INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-09 06:26 UTC

ShinyHunters Maintains Persistent Access to Instructure Canvas LMS; Hundreds of Millions of PII Records at Active Risk

DATA BREACH | HIGH | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0117
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Instructure Canvas LMS (cloud-hosted platform; specific version not publicly disclosed)
Published	2026-05-08T16:08:06
Discovery Source	Rss

Executive Summary

ShinyHunters, a prolific financially motivated threat group, has confirmed unauthorized access to Instructure's Canvas LMS environment and reportedly maintains that access as of publication, making this an active, uncontained compromise affecting approximately 8,800 educational institutions globally. Hundreds of millions of student, faculty, and staff records are at risk, including names, email addresses, and institutional identifiers across K-12 and higher education. Organizations relying on Canvas face immediate operational disruption, significant regulatory exposure under student data protection laws, and heightened risk of downstream fraud, phishing campaigns, and reputational damage.

Technical Analysis

ShinyHunters has conducted a second confirmed intrusion against Instructure, the cloud-hosted provider of Canvas LMS. No CVE has been assigned. Specific affected platform versions have not been publicly disclosed by Instructure. The attack surface is consistent with cloud-hosted SaaS credential compromise, with the following CWEs cited: CWE-287 (Improper Authentication), CWE-522 (Insufficiently Protected Credentials), and CWE-284 (Improper Access Control). Relevant MITRE ATT&CK techniques include T1078 (Valid Accounts) for credential-based persistence, T1539 (Steal Web Session Cookie), T1098 (Account Manipulation), T1190 (Exploit Public-Facing Application), T1530 (Data from Cloud Storage), T1555 (Credentials from Password Stores), and T1567 (Exfiltration Over Web Service). T1486 (Data Encrypted for Impact) was considered based on initial reporting but ransomware involvement has not been authoritatively confirmed and is not included in primary threat assessment. Instructure reportedly disabled the Canvas platform following discovery, indicating

emergency containment. This is ShinyHunters' second confirmed attack against Instructure, suggesting either incomplete remediation of a prior incident or reacquisition via a separate attack path. Patch status: no vendor patch or official advisory has been publicly released as of available sourcing. Data categories at risk include names, email addresses, institutional identifiers, and potentially academic records consistent with LMS-resident data. Scope is global across K-12 and higher education.

Action Checklist

1. Containment: Contact your Instructure/Canvas account representative immediately to confirm the status of your institution's tenant, determine whether your data was within scope of the compromise, and request written confirmation of isolation status. If Canvas is operational in your environment, treat all active Canvas sessions as potentially compromised until Instructure provides tenant-level clearance.
2. Detection: Review identity provider (IdP) and SSO logs for anomalous Canvas authentication events: logins from unexpected geolocations, off-hours access, bulk data export activity, or API calls inconsistent with normal user behavior. If Canvas is federated via SAML or OAuth, audit federation logs for unauthorized token issuance. Correlate with email gateway logs for any Canvas-originated phishing indicators targeting staff or students.
3. Eradication: Force-rotate all Canvas administrative credentials and API tokens. Revoke and reissue any service account credentials used for Canvas integrations. Audit and remove any unrecognized OAuth application authorizations within your Canvas tenant. Review and tighten Canvas API access controls, particularly for third-party LTI integrations. No vendor-issued patch is available as of sourcing; follow Instructure's guidance when released.
4. Recovery: Before restoring full Canvas access, obtain written confirmation from Instructure that your institutional tenant has been isolated, assessed, and cleared. Validate that MFA is enforced for all Canvas admin accounts and API integrations. Monitor Canvas audit logs and IdP logs for at least 30 days post-clearance for re-access indicators consistent with T1078 (Valid Accounts) persistence.
5. Post-Incident: This incident exposes reliance on a single cloud-hosted SaaS provider for bulk PII storage without compensating controls. Conduct a third-party SaaS risk review covering data residency, breach notification SLAs, and tenant isolation guarantees. Evaluate whether student and staff PII volume stored in Canvas can be reduced. Review your institution's incident response plan for third-party SaaS compromise scenarios.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to institutional legal counsel, CISO, and privacy officer immediately if Instructure confirms your tenant's data was within scope of the ShinyHunters compromise, as this triggers mandatory FERPA breach notification assessment, potential state student privacy law obligations, and cyber insurance claim procedures — and given ShinyHunters' documented history of public data extortion, student and staff notification timelines must be established before threat actor publication.

Recovery Notes	Do not restore full Canvas user access until Instructure provides written, tenant-specific confirmation of isolation and remediation — not a generic all-clear advisory. Post-clearance, monitor Canvas audit logs and IdP authentication logs daily for a minimum of 30 days, specifically hunting for MITRE ATT&CK T1078 (Valid Accounts) indicators: authentication events from IP ranges not present in your pre-incident baseline, API calls to user enumeration endpoints, and OAuth token issuance for recently rotated accounts, all consistent with ShinyHunters' documented SaaS persistence tradecraft. Retain all logs from the compromise window for a minimum of 12 months to support regulatory obligations and any subsequent law enforcement cooperation.
Forensic Artifacts	Canvas Data 2 API authentication event exports (endpoint: /api/v1/audit/authentication/accounts/:account_id) — will show anomalous admin logins, bulk API calls to user/enrollment enumeration endpoints, and OAuth token issuance events attributable to ShinyHunters' automated harvesting activity | IdP authentication logs (Okta System Log, Azure AD Sign-In Logs, or Google Workspace Admin Reports) filtered to the Canvas application — will reveal logins from non-baseline geolocations, off-hours access by admin accounts, and SAML assertion anomalies consistent with credential compromise or session hijacking | Canvas Developer Keys and OAuth application authorization audit (Admin > Developer Keys in Canvas admin console) — will expose any unrecognized OAuth applications or LTI integrations registered by the threat actor as a persistence mechanism within your tenant | Email gateway logs (O365 Defender, Proofpoint, or Google Workspace mail logs) filtered for Canvas-branded sender domains, Canvas password reset flows, and outbound messages referencing Canvas credentials — relevant given ShinyHunters' post-breach pattern of targeted phishing and extortion communications to affected institution staff | Instructure-issued tenant activity reports and security notifications — official vendor documentation of which tenant data partitions were accessed, what data categories were exposed, and the timeline of unauthorized access; critical for FERPA breach assessment and establishing the authoritative exposure scope for regulatory notification purposes

Per-Action IR Details

Containment — Contact your Instructure/Canvas account representative immediately to confirm the status of your institution's tenant, determine whether your data was within scope of the compromise, and request written confirmation of isolation status. If Canvas is operational in your environment, treat all active Canvas sessions as potentially compromised until Instructure provides tenant-level clearance.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST IR-7 (Incident Response Assistance), CIS 6.2 (Establish an Access Revoking Process)

Compensating: If your institution lacks a dedicated vendor relationship manager, escalate directly to Instructure's security disclosure contact and simultaneously open a support ticket flagged as a security incident. Document all communications with timestamps. In parallel, use your IdP admin console (e.g., Okta, Azure AD, Google Workspace) to immediately disable Canvas SSO application access for all users except essential administrators, effectively suspending active Canvas sessions without waiting for Instructure confirmation.

Evidence: Before suspending sessions, export a snapshot of all active Canvas session tokens and authenticated user sessions from your IdP's session management console. Capture Canvas audit log entries (Admin > Settings > Logging in Canvas admin panel, or via Canvas Data 2 API endpoint /api/v1/audit/authentication) covering at least the prior 90 days. Preserve any Instructure-issued incident notifications or tenant status communications as legal evidence for subsequent breach notification obligations.

Detection — Review identity provider (IdP) and SSO logs for anomalous Canvas authentication events: logins from unexpected geolocations, off-hours access, bulk data export activity, or API calls inconsistent with normal user behavior. If Canvas is federated via SAML or OAuth, audit federation logs for unauthorized token issuance. Correlate with email gateway logs for any Canvas-originated phishing indicators targeting staff or students.

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-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Python or PowerShell to parse IdP authentication logs exported as CSV or JSON. For Azure AD: run `Get-AzureADAuditSignInLogs | Where-Object {$_.AppDisplayName -eq 'Canvas' -and $_.RiskLevelDuringSignIn -ne 'none'}`. For Okta: query the System Log API (`/api/v1/logs?filter=target.displayName+eq+"Canvas"`) and filter for `authentication.sessions.create` events from non-baseline geolocation ASNs. For Canvas API abuse, pull Canvas Data 2 daily dumps and grep for bulk `GET /api/v1/users` or `GET /api/v1/courses/:id/enrollments` calls with non-standard User-Agent strings consistent with scripted harvesting (ShinyHunters is known to use automated exfiltration tooling). For SAML federation, review your IdP's SAML assertion logs for assertions issued to Canvas service provider entity IDs outside business hours or for administrative role accounts.

Evidence: Capture raw IdP authentication logs (Okta System Log, Azure AD Sign-In Logs, or Google Workspace Admin Reports > Login) filtered to the Canvas application for a minimum 90-day lookback. Export Canvas API access logs via the Canvas Data 2 API or your institution's Canvas admin reporting panel — focus on endpoints that enumerate user PII: `/api/v1/accounts/:id/users`, `/api/v1/courses/:id/enrollments`, `/api/v1/users/:id/profile`. Preserve SAML assertion logs showing SP entity ID, NameID values, and session index attributes for any anomalous assertions. Capture email gateway (O365 Defender, Google Workspace, Proofpoint) logs for outbound or inbound messages referencing Canvas password reset flows or Canvas-branded phishing lures, consistent with ShinyHunters' post-breach credential harvesting and extortion campaigns.

Eradication — Force-rotate all Canvas administrative credentials and API tokens. Revoke and reissue any service account credentials used for Canvas integrations. Audit and remove any unrecognized OAuth application authorizations within your Canvas tenant. Review and tighten Canvas API access controls, particularly for third-party LTI integrations. No vendor-issued patch is available as of sourcing — follow Instructure's guidance when released.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Canvas administrative credential rotation can be performed directly in the Canvas admin console under Account > Admins; for API tokens, navigate to Account > Settings > Approved Integrations and revoke all listed tokens, then reissue only to verified, named individuals. For OAuth app auditing without automated tooling, run a Canvas API query: `curl -H 'Authorization: Bearer ' https://.instructure.com/api/v1/accounts/:account_id/scopes` and cross-reference all authorized OAuth clients against your known LTI integration inventory. For LTI integrations, navigate to Admin > Developer Keys and disable any key not in your documented integration register — use `canvas-lms-api-key-auditor` scripts available in the Canvas community GitHub repositories as a free enumeration aid.

Evidence: Before revoking any credential, document the full list of existing Canvas admin accounts (Admin > People, filtered to admin role), all active API tokens with their associated user accounts and creation dates, and all authorized OAuth/LTI developer keys. Export this inventory as a timestamped CSV. Capture Canvas audit log entries for any API token creation or OAuth authorization events in the prior 90 days to identify any tokens or applications created by a threat actor maintaining persistence — ShinyHunters is known to establish persistent API access as a dwell mechanism in SaaS environments.

Recovery — Before restoring full Canvas access, obtain written confirmation from Instructure that your institutional tenant has been isolated, assessed, and cleared. Validate that MFA is enforced for all Canvas admin accounts and API integrations. Monitor Canvas audit logs and IdP logs for at least 30 days post-clearance for re-access indicators consistent with T1078 (Valid Accounts) persistence.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-7 (Software, Firmware, And Information Integrity), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For MFA enforcement without enterprise IAM tooling: if Canvas is federated via Google Workspace or Azure AD, enforce MFA at the IdP level for the Canvas application specifically using Conditional Access (Azure) or Context-Aware Access (Google) policies — both are included in standard institutional licensing. If Canvas uses native authentication, enforce MFA in Canvas Admin > Settings > Security. For the 30-day monitoring requirement with no SIEM, configure a scheduled daily cron job or Task Scheduler entry to pull Canvas Data 2 authentication event exports and pipe through a grep filter for MITRE T1078 indicators: new admin-role logins, API calls from previously unseen IP ranges, or OAuth token issuance for accounts that were recently rotated. Alert on any match via email to the IR team.

Evidence: Before restoring full user access, capture a baseline snapshot of all current Canvas admin accounts, active API tokens, and authorized OAuth applications as a post-eradication clean-state reference. Retain Instructure's written tenant clearance notification. Establish a log retention baseline: preserve all IdP authentication logs and Canvas audit logs from the compromise window through at least 12 months post-incident to support regulatory breach notification obligations (FERPA, state-level student privacy statutes) and potential law enforcement referral, given ShinyHunters' history of law enforcement engagement.

Post-Incident — This incident exposes reliance on a single cloud-hosted SaaS provider for bulk PII storage without compensating controls. Conduct a third-party SaaS risk review covering data residency, breach notification SLAs, and tenant isolation guarantees. Evaluate whether student and staff PII volume stored in Canvas can be reduced. Review your institution's incident response plan for third-party SaaS compromise scenarios.

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-12 (Information Management And Retention), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For institutions without a formal third-party risk management program, use the HECVAT (Higher Education Community Vendor Assessment Toolkit) — a free, education-sector-specific vendor risk questionnaire — to conduct a structured reassessment of Instructure's security posture, focusing on sections covering breach notification timelines, multi-tenant isolation architecture, and data residency. For PII minimization in Canvas, audit Canvas course content and user profile fields using Canvas Data 2 exports and identify fields storing sensitive identifiers beyond what is required for LMS functionality. Document findings in a lessons-learned report per NIST 800-61r3 §4 and update your institution's IR plan to include a SaaS-compromise decision tree addressing tenant isolation verification, regulatory notification triggers, and communication templates for affected students and staff.

Evidence: For post-incident documentation, compile the full incident timeline from IdP authentication logs, Canvas audit logs, and Instructure communications. Quantify the PII exposure scope: total number of affected user records (student, faculty, staff) within your tenant, data categories involved (names, email addresses, institutional identifiers), and data retention periods. This documentation is required evidence for FERPA breach assessment, state student privacy law notifications (e.g., California SOPIPA, New York Education Law 2-d), and any institutional cyber insurance claims. Preserve all Instructure incident communications and your institution's internal IR timeline in tamper-evident, access-controlled storage.

Detection Guidance

Primary detection focus is unauthorized credential use and data access, not a network-layer exploit. Check the following: (1) Identity provider logs, filter for Canvas authentication events from new ASNs, countries, or IP ranges not associated with your institution; look for session token reuse from multiple source IPs. (2) Canvas audit logs, review for bulk enrollment data exports, unusual API query volume, or access to student data repositories outside normal administrative patterns. (3) Email gateway and SIEM, watch for phishing lures referencing Canvas, password reset requests, or OAuth consent phishing targeting Canvas credentials. (4) Behavioral indicators aligned to T1078: valid user accounts accessing Canvas outside business hours or from endpoints not enrolled in your MDM. (5) If Canvas API tokens are used in integrations, audit token usage logs for calls inconsistent with integration scope. No confirmed IOCs (hashes, IPs, domains) have been publicly attributed to this specific campaign as of available sourcing.

Framework Mappings

MITRE-ATTACK

- **T1539** — Steal Web Session Cookie
- **T1078** — Valid Accounts
- **T1589.002** — Email Addresses
- **T1567** — Exfiltration Over Web Service
- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1098** — Account Manipulation
- **T1530** — Data from Cloud Storage
- **T1555** — Credentials from Password Stores
- **T1657** — Financial Theft

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement

- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design
- **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
- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management
- **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.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1539	Steal Web Session Cookie	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1589.002	Email Addresses	Reconnaissance
T1567	Exfiltration Over Web Service	Exfiltration

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1098	Account Manipulation	Persistence
T1530	Data from Cloud Storage	Collection
T1555	Credentials from Password Stores	Credential-Access
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/shinyhunters...	T3
Canvas Online Learning Platform Disabled After Breach by Hackers	https://www.nytimes.com/2026/05/07/education/canvas-hacked-down-dat...	T2
Instructure hacker claims data theft from 8,800 schools, universities	https://www.bleepingcomputer.com/news/security/instructure-hacker-c...	T3
Canvas (Instructure) LMS seems to have been hit by ransomware	https://www.reddit.com/r/sysadmin/comments/1t6m7e0/canvas_instructu...	T3
ShinyHunters' Instructure Canvas LMS and Vimeo Breaches Impact ...	https://hackread.com/shinyhunters-instructure-canvas-lms-vimeo-data...	T3

Generated 2026-05-09 06:26 UTC by TJS Security Command Center