Scattered Spider's Old Tactics Still Opening New Doors

C-Suite level threat review by applicable business area addressing active threats.

One year ago, our July 2024 newsletter detailed how Scattered Spider relied on help desk impersonation and social engineering to reset multi-factor authentication and compromise accounts. One year later, the group has not only maintained that core playbook but has scaled it globally, broadened the targeted industries, and developed more technical tooling. This newsletter covers how Scattered Spider has used these tactics in 2025 and the persistent threat they pose.

In 2025, Scattered Spider expanded its operations beyond U.S.-based telecommunications, finance, and entertainment to also target the airline, retail, and insurance industries across the U.S., U.K., and Australia. Despite the geographical and industry expansion, the group remains consistent in its initial access tactic of impersonating IT help desks and employees through highly credible social engineering.

Scattered Spider demonstrated this tactic in two high-impact breaches in the second quarter of 2025. In late June, Qantas Airlines reported that attackers manipulated a call center employee into granting access to a third-party platform. This unauthorized access exposed 5.7 million customer records. Similarly, Marks & Spencer, one of the UK's largest retailers, suffered a ransomware attack attributed to Scattered Spider and its affiliate DragonForce. Reports state that the attackers impersonated a legitimate employee and contacted a third-party IT provider that manages help desk operations. The provider is believed to have reset the employee's credentials, granting the attackers access to internal systems. From there, they exfiltrated data and deployed DragonForce Ransomware.

These recent attacks from Scattered Spider highlight the group's ability to exploit human vulnerabilities during the initial access stage. Once inside, Scattered Spider continues to spin its web with advanced tactics across the attack lifecycle.

Scattered Spider

Threat Level: High

Attack:

After gaining access through social engineering, Scattered Spider sets up remote access with tools like AnyDesk and Ngrok to establish persistent access and enable communication with compromised systems (MITRE T1566, T1586, T1219). These tools are often used for legitimate IT work, allowing attackers to blend in with normal traffic and avoid detection (MITRE T1036). Once inside, the group elevates privileges by exploiting weak certificate templates. This exploitation tricks internal systems into granting them access across the network. Scattered Spider also deploys vulnerable drivers to disable antivirus and endpoint defenses (MITRE T1562, T1068). The group steals credentials from memory and extracts the NTDS.dit file from domain controllers, which contains Active Directory credentials (MITRE T1003). With these credentials, they can move laterally and expand their control across the environment. Scattered Spider then exfiltrates sensitive data such as emails, credentials, and financials, disrupts backup systems, and ultimately deploys ransomware such as DrangonForce to encrypt files and disrupt operations (MITRE T1490, T1486).

Recommendations:

- Block unauthorized remote access tools and monitor unusual remote access traffic patterns, especially during off-hours.
- Conduct live social engineering simulations and training sessions to help train support staff on common manipulation tactics.
- Require in-person identity verification for password and MFA resets whenever possible. If in-person is not possible, require live video verification where users must show their valid ID and confirm personal details.

Scattered Spider:

- **Outline of Scattered Spider Tactics**: https://www.halcyon.ai/blog/scattered-spider-tactics-observed-amid-shift-to-us-targets
- **Qantas Airline Breach**: https://www.adminbyrequest.com/en/blogs/scattered-spider-suspected-in-qantas-breach-as-aviation-attacks-mount
- **Marks and Spencer Breach:** https://www.blackfog.com/marks-and-spencer-ransomware-attack/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports

FBI Scattered Spider Alert

FBI – Federal Bureau of Investigation
June 27 at 7:55 PM ·

ALERT—The FBI has recently observed the cybercriminal group Scattered Spider expanding its targeting to include the airline sector. These actors rely on social engineering techniques, often impersonating employees or contractors to deceive IT help desks into granting access. These techniques frequently involve methods to bypass multi-factor authentication (MFA), such as convincing help desk services to add unauthorized MFA devices to compromised accounts. They target large corporations and their third-party IT providers, which means anyone in the airline ecosystem, including trusted vendors and contractors, could be at risk.

Once inside, Scattered Spider actors steal sensitive data for extortion and often deploy ransomware. The FBI is actively working with aviation and industry partners to address this activity and assist victims. Early reporting allows the FBI to engage promptly, share intelligence across the industry, and prevent further compromise. If you suspect your organization has been targeted, please contact your local FBI office.