INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-16 06:38 UTC

BlackFile (UNC6671): Vishing-Driven AiTM Extortion Campaign Bypasses MFA Across Enterprise SaaS Platforms

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0323
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Microsoft 365, Microsoft SharePoint, Microsoft OneDrive, Microsoft Entra, Okta, Salesforce, Zendesk, ServiceNow
Published	2026-05-15T14:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

UNC6671, operating as 'BlackFile,' is running an active extortion campaign that combines targeted phone calls with real-time credential interception to bypass multi-factor authentication across Microsoft 365, Okta, and related SaaS platforms. The group has compromised organizations across North America, Australia, and the UK since early 2026, with reported file exfiltration and ransom demands in the millions of dollars according to Google Threat Intelligence. A suspected logging gap in Microsoft 365 means mass file theft via API may be misclassified as routine access, potentially making this campaign difficult to detect with standard SOC tooling.

Technical Analysis

UNC6671 (BlackFile) executes a three-phase operation: (1) adversary-in-the-middle (AiTM) proxy infrastructure intercepts OAuth/SAML session tokens in real time, defeating TOTP and push-based MFA; (2) concurrent voice phishing (vishing) manipulates targets into approving authentication prompts or providing OTPs during the live call; (3) post-access, automated Python and PowerShell scripts exfiltrate files from SharePoint, OneDrive, and connected SaaS platforms before ransom demands are issued. Suspected detection gap in Microsoft 365 Unified Audit Log: bulk file access via Graph API direct calls may log as 'FileAccessed' events rather than 'FileDownloaded,' potentially suppressing volume-based exfiltration alerts. Affected platforms: Microsoft 365, SharePoint, OneDrive, Microsoft Entra, Okta, Salesforce, Zendesk, ServiceNow. No CVE assigned; the campaign exploits architectural trust gaps rather than unpatched vulnerabilities. CWE coverage: CWE-287

(Improper Authentication), CWE-308 (Single-Factor Authentication), CWE-522 (Insufficiently Protected Credentials), CWE-359 (Exposure of Private Personal Information). MITRE ATT&CK techniques include T1557 (Adversary-in-the-Middle), T1621 (MFA Request Generation), T1566.004 (Spearphishing Voice), T1078 (Valid Accounts), T1530 (Data from Cloud Storage), T1567.002 (Exfiltration to Cloud Storage), T1059.001 (PowerShell), T1059.006 (Python), T1539 (Steal Web Session Cookie), T1657 (Financial Theft), and T1486 (Data Encrypted for Impact). Source: Google Threat Intelligence Group, https://cloud.google.com/blog/topics/threat-intelligence/blackfile-vishing-extortion-operation/.

Action Checklist

1. Containment: Disable IMAP, POP3, and SMTP AUTH for all Microsoft 365 accounts; disable SMS and voice OTP fallback in Entra Conditional Access by requiring FIDO2 hardware keys or certificate-based authentication for all critical users; configure Okta FastPass without OTP phone fallback. Test on non-production accounts before enterprise enforcement to validate no integrations break.
2. Detection: Query Microsoft 365 Unified Audit Log for anomalous 'FileAccessed' event volume spikes (baseline per-user volume, alert on 3x-5x increase within 60 minutes) combined with atypical sign-in geography or Graph API user-agent strings (python-requests, msal, Invoke-RestMethod); alert on Entra sign-in logs showing token issued from one IP and used from geographically disparate IP within minutes; alert on Okta System Log events for MFA challenge followed by approval from different IP or device fingerprint.
3. Eradication: Revoke all active sessions and refresh tokens for any account flagged during detection using Entra's 'Revoke Sign-In Sessions' and Okta's 'Revoke All Sessions' API; rotate credentials for service accounts with SharePoint/OneDrive API access; audit and remove unauthorized OAuth app registrations and delegated permissions in Entra and connected SaaS platforms.
4. Recovery: Re-baseline normal 'FileAccessed' event volume per user and per application in Microsoft 365 audit logs; enable Microsoft Purview Audit (Premium) to capture richer file access telemetry; validate Conditional Access policies enforce compliant device and phishing-resistant MFA conditions; confirm no persistent backdoor accounts or forwarding rules remain in compromised mailboxes.
5. Post-Incident: Build SIEM correlation rules that aggregate 'FileAccessed' event counts per session and alert on bulk access thresholds; implement user training targeting vishing and MFA fatigue attack patterns; review SaaS platform OAuth delegated permissions quarterly; document session token lifetime policies and reduce token validity windows per Microsoft Conditional Access token protection controls.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and external IR retainer immediately if: (1) UAL FileAccessed event volume or the confirmed audit logging gap cannot bound the exfiltration scope below regulatory breach notification thresholds for PII/PHI under GDPR, HIPAA, or applicable state breach laws; (2) ransom demand from UNC6671/BlackFile is received; or (3) evidence of persistent OAuth app access or backdoor accounts is confirmed, indicating active ongoing exfiltration beyond the initial AiTM session.

Recovery Notes	Post-containment, monitor Microsoft 365 UAL and Entra sign-in logs continuously for a minimum of 30 days for re-emergence of Graph API user agents (python-requests, PowerShell) accessing SharePoint/OneDrive at volume, as UNC6671 may retain persistence via OAuth app registrations or guest accounts created during the compromise window that survived initial eradication. Validate daily that Conditional Access token protection policies remain enforced and that no new legacy authentication sign-in successes appear in Entra logs, as the group is known to probe for fallback authentication paths after initial containment. Engage Microsoft's Detection and Response Team (DART) or a qualified IR provider if the audit logging gap prevents a defensible determination of exfiltration scope, as regulatory breach notification timelines (typically 72 hours under GDPR) may be running.
Forensic Artifacts	Microsoft 365 Unified Audit Log — 'FileAccessed', 'FileDownloaded', 'FilePreviewed' operations in SharePoint and OneDrive workloads, filtered for Graph API and Python/PowerShell user-agent strings; critical for scoping UNC6671 bulk exfiltration volume, but note confirmed logging gap may render pre-Purview-Premium-enablement records incomplete or absent — document gap window with timestamps | Entra ID Sign-In Logs — entries where 'authenticationDetails.authenticationMethod' = 'Previously satisfied' combined with 'ipAddress' outside known user geographies and 'riskEventType' = 'unfamiliarFeatures' or 'tokenIssuerType' = 'AzureAD' with mismatched device compliance state; these are the direct forensic signature of UNC6671's AiTM-stolen session token replay bypassing MFA | Entra Audit Logs — 'Add OAuth2PermissionGrant', 'Consent to application', and 'Add app role assignment to service principal' events created during the compromise window; identifies the specific Graph API delegated permissions (Files.Read.All, Sites.Read.All, Mail.Read) UNC6671's illicitly registered applications were granted for persistent programmatic SharePoint/OneDrive access | Exchange Online Mailbox Audit Log and Inbox Rules — 'New-InboxRule' and 'Set-InboxRule' operations on compromised mailboxes, plus 'ForwardTo' and 'RedirectTo' rule configurations; UNC6671 commonly plants forwarding rules post-AiTM to intercept ongoing communications and gather intelligence for targeted extortion demands | Okta System Log — 'user.authentication.auth_via_mfa' events with 'factor' = SMS/voice OTP or TOTP correlated with 'user.session.start' events from IP addresses matching known AiTM proxy infrastructure (Evilginx2/Modlishka reverse proxy exit nodes), and 'app.oauth2.token.grant.access_token' events for Okta-connected SaaS platforms (Salesforce, ServiceNow, Zendesk) that UNC6671 may have pivoted to after initial M365 compromise

Per-Action IR Details

Containment — Enforce phishing-resistant MFA (FIDO2/hardware security keys or certificate-based authentication) for all Microsoft 365, Entra, and Okta accounts immediately; disable legacy authentication protocols and SMS/voice OTP fallbacks across all affected SaaS platforms per Microsoft Entra Conditional Access and Okta FastPass guidance.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without Entra P2 licensing to enforce Conditional Access at scale: use Microsoft's free Security Defaults in Entra (blocks legacy auth and enforces MFA globally) as an interim measure via portal.azure.com > Entra ID > Properties > Manage Security Defaults. For Okta, enable 'Authenticator Enrollment Policy' restricting enrollment to FIDO2 via the Admin Console > Security > Authenticators. Block legacy auth protocols (SMTP AUTH, IMAP, POP3, Basic Auth) immediately via Exchange Online PowerShell: 'Set-TransportConfig -SmtpClientAuthenticationDisabled $true' and 'Get-CASMailbox -ResultSize Unlimited | Set-CASMailbox -ImapEnabled

$false -PopEnabled $false -SmtpClientAuthenticationDisabled $true'. Enumerate all Entra service principals still using password-based auth via: 'Get-MgServicePrincipal -All | Where-Object {$_.PasswordCredentials -ne $null}'.

Evidence: Before enforcing MFA policy changes, preserve: (1) Entra sign-in logs (portal.azure.com > Entra ID > Monitoring > Sign-in logs) filtered for 'Authentication method' = SMS/voice OTP or legacy Basic Auth within the past 90 days — export as CSV to document which accounts UNC6671 may have targeted via vishing-assisted OTP interception; (2) Okta System Log entries with eventType 'user.authentication.auth_via_mfa' where 'factor' = 'token:software:totp' or 'token:software:sms' to identify accounts authenticated via interceptable factors before FIDO2 enforcement; (3) Entra Conditional Access policy export (JSON) via Graph API 'GET /identity/conditionalAccessPolicies' to baseline pre-remediation policy state as evidence of the gap that enabled AiTM bypass.

Detection — Query Microsoft 365 Unified Audit Log for anomalous 'FileAccessed' event volume spikes (especially via Graph API user agents) combined with atypical sign-in geography or token issuance patterns; alert on Entra sign-in logs showing token replay (same refresh token reused from multiple IPs), unusual OAuth app consent grants, and PowerShell or Python user-agent strings accessing SharePoint/OneDrive at scale.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a SIEM, run the following Microsoft 365 Management Activity API query directly via PowerShell using the ExchangeOnlineManagement and MSOnline modules. Step 1 — Pull UAL FileAccessed events: 'Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -Operations FileAccessed -ResultSize 5000 | Where-Object {$_.UserAgent -match "python|powershell|graph"} | Group-Object UserIds | Sort-Object Count -Descending'. Step 2 — Identify token replay by querying Entra sign-in logs via MS Graph for the same 'correlationId' or 'refreshTokenId' appearing across more than one IP: 'GET /auditLogs/signIns?$filter=tokenIssuerType eq "AzureAD" and ipAddress ne ""'. Step 3 — Use the free Hawk tool (github.com/T0pCyber/hawk) to automate UAL extraction and cross-correlate FileAccessed volume with sign-in anomalies for a named user: 'Start-HawkUserInvestigation -UserPrincipalName victim@domain.com'.

Evidence: Capture before analysis actions alter log state: (1) Microsoft 365 Unified Audit Log raw export for Operations 'FileAccessed', 'FilePreviewed', 'FileDownloaded', 'SharingInvitationCreated' scoped to SharePoint and OneDrive workloads — note confirmed logging gap means events prior to Purview Audit Premium enablement may be absent or truncated, document this gap explicitly; (2) Entra sign-in logs showing 'riskEventType' = 'unfamiliarFeatures' or 'anonymizedIPAddress' correlated with 'authenticationDetails.authenticationMethod' = 'Previously satisfied' (indicating AiTM-stolen session token reuse); (3) Entra audit logs for 'Add app role assignment to service principal' and 'Consent to application' events that UNC6671 may have triggered via OAuth phishing to establish persistent Graph API access for bulk OneDrive enumeration.

Eradication — Revoke all active sessions and refresh tokens for any account flagged during detection using Entra's 'Revoke Sign-In Sessions' and Okta's 'Revoke All Sessions' API; rotate credentials for service accounts with SharePoint/OneDrive API access; audit and remove unauthorized OAuth app registrations and delegated permissions in Entra and connected SaaS platforms.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Session revocation for all flagged accounts in bulk via Microsoft Graph PowerShell: 'Get-Content flagged_users.txt | ForEach-Object { Revoke-MgUserSignInSession -UserId $_ }' — confirm each returns HTTP 204. For Okta, use the Admin API: 'curl -X DELETE "https://{yourOktaDomain}/api/v1/users/{userId}/sessions" -H "Authorization: SSWS {api_token}"' for each flagged userId. Enumerate and remove unauthorized OAuth app registrations via Graph: 'Get-MgApplication -All | Where-Object {$_.CreatedDateTime -gt "2026-01-01"} | Select-Object

DisplayName, AppId, CreatedDateTime' — cross-reference against your approved app inventory and remove unknowns with 'Remove-MgApplication -ApplicationId {id}'. For service account credential rotation on SharePoint/OneDrive API access, identify all app registrations with Files.Read.All or Sites.Read.All permissions: 'Get-MgServicePrincipalAppRoleAssignment -ServicePrincipalId {id} | Where-Object {$_.ResourceDisplayName -eq "Microsoft Graph"}'.

Evidence: Before revoking sessions or rotating credentials, preserve: (1) Entra audit log entries for 'Add OAuth2PermissionGrant' and 'Add delegated permission grant' events — these record the exact permissions UNC6671's illicitly registered OAuth apps were granted for Graph API bulk file access against SharePoint/OneDrive; (2) Full list of active refresh tokens and their associated IP addresses from Entra sign-in logs ('tokenIssuerType', 'ipAddress', 'userAgent' fields) to document the AiTM proxy infrastructure before tokens are invalidated; (3) Okta System Log snapshot for 'app.oauth2.token.grant.access_token' events associated with compromised accounts — export via Okta API 'GET /api/v1/logs?filter=eventType eq "app.oauth2.token.grant.access_token"&since={incident_start}' before session revocation destroys the correlation window.

Recovery — Re-baseline normal 'FileAccessed' event volume per user and per application in Microsoft 365 audit logs; enable Microsoft Purview Audit (Premium) to capture richer file access telemetry; validate Conditional Access policies enforce compliant device and phishing-resistant MFA conditions; confirm no persistent backdoor accounts or forwarding rules remain in compromised mailboxes.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 8.2 (Collect Audit Logs), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without Purview Audit Premium licensing, maximize standard UAL retention by ensuring audit logging is enabled on all mailboxes (default is 90 days for E3): 'Get-OrganizationConfig | Select-Object AuditDisabled' and 'Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true'. Check for backdoor inbox rules on all compromised mailboxes: 'Get-InboxRule -Mailbox victim@domain.com | Select-Object Name, ForwardTo, RedirectTo, DeleteMessage, ForwardAsAttachmentTo' — UNC6671 may have set forwarding rules to exfiltrate ongoing communications post-compromise. Check for new Entra guest accounts or external collaboration enablements created during the compromise window: 'Get-MgUser -Filter "userType eq ''Guest''" | Where-Object {$_.CreatedDateTime -gt "2026-01-01"}'. Validate Conditional Access named locations and trusted IP ranges have not been modified to whitelist attacker IPs: 'Get-MgIdentityConditionalAccessNamedLocation'.

Evidence: Before declaring recovery complete, document: (1) Microsoft 365 UAL baseline — run 'Search-UnifiedAuditLog -Operations FileAccessed -StartDate {30 days pre-incident} -EndDate {incident_start}' to establish per-user and per-app 'FileAccessed' daily averages as the clean-state benchmark against which post-recovery behavior will be compared; (2) Exchange Online mailbox audit log for 'Create' and 'Set' inbox rule operations ('Search-UnifiedAuditLog -Operations New-InboxRule,Set-InboxRule') to document any UNC6671-planted forwarding rules before they are removed; (3) Entra Conditional Access policy configuration export post-remediation (JSON via Graph API) to confirm phishing-resistant MFA and compliant device conditions are active, serving as the verified clean-state configuration record.

Post-Incident — Close the audit logging gap by building SIEM correlation rules that aggregate 'FileAccessed' event count per session and alert on bulk access thresholds; implement user training targeting vishing and MFA fatigue attack patterns; review SaaS platform OAuth delegated permissions quarterly; document session token lifetime policies and reduce token validity windows per Microsoft's recommended Conditional Access token protection controls.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish

and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a commercial SIEM, implement detection using the following free controls: (1) Deploy the Sigma rule 'microsoft365_sharepoint_file_mass_download.yml' (available in the SigmaHQ repository) against UAL exports to detect bulk FileAccessed events exceeding threshold — convert to PowerShell using sigma-cli: 'sigma convert -t powershell rules/microsoft365_sharepoint_file_mass_download.yml'. (2) Schedule a weekly PowerShell cron-equivalent (Windows Task Scheduler) that queries the UAL for FileAccessed counts per user per 24-hour window and emails an alert if any user exceeds 500 file access events: 'Search-UnifiedAuditLog -Operations FileAccessed -StartDate (Get-Date).AddDays(-1) -EndDate (Get-Date) -ResultSize 5000 | Group-Object UserIds | Where-Object {$_.Count -gt 500}'. (3) For vishing/MFA fatigue training, use the free Microsoft Attack Simulator (included in M365 E3/E5) to run simulated vishing-style credential harvest campaigns targeting the specific pretext UNC6671 uses — impersonation of IT helpdesk requesting MFA re-enrollment. (4) For token lifetime reduction without Entra P2, configure token lifetime policies via Graph API: 'PATCH /policies/tokenLifetimePolicies/{id}' setting 'AccessTokenLifetime' to 'PT1H' and 'RefreshTokenMaxInactiveTime' to 'P14D'.

Evidence: For lessons-learned documentation, preserve and attach to the post-incident report: (1) The full UAL gap analysis — a timestamped record of the period during which 'FileAccessed' events were absent or below expected volume due to the confirmed Microsoft 365 audit logging gap, establishing the maximum possible exfiltration window UNC6671 exploited; (2) Entra sign-in log entries showing the AiTM token replay chain — specifically entries where 'authenticationDetails.succeeded' = true with 'authenticationMethod' = 'Previously satisfied' from IP addresses not matching the legitimate user's known locations, documenting the exact mechanism that bypassed MFA; (3) The OAuth app permission audit report generated during eradication, retained as evidence of the delegated permission scope UNC6671's apps held against SharePoint/OneDrive (Files.Read.All, Sites.FullControl.All) to inform future quarterly review benchmarks.

Detection Guidance

Primary detection surface is the Microsoft 365 Unified Audit Log. Because UNC6671 exploits suspected logging behavior differences ('FileAccessed' vs. 'FileDownloaded' event classification), standard exfiltration alerts may not fire. Build detections on: (1) high-volume 'FileAccessed' events from a single user principal or OAuth app within a short window (baseline your environment, flag 3x-5x normal volume within 60 minutes); (2) Graph API access using non-standard user-agent strings, particularly Python (python-requests, msal) or PowerShell (Invoke-RestMethod) clients; (3) Entra Sign-In logs showing token issuance from one IP followed by token use from a geographically disparate IP within minutes, indicator of AiTM session hijack; (4) Okta System Log events for MFA challenge followed immediately by approval from a different IP or device fingerprint than the challenged session; (5) new OAuth application consent events or delegated permission grants issued during or after the suspicious session window. Hunting hypothesis: query for users with >500 'FileAccessed' events in any 60-minute window, cross-referenced against sign-in risk score in Entra Identity Protection. No public IOCs (IPs, domains, hashes) have been confirmed and published in the primary source at this time; do not populate IOC blocklists from unverified secondary sources.

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact
- **T1588.005** — Exploits
- **T1566.004** — Spearphishing Voice

- **T1621** — Multi-Factor Authentication Request Generation
- **T1567.002** — Exfiltration to Cloud Storage
- **T1539** — Steal Web Session Cookie
- **T1567** — Exfiltration Over Web Service
- **T1598** — Phishing for Information
- **T1059.001** — PowerShell
- **T1056.003** — Web Portal Capture
- **T1585.002** — Email Accounts
- **T1059.006** — Python
- **T1078** — Valid Accounts
- **T1557** — Adversary-in-the-Middle
- **T1530** — Data from Cloud Storage

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **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)
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

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

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
- **5.2** — Use Unique Passwords
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

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)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact
T1588.005	Exploits	Resource-Development
T1566.004	Spearphishing Voice	Initial-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1539	Steal Web Session Cookie	Credential-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1598	Phishing for Information	Reconnaissance
T1059.001	PowerShell	Execution
T1056.003	Web Portal Capture	Collection
T1585.002	Email Accounts	Resource-Development
T1059.006	Python	Execution
T1078	Valid Accounts	Defense-Evasion

Technique ID	Technique Name	Tactic
T1557	Adversary-in-the-Middle	Credential-Access
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Threat Intelligence	https://cloud.google.com/blog/topics/threat-intelligence/blackfile-...	T3
Disrupting active exploitation of on-premises SharePoint ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting...	T1
DevOps Vulnerability Integrations release notes - ServiceNow	https://www.servicenow.com/docs/r/store-release-notes/store-rn-devo...	T3
SharePoint, OneDrive, and Office 365 Collaboration Known Behaviors	https://success.skyhighsecurity.com/Skyhigh_CASB/06_Skyhigh_CASB_Sa...	T3
This Microsoft Entra ID Vulnerability Could Have Been Catastrophic	https://www.reddit.com/r/sysadmin/comments/1nlbl8r/this_microsoft_e...	T3

Generated 2026-05-16 06:38 UTC by TJS Security Command Center