WELLS FARGO

Scattered Spider

A global menace

Summary

- Global losses exceed $1.3 billion
- Over $115 million in ransom payments
- Over 100 organizations breached 47
- U.S. victims extorted
- Weaponization of Artificial Intelligence

Source: Cybernews [1]

Threat actor background

Scattered Spider, also known as UNC3944, Muddled Libra, Starfraud, Scatter Swine, and Oktapus, have engaged in data extortion and other criminal activities since May 2022. They are considered experts in social engineering tactics including phishing, Multi Factor Authentication (MFA) push bombing, and Subscriber Identity Module (SIM) swap attacks which are used to obtain initial access into victim networks.

The group is composed primarily of native-English-speaking young adults (16 – 25 yrs old) from the U.S. and U.K. Known for their decentralized structure, they operate a loosely connected network of cyber actors.[2]

Scattered Spider employs various social engineering tactics to gain initial access to target networks. They initially targeted telecommunications and Business Process Outsourcing (BPO) organizations across several countries including the U.S, U.K., Germany, France, Italy, Canada, Australia, and Japan.

Since the start of their campaigns, Scattered Spider has breached more than 100 organizations spanning various industries including retail, hospitality, gaming, manufacturing, transportation, food and agriculture, and finance. These cybercriminals have demonstrated their ability to launch sophisticated attacks against many different sectors due to their ability to exploit the human element and their technical expertise, posing a significant threat to U.S. businesses and organizations.

Notable attacks

Cyber attack at a casino

In September 2023, Scattered Spider launched a ransomware attack against a major casino, causing over $100 million in damages. This attack crippled the casino's network for 10 days and impacted business operations including slot machines, digital hotel room keys, websites, and payment systems. Reportedly, the casino refused to pay the ransom.

According to a Government Technology report, a cybercriminal actor allegedly found an employee on LinkedIn and impersonated the employee by calling the IT department to ask for a password reset. Once the reset was granted, the hacker reportedly had access to the casino's internal systems "in 10 minutes."[3]

The financial cost of cyber incidents like this mostly pertains to the loss of business revenue from the disruption, costs of incident response and recovery, legal and regulatory expenses, and potential class action litigation costs. The financial impact on the victim is detrimental and can jeopardize the very survival of an organization.

Social engineering attacks also exploit human trust and our desire to help others. It only took 10 minutes for Scattered Spider actors to negotiate authentication procedures and convince an IT help desk technician to reset an employee's password to gain access to the casino's network. This carefully planned social engineering tactic was successful because the threat actors conducted research on the casino's employee who made their employment information available on social media.

Cybercriminals can easily gather information about their intended targets, as many people use social media and post information about their families, employment, hobbies, interests, and location.

Organizations should review security policies, establish incident response plans, and develop business continuity plans to respond to cyber incidents.

Cyber incident at a second casino

In September 2023, Scattered Spider launched a ransomware attack against a second major casino. The initial attack began when attackers impersonated legitimate employees to trick an outsourced IT vendor to grant access to the casino's systems. The threat actors exfiltrated sensitive customer data and demanded a ransom. The casino reportedly paid
$15 million (half of the initial $30 million ransom demand) to prevent the public release of stolen data.

Multiple cybersecurity vendors and law enforcement sources attributed the attack to Scattered Spider. The incident occurred concurrently with the first casino's attack and highlights the group's coordinated targeting of the gaming and hospitality sector.[4]

Organizations should establish incident response plans and participate in wargaming exercises to rehearse actions during a simulated cyber incident.

Cryptocurrency exchange incident

In December 2024, cybercriminals affiliated with Scattered Spider and other cybercriminal groups known as ShinyHunters and TheCom were linked to a major cyber breach of a cryptocurrency exchange platform. The breach affected the information of nearly 70,000 customers and was the result of malicious insiders who, while acting as third-party workers in India, provided customer credentials to the attackers. The insiders were allegedly bribed by cybercriminals to leak sensitive customer data containing personally identifiable information (PII), identification documents, and financial information. The threat actors then used the stolen data for social engineering scams and extortion.[8]

Fortunately for the exchange, cryptocurrency accounts, passwords, and private keys remained secure. Despite the limited impact on its main cryptocurrency operations, exchange's remediation costs were estimated to range from $180M to $400M. Cybercriminals have historically offered bribery payments and bounties to employees in exchange for assistance in gaining access to customer accounts and an initial foothold into networks.

Organizations should monitor for insider threat activity, develop robust identity verification, and zero-trust architectures to limit this risk.

Cyber incident at a retailer

In April 2025, Scattered Spider conducted a ransomware attack against a U.K.-based multinational retailer causing significant business disruption and financial losses estimated at over $1B in profit and stock market value.[5] This incident impacted normal business operations, leaving customers unable to complete online orders and creating inventory challenges that left stores with bare shelves. The threat actors also stole customer data containing sensitive PII and business records.

Scattered Spider actors obtained unauthorized access to the retailer's networks by using compromised credentials from user accounts at a third-party IT services provider.

Third party employees' credentials were obtained through phishing and social engineering tactics targeted to the retailer's IT help desks. The UK's National Cyber Security Centre (NSCS) acknowledged that social engineering techniques aimed at IT help desks were used for initial access at the retailer.[6] The CEO confirmed that the incident was the result of "human error." This human error ultimately led to the downgrade of the retailer's annual operating profit by 30%, equivalent to over $400M, for the year.[7] This incident highlights third-party cyber risks and the risks of interconnectivity when doing business in today's world.

Organizations should provide cyber awareness training to employees regularly in order to reduce the risks of human errors. They should also review third-party access controls.

Common tactics

Scattered Spider is known for advanced social engineering attacks including impersonating IT staff and help desk manipulation. According to an advisory published by the FBI and CISA in July 2025[9], Scattered Spider threat actors have:

- Posed as company IT and/or help desk staff, using phone calls or SMS messages to obtain credentials from employees and gain access to the network.
- Posed as company IT and/or help desk staff to direct employees to run commercial remote access tools, enabling initial access.
- Posed as IT staff to convince employees to share their one-time password (OTP) and multi-factor authentication (MFA) authentication code.
- Sent repeated MFA notification prompts leading to employees pressing the "Accept" button (also known as MFA fatigue).
- Convinced cellular carriers to transfer control of a targeted user's phone number to a SIM card they controlled, gaining control over the phone and access to MFA prompts.
- Monetized access to victim networks in numerous ways including extortion enabled by ransomware and data theft.

Scattered Spider actors are highly adept at social engineering and conducting reconnaissance of their intended target prior to launching attacks. Sources of their research are social media platforms, public records, online data aggregators, and dark web marketplaces for breached data. They are known to conduct multiple reconnaissance of their targets to better understand the procedures of resetting passwords and MFA and to increase their success in gaining initial access to the networks.

Once inside a victim's network, Scattered Spider is known for Living-Off-the-Land (LOL) techniques that use legitimate tools within victim networks, like AnyDesk and TeamViewer, to evade detection. This allows the actors to remain undetected within a victim's network for a longer duration of time, known as dwell time, to accomplish their objectives and circumvent established endpoint and network detection efforts.

Scattered Spider actors will exploit identity platforms like Okta, AzureAD, and AWS IAM to acquire greater access to victim network resources and penetrate deeper into networks. The compromise of identity platforms aids in escalating privileges of threat actors to execute commands typically reserved for system administrators and privileged users. Scattered Spider actors then register their own MFA tokens or change group policies to bypass authentication and install remote monitoring and management (RMM) tools to establish persistence on the victim network.

After persistence is established on the victim network, the threat actors will map out the network to search for critical assets. Scattered Spider actors will search for critical assets of the victim, known as the “crown jewels” of the organization, such as credential files, backups, virtual machine infrastructure, SharePoint sites, and Virtual Private Networks (VPN). The threat actors then search for the existence of the victim’s data storage locations, such as cloud-based data storage platforms and on-premises storage servers to exfiltrate large volumes of data. The threat actors will also target the Active Directory and acquire code repositories, code-signing certificates, and source code for exfiltration. They will move laterally within the network to locate sensitive data and create a centralized folder or database prior to exfiltrating the victim’s data to an external site, particularly favoring Mega.nz and other cloud storage providers.

Scattered Spider actors have been known to deploy ransomware after exfiltration of victim data and have worked with Blackcat/AlphV and DragonForce ransomware variants, though the deployment of ransomware is not always present in their operations. Ransomware is a malware that will encrypt the files of victims and render the files inoperable until a decryption key is obtained by paying a ransom. Scattered Spider actors will provide a ransom note that is specific to the victim and provide instructions for payment, deadline for payment, and communication instructions to the threat actors. The threat actors often demand payment in cryptocurrency in return for the decryption key, or the victim’s sensitive data will be released to the public or sold in illicit dark web marketplaces where other cybercriminals can purchase it to perpetuate other crimes.
Sometimes, the threat actors have leveraged the victim’s clients to put additional pressure on the victim to pay the ransom.

Scattered Spider actors have monitored internal communications and joined conference calls to gather information related to the victim’s incident response plan, adjusting their tactics to make remediation of the victim’s network more difficult and time consuming.

In July 2025, Palo Alto Networks revealed that Scattered Spider adopted tactics to destroy victim virtual infrastructure and cloud-based assets. The attackers leveraged legitimate management platforms like ESXi to delete virtual machines and used cloud access platforms to destroy critical business systems. Such attacks will destroy victim infrastructure and are not recoverable with backups. [10]

Recent activity

July 2025

Law enforcement authorities in the U.K. arrested four members of Scattered Spider. Multiple sources close to the investigation said those arrested included Owen David Flowers, a U.K. man alleged to have been involved in the cyber intrusion and ransomware attack that shut down the casino's properties in September 2023.[11]

September 2025

The FBI and Department of Justice unsealed an indictment against Thalha Jubair, a U.K. national indicted for conspiracies to commit computer fraud, wire fraud, and money laundering. The indictment was connected to an investigation into Scattered Spider that involved at least 120 computer network intrusions as well as extortions involving 47 U.S. entities. The indictment alleges victims paid at least $115,000,000 in ransom payments.[12]

September 2025

With the arrest of Scattered Spider actors in the U.K., and the likely disruption of their illicit operations, Scattered Spider announced its "retirement".[13] Notably, this retirement was short lived, or rather, non-existent. Soon after this announcement, multiple operations attributed to Scattered Spider and Shiny Hunters have occurred, further complicating proper attribution to a particular group and underscoring the collaboration between cybercriminal groups.

Best practices

Wells Fargo recommends the following best practices to help protect against common Scattered Spider tactics and techniques. These best practices are widely recommended by cybersecurity experts. However, each company should consult with its key personnel or external advisors and act in accordance with its own policies, procedures, and legal obligations.

Cyber human defense

- Train and prepare employees, especially IT help desk personnel, against social engineering techniques.
- Stay vigilant against phishing, spearphishing, smishing, and vishing tactics.
- Conduct regular phishing tests of employees to ensure personnel respond effectively to phishing attempts.
- Conduct regular cybersecurity trainings to increase awareness, sustain vigilance, and review protocols in the event of cyber attacks.
- Wells Fargo clients can participate in cyber education and awareness engagements, which provide general guidance and industry best practices on today's cyber threat landscape, common tactics used by threat actors, and strategies organizations can use to help strengthen their security posture. These educational sessions often include scenario-based discussions and practical learning opportunities designed to help clients enhance their internal preparedness. For more information, existing clients should contact their Wells Fargo relationship manager.

Passwords

- Use strong passwords that have at least 12 – 16 characters and contain a mix of uppercase and lowercase letters, numbers, and symbols.
- Do not reuse passwords for multiple accounts.

Multi-factor authentication (MFA)	➢ Use phishing resistant MFA like passkeys or physical hard token keys, when possible. ➢ Avoid using SMS text as MFA when possible and contact your telecommunications carrier to block unauthorized SIM transfer attempts.
Monitoring and detection	➢ Establish a baseline of normal network traffic to more effectively identify anomalous and suspicious activity. ➢ Use Intrusion Detection Systems (IDS) and Network Detection Systems (NDS) to identify suspicious activity and the presence of malware. ➢ Look for suspicious domains in the URL and block them across your network. ➢ Monitor for exfiltration of data, especially to Mega.nz domains. ➢ Identify any known Indicators of Compromise (IOCs) within your network.
Data protection	➢ Establish a Data Loss Prevention (DLP) plan. ➢ Encrypt data at rest and data in transit. ➢ Create backups and keep them offline. ➢ Verify backups to ensure they work.
Preparation strategies	➢ Establish and test an incident response plan. ➢ Ensure that key decision makers understand their roles and responsibilities, and delegates are outlined in the plan. ➢ Conduct wargaming exercises to rehearse a possible incident response and address any gaps. ➢ Develop a communication plan to ensure key stakeholders including employees, customers, and service providers are notified of any potential impacts and recovery activities. ➢ Establish out-of-band communications for use in the event of a cyber incident. ➢ Perform regular audits of email and financial systems.

Emerging techniques

There are numerous reports detailing the weaponization of artificial intelligence (AI) by cybercriminals to conduct attacks. Scattered Spider has leveraged AI capabilities to:

- Develop advanced malware and phishing kits.
- Automate vulnerability assessments against their targets.
- Facilitate network navigation and lateral movement.[10]
- Increase the scale and speed of their campaigns.
- Generate deepfakes and voice cloning to impersonate individuals and potentially dupe intended targets.

Conclusion

Preparation is key to defending against cyberattacks and ensuring organizational resiliency. Organizations should strive to prevent attacks, but they should also be prepared to quickly detect anomalous activity to reduce impacts in the event of an intrusion. People are the most critical assets of an organization, but they can also be the most vulnerable point.

In today's cyber threat landscape, it is critical that organizations embrace and implement good cyber hygiene practices to defend against cyber threats.

Wells Fargo strives to provide world-class cyber protection for existing clients through defense and in-depth strategies ranging from cyber threat intelligence, a 24/7/365 Cyber Threat Fusion Center, and robust incident response teams to mitigate cyber threats. The Cyber Client Advisory (CCA) team has industry experts with decades of cybersecurity knowledge and experience that can provide, at no-cost, educational resources to help clients understand the cyber threat landscape, common tactics employed by cyber threat actors, and best practices to provide mitigation strategies to help reduce risks.

For more information, Wells Fargo clients should contact their relationship managers.

Glossary

Amazon S3 Bucket — A cloud storage and file hosting service provided by Amazon Web Services (AWS) that is commonly used by cybercriminals for data exfiltration.

Crown jewels — The most critical and valuable assets in an organization, like sensitive data or key systems.

Dark web marketplaces — Hidden websites typically used for illegal trade including stolen data, hacking tools, and drugs.

Data at rest — Data stored on a device or server, not actively moving through a network.

Data in transit — Data being sent or received across a network, like emails or file transfers.

Data Loss Prevention (DLP) program — Tools and policies that help prevent sensitive data from being leaked or stolen.

Deepfake — Fake videos or images created using artificial intelligence that look real, often used to deceive or impersonate.

Exfiltration — Unauthorized transfer or theft of data from a system.

Group Policy — A Windows feature that lets IT administrators manage settings across many computers at once.
Hard token keys — Physical devices (like USB keys or key fobs) used for secure login.

Incident response — The process of identifying, managing, and recovering from a cybersecurity incident.

Indicators of Compromise (IOCs) — Signs, such as strange files or network activity, that indicate a system may have been attacked; these indicators provide insight into cyber threat actors and help with attribution.

Intrusion Detection System (IDS) — A tool that monitors network traffic and alerts when it detects suspicious behavior.

Lateral movement — When cyber threat actors move from one system to another inside a network after gaining access.

Living-Off-the-Land (LOL) — Cyber threat actors that use built-in system tools to avoid detection and carry out attacks.

Mega.nz — A cloud storage and file hosting service based in New Zealand that is commonly used by cybercriminals for data exfiltration.

Multi-factor authentication (MFA) — A login method requiring two or more proofs of identity, like a password and phone code/biometrics.

MFA bombing attack — When cyber threat actors flood a user with MFA requests hoping the recipient will approve one by mistake, which then gives the threat actor unauthorized access into the account.

Network Detection System (NDS) — Monitors network traffic to detect threats, often with more advanced capabilities than IDS.

One-time password (OTP) — A temporary code used for logging in, valid only once and usually sent to your device.

Out-of-Band (OOB) communications — A backup communication method that uses a separate channel from the main network to prevent cyber adversaries from conducting surveillance on incident response.

Passkey — A secure login method that replaces passwords, often using biometrics or device-based authentication.

Persistence — Techniques that cyber adversaries use to stay hidden and maintain access to a victim's network over time.

Personally identifiable information (PII) — Information that can identify a person, like name, address, or social security number.

Phishing — Fake messages (usually emails) that convince the recipient to click on a link that is malicious or contains an attachment that contains malware when downloaded.

Ransomware — A type of malware that encrypts and locks files, allowing cyber adversaries to demand ransom payment in order to provide the victim with a private key to decrypt and unlock the files.

Remote Monitoring and Management (RMM) — Tools used by IT teams to manage systems remotely that can also be misused by cyber adversaries to conduct cyber attacks.

SIM swap attack — Cybercriminals will convince a phone company to switch your phone number to their SIM card in order to gain unauthorized access to victim accounts.

Social engineering attack — A cybercrime that relies on manipulating people into divulging confidential information or performing actions that compromise security.

Spearphishing — A targeted phishing attack aimed at a specific person or organization.

Uniform Resource Locator (URL) — Web address, like https://example.com.

Vishing — Short for voice phishing; scams done over the phone to steal personal information or convince the intended target to act, often leading to financial loss.

Vulnerability assessments — A security check to find weaknesses in systems and address vulnerabilities to reduce the risk of attacks.

Wargame — A simulated cyber attack exercise to test defenses and response strategies involving key personnel from executive staff, legal counsel, incident response teams, public relations, etc.

Sources

1. https://cybernews.com/news/scattered-spider-victims-ransom-payments/
2. https://www.quorumcyber.com/wp-content/uploads/2025/05/Threat-Actor-Profile-Scattered-Spider_V3.pdf
3. https://www.govtech.com/security/teen-arrested-on-suspicion-of-100m-vegas-strip-cyber-attack
4. https://www.bbrown.com/us/insight/a-look-back-at-the-mgm-and-caesars-incident/
5. https://www.bbc.com/news/articles/c0el31nqnpvo
6. https://dailysecurityreview.com/security-spotlight/scattered-spider-breached-ms-via-third-party-tcs- credentials-sources-confirm/
7. https://www.cnbc.com/2025/05/21/ms-cyberattack-to-wipe-out-nearly-one-third-of-annual-profits.html?msockid=0f9326b38c6062bd2ed730c58deb63b9
8. https://www.csoonline.com/article/4042522/behind-the-coinbase-breach-bribery-is-an-emerging-enterprise- threat.html
9. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
10. https://www.paloaltonetworks.com/blog/2025/07/muddled-libra-social-engineering-enterprise-scale- disruption/
11. https://krebsonsecurity.com/2025/07/uk-charges-four-in-scattered-spider-ransom-group/
12. https://www.justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including- critical
13. https://www.csoonline.com/article/4057074/scattered-spiders-retirement-announcement-genuine-exit-or- elaborate-smokescreen.html

April 2026

© 2026 Wells Fargo and Company.

Wells Fargo provides best practice and general information related to cyber risk and/or topics for educational and informational purposes only. The information provided in this document is not designed for any particular recipient but for the purpose of highlighting industry best practices for operating in a more secure manner. This document does not provide a complete list of all cyber threats or risk mitigation activities, nor does it document all types of best practices. Wells Fargo is not providing cyber-related advice or consulting services and recipients should decide whether to engage a cybersecurity firm for specific questions or advice.