General

Scattered Spider attacks: mitigation strategies for cyber teams

Control Risks Cyber intelligence update (CYBINT-01) | 9 July 2025

Intelligence cut-off: 13:00 | 10 July 2025

Since April 2025, threat activity associated with the cybercriminal group Scattered Spider has increased significantly, following the highly impactful and disruptive attacks against UK retailers M&S and Co-op. These initial attacks have drawn significant media attention due to the level of disruption and the financial cost of the incidents, with the M&S incident costing the victim approximately GBP 650m.[1]

The US FBI warned on 28 June that the sophisticated cybercriminal group Scattered Spider had been observed expanding its targeting to the aviation sector. The warning followed airline entities WestJet on 13 June and Hawaiian Airlines on 23 June, disclosing separate cyber security incidents. Additional aviation and transport sector entities are also believed to have been targeted.

Four members of Scattered Spider (aged between 17 and 20), on 10 July, were arrested for computer misuse and money laundering offences connected to the M&S hack in April, since the latest US and Canadian aviation sector incidents. This isn't the first time Scattered Spider members have been arrested with previous arrests having limited impact, due to the loose-knit nature of the group. As such, we expect the group to continue to pose a disruptive threat to large brands, aviation, insurance and retail organisations in the US, UK and Canada in the long term.

Key takeaways

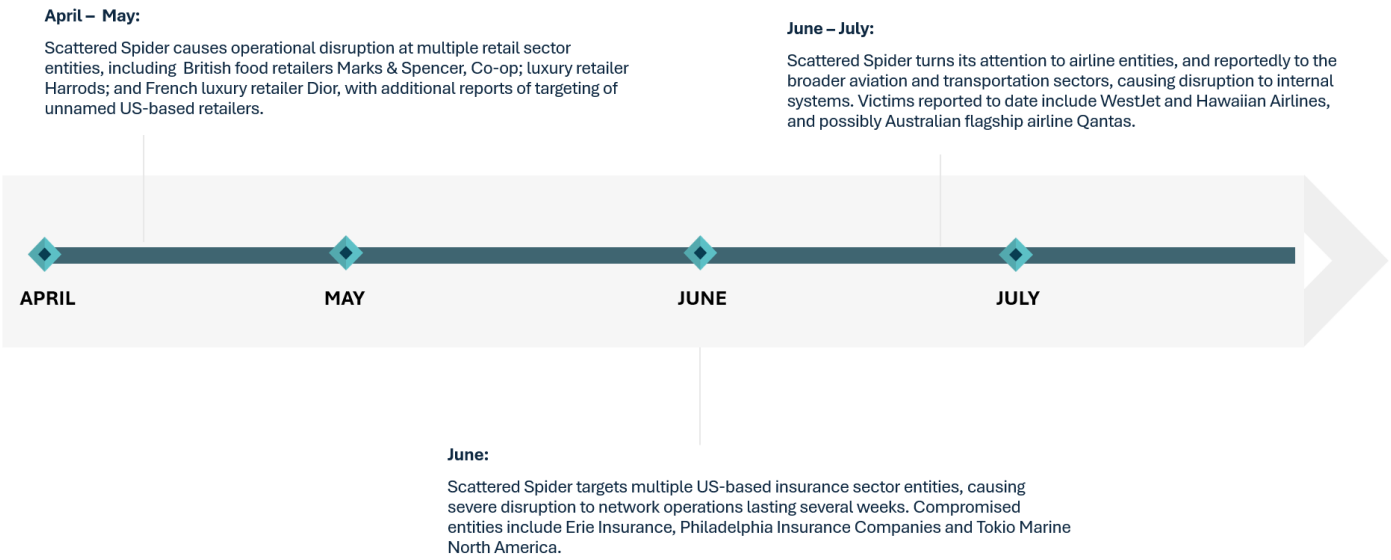
- **Scattered Spider has the intent, capability and resources to successfully target multiple sectors at pace:** The targeting of the aviation sector in July is a pivot from a focus on the insurance sector in June, which, in turn, was preceded by a focus on the retail sector in April and May. Scattered Spider has historically tended to focus on one sector at a time, as exemplified by the group's concurrent September 2023 operations against US casino entities Caesars and MGM Resorts, both of which caused significant operational disruption to the victims.
- **Scattered Spider has maintained its primary focus on targets based in the UK and US:** Scattered Spider has regularly targeted entities based in other countries, including France-based Dior, as part of the recent campaign against the retail sector. However, the vast majority of victims of Scattered Spider

[1] www.independent.co.uk/bulletin/news/marks-spencer-coop-hack-cyberattack-b2745564.html#:~:text=The%20hackers%20tricked%20IT%20help%20desk%20workers%20into,online%20services%2C%20including%20contactless%20payments%20and%20click-and-collect%20orders.

operations are UK- or US-based entities. With Scattered Spider operatives believed to originate from the UK and US, this could be a result of linguistic and cultural overlap, simplifying social engineering activity.

- **Scattered Spider remains a primary threat in the cybercriminal landscape:** The large number of high-profile breaches tied to Scattered Spider in recent months have served to showcase the group's continually high sophistication, as well as a sudden increase in intent on part of the group, following a period of operational quiet following the arrest of five Scattered Spider members in November 2024.

Recent activity tied to Scattered Spider



Scattered Spider profile

Overview

Scattered Spider (also tracked under names UNC3944, Octo Tempest and Muddled Libra) is a loose cybercriminal grouping, believed to primarily consist of young UK- and US-based operatives. The financially motivated group first emerged in 2022, conducting its first high-profile compromises in 2023.

Motive and impact

Typically focused on utilising ransomware payloads and data theft to extort victims, Scattered Spider has caused significant disruption to multiple victims, with multiple victims reporting **weeks-long disruption to critical business systems**, recovery costs ranging in the **hundreds of millions of dollars (USD)** and **loss of sensitive company and customer data.**

Victimology

- **Changing target sectors:** Scattered Spider has tended to target a single sector at a time, victimising multiple similar entities within a short space of time before pivoting to targeting another industry. Historically, the group has also let initial compromises of managed service providers, such as cloud

infrastructure company Snowflake, guide its targeting rationale, resulting in multiple compromises of customers in various sectors.

- **Maintained geographical focus:** Scattered Spider has consistently focused its efforts primarily on companies based in the UK and US. This set targeting rationale may be a result of the group's origin in these countries, with linguistic and cultural overlap enabling particularly convincing social engineering attacks. It could also plausibly be a result of UK- and US-based companies tending to have higher financial turnover, making them particularly lucrative targets.
- **Big-game hunting:** Scattered Spider has historically focused on compromising large, reputable companies with high revenue, likely to increase the possibility of obtaining large ransom payments.

Tempo

Since April, Scattered Spider has operated at a quick pace. Compared with other highly active cybercriminal groups, Scattered Spider has conducted a notably large number of high-profile compromises in a short space of time. This is particularly noteworthy when considering the group is leveraging sophisticated social engineering and third-party compromise methods as part of its modus operandi.

Key tactics, techniques and procedures (TTPs)

Preparatory reconnaissance and resource development

Scattered Spider's sophisticated social engineering attacks are enabled by persistent preparatory phases, wherein operatives build detailed domain knowledge of their target sector and acquire typosquatted domains customised to their targets.

Phishing for credentials

Scattered Spider regularly uses traditional phishing techniques, such as emails impersonating HR or IT staff, to lure employees to access credential stealing websites, masquerading as legitimate services.

The group is believed to favour executive accounts, likely due to their privileged access levels and the urgency with which requests believed to come from C-suite individuals are likely to be treated.

Social engineering for valid account access

Scattered Spider impersonates employees or contractors to lure IT helpdesk or call centre personnel to provide them with full access to corporate infrastructure. Actions encouraged by operatives typically include resetting of credentials and adding unauthorised MFA devices to bypass MFA.

Scattered Spider also regularly conducts MFA bypass activity, employing techniques like MFA fatigue and SIM swapping.

System persistence and discovery activity

Having accessed corporate networks, Scattered Spider utilises living-off-the-land techniques and legitimate RMM software to establish persistence and collect corporate data. To evade corporate cyber defences, the group has gone as far as impersonating incident response employees to discourage investigatory activity.

Actions on objectives

Scattered Spider extorts victims using a combination of data theft and ransomware deployment.

The group, which is known to employ a range of open-source tools, has been known to use varying ransomware payloads, including DragonForce and Qilin, making attribution of operations to the group trickier.

Typical toolset

- **Legitimate remote access tools:** The group typically uses legitimate tools, such as AnyDesk, TeamViewer and ScreenConnect, allowing its activity to remain undetected on victim networks.
- **Stealer malware:** The group uses easily accessible tools like Raccoon Stealer, Vidar Stealer and the WarZone RAT to steal data from victim organisations.

- **Ransomware payloads:** Scattered Spider has been tied to the use of DragonForce, ALPHV/BlackCat, Qilin and possibly Avaddon ransomware payloads for extortion purposes.

Outlook

- **Persistent use of sophisticated social engineering techniques for initial access**: As showcased by the group's return to significant threat activity in recent months, Scattered Spider remains a key threat actor within the cybercriminal landscape. The group's operatives have continuously shown themselves to be particularly capable social engineering actors, providing them with initial access that is proficiently utilised to conduct data theft and system encryption.
- **Operational success to drive intent**: Publicly reported Scattered Spider operations have caused significant operational disruption to victims, with recovery periods ranging from weeks to months, and with the estimated costs of incidents ranging up to GBP 300m. We assess that Scattered Spider's recent operational successes will highly likely motivate the group's operatives to maintain threat activity levels in the short to medium term.
- **Maintained focus on UK and US entities, continuously shifting target sector**: Although the group has consistently focused its operations primarily on UK- and US-based entities, changes to its sector-based targeting rationale remain difficult to predict. The group continues to show a preference for focusing on a single sector at a time, with quick pivoting to a different industry once objectives have been satisfied. Still, with a demonstrated and consistent preference for social engineering tactics, we assess it to be likely that sectors that are dependent on public-facing call centres, as is the case for the casino, airline and retail sectors, are more likely to be future targets.

Mitigation

- **Group awareness and mitigation review: We strongly recommend that** entities across sectors, particularly in the UK and US, familiarise themselves with Scattered Spider's known tactics, techniques and procedures (TTPs) and ingest indicators of compromise (IoCs) for endpoint detection of malicious activity. Organisations should consider reviewing existing mitigations and controls against the TTPs outlined in this document to build a layered defence against the group.
- **Attack simulation and exercising:** Large brands in the retail, aviation, transport, insurance and financial services sectors in the countries mentioned above should consider red teaming a Scattered Spider attack simulation scenario, using the confirmed TTPs in this document mapped to the organisation's critical assets. This could also be followed by a crisis management exercise leveraging on the outcomes of the Scattered Spider attack simulation.
- **Phishing and social engineering awareness:** Conducting general employee training on phishing techniques associated with Scattered Spider would also be valuable. Call centre and IT desk employees should be provided with specialised training on the threat of vishing scams and be advised to follow set procedures for credential resets and multi-factor authentication (MFA) access.
- **Third-party engagement:** Organisations should consider sharing this report with third-party organisations with customer-facing responsibilities to understand their proactive and preparatory activities to mitigate a Scattered Sider attack. Third parties should also be resilient in the event that they are successfully targeted, where understanding their resilience and redundancy approach would be valuable.

Scattered Spider tactics, techniques and procedures (TTPs)

Table 1: MITRE techniques

MITRE tactic	MITRE technique name	MITRE technique number
Reconnaissance	Gather Victim Identity Information	T1589
Reconnaissance	Phishing for Information	T1598
Resource Development	Acquire Infrastructure: Domains	T1583.001
Resource Development	Establish Accounts: Social Media Accounts	T1585.001
Resource Development	Obtain Capabilities: Tool	T1588.002
Initial Access	Phishing	T1566
Initial Access	Phishing: Spearphishing Voice	T1566.004
Initial Access	Valid Accounts	T1078
Initial Access	Valid Accounts: Domain Accounts	T1078.002
Initial Access	Trusted Relationship	T1199
Initial Access	Exploit Public-Facing Application	T1190
Initial Access (Mobile)	Phishing	T1660
Initial Access (Mobile)	SIM Card Swap	T1451
Execution	Command and Scripting Interpreter	T1059
Execution	Serverless Execution	T1648
Execution	User Execution	T1204
Execution	System Services: Service Execution	T1569.002
Execution	Windows Management Instrumentation	T1047
Persistence	Create Account	T1136
Persistence	Modify Authentication Process: Multi-Factor Authentication	T1556.006
Persistence	Valid Accounts	T1078
Privilege Escalation	Domain Policy Modification: Domain Trust Modification	T1484.002
Defense Evasion	Modify Registry	T1112
Defense Evasion	Modify Cloud Compute Infrastructure: Create Cloud Instance	T1578.002
Defense Evasion	Impersonation	T1656
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001
Defense Evasion	Subvert Trust Controls: Code Signing	T1553.002
Defense Evasion	Hide Artifacts	T1564
Defense Evasion	Direct Volume Access	T1006
Defense Evasion	Obfuscated Files or Information	T1027
Defense Evasion	Masquerading	T1036
Credential Access	OS Credential Dumping	T1003
Credential Access	Forge Web Credentials	T1606

Credential Access	Multi-Factor Authentication Request Generation	T1621
Credential Access	Unsecured Credentials: Credentials in Files	T1552.001
Credential Access	Unsecured Credentials: Private Keys	T1552.004
Credential Access	Steal Web Session Cookie	T1539
Discovery	Browser Information Discovery	T1217
Discovery	Cloud Service Dashboard	T1538
Discovery	File and Directory Discovery	T1083
Discovery	Remote System Discovery	T1018
Discovery	Steal Web Session Cookie	T1539
Discovery	Cloud Service Discovery	T1526
Discovery	System Network Configuration Discovery	T1016
Discovery	Account Discovery	T1087
Discovery	Permission Groups Discovery	T1069
Discovery	Network Service Discovery	T1046
Lateral Movement	Remote Services: Cloud Services	T1021.007
Collection	Data from Information Repositories: Code Repositories	T1213.003
Collection	Data from Information Repositories: SharePoint	T1213.002
Collection	Data Staged	T1074
Collection	Email Collection	T1114
Collection	Data from Cloud Storage	T1530
Command and Control	Application Layer Protocol	T1071
Command and Control	Remote Access Software	T1219
Command and Control	Protocol Tunneling	T1572
Command and Control	Web Service	T1102
Command and Control	Proxy	T1090
Command and Control	Ingress Tool Transfer	T1105
Command and Control	Data Encoding	T1132
Exfiltration	Exfiltration Over Web Service	T1567
Exfiltration	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
Impact	Data Encrypted for Impact	T1486
Impact	Financial Theft	T1657

Control Risks via multiple sources

Scattered Spider indicators of compromise (IoCs)

Table 2: IoCs associated with Scattered Spider

Remote Access IPs
45.132.227.213
119.93.5.239
146.70.103.228

144.76.136.153
67.43.235.122
82.180.146.31
91.242.237.100
89.46.114.164
98.100.141.70
62.182.98.170
MFA Registration IPs
136.144.19.51
146.70.127.42
173.239.204.129
198.44.136.180
Phishing and malicious domains
authenticate-bt.com
creditkarma-help.com
ibexglobai.com
login.five9-hr.com
login.uscc-hr.com
revolut-ticket.com
securian-hr.com
servicenow-help.com
MD5 File Hashes
1d05a83a639031913574c0bbb06026a4
586bd54b564926682b75330b190cbace
8445274c237eb83d56070e499f43641f
b233ff9dcf5520d69f9b75e1424f3271
c7497366fd0d8c9d72f96e7190632a51
cc230dcea35be180e3487b53e4b2cfba

Control Risks via multiple sources