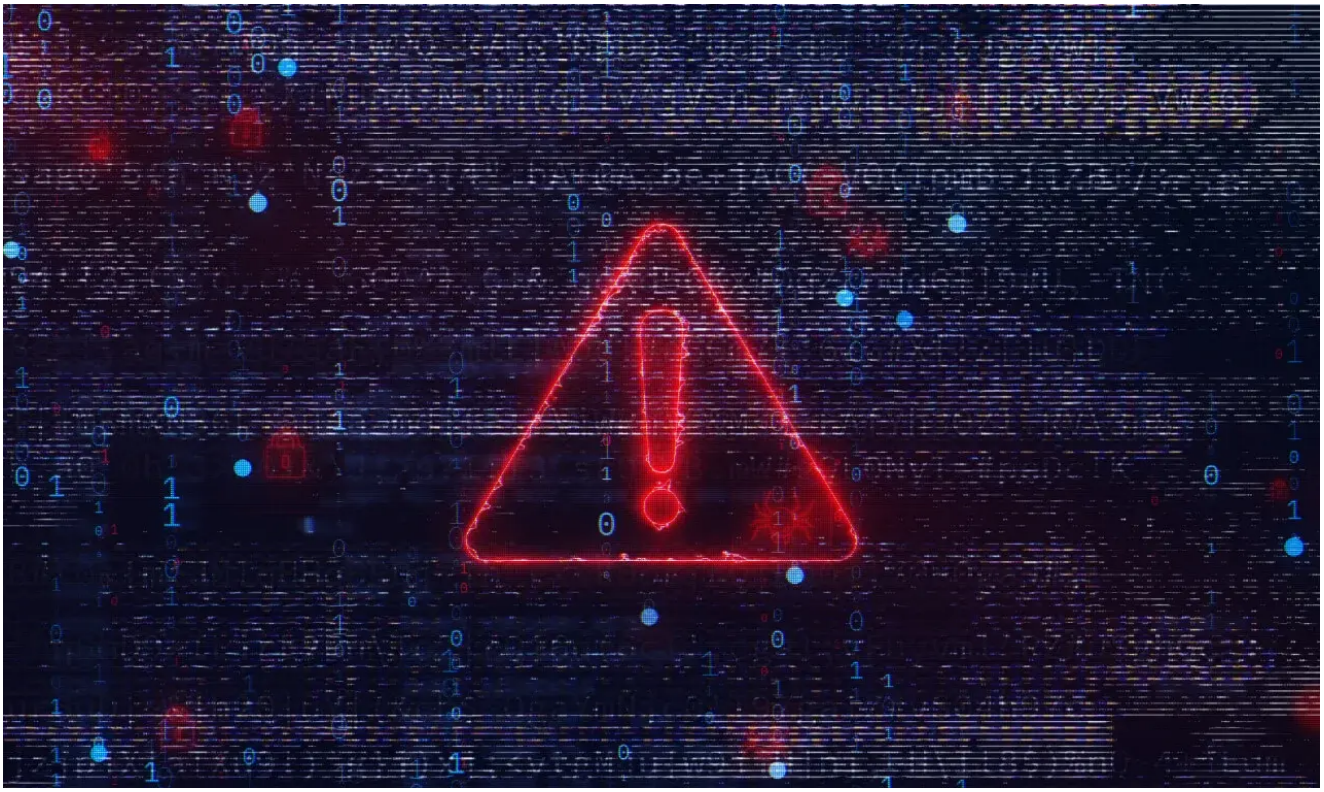
Scattered Spider: Rapid7 Insights, Observations, and Recommendations

rapid7.com/blog/post/scattered-spider-rapid7-insights-observations-and-recommendations/



Overview of Scattered Spider and recent activity

Scattered Spider (also tracked as UNC3944, Scatter Swine, Muddled Libra, among other aliases) is a financially motivated cybercriminal group active since at least May 2022. The group is notorious for targeting large enterprises — especially telecommunications, outsourcing firms, cloud/tech companies, and more recently, retail, finance, and the airline sector — often by exploiting IT help desks via social engineering.

Incidents taking place in the past few months — including high-profile breaches of UK retailers and airlines — demonstrate that Scattered Spider continues to refine its tactics and broaden its targets. Based on this escalation, we recommend practitioners become more familiar with their tactics and increase their vigilance by implementing defense best practices.

Below, we outline the group's known tactics, techniques, and procedures (TTPs), highlight novel elements observed in a recent case, and provide defensive recommendations.

Tactics, techniques, and procedures (TTPs)

Over the years, Scattered Spider has evolved from primarily conducting phishing and SIM-swapping campaigns targeting telecom and tech firms to executing full-spectrum, multi-stage intrusions across cloud and on-prem environments. Their tactics have matured to include sophisticated help desk impersonation, exploitation of identity infrastructure, abuse of legitimate tools like AWS Session Manager and Teleport for persistence, and even defense evasion via bring-your-own-vulnerable-driver (BYOVD) techniques. Despite arrests, the group remains active and adaptive, expanding targets and tactics while maintaining its core identity-focused attack strategy.

Scattered Spider's operations typically involve data theft for extortion and sometimes ransomware deployment in collaboration with groups like ALPHV/BlackCat.

Initial access via social engineering (phishing/vishing)

Scattered Spider is an expert in social engineering, relying on human deception to gain initial access. Common techniques include phishing emails/SMS and phone-based attacks (vishing). Notably, the group often impersonates company IT staff or help desk personnel in calls or texts to trick employees into revealing credentials or performing unsafe actions.

For example, Scattered Spider actors have:

- Phished for credentials and MFA codes via fake login pages or real-time interception of one-time passwords. (This aligns with MITRE ATT&CK techniques Phishing (T1566) and Phishing for Information (T1598)).
- Posed as IT support via phone/SMS to convince victims to share their multi-factor authentication code or to *install remote access software*, granting the attacker a foothold. (Related ATT&CK: User Execution of Malicious Tools – T1204, – Remote Services T1219).
- MFA fatigue "push bombing" — sending repeated MFA requests to prompt a user to accept out of annoyance — to defeat MFA protections (ATT&CK: T1621 Multi-factor Abuse).
- SIM swapping to hijack a target's phone number (and thereby intercept MFA SMS codes).

A hallmark of Scattered Spider's initial access is the help desk scam. The attacker calls an organization's IT help desk, armed with personal details of an employee (often scraped from sources like LinkedIn), and impersonates that user with a convincing backstory. The goal is to persuade the help desk to reset the user's password and/or MFA device, thus handing control of the account to the attacker. By targeting high-privilege or sensitive accounts for these resets, Scattered Spider often sidesteps the need for traditional privilege escalation — they start with the keys to the kingdom.

Persistence and remote access tools

Once inside a network or cloud environment, Scattered Spider establishes persistence using legitimate remote administration tools. The group has shown a preference for commercial remote monitoring and management (RMM) tools and remote desktop software, repurposing them as backdoors. According to the FBI/CISA, they have been observed using tools like TeamViewer, ScreenConnect (ConnectWise Control), Splashtop, AnyDesk, Ngrok tunnels, FleetDeck, and more. These legitimate tools enable stealthy remote access since they blend in with IT usage (ATT&CK T1219 – Remote Access Software). In past cases, Scattered Spider also leveraged VPN clients and even built-in OS features to maintain access. For example, they have used Windows Scheduled Tasks for persistence (ATT&CK T1053), as well as created new accounts or used stolen valid accounts (ATT&CK T1078) to ensure continued access.

A novel persistence mechanism Rapid7 observed in an incident was the use of Teleport, an infrastructure access platform not previously associated with this group. After obtaining admin-level cloud access, the attacker installed a Teleport agent on compromised Amazon EC2 servers to establish a persistent remote command-and-control (C2) channel. Teleport is a legitimate open-source tool for managing remote infrastructure, but here it was co-opted for malicious purposes. This effectively gave the attacker persistent remote shell access to those cloud servers even if their initial user credentials or VPN access were revoked. The use of Teleport indicates Scattered Spider's adaptability in using new tools for persistence and command-and-control. By using standard administrative software, they reduce the chance of detection by security tools that might flag custom malware.

Lateral movement and cloud techniques

Scattered Spider's operations often span both cloud and on-premises environments. Once initial access is gained (for instance, via a compromised user account), the group performs extensive reconnaissance and lateral movement to expand their foothold:

- **Cloud environment enumeration:** Systematically listing EC2 instances and queried IAM instance profiles via AWS API calls. Such information could allow the attacker to assume roles or find trust relationships to pivot further (mapping to ATT&CK T1526 – Cloud Service Discovery). These techniques illustrate Scattered Spider's competence in abusing cloud management tools for lateral movement (ATT&CK T1563.002 – Remote Services: Cloud Management Console). The use of built-in cloud tools (SSM, console) allows the attackers to move within a victim's cloud environment without deploying custom malware.

- **On-premises lateral movement:** When Scattered Spider pivots into corporate networks (often after obtaining VPN or Okta access through stolen credentials), they employ standard internal tactics. They have been observed using Windows Remote Desktop (RDP) and SMB (psexec) to move between machines (ATT&CK T1021 and T1569.002). With any harvested or high-privilege credentials, Scattered Spider will try to move laterally and escalate privileges — for instance, attempting to RDP into additional servers or using admin shares via PsExec. This on-prem activity aligns with many MITRE ATT&CK techniques, such as Credential Dumping (T1003) and Internal Reconnaissance (T1016). Importantly, Scattered Spider's initial social engineering often gives them elevated access from the start, but they still perform internal recon to identify valuable systems (databases, file servers, etc.) and to ensure they maintain access via multiple pathways.

Tools, malware, and evasion techniques

Unlike nation-state APTs, Scattered Spider largely relies on off-the-shelf tools and living-off-the-land techniques rather than custom malware. Their toolkit includes:

- **Legitimate administrative tools** for remote access and persistence (as noted, TeamViewer, AnyDesk, ConnectWise, Teleport, etc.). These don't trigger antivirus and provide full interactive control.

- **Credential theft tools** like Mimikatz (for extracting Windows passwords and hashes). Dumping credentials allows them to pivot and possibly achieve domain administrator privileges if not already obtained.

- **Custom exploit tools:** The group has exploited known vulnerabilities to broaden access. For example, Scattered Spider has been linked to exploitation of CVE-2021-35464 (ForgeRock AM) to achieve remote code execution in a victim's AWS-hosted identity service, and even legacy bugs like CVE-2015-2291 in Intel driver software to run code in kernel mode. They are adept at identifying and abusing misconfigurations or unpatched systems to advance their attack (ATT&CK T1190 – Exploit Public-Facing Application).

- **Defense evasion via BYOVD:** A particularly advanced tactic in Scattered Spider's playbook is using malicious or vulnerable drivers to disable security software. They have deployed a toolkit known as STONESTOP and POORTRY, which involves a userland loader (STONESTOP) installing a malicious signed driver (POORTRY) to kill processes like endpoint protection agents. By using a Microsoft-signed vulnerable driver (the BYOVD technique), they bypass driver signature enforcement and terminate antivirus/EDR services. This tactic (ATT&CK T1562.001 – Disable or Modify Tools) allows the group to operate without detection during critical phases of the attack, such as data exfiltration or ransomware deployment.

- **Extortion and ransomware:** Scattered Spider's end goals are typically data theft and extortion. In some intrusions, they have partnered with or acted as affiliates of ransomware gangs. The group has been associated with ALPHV/BlackCat ransomware deployments and more recently with the DragonForce ransomware (as seen in the 2025 attacks on UK retailers). Even when ransomware is used, the emphasis is often on exfiltrating sensitive data first — enabling the attackers to threaten leaks for payment (a double extortion approach). If the victim refuses to pay, the impact can be severe: for example, in the MGM Resorts casino attack of 2023 (attributed to Scattered Spider), the hackers stole ~6 TB of data and caused widescale IT outages, reportedly costing the company $100M+ in damages.

Defensive best practices and recommendations

Defending against Scattered Spider requires a combination of hardened identity security, vigilant monitoring, and user awareness. Given this group's reliance on tricking humans and abusing legitimate tools, enterprises should adopt a *defense-in-depth* approach focusing on both preventive controls and detective measures. Key recommendations include:

- **Strengthen help desk and account recovery processes:** Since help/service desks are a prime target, implement strict verification for password resets and MFA resets. For high-privilege accounts, require multi-factor or multi-person approval for any credential reset or new device enrollment. Consider requiring the user to show up in person or via a verified video call for critical account resets, rather than relying on phone/email requests. Establish clear procedures so that help desk personnel know to verify the requester's identity out-of-band (e.g. calling back a known number on file) and to be wary of urgent pleas or unusual requests. Regularly train help desk staff to recognize social engineering red flags (e.g. callers pressing for quick reset due to an "emergency"). Additionally, limit which support staff can reset admin-level accounts and log all such actions with management oversight.

- **Implement phishing-resistant MFA and monitor MFA changes:** Ensure that all user accounts, especially administrators, use strong MFA methods (FIDO2 security keys or app-based OTP with number matching) that are less prone to social engineering. Educate users never to approve MFA prompts they did not initiate. Deploy MFA push notification protection (such as number matching or limiting push attempts) to counter MFA fatigue attacks. Monitor for unusual patterns like multiple MFA reset requests or device re-enrollments, and consider temporarily suspending self-service resets if suspicious activity is detected. Quick detection of an account takeover — for instance, seeing a new device added for MFA or an IP geolocation anomaly — can allow security teams to intervene before the attacker pivots further.

- **Cloud security and monitoring:** Since Scattered Spider is cloud-fluent, lock down cloud management pathways. For AWS, restrict the use of Systems Manager Session Manager and the EC2 Serial Console to only authorized admin users; generate alerts if these are used from unusual IPs or by new users. Monitor cloud audit logs (AWS CloudTrail, Azure AD logs, etc.) for signs of intrusions — e.g. a spike in GetInstanceProfile or IAM role enumeration calls, or a new IAM user creation that wasn't planned. Use behavior analytics to detect when a normally low-privilege user begins performing admin-level actions in cloud accounts (which could indicate compromise). Employ the principle of least privilege for cloud roles: ensure that an Okta/SSO user account that gets compromised cannot by itself administer the entire cloud environment. For instance, separate high-level cloud admin accounts that are not integrated with regular SSO, and protect them with extra safeguards.

- **Endpoint and network monitoring:** Deploy robust Endpoint Detection and Response (EDR) on servers and workstations to catch suspicious behavior (though keep in mind Scattered Spider's ability to disable some EDRs via BYOVD). Enable features like Windows Driver Blocklist or Hypervisor-Protected Code Integrity (HVCI) to mitigate vulnerable driver attacks, which can stop tools like POORTRY from functioning. Monitor for common post-compromise tools and behaviors: for example, sudden use of PsExec, Mimikatz, or tools launching from temp directories should raise alerts. Network monitoring can also help — e.g. detect new outbound connections to uncommon hosts (such as an IP or domain like teleport.sh if your environment doesn't normally use Teleport) or large data transfers that might indicate exfiltration. Keep system logs for authentication, process creation, and network connections centralized and analyzed for anomalies (failed login sprees, new services installed, etc.).

- **Limit and audit remote administration tools:** Create an inventory of approved remote access tools in your enterprise. Block or tightly control the installation of any remote administration software outside this list (for example, if your IT uses TeamViewer, then block others like AnyDesk or Teleport by policy). At minimum, enable alerts when such tools are executed or when new services (like a Teleport service or ScreenConnect client) are installed on servers. Legitimate tools used maliciously often leave some trace — e.g. an unexpected listening port, a new Windows service, or an outbound connection to a non-corporate server. Regularly audit administrative accounts and sessions; if an IT admin is remotely logging in at odd hours or from foreign IPs, verify it's legitimate.

- **Identity hygiene and least privilege:** Given Scattered Spider's focus on abusing credentials, ensure your identity and access management is robust. Use unique accounts for high-privilege tasks (no employees should use their day-to-day account for domain admin or cloud admin roles). Implement just-in-time elevation for sensitive roles so that even if an account is compromised, the attacker cannot immediately escalate without an approved request. Regularly review user access rights, and disable or remove unnecessary privileged accounts (including contractor or helpdesk accounts that can reset credentials).

  Backup and response plan: Finally, prepare for the worst-case scenario of ransomware or extortion. Maintain offline, encrypted backups of critical data and regularly test your restore procedures. Develop an incident response plan specifically for identity breaches, since Scattered Spider-type incidents move quickly from an account compromise to full domain/domain admin compromise. This plan should include steps like rapidly invalidating all active sessions and tokens (to kick the attackers out), forcing enterprise-wide password resets, temporarily locking down help desk password resets, and engaging incident response teams. Exercise this plan in drills (and include scenarios like a rogue VPN or cloud session popping up) to ensure your team can react swiftly when an attack is in progress.

By combining these measures, organizations can significantly reduce the risk of a Scattered Spider intrusion or limit its impact. This group's techniques, while sophisticated in execution, often exploit lapses in basic security practices — such as over-reliance on help desk identity proofing, or unmonitored use of admin tools. Strengthening those areas, along with user education and modern authentication controls, provides a strong defense against Scattered Spider's blend of social engineering and technical prowess.