Subgroup: Scattered Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:06:38 UTC

APT group: Subgroup: Scattered Spider

Names	Scattered Spider *(CrowdStrike)* UNC3944 *(Mandiant)* 0ktapus *(Group-IB)* Muddled Libra *(Palo Alto)* Scatter Swine *(Okta)* Storm-0875 *(Microsoft)* Octo Tempest *(Microsoft)* LUCR-3 *(Permiso)* Star Fraud *(self given)*
Country	[Unknown]
Motivation	Financial gain
First seen	2022
Description	An affiliate group of ALPHV, BlackCat Gang (Mandiant) UNC3944 is a financially motivated threat cluster that has persistently used phone-based social engineering and SMS phishing campaigns (smishing) to obtain credentials to gain and escalate access to victim organizations. At least some UNC3944 threat actors appear to operate in underground communities, such as Telegram and underground forums, which they may leverage to acquire tools, services, and/or other support to augment their operations. This activity overlaps with activity that has been reported in open sources as '0ktapus,' 'Scatter Swine,' and 'Scattered Spider.' Since 2022 and through early 2023, UNC3944 appeared to focus on accessing credentials or systems used to enable SIM swapping attacks, likely in support of secondary criminal operations occurring outside of victim environments. However, in mid-2023, UNC3944 began to shift to deploying ransomware in victim environments, signaling an expansion in the group's monetization strategies. These changes in their end goals signal that the industries targeted by UNC3944 will continue to expand; Mandiant has already directly observed their targeting broaden beyond telecommunication and business process outsourcer (BPO) companies to a

	wide range of industries including hospitality, retail, media and entertainment, and financial services. Around July 2025, ShinyHunters teamed up or merged with Scattered Spider. They share their Telegram channel also with Lapsus$, so they may all work together now – see the DataBreaches.net references in the Information section under ShinyHunters.	
Observed	Countries: Worldwide.	
Tools used	ADRecon, AnyDesk, DCSync, FiveTran, FleetDeck, gosecretsdump, Govmomi, Hekatomb, Impacket, LaZagne, LummaC2, Mimikatz, Ngrok, PingCastle, ProcDump, PsExec, Pulseway, Pure Storage FlashArray, RedLine, Rsocx, RustDesk, ScreenConnect, SharpHound, Socat, Spidey Bot, Splashtop, Stealc, TacticalRMM, Tailscale, TightVNC, VIDAR, WinRAR, WsTunnel, Living off the Land.	
Operations performed	Aug 2023	“Can you reset my password?” How a simple service desk attack cost Clorox $400 million <https://specopssoft.com/blog/clorox-password-social-engineering/>
	Sep 2023	MGM Resorts shuts down IT systems after cyberattack <https://www.bleepingcomputer.com/news/security/mgm-resorts-shuts-down-it-systems-after-cyberattack/> <https://www.databreaches.net/alphv-responds-to-mgm-incident-and-sloppy-reporting/>
	Sep 2023	Caesars Entertainment confirms ransom payment, customer data theft <https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/> <https://www.darkreading.com/attacks-breaches/-scattered-spider-mgm-cyberattack-casinos>
	Sep 2023	Hackers who breached casino giants MGM, Caesars also hit 3 other firms, Okta says <https://www.reuters.com/technology/hackers-who-breached-casino-giants-mgm-caesars-also-hit-3-other-firms-okta-says-2023-09-19/>
	Sep 2023	‘Scattered Spider’ group launches ransomware attacks while expanding targets in hospitality, retail <https://therecord.media/scattered-spider-ransomware-attacks-hospitality-retail>
	Sep 2023	Luxury Hotels Remain Major Target of Ongoing Social Engineering Attack

	<https://cofense.com/blog/luxury-hotels-remain-target-of-social-engineering-attack/>
Jan 2024	Muddled Libra's Evolution to the Cloud <https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/>
Oct 2024	Scattered Spider x RansomHub: A New Partnership <https://www.reliaquest.com/blog/scattered-spider-x-ransomhub-a-new-partnership/>
2025	Scattered Spider: Still Hunting for Victims in 2025 <https://www.silentpush.com/blog/scattered-spider-2025/>
Apr 2025	Marks & Spencer breach linked to Scattered Spider ransomware attack <https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/> <https://cybermonitoringcentre.com/2025/06/20/cyber-monitoring-centre-statement-on-ransomware-incidents-in-the-retail-sector-june-2025/>
Apr 2025	Harrods the next UK retailer targeted in a cyberattack <https://www.bleepingcomputer.com/news/security/harrods-the-next-uk-retailer-targeted-in-a-cyberattack/>
Apr 2025	Co-op confirms data theft after DragonForce ransomware claims attack <https://www.bleepingcomputer.com/news/security/co-op-confirms-data-theft-after-dragonforce-ransomware-claims-attack/>
May 2025	Hackers behind UK retail attacks now targeting US companies <https://www.bleepingcomputer.com/news/security/google-scattered-spider-switches-targets-to-us-retail-chains/>
May 2025	Large Retailers Land in Scattered Spider's Ransomware Web <https://www.darkreading.com/threat-intelligence/large-retailers-scattered-spider-ransomware-web>
Jun 2025	Hackers switch to targeting U.S. insurance companies <https://www.bleepingcomputer.com/news/security/google-warns-scattered-spider-hackers-now-target-us-insurance-companies/>
Jun 2025	Aflac discloses breach amidst Scattered Spider insurance attacks <https://www.bleepingcomputer.com/news/security/aflac-discloses-breach-amidst-scattered-spider-insurance-attacks/>

	Jun 2025	Scattered Spider hackers shift focus to aviation, transportation firms <https://www.bleepingcomputer.com/news/security/scattered-spider-hackers-shift-focus-to-aviation-transportation-firms/>
	Jun 2025	WestJet investigates cyberattack disrupting internal systems <https://www.bleepingcomputer.com/news/security/westjet-investigates-cyberattack-disrupting-internal-systems/>
	Jun 2025	Hawaiian Airlines discloses cyberattack, flights not affected <https://www.bleepingcomputer.com/news/security/hawaiian-airlines-discloses-cyberattack-flights-not-affected/>
	Jul 2025	Qantas discloses cyberattack amid Scattered Spider aviation breaches <https://www.bleepingcomputer.com/news/security/qantas-discloses-cyberattack-amid-scattered-spider-aviation-breaches/>
	Aug 2025	Scattered Spider has a new Telegram channel to list its attacks <https://databreaches.net/2025/08/09/scattered-spider-has-a-new-telegram-channel-to-list-its-attacks/>
Counter operations	Jun 2024	Alleged Boss of ‘Scattered Spider’ Hacking Group Arrested <https://krebsonsecurity.com/2024/06/alleged-boss-of-scattered-spider-hacking-group-arrested/>
	Jul 2024	Walsall teenager arrested in joint West Midlands Police and FBI operation <https://www.westmidlands.police.uk/news/west-midlands/news/news/2024/july/walsall-teenager-arrested-in-joint-west-midlands-police-and-fbi-operation/>
	Nov 2024	US charges five linked to Scattered Spider cybercrime gang <https://www.bleepingcomputer.com/news/security/us-charges-five-linked-to-scattered-spider-cybercrime-gang/>
	Dec 2024	US arrests Scattered Spider suspect linked to telecom hacks <https://www.bleepingcomputer.com/news/security/us-arrests-scattered-spider-suspect-linked-to-telecom-hacks/>
	Jul 2025	Retail cyber attacks: NCA arrest four for attacks on M&S, Co-op and Harrods <https://www.nationalcrimeagency.gov.uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods>
Information	<https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware> <https://unit42.paloaltonetworks.com/muddled-libra/>	

	<https://thehackernews.com/2023/10/lucr-3-scattered-spider-getting-saas-y.html> <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a> <https://www.reliaquest.com/wp-content/uploads/2023/11/231121_EXTERNAL_ScatteredSpiderThreatReport.pdf> <https://therecord.media/scattered-spider-challenge-for-FBI> <https://www.guidepointsecurity.com/blog/worldwide-web-an-analysis-of-tactics-and-techniques-attributed-to-scattered-spider/> <https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications/> <https://www.bleepingcomputer.com/news/security/microsoft-links-scattered-spider-hackers-to-qilin-ransomware-attacks/> <https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations> <https://www.theregister.com/2025/05/18/ex_nsa_scattered_spider_call/> <https://www.theregister.com/2025/05/21/scattered_spider_snared_financial_orgs/> <https://www.darkreading.com/cyberattacks-data-breaches/blurring-lines-scattered-spider-russian-cybercrime> <https://www.bleepingcomputer.com/news/security/scattered-spider-three-things-the-news-doesnt-tell-you/> <https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations> <https://reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025/> <https://reliaquest.com/blog/scattered-spiders-calculated-path-from-cfo-to-compromise/> <https://blog.checkpoint.com/research/exposing-scattered-spider-new-indicators-highlight-growing-threat-to-enterprises-and-aviation/> <https://www.halcyon.ai/blog/scattered-spider-and-other-criminal-compromise-of-outsourcing-providers-increases-victim-attacks> <https://www.microsoft.com/en-us/security/blog/2025/07/16/protecting-customers-from-octo-tempest-attacks-across-multiple-industries/> <https://cloud.google.com/blog/topics/threat-intelligence/defending-vsphere-from-unc3944/> <https://www.ic3.gov/CSA/2025/250729.pdf> <https://unit42.paloaltonetworks.com/why-the-focus-on-muddled-libra/> <https://unit42.paloaltonetworks.com/muddled-libras-strike-teams/>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=muddled-libra>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
