Clop ransomware claims Saks Fifth Avenue, retailer says mock data stolen

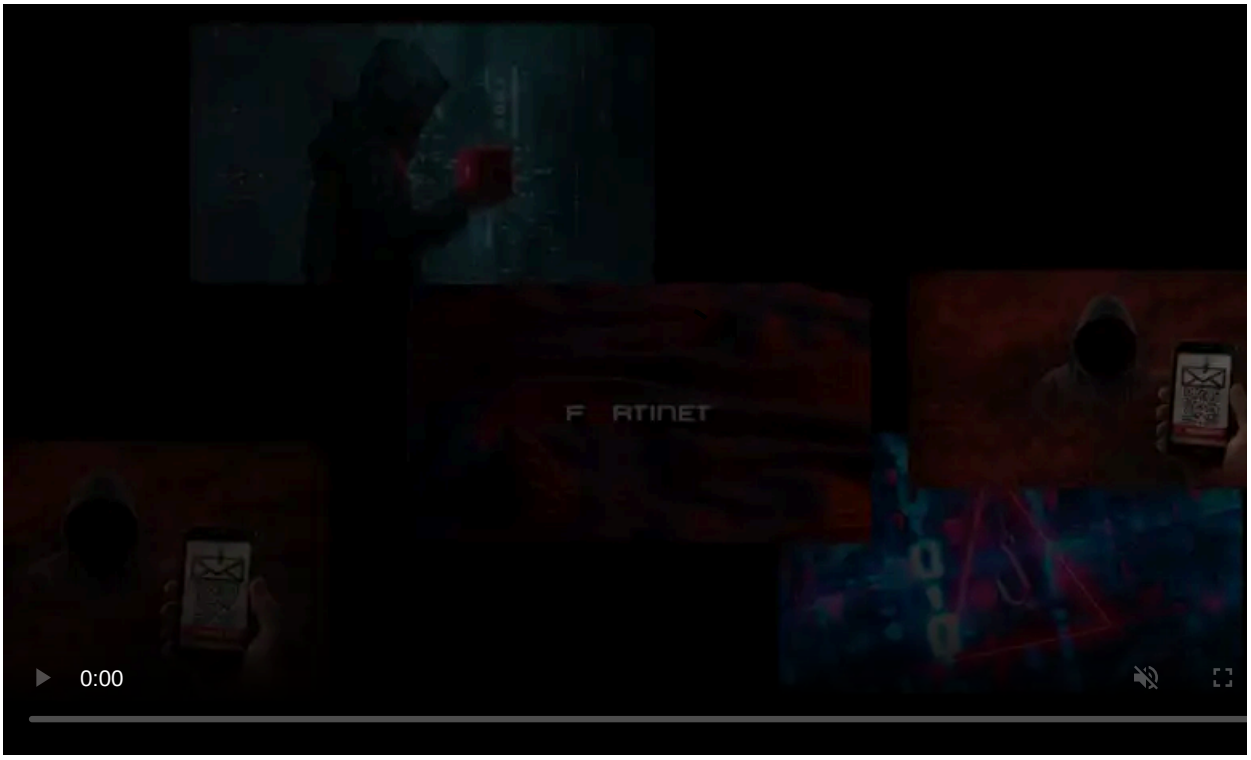
By Ax Sharma

Published: 2023-03-21 · Archived: 2026-04-05 22:31:29 UTC

The Clop ransomware gang claims to have attacked Saks Fifth Avenue on its dark web leak site.

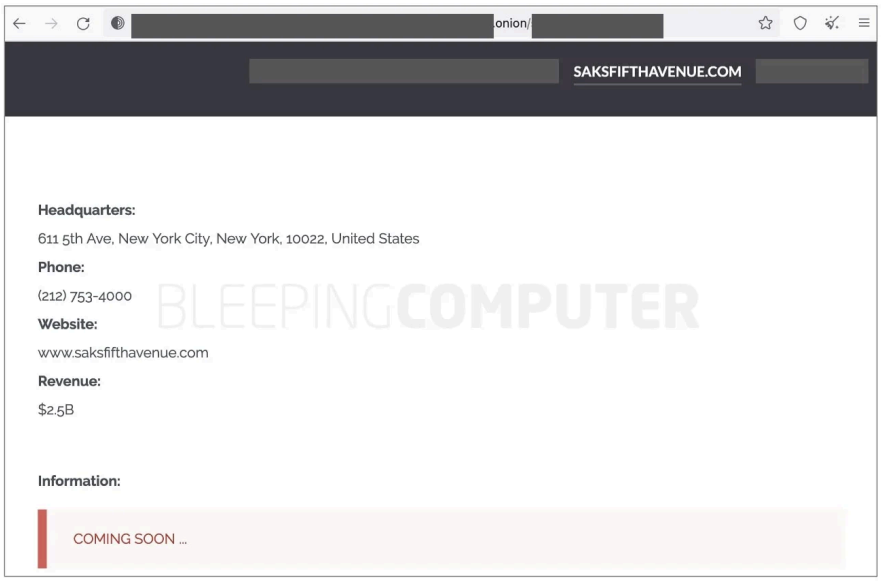
The cyber security incident is among Clop's ongoing attacks against vulnerable GoAnywhere MFT servers belonging to established enterprises. Although the company states no real customer data is impacted, it did not address if corporate or employee data was stolen.

Founded in 1867 by Andrew Saks and headquartered in New York City, Saks Fifth Avenue remains among prominent luxury brand retailers serving the U.S., Canada and parts of the Middle East.


F RTINET
0:00

Clop on a GoAnywhere exploit spree

Yesterday, the Clop ransomware gang listed "Saks Fifth Avenue" on its data leak website among their latest victims, as seen by BleepingComputer:



Cl0p ransomware claims to have attacked Saks Fifth Avenue (BleepingComputer)

The threat actor has not yet disclosed any additional information, such as what all data it stole from the luxury brand retailer's systems, or details about any ongoing ransom negotiations.

BleepingComputer has confirmed, however, the cyber security incident is linked to Clop's ongoing attacks targeting GoAnywhere servers vulnerable to a security flaw.

The flaw, now tracked as CVE-2023-0669, enables attackers to gain remote code execution on unpatched GoAnywhere MFT instances with their administrative console exposed to Internet access.

GoAnywhere MFT's developer Fortra (formerly HelpSystems) had previously disclosed to its customers that the vulnerability had been exploited as a zero-day in the wild and urged customers to patch their systems. The official advisory remains hidden to the public, but was earlier made public by investigative reporter Brian Krebs.

In February, Clop reached out to BleepingComputer and claimed it had breached 130+ organizations and stolen their data over the course of ten days by exploiting this particular vulnerability on enterprise servers.

This month, Hitachi Energy disclosed a data breach by Clop resulting from the same zero-day.

Saks says no real customer data stolen

BleepingComputer reached out to Saks to better understand the scope of this incident. A spokesperson confirmed the incident was linked to Fortra.

"Fortra, a vendor to Saks and many other companies, recently experienced a data security incident that led to mock customer data being taken from a storage location used by Saks," a Saks spokesperson told BleepingComputer.

"The mock customer data does not include real customer or payment card information and is solely used to simulate customer orders for testing purposes."

While the retail giant states no "real" customer data or payment information was stolen, it did not answer our follow up question, as to whether corporate or employee data was compromised in this incident.

"We take information security very seriously, and are conducting an ongoing investigation into this incident alongside outside experts and law enforcement. As organizations increasingly face cybersecurity threats, we remain committed to ensuring the safety of the information we hold," concluded Saks in its statement to us.

For the avoidance of doubt, Saks OFF 5TH—while previously a subsidiary of Saks Inc., is now a separate company and as such not linked to this incident.

In 2018, the Fin7 cybercrime syndicate had hacked Saks Fifth Avenue and Lord & Taylor to steal payment card information of 5 million customers. Nearly a year prior to that, BuzzFeed News had reported that Saks Fifth Avenue was storing personal information of tens of thousands of customers on publicly-accessible pages.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-saks-fifth-avenue-retailer-says-mock-data-stolen/