Scattered Spider and Other Criminal Compromise of Outsourcing Providers Increases Victim Attacks

By Halcyon RISE Team

Published: 2025-07-02 · Archived: 2026-04-05 17:17:27 UTC

Independent Halcyon research and open-source intelligence have identified several recent instances of cybercriminals, including Scattered Spider, compromising call centers and other third-party service companies—known as Business Process Outsourcing (BPO) providers—to facilitate their attacks against larger numbers of victims, often focused in one or a few sectors.

In the first half of 2025, these compromises have enabled threat actors to steal hundreds of millions of dollars from a crypto firm, as well as Scattered Spider's compromise of multiple victims in the retail and insurance industries.

Executive Summary:

- Enforce phishing-resistant MFA (e.g., number-matching, hardware tokens) across both internal users and third-party service accounts.
- Eliminate voice/text-based MFA and disable legacy authentication protocols to prevent credential replay and bypass.
- Audit access and activity from BPO or managed service provider (MSP) partners, especially device monitoring, privileged access use, and insider risk reporting.
- Monitor for spoofed domains, suspicious login flows, or cloned authentication pages—especially those mimicking helpdesk or HR communications.

Operational Impact

A successful intrusion at a BPO can lead to rapid lateral access across dozens of client environments, introducing a dangerous multiplier effect for organizations that rely on third-party service providers.

Recent Scattered Spider attacks against UK retail and US insurance industries likely originated, at least in part, from the group's compromise of BPO companies. Scattered Spider (also tracked as UNC3944, Starfraud, Scatter Swine, and Muddled Libra) has shown sustained activity since 2022. The group is highly adept at social engineering, often masquerading as IT staff, and is known for deep reconnaissance of victim environments before moving to active stages of attack.

Scattered Spider has used BPO compromise at least since its compromise of a major casino in 2023. As the group intensifies its focus on high-value sectors in the United States, use of BPO providers without additional safeguards presents a significant supply chain risk.

For business leaders, this represents more than an IT issue—it's a business continuity risk. Threat actors can lock down cloud infrastructure, steal sensitive IP, or extort companies with stolen data. In extreme cases, organizations may lose access to their primary identity providers or SaaS environments, halting operations for days or weeks. The cost of such an attack can far exceed ransom demands, with reputational damage, legal exposure, and operational losses compounding quickly.

This report expands upon the Halcyon analysis of Scattered Spider's attack chain and pulls back the curtain on their suspected BPO-centric attack lifecycle. What follows is a phase-by-phase breakdown specific to the group's leveraging of BPO providers mapped to the MITRE ATT&CK framework to equip defenders with the context and understanding needed to detect, disrupt, and reduce organizational risk regarding this evolving and highly impactful ransomware threat.

Targeting and Industry Rotation

Scattered Spider demonstrates a calculated and opportunistic targeting strategy, rotating across industries and geographies based on visibility, payout potential, and operational heat. The group recently shifted its focus more heavily toward US sectors such as transportation (aviation)—industries with high reliance on remote access infrastructure and high-value extortion potential. This adaptive targeting pattern allows Scattered Spider to stay operational and profitable even as defenders close gaps in previously targeted regions and sectors.

Other known sectors targeted by the group include insurance, manufacturing, and food production—all of which are heavily reliant on BPOs, third-party SaaS platforms, and remote access tools. These industries often present complex supply chains, inconsistent security hygiene, and high consequences for downtime, making them ideal candidates for extortion-based operations.

This adaptive strategy allows Scattered Spider to remain operational and profitable even as law enforcement attention intensifies, reinforcing the need for cross-sector threat intelligence sharing and proactive detection of lateral movement within interconnected vendor environments. [T1589.001, T1591.002, T1598.002, T1584]

Insider Recruitment & BPO Weaknesses

Scattered Spider has consistently leveraged insider recruitment as a strategic enabler, particularly within poorly monitored BPO environments. These operations often exploit a combination of social engineering, financial incentives, and personal vulnerabilities to convince employees to facilitate access or execute specific tasks on behalf of the attackers.

Recruitment efforts typically begin via platforms like LinkedIn, Telegram, or WhatsApp, where operators identify individuals with privileged access or exposure to identity systems, customer service platforms, or endpoint tooling. Employees facing financial stress, social instability, or limited institutional oversight are especially at risk. In some cases, insiders are paid by the threat actors to install remote access software, approve MFA prompts, or temporarily hand off control of their session. In others, they may be asked to test detection boundaries by deploying tooling or copying files.

These insider facilitators are instrumental in establishing or maintaining long-term access—particularly in BPO environments where endpoint logging, identity governance, or behavioral monitoring is limited or fragmented.

[T1585.001, T1586.003, T1566.002]

Initial Access

After gaining access to a BPO provider, initial access vectors against downstream victims would likely have included credential phishing via spoofed HR messages (e.g., fake reduction-in-force notifications) and IT alerts crafted to induce urgency or compliance.

These lures are typically engineered using typographical obfuscation (e.g., Cyrillic characters, swapped letters) and link to cloned login portals that closely mimic legitimate authentication pages, often replicating the organization's exact MFA workflow, such as Duo push prompts or Okta sign-ins.

In parallel, callback phishing campaigns may have been used to reinforce trust or escalate access. Victims receive messages over email or Microsoft Teams instructing them to call a fake support number, where operators impersonate IT staff and guide users through downloading remote access tools like AnyDesk or ScreenConnect.

This hybrid social engineering approach allows the attackers to bypass technical controls and gain interactive access to privileged user sessions, effectively accelerating the compromise chain. [T1566.001, T1566.002, T1078]

Persistence and Privilege Escalation

Once inside, the threat actors likely enrolled new MFA tokens to maintain persistent access and evade detection. They have been observed using Azure Intune to execute Base64-encoded PowerShell payloads, which deploy additional tooling or manipulate device management policies. This allows them to sideload custom endpoint detection and response (EDR) bypasses or maintain long-term presence under the guise of legitimate administrative activity.

To escalate privileges, the group may exploit misconfigurations or leverage existing elevated accounts, including service principals or unattended admin sessions. In multiple documented cases, Scattered Spider actors removed all global administrators from compromised Azure tenants, effectively locking out defenders and delaying remediation.

This tactic disables centralized visibility and control, forcing victims into a reactive position and complicating recovery timelines. Additionally, the group is known to persist via compromised service accounts or devices masquerading as trusted endpoints, further reducing the likelihood of detection. [T1078.004, T1546.008, T1068, T1548]

Data Exfiltration

The group likely focused heavily on the exfiltration of internal IT documentation like detailed blueprints of the victim's infrastructure, access controls, and privileged workflows. These documents often contain hardcoded credentials, API tokens, cloud tenant mappings, network diagrams, and service account usage patterns, making them incredibly valuable for both immediate exploitation and resale to other threat actors.

Scattered Spider actors have been observed using legitimate backup and file replication tools like Veeam, as well as cloud storage services such as Mega, GoFile.io, Transfer.sh, and Zenfiles, to exfiltrate this data covertly. In

more sophisticated cases, exfiltration occurs through compromised cloud tenants, allowing attackers to stage and transfer data under the guise of normal business operations. These tactics allow the group to bypass outbound filtering and detection, especially in environments where backup or sync tools are already allow-listed by default.

The result is a high-fidelity theft operation that is often completed before encryption or other disruptive actions occur, giving Scattered Spider significant leverage during the extortion phase. [T1041, T1567.002]

Ransomware Deployment

Encryption is typically not the immediate goal for Scattered Spider, but rather an escalation tactic deployed when victims resisted extortion demands or showed signs of initiating incident response. This approach aligns with a broader data-first extortion model, where the threat actor seeks to monetize exfiltrated information before triggering visible disruption.

The group has been linked to multiple ransomware payloads, including Akira, Play, Qilin, and DragonForce, each of which offers varying degrees of customization and stealth. Notably, Scattered Spider appears to favor Conti-based encryptors, which are designed for speed and irreversibility. These payloads typically employ multi-threaded AES-256 encryption, with RSA-based key wrapping, and leave no built-in decryption path outside of payment. This technical choice reflects a strategic intent to maximize pressure on the victim, either to push them toward ransom negotiations or punish them for defiance.

Because encryption is often delayed until late in the attack lifecycle, organizations may not realize they have been compromised until business operations are already at risk. [T1486, T1489, T1562.001]

Detection and Containment Gaps

Scattered Spider's use of Bring Your Own Vulnerable Driver (BYOVD) techniques, endpoint detection and response (EDR) evasion via custom Rust- and Go-based binaries, and selective targeting of poorly monitored systems reveals a sophisticated awareness of modern detection blind spots. BYOVD payloads are often deployed to disable kernel-level protections, terminate EDR processes, or sideload malicious code under the guise of legitimate drivers. These drivers are sometimes custom-compiled or sourced from leaked vulnerability repositories and paired with obfuscated loaders to further reduce detection.

In addition to BYOVD, the group develops lightweight custom payloads often written in Rust or Go that are designed for speed, in-memory execution, and low forensic footprint. These payloads may be used to disable logging, bypass Antimalware Scan Interface (AMSI), or interact directly with APIs to enumerate or disable endpoint defenses.

Scattered Spider prioritizes lateral movement toward systems explicitly excluded from monitoring, such as public-facing web apps, jump boxes, or environments running legacy software. They also take advantage of over-permissive allow-lists within EDR and Security Information and Event Management (SIEM) tooling by staging payloads in directories trusted by default or used by third-party applications. This allows them to remain undetected long enough to deploy payloads or exfiltrate data. [T1027, T1218, T1562, T1053.005, T1548.002, T1611]

Behavioral Triggers

Operators closely monitor internal communications, ticketing systems, and file shares for any reference to their aliases or activity, including names like Scattered Spider, Muddled Libra, Starfraud, or related IOCs. This internal surveillance is often enabled through compromised email inboxes, cloud admin panels, or service accounts with access to shared collaboration tools. Their goal is to identify when defenders have detected their presence or are preparing for an incident response operation.

Mentions of specific security vendors such as Halcyon, CrowdStrike, or Mandiant can serve as a trigger for attack escalation. When detected, operators are known to shift into a rapid execution phase, deploying ransomware and locking out admin users within hours, sometimes the same day. In many cases, these accelerations occur before the victim's security team has a chance to fully mobilize.

This defensive evasion tactic transforms passive reconnaissance into an active kill switch, where the threat actor controls when and how disruption occurs based on perceived detection. [T1114.002, T1087.002, T1056.001]

Group Structure and Tradecraft Variation

Scattered Spider operates as a decentralized but tightly aligned group, with a clear division of roles and responsibilities among its members. Senior operators and group leaders often function as project managers, coordinating initial access brokers, ransomware affiliates, and negotiators while managing communications and operational timing. Meanwhile, junior affiliates or newcomers are frequently observed conducting lower-tier operations to prove themselves, such as deploying off-the-shelf tools, testing detection thresholds, or handling initial phishing campaigns.

This tiered structure results in variable tradecraft: some intrusions are executed with extreme speed and precision featuring ransomware deployment in under an hour, while others involve weeks of stealthy lateral movement, data staging, and extortion preparation. Tradecraft variation is often a function of operator maturity, assigned objective, and the group's perceived level of urgency. In some cases, operators deliberately slow-roll intrusions to avoid triggering defenses and preserve long-term access to high-value targets.

The group's organizational model enables scalability while minimizing risk exposure and may draw talent or tooling from other ransomware crews, including former members of Conti or Black Basta. [T1583.001, T1584.001, T1585.002]

Detection, Mitigation & Incident Response

Organizations should assume that Scattered Spider or similar threat actors may already be present within outsourced environments, particularly BPO infrastructures. Effective response requires:

- **Strengthen Endpoint Coverage:** Ensure all systems—especially those managed by vendors—are protected with EPP and EDR/XDR. To detect attacks that routinely evade traditional tools, organizations should also deploy dedicated anti-ransomware and anti-exfiltration solutions capable of identifying stealthy encryption and data theft behaviors.

- **Log Visibility Across Third Parties:** Ensure security teams have access to relevant logs, including authentication events, from vendors and support providers.
- **Audit Remote Tools:** Look for unauthorized or excessive use of remote monitoring and management (RMM) tools (e.g., AnyDesk, ScreenConnect, Atera) and scripting platforms such as PowerShell or cmd-based launchers.
- **Watch for Intune Abuse:** Monitor for unusual Base64 task execution through Microsoft Intune or similar platforms.
- **Detect MFA Changes:** Flag unexpected MFA device registrations—especially from unrecognized geographies or source networks.
- **Monitor for Known C2 Patterns:** Block or alert on traffic to ngrok, Mega, GoFile.io, and similar services often abused for command-and-control or exfiltration.
- **Harden Identity Infrastructure:** Temporarily disable legacy authentication, enforce conditional access policies, and cut SSO integration into critical tools in the event of an incident.
- **Prepare for Tenant Lockout Scenarios:** Develop and rehearse recovery playbooks that assume loss of control over cloud tenants or identity providers.

Conclusion

This report builds on prior Halcyon analysis of Scattered Spider's TTPs to spotlight how supply chain exposure—particularly through Business Process Outsourcing (BPO) providers—can rapidly cascade across sectors and borders. The group's use of social engineering, insider recruitment, and infrastructure abuse illustrates how modern ransomware actors have evolved into full-spectrum, persistent threats capable of operating across both technical and human attack surfaces.

Organizations will reduce this significant risk by going beyond hardening internal defenses, to also continuously assess the security posture of their third-party partners, especially those with elevated access or remote management roles. This includes validating identity governance controls, understanding how insider risk is reported and managed, and ensuring visibility into outsourced operations.

Halcyon eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies – talk to a Halcyon expert today to find out more, and check out our quarterly RaaS and extortion group reference guide, Power Rankings: Ransomware Malicious Quartile.
