INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 13:36 UTC

Dragonforce Ransomware Group Claims Attack on UK Production Studio Ink

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0171
Type	Data Breach
Severity	HIGH
Affected Products	Ink (UK-based production studio, London)
Published	2026-06-14
Discovery Source	Gemini

Executive Summary

The DragonForce ransomware group has claimed a cyberattack on Ink, a London-based production studio, via its dark web leak site. The claim follows DragonForce's established double-extortion model, suggesting data was both encrypted and exfiltrated, with potential exposure of internal documentation, contractor information, software assets, and business correspondence. For organizations in the creative and media sector, this incident signals active targeting by a capable RaaS operation and highlights the risk of operational disruption and sensitive data exposure.

Technical Analysis

DragonForce is a ransomware-as-a-service operation active since at least 2023. The group employs a double-extortion model: encrypting victim files to disrupt operations while exfiltrating data to a dark web leak site to pressure payment. No CVE, specific exploitation vector, or technical indicators of compromise have been publicly disclosed for this incident. The MITRE ATT&CK techniques associated with this claim are: T1486 (Data Encrypted for Impact), T1041 (Exfiltration Over C2 Channel), T1114 (Email Collection), T1078 (Valid Accounts), and T1657 (Financial Theft, extortion payment demand). No CVSS score or CWE applies, this is a claimed breach, not a disclosed software vulnerability. The source material confirms the dark web listing but does not provide forensic detail; no patch, vendor advisory, or confirmed technical vector is available at this time.

Action Checklist

1. Step 1: Containment, If Ink is a vendor, partner, or contractor in your supply chain, immediately review shared access, credentials, and data exchange agreements. Revoke or suspend any active integrations or

shared accounts pending confirmation of scope (NIST AC-2: Account Management; CIS 6.2: Establish an Access Revoking Process).

2. Step 2: Detection, Review logs for anomalous outbound data transfers, unexpected archive creation, or email collection activity consistent with T1041, T1114, and T1078. Audit authentication logs for use of valid accounts at unusual hours or from unusual locations. Check endpoint and EDR telemetry for encryption activity consistent with T1486 (NIST AU-6: Audit Record Review, Analysis, and Reporting; CIS 8.2: Collect Audit Logs).

3. Step 3: Eradication, No patch or specific remediation vector has been disclosed. For your own environment, enforce MFA on all externally exposed and administrative accounts to reduce risk from valid account abuse (T1078) (CIS 6.3: Require MFA for Externally-Exposed Applications; CIS 6.5: Require MFA for Administrative Access; D3-MFA: Multi-factor Authentication).

4. Step 4: Recovery, Verify integrity of backup systems and confirm backups are isolated from primary network segments. Validate that no lateral movement or credential exposure has occurred across connected systems. Monitor dark web sources for publication of data attributed to Ink that may include your organization's information (NIST AU-9: Protection of Audit Information; NIST CP controls apply for backup validation).

5. Step 5: Post-Incident, Review third-party vendor risk assessments for creative and media sector partners. Confirm that vendor access is governed by least-privilege principles and that access is revoked promptly when engagements end. Assess whether email and document-handling controls adequately limit exfiltration pathways consistent with T1114 and T1041 (NIST AC-6: Least Privilege; CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP: User Account Permissions).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and data protection officer if logs confirm that data shared with Ink (including any PII of employees, contractors, or clients) appears in DragonForce's published leak set, or if any internal accounts show authentication activity consistent with lateral movement originating from Ink-connected access paths, triggering UK GDPR Article 33 breach notification obligations to the ICO within 72 hours.
Recovery Notes	Post-containment, prioritize confirming that VSS shadow copies and offline backups are intact and have not been accessed by Ink-associated accounts or any accounts exhibiting lateral movement indicators — DragonForce affiliates routinely target backup infrastructure to eliminate recovery options before deploying the encryptor. Monitor your organization's name and any shared project identifiers against DragonForce's dark web leak site for a minimum of 90 days, as double-extortion operators typically release data in tranches to maintain pressure. Revalidate all third-party access grants for creative and media sector partners within 30 days, prioritizing any vendors who shared network access, cloud storage, or email threads with Ink on active projects.

Forensic Artifacts	Windows Security Event Log — Event IDs 4624, 4648, 4672, 4776 on systems accessible by Ink-associated accounts, specifically filtering for logon type 3 (network) and type 10 (RemoteInteractive) from non-corporate source IPs, which would indicate credential use following a compromise at Ink | File system metadata and MFT records for recently created archive files (.zip, .7z, .rar, .tar.gz) in user temp directories, ProgramData, and any shared project folders — DragonForce affiliates compress and stage data prior to exfiltration, leaving $MFT and $LogFile entries that persist even after archive deletion \| VSS shadow copy inventory via 'vssadmin list shadows' — absence of expected shadow copies or tampered VSS metadata indicates DragonForce's pre-encryption shadow deletion activity (commonly executed via 'vssadmin delete shadows /all /quiet') and is a high-confidence indicator of ransomware deployment on a connected host \| Email server auto-forward and delegation rules — export all mailbox forwarding rules via 'Get-InboxRule -Mailbox * \| Where-Object {$_.ForwardTo -ne $null -or $_.RedirectTo -ne $null}' (Exchange/M365) to detect T1114 persistence rules that DragonForce affiliates configure to maintain email collection after initial credential use | Outbound proxy or firewall logs filtered for connections to Mega.nz, Dropbox API endpoints, or Tor exit nodes from internal hosts during the 14-day window preceding the DragonForce claim date — these represent the exfiltration channel most consistent with DragonForce's documented RaaS affiliate TTPs and would confirm whether your environment was a secondary target or data relay point

Per-Action IR Details

Step 1: Containment — If Ink is a vendor, partner, or contractor in your supply chain, immediately review shared access, credentials, and data exchange agreements. Revoke or suspend any active integrations or shared accounts pending confirmation of scope (NIST AC-2: Account Management; CIS 6.2: Establish an Access Revoking Process).

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export all active accounts with Ink-associated email domains or API tokens using 'Get-ADUser -Filter {EmailAddress -like "*ink*"} | Select Name,SamAccountName,Enabled' (AD) or 'az ad user list --query "[?contains(mail,\'ink\')]"\' (Azure). Manually disable each account and document revocation timestamp. For shared API keys or webhook tokens issued to Ink, enumerate them via your application's admin console and rotate immediately. Two-person team can complete enumeration and revocation in under two hours with a shared checklist.

Evidence: Before revoking any shared accounts or API tokens, capture: (1) current active session records from your IdP or VPN logs showing Ink-associated accounts — export to CSV with timestamps; (2) recent authentication events for those accounts from Windows Security Event Log Event ID 4624 (successful logon) and 4648 (logon using explicit credentials); (3) any active file-share or cloud storage access logs showing Ink accounts accessing your data repositories within the last 30 days. DragonForce double-extortion operators typically stage exfiltrated data before encryption — preserve these logs to establish whether data egress preceded the claimed attack date.

Step 2: Detection — Review logs for anomalous outbound data transfers, unexpected archive creation, or email collection activity consistent with T1041, T1114, and T1078. Audit authentication logs for use of valid accounts at unusual hours or from unusual locations. Check endpoint and EDR telemetry for encryption activity consistent with T1486 (NIST AU-6: Audit Record Review, Analysis, and Reporting; CIS 8.2: Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM: (1) Run 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.TimeCreated -gt (Get-Date).AddDays(-30)}' and filter for logon type 3 (network) or 10 (remote interactive) from non-standard source IPs, especially outside business hours. (2) Use Sysmon Event ID 11 (FileCreate) filtered on .zip, .7z, .rar, .tar.gz creation in temp or user-profile directories — DragonForce affiliates commonly stage archives prior to exfil. (3) Run 'netstat -ano' and cross-reference established outbound connections against known DragonForce C2 infrastructure using AbuseIPDB or Shodan CLI lookups on each external IP. (4) Check Outlook OST/PST modification timestamps and mail export folder creation as indicators of T1114 mailbox collection.

Evidence: This is a detection/analysis step — capture and preserve before any remediation action: (1) Windows Security Event Log — Event ID 4624, 4648, 4672 (special privileges assigned) for all accounts, specifically filtering on Ink-associated accounts or any accounts with access to shared creative assets or project files; (2) file system metadata for recently created archive files (.zip, .7z, .rar) in staging paths such as C:\Users*\AppData\Local\Temp\ or C:\ProgramData\ — DragonForce affiliates commonly compress data prior to exfiltration; (3) DNS query logs or proxy logs for outbound connections to Mega.nz, Dropbox, or other cloud storage services, which DragonForce has used for exfiltration staging; (4) email server Send logs and mailbox export records to detect T1114 collection before the ransomware deployment phase.

Step 3: Eradication — No patch or specific remediation vector has been disclosed. For your own environment, enforce MFA on all externally exposed and administrative accounts to reduce risk from valid account abuse (T1078) (CIS 6.3: Require MFA for Externally-Exposed Applications; CIS 6.5: Require MFA for Administrative Access; D3-MFA: Multi-factor Authentication).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AC-7 (Unsuccessful Logon Attempts)

Compensating: For organizations without enterprise identity platforms: enable MFA on Microsoft 365 or Google Workspace admin consoles at no additional cost (both include built-in MFA). For VPN, enable TOTP-based MFA via FreeRADIUS + Google Authenticator if no commercial MFA solution exists. Audit all externally exposed services using 'nmap -sV --open -p 443,3389,22,8080,8443 ' to enumerate exposed authentication surfaces — DragonForce affiliates have leveraged exposed RDP and VPN portals as initial access vectors. Disable any accounts not yet MFA-enrolled before re-enabling external access.

Evidence: Before enforcing MFA policy changes that may terminate active sessions or lock accounts: capture (1) current list of all accounts without MFA enrollment from your IdP (e.g., 'Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}' for Azure AD); (2) active authenticated sessions for admin accounts — export from Azure AD Sign-In logs or on-prem IIS/VPN logs; (3) Windows Security Event ID 4672 (special privilege logon) for the prior 30 days to identify any privileged account use that may have preceded this step and warrants investigation. DragonForce affiliates rely on valid account abuse (T1078) as a persistence mechanism — document all privileged sessions before policy enforcement to preserve forensic chain of custody.

Step 4: Recovery — Verify integrity of backup systems and confirm backups are isolated from primary network segments. Validate that no lateral movement or credential exposure has occurred across connected systems. Monitor dark web sources for publication of data attributed to Ink that may include your organization's information (NIST AU-9: Protection of Audit Information; NIST CP controls apply for backup validation).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AC-4 (Information Flow Enforcement), CIS 3.4 (Enforce Data Retention)

Compensating: Verify backup isolation without enterprise backup tooling: (1) Confirm backup hosts have no active inbound network connections from primary subnets using 'netstat -ano' on the backup server and cross-referencing

against your network diagram; (2) hash-verify a sample of recent backup archives using 'Get-FileHash -Algorithm SHA256 ' and compare against stored manifest hashes — DragonForce affiliates have been observed targeting and corrupting VSS snapshots, so also run 'vssadmin list shadows' to confirm shadow copies are intact; (3) for dark web monitoring without a commercial feed, manually check DragonForce's Tor leak site (accessible via Tor Browser) at the URL published in threat intelligence reports — note any data dumps referencing Ink and search for your organization's domain or identifiable project names in any leaked file listings.

Evidence: Before initiating any recovery actions that write to or modify backup media: (1) acquire a read-only image or file listing of the most recent backup set and verify against the last known-good manifest — do not mount backups read-write until integrity is confirmed; (2) run 'vssadmin list shadows' and capture output before any recovery operation that might overwrite VSS snapshots; (3) export Windows Security Event ID 4648 and 4776 (credential validation) from backup server event logs to check for unauthorized access attempts against the backup infrastructure — DragonForce operators often target backup systems specifically to maximize ransom leverage; (4) document the state of network segmentation rules (firewall ACLs, VLAN assignments) for backup segments before any changes, as this establishes the pre-recovery network baseline.

Step 5: Post-Incident — Review third-party vendor risk assessments for creative and media sector partners. Confirm that vendor access is governed by least-privilege principles and that access is revoked promptly when engagements end. Assess whether email and document-handling controls adequately limit exfiltration pathways consistent with T1114 and T1041 (NIST AC-6: Least Privilege; CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP: User Account Permissions).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For a two-person team conducting post-incident vendor review: (1) build a vendor access matrix in a spreadsheet listing every third-party (creative studios, production contractors, post-production vendors) with columns for: access type, systems accessible, MFA status, last access review date, and offboarding date — this is the minimum viable vendor inventory; (2) query Active Directory for stale accounts using 'Search-ADAccount -AccountInactive -TimeSpan 45 -UsersOnly | Select Name,LastLogonDate' and flag any associated with media/production vendors for immediate review; (3) deploy Microsoft's free Attack Surface Analyzer or use 'Get-MailboxAuditLog' (Exchange/M365) to enumerate mailbox export and forwarding rules — DragonForce affiliates configure auto-forward rules as a persistence mechanism for ongoing T1114 collection even after initial access is remediated.

Evidence: Post-incident evidence preservation for lessons-learned and potential regulatory reporting: (1) retain all authentication logs, email server logs, and file access logs for a minimum of 12 months — if any shared data with Ink included PII of UK data subjects, the ICO breach notification window (72 hours under UK GDPR) may already be triggered and logs constitute regulatory evidence; (2) document the full timeline of Ink-associated account activity from your logs — first access grant date, last activity, revocation date — to support vendor risk review and potential contractual or regulatory disclosure; (3) preserve any dark web monitoring screenshots or threat intelligence reports referencing the DragonForce Ink claim as supporting documentation for your risk assessment update; (4) record the compensating controls implemented during this incident as the baseline for the updated vendor onboarding security requirements.

Detection Guidance

No confirmed IOCs have been publicly released for this incident. Detection efforts should focus on behavioral patterns consistent with the ATT&CK techniques mapped to DragonForce's model. Monitor for: large-volume outbound transfers over C2 channels (T1041) using network flow analysis and proxy logs; email collection activity such as bulk mailbox access, forwarding rule creation, or PST export events in Exchange or M365 audit logs (T1114); authentication events using valid credentials from unexpected geolocations or at atypical hours, particularly for privileged accounts (T1078); and file system telemetry showing mass encryption activity, shadow

copy deletion, or ransomware-consistent file extension changes (T1486). If Ink is a known vendor or counterparty, treat any shared credentials or API tokens as potentially compromised and rotate them (D3-CRO: Credential Rotation). Monitor dark web intelligence feeds for Ink data publications that may name your organization. No specific event IDs, hashes, or network indicators are confirmed at this time.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1114** — Email Collection
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1114	Email Collection	Collection
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Privacy, Security and Compliance | Movable Ink	https://movableink.com/privacy-security-and-compliance	T3
Black Duck: Application Security Testing | Software Composition ...	https://www.blackduck.com/	T3
Cybersecurity Risks in the Motion Picture and Film Industry	https://frameworksecurity.com/post/cybersecurity-risks-in-the-motio...	T3
Cutting-edge AI Security. Guided by Europe's Leading Experts.	https://www.eye.security/	T3
CrowdStrike Research: Security Flaws in DeepSeek-Generated ...	https://www.crowdstrike.com/en-us/blog/crowdstrike-researchers-iden...	T3

Generated 2026-06-14 13:36 UTC by TJS Security Command Center