Cross-Sector Mitigations: Scattered Spider

Guidance for Proactive Defense

Produced by Financial Services ISAC, Information Technology ISAC, Food and Agriculture ISAC, Health ISAC, Aviation ISAC, Automotive ISAC, Retail and Hospitality ISAC, the Maritime Transportation System ISAC, Electricity ISAC, and the National Council of ISACs, with contributions from Communications ISAC private sector partners

Scattered Spider Threat Analysis

Contents

Scattered Spider Threat Analysis

Introduction

Members of the National Council of ISACs (NCI) assess with high confidence that the threat actor group Scattered Spider presents a real threat, and that its ability to exploit human vulnerabilities through social engineering makes the group a significant risk to organizations.

This analysis details Scattered Spider's activity based on its observed tradecraft across sectors as of May 2025, providing:

- Background on Scattered Spider so that firms can better scope their threat surface
- Technical procedures and cultural practices to thwart Scattered Spider attacks
- Analysis of Information Sharing and Analysis Center (ISAC) member and FBI intelligence and corresponding MITRE ATT&CK® mitigations

The recommended measures have proven effective against Scattered Spider and similar threat actors, according to expert assessment of intelligence. The mitigations incorporate the baseline necessities of FS-ISAC's cyber fundamentals, keyed to Scattered Spider TTPs (tactics, techniques, and procedures) based on known threats.

However, threat actors such as Scattered Spider are constantly innovating, so organizations must be diligent in continually monitoring their processes and identities to look for new exploits.

These findings were produced collaboratively by the Financial Services, Information Technology, Food and Agriculture, Health, Aviation, Automotive, Retail and Hospitality, and Maritime Transportation System ISACs, and the NCI. The NCI comprises 28 organizations and is designed to maximize information flow across private sector critical infrastructures and government agencies.

Scattered Spider Threat Analysis

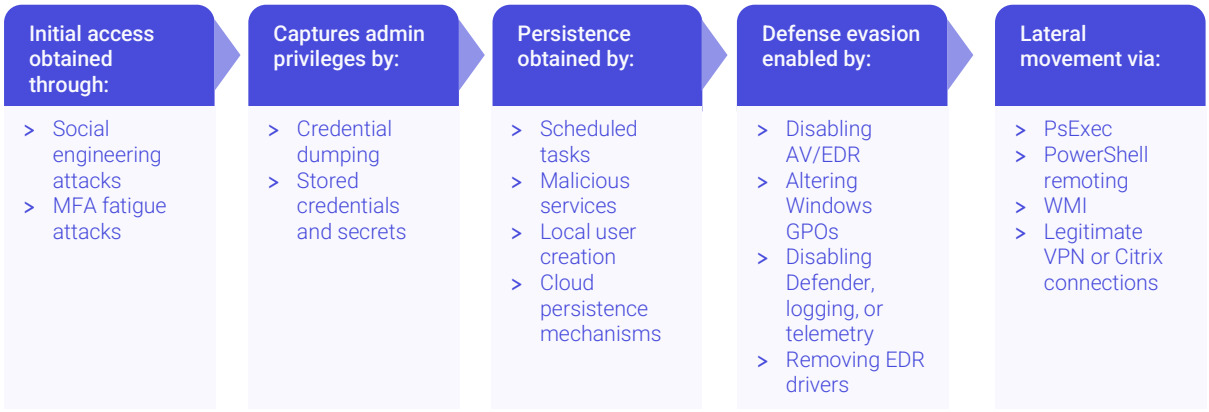
Background and TTPs

Scattered Spider is a financially – rather than ideologically – motivated group of young independent operators in the UK, US, and Canada. According to researchers, Scattered Spider is part of a larger hacking community known as The Community or The Com, which organizes via online platforms, including Discord and Telegram group chats. Scattered Spider uses highly effective social engineering techniques and credential theft to gain entry to target networks, then monetizes its attacks through data theft, extortion, or affiliate ransomware operations. The group is known for its extensive reconnaissance that identifies personas to adopt or employees to target. Much of Scattered Spider's success is attributed to its speed and low-effort, adaptable targeting.

> "The threat actors frequently join incident remediation and response calls and teleconferences, likely to identify how security teams are hunting them and proactively develop new avenues of intrusion in response to victim defenses. This is sometimes achieved by creating new identities in the environment and is often upheld with fake social media profiles to backstop newly created identities."
>
> *Cybersecurity Advisory: Scattered Spider* – a joint Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) advisory

Active since early 2022, Scattered Spider was initially observed targeting telecommunications and business process outsourcing (BPO) entities, likely as a springboard for social engineering operations to gain unauthorized access to other targets and their stakeholders. Since then, the group has been linked to over 100 attacks across multiple market verticals, but tends to target one sector at a time. Scattered Spider is notorious for the 2023 compromise of Caesars Entertainment and MGM Resorts and the 2022 attack on Twilio, which resulted in a supply chain attack that impacted the Signal messaging app. It targeted US and UK retailers in April and May 2025, then shifted its focus to the financial sector, particularly insurance firms, and the aviation sector.

Scattered Spider Threat Analysis



A typical tactic is to persuade IT helpdesk agents to perform self-service password resets (SSPRs) for targeted accounts. Scattered Spider's techniques include the use of short message service (SMS) messages — i.e., texting — and voice phishing (smishing and vishing) to capture credentials for single sign-on (SSO) dashboards, Microsoft Office 365/Azure, VPNs, and edge devices.

The group is also known to hijack multifactor authentication (MFA) via subscriber identity module (SIM)-swapping. Then it defeats MFA via notification fatigue or convinces helpdesk agents to reset the MFA method of targeted accounts.

After successfully compromising a user's account, Scattered Spider operatives register other devices under the account. When it can gain administrative privileges, it creates attacker-controlled accounts within the victim's environment. Then the threat actor establishes persistence for unauthorized access to the victim's environment and builds in redundancy to thwart attempts to remove malware or access.

Subsequent reconnaissance activity includes attempting to discover corporate platforms – including Windows, Linux, Google Workspace, Microsoft Entra ID (formerly Azure Active Directory), Microsoft 365, AWS, and other tools hosted within cloud infrastructure – and moving laterally, downloading the appropriate tools to exfiltrate sensitive data.

Health-ISAC recieved intelligence linking the Amadey botnet to Scattered Spider attacks. The Amadey botnet has been used by ransomware actors such as BlackSuit, BlackBasta, and Akira to drop malware loaders into victim networks. The botnet has evaded law enforcement action against malware-as-a-service (MaaS) platforms, allowing it to evolve since 2018.

Scattered Spider Threat Analysis

This deep understanding of the victim's native infrastructure enables Scattered Spider to execute nefarious follow-on activities. It is through this deep understanding – e.g., their ability to execute living-off-the-land techniques – that the group can evade standard detection methods. The threat group can also deploy malware that drops malicious signed drivers designed to terminate processes associated with security software and delete files.

Scattered Spider uses recently registered and highly convincing phishing domain names that mimic legitimate login portals, especially Okta authentication pages. These domains have a short lifespan or uptime, making detection difficult.

Since 2023, Scattered Spider has been observed using five distinct phishing kits, as the group's deployment strategies have evolved to include Dynamic DNS providers. Additionally, the group has included the Spectre remote access trojan (RAT) into their attack chain for malware deployment on compromised systems to gain persistent access. This malware includes mechanisms for remote uninstallation and brokering connections to additional command and control (C2) servers, suggesting the group may be using C2 infrastructure to conduct post-exploitation actions on victim networks.

Known Domain Names Used by Scattered Spider

- targetsname-sso[.]com
- targetsname-servicedesk[.]com
- targetsname-okta[.]com
- targetsname-cms[.]com
- targetsname-helpdesk[.]com
- oktalogin-targetcompany[.]com

Scattered Spider Cybersecurity Advisory produced jointly by the FBI, CISA, Royal Canadian Mounted Police, Australian Signals Directorate's Australian Cyber Security Centre, Australian Federal Police, Canadian Centre for Cyber Security, and United Kingdom's National Cyber Security Centre

Recommendations

The following recommendations have proven effective for ISAC members. Many are drawn from FS-ISAC's cyber fundamentals, a risk-based, defense-in-depth approach of baseline cybersecurity necessities applicable to organizations at any level of cyber maturity.

Use a multi-channel verification process — No organization should rely on a single channel of communication for employees' password changes or MFA-reset requests. Some firms may benefit from using a predetermined list of questions that only the employee could answer to initiate password and MFA resets. And IT employees should always feel empowered to challenge any other employee's verification request.

Action Steps:

- The IT department should use multi-channel verification, including
  - Verification of requests made via email, text, or phone with a call back on a pre-registered and known-good phone number
  - Static PINs on a physical badge
  - Visual validation
- Employ a vocal password only known to employees, or a set of responses to questions that are not easily guessed, i.e., "What is your mother's maiden name? What was your start date of employment? What is the asset tag of your work laptop?"
- Require two employees to approve certain types of requests — such as large financial transfers — or requests from employees with a high level of privileges.
- Contact the employee's manager when the employee requests a reset of both credentials and MFA.
- Foster a culture where IT staff are expected and empowered to question any unusual or highly sensitive requests, even from executives, without fear of repercussions.

Focus on Social Engineering Tactics — Scattered Spider relies on social engineering exploits and is very creative in its use of phishing, vishing, and smishing. The threat group often instills a sense of urgency in its lures and preys on victims' fears, empathy, and respect for authority. Include those TTPs in simulations and test employees' responses to them.

Action Steps:

- Implement ongoing, mandatory security awareness training and phishing simulations with common and current lures.

- Tailor training to the role — IT helpdesk, customer service representatives, HR staff, and C-Suite executives may require more detailed and specific training on threat actor tactics and current campaigns.
- Train customer service representatives on helpdesk procedures. For example, reinforce that their helpdesk will never ask an employee to install remote assistance software or bypass any security control.
- Use least privilege so that employees, notably customer service representatives, require additional verification from the end user before providing greater access.

Review Social Media Profiles of Admins, Particularly Cloud Admins – Admins' social media profiles and posts can inadvertently display job-related information – i.e., responsibilities, work history, colleagues, daily routine – that threat actors use to tailor attacks (e.g., leveraging travel itineraries to establish credibility or urgency in a vishing campaign). Cloud administrators are particular targets. Obtaining their access privileges would provide threat actors with access to and control over valuable cloud resources and the ability to cause widespread damage. Firms should institute social media policies that describe the information threat actors exploit and prohibit such information in social media posts. Regularly review admins' social media – especially cloud admins' posts – for alignment to the social media policy.

Action Steps:

- Develop and enforce detailed, access-specific social media policies that explain the types of information that are — and are not — permissible to post.
- Conduct audits to ensure compliance.
- Provide training on the risks of sharing sensitive professional details.

Assess Helpdesk Access Rights – Helpdesk rights can drift over time, sometimes giving privileges to all admin consoles, such as mail flow, security controls, etc. Auditing helpdesk access rights ensures alignment with operational needs, while preventing unauthorized access that could be exploited by threat actors like Scattered Spider. Automated management systems enhance oversight.

Action Steps:

- Implement automated systems for continuous monitoring and adjustment of access rights.
- Schedule regular access reviews to ensure alignment with job functions.

Monitor Virtual Machines in Cloud Environments – Implement monitoring tools to provide alerts on unauthorized virtual machine (VM) activities such as suspicious services, abnormal resource usage, and privilege escalation attempts, with protocols to isolate and shut down suspicious VMs swiftly. This rapid response capability is crucial to identifying suspicious activity, preventing potential breaches, and mitigating threats.

Action Steps:

- Develop a list of permitted activities.
- Deploy monitoring and alerting systems and look for gaps in them.
- Establish rapid response protocols for unauthorized activities.
- Eliminate unnecessary RMM tools and incorporate honeytokens around RMM tool usage for early detection and fingerprint definition.
- Configure browsers and tasks to regularly delete persistent cookies.
- Minimize the length of time a web cookie is viable — Scattered Spider uses them to establish persistent access and data exfiltration.

Review Security Controls of Virtual Desktop Infrastructure – Ensure virtual desktop infrastructure (VDI) environments are secured with MFA, and continuously monitor user activities.

Action Steps:

- Review the list of VDI users to ensure it is up to date.
- Enforce MFA.
- Do not permit personal devices to have direct access to Office 365, Enterprise Google Workspace, corporate VPNs, etc.
  - Require phishing-resistant MFA, such as YubiKeys, Windows Hello for Business, etc. Do not trust users to approve MFA requests or give out codes.

- If an organization has VDI to allow third-party access, ensure those VDIs cannot access Secure Shells (SSH) or remote desk protocols (RDP), or reach websites that aren't necessary for the user to perform their job.
- Conduct regular audits and real-time monitoring of all user sessions.
- Confirm there are no MFA via SMS in any applications, including vendor applications. SMS-based MFA can introduce significant risks because:
  - SMS messages can be intercepted because they are unencrypted
  - Attackers can bypass MFA through social engineering
  - Threat actors can gain control of a phone number, intercept SMS messages, and gain unauthorized access via SIM swapping
  - Outages can prevent users from receiving authentication codes

Identify Access Points and Block High-Risk Access – Many organizations must permit employees, regulatory agencies, third-party vendors, and others access to their digital infrastructures. Safeguard all entry points – especially the high-risk ones – with controls or blocks, and assume that all managed service providers are compromised.

Action Steps

- Don't give any third party unfettered access to a corporate network.
- Replace site-to-site VPNs with VDIs using phishing-resistant MFA and zero trust wherever possible.
- Identify and block newly created domains that appear to be potential phishing sites (e.g., typosquatting domain names).
- Block any RAT executables from running on managed devices.
- Block the websites of all known commercial remote assistance tools.
- Implement geographic blocking where feasible.
  - Block commercial VPNs connecting to the corporate VPN or VDI with a service like ip2proxy or Spur.
  - Block device types at the VPN if they are not used by customer service representatives. (Adversaries have often used Android device x86.)

Audit Permissions Granted to HR – Strictly aligning HR permissions with operational necessities protects sensitive employee and financial data.

Action Steps:

- Perform a comprehensive audit of HR access permissions.
- Review vendor and provider access rights.
- Educate HR personnel on cybersecurity risks and proper data handling.

Research Data Movement Utilities in SaaS Applications – Monitoring and tracking data movements within SaaS systems (e.g., Salesforce or ServiceNow) is critical because SaaS applications often have (third-party) Data Movement Utilities available for various purposes and can contain sensitive information.

Action Steps:

- Integrate data movement utility monitoring into log data.
- Set up automated alerts and controls for unusual data activity.

Review Trusted IP Addresses Exempt From MFA – Organizations may lower MFA rigor regarding requests from a trusted network, such as a VPN, office network, etc. Minimizing these MFA exemptions strengthens network access controls, a vital step in securing financial and sensitive data.

Action Steps:

- Reevaluate and update the list of trusted IP addresses in the environment.
- Replace static IP whitelisting with dynamic conditional access policies.

Recognize the Insider Threat Posed by Customer Service Representatives – Scattered Spider often obtains initial access to business systems by tricking customer service representatives – but it also recruits them. Scan for potentially malicious activity regularly.

Action Steps

- Screen customer service representatives' activity for signs of potential compromise such as:
  - A high number of password resets or account views in a short period of time
  - Accessing customer accounts without matching verification steps (e.g., inputting customer PIN, matching to ANI, etc.)
  - "Credential juggling," i.e., logging into VPN under credentials different from those used to access CSR tools
- Search chat/email support text logs for recruitment attempts by using string searches that reference common terms used in solicitations, such as "Telegram," "Wickr," or "Get rich."
- Implement time-bound access for customer service representatives for credentials and VPN, and alert on any logins outside agents' normal working hours.

Scattered Spider Tactics and Mitigations

The following table includes ISAC cybersecurity experts' analysis of intelligence shared by thousands of member organizations. Many of the tactics were discovered by the FBI during investigations of Scattered Spider, which are outlined in the joint CISA and FBI Scattered Spider cybersecurity advisory. The MITRE ATT&CK mitigations are drawn from its analysis of TTPs, based on the organization's real-world observations.

Tactic	Recommended Action	Observed Threat Actor Behavior	MITRE ATT&CK Mitigations
Initial Access	> Apply proper user account management and user training > Keep antivirus software updated > Perform regular systems audit > Enable network intrusion and prevention systems to scan and remove malicious email attachments > Block unknown attachments	Scattered Spider initiates its attacks with social engineering techniques, e.g., SMS or Telegram phishing lures, email impersonation of HR/IT, and vishing using real-time or AI-generated voices. The group also leverages MFA fatigue attacks – the practice of sending so many requests	M1049 M1047 M1031 M1021 M1054 M1018 M1017

	> Restrict web-based content and software configurations to validate emails > Enable phishing-resistant MFA and use OTP-based methods instead of push notifications (M1032) to mitigate MFA fatigue attacks	that the user accepts them out of sheer confusion.	
Privilege Escalation	> Reduce attack surface on endpoints > Install credential access protection against LSA secrets that can be obtained through credential dumping > Disable NTLM and review password policies > Enable privilege account management, process integrity, and user training	After access, Scattered Spider seeks domain admin privileges through credential dumping using tools like Mimikatz or secretsdump. It often targets LSASS, dump NTDS.dit via shadow copies, or searches file systems for stored credentials and secrets (e.g., AWS CLI tokens, logins.json).	M1040 M1043 M1028 M1027 M1026 M1025 M1017 M1047 M1022
Persistence	> Use PowerSploit to explore permission weakness in scheduled tasks used to escalate privileges > Set policies that force scheduled tasks to run with an authenticated account instead of SYSTEM > Restrict file and directory permissions not specific to users or privileged accounts	Scattered Spider maintains persistence through scheduled tasks, malicious services, local user creation, or cloud persistence mechanisms like rogue OAuth apps, MFA registration, and mailbox rules. RMM tools (AnyDesk, TeamViewer, ConnectWise) are often used.	M1047 M1028 M1026 M1022 M1018
Defense Evasion	> Enforce least-privilege access to limit capabilities of the bad actor > Automatically forward logs to a secure repository to prevent local tampering	Scattered Spider disables AV/EDR via BYOVD (e.g., STONESTOP, POORTRY). It may crash endpoint security or alter Windows GPOs. It uses group policy or registry settings to disable Defender,	M1029 M1026 M1024 M1022 M1018

	> Limit file/directory access to prevent payload relocation or deletion > Protect security tools > Restrict file/directory permissions, protecting security tools from unauthorized modification	logging, or telemetry. It may also silently remove EDR drivers.	
Lateral Movement	> Segment networks > Disable WMI where not needed > Restrict accounts that can access WMI remotely > Configure to limit remote access and auditing > Disable PowerShell if not needed or limit script execution ability > Set PowerShell execution policy to execute signed scripts only > Use application whitelisting to block unauthorized scripts > Enable privileged account management to ensure that only select users (e.g., administrators) can access PowerShell but with limited access to certain features	Scattered Spider can move laterally using PsExec, PowerShell remoting, WMI (Impacket), and legitimate VPN or Citrix connections. It targets backup infrastructure, ESXi servers, or high-value admin jump boxes.	M1054 M1049 M1045 M1042 M1040 M1038 M1030 M1026 M1021 M1018
Collection *This attack technique cannot be easily mitigated with preventive controls because it is based on the*	> Use enterprise email solutions in the monitoring and encryption of information sent over emails > Use MFA and out-of-band authentication to verify critical actions initiated via emails (password resets, access requests, etc.)	Scattered Spider stages data using 7-Zip or Rclone, then copies the data to shared drives or cloud sync folders. The group searches Slack/Teams/ Exchange email and browses GitHub and SharePoint for incident response notes, credentials, and VPN setup guides.	M1047 M1041 M1032 M1060 M1018

abuse of system features	> Enforce the principle of least privilege in user account management		
Command and Control	> Utilize network intrusion, detection, and prevention systems > Filter and block traffic to known anonymity and C2 infrastructures > Disable unnecessary remote connection functionality and limit hardware installation	Command and control is often established via public services (GitHub, file.io) or reverse proxies (rsocx). RMM tools provide interactive shell access. The group uses SSH tunneling to bypass perimeter defenses.	M1031 M1037 M1020 M1042 M1038 M1034
Exfiltration	> Enforce network communication policies preventing the use of unauthorized external services	Scattered Spider exfiltrates data to MEGA, Google Drive, etc. via browser uploads, cloud APIs, or Rclone. It may use scripts to automate the extraction of stolen archives.	M1021
Impact	> Enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block execution of files that resemble ransomware > In AWS environments, create an IAM policy to restrict or block the use of SSE-C on S3 buckets > Implement IT disaster recovery plans that contain procedures for regularly taking and resting data backups used to restore organizational data. Store them off-system in a safe and secure location to prevent unauthorized access.	Scattered Spider uses ransomware (BlackCat, DragonForce) to encrypt files on ESXi/Hyper-V environments. It employs scripts to shut down VMs to speed up encryption and avoid locked files. Double extortion follows.	M1040 M1053