ECKERT SEAMANS
ATTORNEYS AT LAW

August 20, 2025

Legal Update

Don't Get Snared in Scattered Spider's Web: Review Your Security Measures Now!

By Lawrence J. Finnell, Matthew H. Meade, Elizabeth Wilson, and Samantha Walter

Scattered Spider, the notorious hacking group responsible for the massive 2023 hack against MGM Resorts, which cost the company over $100 million dollars to address, recently laid siege on airline, transportation, and insurance companies. This is consistent with Scattered Spider's modus operandi that targets specific sectors for multiple weeks at a time and then shifts focus to another industry. [1]On July 30, 2025, UK authorities arrested four of the group's members, which appeared to result in a pause in Scattered Spider's criminal operations[2]. However, another criminal hacker organization "ShinyHunters" recently revealed that Scattered Spider merged with ShinyHunters, which may explain the perceived pause in Scattered Spider's activities[3].

Scattered Spider's Hacking Methods

Scattered Spider utilizes several methods to infiltrate an organization and are known for changing their TTPs ("Tactics, Techniques, and Procedures") to avoid getting caught. The group also employs an affiliate model that "enables it to regroup and evade detection despite police action"[4].

Some of Scattered Spider's TTPs include the following methods below.

- *Push Bombing*: Hackers send a high volume of repeated multi-factor authentication (MFA) push notifications at once to trick a user into approving a hacker's MFA login request.
- *Voice or Text Phishing*: Hackers may call or text employees on the phone or via text pretending to be the IT department and tricking employees to (i) provide their computer credentials or one time MFA authentication code or (ii) allow the hacker to remote access into the employee's computer for "IT support" purposes. Hackers also call or text IT help deck staff pretending to be an employee who is locked out of their account and tricking the IT staff member into providing or resettling user credentials and/or transfer the employee's multifactor identification

[1] Dissent, *Alert: Scattered Spider has added North American airline and transportation organizations to their target list*, DATABREACHES.NET, June 27, 2025, *available at:* https://databreaches.net/2025/06/27/alert-scattered-spider-has-added-north-american-airline-and-transportation-organizations-to-their-target-list/.
[2] Dissent, *Scattered Spider is NOT quiet. They're just under another name now*, DATABREACHES.NET, August 5, 2025, *available at:* https://databreaches.net/2025/08/05/scattered-spider-is-not-quiet-theyre-just-under-another-name-now/.
[3] *Id.*
[4] Akshaya Asokan, *Scattered Spider Targeting American Insurance Firms*, DATA BREACH TODAY, June 17, 2025, *available at:* https://www.databreachtoday.com/scattered-spider-targeting-american-insurance-firms-a-28723?highlight=true.

("MFA") credentials to a hacker controlled device. Hackers also use this method to gain access to users' Snowflake accounts.

- *Subscriber Identity Module (SIM) Swap Attacks*: Hackers gather personal information on an individual target, and then using this personal information, trick the target's mobile phone carrier into switching the target's cell phone number onto a new SIM card. After the SIM card is swapped, the hacker can access the target's phone calls and text messages, including one-time passwords to gain access to the target's online accounts and systems.

- *Infiltrate Third Party Systems*. Hackers also exploit security vulnerabilities from third party providers who have access to an intended target by hacking into the third party's systems to gain access to the target entity's network.

Once inside the network, hackers (i) install legitimate remote access tools and/or utilize existing applications on the target's network to steal sensitive data and/or (ii) install malware to encrypt data. The hackers then extort their target in return for not selling the stolen data on the Dark Web and/or providing the encryption key to their data.

How to Prevent and/or Mitigate a Cyber Attack.

Mandiant[5], Google's threat intelligence group, and the Cybersecurity and Infrastructure Security Agency ("CISA")[6] recently provided guidance to entities on how to prevent and/or mitigate a Scattered Spider cyber-attack, which are described below.

- *HelpDesk Procedures*: Entities should implement an identity verification process that verifies a user's identity before doing any of the following: (i) changing or adding a new phone number to a user's account, (ii) resetting passwords, (iii) adding devices to MFA solutions, or (iv) providing employee information that could be used to facilitate social engineering attacks[7].

- *Offline Backups*. Entities should maintain and regularly test encrypted offline data backups that are stored separately from the source systems. Organizations should also create and adopt a data recovery plan to address data loss.

- *Enhanced MFA*. Entities should enable and enforce phishing-resistant multifactor authentication (MFA) such as FIDO/WebAuthn authentication (uses biometrics or security keys) or Public Key Infrastructure (PKI) (uses encrypted digital certificates

- *Application Controls*. Organizations should implement application controls to prevent unauthorized software from being installed on networks or devices. Allow-listed software and applications on the network should be patched regularly.

---

[5] *See* GOOGLE CLOUD BLOG, *Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines*, May 6, 2025, *available at:* https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations.

[6] *See* CISA, *Cybersecurity Advisory, Scattered Spider*, July 29, 2025, *available at:* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a.

[7] *See* Footnote 1.

- *Remote Access / Remote Desktop Tools*. Entities should identify and monitor what remote access and/or remote desktop tools are on their network and devices and implement software to detect and/or block unauthorized tools.

- *Password Policies*. Organizations should require employees to select complex passwords that are changed regularly and implement mechanisms that lock an account after several failed log in attempts. Entities should only allow administrative credentials to install any software or applications on their network or devices.

- *Network Measures*. Entities should consider segmenting their network to prevent further infiltration during a cyber-attack. Organizations should also disable unused ports/protocols.

- *Activity Monitoring*. Organizations should regularly monitor their network and systems for suspicious activity. There are several third-party tools available such as endpoint and/or managed detection and response tools. Entities should identify and closely monitor "risky logins" that have been previously flagged as potentially compromised.

- *Email Security*. Entities should consider (i) adding an email banner, so it is clear which emails originate outside their organization and (ii) disabling hyperlinks in received emails.

- *Staff Training*. Organizations should regularly train their staff on security awareness (including providing regular security newsletters and/or security email updates) and employ periodic phishing email tests with their staff members.

Department of Labor Considerations

Given that insurers are among Scattered Spider's known targets, plan sponsors, insurers, and other plan service providers should be especially mindful of cybersecurity threats. Insurers often wear multiple hats, both acting as the insurance carrier as well as serving as plan recordkeepers, preserving and securing plan records and sensitive participant data. As a result, it is essential for plan fiduciaries to ensure that their insurance carriers and other service providers implement strong cybersecurity practices to guard against attacks.

The U.S. Department of Labor ("DOL") has issued detailed cybersecurity guidance applicable to plan sponsors, fiduciaries, record-keepers, participants and beneficiaries, and other plan service providers. The DOL guidance primarily focuses on three specific topics: hiring service providers, managing cybersecurity risks, and online security tips for participants to avoid risk of fraud and loss. While initially focused on retirement plans, the DOL recently expanded its guidance to health and welfare plans by endorsing resources from the Department of Health and Human Services ("HHS") that are related to managing cyber threats and protecting patient information. For a summary of the DOL's guidance, please see our prior Employee Benefits Alert here. Please note that in addition to DOL guidance requirements, health plan providers must also ensure compliance with existing administrative, physical, and technical safeguards required under the HIPAA Security Rule at 45 CFR Part 160 and Subparts A and C of Part 164.

Plan fiduciaries should ensure that they incorporate DOL best practices, and HIPAA safeguards if applicable, when hiring service providers and reviewing contracts with their vendors. Contracts should

include appropriate cybersecurity provisions, including, but not limited to, mandating cyber insurance coverage for losses in the event of a breach, requiring third party audits to ensure vendors maintain sufficient protection, and incorporating indemnification provisions to shield plans from liability. Periodic review of service provider contracts and operations are also recommended. In addition, plan sponsors should assess their own practices to align with DOL guidance to safeguard plan data.

How We Can Help

ECKERT SEAMANS ATTORNEYS AT LAW

This joint Cybersecurity, Data Protection & Privacy and Employee Benefits Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Larry Finnell at 609-989-5015 or lfinnell@eckertseamans.com, Matt Meade at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, Samantha Walter at 412-566-1920 or swalter@eckertseamans.com, or any other attorney in our Cybersecurity, Data Protection & Privacy or Employee Benefits Practice Groups, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.