Scattered Spider

Scattered Spider, also referred to as **UNC3944** and, more recently identified as ShinyHunters,[1] is a hacking group mostly made up of teens and young adults believed to live in the United States and the United Kingdom.[2][3] The group is believed to be affiliated with cybercriminal network, "The Com", or more specifically the Hacker Com, a subset of The Com.[4][5]

The group gained notoriety for their involvement in the hacking and extortion of Caesars Entertainment and MGM Resorts International, two of the largest casino and gambling companies in the United States. Scattered Spider has also targeted Visa, Marks & Spencer, PNC Financial Services, Transamerica, New York Life Insurance, Synchrony Financial, Truist Bank, Twilio,[6] and JLR.[7]

Members of Scattered Spider have been connected with the hacks against Snowflake cloud storage customers in the US.[8][9][10] More recently, members of Scattered Spider have been connected with the hacks against Qantas, the flag carrier of Australia.[11][12][13]

Scattered Spider, ShinyHunters

Nickname	See § Names
Formation	c. May 2022
Type	Hacker group
Purpose	Ransomware, cyberattacks, data theft extortion
Region	United States and United Kingdom
Methods	Social engineering, ransomware as a service, password cracking
Affiliations	ALPHV, ShinyHunters

The Scattered Spider group is now believed to be part of, or identical to, the ShinyHunters cybercriminal group.[14][15]

Names

The group's most common name as used in press releases and by journalists is Scattered Spider, though many other names have been attributed to the group. **Star Fraud**, **Octo Tempest**, **Scatter Swine**, and **Muddled Libra** have all been names used to refer to the group previously.[1][16]

Scattered Spider is a component of a larger global hacking community, known as "the Community" or "The Com", itself having members who have hacked major American technology companies.[16]

History

Scattered Spider is believed to have been founded in May 2022, when the group was focused on attacks on telecommunications firms. The group utilized SIM swap scams, multi-factor authentication fatigue attacks, and phishing by SMS and Telegram.[1] The group typically exploited the security bug CVE-2015-2291 (https://nvd.nist.gov/vuln/detail/cve-2015-2291), a cybersecurity issue in Windows' anti-DoS software,[17] to terminate security software, allowing the group to evade detection. The group is believed to have a deep understanding of Microsoft Azure, the ability to conduct reconnaissance in cloud computing platforms powered by Google Workspace and AWS, and utilizes legitimately-developed remote-access tools.[1]

The group later became known for targeting critical infrastructure prior to moving on to its 2023 casino hacks.[18] In 2025, DataBreaches.net[19] reported that Scattered Spider have merged with ShinyHunters or vice versa.[20][21]

Casino hacks (2023)

Scattered Spider gained access to both Caesars' and MGM's internal systems through the use of social engineering. The group was able to bypass multi-factor authentication technologies by attaining login credentials and one-time passwords.[22][23] The group claims that it targeted MGM due to them catching the group attempting to rig slot machines in their favor.[24]

Caesars

Caesars Entertainment paid a ransom of $15 million to Scattered Spider, half their original demand of $30 million. Scattered Spider, using similar tactics to its attack on MGM, was able to access driver's license numbers and possibly Social Security numbers, for a "significant number" of Caesars' customers. Statements made by Caesars noted that while the company cannot guarantee the deletion of the information attained by Scattered Spider, the casino operator will take all necessary actions to attain such result.[2]

Sources dispute on whether Scattered Spider was the group which targeted Caesars, with some believing it was the British-American group while others say the perpetrators were not the group or unknown.[25][26][24]

MGM Resorts

Scattered Spider collaborated with ALPHV, a software development team which provides ransomware as a service. Scattered Spider called MGM's help desk posing as an employee it found on LinkedIn to gain internal access. The group gained access on September 11, 2023.[22]

MGM Resorts first disclosed the cyberattack on September 12, 2023, in a Form 8-K report with the SEC the next day.[27][28] The company stated that though it has "dealt" with the cyberattack, many of the computer systems at its resorts remain offline, which include but are not limited to credits for food, beverages, and free credits. The attack further disabled on-site ATMs as well as remote room keys, and prevented MGM from charging patrons for parking.[23]

In July 2024, a 17-year old hacker from the United Kingdom was arrested in connection with the hack and attempted ransom. He has been released on bail pending trial.[29] The arrest was coordinated by local and international law enforcement.

Aftermath

MGM and the US FTC and FBI are at present investigating the cyberattack, and the casino operator temporarily took down its website.[3] Moody's Corporation has stated that due to MGM's heavy reliance on computers for much of its operations, its credit rating could go down as a result of the cyberattack.[18] Upon the announcement of both companies' attacks, the stock prices for both Caesars and MGM dropped. MGM's CEO William Hornbuckle went on to note at an industry conference that the hack caused the company to be "completely in the dark" about its properties.[16]

Both MGM and Caesars were sued in class action lawsuits by customers following the hacks, with all stating that the failure for both of the casino operators to adequately secure their data constituted breach of contract. The law firms' clients also all demanded jury trials.[30][31] In January 2025, MGM agreed to pay a $45 million settlement to the victims of the breach.[32][33]

Snowflake hacks

Two members of the group have been connected with hacks against customers of Snowflake's cloud computing. The hackers accessed and stole customer data, demanding millions of dollars. Nearly a hundred victims were targeted, including AT&T, Ticketmaster, Advance Auto Parts, LendingTree and Neiman Marcus.[8][34]

Arrests

In January 2024, Noah Michael Urban, a member of the group[35] and known as "Sosa", "King Bob", "Elijah", and other aliases, was arrested in Florida for the cumulative theft of about $800,000 in cryptocurrency.[36] Sosa used SIM-swapping techniques in order to compromise victims' email and financial account details.

In June 2024, the alleged leader of the group, Tyler Buchanan (aka TylerB), was arrested in Spain when attempting to board a flight to Italy.[37][38] At the time of his arrest, Spanish police allege that Buchanan possessed Bitcoins worth $27 million.

In July 2024, the West Midlands Police with the help of the FBI arrested a 17-year old juvenile in connection with the MGM cyberattacks. The suspect, who lives in Walsall and whose name was not published, was released on bail while law enforcement examined his devices.[39]

19-year-old Remington Ogletree was arrested in November 2024 on charges related to his alleged involvement with the group.[40]

On September 17, 2025, a juvenile suspect local to the casino-hacking case surrendered to Clark County Juvenile Detention Center.[41]

See also

- LockBit

References

1. "Scattered Spider: The Modus Operandi" (https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html). *www.trellix.com*. Retrieved September 14, 2023.
2. "Caesars Entertainment says it was also a victim of a cyberattack" (https://www.nbcnews.com/tech/security/caesars-entertainment-says-was-also-victim-cyberattack-rcna105050). *NBC News*. September 14, 2023. Retrieved September 14, 2023.
3. Bracken, Becky (September 14, 2023). " 'Scattered Spider' Behind MGM Cyberattack, Targets Casinos" (https://www.darkreading.com/attacks-breaches/-scattered-spider-mgm-cyberattack-casinos). *Dark Reading*. Retrieved September 14, 2023.
4. "Internet Crime Complaint Center (IC3) | Hacker Com: Cyber Criminal Subset of The Community (Com) is a Rising Threat to Youth Online" (https://www.ic3.gov/PSA/2025/PSA250723). *www.ic3.gov*. Retrieved September 23, 2025.
5. Jones, David (July 30, 2025). "What we know about the cybercrime group Scattered Spider" (https://www.cybersecuritydive.com/news/what-we-know-about-the-cybercrime-group-scattered-spider/756312/). *Cybersecurity Dive*.
6. "ShinyHunters Leak What They Claim Are 33M Twilio Authy Phone Numbers, Neiman Marcus and Truist Bank Data" (https://databreaches.net/2024/07/05/shinyhunters-leak-what-they-claim-are-33m-twilio-authy-phone-numbers-neiman-marcus-and-truist-bank-data/). *DataBreaches.Net*. July 5, 2024. Retrieved September 8, 2025.
7. Almeida, Lauren (September 16, 2025). "Jaguar Land Rover extends production shutdown after cyber-attack" (https://www.theguardian.com/business/2025/sep/16/jaguar-land-rover-production-shutdown-cyber-attack). *The Guardian*. ISSN 0261-3077 (https://search.worldcat.org/issn/0261-3077). Retrieved September 19, 2025.

8. "Snowflake Hacker Still Active, Finding New Victims, Expert Says" (https://www.bloomberg.com/news/articles/2024-09-20/snowflake-hacker-still-active-finding-new-victims-expert-says). *Bloomberg.com*. September 20, 2024. Retrieved January 15, 2025.
9. Mapp, Karis (November 28, 2024). "Kitchener, Ont., man arrested in massive Snowflake hacking scheme faces possible extradition to U.S." (https://www.cbc.ca/news/canada/kitchener-waterloo/snowflake-data-breach-kitchener-accused-possible-extradition-1.7394891) *CBC News*. CBC. Retrieved May 24, 2025.
10. Tidy, Joe (May 21, 2025). "Retail hackers believed to be young and from US and UK, detectives say" (https://www.bbc.com/news/articles/ckgnndrgxv3o). *BBC News*. BBC World Service. Retrieved May 24, 2025.
11. "What we know about Scattered Spider, the hacker group targeting airlines" (https://www.abc.net.au/news/2025-07-02/who-are-scattered-spider-hackers-qantas-data-breach/10548567 4). *ABC News*. July 2, 2025. Retrieved July 12, 2025.
12. Abrams, Lawrence. "Qantas discloses cyberattack amid Scattered Spider aviation breaches" (https://www.bleepingcomputer.com/news/security/qantas-discloses-cyberattack-amid-scattered-spider-aviation-breaches/). *BleepingComputer*. Retrieved September 8, 2025.
13. Abrams, Lawrence. "ShinyHunters behind Salesforce data theft attacks at Qantas, Allianz Life, and LVMH" (https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/). *BleepingComputer*. Retrieved September 8, 2025.
14. "Are Scattered Spider and ShinyHunters one group or two? And who did France arrest? (1)" (https://databreaches.net/2025/08/03/are-scattered-spider-and-shinyhunters-one-group-or-two-and-who-did-france-arrest/). *DataBreaches.Net*. August 3, 2025. Retrieved September 8, 2025.
15. Abrams, Lawrence. "ShinyHunters behind Salesforce data theft attacks at Qantas, Allianz Life, and LVMH" (https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/). *BleepingComputer*. Retrieved September 8, 2025.
16. Whitaker, Bill; Chasan, Aliza; Messick, Graham; Weingart, Jack (April 14, 2024). "Criminal exploits of Scattered Spider earn respect of Russian ransomware hackers - CBS News" (https://www.cbsnews.com/news/scattered-spider-blackcat-hackers-ransomware-team-up-60-minutes/). *www.cbsnews.com*. Retrieved April 23, 2024.
17. "CVE-2015-2291 : (1) IQVW32.sys before 1.3.1.0 and (2) IQVW64.sys before 1.3.1.0 in the Intel Ethernet diagnostics driver for Windows all" (https://www.cvedetails.com/cve/CVE-2015-2291/). *www.cvedetails.com*. Retrieved September 14, 2023.
18. "MGM Resorts breached by 'Scattered Spider' hackers: Sources" (https://www.businessinsurance.com/article/20230914/NEWS06/912359825/MGM-Resorts-breached-by-%E2%80%98Scattered-Spider%E2%80%99-hackers-Sources). *Business Insurance*. Retrieved September 14, 2023.
19. "Are Scattered Spider and ShinyHunters one group or two? And who did France arrest? (1)" (https://databreaches.net/2025/08/03/are-scattered-spider-and-shinyhunters-one-group-or-two-and-who-did-france-arrest/). *DataBreaches.Net*. August 3, 2025. Retrieved September 8, 2025.
20. Kovacs, Eduard (August 6, 2025). "Google Discloses Data Breach via Salesforce Hack" (https://www.securityweek.com/google-discloses-salesforce-hack/). *SecurityWeek*. Retrieved August 30, 2025.
21. "Are Scattered Spider and ShinyHunters one group or two? And who did France arrest? (1)" (https://databreaches.net/2025/08/03/are-scattered-spider-and-shinyhunters-one-group-or-two-and-who-did-france-arrest/). *DataBreaches.Net*. August 3, 2025. Retrieved September 8, 2025.
22. Siddiqui, Zeba; Bing, Christopher; Bing, Christopher (September 13, 2023). "MGM Resorts breached by 'Scattered Spider' hackers: sources" (https://www.reuters.com/technology/moodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13/). *Reuters*. Retrieved September 14, 2023.
23. "Young hackers are sticking up Las Vegas casinos for hefty ransoms" (https://qz.com/young-hackers-are-sticking-up-las-vegas-casinos-for-hef-1850837238). *Quartz*. September 14, 2023. Retrieved September 14, 2023.

24. Srivastava, Mehul (September 14, 2023). "MGM hack followed failed bid to rig slot machines, 'Scattered Spider' group claims" (https://www.ft.com/content/a25d2897-b0ce-4ba7-92ed-ff5df09d1b47). *Financial Times*. Retrieved September 15, 2023.
25. Murphy, Aislinn (September 13, 2023). "Caesars Entertainment reportedly paid ransomware demand" (https://www.foxbusiness.com/markets/caesars-entertainment-reportedly-paid-ransomware-demand). *FOXBusiness*. Retrieved September 15, 2023.
26. Gendron, Will. "MGM Resorts is still suffering from a massive outage after a notorious group of young hackers apparently tricked workers into handing over access to the company's network" (https://www.businessinsider.com/mgm-caesars-las-vegas-casinos-targeted-scattered-spider-hacking-group-2023-9). *Business Insider*. Retrieved September 15, 2023.
27. "Investors - Financial Info - SEC Filings - SEC Filings Details" (https://investors.mgmresorts.com/investors/financial-info/sec-filings/sec-filings-details/default.aspx?FilingId=16927190). *investors.mgmresorts.com*.
28. "FORM 8-K - MGM Resorts International" (https://web.archive.org/web/20230915000105/https://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/a390c443-0c40-4025-aba2-74505ab3c9e3.pdf) (PDF). Archived from the original (https://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/a390c443-0c40-4025-aba2-74505ab3c9e3.pdf) (PDF) on September 15, 2023.
29. Encinas, Amaris. "U.K. police arrest 17-year-old in connection with last year's MGM cyberattack" (https://www.usatoday.com/story/tech/news/2024/07/19/uk-police-arrest-teen-for-mgm-cyberattack/74477012007/). *USA TODAY*. Retrieved July 22, 2024.
30. "Complaints filed say MGM Resorts, Caesars Entertainment failed to protect information from cyberattack" (https://www.ktnv.com/news/complaints-filed-say-mgm-resorts-caesars-entertainment-failed-to-protect-information-from-cyberattack). *Channel 13 Las Vegas News KTNV*. September 26, 2023. Retrieved September 26, 2023.
31. Croft, Daniel (September 26, 2023). "5 class actions launched against MGM, Caesars" (https://www.cybersecurityconnect.com.au/commercial/9607-5-class-actions-launched-against-mgm-caesars). *www.cybersecurityconnect.com.au*. Retrieved September 26, 2023.
32. Weatherbed, Jess (January 29, 2025). "MGM will pay $45 million to settle data breach lawsuit" (https://www.theverge.com/news/601733/mgm-resorts-45-million-settlement-data-breaches). *The Verge*. Retrieved March 14, 2025.
33. "Owens v. MGM Resorts International" (https://storage.courtlistener.com/recap/gov.uscourts.nvd.164564/gov.uscourts.nvd.164564.63.0.pdf) (PDF). *CourtListener*. Retrieved March 14, 2025.
34. Burgess, Matt. "The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever" (https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/). *Wired*. ISSN 1059-1028 (https://search.worldcat.org/issn/1059-1028). Retrieved January 15, 2025.
35. "Fla. Man Charged in SIM-Swapping Spree is Key Suspect in Hacker Groups Oktapus, Scattered Spider – Krebs on Security" (https://krebsonsecurity.com/2024/01/fla-man-charged-in-sim-swapping-spree-is-key-suspect-in-hacker-groups-oktapus-scattered-spider/). January 30, 2024. Retrieved July 22, 2024.
36. Fernandez, Frank. "Palm Coast teen accused in cryptocurrency scheme seeks jail release as he awaits trial" (https://www.news-journalonline.com/story/news/courts/2024/04/03/palm-coast-teen-in-cryptocurrency-scam-seeks-release-from-jail/73148333007/). *Daytona Beach News-Journal Online*. Retrieved July 22, 2024.
37. "Alleged Boss of 'Scattered Spider' Hacking Group Arrested – Krebs on Security" (https://krebsonsecurity.com/2024/06/alleged-boss-of-scattered-spider-hacking-group-arrested/). June 16, 2024. Retrieved July 22, 2024.
38. "U.K. Hacker Linked to Notorious Scattered Spider Group Arrested in Spain" (https://thehackernews.com/2024/06/uk-hacker-linked-to-notorious-scattered.html). *The Hacker News*. Retrieved July 22, 2024.
39. Roth, Emma (July 19, 2024). "UK teen arrested in connection to MGM hack" (https://www.theverge.com/2024/7/19/24202142/uk-teen-mgm-hack-arrested-fbi). *The Verge*. Retrieved July 22, 2024.

40. "California Teen Suspected of Being a Member of Scattered Spider Hacking Gang" (https://www.bloomberg.com/news/articles/2024-12-03/scattered-spider-hacking-gang-arrests-mount-with-california-teen). *Bloomberg.com*. December 3, 2024. Retrieved December 4, 2024.
41. "Teenage hacker arrested for cyberattacks against Las Vegas casinos" (https://www.usatoday.com/story/news/crime/2025/09/22/teen-arrested-vegas-2023-casino-cyberattack/86299664007/). *USA TODAY*. Retrieved September 24, 2025.

External links

- Scattered Spider Cybersecurity Advisory (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a); Cybersecurity and Infrastructure Security Agency website.