22/02/23

Insurance sector under assault via social engineering campaigns

Summary: In June 2025, the insurance sector was beset by attacks conducted through a social engineering campaign. Among the confirmed targets were Aflac, Philadelphia Insurance Companies, and Erie Insurance. New York Life Insurance Co. was also a suspected victim. These attacks were conducted against a vendor for these companies and resulted in the release of sensitive personal and medical data for millions of customers. The group responsible for these attacks is a loosely affiliated group of criminals called SCATTERED SPIDER by intelligence companies and law enforcement agencies.

SCATTERED SPIDER is financially motivated and has a long, successful history of engineering attacks in conjunction with other cyber criminal organizations. In 2023, they were responsible for the attacks on MGM Resorts and Caesar's Palace that resulted in $100 million in losses, with Caesar's paying $15 million to prevent the release of stolen data. SCATTERED SPIDER was also responsible for the Snowflake data breach last year that affected 165 different organizations. In 2025, they were responsible for the chain of attacks against UK retailers, including Marks and Spencer's and The Co-op. In May, through the compromise of another vendor, they released customer data from Adidas and Victoria's Secret. Aside from the previously stated insurance companies, June also saw SCATTERED SPIDER begin attacking aviation services providers like Hawaiian Airlines, WestJet, and Qantas.

On 10 July 2025, four suspected members of SCATTERED SPIDER were arrested across the UK. While this is a setback for them, it certainly does not mean that they are defunct. In November 2024, five members were indicted in the US, indicating that their loose professional affiliation is an asset and contributes to their resiliency in the cyber criminal sphere.

Analysis: SCATTERED SPIDER tends to gain initial access to a network through social engineering and voice phishing (vishing). After an extensive reconnaissance period utilizing open source assets like LinkedIn and Dark Web resources like previous breaches, SCATTERED SPIDER will call the target's Help Desk pretending to be an employee in distress and attempt to cajole the Help Desk into bypassing credentials, resetting passwords, or overriding MFA. Occasionally, they have also used SIM-swapping, impersonating the legitimate employee's phone to bypass MFA. Once inside a network using the new credentials, SCATTERED SPIDER will utilize legitimate administrative programs to avoid detection while exfiltrating data and/or deploying ransomware packages (such as the DragonForce package used against the UK targets). SCATTERED SPIDER will then utilize a double extortion method, demanding payment for 1) unlocking a system's data and 2) destruction of the exfiltrated data.

DeepSeas Recommendations: The DeepSeas TIDE crew recommends a robust communication channel for suspicious messages and help desk calls, as well as proper training and alerting of help desk and general staff of this type of activity. DeepSeas has assisted

in several penetration tests focused on evaluating the preparedness and training of Help Desks and IT support to protect against these social engineering attacks.