Aflac discloses breach amidst Scattered Spider insurance attacks

By Sergiu Gatlan

Published: 2025-06-20 · Archived: 2026-04-29 08:09:09 UTC

On Friday, American insurance giant Aflac disclosed that its systems were breached in a broader campaign targeting insurance companies across the United States by attackers who may have stolen personal and health information.

Aflac (short for American Family Life Assurance Company) is the largest supplemental insurance provider in the U.S. and a Fortune 500 company that provides insurance services to millions of customers in the U.S. and Japan.

In a press release earlier today, the insurance company added that its network was not affected by ransomware. It is unclear, though, if ransomware was deployed and blocked or if this was just a data theft attack.

"We promptly initiated our cyber incident response protocols and stopped the intrusion within hours. Importantly, our business remains operational, and our systems were not affected by ransomware," Aflac stated.

"We continue to serve our customers as we respond to this incident and can underwrite policies, review claims, and otherwise service our customers as usual. This attack, like many insurance companies are currently experiencing, was caused by a sophisticated cybercrime group. This was part of a cybercrime campaign against the insurance industry."

After detecting the breach, Aflac hired external cybersecurity experts to investigate the incident and review the contents of files potentially exposed during the attack.

As the company explained in a filing with the U.S. Securities and Exchange Commission (SEC), these documents contain a wide range of sensitive information related to customers, beneficiaries, employees, agents, and other individuals, ranging from claims and health information to social security numbers and/or other personal information.

Scattered Spider attacks targeting insurance firms

While an Aflac spokesperson couldn't attribute the breach to a specific cybercrime group, the breach exhibits all the signs of a Scattered Spider attack.

Scattered Spider (also tracked as 0ktapus, UNC3944, Scatter Swine, Starfraud, and Muddled Libra) is a group of threat actors known for their sophisticated social engineering attacks against high-profile organizations worldwide, with tactics that include phishing, SIM swapping, and multi-factor authentication (MFA) bombing.

In September 2023, they escalated their attacks by breaching MGM Resorts and encrypting over 100 VMware ESXi hypervisors using BlackCat ransomware after gaining access by impersonating an employee. They've also partnered with other ransomware operations, such as RansomHub, Qilin, and DragonForce. Other organizations targeted by Scattered Spider include Twilio, Coinbase, DoorDash, Caesars, MailChimp, Riot Games, and Reddit.

As John Hultquist, Chief Analyst at Google Threat Intelligence Group (GTIG), told BleepingComputer earlier this week, Scattered Spider has recently been targeting and breaching U.S. insurance companies.

Hultquist also told BleepingComputer today that "the insurance industry should be on high alert" and pay particular attention to potential social engineering attempts on help desks and call centers, "given this actor's history of focusing on a sector at a time."

The most recent examples are Philadelphia Insurance Companies (PHLY) and Erie Insurance, which experienced outages and disruptions after detecting unauthorized network access.

In May, GTIG's chief analyst also warned that Scattered Spider switched from targeting retail chains in the United Kingdom to targeting retailers in the United States. "The actor, which has reportedly targeted retail in the UK following a long hiatus, has a history of focusing their efforts on a single sector at a time," he added

---

Source: https://www.bleepingcomputer.com/news/security/aflac-discloses-breach-amidst-scattered-spider-insurance-attacks/