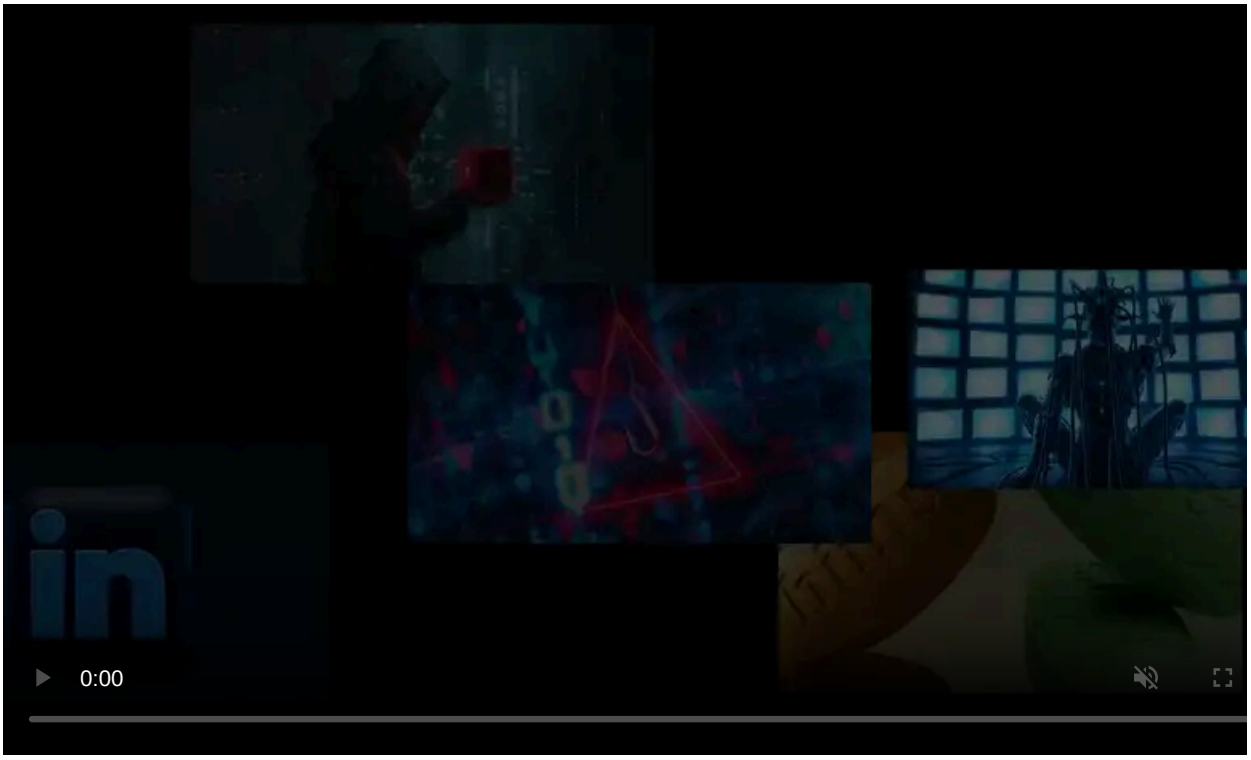
By Sergiu Gatlan

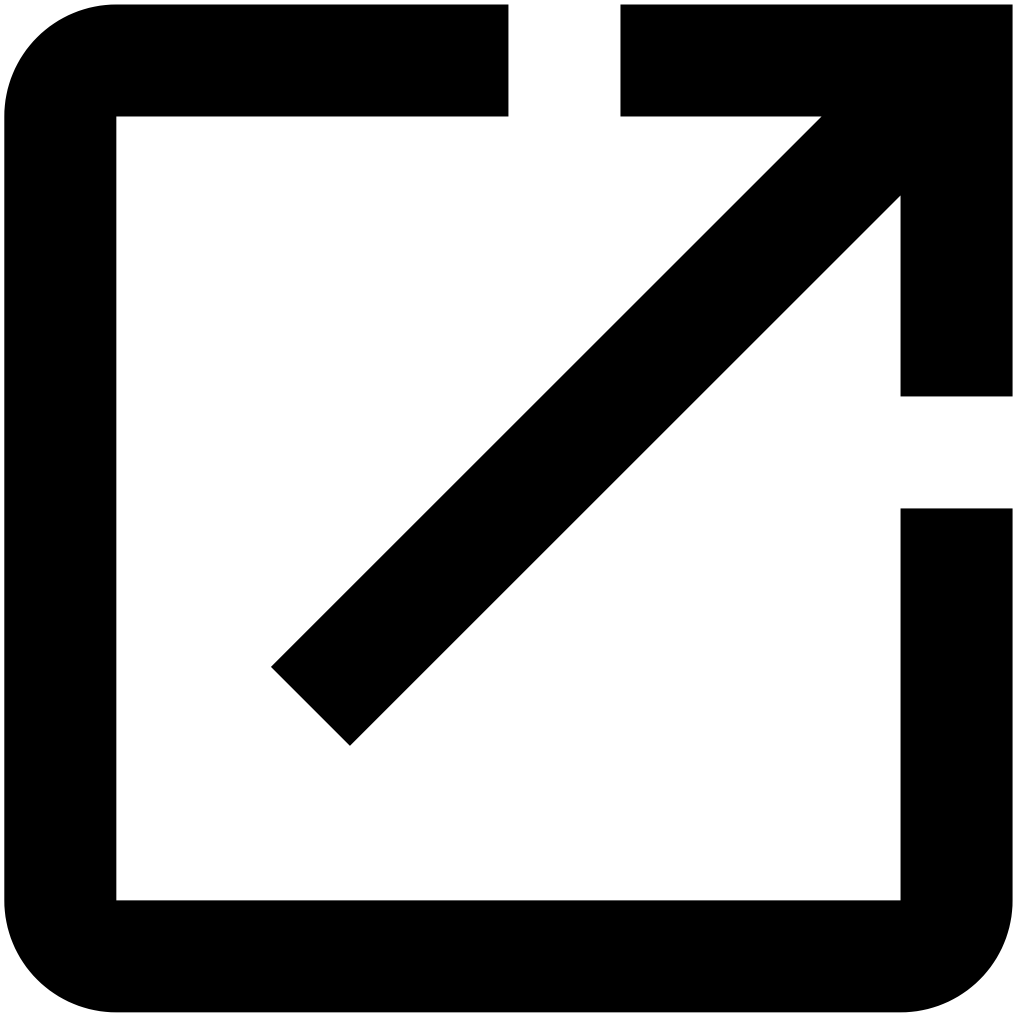
Published: 2024-06-10 · Archived: 2026-04-05 15:25:53 UTC

Cybersecurity company Cylance confirmed the legitimacy of data being sold on a hacking forum, stating that it is old data stolen from a "third-party platform."

A threat actor known as Sp1d3r is selling this stolen data for $750,000, as first spotted by Dark Web Informer.

The data allegedly includes a substantial amount of information, such as 34,000,000 customer and employee emails and personally identifiable information belonging to Cylance customers, partners, and employees.


0:00



However, researchers have told BleepingComputer that the leaked samples appear to be old marketing data used by Cylance.

BlackBerry Cylance told BleepingComputer that they're aware of and investigating the threat actor's claims but that no "BlackBerry data and systems related to [..] customers, products, and operations have been compromised."

"Based on our initial reviews of the data in question, no current Cylance customers are impacted, and no sensitive information is involved," the company added.

"The data in question was accessed from a third-party platform unrelated to BlackBerry and appears to be from 2015-2018, predating BlackBerry's acquisition of the Cylance product portfolio."

Cylance data for sale (Dark Web Informer)

Links to Snowflake attacks

While the company has yet to reply to a follow-up request for more details regarding the name of the third-party platform that was breached to steal what it claims to be old data, the same threat actor is also selling 3TB of data from automotive aftermarket parts provider Advance Auto Parts, stolen after breaching the company's Snowflake account.

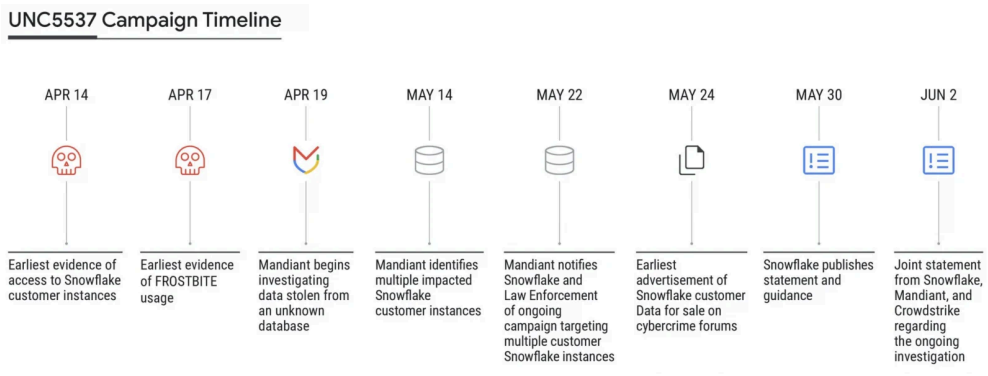
BleepingComputer found a link to a Snowflake web management console located at https://cylance.snowflakecomputing.com/ that appears to be linked to Cylance. However, a BlackBerry spokesperson told BleepingComputer that the dashboard is "old and invalid" and "BlackBerry Cylance is not a Snowflake customer."

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

In a joint advisory with CrowdStrike and Mandiant, Snowflake said that attackers had used stolen customer credentials to target accounts without multi-factor authentication protection.

Today, Mandiant published a report linking the Snowflake attacks to a financially motivated threat actor it tracks as UNC5537. The actor gained access to Snowflake customer accounts using customer credentials stolen in infostealer malware infections from as far back as 2020.

Mandiant has been tracking the UNC5537 since May 2024. The financially motivated threat actor has targeted hundreds of organizations worldwide, extorting victims for financial gain.



UNC5537 Snowflake attack timeline (Mandiant)

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

"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."

Mandiant says it has identified hundreds of customer Snowflake credentials exposed in Vidar, RisePro, Redline, Racoon Stealer, Lumm, and Metastealer infostealer malware attacks since at least 2020.

To date, Snowflake and Mandiant have notified around 165 organizations potentially exposed to these ongoing attacks.

Update June 11, 07:13 EDT: Added BlackBerry statement saying Cylance is not a Snowflake customer.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
