INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-24 18:44 UTC

BlackFile Extortion Group Targets Retail and Hospitality with Vishing-Driven MFA Bypass and API Data Theft

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0216
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Salesforce (CRM platform), Microsoft SharePoint, Microsoft 365 (SSO/identity layer); VoIP/CNAM spoofing infrastructure used as attack vector
Published	2026-04-24T14:26:27
Discovery Source	Rss

Executive Summary

BlackFile is an active extortion group targeting retail and hospitality organizations by calling employees, impersonating IT helpdesk staff, and tricking them into approving login requests or registering attacker-controlled devices. Once inside, the group uses legitimate Salesforce and SharePoint API functions to steal customer and operational data, then demands seven-figure payments under threat of public disclosure. Palo Alto Unit 42 and Mandiant have been engaged in active incident response against BlackFile campaigns, making this an operationally live threat requiring immediate identity and access controls review.

Technical Analysis

BlackFile (also tracked as CL-CRI-1116, UNC6671, Cordial Spider) has been active since February 2026. The attack chain begins with CNAM/caller-ID spoofing over VoIP infrastructure to impersonate corporate IT helpdesk. Operators social-engineer employees into either approving MFA push prompts (MFA fatigue variant) or registering attacker-controlled devices against corporate identity platforms (Microsoft 365 SSO layer). No software vulnerability is exploited; initial access relies entirely on social engineering and misconfiguration. Post-authentication, actors abuse legitimate Salesforce CRM APIs and Microsoft SharePoint APIs (T1213, T1213.002, T1530, T1567) to exfiltrate data in a manner consistent with authorized administrative activity, reducing visibility to anomaly detection systems that rely on behavioral baselines. No CVE is assigned. Relevant CWEs: CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), CWE-522

(Insufficiently Protected Credentials), CWE-940 (Improper Verification of Source of Communication Channel). CVSS base score: 7.5 (analyst-assigned; no vendor CVSS vector published). MITRE ATT&CK coverage includes T1566.004 (Spearphishing Voice), T1621 (MFA Request Generation), T1098 (Account Manipulation), T1556.006 (Multi-Factor Authentication), T1078 (Valid Accounts), T1591.004 (Gather Victim Identity Information), T1213/T1213.002 (Data from Information Repositories/SharePoint), T1530 (Data from Cloud Storage), T1567 (Exfiltration Over Web Service), T1657 (Financial Theft), T1598 (Phishing for Information). No patch is available or applicable; remediation is entirely defensive control and detection-layer.

Action Checklist

1. Containment. Audit all device registrations and MFA enrollment events in Microsoft Entra ID (formerly Azure AD) for the past 90 days; immediately revoke any devices or authenticators not recognized by the owning employee. Suspend self-service device registration in Microsoft 365 tenant settings if not operationally required. Review Salesforce connected app authorizations and revoke unrecognized OAuth tokens via Setup > Connected Apps > OAuth Usage.
2. Detection. Query Microsoft Entra ID sign-in logs for MFA approval events preceded by helpdesk-initiated contact patterns; filter on device registration events (event category: DeviceRegistration) from unfamiliar geographies or device types. In Salesforce, enable and review API Usage and User Event Monitoring logs for bulk SOQL queries, large record exports, or Connected App activity outside normal business hours. Look for T1621 indicators: repeated MFA push approvals within short windows, especially outside normal user hours.
3. Eradication. Enforce number-matching or phishing-resistant MFA (FIDO2/hardware keys) across Microsoft 365 to eliminate push-approval social engineering. Disable legacy authentication protocols in Microsoft 365 (Basic Auth, SMTP AUTH where unused). In Salesforce, restrict API access by IP allowlisting under Setup > Network Access and enforce named credentials for service accounts. Remove any attacker-registered devices or OAuth grants identified during containment.
4. Recovery. Validate that no unauthorized conditional access policies, mail forwarding rules, or OAuth grants persist post-remediation. Run a Salesforce Data Export audit and compare against expected data access patterns to scope potential exfiltration volume. Re-verify all helpdesk call-back verification procedures are enforced; confirm employees know to refuse MFA approvals they did not initiate. Monitor Entra ID Identity Protection risk detections for 30 days post-remediation.
5. Post-Incident. Conduct targeted security awareness training focused specifically on vishing and MFA fatigue attacks for retail and hospitality front-line and IT helpdesk staff. Implement a callback verification protocol requiring employees to hang up and call back on a number from the internal directory before approving any MFA or device registration request. Review API audit logging completeness in both Salesforce and SharePoint; confirm logs are forwarded to SIEM with retention sufficient for breach investigation (minimum 90 days, 1 year preferred).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to legal counsel and executive leadership immediately if Salesforce Data Export audit or EventLogFile ReportExport analysis confirms bulk access to customer PII (names, contact data, payment indicators) exceeding state breach notification thresholds (typically 500+ residents for multi-state retailers) or if the organization is subject to PCI-DSS, as cardholder data exposure triggers mandatory notification to card brands within 72 hours of confirmation.
Recovery Notes	Post-containment, validate clean state in both the Microsoft 365 identity layer and Salesforce simultaneously — BlackFile is known to establish redundant persistence through both OAuth grants and attacker-enrolled MFA devices, so remediating only one platform leaves a re-entry path. Monitor Entra ID Identity Protection risk detections and Salesforce Login History for the 30 days following remediation, specifically watching for sign-ins from the same ASNs or IP ranges identified during the intrusion, as the group has been observed returning to partially-remediated environments. Require all helpdesk staff to complete callback verification protocol training and confirm completion before restoring self-service device registration capabilities in the Microsoft 365 tenant.
Forensic Artifacts	Microsoft Entra ID Audit Logs — DeviceRegistration category events showing attacker-enrolled authenticator apps or FIDO keys with RegisteredOwner mismatched from the account's normal device inventory; preserve full JSON via Graph API `/auditLogs/directoryAudits` before any revocation activity | Salesforce EventLogFile records (types: API, ReportExport, ConnectedApp, Login) — bulk SOQL queries against Contact, Account, Lead, and Opportunity objects with RowsProcessed counts anomalously high relative to the authenticated user's role; these rotate on a 24-30 day cycle and must be downloaded immediately | Microsoft Entra ID Sign-In Logs — MFA approval events (AuthenticationRequirement='multiFactorAuthentication', AuthenticationDetails.succeeded=true) from IP addresses resolving to residential VPN or datacenter ASNs inconsistent with the employee's normal sign-in geography, temporally correlated with inbound VoIP calls to the helpdesk | Salesforce Setup Audit Trail — entries in the Section 'Connected Apps' and 'Network Access' showing OAuth grants issued to unrecognized application ClientIds or IP allowlist modifications made during the intrusion window; downloadable under Setup > Audit Trail as a CSV covering the last 180 days | VoIP/PBX Call Detail Records (CDRs) — inbound call logs to helpdesk DDI numbers showing spoofed CNAM values (caller ID displaying internal IT department names) from external DIDs; these establish the social engineering timeline and are essential for correlating the precise moment of credential compromise with downstream Entra ID and Salesforce activity

Per-Action IR Details

Containment — Audit all device registrations and MFA enrollment events in Microsoft Entra ID (formerly Azure AD) for the past 90 days; immediately revoke any devices or authenticators not recognized by the owning employee. Suspend self-service device registration in Microsoft 365 tenant settings if not operationally required. Review Salesforce connected app authorizations and revoke unrecognized OAuth tokens via Setup > Connected Apps > OAuth Usage.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export Entra ID audit logs via Microsoft Graph API using PowerShell: `Get-MgAuditLogSignIn -Filter "category eq 'DeviceRegistration'" | Export-Csv entra_devices.csv`. For Salesforce OAuth grants without a SIEM, query the ConnectedApplication and AuthSession objects via the Salesforce CLI: `sfdx force:data:soql:query -q "SELECT ConnectedApplication.Name, User.Username, CreatedDate FROM AuthSession ORDER BY CreatedDate

DESC" -u `. Cross-reference output against HR-verified employee device lists maintained in a spreadsheet. Two-person team: one works Entra, one works Salesforce simultaneously.

Evidence: BEFORE revoking any token or device, export and preserve: (1) Microsoft Entra ID audit log entries for DeviceRegistration and MFA enrollment events — capture the full JSON via Graph API endpoint `/auditLogs/directoryAudits?$filter=activityDisplayName eq 'Register device'`; (2) Salesforce Setup Audit Trail (downloadable under Setup > Audit Trail) showing Connected App authorization events, capturing ActorName, Action, Section, and CreatedDate fields; (3) Entra ID sign-in logs for the accounts flagged during vishing window — preserve the RiskDetail, ConditionalAccessStatus, and DeviceDetail fields which will show attacker-registered device fingerprints; (4) Screenshot or export of current OAuth token grants under Salesforce Setup > Connected Apps > OAuth Usage before any revocation to document pre-remediation state for breach scope analysis.

Detection — Query Microsoft Entra ID sign-in logs for MFA approval events preceded by helpdesk-initiated contact patterns; filter on device registration events (event category: DeviceRegistration) from unfamiliar geographies or device types. In Salesforce, enable and review API Usage and User Event Monitoring logs for bulk SOQL queries, large record exports, or Connected App activity outside normal business hours. Look for T1621 indicators: repeated MFA push approvals within short windows, especially outside normal user hours.

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 Entra ID without SIEM: use the Microsoft Graph PowerShell module to pull sign-in logs and pivot on MFA result — `Get-MgAuditLogSignIn -Filter "status/additionalDetails eq 'MFA completed in Azure AD'" | Where-Object { $_.Location.CountryOrRegion -notin @('US') }`. For Salesforce Event Monitoring without a paid add-on, enable the free-tier EventLogFile object and download API event logs via the Salesforce CLI: `sfdx force:data:soql:query -q "SELECT LogDate, EventType, LogFile FROM EventLogFile WHERE EventType='API' ORDER BY LogDate DESC LIMIT 50"`. Detect T1621 MFA fatigue manually by sorting sign-in logs by UserPrincipalName and counting AuthenticationRequirement='multiFactorAuthentication' entries per user per hour — flag any user with more than 3 MFA prompts in 60 minutes.

Evidence: Capture before analysis so artifacts are not overwritten by normal system activity: (1) Salesforce EventLogFile records of type 'API', 'ReportExport', 'ConnectedApp', and 'Login' for the 90-day window — download raw CSV files via Tooling API as these rotate and may be lost; (2) Microsoft Entra ID sign-in logs filtered on `authenticationRequirement eq 'multiFactorAuthentication'` and cross-referenced with VoIP call records or helpdesk ticket timestamps to establish the vishing call window; (3) Entra ID Identity Protection risk detection events (riskyUsers and riskDetections endpoints via Graph API) flagging impossible travel, unfamiliar sign-in properties, or token anomalies coinciding with the attack window; (4) CNAM/caller ID records from your VoIP provider or PBX call logs showing inbound calls to helpdesk staff — these establish the social engineering timeline and are critical for breach notification narrative.

Eradication — Enforce number-matching or phishing-resistant MFA (FIDO2/hardware keys) across Microsoft 365 to eliminate push-approval social engineering. Disable legacy authentication protocols in Microsoft 365 (Basic Auth, SMTP AUTH where unused). In Salesforce, restrict API access by IP allowlisting under Setup > Network Access and enforce named credentials for service accounts. Remove any attacker-registered devices or OAuth grants identified during containment.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST SC-8 (Transmission Confidentiality and Integrity), NIST CM-6 (Configuration Settings), NIST SI-2 (Flaw Remediation), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without an MDM to push FIDO2 policy, enforce number-matching MFA immediately via Microsoft Entra ID Conditional Access (free with Entra ID P1 — available to most M365 Business Premium tenants): navigate to

Entra ID > Security > Authentication Methods > Microsoft Authenticator > Configure > Require Number Matching. Block legacy auth with a Conditional Access policy targeting 'Exchange ActiveSync clients and other clients' with grant control 'Block'. For Salesforce IP allowlisting on a budget: export current user IP ranges from Setup > Network Access, then add your organization's NAT egress IPs — this is a native Salesforce feature requiring no additional licensing. Verify legacy auth is blocked by running the free Microsoft Sign-in Diagnostic: `Invoke-MgGraphRequest -Method GET -Uri '/reports/authenticationMethods/userRegistrationDetails'` and filtering on `methodsRegistered`.

Evidence: Before removing attacker artifacts, preserve: (1) Full details of each attacker-registered device from Entra ID — capture DeviceId, DisplayName, OperatingSystem, TrustType, RegisteredOwner, and ApproximateLastSignInDateTime via `Get-MgDevice | Where-Object { $_.TrustType -eq 'Workplace' }` filtered to the attack window; (2) Salesforce Setup Audit Trail entries for any changes to Network Access settings, Named Credentials, or Profile API access permissions made during the intrusion window — attackers may have modified these to preserve access; (3) Export any Conditional Access policy changes from Entra ID audit logs (activityDisplayName eq 'Update conditional access policy') — BlackFile is known to create or modify CA policies to exclude attacker-controlled accounts from MFA requirements; (4) List of all accounts where legacy authentication sign-ins succeeded during the intrusion window via `Get-MgAuditLogSignIn -Filter "clientAppUsed ne 'Browser' and clientAppUsed ne 'Mobile Apps and Desktop clients'"`.

Recovery — Validate that no unauthorized conditional access policies, mail forwarding rules, or OAuth grants persist post-remediation. Run a Salesforce Data Export audit and compare against expected data access patterns to scope potential exfiltration volume. Re-verify all helpdesk call-back verification procedures are enforced; confirm employees know to refuse MFA approvals they did not initiate. Monitor Entra ID Identity Protection risk detections for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CA-7 (Continuous Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Audit mail forwarding rules across all M365 mailboxes using free Exchange Online PowerShell: `Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object { $_.ForwardTo -ne $null -or $_.RedirectTo -ne $null } | Select-Object MailboxOwnerID, Name, ForwardTo, RedirectTo | Export-Csv forwarding_rules.csv`. Audit Conditional Access policies via: `Get-MgIdentityConditionalAccessPolicy | Select-Object DisplayName, State, CreatedDateTime, ModifiedDateTime | Export-Csv ca_policies.csv` — flag any policy created or modified during the intrusion window. For Salesforce exfiltration scoping without a DLP tool, query the EventLogFile for ReportExport and DataExport event types and sum the RowsProcessed field per user to estimate records accessed: `sfdx force:data:soql:query -q "SELECT CreatedBy.Username, SUM(RowsProcessed) total FROM EventLogFile WHERE EventType='ReportExport' GROUP BY CreatedBy.Username"`.

Evidence: Capture post-remediation state as a verified clean baseline: (1) Export the full list of active Conditional Access policies with creation and modification timestamps — this becomes the authorized CA policy inventory; (2) Salesforce Data Export Service logs and ReportExport EventLogFile entries summarizing records accessed per object type (Contact, Account, Opportunity) — required to quantify PII exposure for breach notification decisions; (3) Entra ID Identity Protection `riskDetections` API export for the 30-day monitoring window — preserve weekly snapshots as evidence of clean state for regulatory purposes; (4) Helpdesk call logs and ticketing system records for the post-remediation period confirming callback verification protocol compliance — these demonstrate due diligence in the event of regulatory inquiry.

Post-Incident — Conduct targeted security awareness training focused specifically on vishing and MFA fatigue attacks for retail and hospitality front-line and IT helpdesk staff. Implement a callback verification protocol requiring employees to hang up and call back on a number from the internal directory before approving any MFA or device registration request. Review API audit logging completeness in both Salesforce and SharePoint; confirm logs are forwarded to SIEM with retention sufficient for breach investigation (minimum 90 days, 1 year preferred).

NIST Phase: Post Incident

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

Controls: NIST IR-2 (Incident Response Training), NIST IR-8 (Incident Response Plan), NIST AU-11 (Audit Record Retention), NIST AU-12 (Audit Record Generation), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 8.2 (Collect Audit Logs), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For awareness training without a commercial LMS: use CISA's free 'Phishing and Vishing' training materials (available at cisa.gov/resources-tools/resources/phishing-infographics) and conduct a live tabletop exercise simulating a BlackFile-style helpdesk call — script the scenario using actual BlackFile TTPs (caller claims to be IT, references employee's name and team, creates urgency around account lockout, requests MFA approval). For log forwarding without a paid SIEM: configure Microsoft 365 Diagnostic Settings to export Entra ID sign-in and audit logs to an Azure Storage Account (lowest-cost retention tier) using the native Entra ID > Diagnostic Settings blade — 90-day retention costs approximately $2-5/month for typical SMB log volumes. For Salesforce, schedule automated weekly downloads of EventLogFile CSVs via a cron job calling the Salesforce REST API and archiving to local NAS or low-cost cloud storage to meet the 1-year retention target.

Evidence: Preserve the following as post-incident lessons-learned documentation: (1) Timeline reconstruction document correlating VoIP call records, Entra ID MFA approval timestamps, first attacker device registration, and first Salesforce API bulk query — this establishes dwell time and is required for breach notification accuracy; (2) Helpdesk ticketing system records showing whether any employees created tickets during or after receiving the vishing calls — absence of tickets is itself a finding that drives the callback verification protocol recommendation; (3) Salesforce and SharePoint API audit log gap analysis — document which log types were not enabled or retained at time of incident (e.g., Salesforce Event Monitoring not licensed, SharePoint Unified Audit Log not enabled) as evidence driving the logging remediation requirement; (4) Entra ID Conditional Access policy inventory snapshot taken at the time of initial compromise discovery — comparison against the post-remediation inventory demonstrates scope of unauthorized changes for the incident report.

Detection Guidance

Microsoft 365 / Entra ID: Query Entra ID audit logs for DeviceRegistration events (AuditLogs | where OperationName == 'Register device') and cross-reference against employee-confirmed registrations. Alert on MFA push approvals (SignInLogs | where AuthenticationDetails contains 'MFA' and ResultType == 0) that occur outside business hours or from unfamiliar IP ranges. Flag multiple MFA push attempts within 60-second windows as potential T1621 fatigue activity. Salesforce: Enable Event Monitoring (requires Enterprise or Unlimited edition) and query ApiEvent logs for high-volume SOQL queries, ListViewEvent for mass record access, and ReportEvent for bulk exports by accounts not designated as integration users. Alert on Connected App OAuth grants issued to unrecognized client IDs. Network/VoIP: If call logging is available, flag inbound calls to helpdesk from spoofed CNAM values claiming to be internal IT; CNAM spoofing will show caller ID matching internal naming conventions from external PSTN numbers. Behavioral indicators: Single employee account accessing >500 Salesforce records or >50 SharePoint documents within a 30-minute window outside normal role baseline; new device enrollment immediately followed by large data query activity.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	[none published]	No specific IOC values have been publicly attributed to BlackFile by Unit 42, Mandiant, or BleepingComputer as of this item's source date. Do not treat absence of published IOCs as absence of threat activity.	LOW

Framework Mappings

MITRE-ATTACK

- **T1591.004** — Identify Roles
- **T1098** — Account Manipulation
- **T1657** — Financial Theft
- **T1621** — Multi-Factor Authentication Request Generation
- **T1213** — Data from Information Repositories
- **T1530** — Data from Cloud Storage
- **T1566.004** — Spearphishing Voice
- **T1213.002** — Sharepoint
- **T1556.006** — Multi-Factor Authentication
- **T1567** — Exfiltration Over Web Service
- **T1598** — Phishing for Information
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness
- **SI-4** — System Monitoring

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access

- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1591.004	Identify Roles	Reconnaissance
T1098	Account Manipulation	Persistence
T1657	Financial Theft	Impact
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1213	Data from Information Repositories	Collection
T1530	Data from Cloud Storage	Collection
T1566.004	Spearphishing Voice	Initial-Access
T1213.002	Sharepoint	Collection
T1556.006	Multi-Factor Authentication	Credential-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1598	Phishing for Information	Reconnaissance
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-blackfile-extort...	T3
Customer guidance for SharePoint vulnerability CVE-2025- ...	https://www.microsoft.com/en-us/msrc/blog/2025/07/customer-guidance...	T1
Microsoft Releases Guidance on Exploitation of SharePoint ...	https://www.cisa.gov/news-events/alerts/2025/07/20/update-microsoft...	T1
Security Update Guide - Microsoft Security Response Center	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/...	T1
Security Advisories	https://security.salesforce.com/security-advisories	T3

Generated 2026-04-24 18:44 UTC by TJS Security Command Center