Exposing Scattered Spider: New Indicators Highlight Growing Threat to Enterprises and Aviation

By laurama

Published: 2025-07-07 · Archived: 2026-04-17 02:06:42 UTC

Check Point Research identifies phishing domain patterns, offering actionable insights to proactively counter threats from the notorious cyber group behind recent airline attacks

Scattered Spider, a sophisticated cyber threat group known for aggressive social engineering and targeted phishing, is broadening its scope, notably targeting aviation alongside enterprise environments. Check Point Research has uncovered specific phishing domain indicators, helping enterprises and aviation companies proactively defend against this emerging threat.

Recent Aviation Attacks Linked to Scattered Spider

In a significant escalation, recent media reports and intelligence advisories have linked Scattered Spider to cyber-attacks on major airlines, notably the July 2025 data breach affecting six million Qantas customers. Cybersecurity analysts noted tactics such as MFA fatigue and voice phishing (vishing), closely matching Scattered Spider's known methods.

Similar incidents involving Hawaiian Airlines and WestJet have further highlighted the urgency of addressing vulnerabilities in aviation-related third-party providers.

Key Targeting Indicators (Phishing Domains)

Check Point Research has identified a consistent pattern in the phishing infrastructure registered by Scattered Spider. These domains closely mimic legitimate corporate login portals and are designed to deceive employees into revealing their credentials.

Typical naming conventions include:

- victimname-sso.com
- victimname-servicedesk.com
- victimname-okta.com

During a targeted investigation, Check Point researchers identified approximately 500 domains that follow Scattered Spider's known naming conventions—indicating potential phishing infrastructure either in use or prepared for future attacks. While some of these domains appear to target technology, retail, and aviation organizations, others impersonate companies across a much broader set of industries, including manufacturing, medical technology, financial services, and enterprise platforms. This cross-sector targeting underscores the group's opportunistic approach, adapting to high-value vulnerabilities rather than focusing on a specific vertical.Examples of observed domains include:

- chipotle-sso[.]com
- gemini-servicedesk[.]com
- hubspot-okta[.]com

While not all domains are confirmed to be actively malicious, their alignment with known TTPs (tactics, techniques, and procedures) strongly suggests targeting intent.

These findings further highlight the importance of industry-agnostic threat monitoring and reinforce that no sector is immune from sophisticated social engineering campaigns.

Group Overview: Who Is Scattered Spider?

Publicly available intelligence outlines Scattered Spider as:

- Active since at least 2022, composed primarily of young individuals (ages 19–22) from the US and UK
- Financially driven, targeting ransomware, credential theft, and cloud infrastructure
- Utilizing advanced social engineering techniques, including MFA manipulation and voice spoofing
- Employing remote access tools and malware for persistent intrusion

Tools & Techniques Used by Scattered Spider

Scattered Spider employs a broad range of sophisticated attack methods to infiltrate targets and maintain long-term access:

Social Engineering Methods:

- Targeted phishing
- SIM swapping
- Multi-Factor Authentication (MFA) fatigue (“push bombing”)
- Phone and SMS impersonation
- Tricking employees into installing remote access tools
- Capturing one-time passwords or coercing users to approve MFA prompts

Remote Access Tools:

- Fleetdeck.io, Level.io, Ngrok, Pulseway, ScreenConnect
- Splashtop, Tactical RMM, Tailscale, TeamViewer
- Mimikatz (credential dumping tool)

Malware:

- WarZone RAT (leaked version)
- Raccoon Stealer
- Vidar Stealer

Ransomware:

- BlackCat / ALPHV (Ransomware-as-a-Service)

Comprehensive Recommendations

Check Point recommends the following defensive strategies tailored for both enterprises and aviation organizations:

For Enterprises:

- **Domain Monitoring:** Continuously scan domain registrations and block suspicious ones matching Scattered Spider patterns.
- **Employee Training:** Conduct simulations and awareness training focused on MFA abuse and vishing.
- **Adaptive Authentication:** Deploy smart MFA solutions with behavioral anomaly detection.
- **Endpoint Security:** Ensure robust endpoint detection and response across the organization.

For Aviation Sector Organizations:

- **Vendor Risk Management:** Audit third-party service providers, particularly call centers, for access controls and security maturity.
- **Strong Identity Verification:** Require layered verification for password resets and MFA-related support requests.
- **Sector-Specific Incident Response:** Establish response playbooks tailored for data breaches involving passenger data and loyalty platforms.

Check Point Solutions to Mitigate Scattered Spider Threats

To effectively counter these emerging risks, Check Point recommends the following security platforms:

- **Check Point Harmony Email & Collaboration:** Prevents phishing and impersonation attacks across inboxes and communication apps.
- **Check Point Harmony Endpoint:** Detects and mitigates threats at the endpoint before they spread.
- **Check Point CloudGuard:** Secures multi-cloud environments and prevents credential-based access abuse.
- **Infinity ThreatCloud AI:** Powers threat intelligence with AI to deliver proactive defenses.
- **Check Point Quantum Security Gateway:** Provides scalable network security with real-time threat prevention.

Further Reading & Resources

Explore additional resources on Scattered Spider:

- CyberInt: Meet Scattered Spider
- HC3 Threat Actor Profile – Scattered Spider (October 2024)

For real-time intelligence and updates, visit Check Point's blog.
