Scattered Spider hackers shift focus to aviation, transportation firms

By Lawrence Abrams

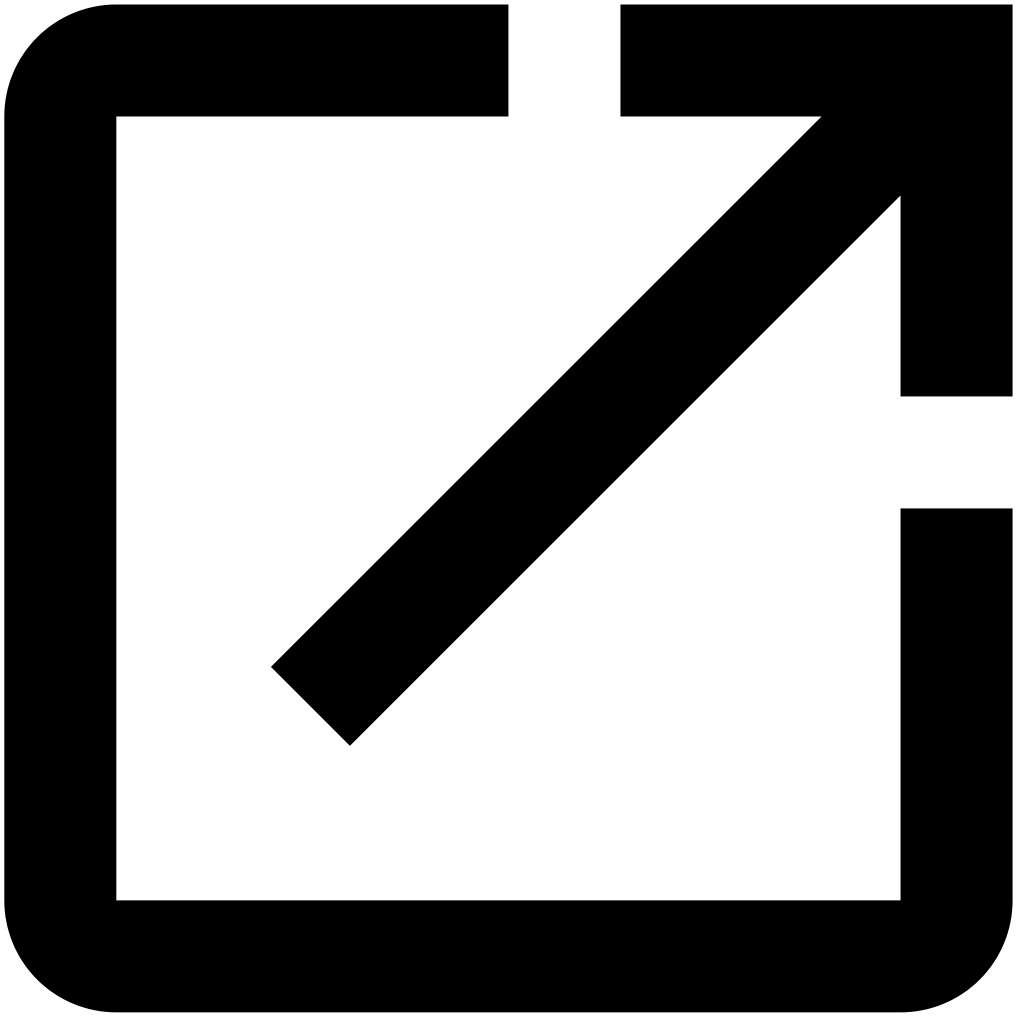
Published: 2025-06-27 · Archived: 2026-04-05 14:29:47 UTC

Hackers associated with "Scattered Spider" tactics have expanded their targeting to the aviation and transportation industries after previously attacking insurance and retail sectors

These threat actors have employed a sector-by-sector approach, initially targeting retail companies, such as M&S and Co-op, in the United Kingdom and the United States and subsequently shifting their focus to insurance companies.

While the threat actors were not officially named as responsible for insurance sector attacks at first, recent incidents have impacted Aflac, Erie Insurance, and Philadelphia Insurance Companies.


DIE LINKE.
0:00



Hackers target the aviation industry

On June 12, Canada's second-largest airline, WestJet, suffered a cyberattack that briefly disrupted the company's internal services and mobile app.

Soon after the breach, sources told BleepingComputer that Palo Alto Networks and Microsoft were assisting in the response to the attack.

The attack was attributed to Scattered Spider, who allegedly compromised the company's data centers and its Microsoft Cloud environment.

BleepingComputer was informed that the threat actor gained access by performing a self-service password reset for an employee, which enabled them to register their own MFA and obtain remote access to the network through Citrix.

While other threat actors conduct identity attacks, Scattered Spider has become associated with this tactic due to their regular targeting of help desks and password and MFA infrastructure.

Today, Hawaiian Airlines also disclosed that they suffered a cyberattack but did not provide any details that could indicate who was behind the attack. However, a source told BleepingComputer that it is believed that the same threat actors are responsible.

Palo Alto Networks' Sam Rubin, SVP of Consulting and Threat Intelligence, has now confirmed on LinkedIn that Scattered Spider has begun targeting the aviation industry.

"Unit 42 has observed Muddled Libra (also known as Scattered Spider) targeting the aviation industry," warned Rubin.

"Organizations should be on high alert for sophisticated and targeted social engineering attacks and suspicious MFA reset requests."

Mandiant's Charles Carmakal also warned that the threat actors have now switched their focus to both the aviation and transportation sectors.

"ALERT: Scattered Spider has added North American airline and transportation organizations to their target list," Carmakal posted to LinkedIn.

"Mandiant (part of Google Cloud) is aware of multiple incidents in the airline and transportation sector which resemble the operations of UNC3944 or Scattered Spider.

"We recommend that the industry immediately take steps to tighten up their help desk identity verification processes prior to adding new phone numbers to employee/contractor accounts (which can be used by the threat actor to perform self-service password resets), reset passwords, add devices to MFA solutions, or provide employee information (e.g. employee IDs) that could be used for a subsequent social engineering attacks."

American Airlines is also currently suffering an IT outage but it is unclear if it is a security incident. BleepingComputer contacted the airline but has not received a response.

What is Scattered Spider

Scattered Spider, also known as 0ktapus, Starfraud, UNC3944, Scatter Swine, Octo Tempest, and Muddled Libra, is a classification of threat actors that are adept at using social engineering attacks, phishing, multi-factor authentication (MFA) bombing (targeted MFA fatigue), and SIM swapping to gain initial network access on large organizations.

These threat actors include young English-speaking people with diverse skill sets who frequent the same hacker forums, Telegram channels, and Discord servers. These mediums are then used to plan and execute attacks in real time.

Some are believed to be part of the "Com" - a loose-knit community of threat actors known for financial fraud, cryptocurrency theft, data breaches, and extortion attacks.

While Scattered Spider is commonly referred to as a cohesive gang, it is actually used to denote threat actors who utilize specific tactics when conducting attacks. As attacks associated with Scattered Spider tactics are also commonly used by different individuals from a loose network of threat actors, it makes it difficult to track them.

Unlike many other English-speaking threat actors, those associated with "Scattered Spider" have been known to partner with Russian-speaking ransomware gangs, such as BlackCat, RansomHub, Qilin, and DragonForce.

Other attacks linked to Scattered Spider include those on MGM, Marks & Spencer, Co-op, Twilio, Coinbase, DoorDash, Caesars, MailChimp, Riot Games, and Reddit.

Organizations defending against this type of threat actor should start with gaining complete visibility across the entire infrastructure, identity systems, and critical management services.

This includes securing self-service password reset platforms and help desks, common targets of these threat actors.

Both Google Threat Intelligence Group (GTIG) and Palo Alto Networks have released guides on hardening defenses against the known "Scattered Spider" tactics used by these threat actors.

All admins are advised to familiarize themselves with these tips and harden their identity platforms and processes.

Update 6/27/25: Added that American Airlines is currently suffering from an IT outage.
