DUCK AND COVER? NOT THIS TIME:

THE AFLAC BREACH

Cora Wilson

CS 462

Professor Bhanuka Mahanama

WHO IS SCATTERED SPIDER?

Scattered Spider is a cybercriminal group believed to consist of six or more individuals, and it is also tracked under several aliases, including UNC3944, Scatter Swine, Oktapus, Octo Tempest, Storm-0875, and Muddled Libra. (CISA, 2023) . Despite ongoing investigations, many details about the group's structure and full scope remain unclear. What is known, however, is that its primary focus is data extortion, often accompanied by other forms of cybercrime such as unauthorized access, credential theft, and system compromise.

The group is known to operate within a broader online underground community referred to as "The Com," where members collaborate, share tactics, and coordinate attacks. Scattered Spider has also demonstrated a strategic pattern of targeting one industry at a time, allowing them to refine their techniques and exploit common vulnerabilities across similar organizations before shifting focus to a new sector (Aflac Data Breach Exposes 22.65 Million in Scattered Spider Insurance Campaign, 2025) .

In carrying out their attacks, Scattered Spider relies heavily on social engineering methods rather than purely technical exploits. Common tactics include push bombing where repeated authentication requests are sent to overwhelm and trick users into approving access and subscriber identity module (SIM) swap attacks, which allow attackers to take control of a victim's phone number. These techniques enable the group to obtain login credentials, install remote access tools, and bypass multi-factor authentication (MFA), making their attacks particularly effective against organizations that rely heavily on human verification processes (CISA, 2023) .

HOW DOES SCATTERED SPIDER WORK?

They impersonate legitimate employees to manipulate IT and helpdesk personnel into revealing sensitive information, resetting account passwords, and transferring multi-factor authentication (MFA) access to devices under the attacker's control. This often involves carefully crafted social engineering tactics designed to build trust, pressure staff, or exploit urgency so that standard verification steps are bypassed.

In many cases, these attackers use separate devices or communication channels to carry out their activities, which helps them avoid detection and makes their actions appear more legitimate. By combining deception with technical persistence, they are able to gain and maintain unauthorized access while blending in with normal support processes, making these attacks especially difficult to identify in real time.

HOW IS SCATTERED SPIDER SO EFFECTIVE?

Focuses heavily on targeting people rather than systems, using manipulation and social engineering to exploit human behavior instead of relying solely on technical vulnerabilities.

Uses legitimate tools and services already present in environments, which allows their activity to blend in with normal operations and makes detection more difficult for security teams.

Operates in coordinated groups, sharing techniques, resources, and access in a structured way that increases efficiency and the success rate of their attacks.

Concentrates on one industry at a time, allowing them to study common systems, workflows, and weaknesses within that sector and refine their attack strategies before moving on to new targets.

Malware	Use
AveMaria	Enables remote access to a targeted organization's systems
Raccoon Stealer	Steals information including login credentials, browser history, cookies, and other data
RattyRAT	Java-based remote access trojan.
VIDAR Stealer	Steals information including login credentials, browser history, cookies, and other data.
DragonForce Ransomware	Infiltrates networks, encrypts data, and demands ransom.

SCATTERED SPIDER'S MALWARE TOOLS

(CISA, 2023)

WHAT HAPPENED?

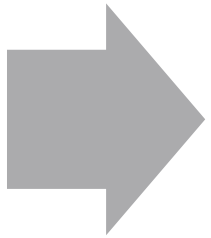
On June 12, 2025, Aflac Incorporated was targeted by a highly sophisticated cyberattack attributed to the cybercriminal group Scattered Spider. (Weisman, 2025) The group leveraged advanced social engineering techniques, a method they are well known for, to gain unauthorized access to Aflac's systems. By exploiting human vulnerabilities rather than relying solely on technical flaws, the attackers were able to bypass security controls and infiltrate sensitive networks. (Aflac Incorporated Discloses Cybersecurity Incident, 2025)

As a result of this breach, the personal and protected health information of approximately 22.65 million individuals was exposed, making it one of the more significant data security incidents in the insurance sector. The scale of the attack highlights both the effectiveness of social engineering tactics and the challenges organizations face in defending against them. (Aflac Data Breach Exposes 22.65 Million in Scattered Spider Insurance Campaign, 2025)

The compromised data included a wide range of highly sensitive information. This included Social Security numbers, government-issued identification such as driver's licenses, detailed medical records, health insurance information, and claims data. The exposure of this type of information poses serious risks, including identity theft, insurance fraud, and long-term privacy concerns for those affected.

HOW IT HAPPENED

While not publicly confirmed by Aflac Incorporated, it is widely believed that Scattered Spider relied on its typical social engineering tactics to carry out the attack. These methods likely included impersonating helpdesk personnel and manipulating IT staff into transferring credentials without proper authorization or falling victim to convincing phishing campaigns.

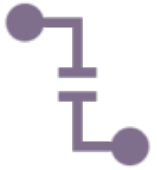


Following initial access, the group is believed to have used techniques such as SIM swapping or the abuse of legitimate remote access tools to gain deeper access to internal systems and devices within the organization. This combination of human manipulation and misuse of trusted tools reflects a common pattern in Scattered Spider's operations and highlights how attackers can bypass traditional security measures by exploiting trust and routine processes (Aflac Data Breach Exposes 22.65 Million in Scattered Spider Insurance Campaign, 2025) .

HOW AFLAC RESPONDED

According to Aflac Incorporated's cybersecurity incident disclosure, the company stated that it "promptly initiated cyber incident protocols and stopped the intrusion within hours" (Aflac Incorporated Discloses Cybersecurity Incident, 2025) . This suggests that Aflac was able to detect and respond to the threat relatively quickly, limiting the duration of unauthorized access.

While the company has not publicly detailed the specific defenses used or the exact components of its incident response protocols, it did confirm that third-party cybersecurity experts were brought in to assist with managing and investigating the incident. This is a common practice in large-scale breaches, as external specialists can provide advanced forensic analysis and help contain ongoing threats.



In addition, Aflac reported that affected passwords were reset and that enhanced monitoring measures were implemented to detect any further suspicious activity. These steps indicate an effort to secure compromised accounts and strengthen visibility across systems following the breach, even though full technical details of the response have not been disclosed. (Morgan, 2025)

PATCHES/ADJUSTMENTS MADE BY AFLAC

Aflac Incorporated followed recommendations from cybersecurity experts by adopting zero-trust security principles, increasing the frequency and depth of employee training on social engineering tactics, and strengthening identity verification procedures for IT support requests. The company also deployed more advanced threat detection systems to improve its ability to identify suspicious activity in real time and reinforced its incident response planning to ensure faster and more effective handling of potential security events. These combined measures reflect a shift toward a more proactive and layered cybersecurity strategy aimed at reducing risk and improving resilience (Morgan, 2025).

IMPACT ON VICTIMS

What truly matters about this attack is not the financial cost to Aflac Incorporated for damage control and system remediation, but the lasting impact on the victims.

The breach left millions of individuals vulnerable to identity theft due to the exposure of Social Security numbers and other personally identifiable information. In addition, the compromise of medical records and insurance data increases the risk of medical identity theft and insurance fraud, which can be significantly more difficult to detect and resolve than traditional identity theft.

Beyond the immediate risks, the incident also creates long-term privacy concerns. Unlike passwords, sensitive personal and health information cannot simply be changed, meaning affected individuals may face ongoing risks for years to come.

LESSONS LEARNED

The human element remains the most significant vulnerability in cybersecurity.

Multi-factor authentication (MFA) alone is insufficient when attackers successfully use social engineering techniques.

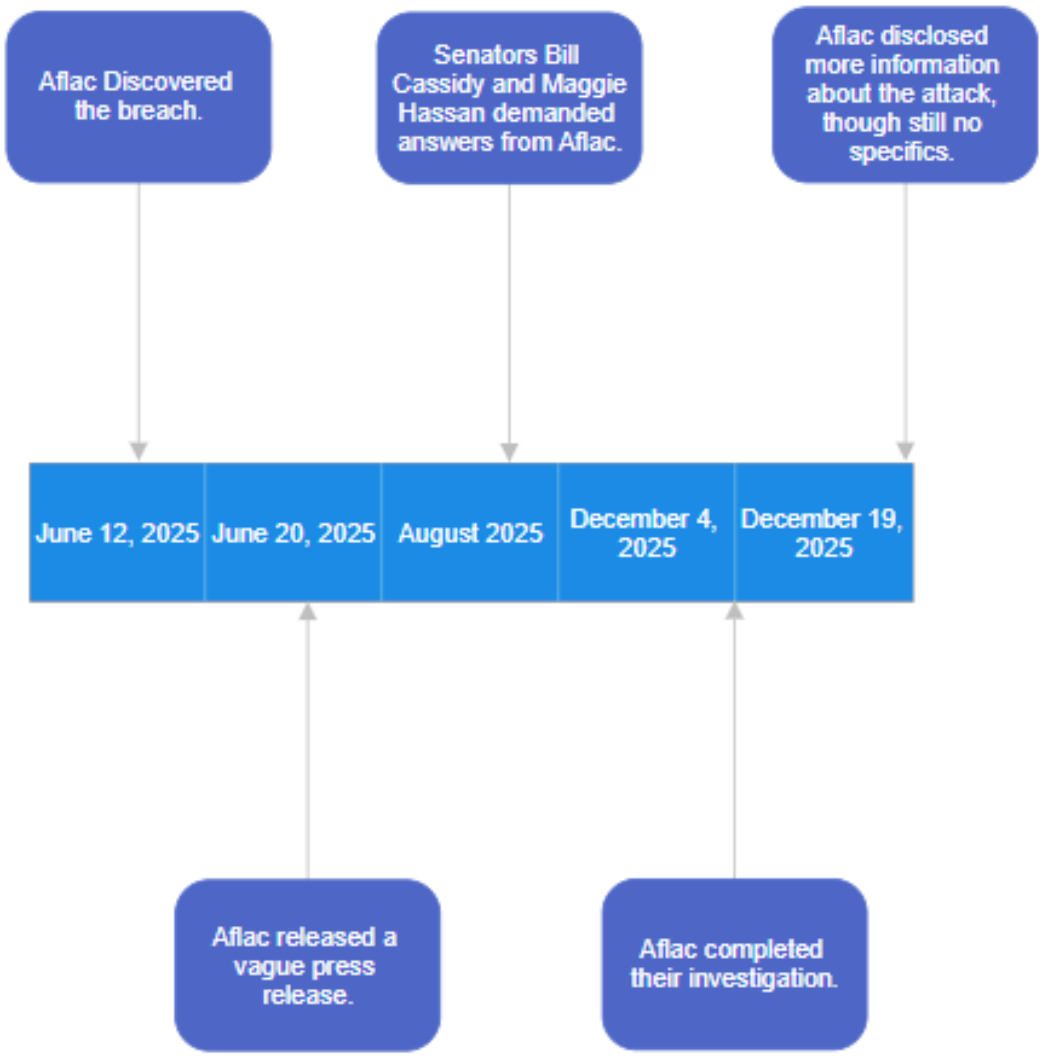
Helpdesk and IT support functions are High-risk entry points that attackers frequently target

A layered security approach is essential, not optional, including zero-trust architecture, continuous employee training, and ongoing monitoring.

HOW ORGANIZATIONS CAN PREVENT SIMILAR ATTACKS

Implement	Implement strict helpdesk verification procedures with no exceptions or shortcuts to confirm user identity.
Use	Use phishing-resistant multi-factor authentication, such as hardware security keys or physical tokens.
Restrict	Restrict remote access tools to only verified, authorized individuals and limit their usage to necessary cases.
Conduct	Conduct continuous employee awareness training to recognize and respond to social engineering and phishing attempts.

TIMELINE


Aflac Discovered the breach.
Senators Bill Cassidy and Maggie Hassan demanded answers from Aflac.
Aflac disclosed more information about the attack, though still no specifics.
June 12, 2025
June 20, 2025
August 2025
December 4, 2025
December 19, 2025
Aflac released a vague press release.
Aflac completed their investigation.

SOURCES/WORK CITED

Aflac Data Breach Exposes 22.65 Million in Scattered Spider Insurance Campaign. (2025, December 30). Breached.company. https://breached.company/aflac-data-breach-exposes-22-65-million-in-scattered-spider-insurance-campaign/?utm_source=chatgpt.com.

Aflac Incorporated Discloses Cybersecurity Incident. (2025, June 20). Aflac.com; Aflac https://investors.aflac.com/press-releases/press-release-details/2025/Aflac-Incorporated-Discloses-Cybersecurity-Incident/default.aspx

CISA. (2023, November 16). *Scattered Spider | CISA*. Www.cisa.gov. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

Morgan, B. (2025, December 30). *Aflac Data Breach: Insurance Giant Confirms Personal Data of 22.65 Million Customers Exposed*. SecureDetectives. https://www.securedetectives.com/news/aflac-data-breach

Weisman, S. (2025, June 21). Aflac Data Breach By Scattered Spider Hackers Is No Quacking Matter. *Forbes*. https://www.forbes.com/sites/steveweisman/2025/06/21/aflac-data-breach-by-scattered-spider-hackers-is-no-quacking-matter/