U.S. Coast Guard Cyber Command

Maritime Cyber Alert

Information Sharing Protocol: **TLP:CLEAR** (https://www.us-cert.gov/tlp)

August 6, 2025

Scattered Spider Targeting Critical Infrastructure

SUMMARY

Government agencies have observed the threat actor Scattered Spider conducting malicious activity against multiple critical infrastructure sectors. Scattered Spider employs various social engineering techniques, ransomware deployment, and data theft to execute monetary extortion schemes. Furthermore, Coast Guard Cyber Command (CGCYBER) observed similar social engineering activity in the Marine Transportation System (MTS). Maritime entities are urged to review this alert and follow the recommendations provided.

Background

The cybercriminal group Scattered Spider targets large organizations in the commercial facility sectors and subsectors with the primary motivation of financial gain. They utilize ransomware, data exfiltration, and a variety of social engineering tactics. Scattered Spider threat actors often alternate Tactics, Techniques and Procedures (TTPs) to evade detection; however, some TTPs remain consistent.[1]

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and multiple foreign government agencies released a joint cybersecurity advisory on July 29th, 2025, warning of Scattered Spider actions and providing recommended mitigations for companies. In late July 2025, CGCYBER observed what is believed to be Scattered Spider threat actors targeting companies in the MTS using similar social engineering techniques, including impersonation of IT help desks to gain access to run remote access tools and use Microsoft 365 applications.

In addition to targeted vishing campaigns, Scattered Spider actors conduct multi-factor authentication (MFA) push bombing and subscriber identity module (SIM) swap attacks to bypass MFA. Once initial access is established, Scattered Spider actors Live off the Land (LOTL) by using legitimate remote access tunneling tools. They also use malware to exfiltrate data, maintain persistence, and encrypt data for ransom.

[1] “Scattered Spider” July 29, 2025. Scattered Spider | CISA

Targeted Applications & Systems

Scattered Spider threat actors conduct initial access, discovery, lateral movement, and exfiltration by:

- Conducting vishing calls via Microsoft Teams
- Searching Microsoft SharePoint
- Searching VMware vCenter infrastructure
- Activating Amazon Web Services (AWS) Systems Manager Inventory
- Searching Snowflake access
- Deploying DragonForce ransomware. which encrypts VMware Elastic Sky X integrated (ESXi) servers
- Monitoring Slack, Microsoft Teams, and Microsoft Exchange Online for communications regarding their intrusion

Scattered Spider actors are targeting applications within the Microsoft 365 application suite. This is relevant to the MTS because in 2024, CGCYBER CPTs found that 80% of MTS mission partners relied upon the Microsoft 365 application suite for business operations. Similarly, Scattered Spider actors are leveraging cloud services such as AWS and Snowflake. CGCYBER CPTs found that 53% of partners in 2024 used cloud-based infrastructure with AWS being one of the most commonly used service providers.[2]

Threat Actor Tactics:

Below are the tactics referenced by MITRE ATT&CK techniques, which are linked to these attacks (Techniques - Enterprise | MITRE ATT&CK®).

- **T1589: Gather Victim Identity Information**
  - □ In 2024, the most common technique successfully used by CPTs during cybersecurity assessments / penetration testing was T1589.001, gathering credentials.
- **T1598 & T1598.004: Phishing for Information & Spearphishing Voice**
  - □ T1598: Phishing for Information has been observed by CGCYBER in MTS cyber incidents three times so far in 2025.
- **T1594, T1597.002, & T1593.001: Search Victim Owned Websites, Search Closed Sources – Purchase Technical Data, & Search Open Websites/Domains – Social Media**
- **T1583.001: Acquire Infrastructure - Domains**
  - □ Threat actors create domains for use in phishing and smishing campaigns. CGCYBER has observed similar activity during phishing campaigns in the MTS in 2025.
- **T1585.001: Establish Accounts – Social Media Accounts**
  - □ Threat actors create fake social media profiles to corroborate fake identities of new user accounts created in targeted organizations.
- **T1566, T1566.004, & T1660: Phishing, Spearphishing Voice, & Phishing (Mobile)**
  - □ Threat actors use broad phishing attempts, pose as help desk personnel to install remote access tools, send SMS smishing messages, and use voice communications to bypass MFA.
  - □ T1566: Phishing was seen in 24% of MTS cyber incidents observed by CGCYBER so far in 2025.
- **T1648: Serverless Execution**
  - □ Threat actors use extract, transform, and load (ETL) tools to collect data in cloud environments.

[2] “2024 Cyber Trends and Insights in the Marine Environment” 2024 Cyber Trends in the Marine Environment

- **T1204: User Execution**
  - Threat actors direct employees to run commercial remote access tools to gain access.
- **T1136 & T1078: Create Account & Valid Accounts**
  - Threat actors establish persistent access by creating accounts and manipulating valid accounts. These are common techniques used by threat actors in the MTS.
- **T1556.006: Modify Authentication Process – Multi-Factor Authentication**
- **T1484.002: Domain Policy Modification – Domain Trust Modification**
  - Threat actors add a federated identity provider to the target's SSO tenant and activate automatic account linking.
- **T1578.002: Modify Cloud Compute Infrastructure – Create Cloud Instance**
  - Threat actors create cloud instances for lateral movement and data collection.
- **T1606: Forge Web Credentials**
  - Threat actors forge MFA tokens to gain access.
- **T1621: Multi-Factor Authentication Request Generation**
  - Threat actors send repeated MFA notifications for employees to accept and provide access to networks.
- **T1552.001 & T1552.004: Unsecured Credentials – Credentials in Files & Private Keys**
  - Threat actors search for unsecured credentials and private keys on organization systems.
- **T1451: SIM Swap**
  - Threat actors steal One Time Passwords, credentials, and security answers to request SIM swaps from mobile carriers. This allows for interception of SMS messages for authentication purposes.
- **T1021.007: Remote Services – Cloud Services**
  - Threat actors use pre-existing cloud instances for lateral movement and data collection.
  - Remote services techniques were the second most used by CPTs during cybersecurity assessments / penetration testing of MTS partner networks in 2024
- **T1213.002 & T1213.003: Data from Information Repositories – SharePoint & Code Repositories**
- **T1114: Email Collection**
  - Threat actors search emails to determine if targets have detected the intrusion or have begun responding.
- **T1530: Data from Cloud Storage**
- **T1219: Remote Access Software**
  - Threat actors impersonate IT helpdesk personnel to lead employees to run commercial remote access tools, resulting in command and control of the network.
- **T1567.002: Exfiltration Over Web Service – Exfiltration to Cloud Storage**
  - Threat actors exfiltrate data using Snowflake Data Cloud to multiple sites including U.S. based data centers and MEGA[.]NZ.
- **T1486: Data Encrypted for Impact**
  - Threat actors recently began encrypting data for ransom. This technique was seen in 24% of MTS cyber incidents in 2025.
- **T1657: Financial Theft**

- This technique has been observed in 14% of MTS cyber incidents in 2025 so far.

Mitigation Measures

CGCYBER recommends MTS partners implement the mitigations below which align with the joint cybersecurity advisory mitigations from the FBI, CISA, and foreign government agencies.

- **Implement application controls**
  - Allowlisting for remote access programs
- **Audit remote access tools on the network**
- **Review logs for execution of remote access software**
- **Require controls on remote access**
  - Only allow remote access to be used from within the network over approved solutions
- **Block inbound and outbound connections**
  - For common remote access ports and protocols at the network perimeter
- **Implement phishing resistant MFA such as FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based MFA.**
  - Only 37% of partners assessed by CGCYBER in 2024 used MFA and for around half of these, MFA was bypassed through phishing campaigns.
- **Strictly limit Remote Desktop Protocol (RDP) use**
- **Implement strong cloud security**
  - Enforce least privilege and Just-In-Time access control in addition to conditional access policies. To secure data in the cloud, encrypt data at rest and use role-based and attribute- based access control.
  - In 2024, CPTs observed multiple cloud environments allowing public access at the user level and granting full privileges to users or services. These findings allow for the manipulation of cloud resources to maintain persistence and exfiltrate data.
- **Maintain regular system backups**
  - CGCYBER observed a company with insufficient backups causing an inability to recover data after a ransomware attack.
- **Ensure proper network segmentation**
  - Improper network segmentation was CGCYBER's top finding in operational technology (OT) assessments from 2024.
- **Conduct user training to help identify phishing attempts**
  - Specifically, awareness of vishing and MFA push bombing used by threat actors.

Resources

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at **202-372-2904**.

Appendix A: IOCs

Scattered Spider IOCs

Tools
Fleetdeck.io
Level.io
Mimikatz
Ngrok
Pulseway
Screenconnect
Splashtop
Tactical.RMM
Tailscalre
TeamViewer
Teleport.sh
AnyDesk

Malware
AveMaria (WarZone)
Raccoon Stealer
VIDAR Stealer
RattyRAT
DragonForce Ransomware

Domains
targetsname-sso[.]com
targetsname-servicedesk[.]com
targetsname-okta[.]com
targetsname-cms[.]com
targetsname-helpdesk[.]com
oktalogin-targetcompany[.]com

References

"Scattered Spider" July 29, 2025. Scattered Spider | CISA

"2024 Cyber Trends and Insights in the Marine Environment" 2024 Cyber Trends in the Marine Environment

The information contained in this cyber alert is provided for **informational purposes only**. This information is based on common standards and best practices, and the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information.