SCATTERED SPIDER Escalates Attacks Across Industries | CrowdStrike

By Counter Adversary Operations

Archived: 2026-04-02 10:59:08 UTC

SCATTERED SPIDER, an eCrime adversary, has recently broadened its target scope to include the aviation sector, in addition to its established focus on the insurance and retail industries, as observed by CrowdStrike Services.

Throughout Q2 2025, SCATTERED SPIDER's activities have primarily centered on U.S.-based insurance and retail entities, along with U.K.-based retail entities. However, incidents in late June 2025, specifically targeting U.S.-based airlines, demonstrated tactics, techniques, and procedures (TTPs) consistent with the adversary's previous operations.

Overview of SCATTERED SPIDER TTPs

The adversary used help desk voice-based phishing in almost all observed 2025 incidents to compromise Microsoft Entra ID, single sign-on (SSO), and virtual desktop infrastructure (VDI) accounts. SCATTERED SPIDER operators routinely accurately respond to help desk verification questions when impersonating legitimate employees in calls made to request password and/or multifactor authentication (MFA) resets.

SCATTERED SPIDER typically pivots from compromised Entra ID, SSO, and VDI accounts to integrated software-as-a-service (SaaS) applications. They use access to these platforms to search for data that may enable lateral movement (such as network architecture diagrams, VPN instructions, or text files containing credentials), extortion, or other monetization activity.

Below are additional TTPs observed in recent SCATTERED SPIDER activity:

- Conducted Active Directory (AD) reconnaissance on on-premises systems using ADExplorer, ADRecon.ps1, and the Get-ADUser PowerShell (PS) cmdlet
- Used VMware vCenter access to create unmanaged virtual machines (VMs); the adversary often attaches domain controller virtual machine disks to their unmanaged VMs, then dumps the AD database ntds.dit on these systems
- Installed legitimate protocol-tunneling and proxy tools on VMware vCenter and adversary-controlled VMs, including Chisel (configured to communicate with trycloudflare[.]com subdomains), MobaXterm, ngrok, Pinggy, Rsocx, and Teleport
- Manually deleted (i.e., HardDelete, SoftDelete, and MoveToDeletedItems operations) and created transport rules (Set-TransportRule) to delete or redirect emails notifying users of suspicious account activity — in one case, the adversary created a mail transport rule to redirect emails intended for a compromised user to a likely adversary-controlled email address with the googlemail[.]com domain

- Used S3 Browser to enumerate victims' Amazon Web Services (AWS) S3 buckets (AWS CloudTrail events: ListBuckets and ListObjects) and exfiltrate data to remote adversary-controlled S3 buckets

SCATTERED SPIDER Assessment

SCATTERED SPIDER's primary goal is deploying ransomware to a victim's VMware ESXi infrastructure. If an incident is contained prior to ransomware deployment, the adversary often threatens to publicly leak stolen data and demands a ransom.

This adversary often targets several organizations within the same sector in a short time frame; however, they don't strictly follow this pattern. For example, CrowdStrike Services responded to one SCATTERED SPIDER incident targeting a retail entity during the same timeframe the adversary was predominantly targeting insurance entities.

Common attack methods for this adversary include:

- **Social Engineering**: Targeting IT help desk and privileged users through sophisticated phone-based attacks and impersonation
- **SIM Swapping and Phone-Based Credential Theft**: Compromising mobile phone accounts to bypass SMS-based MFA
- **Abuse of Legitimate Remote Access Tools**: Leveraging TeamViewer, AnyDesk, and similar tools for persistent access
- **VMware Infrastructure Compromise**: Targeting vCenter and ESXi environments for ransomware deployment
- **Cloud Environment Lateral Movement**: Exploiting cloud identity providers and moving laterally through cloud resources
- **Data Exfiltration**: Stealing sensitive data before deploying ransomware for double extortion

Common targets include:

- VMware vCenter and ESXi virtualization environments
- Cloud identity providers (Azure AD/Entra ID, AWS IAM, Google Cloud Identity, Okta)
- Privileged access management systems and administrative accounts
- VPN and remote access solutions
- Backup and recovery systems
- Help desk and IT support personnel

CrowdStrike Customers: Enable Falcon Platform Features

CrowdStrike customers can maximize detection capabilities, enhance visibility, and improve response times by deploying priority log sources, activating correlation rules, and integrating cloud security. All of these capabilities are available in the CrowdStrike Falcon® platform.

Falcon Next-Gen SIEM: Critical Log Source Integration

Endpoint customers will need to enable log ingestion connectors and the parser, so these logs can be ingested into CrowdStrike Falcon® Next-Gen SIEM to detect compromise.

Below are the highest priority logs to ingest into Falcon Next-Gen SIEM to detect SCATTERED SPIDER activity. For more detailed walkthroughs on Falcon Next-Gen SIEM log parsing, please refer to this blog.

Infrastructure Monitoring (Highest Priority)

- **VMware vCenter and ESXi**: Essential for detecting virtual infrastructure manipulation and unauthorized access
- **Firewall Logs**: Critical for identifying network-based attack patterns and lateral movement
- **DNS Logs**: Vital for detecting command-and-control communications and data exfiltration attempts
- **Web Proxy Logs**: Monitor for suspicious web traffic and potential data exfiltration

Identity and Authentication Systems

- **SSO Platforms**: Track authentication anomalies and suspicious login patterns
- **Entra ID Sign-on and Audit Logs**: Monitor for identity-based attacks and privilege escalation attempts
- **PAM Applications**: Detect unauthorized privileged access and credential misuse

Cloud and SaaS Applications

- **AWS CloudTrail, Google Cloud, Azure Activity Logs**: Monitor cloud resource manipulation and configuration changes
- **Critical SaaS Applications**: Monitor SaaS applications for application-level threat detection

Deploy Critical Correlation Rule Templates

Correlation rule templates (CRTs) are critical to increase monitoring and detection posture. Once logs have been ingested into Falcon Next-Gen SIEM, the following CRTs will help detect anomalous behavior.

VMware Infrastructure Protection

Essential rules for virtual environment security:

1. VMware - vCenter - Virtual Machine Created with Recently Uploaded ISO
2. VMware - vCenter - Sensitive Resource Search
3. VMware - ESXi - Successful Login to the ESXi Host Client Web Administration Interface
4. VMware - ESXi - New IP for SSH Login Detected
5. VMware - ESXi - SFTP Server Enabled

Entra ID Identity Protection

Critical Identity Security Rules:

1. Microsoft - Entra ID - Risky Sign-in
2. Microsoft - Entra ID - Admin Deleted MFA Authentication Method

3. Microsoft - Entra ID - Bulk Download User List
4. Microsoft - Entra ID - Temporary Access Pass Added to User Account
5. Microsoft - Entra ID - Global Administrator Role Assigned

Falcon Shield: Priority Integration Deployment

CrowdStrike Falcon® Shield is our cloud application security module that provides visibility and threat detection across SaaS and cloud platforms. CrowdStrike provides multiple High and Medium severity alerts out of the box, which are helpful for detecting these types of attacks.

Customers should also increase Falcon Shield integrations and detection capabilities for automated continuous detection. Integrations with the below list of applications should be prioritized.

Core SaaS Applications

- **Microsoft 365 Suite**: Exchange, SharePoint, OneDrive, Teams for comprehensive cloud application monitoring
- **Microsoft Defender**: Enhanced integration for security event correlation
- **Google Workspace**: Complete visibility into Google Cloud activities

Security Platform Integration

- **Enhanced Falcon Integration**: Maximize native CrowdStrike detection capabilities
- **Zscaler Cloud Security**: Monitor secure web gateway and cloud access security broker activities
- **CyberArk PAM**: Comprehensive privileged access monitoring and threat detection

Business-Critical Applications

- **Snowflake Data Platform**: Monitor for unauthorized data access and exfiltration attempts
- **Workday HR Systems**: Detect suspicious employee data access and modifications
- **GitHub Repositories**: Monitor code repository access and potential intellectual property theft
- **Confluence**: Monitor for suspicious query and searching activity
- **Salesforce**: Track suspicious activities in collaboration and CRM platforms

Falcon Cloud Security: Comprehensive Cloud Visibility

Registering cloud tenants into CrowdStrike Falcon® Cloud Security also allows for monitoring of suspicious activity and rogue cloud asset creation within cloud environments. Falcon Cloud Security enables real-time visibility of cloud management and authentication platforms including Entra ID, which allows for rapid correlation rule creation.

With Falcon Cloud Security enabled, it is recommended to deploy the VMware Asset Inventory Collector to all vCenter devices. This allows organizations to monitor for unmanaged and rogue virtual machine creation.

Cloud Tenant Registration

- Register all AWS, Azure, and Google Cloud tenants for real-time cloud management activity monitoring
- Enable automated alerting for suspicious cloud resource creation and configuration changes
- Implement continuous compliance monitoring across all cloud environments

VMware Asset Inventory Collector Deployment

- Deploy collectors to all vCenter devices for complete virtual infrastructure visibility
- Monitor for unmanaged and rogue virtual machine creation
- Track virtual infrastructure changes and detect unauthorized modifications
- Implement automated asset discovery and classification for comprehensive inventory management

Proactive Hardening and Monitoring Improvements

These are some of the proactive monitoring and employee best practices enterprises must enable to watch for attacks such as SCATTERED SPIDER.

Identity Protection

- Deploy phishing-resistant MFA (no SMS) and isolate privileged accounts
- Strengthen password reset processes and limit help desk MFA enrollment

Detection and Monitoring

- Track authentication anomalies, administrative actions, and network traffic to critical systems
- Enable comprehensive logging and behavioral analytics
- Monitor for anomalous application usage, suspicious search terms, and unusual data access patterns

Infrastructure Security

- Secure VMware environments, segment networks, and block unauthorized tools
- Apply least privilege in cloud environments and disable legacy authentication

Incident Readiness

- Maintain isolated backups, develop response playbooks, and conduct regular assessments
- Train IT/help desk staff on social engineering threats

Conclusion

This comprehensive approach leverages CrowdStrike Falcon platform capabilities while implementing fundamental security hardening measures to significantly reduce organizations' exposure to SCATTERED SPIDER and similar advanced threat actors. The Falcon platform's precise technical controls and robust security capabilities provide defense-in-depth against sophisticated social engineering and infrastructure compromise attacks.

Additional Resources

- *Check out this upcoming webinar: Advanced Threat Hunting to Track SCATTERED SPIDER: How to Hunt Sophisticated Adversaries in Third-Party Data*
- *SaaS Threat Simulation: Detecting and Stopping SCATTERED SPIDER*
- *Hands-on Workshop: From Login to Lockdown: Stop Identity Breaches from SCATTERED SPIDER*
- *Learn more about how Falcon Next-Gen SIEM protects enterprises from threat targeting VMWare VCenter.*
