INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-30 19:01 UTC

Cyber-Enabled Cargo Theft Surges 60%: Phishing and Account Takeover Drive $725M in Freight Losses

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0244
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Freight broker and carrier platforms, online load boards (e.g., DAT, Truckstop), FMCSA carrier registration systems; no specific software vendors named
Published	2026-04-30T12:32:18
Discovery Source	Rss

Executive Summary

Threat actors are compromising freight broker and carrier accounts through phishing and credential theft, then using those accounts to divert physical shipments. Law enforcement and industry sources report this as a structured pattern of activity, with estimated cargo losses in the U.S. and Canadian freight industries reported at approximately $725 million in 2025, representing a significant year-over-year increase. Any organization that books, brokers, or manages freight through digital load boards or carrier platforms faces direct exposure to financial loss, supply chain disruption, and liability for diverted goods.

Technical Analysis

The campaign chains cyber intrusion with physical logistics fraud across two phases. In the cyber phase, threat actors use spear-phishing (T1566, T1566.002) and credential theft to compromise freight broker and carrier accounts on platforms such as DAT and Truckstop, and exploit weak or missing authentication in FMCSA carrier registration workflows. In the physical phase, they impersonate legitimate carriers (T1036, T1656) to accept loads, then divert shipments. Established accounts are purchased or compromised via account takeover (T1078, T1586), and fraudulent accounts are created to expand operational capacity (T1585, T1585.001). Relevant weaknesses include CWE-287 (improper authentication), CWE-306 (missing authentication for critical functions in FMCSA workflows), and CWE-1021 (UI redressing or spoofing to deceive platform users). No CVE identifiers have been published. No vendor patches are available; the attack surface spans platform authentication controls, carrier verification workflows, and load board vetting processes. Specific threat actor

groups have not been publicly identified by law enforcement.

Action Checklist

1. Step 1: Containment. Audit active freight broker and carrier accounts on DAT, Truckstop, and any internal load board integrations. Suspend accounts showing login anomalies (unexpected geolocation, new device, off-hours access). Require re-authentication for any account that has accepted or posted loads in the past 30 days.
2. Step 2: Detection. Request activity logs from freight platforms (DAT, Truckstop, etc.) for your accounts, focusing on new logins, new carrier onboarding, and load activity. Cross-reference carrier MC/DOT numbers in these logs against FMCSA SAFER database records in real time. Review internal email gateway and VPN logs for phishing attempts targeting freight platform users. Flag any carrier whose FMCSA registration date is under 90 days old yet immediately accepts high-value loads.
3. Step 3: Eradication. Enforce multi-factor authentication on all freight broker and carrier portal accounts where the platform supports it. Remove saved credentials from shared or unmanaged workstations used by dispatch or operations staff. For high-value loads, verify carrier identity through direct callback to the phone number registered with FMCSA (not the number provided in the load tender). Implement programmatic FMCSA SAFER database API lookups where available to automate this cross-reference.
4. Step 4: Recovery. Confirm that all active loads in transit are assigned to verified carriers whose FMCSA records match the tendering documentation. Monitor shipment tracking for route deviations or unexpected handoffs. After account compromise, rotate all credentials and review load history for the prior 60 days for unauthorized activity.
5. Step 5: Post-Incident. Conduct a gap assessment against carrier vetting procedures, focusing on FMCSA verification integration, multi-factor authentication coverage, and employee phishing awareness for dispatch and operations roles. Document findings and update vendor onboarding checklists to require identity verification steps that cannot be satisfied by email alone.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and the FBI's Internet Crime Complaint Center (IC3) if any active in-transit load is confirmed or suspected to be in the possession of an adversary-controlled carrier, if financial payments have been disbursed to fraudulent carrier accounts, or if the organization lacks the internal capability to freeze compromised load board accounts within four hours of detection.
Recovery Notes	After containment, verify every active load in transit against FMCSA records before releasing payment to any carrier whose account showed login anomalies — payment misdirection is the primary financial harm vector in this campaign. Monitor load board accounts and TMS activity for a minimum of 90 days post-incident, as adversary groups conducting freight fraud frequently re-register under new MC numbers after initial detection and return to target the same brokers. Coordinate with your load board platform's fraud team (DAT and Truckstop both maintain internal fraud reporting channels) to flag adversary-associated MC/DOT numbers and email addresses for platform-wide blocking.

Forensic Artifacts	Load board login event logs from DAT, Truckstop, or internal TMS portals showing the authentication sequence — specifically the credential stuffing pattern of failed logins followed by successful logins from new IPs or device fingerprints, which is the adversary's initial access method in this campaign. | FMCSA SAFER query records and comparison documentation showing discrepancies between the carrier identity presented in load tenders and the legal name, phone number, and business address on file with FMCSA — the primary indicator of a cloned or fictitious carrier entity. | Phishing email samples preserved as .eml files with full SMTP headers, identifying the adversary's sending infrastructure (domain registrar, hosting IP, spoofed brand), relevant to FBI IC3 reporting and platform-level blocking on DAT/Truckstop. | TMS and load board payment records showing any ACH routing number or check mailing address changes made on carrier accounts within 30 days of a flagged login event — direct evidence of the financial fraud component of this campaign. | Windows Credential Manager exports and browser credential store contents from shared dispatch workstations, establishing which load board portal credentials were stored in recoverable form and were therefore accessible to adversaries who gained physical or remote access to dispatch systems.

Per-Action IR Details

Step 1: Containment — Audit active freight broker and carrier accounts on DAT, Truckstop, and any internal load board integrations. Suspend accounts showing login anomalies (unexpected geolocation, new device, off-hours access). Require re-authentication for any account that has accepted or posted loads in the past 30 days.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Export account activity logs from DAT and Truckstop portals via their admin or reporting interfaces (CSV/XLSX). Use a two-person manual review: one analyst cross-references login IP geolocation against known dispatcher office IPs using a free tool such as ip-api.com batch lookup; the second flags any account with a login country mismatch or device fingerprint change within the past 30 days. Suspend flagged accounts via the platform admin console and force a password reset email to the registered address on file — not any address supplied in a recent support ticket or load tender.

Evidence: Before suspending accounts, capture and preserve: (1) Full login history exports from DAT, Truckstop, and any internal TMS (Transportation Management System) portal for the prior 30 days, noting source IP, device user-agent string, and timestamp. (2) Any load acceptance or posting events tied to flagged accounts, including carrier MC/DOT numbers associated with accepted loads. (3) Email headers from phishing lures if reported by dispatch staff, preserving the original .eml file with full Received headers to identify adversary infrastructure. (4) Browser session cookies or saved credential stores on shared dispatch workstations, which may contain stolen session tokens used to bypass password authentication on load board portals.

Step 2: Detection — Query identity and access management logs for failed logins followed by successful logins from new IPs or devices on freight platform accounts. Review load board activity logs for newly onboarded carriers with FMCSA registration dates under 90 days. Flag any carrier whose MC number or DOT number does not match FMCSA records in real time.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell to parse exported DAT/Truckstop login CSV logs: group by username, sort by timestamp, and flag any account where a failed login attempt (status='FAIL') is followed within 10 minutes by a successful login (status='SUCCESS') from a different IP address. Command template: `Import-Csv login_export.csv | Group-Object Username | ForEach-Object { $_.Group | Sort-Object Timestamp } | Where-Object { }`. For FMCSA carrier verification, query the FMCSA SAFER system API (free, public) at https://safer.fmcsa.dot.gov/query.asp using the MC or DOT number from the load tender and compare the legal name and phone number fields against what the carrier provided. Flag any discrepancy for manual callback.

Evidence: Before concluding detection sweep: (1) Preserve raw IAM/SSO log exports showing authentication event sequences — specifically the pattern of credential stuffing: multiple failed attempts across many accounts from a single IP range, consistent with automated attack tooling used in freight account takeover campaigns. (2) Capture load board onboarding records for any carrier created within the past 90 days that has accepted loads, including the email address, phone number, and bank account or payment details provided at registration — these are the adversary's data points. (3) Pull FMCSA SAFER query results and compare the FMCSA-registered business address and phone against what appears in the load tender; document any delta as an IOC. (4) If phishing is suspected, query email gateway logs for messages originating from domains spoofing DAT, Truckstop, or known freight broker brands, including lookalike domains (e.g., dat-loadboard[.]com, truckstop-login[.]net).

Step 3: Eradication — Enforce MFA on all freight broker and carrier portal accounts where the platform supports it. Remove saved credentials from shared or unmanaged workstations used by dispatch or operations staff. Verify carrier identity through direct callback to the phone number on file with FMCSA, not the number provided in the load tender.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For shared dispatch workstations without enterprise credential management: run the following to remove stored browser credentials on Windows — open Credential Manager (`control /name Microsoft.CredentialManager`) and delete any entries for DAT, Truckstop, or TMS portal URLs. For Chrome-based browsers, navigate to `chrome://settings/passwords` and remove saved entries, or use the CLI: `sqlite3 '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data' 'DELETE FROM logins WHERE origin_url LIKE "%dat.com%" OR origin_url LIKE "%truckstop.com%";'`. Where MFA is not natively supported by a load board portal, implement application-level access controls by restricting portal access to a fixed list of egress IP addresses using the platform's IP allowlist feature (available in DAT enterprise accounts).

Evidence: Before eradicating saved credentials, image or export the credential store from affected workstations to document which platform accounts were stored in plaintext or browser storage — this establishes the adversary's likely access vector and scope. Specifically preserve: (1) Windows Credential Manager exports (`cmdkey /list`) from dispatch workstations. (2) Browser local storage and cookie files (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies`) to identify any active stolen session tokens for load board portals. (3) A full list of carriers whose identity was verified only by the phone number or email supplied in the load tender (not cross-referenced to FMCSA) — these represent loads at risk of physical diversion and must be prioritized for Step 4 transit verification.

Step 4: Recovery — Confirm that all active loads in transit are assigned to verified carriers whose FMCSA records match the tendering documentation. Monitor shipment tracking for route deviations or unexpected handoffs. After account compromise, rotate all credentials and review load history for the prior 60 days for unauthorized activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-11 (Audit Record Retention), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without automated shipment visibility platforms: build a manual verification spreadsheet mapping every active load's PRO number or load ID to the carrier MC/DOT, driver name, truck plate, and scheduled delivery window. Cross-reference each MC/DOT against FMCSA SAFER in real time. For route deviation detection without GPS telematics, establish a direct phone contact cadence with the consignee at each delivery stop — if the carrier or driver cannot be reached at the scheduled check-in, treat it as a potential diversion event and escalate immediately. For the 60-day load history review, export all load acceptance records from the TMS and flag any load assigned to a carrier whose FMCSA registration date is under 90 days or whose payment destination changed after initial tender.

Evidence: Before closing out active loads and rotating credentials: (1) Preserve TMS and load board records for every load accepted under any compromised account during the past 60 days, including carrier MC/DOT, pickup/delivery addresses, and payment disbursement records — these are the primary evidence set if cargo theft is confirmed and law enforcement (FBI, cargo theft task forces) becomes involved. (2) Capture any ELD (Electronic Logging Device) or GPS tracking data showing the actual route taken versus the contracted route for loads assigned to unverified carriers. (3) Document payment records: adversary-controlled carriers frequently redirect broker payments via ACH or check to fraudulent accounts — preserve any payment routing changes made within 30 days of a flagged login event as potential financial fraud evidence.

Step 5: Post-Incident — Conduct a gap assessment against carrier vetting procedures, focusing on FMCSA verification integration, multi-factor authentication coverage, and employee phishing awareness for dispatch and operations roles. Document findings and update vendor onboarding checklists to require identity verification steps that cannot be satisfied by email alone.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-5 (Vulnerability Monitoring and Scanning), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Conduct a tabletop exercise specific to this threat vector: simulate a freight broker receiving a load tender from a carrier whose MC number has been cloned by an adversary. Walk dispatch and operations staff through the FMCSA SAFER callback verification procedure step by step. Use the FBI's IC3 and the National Cargo Theft Task Force (NCTTF) advisories as training reference material — both are freely available. For phishing simulation without a commercial platform, send a controlled internal test email mimicking a DAT or Truckstop login prompt to dispatch staff and measure click rates; use GoPhish (open source) for low-cost delivery. Update the carrier onboarding checklist to require a video call identity verification step and physical document upload (operating authority certificate) that cannot be spoofed by email alone.

Evidence: Compile the following artifacts into a post-incident report for lessons learned and regulatory notification review: (1) A timeline of the compromise — first malicious login, first fraudulent load acceptance, and first confirmed diversion — sourced from preserved TMS and load board logs. (2) A list of all carriers vetted solely by email during the incident window, flagged for shipper and consignee notification where cargo may have been diverted. (3) The phishing lure samples and sending infrastructure details (domain, IP, mail headers) submitted to CISA's phishing reporting portal and the FBI's IC3 for threat intelligence sharing. (4) Documentation of any financial payments made to adversary-controlled carrier accounts, required for potential FBI referral and for the organization's cyber insurance claim.

Detection Guidance

Monitor identity and access management logs for the following behavioral patterns: (1) successful logins to freight platform accounts from IP addresses not previously associated with that account, particularly in rapid succession following failed attempts; (2) new carrier accounts created within 90 days of FMCSA registration that immediately begin accepting high-value loads; (3) load tenders accepted by carriers whose contact phone numbers differ from FMCSA-registered numbers. Cross-reference carrier MC and DOT numbers against the

FMCSA SAFER database in real time. Flag discrepancies between the tendering carrier identity and the driver or equipment that appears at pickup. MITRE techniques to hunt for include T1078 (valid account abuse), T1036 (masquerading), and T1566 (phishing) in email gateway logs and freight platform activity logs. No public IOC list has been released by law enforcement at this time.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No public IOCs released`	The FBI has not published specific indicators of compromise for this campaign as of the available reporting. Monitor FBI IC3 and CISA for future releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1585.001** — Social Media Accounts
- **T1078** — Valid Accounts
- **T1656** — Impersonation
- **T1036** — Masquerading
- **T1565** — Data Manipulation
- **T1566.002** — Spearphishing Link
- **T1585** — Establish Accounts
- **T1586** — Compromise Accounts
- **T1566** — Phishing
- **T1219** — Remote Access Tools
- **T1534** — Internal Spearphishing
- **T1133** — External Remote Services

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection

- **CA-7** — Continuous Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **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
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1585.001	Social Media Accounts	Resource-Development
T1078	Valid Accounts	Defense-Evasion
T1656	Impersonation	Defense-Evasion
T1036	Masquerading	Defense-Evasion
T1565	Data Manipulation	Impact
T1566.002	Spearphishing Link	Initial-Access
T1585	Establish Accounts	Resource-Development
T1586	Compromise Accounts	Resource-Development
T1566	Phishing	Initial-Access
T1219	Remote Access Tools	Command-And-Control

Technique ID	Technique Name	Tactic
T1534	Internal Spearphishing	Lateral-Movement
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fbi-links-cybercrimi...	T3
	https://www.bleepingcomputer.com/news/security/fbi-links-cybercrimi...	T3
	https://www.bleepingcomputer.com/news/security/romanian-leader-of-o...	T3
89 Agents. 1.67 Million Carriers. A Broken System. There is a federal ...	https://www.facebook.com/61576097801435/posts/89-agents-167-million...	T3
Criminals are posing as trucking companies to hack into freight ...	https://www.facebook.com/NEWSMAX/posts/criminals-are-posing-as-truc...	T3

Generated 2026-04-30 19:01 UTC by TJS Security Command Center