Retail giant Sam’s Club investigates Clop ransomware breach claims

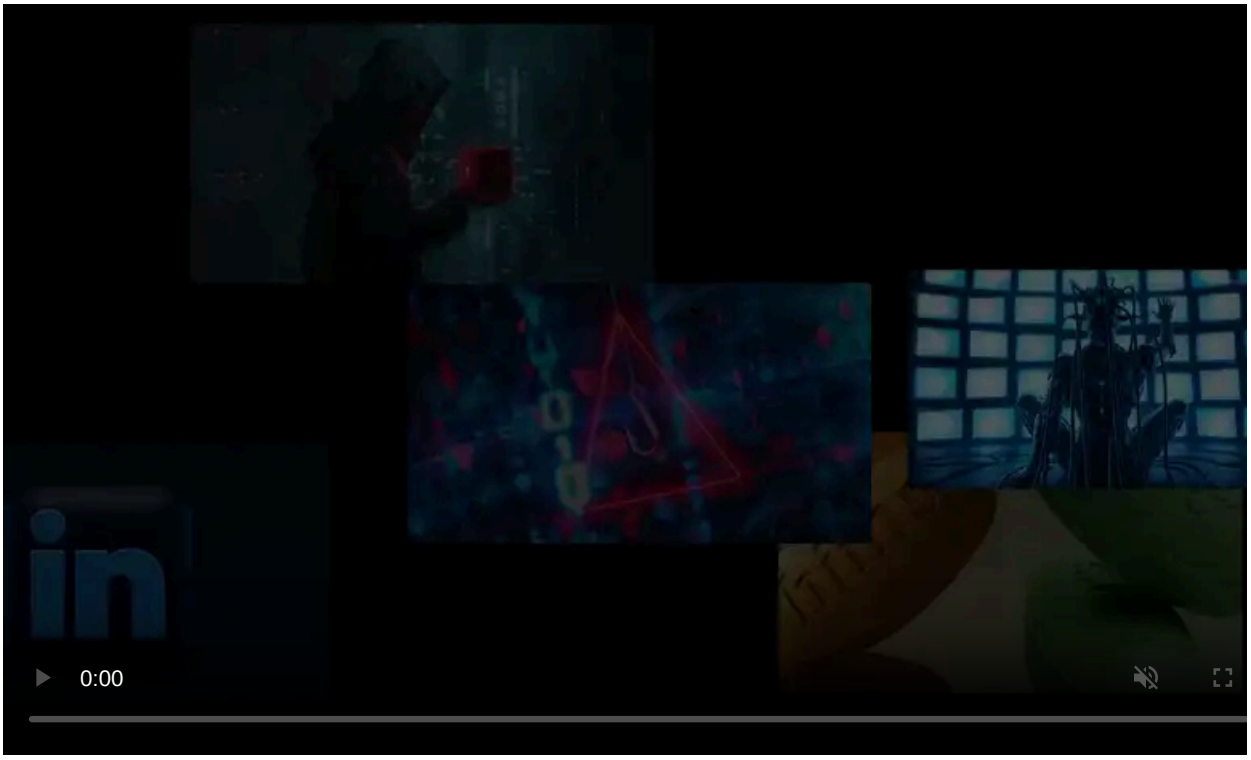
By Sergiu Gatlan

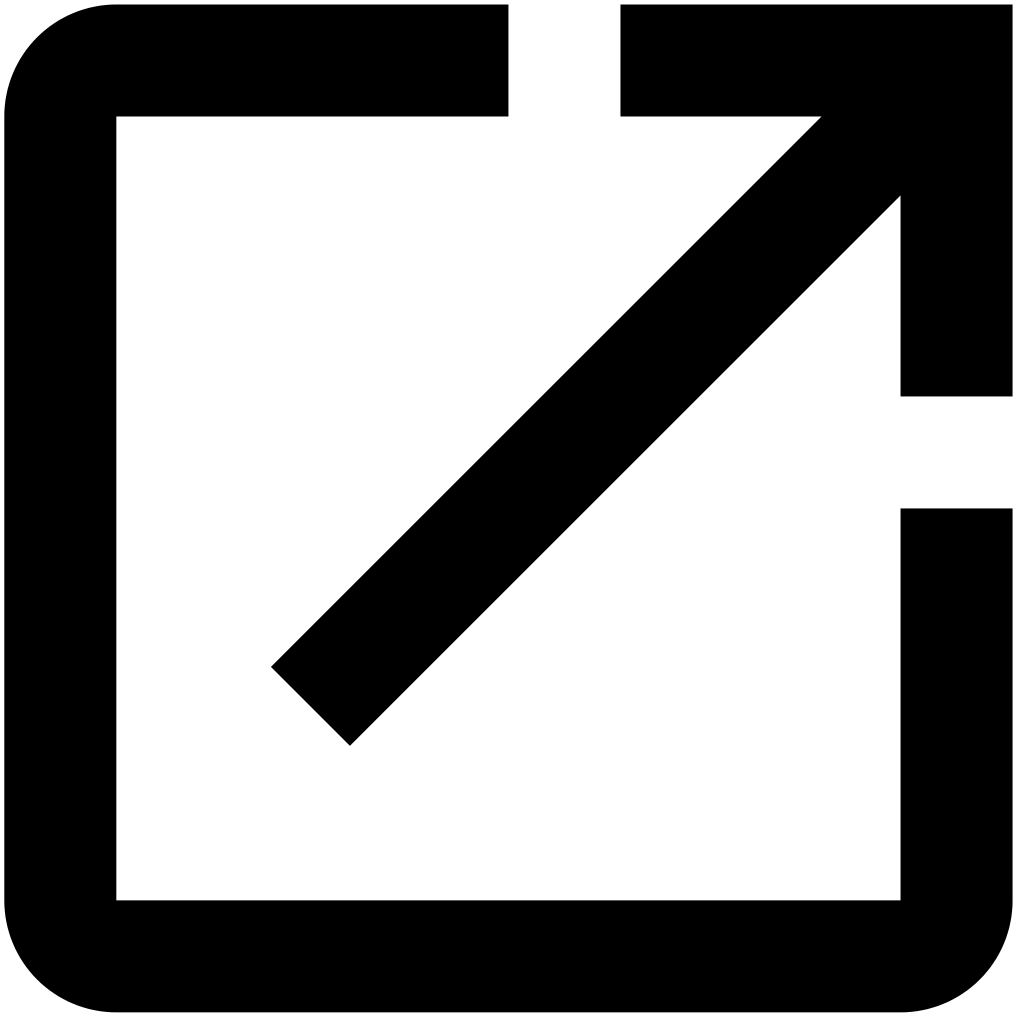
Published: 2025-03-28 · Archived: 2026-04-05 16:31:34 UTC

Sam's Club, an American warehouse supermarket chain owned by U.S. retail giant Walmart, is investigating claims of a Clop ransomware breach.

The Walmart division operates over 600 warehouse clubs with millions of members across the United States and Puerto Rico and almost 200 additional locations in Mexico and China.

Sam's Club has over 2.3 million employees and reported a total revenue of $84.3 billion for the fiscal year ending January 31, 2023.


0:00



"We are aware of reports regarding a potential security incident and are actively investigating the matter," a Sam's Club spokesperson told BleepingComputer. "Protecting the privacy and security of our members' information is a top priority at Sam's Club. We take these concerns seriously and will communicate further as appropriate."

While the company didn't provide additional details regarding this ongoing investigation, the Clop ransomware gang added a new Sam's Club entry to its dark web leak site on Friday.

The cybercrime group has yet to publish any proof of the breach, and so far, the threat actors only said on their leak site that the Arkansas wholesaler "doesn't care about its customers, it ignored their security."

Sam's Club entry on Clop's site (BleepingComputer)

Clop's claims of a Sam's Club breach come after the ransomware gang also started extorting dozens of victims in January, breached in a massive wave of data theft attacks targeting a zero-day vulnerability (CVE-2024-50623) in Cleo secure file transfer software patched in October.

While it's currently unknown how many companies were breached in the Cleo zero-day attacks, Cleo claims its products are used by over 4,000 organizations worldwide.

Arizona-based Western Alliance Bank, one of many companies added to Clop's leak site in January, notified nearly 22,000 customers last week that their personal information was stolen in October after exploiting a vulnerability in third-party secure file transfer software.

The Clop ransomware gang was previously linked to other data theft campaigns targeting zero-day flaws in Accellion FTA, MOVEit Transfer, and GoAnywhere MFT.

This isn't the first security incident that impacted Sam's Club customers in recent years. In October 2020, Sam's Club notified some customers that their accounts were compromised in credential stuffing attacks and automatically reset their SamsClub.com passwords.

"This was not a breach of our systems, but rather a case of these parties obtaining user names and passwords from phishing campaigns, planting malware or breaches at other companies," a Sam's Club spokesperson told BleepingComputer at the time. "We have reset passwords for these accounts and are taking additional measures to protect the accounts from fraudulent activity."

Source: https://www.bleepingcomputer.com/news/security/retail-giant-sams-club-investigates-clop-ransomware-breach-claims/