Scattered Spider Targets Tech Companies for Help-Desk Exploitation

reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025/

Key Points

81% of “Scattered Spider’s” domains impersonate technology vendors, targeting high-value credentials like those of system administrators and executives.

The group primarily leverages phishing frameworks like Evilginx and social engineering methods like vishing to gain initial access into organizations.

70% of Scattered Spider’s targets belong to technology, finance, and retail trade sectors, making them especially vulnerable to credential theft and ransomware attacks.

Scattered Spider and “DragonForce” are increasingly targeting managed service providers (MSPs) and IT contractors, exploiting their "one-to-many" access to breach multiple client networks through a single point of compromise.

In May 2025, a wave of cyber attacks hit UK retailers, including Marks & Spencer, Co-op, and Harrods, with many attributing the breaches to the notorious hacking collective “Scattered Spider” (aka UNC3944, Octo Tempest). That same month, similar breaches hit

major US retailers. While nothing definitive has tied these incidents to Scattered Spider, their coordinated nature hints at a broader, orchestrated campaign.

Scattered Spider is rewriting the rules of the digital battlefield. What started as a run-of-the-mill SIM-swapping crew has morphed into a global threat, armed with advanced social engineering skills and relentless ambition.

This wave of retail attacks prompted us to dig deeper into Scattered Spider's evolving playbook—exploring how the group constructs its infrastructure and exploits human trust to secure initial access, and investigating whether these incidents represent a coordinated attack against this industry vertical.

In this report, we identified:

- **Scattered Spider's Tactics:** The group relies heavily on social engineering to exploit human trust, combined with phishing campaigns using typosquatted domains and tools like Evilginx to bypass multifactor authentication (MFA).
- **A Focus on Technology:** By targeting managed service providers (MSPs) and IT vendors, Scattered Spider leverages "one-to-many" access to breach multiple organizations through a single compromise.
- **Infrastructure Trends:** 81% of its registered domains impersonate technology vendors. The group has shifted from hyphenated domains to subdomain-based keywords to better evade detection.
- **Actionable Recommendations:** Practical steps organizations can take to mitigate risks, strengthen defenses, and respond effectively to this persistent threat.

What is Scattered Spider?

Scattered Spider is a financially motivated cybercriminal gang associated with the hacking collective "The Community." Originally known for SIM-swapping attacks, the group has evolved into running sophisticated social engineering campaigns. Through strategic alliances with major ransomware operators "ALPHV," "RansomHub," and "DragonForce," Scattered Spider gains access to infrastructure, ransomware deployment tools, and platforms for ransom negotiations. Often fluent in English, its members exploit help-desk systems and impersonate employees to breach organizations, targeting high-value industries like retail trade, technology, and finance. It also focuses on organizations with substantial capital for ransom payments or valuable data to leverage in negotiations.

Our analysis of Scattered Spider's incidents reveals a significant reliance on phishing and social engineering as its primary methods for gaining initial access into organizations. By impersonating trusted platforms using typosquatted domains and phishing kits, it

manipulates victims into divulging credentials and session data. To better understand its tactics and how they link to the wave of retail attacks, we conducted a focused analysis of its domain registration patterns (including specific keywords, hosting providers, and registrars), phishing frameworks, and operational infrastructure.

Scattered Spider's Focus: 81% of Domains Target Tech

Research Methodology

Historical Domain Review

We reviewed a publicly sourced dataset comprising over 600 domains previously linked to Scattered Spider through community-shared indicators of compromise (IOCs) between Q1 2022 and Q1 2025. This analysis focused on domain creation patterns such as specific keywords, registrars, and hosting providers. The goal was to identify high-fidelity patterns that reveal how the group registers and configures domains to impersonate trusted entities and evade detection.

Domain and Subdomain Impersonation Patterns

To assess whether ReliaQuest customers had been potentially targeted by Scattered Spider, we examined domain and subdomain impersonation alerts flagged by ReliaQuest's GreyMatter Digital Risk Protection (DRP) service over the past six months. The analysis focused on identifying domain registrations matching Scattered Spider's previously known patterns, such as:

- Domains and subdomains containing specific keywords like "**okta**," "**vpn**," "**helpdesk**," and "**sso**."
- Typosquatting techniques that slightly alter legitimate domain names to deceive users (e.g., replacing letters with numbers, such as "c0mpany[.]com" instead of "company[.]com").
- Domains hosted by providers and purchased from registrars historically linked to Scattered Spider's operations.

Analysis of Phishing Kit Activity

To better understand Scattered Spider's phishing tactics, we analyzed a cluster of phishing pages created using the "Evilginx" framework—a tool that mimics legitimate login pages to capture credentials and session cookies in real time, bypassing MFA. While the dataset included phishing activity from various actors, we filtered the data to focus on pages aligned with Scattered Spider's tactics, such as specific domain keywords, registrars, and hosting

providers. This analysis aimed to determine whether Scattered Spider is using the Evilginx framework and to identify the types of organizations and systems most frequently targeted through this approach.

Research Findings

Tech Targets

In the weeks after the UK retail attacks, investigators who were allegedly working closely with Marks & Spencer revealed that Scattered Spider exploited compromised accounts from the global IT contractor Tata Consultancy Services (TCS) to gain initial access. The Co-op has also partnered with TCS for over a decade, but the link between TCS and these breaches remains unclear while the incidents are still under investigation.

These incidents illustrate Scattered Spider's strategic focus on targeting IT providers and third-party contractors as a means to infiltrate their clients' networks, rather than attacking retail companies directly. By compromising trusted vendors like TCS, Scattered Spider gains access to multiple organizations through a single point of entry, amplifying its reach and enabling widespread attacks.

Our findings further underscore this focus on IT providers and technology vendors:

- **81% of Scattered Spider's domains impersonate technology vendors**, according to a historical dataset of 600-plus publicly shared IOCs. These domains target services like single sign-on (SSO), Identity Providers (IdP), VPNs, and IT support systems to harvest credentials from high-value users, including system administrators, CFOs, COOs, and CISOs.
- **35% of domains identified in internal GreyMatter DRP alerts belonged to the technology sector**, while **20% were tied to finance** and **15% to retail trade**. This demonstrates Scattered Spider's reliance on tech organizations as gateways, while also highlighting its interest in high-value industries that depend on technology for critical operations and customer data.
- **60% of the Scattered Spiders Evilginx phishing domains targeted technology organizations and vendors.** These domains used advanced phishing kits to bypass MFA and gain access to critical systems across industries.

Highest-Fidelity Indicators

To help organizations detect and respond to Scattered Spider's tactics, we detail below the highest-fidelity indicators uncovered during our analysis. These include domain creation patterns, such as specific keywords and hosting Autonomous System Numbers (ASNs), that

align with the group's known infrastructure and behaviors. Incorporating these indicators into proactive monitoring efforts allows organizations to identify malicious activity early and disrupt Scattered Spider's operations before it can exploit networks.

Recent trends (Q1 2025 to present) show a shift in Scattered Spider's tactics: the group has moved away from hyphenated domains (e.g., SSO-company[.]com)—once a reliable indicator—and now favors subdomain-based keywords (e.g., SSO.company[.]com) to evade automated domain impersonation detections. Organizations must monitor both patterns to effectively identify malicious activity.

Top Keywords:

- "internal," "connect," "duo," "vpn," "helpdesk," "servicenow," "corp," "schedule," "okta," "servicedesk," "rsa," "info," "support," "mfa," "sso," "help," and "service."
- Patterns to watch for:
    - Hyphenated domains, e.g. SSO-company[.]com
    - Subdomain variations, e.g. SSO.c0mpany[.]com
    - Keywords and typo squats without hyphenation, e.g. c0mpanysso[.]com

Top Hosting ASNs:

- AS39287 (ABSTRACT, FI)
- AS13335 (Cloudflare, Inc)
- AS399486 (VIRTUO, CA)
- AS14061 (DIGITALOCEAN-ASN, US)
- AS20473 (AS-CHOOPA, US)

Top Domain Registrars:

- NiceNIC
- Hosting Concepts B.V.
- NameSilo, LLC
- GoDaddy

While these indicators showed the most overlap in our analysis, Scattered Spider frequently changes its infrastructure for domain hosting and domain registration—typically every one to two months. As such, expanding hunts beyond the ASNs listed above is strongly recommended. To effectively hunt for these indicators, we suggest the following:

- **Domain Registration Analysis**: Scattered Spider often creates tailored domains to target specific organizations. Look for newly registered domains containing the keywords listed above alongside your organization's name to identify potential threats early.
- **Automation and Scheduling**: Scattered Spider's domains are typically active for **less than seven days,** making automated or scheduled hunting crucial for timely detection and response. Regular scans of DNS data and network logs can significantly improve detection of these threats.
- **Network Connection Monitoring**: Hunt for network connections to domains that contain the listed keywords and known Scattered Spider domains. These domains often mimic legitimate services to deceive users and gather credentials, making vigilant monitoring critical to detecting suspicious activity.

Implications for Defenders

For groups like Scattered Spider, IT providers are the master key—the ultimate shortcut to infiltrating multiple organizations at once. These providers manage critical systems and valuable data, making them irresistible targets for hackers who want to maximize their impact with minimal effort. These tactics aren't just limited to Scattered Spider. For instance, we observed an XSS forum user (see Figure 1) selling access to a remote monitoring and management (RMM) tool dashboard that manages over 200 hosts across many small businesses.

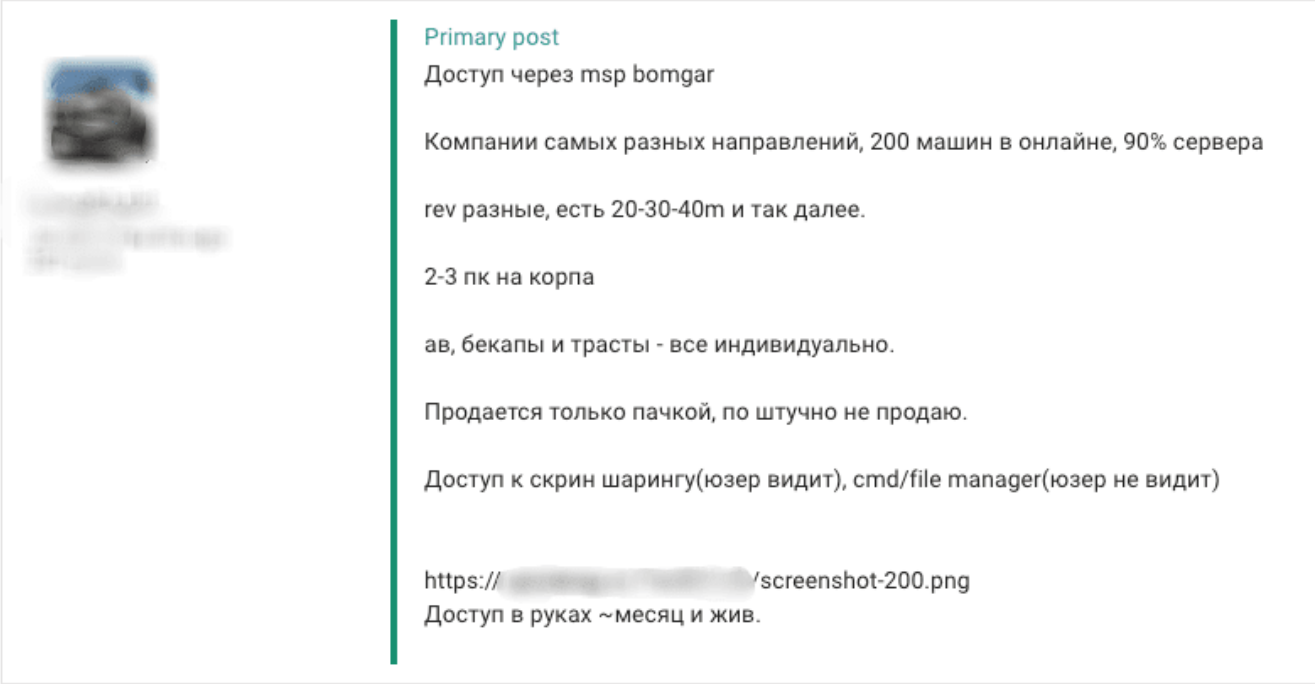

Figure 1: XSS user selling access to an MSP that manages at least 200 machines

Scattered Spider, in partnership with DragonForce, recently executed a sophisticated ransomware attack targeting MSPs by exploiting vulnerabilities in SimpleHelp RMM software. By compromising the MSP's infrastructure, attackers deployed ransomware encryptors across client networks, leveraging the "one-to-many" structure to maximize their reach. This approach not only enabled widespread encryption but also introduced double extortion tactics, where stolen data was used to pressure victims into paying ransoms.

Scattered Spider's tactics pose a serious threat to businesses, particularly those dependent on IT providers and MSPs. By exploiting trusted platforms like RMM software, the group infiltrates supply chains, compromises systems, and deploys ransomware at scale. It's clear from the volume of suspicious domain registrations that Scattered Spider's strategies have inspired copycat groups. While these mimicry efforts often cast a wider net targeting general platforms, Scattered Spider's approach is deliberate and highly targeted, focusing on high-value organizations and individuals.

The Human Factor: Playbook for Initial Access

When phishing doesn't do the trick, Scattered Spider doesn't give up—it gets creative. Using platforms like LinkedIn and ZoomInfo, the group digs into the lives of key employees within a target organization, piecing together everything from job titles to contact details. Once the perfect profile is built, it doesn't target systems, it targets people.

Urgent Request or Perfect Deception?

We've seen it play out during our investigations: A help-desk employee receives a panicked call from their "CFO," urgently requesting a password reset or the registration of a new MFA device. It's a scenario of high-stakes deception, and Scattered Spider excels at exploiting trust, weaponizing human vulnerability to devastating effect.

This tactic reflects a growing trend in cybercrime, where Russia-aligned groups collaborate with English-speaking actors to target Western organizations. Previously, such partnerships were rare due to cultural differences and concerns over operational security. But times are changing. Even the arrests of at least five alleged Scattered Spider members in 2024 have done little to slow these partnerships. Instead, Russian adversaries are doubling down, enlisting native English speakers who can seamlessly navigate Western norms and deliver highly convincing impersonation attacks.

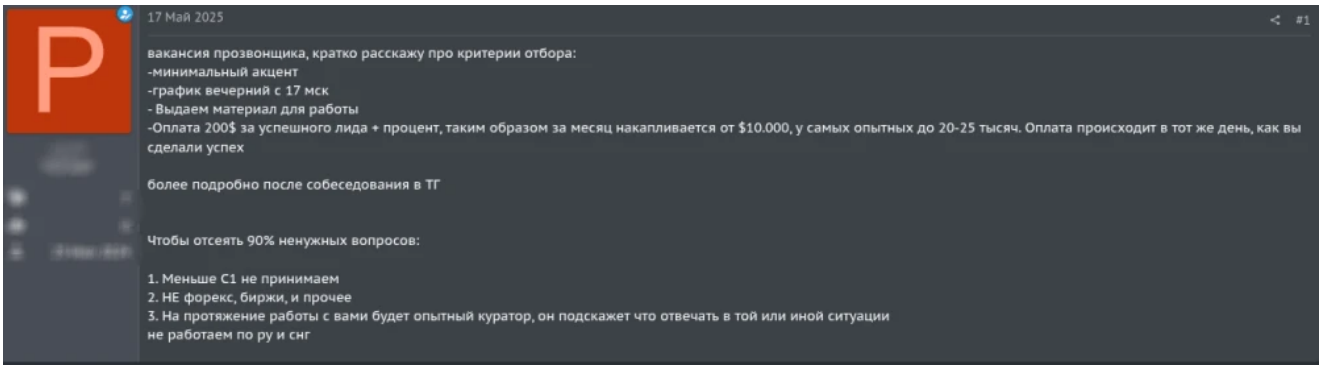

Figure 2: Forum user looking for English-speaking social engineers

To further refine their impersonation tactics, Russian actors actively recruit social engineers with highly specific qualifications. While monitoring cybercriminal forums, we observed discussions outlining the criteria these groups prioritize (see Figure 2):

- **Minimal Accent:** To sound convincing and avoid raising suspicion when interacting with help-desk staff. In some cases, we've even observed preferences for specific regional accents, such as a Southern accent, to make impersonations more credible and relatable to targets.
- **Fluency at a C1 Level or Higher:** Equivalent to a young adult native speaker, this level of fluency ensures callers can navigate complex conversations and adapt their approach in real-time without tipping off their victims.
- **Evening Shifts Starting at 5 p.m. Moscow Time:** To align with Western business hours, maximizing the chances of successfully reaching targets.
- **Payment per Lead Plus Commission:** Social engineers can reportedly earn **$10,000-$25,000** monthly by generating leads.

Callers are also provided with detailed scripts and real-time guidance from a so-called curator to help them handle any situation during the call. Notably, the job posting specifies that targets are strictly Western organizations, avoiding businesses in Russia and the Commonwealth of Independent States (CIS).

The collaboration between Russian-aligned groups and English-speaking social engineers significantly raises the stakes for businesses. This partnership combines technical expertise with cultural fluency, enabling attackers to convincingly impersonate employees and leadership, bypass security protocols, and exploit trust-based systems like help desks.

To combat this evolving threat, businesses must invest in robust social engineering defenses, including ongoing employee training and penetration tests against help desks, stricter identity verification protocols, and enhanced monitoring of help-desk interactions.

Step Up Your Defenses Against Scattered Spider

ReliaQuest's Approach

ReliaQuest offers its customers a suite of capabilities to help detect Scattered Spider-related threats early and respond rapidly.

GreyMatter DRP: By monitoring domain registrations, we alert organizations to impersonation attempts like typosquatting or phishing campaigns targeting their brand. These early warnings allow defenders to block potential attack vectors before they escalate into full-scale breaches.

AI Agent: TheReliaQuest GreyMatter platform integrates an agentic AI agent that enhances security operations by autonomously analyzing threat patterns, automating ransomware detection, and enriching investigations to accelerate response times. This capability significantly cuts the mean time to contain (MTTC) threats, empowering organizations to respond to attacks more effectively while strengthening their cybersecurity defenses.

Detection Rules: ReliaQuest's tailored detection rules, built on the latest threat intelligence and research, help organizations identify Scattered Spider activity within their environment.

By deploying these tailored detections alongside the following GreyMatter Automated Response Playbooks, organizations can significantly reduce their MTTC from hours to just minutes, minimizing the impact of Scattered Spider's ransomware and credential theft campaigns:

- **Terminate Active Sessions** and **Reset Passwords:** Ransomware affiliates like Scattered Spider abuse stolen credentials to move laterally and gain access to high-value data. This Playbook cuts off attackers' access by terminating hijacked sessions and resetting compromised credentials.

- **Delete File:** This Playbook can automatically remove malware payloads from a host's directory, halting the execution of malware before it can execute on critical systems, minimizing attack impact.
- **Disable User:** It's very common for ransomware affiliates like Scattered Spider to compromise user or service accounts. This Playbook allows for immediate disabling of a compromised user to stop attackers in their tracks.

Your Action Plan

- **Adopt Risk-Based Authentication**: Dynamically adjust access requirements based on user behavior, device, and location. Set policies to flag unusual activity, like logins from unknown locations, to prevent breaches before they escalate.
- **Conduct Social Engineering Assessments:** Regularly test help-desk policies and train employees to recognize and respond to social engineering attacks. These assessments ensure your organization is prepared to detect and neutralize attempts to manipulate human vulnerabilities.
- **Use Hardened Jumpboxes with Mandatory MFA:** Require MSPs, contractors, and privileged users to access high-value systems through secured jumpboxes. Mandate the use of MFA for all RDP connections to and from the jumpbox to slow down the use of stolen contractor credentials.
- **Restrict SharePoint Permissions:** Limit access to sensitive files, such as ESXi documentation and IT network diagrams, to reduce the risk of exploitation during lateral movement. Only employees with a legitimate need should have visibility into these resources.

Key Takeaways and What's Next

Scattered Spider continues to rely heavily on social engineering, using human trust as a weapon alongside phishing campaigns powered by typosquatted domains and advanced tools like Evilginx to bypass MFA. Its focus on MSPs and IT vendors allows it to breach multiple organizations through a single compromise, maximizing its reach and impact. Strategic alliances with ransomware operators like ALPHV and DragonForce further enhance the group's capabilities, solidifying Scattered Spider's reputation as a persistent and high-stakes adversary.

Looking ahead, we predict with high confidence that Scattered Spider will maintain its focus on high-value sectors like technology, finance, and retail trade across non-CIS countries. Although most media reporting has focused on the group's retail victims, it is highly likely that Scattered Spider has already compromised finance or retail trade oragnizations that have yet to publicly reveal an incident.

In addition, as the group refines its operations, we anticipate the adoption of deepfake AI voice technology to impersonate employees and leadership roles, reducing the need to recruit human social engineers. This shift would streamline the group's ability to manipulate trust-based systems like help desks, while continuing to target organizations with substantial capital or valuable data.

Organizations must be ready to counter increasingly deceptive tactics by implementing defenses that can adapt with these evolving threats. Staying ahead of attackers requires actionable intelligence, proactive monitoring, and resilient security measures—like those detailed in this report—to effectively combat adversaries such as Scattered Spider.

ShadowTalk: Powered by ReliaQuest

Stay in the know with our weekly podcast, where threat research experts break down the latest threats and top cybersecurity stories. Tune in on our website or your favorite podcast platform.

Listen to Recent Episodes