JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-320A

November 16, 2023

Scattered Spider

SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) in response to recent activity by Scattered Spider threat actors against the commercial facilities sectors and subsectors. This advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations as recently as November 2023.

Actions to take today to mitigate malicious cyber activity:

- Maintain offline backups of data.
- Enable and enforce phishing-resistant multifactor authentication (MFA).
- Implementing application controls to manage and control software execution.

Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs.

FBI and CISA encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of a cyberattack by Scattered Spider actors.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See the MITRE ATT&CK® Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. 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.

Overview

Scattered Spider (also known as Starfraud, UNC3944, Scatter Swine, and Muddled Libra) engages in data extortion and several other criminal activities.[1] Scattered Spider threat actors are considered experts in social engineering and use multiple social engineering techniques, especially phishing, 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],[3],[4]:

- 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.
- Sent repeated MFA notification prompts leading to employees pressing the “Accept” button (also known as MFA fatigue) [T1621].[5]
- 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 [T1657].

After gaining access to networks, FBI observed Scattered Spider threat actors 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 criminal activity. Users should review the Scattered Spider indicators of compromise (IOCs) and TTPs discussed in this CSA 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.

Tool	Intended Use
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.

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
AveMaria (also known as WarZone [S0670])	Enables remote access to a victim's systems.
Raccoon Stealer	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.

Scattered Spider threat actors have historically evaded detection on target networks by using living off the land techniques and allowlisted applications to navigate victim networks, as well as frequently modifying their TTPs.

Observably, Scattered Spider threat actors have exfiltrated data [TA0010] after gaining access and threatened to release it without deploying ransomware; this includes exfiltration to multiple sites including U.S.-based data centers and MEGA[.]NZ [T1567.002].

Recent Scattered Spider TTPs

New TTP - File Encryption

More recently, FBI has identified Scattered Spider threat actors now encrypting victim files after exfiltration [T1486]. After exfiltrating and/or encrypting data, Scattered Spider threat actors communicate with victims via TOR, Tox, email, or encrypted applications.

Reconnaissance, Resource Development, and Initial Access

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

Table 3: Domains Used by Scattered Spider Threat Actors

Domains
victimname-sso[.]com
victimname-servicedesk[.]com
victimname-okta[.]com

In most instances, Scattered Spider threat actors conduct SIM swapping attacks against users that respond to the phishing/smishing attempt. The threat actors then work to identify the personally identifiable information (PII) of the most valuable users that succumbed to the phishing/smishing, obtaining answers for those users' security questions. After identifying usernames, passwords, PII [T1589], and conducting SIM swaps, the threat actors then use social engineering techniques [T1656] to convince IT help desk personnel to reset passwords and/or MFA tokens [T1078.002],[T1199],[T1566.004] to perform account takeovers against the users in single sign-on (SSO) environments.

Execution, Persistence, and Privilege Escalation

Scattered Spider threat actors then register their own MFA tokens [T1556.006],[T1606] after compromising a user's account to establish persistence [TA0003]. Further, the threat actors add a federated identity provider to the victim's SSO tenant and activate automatic account linking [T1484.002]. The threat actors are then able to sign into any account by using a matching SSO account attribute. At this stage, the Scattered Spider threat actors already control the identity provider and then can choose an arbitrary value for this account attribute. As a result, this activity allows the threat actors to perform privileged escalation [TA0004] and continue logging in even when passwords are changed [T1078]. Additionally, they leverage common endpoint detection and response (EDR) tools installed on the victim networks to take advantage of the tools' remote-shell capabilities and executing of commands which elevates their access. They also deploy remote monitoring and management (RMM) tools [T1219] to then maintain persistence.

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 (VPN) [TA0007]. The threat actors enumerate the victim's Active

Directory (AD), perform discovery and exfiltration of victim'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]. According to trusted third parties, where more recent incidents are concerned, Scattered Spider threat actors may have deployed BlackCat/ALPHV ransomware onto victim networks—thereby encrypting VMware Elastic Sky X integrated (ESXi) servers [T1486].

To determine if their activities have been uncovered and maintain persistence, Scattered Spider threat actors often search the victim's Slack, Microsoft Teams, and Microsoft Exchange online for emails [T1114] or conversations regarding the threat actor's 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 victim defenses. 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.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 4 through 17 for all referenced threat actor tactics and techniques in this advisory.

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 victim's network.

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.

Technique Title	ID	Use
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 have posed 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 a victim.
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 victim's network.

Table 8: Persistence

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 victim'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 identify provider to the victim'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 will create cloud instances for use during lateral movement and data collection.
Impersonation	TA1656	Scattered Spider threat actors pose as company IT and/or helpdesk staff to gain access to victim's networks. Scattered Spider threat actors use social engineering to convince IT help desk 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.
Forge Web Credentials	T1606	Scattered Spider threat actors may forge MFA tokens to gain access to a victim'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 victim's systems.
Unsecured Credentials: Private Keys	T1552.004	Scattered Spider threat actors search for insecurely stored private keys on victim's systems.

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.

Technique Title	ID	Use
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
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 victim's emails to determine if the victim 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 victim's network. Scattered Spider threat actors leverage third-party software to facilitate lateral movement and maintain persistence on a target organization's network.

Table 16: Exfiltration

Technique Title	ID	Use
Exfiltration	TA0010	Scattered Spider threat actors exfiltrate data from a target network to for data extortion.

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 has 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 victim networks in numerous ways including extortion-enabled ransomware and data theft.

MITIGATIONS

FBI and CISA recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on the threat actor activity and to reduce the risk of compromise by Scattered Spider threat actors. 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 Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

> These mitigations apply to all critical infrastructure organizations and network defenders. FBI and CISA recommend that software manufactures incorporate secure-by-design and -default principles and tactics into their software development practices limiting the impact of ransomware techniques, thus, strengthening the secure posture for their customers.
>
> For more information on secure by design, see CISA's Secure by Design and Default webpage and joint guide.

- **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 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.
- **Implementing FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based MFA**. These MFA implementations are resistant to phishing and not suspectable 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 multifactor authentication (MFA).
  - Log RDP login attempts.

In addition, the authoring authorities of this CSA 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 maintain backup and restoration (daily or weekly at minimum). 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 account, admin accounts, and domain admin accounts) **to comply** with NIST's standards for developing and managing password policies.
  - Use longer passwords consisting of at least eight characters and no more than 64 characters in length [CPG 2.B].
  - Store passwords in hashed format using industry-recognized password managers.
  - Add password user "salts" to shared login credentials.
  - Avoid reusing passwords [CPG 2.C].
  - Implement multiple failed login attempt account lockouts [CPG 2.G].
  - Disable password "hints."
  - Refrain from requiring password changes more frequently than once per year.
    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].
- **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, implement 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].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **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** (i.e., ensure backup data cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, FBI and CISA 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. FBI and CISA recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 4-17).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your 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.

FBI and CISA 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

FBI and CISA are seeking any information that can be shared, to include a sample ransom note, communications with Scattered Spider group actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. FBI and CISA do not encourage paying ransom as payment does not guarantee victim 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 a local FBI Field Office, report the incident to FBI's Internet Crime Complaint Center (IC3) at IC3.gov, or CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

REFERENCES

[1] MITRE ATT&CK – Scattered Spider

[2] Trellix - Scattered Spider: The Modus Operandi

[3] Crowdstrike - Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies

[4] Crowdstrike - SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security

[5] Malwarebytes - Ransomware group steps up, issues statement over MGM Resorts compromise

DISCLAIMER

VERSION HISTORY

November 16, 2023: Initial version.