INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-20 13:38 UTC

Scattered Spider Accountability Expands: Buchanan Guilty Plea Signals Sustained Law Enforcement Pressure on English-Speaking Cybercrime Networks

THREAT ACTOR | MEDIUM | CVSS 5.0

SCC Item ID	SCC-TAC-2026-0007
Type	Threat Actor
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Multiple sectors including entertainment, telecommunications, technology, BPO, IT, cloud communications, and virtual currency; named victims include MGM Resorts, Caesars, Riot Games, MailChimp, Twilio, DoorDash, Reddit, and Transport for London
Published	2026-04-20T09:33:42
Discovery Source	Rss

Executive Summary

Tyler Buchanan, an alleged leader of the Scattered Spider threat collective, pleaded guilty to wire fraud and aggravated identity theft charges in the US, facing up to 22 years in prison. This follows a 10-year sentence for co-conspirator Noah Urban and active UK prosecutions tied to attacks on Transport for London and major retailers. Despite these arrests, Scattered Spider continues operating, with newer members using the same social engineering and identity-based attack methods that have enabled over $115 million in reported ransom payments across entertainment, telecommunications, technology, and financial sectors.

Technical Analysis

Scattered Spider (also tracked as UNC3944, Octo Tempest, 0ktapus) is a loosely organized, English-speaking threat collective specializing in identity-based intrusion. Core techniques include SIM swapping (T1586.002), MFA fatigue and push bombing (T1621), spearphishing for credentials (T1598.003), and help desk social engineering to bypass authentication controls. The group exploits weak identity verification at IT support functions to register attacker-controlled devices or reset MFA, gaining valid account access (T1078) without exploiting software vulnerabilities. Post-access, they pivot using internal spearphishing (T1534), steal session

cookies (T1539), and have engaged in financial extortion (T1657). Underlying weaknesses map to CWE-287 (improper authentication), CWE-308 (insufficient MFA), and CWE-1390 (weak identity verification). No CVE is associated; the attack surface is procedural and identity-layer, not software-vulnerability-based. The group's decentralized structure has sustained operations through multiple arrests across two jurisdictions.

Action Checklist

1. Step 1: Containment. Audit help desk and IT support authentication workflows immediately. Suspend any callback or reset procedures that rely solely on caller-provided information (name, employee ID, last four of SSN). Require out-of-band identity verification (manager approval, video confirmation, or hardware token verification) before any MFA reset or SIM-linked account change.
2. Step 2: Detection. Review identity provider (IdP) logs (Okta, Azure AD, Ping) for anomalous MFA push sequences (10+ push attempts in under 5 minutes), out-of-hours MFA resets initiated by help desk accounts, new device enrollments immediately following a help desk ticket, and SIM swap events correlating with account access from new geographic locations. MITRE T1621 and T1586.002 are the primary indicators.
3. Step 3: Eradication. Enforce phishing-resistant MFA (FIDO2/WebAuthn hardware keys or passkeys) for all privileged accounts and remote access paths. Remove SMS and voice call as MFA factors for administrator and privileged user accounts. Require re-enrollment on hardware-bound authenticators for any account that completed a help desk reset in the past 90 days.
4. Step 4: Recovery. Validate that no attacker-registered devices remain enrolled in your IdP by auditing all device registrations completed within the past 90 days. Monitor for anomalous OAuth token issuance and session cookie reuse (T1539) post-remediation. Confirm SIM swap alert subscriptions are active with your mobile carrier for all corporate-liable devices.
5. Step 5: Post-Incident. Conduct a tabletop exercise simulating a help desk social engineering call targeting MFA reset. Assess whether current identity verification procedures would have stopped the attempt. Map gaps to NIST SP 800-63B identity assurance levels and update help desk runbooks to require IAL2-equivalent verification before any account recovery action. Document findings for GRC review.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if Okta or Azure AD logs confirm a successful help desk-initiated MFA reset followed by authentication from an unrecognized device or geolocation, or if any corporate-liable SIM swap is confirmed by the mobile carrier — both conditions indicate active Scattered Spider compromise and may trigger breach notification obligations under state PII laws or sector-specific regulations (e.g., FCC for telecom, GLBA for financial, FTC Safeguards Rule).

Recovery Notes	Post-containment, maintain elevated monitoring of all IdP authentication events for a minimum of 90 days given Scattered Spider's documented persistence through OAuth refresh token abuse (T1539) and attacker-registered device reuse after initial access is re-established. Revoke all active sessions and refresh tokens for accounts confirmed to have undergone a help desk reset during the exposure window, forcing full re-authentication on phishing-resistant MFA — do not assume session revocation alone is sufficient if device enrollment was also compromised. Verify SIM swap alert subscriptions are active and tested for all corporate-liable devices, and re-run IdP device enrollment audits at 30 and 60 days post-remediation to catch any delayed attacker-registered device activations.
Forensic Artifacts	Okta System Log entries for 'user.mfa.factor.deactivate' and 'user.mfa.factor.activate' event types — Scattered Spider's vishing workflow consistently triggers a help desk-initiated factor removal followed immediately by attacker-controlled factor enrollment, producing a detectable deactivate→activate sequence within minutes on the same account | Azure AD or Okta device enrollment records showing a new device registration from an IP address geolocation inconsistent with the account owner's historical sign-in pattern, occurring within 0–30 minutes of a help desk ticket closure — this is the attacker's post-social-engineering device registration footprint | Mobile carrier SIM swap event logs or number porting confirmation records for corporate-liable devices, time-correlated against IdP authentication events showing the account's MFA phone number changing to an attacker-controlled SIM (MITRE T1586.002) | OAuth refresh token grant logs in Azure AD or Okta showing 'offline_access' scope issuance from the compromised session — Scattered Spider leverages persistent refresh tokens to maintain access after password resets, making token audit logs a critical persistence indicator (MITRE T1539) | Help desk ticketing system records (ServiceNow, Zendesk, Jira Service Management) for all MFA reset, account unlock, and SIM change tickets in the past 90 days — cross-reference caller-provided identity fields against HR records to identify social engineering pretext patterns consistent with Scattered Spider's known use of OSINT-sourced employee PII from LinkedIn, corporate directories, and data broker sites

Per-Action IR Details

Step 1: Containment — Audit help desk and IT support authentication workflows immediately. Suspend any callback or reset procedures that rely solely on caller-provided information (name, employee ID, last four of SSN). Require out-of-band identity verification (manager approval, video confirmation, or hardware token verification) before any MFA reset or SIM-linked account change.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST IA-12 (Identity Proofing), NIST AC-2 (Account Management), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Immediately publish an emergency help desk policy memo halting all SMS/voice MFA resets until out-of-band verification is implemented. For teams with no helpdesk ticketing budget, create a mandatory verification form in Google Forms or Microsoft Forms requiring the requestor's manager email CC and a timestamped photo ID upload before any ticket is processed. Use a free Signal or Teams group channel to perform real-time video verification for high-privilege account resets.

Evidence: Before suspending reset procedures, capture the following: export all help desk tickets from the past 90 days involving MFA reset, SIM change, or account recovery requests; extract Okta System Log or Azure AD audit log entries for 'user.mfa.factor.deactivate' and 'user.mfa.factor.activate' events correlated with help desk ticket timestamps; pull call recording metadata (if available from your telephony platform) for inbound support calls exceeding 5 minutes that preceded a credential reset; document any caller-provided PII fields used to authenticate the request (these

represent Scattered Spider's social engineering pretext inputs per MITRE T1566.004 and T1586.002).

Step 2: Detection — Review identity provider (IdP) logs (Okta, Azure AD, Ping) for anomalous MFA push sequences (10+ push attempts in under 5 minutes), out-of-hours MFA resets initiated by help desk accounts, new device enrollments immediately following a help desk ticket, and SIM swap events correlating with account access from new geographic locations. MITRE T1621 and T1586.002 are the primary indicators.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a SIEM, use the Okta free-tier System Log export (Admin > Reports > System Log) and run the following PowerShell against the JSON export to flag MFA push storms: `Get-Content okta_log.json | ConvertFrom-Json | Where-Object { $_.eventType -eq 'user.mfa.attempt_bypass' -or $_.eventType -eq 'system.mfa.factor.deactivate' } | Group-Object { $_.actor.displayName } | Where-Object { $_.Count -gt 5 }`. For Azure AD without Sentinel, use Microsoft Entra ID's free Sign-in logs filtered on 'MFA result: MFA denied, user declined' to detect MFA fatigue push sequences (MITRE T1621). Deploy the free Sigma rule 'win_security_mfa_enumeration' adapted for Okta log fields to flag 10+ push attempts within a 5-minute window per actor.

Evidence: Collect before analysis: Okta System Log JSON export filtered on event types 'user.mfa.factor.deactivate', 'user.mfa.factor.activate', 'user.session.start' with 'authenticationContext.credentialType: PASSWORD' from a new IP; Azure AD Sign-in logs for 'Interrupted' sign-in status with MFA method 'Phone call' or 'SMS' immediately followed by a successful authentication from a new country; mobile carrier SIM swap notification logs or customer portal change history for corporate-liable device numbers; Okta ThreatInsight or Azure AD Identity Protection risk event logs flagging 'unfamiliar sign-in properties' or 'impossible travel' correlated within 24 hours of a help desk ticket.

Step 3: Eradication — Enforce phishing-resistant MFA (FIDO2/WebAuthn hardware keys or passkeys) for all privileged accounts and remote access paths. Remove SMS and voice call as MFA factors for administrator and privileged user accounts. Require re-enrollment on hardware-bound authenticators for any account that completed a help desk reset in the past 90 days.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST IA-2 (Identification and Authentication — Organizational Users), NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams that cannot immediately procure FIDO2 hardware keys, use Google's free Titan Security Key pilot program or distribute passkeys via Apple iCloud Keychain or Windows Hello (free, built-in) as an interim phishing-resistant factor. In Okta, navigate to Security > Authenticators and set 'Phone' and 'SMS' authenticator status to 'Disabled' for the 'Privileged Users' group policy — this is a configuration change, not a purchase. In Azure AD, use Conditional Access (free with Azure AD P1) to block legacy authentication and require FIDO2 or Windows Hello for Business for all accounts in the 'Global Administrators' and 'Privileged Role Administrators' roles.

Evidence: Before removing SMS/voice factors, capture: full export of all accounts still enrolled with SMS or voice as their only MFA factor (Okta Admin > Reports > Users by Factor Type; Azure AD: `Get-MgUserAuthenticationMethod` via Microsoft Graph PowerShell); list of all privileged accounts (Global Admin, Help Desk Admin, User Admin roles) cross-referenced against accounts that had a help desk-initiated factor reset in the past 90 days — this is your Scattered Spider high-risk population; Okta or Azure AD audit log entries showing 'factor enrolled' events for the re-enrollment campaign as a before/after baseline.

Step 4: Recovery — Validate that no attacker-registered devices remain enrolled in your IdP by auditing all device registrations completed within the past 90 days. Monitor for anomalous OAuth token issuance and session cookie reuse (T1539) post-remediation. Confirm SIM swap alert subscriptions are active with your mobile carrier for all corporate-liable devices.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AU-11 (Audit Record Retention), NIST IR-4 (Incident Handling), NIST SC-23 (Session Authenticity), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run the following Microsoft Graph PowerShell command to enumerate all device registrations in the past 90 days: `Get-MgDevice | Where-Object { $_.RegistrationDateTime -gt (Get-Date).AddDays(-90) } | Select-Object DisplayName, RegistrationDateTime, OperatingSystem, TrustType | Export-Csv suspicious_devices.csv`. For Okta, use the System Log query `eventType eq 'device.enrollment.create' AND published gt "2025-12-01T00:00:00Z"` in the Okta System Log API. To detect OAuth token abuse (T1539) without a SIEM, review Okta's Token Lifetime report and flag any refresh tokens with lifetimes exceeding your policy, or use Microsoft's free Entra ID Sign-in logs filtered on 'Token issuance policy' anomalies. Contact your mobile carrier's business account team to enroll in their free SIM swap notification API or alert service (AT&T, Verizon, and T-Mobile all offer these for business accounts at no cost).

Evidence: Capture before and during recovery validation: Okta or Azure AD device registration logs for the past 90 days — flag any device registered from an IP geolocation inconsistent with the account owner's normal work location; OAuth token grant logs showing 'offline_access' scope grants (enabling persistent refresh tokens) issued during the suspected compromise window; Conditional Access or Okta sign-on policy logs showing authentication from new device + new location combinations that succeeded during the 90-day window; mobile carrier account change logs for corporate-liable SIM swap events, porting requests, or account PIN changes correlated with the incident timeline.

Step 5: Post-Incident — Conduct a tabletop exercise simulating a help desk social engineering call targeting MFA reset. Assess whether current identity verification procedures would have stopped the attempt. Map gaps to NIST SP 800-63B identity assurance levels and update help desk runbooks to require IAL2-equivalent verification before any account recovery action. Document findings for GRC review.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (Lessons Learned)

Controls: NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST IR-8 (Incident Response Plan), NIST IA-12 (Identity Proofing), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Use the free CISA Tabletop Exercise Package (CTEP) framework as your exercise scaffold — no commercial tool required. Script the tabletop scenario specifically around a Scattered Spider-style vishing call: caller claims to be a remote employee locked out of Okta before a critical deadline, provides name, employee ID, and partial SSN, and requests an SMS MFA reset. Run the scenario against your actual help desk team with a neutral observer scoring whether current runbook steps would have stopped the reset. Document gaps using a free NIST SP 800-63B IAL2 checklist (available at pages.nist.gov/800-63-4) and capture findings in a GRC ticketing item mapped to NIST IR-8 plan update requirements.

Evidence: Document for GRC and lessons learned: all help desk tickets from the past 12 months involving MFA reset, account unlock, or SIM change requests — annotate which verification method was used for each; a gap analysis comparing your current help desk identity verification procedure against NIST SP 800-63B IAL2 requirements (government-issued photo ID + biometric or supervised remote identity proofing); tabletop exercise scoring sheet with specific decision points where the simulated Scattered Spider vishing attempt would have succeeded under pre-incident procedures; updated help desk runbook version with change log entry citing this incident review as the trigger.

Detection Guidance

Focus detection on the identity and authentication layer, not the network perimeter. Key log sources: Okta System Log, Azure AD Sign-In and Audit Logs, Duo Admin Panel, and telecom carrier SIM change alerts. Behavioral indicators: (1) MFA push floods, more than 5 push requests to a single account within 10 minutes, especially outside business hours (T1621); (2) help desk tickets followed within 30 minutes by a new device

enrollment or MFA factor change on the same account; (3) account logins from a new IP or country within 1 hour of a completed help desk reset; (4) SIM swap events on corporate-liable numbers correlating with subsequent account access (T1586.002); (5) internal phishing messages originating from a recently compromised internal account (T1534). SIEM query logic should correlate help desk ticket creation timestamps against IdP device enrollment and MFA change events for the same user. No public IOC list (IPs, domains, hashes) is reliably current for this collective given its social-engineering-first methodology; behavioral patterns are the primary detection surface.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No current, verified IOC list available`	Scattered Spider relies on social engineering and legitimate identity provider features rather than fixed infrastructure. Published IOC lists for this group go stale rapidly. CISA Advisory AA23-243A (released September 2023) contains the most authoritative published TTPs; organizations should reference that advisory directly for any historical indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1598.003** — Spearphishing Link
- **T1598** — Phishing for Information
- **T1586.002** — Email Accounts
- **T1621** — Multi-Factor Authentication Request Generation
- **T1657** — Financial Theft
- **T1566** — Phishing
- **T1556** — Modify Authentication Process
- **T1539** — Steal Web Session Cookie
- **T1586** — Compromise Accounts
- **T1078** — Valid Accounts
- **T1534** — Internal Spearphishing

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1598.003	Spearphishing Link	Reconnaissance
T1598	Phishing for Information	Reconnaissance
T1586.002	Email Accounts	Resource-Development
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1657	Financial Theft	Impact
T1566	Phishing	Initial-Access
T1556	Modify Authentication Process	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1586	Compromise Accounts	Resource-Development

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1534	Internal Spearphishing	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/british-scattered-sp...	T3
	https://www.bleepingcomputer.com/news/security/british-scattered-sp...	T3
	https://www.bleepingcomputer.com/news/security/scattered-spider-tee...	T3
	https://www.bleepingcomputer.com/news/security/scattered-spider-hac...	T3
[Dark Reading] MGM / Caesars hack started with social engineering ...	https://www.reddit.com/r/cybersecurity/comments/16k4u7g/dark_readin...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-20 13:38 UTC by TJS Security Command Center