Recent Scattered Spider Infrastructure Hints at Possible Targeting of Oil and Gas Industry

Overview

Active since late 2022, Scattered Spider is a sophisticated threat actor group consisting of mostly U.S. and U.K. residents best known for adept social engineering leveraging native fluency in English, as well as phishing to gain initial access to enterprise environments.

The group has previously enabled major ransomware attacks, such as the BlackCat/ALPHV compromise of MGM Resorts in 2023 and has made a recent return to headline-grabbing attacks in 2025. So far this year, Scattered Spider has targeted organizations sector-by-sector, initially focusing on retail, then insurance, and more recently aviation, indicating a possible trajectory toward critical infrastructure.

Recent reporting from Doppel Threat Intelligence notes that alongside a spike in aviation-themed domains, Scattered Spider has registered a significant number of oil and gas-themed domains. This parallel activity raises concerns that the group is pivoting its focus towards the energy sector. This development is particularly alarming for organizations in Alberta – a central hub for Canada's oil and gas industry. It underscores the urgent need for heightened vigilance and proactive domain-monitoring practices across Alberta's critical infrastructure.

Resource Development: Common Patterns in Scattered Spider Domains

Threat researchers from multiple organizations have independently aligned their recent analyses of Scattered Spider around a common theme: domain registration patterns. Silent Push, ReliaQuest, and most recently, Doppel Threat Intelligence Group have each observed similarities across the domains attributed to Scattered Spider. Across their respective reports, the following characteristics consistently emerge:

- The presence of the helpdesk or authentication themed keywords
  - "info"
  - "support"
  - "help"
  - "service"
  - "vpn"
  - "internal"
  - "connect"
  - "duo"
  - "okta"
  - "mfa"
  - "sso"
  - "corp"
  - "helpdesk"
  - "schedule"
  - "Servicenow"
  - "hardware-refresh"
  - "rsa"
- Common top-level domains (TLDs)
  - ".com"
  - ".co"
  - ".us"
  - ".net"
  - ".org"
  - ".help"

- The hyphenation of the above-mentioned keywords with target company names (e.g., **hepdesk-company[.]com**), subdomain variations (e.g., **helpedesk.company[.]com**), and typosquatted domains with keywords (e.g., **helpdeskc0mpany[.]com**).
- Domains resolve to IPs from preferred hosting providers
  - AS39287 (ABSTRACT, FI)
  - AS13335 (Cloudflare, Inc)
  - AS399486 (VIRTUO, CA)
  - AS14061 (DigitalOcean, LLC)
  - AS20473 (Choopa, LLC)
  - AS47583 (Hostinger)
  - AS63949 (Akamai-Linode)
  - AS22612 (Namecheap)
- Use of preferred domain registrars
  - NiceNIC
  - Hosting Concepts
  - NameSilo
  - GoDaddy

These patterns can support user-awareness training aimed at identifying potential Scattered Spider domains but can also aid network defenders in investigating domains impersonating their organization or affiliated third parties and authentication platforms.

Initial Access: Social Engineering Unlike Many Others

Scattered Spider is best known for leveraging sophisticated social engineering and phishing techniques to gain initial access.

The group frequently deploys phishing campaigns using domains crafted with the Evilginx framework to mimic enterprise login portals, such as Okta or VPN gateways, to harvest credentials and session tokens. These phishing sites are often fronted by spoofed browser challenges, including fake Cloudflare Turnstiles, designed to evade detection by automated security scanners.

In parallel, they employ English-speaking operators with native-level fluency to conduct highly convincing voice-based attacks targeting organizations in Western countries – primarily Canada, the U.S., the U.K., and Australia. Although Scattered Spider has been observed directly targeting organizations, the group favors compromising third-party IT providers and managed service platforms (MSPs). This strategy allows them to achieve one-to-many access, forcing organizations to assess both direct and third-party exposure.

While many of Scattered Spider's techniques are used by other threat actors, it is the group's exceptional use of reconnaissance and social engineering to exploit human vulnerabilities that set them apart. After profiling target organizations and employees through sources such as LinkedIn and ZoomInfo, Scattered Spider uses this intelligence to craft highly tailored attacks.

Help desks are heavily targeted with vishing calls, during which Scattered Spider impersonates employees to persuade support staff into resetting credentials for initial access or enrolling attacker-controlled devices onto MFA for persistence and defence evasion. These calls are often augmented with spoofed caller IDs and real-time coaching to sustain a convincing pretext and increase the likelihood of success. And in previous cases, they've employed SIM swapping to bypass SMS-based multi-factor authentication by hijacking victims' phone numbers.

Recommendations

To help mitigate the threat from Scattered Spider, network defenders of critical infrastructure are encouraged to consider adopting the following measures:

- **Proactively investigate network logs for activity associated with potential Scattered Spider domains.** Leverage your organization's telemetry to hunt for connections to domains containing known Scattered Spider-related keywords. This could help uncover previously undetected malicious activity in your environment.

- **Analyze recently registered domains for early indicators of attack.** Analyze new domain registrations using the patterns outlined in this and other threat reports. This may help identify any impersonation attempts of your organization directly, or key third-party partners.
- **Raise awareness to the Scattered Spider threat among users and help desk personnel.** While tracking domains can be valuable, the patterns driving their creation will evolve, making tracking difficult, yet the attacks leveraging them persist. This places a requirement on enhanced user awareness training updated to include Scattered Spider's sophisticated social engineering techniques, and use of phishing kits that mirror organization assets. Training should be provided to internal users and third-party partners, particularly outsourced help desk personnel.
- **Ensure deployment of phishing-resistant MFA and periodically review MFA enrolments.**
  - Enable MFA as a requirement for connections from third-party partner to internal networks to mitigate lateral movement opportunities.
  - Ensure MFA is performed via an authenticator app instead of SMS-based, mitigating SIM-swapping attacks previously performed by Scattered Spider.
  - Conduct periodic reviews of MFA enrolments to uncover anomalous activity.