INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-08 14:00 UTC

ShinyHunters Escalates Instructure Breach: 330 Canvas Portals Defaced in Active Extortion Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0291
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Instructure Canvas LMS, approximately 330 colleges, universities, and K-12 institutions; Canvas mobile app
Published	2026-05-07T18:36:54
Discovery Source	Rss

Executive Summary

On May 7, 2026, the ShinyHunters threat group defaced login portals for approximately 330 institutions using Instructure's Canvas LMS platform and claims to have exfiltrated roughly 280 million student and staff records. Instructure took Canvas offline in response, disrupting course delivery across hundreds of colleges, universities, and K-12 districts. ShinyHunters has set a May 12 ransom deadline, after which the group has threatened to release the stolen data publicly, creating compounding legal, regulatory, and reputational exposure for every affected institution.

Technical Analysis

On May 7, 2026, ShinyHunters executed a multi-stage attack against Instructure's Canvas LMS infrastructure. The group defaced login portals for approximately 330 institutions (T1491.002, External Defacement) and claims prior exfiltration of approximately 280 million records via bulk API abuse (T1567, T1530). Instructure has not publicly disclosed the exploited vulnerability. Candidate weakness classes based on available reporting: CWE-285 (Improper Authorization, portal-level content modification without authorization), CWE-287 (Improper Authentication, likely SSO/token abuse for initial access, possibly via device code flow or MFA fatigue, T1528, T1621), and CWE-200 (Exposure of Sensitive Information, bulk API data export, T1078). The attack pattern is consistent with ShinyHunters' documented history of API credential abuse and cloud storage exfiltration. Canvas's cloud-hosted multi-tenant architecture means a single platform-level compromise propagates across all tenant institutions simultaneously. Instructure has not confirmed patch availability, affected API versions, or

specific remediation guidance as of the incident date. CVSS base score assessed at 9.5 given multi-tenant blast radius, data volume, and active exploitation (editorial assessment; no CVE assigned). No CVE assigned as of available reporting.

Action Checklist

1. Containment: Treat Canvas as a compromised third-party service until Instructure issues a clean bill of health. Suspend active Canvas API integrations, revoke Canvas-issued OAuth tokens and API keys from institutional identity platforms (SAML, Shibboleth, Azure AD/Entra ID). Block outbound connections from Canvas-integrated systems to non-institutional endpoints where policy permits. Do not wait for Instructure communication before beginning token hygiene.
2. Detection: Review IdP (identity provider) logs for Canvas authentication events from May 1-7, 2026, focusing on anomalous OAuth device code flow requests (T1528), MFA push floods (T1621), and bulk API calls originating from unexpected IPs or service accounts. Query SIEM for T1491.002 indicators: portal content modification events or unexpected HTTP 200 responses to Canvas login portal endpoints returning non-standard content. Cross-reference Canvas audit logs (if accessible via your institution's admin console) for bulk data export events or API calls exporting records at unusual volume.
3. Eradication: Rotate all Canvas API keys, OAuth client secrets, and integration credentials institution-wide immediately. Do not wait for Instructure to issue a patch. Force re-authentication for all Canvas accounts. Audit SSO trust relationships and remove any unused Canvas service provider entries. Before restoring integrations post-incident, require Instructure to provide a written incident summary confirming root cause, scope, and remediation steps taken. Monitor https://status.instructure.com and Instructure's official security communications channel for remediation guidance.
4. Recovery: Before reconnecting Canvas integrations post-restoration, require Instructure to provide a written incident summary confirming root cause, scope, and remediation steps taken. Validate that portal content has returned to institutional-controlled state. Monitor authentication logs for 30 days post-restoration for re-exploitation indicators. Notify your student information system (SIS) administrators to audit any Canvas-SIS sync activity during the incident window.
5. Post-Incident: This incident exposes the risk of over-privileged API integrations with cloud-hosted SaaS platforms in education environments. Conduct a privilege audit of all third-party SaaS API integrations. Implement API access controls limiting bulk export capabilities. Review your institution's third-party vendor risk program to require SaaS providers to contractually commit to breach notification timelines. Evaluate whether your institution's incident response plan covers scenarios where the primary platform is controlled by a vendor and taken offline without notice.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to institutional legal counsel, privacy officer, and CISO if Canvas audit logs or SIS records confirm bulk export of student or staff PII during May 1–7, 2026, as this triggers FERPA breach notification obligations and potentially state data breach notification statutes with notification deadlines as short as 30–72 hours depending on jurisdiction; also escalate if ShinyHunters posts institutional data publicly after the May 12 deadline, which elevates the incident from suspected to confirmed exfiltration and activates regulatory reporting timelines.
Recovery Notes	Do not restore Canvas API integrations until Instructure provides a written root cause statement confirming the initial access vector has been closed — reconnecting OAuth integrations before this confirmation risks re-exposure if ShinyHunters retained access via a persistent backdoor in Instructure's infrastructure. Monitor Azure AD/Entra ID sign-in logs and Canvas API access logs daily for 30 days post-restoration, specifically watching for OAuth device code flow requests (T1528) and bulk API calls to user enrollment or account export endpoints that were not present in pre-incident baselines. Coordinate with SIS administrators to verify no unauthorized Canvas-SIS sync jobs ran during the incident window, as SIS data (SSNs, financial records, enrollment history) represents the highest-sensitivity data tier in the Canvas integration surface for most institutions.
Forensic Artifacts	Azure AD / Entra ID Sign-In Logs (30-day retention): Filter on Canvas application ID for the May 1–7, 2026 window — specific indicators include OAuth device code flow authentication attempts (authentication detail field 'deviceCode'), MFA denial events (resultType 70044 or 500121) indicating T1621 push flood attempts, and sign-ins from ASNs inconsistent with institutional user geography; export immediately as JSON before the 30-day retention window closes. | Canvas API Access Logs via Admin Console (Account > Settings > Logs): Bulk GET requests to /api/v1/accounts/*/users, /api/v1/courses/*/students, /api/v1/users/*/profile, or /api/v1/sis_imports during May 1–7 from service account tokens or unexpected source IPs — response payload sizes exceeding normal per-page API limits (100 records default) indicate automated bulk harvesting consistent with ShinyHunters' claimed 280 million record exfiltration. | Canvas SIS Import/Export History (Canvas Admin > SIS Imports): Timestamped records of all SIS data imports and exports during the incident window, including the initiating user account, file size, and record counts — anomalously large exports or exports initiated by non-standard service accounts during off-hours on May 1–7 would corroborate data exfiltration through the Canvas-SIS integration pathway. | Shibboleth IdP Audit Log (/opt/shibboleth-idp/logs/idp-audit.log) or ADFS Event Log (Event ID 1200 — AD FS issued a valid token; Event ID 1202 — AD FS validated credentials): Filter on Canvas SP entityID (typically 'https://canvas.instructure.com/saml2') for the incident window to identify anomalous SAML assertion volumes, assertions issued to unexpected relying parties, or attribute release of PII fields (eduPersonPrincipalName, mail, givenName) at volumes inconsistent with normal Canvas session activity. | Institutional Network Perimeter Logs / DNS Query Logs: Outbound DNS queries and HTTPS connections from Canvas-integrated internal servers (SIS servers, integration middleware, Canvas data sync agents) to Instructure-operated infrastructure or unexpected third-party endpoints during May 1–7 — specifically look for DNS lookups to non-standard Instructure subdomains or data exfiltration staging infrastructure; if a next-gen firewall or proxy is in place, filter for large outbound POST or PUT payloads to non-institutional destinations from systems with Canvas integration roles.

Per-Action IR Details

Containment — Treat Canvas as a compromised third-party service until Instructure issues a clean bill of health. Suspend active Canvas API integrations, revoke Canvas-issued OAuth tokens and API keys from institutional identity platforms (SAML, Shibboleth, Azure AD/Entra ID). Block outbound connections from

Canvas-integrated systems to non-institutional endpoints where policy permits. Do not wait for Instructure communication before beginning token hygiene.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without SIEM/enterprise IAM tooling: enumerate all active Canvas OAuth tokens via your IdP's admin console — in Azure AD/Entra ID run 'Get-AzureADServicePrincipal | Where-Object {$_.DisplayName -like "*Canvas*"}' and revoke app permissions via 'Remove-AzureADServicePrincipalOAuth2PermissionGrant'; for Shibboleth, expire all active sessions by restarting the IdP service and clearing session cache at /opt/shibboleth-idp/metadata/; use host-based firewall rules (iptables or Windows Firewall via 'netsh advfirewall') to block outbound 443 to Canvas LMS IP ranges (available from Instructure's network documentation) on SIS and integration servers.

Evidence: Before revoking tokens, export a complete snapshot of all active OAuth grants and API key metadata from your IdP — in Azure AD/Entra ID export via 'Get-AzureADOAuth2PermissionGrant -All $true | Export-Csv'; capture Shibboleth IdP audit logs at /opt/shibboleth-idp/logs/idp-audit.log covering May 1–7, 2026 for Canvas SP entityID entries; preserve firewall flow logs showing outbound connections from Canvas-integrated servers to Instructure-operated IP ranges during the incident window before any blocking rules are applied.

Detection — Review IdP (identity provider) logs for Canvas authentication events from May 1–7, 2026, focusing on anomalous OAuth device code flow requests (T1528), MFA push floods (T1621), and bulk API calls originating from unexpected IPs or service accounts. Query SIEM for T1491.002 indicators: portal content modification events or unexpected HTTP 200 responses to Canvas login portal endpoints returning non-standard content. Cross-reference Canvas audit logs (if accessible via your institution's admin console) for bulk data export events or API calls exporting records at unusual volume.

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: Without a SIEM: use PowerShell to parse Azure AD sign-in logs exported as JSON — filter for 'appDisplayName' containing 'Canvas' and 'conditionalAccessStatus' of 'failure' or device code flow indicator 'deviceCode' in the authentication detail field; for MFA push floods (T1621), query Azure AD logs for 'resultType' 70044 (MFA denied) or 500121 (MFA required but not satisfied) with more than 5 events per user in a 10-minute window using 'Group-Object UserPrincipalName'; use 'grep' against exported Canvas API access logs for bulk GET requests to /api/v1/accounts/*/users or /api/v1/courses/*/students with response sizes exceeding 1MB from a single IP in the May 1–7 window; for T1491.002 defacement detection, use curl to compare live portal HTTP response body hashes against a known-good baseline captured from institutional Canvas subdomain.

Evidence: Preserve Azure AD/Entra ID sign-in logs (retention window is 30 days for P1/P2 tenants — export immediately to avoid loss) filtering on Canvas application ID; extract Canvas API access logs from your institution's Canvas admin console under Account > Settings > Logs covering May 1–7, 2026, specifically CSV exports of SIS import/export events and API usage reports showing endpoints hit, request volumes, and source IPs; capture any WAF or reverse proxy logs (nginx access.log, Apache access.log, or load balancer access logs) for your institution's Canvas subdomain showing HTTP response codes and content-length anomalies on the login portal endpoint during the defacement window.

Eradication — Rotate all Canvas API keys, OAuth client secrets, and integration credentials institution-wide. Force re-authentication for all Canvas accounts. Audit SSO trust relationships and remove any Canvas service provider entries that are no longer operationally required. Instructure has not issued a specific patch or remediation advisory as of the incident date — monitor https://status.instructure.com and Instructure's official security communications channel for remediation guidance before restoring integrations.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), 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: For teams without enterprise PAM or automated credential rotation: generate a complete list of Canvas API key holders via Canvas Admin console (Account > Developer Keys) and manually invalidate each key, documenting the key ID, associated user/service account, and revocation timestamp in a shared incident log; remove stale Canvas SP entries from Shibboleth metadata by editing /opt/shibboleth-idp/conf/metadata-providers.xml and reloading the IdP; in Azure AD, remove the Canvas enterprise application's delegated and application permissions via 'Remove-AzureADServicePrincipal' after confirming no active integrations depend on it; force global Canvas session invalidation by contacting Instructure support to request server-side session purge for your institution's subdomain while the platform is offline.

Evidence: Before rotation, document all existing Canvas Developer Key IDs, their associated service accounts, creation dates, and last-used timestamps from the Canvas Admin console — this establishes the pre-incident credential surface for post-incident review; preserve a copy of your Shibboleth or ADFS metadata configuration showing all registered Canvas SP entityIDs and attribute release policies, which will serve as the baseline for the SSO trust audit; retain Azure AD application permission export showing Canvas app's OAuth scopes prior to removal as evidence of over-permissioning for the post-incident review.

Recovery — Before reconnecting Canvas integrations post-restoration, require Instructure to provide a written incident summary confirming root cause, scope, and remediation steps taken. Validate that portal content has returned to institutional-controlled state. Monitor authentication logs for 30 days post-restoration for re-exploitation indicators. Notify your student information system (SIS) administrators to audit any Canvas-SIS sync activity during the incident window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without automated integrity monitoring: use curl to fetch your institution's Canvas login portal and hash the response body with 'curl -s https://.instructure.com/login/saml | sha256sum' — compare against a known-good hash stored in your incident documentation; for SIS sync audit, export your SIS (Ellucian Banner, Colleague, PowerSchool, etc.) integration logs and cross-reference Canvas SIS import history (Canvas Admin > SIS Imports) for any imports or exports initiated between May 1–7, 2026 that were not initiated by authorized SIS administrators; configure a cron job to run daily authentication log exports from Azure AD for the 30-day monitoring window and flag any Canvas app sign-in from a new IP or device not seen in the pre-incident baseline.

Evidence: Obtain and preserve Instructure's written root cause summary before restoring integrations — this document is critical evidence for regulatory breach notification filings and internal post-incident review; export SIS integration audit logs covering the incident window from your SIS platform, specifically any Canvas-initiated data pulls via SIS API or SFTP file drops to Canvas-managed storage; capture a baseline screenshot and HTTP response hash of the restored Canvas login portal for your institution's subdomain immediately upon Instructure's confirmation of restoration, timestamped and stored in your incident case file.

Post-Incident — This incident exposes the risk of over-privileged API integrations with cloud-hosted SaaS platforms in education environments. Conduct a privilege audit of all third-party SaaS API integrations. Implement API access controls limiting bulk export capabilities. Review your institution's third-party vendor risk program to require SaaS providers to contractually commit to breach notification timelines. Evaluate whether your institution's incident response plan covers scenarios where the primary platform is controlled by a vendor and taken offline without notice.

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 RA-3 (Risk Assessment), NIST SA-9 (External System Services), NIST SI-4 (System Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For institutions without a formal vendor risk program: create a SaaS integration inventory spreadsheet documenting every third-party platform with Canvas-equivalent API access to student PII (SIS, LMS, proctoring tools, advising platforms) — include OAuth scopes, data categories accessible, breach notification SLA, and last security review date; use Canvas Developer Keys admin view to enforce per-key rate limits and disable the 'Allow This Key to Act as Users' (user impersonation) scope on all non-administrative integrations as an immediate bulk export control; draft a one-page IR plan addendum specifically covering 'vendor-controlled platform outage with suspected breach' scenarios, defining who contacts Instructure, what alternative course delivery mechanism activates (e.g., campus LMS fallback or email-based delivery), and which FERPA/state breach notification obligations are triggered when a SaaS vendor holds institutional student PII.

Evidence: Compile the complete incident timeline — from first defacement detection through Instructure's restoration — for the lessons learned report, referencing ShinyHunters' May 7 defacement of 330 portals and the May 12 ransom deadline as documented threat actor TTPs; preserve all Instructure status page notifications, email communications, and support ticket transcripts as vendor accountability documentation for your institution's legal and compliance teams; retain the full OAuth grant and API key inventory captured at containment as the baseline for the privilege audit, enabling before/after comparison of your institution's third-party SaaS exposure.

Detection Guidance

Key detection focus areas given the attack pattern: (1) IdP/SSO logs, search for Canvas authentication events showing device code flow grants (OAuth 2.0 device authorization grant), MFA push requests not followed by successful user confirmation, or token issuance for service accounts outside normal hours; (2) API gateway or proxy logs, look for bulk GET requests to Canvas REST API endpoints such as /api/v1/accounts/{id}/users or /api/v1/courses/{id}/enrollments with response sizes significantly above baseline, particularly from service account credentials; (3) Web access logs, HTTP responses to Canvas login portal paths returning content-length or body hash values inconsistent with the institutional baseline (indicator of defacement); (4) SIEM correlation, build a rule correlating high-volume Canvas API calls (T1530/T1567) with service account logins outside business hours (T1078). IOCs: No confirmed IP addresses, domains, or file hashes have been publicly attributed to this campaign in available reporting. Use behavioral indicators above until Instructure or a vetted threat intelligence source publishes campaign-specific IOCs.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Canvas login portal pages displaying ransom demand content`	Defacement indicator — login portals for approximately 330 institutions displayed ShinyHunters ransom messages on May 7, 2026. Specific URLs vary by institution subdomain.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1530** — Data from Cloud Storage
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1485** — Data Destruction
- **T1657** — Financial Theft
- **T1566** — Phishing
- **T1491.002** — External Defacement
- **T1621** — Multi-Factor Authentication Request Generation
- **T1190** — Exploit Public-Facing Application
- **T1528** — Steal Application Access Token

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

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

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
- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1530	Data from Cloud Storage	Collection
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1485	Data Destruction	Impact
T1657	Financial Theft	Impact
T1566	Phishing	Initial-Access
T1491.002	External Defacement	Impact
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1528	Steal Application Access Token	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/canvas-login-portals...	T3
Canvas Online Learning Platform Disabled After Breach by Hackers	https://www.nytimes.com/2026/05/07/education/canvas-hacked-down-dat...	T2
Cyberattack shutters Canvas learning platform for schools across ...	https://www.cbsnews.com/news/cyberattack-shutters-canvas-learning-p...	T3
Hackers breach Canvas learning platform, exposing data on millions ...	https://www.abc10.com/article/news/nation-world/canvas-hack-shinyhu...	T3
Massive data breach affects schools using Canvas nationwide - 6ABC	https://6abc.com/post/canvas-hacked-massive-data-breach-affects-sch...	T3

Generated 2026-05-08 14:00 UTC by TJS Security Command Center