Scattered Spider | CISA

Published: 2025-07-29 · Archived: 2026-04-05 13:33:57 UTC

1. Maintain offline backups of data **that are stored separately from the source systems and tested regularly**.
2. Enable and enforce phishing-resistant multifactor authentication (MFA).
3. Implementing application controls to manage and control software execution.

Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Royal Canadian Mounted Police (RCMP), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Australian Federal Police (AFP), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as the authoring organizations—are releasing this joint Cybersecurity Advisory in response to recent activity by Scattered Spider threat actors against the commercial facilities sectors, subsectors, and other sectors. This advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations as recently as June 2025.

Note: Originally published Nov. 16, 2023, this advisory has been updated through several iterations:

- **Nov. 16, 2023:** Initial version.
- **Nov. 21, 2023:** Updated password recommendation language on page 12.
- **July 29, 2025:** U.S. and international federal organizations identified new TTPs associated with the Scattered Spider cybercriminal group. In addition to new TTPs that include more sophisticated social engineering techniques, the advisory describes additional malware and ransomware variants used to exfiltrate data and encrypt targeted organizations' systems.

Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks.

Update July 29, 2025:

Per trusted third parties, Scattered Spider threat actors typically engage in data theft for extortion and also use several ransomware variants, most recently deploying DragonForce ransomware alongside their usual TTPs. While some TTPs remain consistent, Scattered Spider threat actors often change TTPs to remain undetected.

Update End

The authoring organizations encourage critical infrastructure organizations and commercial facilities to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of Scattered Spider malicious activity.

Download the original PDF version of this report:

Download the PDF version of this report:

The referenced media source is missing and needs to be re-embedded.

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 17. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for tables of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Overview

Scattered Spider (also known as, UNC3944, Scatter Swine, Oktapus, Octo Tempest, Storm-0875, and Muddled Libra) engages in data extortion and several other criminal activities.[1] Scattered Spider threat actors use multiple social engineering techniques—including push bombing—and subscriber identity module (SIM) swap attacks, to obtain credentials, install remote access tools, and/or bypass multi-factor authentication (MFA). According to public reporting, Scattered Spider threat actors have:[2]

- Posed as company IT and/or helpdesk staff using phone calls or SMS messages to obtain credentials from employees and gain access to the network [T1598] [T1656].
- Posed as company IT and/or helpdesk staff to direct employees to run commercial remote access tools enabling initial access [T1204] [T1219] [T1566].
- Posed as IT staff to convince employees to share their one-time password (OTP), an MFA authentication code.

Update July 29, 2025:

- Posed as employees to convince IT and/or helpdesk staff to provide sensitive information, reset the employee's password, and transfer the employee's MFA to a device they control on separate devices.

Update End

- Sent repeated MFA notification prompts leading to employees pressing the "Accept" button (also known as MFA fatigue) [T1621].[3]
- Convinced cellular carriers to transfer control of a targeted user's phone number to a SIM card in their possession, gaining control over the phone and access to MFA prompts.
- Monetized access to targeted organization's networks in numerous ways including extortion enabled by ransomware and data theft [T1657].

The FBI observed Scattered Spider threat actors, after gaining access to networks, using publicly available, legitimate remote access tunneling tools. **Table 1** details a list of legitimate tools Scattered Spider repurposed and used for their criminal activity.

Note: The use of these legitimate tools alone is not indicative of malicious activity. Users should review the Scattered Spider IOCs and TTPs discussed in this advisory to determine whether they have been compromised.

Table 1: Legitimate Tools Used by Scattered Spider

Tool	**Intended Use**
Fleetdeck.io	Enables remote monitoring and management of systems.
Level.io	Enables remote monitoring and management of systems.
Mimikatz [S0002]	Extracts credentials from a system.
Ngrok [S0508]	Enables remote access to a local web server by tunneling over the internet.
Pulseway	Enables remote monitoring and management of systems.
Screenconnect	Enables remote connections to network devices for management.
Splashtop	Enables remote connections to network devices for management.
Tactical.RMM	Enables remote monitoring and management of systems.
Tailscale	Provides virtual private networks (VPNs) to secure network communications.
TeamViewer	Enables remote connections to network devices for management.
Update July 29, 2025: Teleport.sh	Enables remote access to a local system by tunneling over the internet.
AnyDesk	Enables remote access to network devices for management, bypassing security alerts due to AnyDesk being a legitimate application.
Teleport.sh	Enables remote access to a local system by tunneling over the internet. **Update End**

In addition to using legitimate tools, Scattered Spider also uses malware as part of its TTPs. See **Table 2** for some of the malware used by Scattered Spider.

Table 2: Malware Used by Scattered Spider

Malware	**Use**

Malware	Use
AveMaria (also known as WarZone [S0670])	Enables remote access to a targeted organization's systems.
Raccoon Stealer [S1148]	Steals information including login credentials [TA0006], browser history [T1217], cookies [T1539], and other data.
VIDAR Stealer	Steals information including login credentials, browser history, cookies, and other data.
Update July 29, 2025: RattyRAT	Java-based remote access trojan, used for persistent, stealth access and internal reconnaissance.[4]
DragonForce Ransomware	Infiltrates networks, encrypts data, and demands ransom. **Update End**

Scattered Spider threat actors historically evade detection on target networks by using living off the land (LOTL) techniques and allowlisted applications to navigate a targeted organization's network, as well as frequently modifying their TTPs. For additional information on LOTL techniques, see the joint advisory, Identifying and Mitigating Living Off the Land Techniques.

Scattered Spider threat actors have observably exfiltrated data [TA0010] after gaining access and threatened to release it without deploying ransomware.

Update July 29, 2025:

Recently, this includes exfiltration to multiple sites including MEGA[.]NZ and U.S.-based data centers such as Amazon S3 [T1567.002].

Update End

Recent Scattered Spider TTPs

File Encryption

Update July 29, 2025:

The FBI has identified that Scattered Spider threat actors may exfiltrate data from targeted organization's systems for extortion and then encrypt data on the system for ransom [T1486]. After exfiltrating and/or encrypting data, Scattered Spider threat actors communicate with targeted organizations via TOR, Tox, email, or encrypted applications.

Update End

Reconnaissance, Resource Development, and Initial Access

Scattered Spider intrusions historically began with broad phishing [T1566] and smishing [T1660] attempts against a target using organization-specific crafted domains, such as the domains listed in **Table 3** [T1583.001].

Table 3: Domains Used by Scattered Spider Threat Actors

Domains
targetsname-sso[.]com
targetsname-servicedesk[.]com
targetsname-okta[.]com
Update July 29, 2025: targetsname-cms[.]com
targetsname-helpdesk[.]com
oktalogin-targetcompany[.]com

The targeted organization's name is often appended with either a *-helpdesk* or a type of single sign-on (SSO) solution to add credibility. While Scattered Spider threat actors have not been observed using these techniques recently, the group continuously evolves its TTPs and these methods could be reused.

Scattered Spider threat actors currently use a variety of methods to gain initial access to a targeted organization's network. In some instances, the threat actors purchase employee or contractor credentials on illicit marketplaces such as Russia Market [T1597.002]. In other cases, the threat actors compromise third party services with access to several potential targeted organization's networks [T1199]. It is common for the threat actors to gather the personally identifiable information (PII) of users with elevated access to their network using online open-source information.

While Scattered Spider initially began their activity relying upon broad phishing campaigns, the threat actors are now employing more targeted and multilayered spearphishing and vishing operations. Scattered Spider searches business-to-business websites to gather information and ultimately determine the individual's role in a target organization [T1594].

After identifying usernames, passwords, PII [T1589], and conducting SIM swaps, the threat actors then use layered social engineering techniques [T1656] which frequently occur over several calls [T1598.004]. The social engineering attempts are designed to first learn what steps are needed to conduct password resets from helpdesks. Once that information is identified, the threat actors continue to conduct phone calls to employees and help desks to gather password reset specific information of a targeted employee.

Finally, the threat actors conduct spearphising calls to convince IT help desk personnel to reset passwords and/or transfer MFA tokens [T1078.002] [T1199] [T1566.004]. At which point, the threat actors perform account takeovers against the users in SSO environments. These social engineering attempts are enriched by access to personal information derived from social media [T1593.001], open-source information, commercial intelligence tools, and database leaks. Scattered Spider threat actor tactics and techniques also make it more difficult for network defenders to warn targeted organizations or to use threat hunting tools to proactively identify intrusions.

Update End

Execution, Persistence, and Privilege Escalation

Scattered Spider threat actors then register their own MFA tokens [T1556.006] [T1606] and deploy remote monitoring and management (RMM) tools [T1219] after compromising a user's account to establish persistence [TA0003]. Historically, the threat actors added a federated identity provider to the targeted organization's SSO tenant and activated automatic account linking [T1484.002]. While the threat actors may still be using this tactic, it has not been identified as a current TTP.

The threat actors were then able to sign into any account by using a matching SSO account attribute. At this stage, Scattered Spider threat actors already controlled the identity provider and then could choose an arbitrary value for this account attribute. This activity allowed the threat actors to perform privilege escalation [TA0004] and continue logging in even when passwords were changed [T1078]. Threat actors achieve elevated privileges by leveraging internal communication tools to contact employees and social engineering.

Discovery, Lateral Movement, and Exfiltration

Once persistence is established on a target network, Scattered Spider threat actors often perform discovery, specifically searching for SharePoint sites [T1213.002], credential storage documentation [T1552.001], VMware vCenter infrastructure [T1018], backups, and instructions for setting up/logging into Virtual Private Networks (VPNs) [TA0007]. The threat actors enumerate the targeted organization's Active Directory (AD) and then perform discovery and exfiltration of the targeted organization's code repositories [T1213.003], code-signing certificates [T1552.004], and source code [T1083] [TA0010]. Threat actors activate Amazon Web Services (AWS) Systems Manager Inventory [T1538] to discover targets for lateral movement [TA0007] [TA0008], then move to both preexisting [T1021.007] and actor-created [T1578.002] Amazon Elastic Compute Cloud (EC2) instances. In instances where the ultimate goal is data exfiltration, Scattered Spider threat actors use actor-installed extract, transform, and load (ETL) tools [T1648] to bring data from multiple data sources into a centralized database [T1074] [T1530].

Update July 29, 2025:

In many instances, Scattered Spider threat actors search for a targeted organization's Snowflake access to exfiltrate large volumes of data in a short time, often running thousands of queries immediately [T1567]. According to trusted third parties, where more recent incidents are concerned, Scattered Spider threat actors may have deployed DragonForce ransomware onto targeted organizations' networks—thereby encrypting VMware Elastic Sky X integrated (ESXi) servers [T1486].

Update End

To determine if their activities have been detected and to maintain persistence within the compromised system, Scattered Spider threat actors often search a targeted organization's Slack, Microsoft Teams, and Microsoft Exchange Online for emails [T1114] or conversations regarding the threat actors' intrusion and any security response. The threat actors frequently join incident remediation and response calls and teleconferences, likely to identify how security teams are hunting them and proactively develop new avenues of intrusion in response to a targeted organizations' defenses.

Update July 29, 2025:

This is sometimes achieved by creating new identities in the environment [T1136] and is often upheld with fake social media profiles [T1585.001] to backstop newly created identities. Scattered Spider threat actors consistently use proxy networks [T1090] and rotate machine names to further hamper detection and response.

Update End

MITRE ATT&CK Tactics and Techniques

See **Table 4** to **Table 17** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool .

Table 4: Reconnaissance

Technique Title	ID	Use
Gather Victim Identity Information	T1589	Scattered Spider threat actors gather usernames, passwords, and PII for targeted organizations.
Phishing for Information	T1598	Scattered Spider threat actors use phishing to obtain login credentials, gaining access to a targeted organization's network.
Search Closed Sources: Purchase Technical Data	T1597.002	Scattered Spider threat actors purchase credentials from illicit marketplaces.
Search Victim-Owned Websites	T1594	Scattered Spider threat actors search targeted organization-owned websites to gather information such as work roles and contact information.
Phishing for Information: Spearphishing Voice	T1598.004	Scattered Spider threat actors call targeted organizations to elicit sensitive and actionable information.
Search Open Websites/Domains: Social Media	T1593.001	Scattered Spider threat actors scour targeted organizations' social media to gather further information about roles and interests of staff.

Table 5: Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Domains	T1583.001	Scattered Spider threat actors create domains for use in phishing and smishing attempts against targeted organizations.
Establish Accounts: Social Media Accounts	T1585.001	Scattered Spider threat actors create fake social media profiles to backstop newly created user accounts in a targeted organization.

Table 6: Initial Access

Technique Title	ID	Use
Phishing	T1566	Scattered Spider threat actors use broad phishing attempts against a target to obtain information used to gain initial access. Scattered Spider threat actors pose as helpdesk personnel to direct employees to install commercial remote access tools.
Phishing (Mobile)	T1660	Scattered Spider threat actors send SMS messages, known as smishing, when targeting an organization.
Phishing: Spearphishing Voice	T1566.004	Scattered Spider threat actors use voice communications to convince IT help desk personnel to reset passwords and/or MFA tokens.
Trusted Relationship	T1199	Scattered Spider threat actors abuse trusted relationships of contracted IT help desks to gain access to targeted organizations.
Valid Accounts: Domain Accounts	T1078.002	Scattered Spider threat actors obtain access to valid domain accounts to gain initial access to a targeted organization.

Table 7: Execution

Technique Title	ID	Use
Serverless Execution	T1648	Scattered Spider threat actors use ETL tools to collect data in cloud environments.
User Execution	T1204	Scattered Spider threat actors impersonating helpdesk personnel direct employees to run commercial remote access tools thereby enabling access to the targeted organization’s network.

Table 8: Persistence

Technique Title	ID	Use

Technique Title	ID	Use
Persistence	TA0003	Scattered Spider threat actors seek to maintain persistence on a targeted organization's network.
Create Account	T1136	Scattered Spider threat actors create new user identities in the targeted organization.
Modify Authentication Process: Multi-Factor Authentication	T1556.006	Scattered Spider threat actors may modify MFA tokens to gain access to a targeted organization's network.
Valid Accounts	T1078	Scattered Spider threat actors abuse and control valid accounts to maintain network access even when passwords are changed.

Table 9: Privilege Escalation

Technique Title	ID	Use
Privilege Escalation	TA0004	Scattered Spider threat actors escalate account privileges when on a targeted organization's network.
Domain Policy Modification: Domain Trust Modification	T1484.002	Scattered Spider threat actors add a federated identity provider to the targeted organization's SSO tenant and activate automatic account linking.

Table 10: Defense Evasion

Technique Title	ID	Use
Modify Cloud Compute Infrastructure: Create Cloud Instance	T1578.002	Scattered Spider threat actors create cloud instances for use during lateral movement and data collection.
Impersonation	T1656	Scattered Spider threat actors pose as company IT and/or helpdesk staff to gain access to targeted organization's networks. Scattered Spider threat actors use social engineering to convince IT helpdesk personnel to reset passwords and/or MFA tokens.

Table 11: Credential Access

Technique Title	ID	Use
Credential Access	TA0006	Scattered Spider threat actors use tools, such as Raccoon Stealer, to obtain login credentials.

Technique Title	ID	Use
Forge Web Credentials	T1606	Scattered Spider threat actors may forge MFA tokens to gain access to a targeted organization’s network.
Multi-Factor Authentication Request Generation	T1621	Scattered Spider sends repeated MFA notification prompts to lead employees to accept the prompt and gain access to the target network.
Unsecured Credentials: Credentials in Files	T1552.001	Scattered Spider threat actors search for insecurely stored credentials on targeted organization’s systems.
Unsecured Credentials: Private Keys	T1552.004	Scattered Spider threat actors search for insecurely stored private keys on targeted organization’s systems.
SIM Swap	T1451	Scattered Spider threat actors steal OTPs, credentials, and security answers.

Table 12: Discovery

Technique Title	ID	Use
Discovery	TA0007	Upon gaining access to a targeted network, Scattered Spider threat actors seek out SharePoint sites, credential storage documentation, VMware vCenter, infrastructure backups and enumerate AD to identify useful information to support further operations.
Browser Information Discovery	T1217	Scattered Spider threat actors use tools (e.g., Raccoon Stealer) to obtain browser histories.
Cloud Service Dashboard	T1538	Scattered Spider threat actors leverage AWS Systems Manager Inventory to discover targets for lateral movement.
File and Directory Discovery	T1083	Scattered Spider threat actors search a compromised network to discover files and directories for further information or exploitation.
Remote System Discovery	T1018	Scattered Spider threat actors search for infrastructure, such as remote systems, to exploit.
Steal Web Session Cookie	T1539	Scattered Spider threat actors use tools, such as Raccoon Stealer, to obtain browser cookies.

Table 13: Lateral Movement

Technique Title	ID	Use

Technique Title	ID	Use
Lateral Movement	TA0008	Scattered Spider threat actors laterally move across a target network upon gaining access and establishing persistence.
Remote Services: Cloud Services	T1021.007	Scattered Spider threat actors use pre-existing cloud instances for lateral movement and data collection.

Table 14: Collection

Technique Title	ID	Use
Data from Information Repositories: Code Repositories	T1213.003	Scattered Spider threat actors search code repositories for data collection and exfiltration.
Data from Information Repositories: SharePoint	T1213.002	Scattered Spider threat actors search SharePoint repositories for information.
Data Staged	T1074	Scattered Spider threat actors stage data from multiple data sources into a centralized database before exfiltration.
Email Collection	T1114	Scattered Spider threat actors search targeted organization's emails to determine if the organization has detected the intrusion and initiated any security response.
Data from Cloud Storage	T1530	Scattered Spider threat actors search data in cloud storage for collection and exfiltration.

Table 15: Command and Control

Technique Title	ID	Use
Remote Access Software	T1219	Impersonating helpdesk personnel, Scattered Spider threat actors direct employees to run commercial remote access tools thereby enabling access to, and command and control of, the targeted organization's network. Scattered Spider threat actors leverage third-party software to facilitate lateral movement and maintain persistence on a target organization's network.
Proxy	T1090	Scattered Spider threat actors use proxy networks to disguise the source of malicious traffic.

Table 16: Exfiltration

Technique Title	ID	Use

Technique Title	ID	Use
Exfiltration	TA0010	Scattered Spider threat actors exfiltrate data from a target network for data extortion.
Exfiltration Over Web Service	T1567	Scattered Spider threat actors exfiltrate data using the Snowflake Data Cloud.

Table 17: Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Scattered Spider threat actors recently began encrypting data on a target network and demanding a ransom for decryption. Scattered Spider threat actors have been observed encrypting VMware ESXi servers.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Scattered Spider threat actors exfiltrate data to multiple sites including U.S.-based data centers and MEGA[.]NZ.
Financial Theft	T1657	Scattered Spider threat actors monetized access to targeted organization's networks in numerous ways including extortion-enabled ransomware and data theft.

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on the threat actors' activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

Update July 29, 2025:

Following speculation in the press about Scattered Spider targeting entities in the UK in May 2025, the NCSC released a blog post with recommended actions for organizations to take.

Update End

- **Implement application controls** to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent installation and execution of portable

versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.

- **Reduce the threat of malicious** actors using remote access tools by:
  - **Auditing remote access tools** on your network to identify currently used and/or authorized software.
  - **Reviewing logs for execution of remote access software** to detect abnormal use of programs running as a portable executable [CPG 2.T].
  - **Using security software** to detect instances of remote access software being loaded only in memory.
  - **Requiring authorized remote access solutions** to be used only from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
  - **Blocking both inbound and outbound connections** on common remote access software ports and protocols at the network perimeter.
  - **Applying recommendations** in the Guide to Securing Remote Access Software.

Update July 29, 2025:

- **Note:** The threat actors' exact remote access tool will vary. One open-source resource for identifying IOCs and Sigma rules associated with remote access tools is LOLRMM.

Update End

- **Implement FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based MFA.** These MFA implementations are resistant to phishing and not susceptible to push bombing or SIM swap attacks, which are techniques known to be used by Scattered Spider actors. See CISA's fact sheet Implementing Phishing-Resistant MFA for more information.
- **Strictly limit the use of Remote Desktop Protocol (RDP) and other remote desktop services.** If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.
  - Apply phishing-resistant MFA.
  - Log and monitor for RDP login attempts.

In addition, the authoring agencies recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).

- **Maintain offline backups of data** and regularly test restoration (no less than once a year). By instituting this practice, an organization limits the severity of disruption to its business practices [CPG 2.R].
- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) **to comply** with NIST's standards for developing and managing password policies.
    - Use "strong" passwords that are unique and random, as well as contain at least fifteen or more characters [CPG 2.B].
    - Do not reuse passwords [CPG 2.C].
    - Consider implementing industry-recognized password managers that align with organizational technology procurement policies.
    - Implement multiple failed login attempt account lockouts [CPG 2.G].
    - Disable password "hints."
    - Refrain from requiring recurring password changes.

      Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication (MFA)** for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems [CPG 2.H]. Organizations should continue to perform diligent employee training against vishing and spearphishing.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement [CPG 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, leverage a tool that logs and reports all network traffic and activity, including lateral movement, on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host [CPG 3.A].

Update July 29, 2025:

- **Enhance monitoring against unauthorized account misuse.** Look for "risky logins" within environments where sign-in attempts have been flagged as potentially compromised due to suspicious activity or unusual behavior.

Update End

- **Disable unused ports and protocols** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].
- **Disable hyperlinks** in received emails.

- **Ensure all backup data is encrypted, immutable, is stored separately from the source files, and is tested regularly** and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring organizations recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 4** to **Table 17**).
2. Align security technologies against the technique.
3. Test technologies against the technique.
4. Analyze detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Reporting

Your organization has no obligation to respond or provide information back to FBI in response to this joint advisory. If, after reviewing the information provided, your organization decides to provide information to FBI, reporting must be consistent with applicable state and federal laws.

FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Scattered Spider threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

The authoring agencies do not encourage paying ransom, as payment does not guarantee targeted organization's files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, FBI and CISA urge you to promptly report ransomware incidents to FBI's Internet Crime Complain Center (IC3), a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center at SOC@mail.cisa.dhs.gov✉ or 1-844-Say-CISA (1-844-729-2472).

Disclaimer

The information in this report is being provided “as is” for informational purposes only. The FBI and CISA do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI and CISA.

Version History

November 16, 2023: Initial version.
November 21, 2023: Updated password recommendation language on page 12.
July 29, 2025: Updated to reflect new co-sealers and TTPs.

Notes

---

[1] Phelix Oluoch and Trellix, “Scattered Spider: The Modus Operandi,” *Trellix* (blog), *Trellix*, last modified August 17, 2023, https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html .

[2] Tim Parisi, “Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies,” *Crowdstrike* (blog), *Crowdstrike*, last modified December 1, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/ ; Crowdstrike Intelligence Team, SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security, *Crowdstrike* (blog), *Crowdstrike*, last modified January 19, 2023, https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/ ; and Christopher Boyd, “Ransomware group steps up, issues statement over MGM Resorts compromise,” *ThreatDown Intelligence* (blog), *Malwarebytes*, last modified September 18, 2023, https://www.malwarebytes.com/blog/personal/2023/09/ransomware-group-steps-up-issues-statement-over-mgm-resorts-compromise .

[3] Boyd, “Ransomware group steps up, issues statement over MGM Resorts compromise .”

[4] Ayelen Torello, “Emulating the Unyielding Scattered Spider,” *AttackIQ* (blog), *AttackIQ*, last modified May 29, 2025, https://www.attackiq.com/2025/05/29/emulating-scattered-spider/ .
