stealthcyber

HACKERS | DEFENDERS | ADVISORS

CTI Report:

Instructure (Canvas LMS) Cyberattack

May 8 2026

PREPARED BY

Alessandra Melo

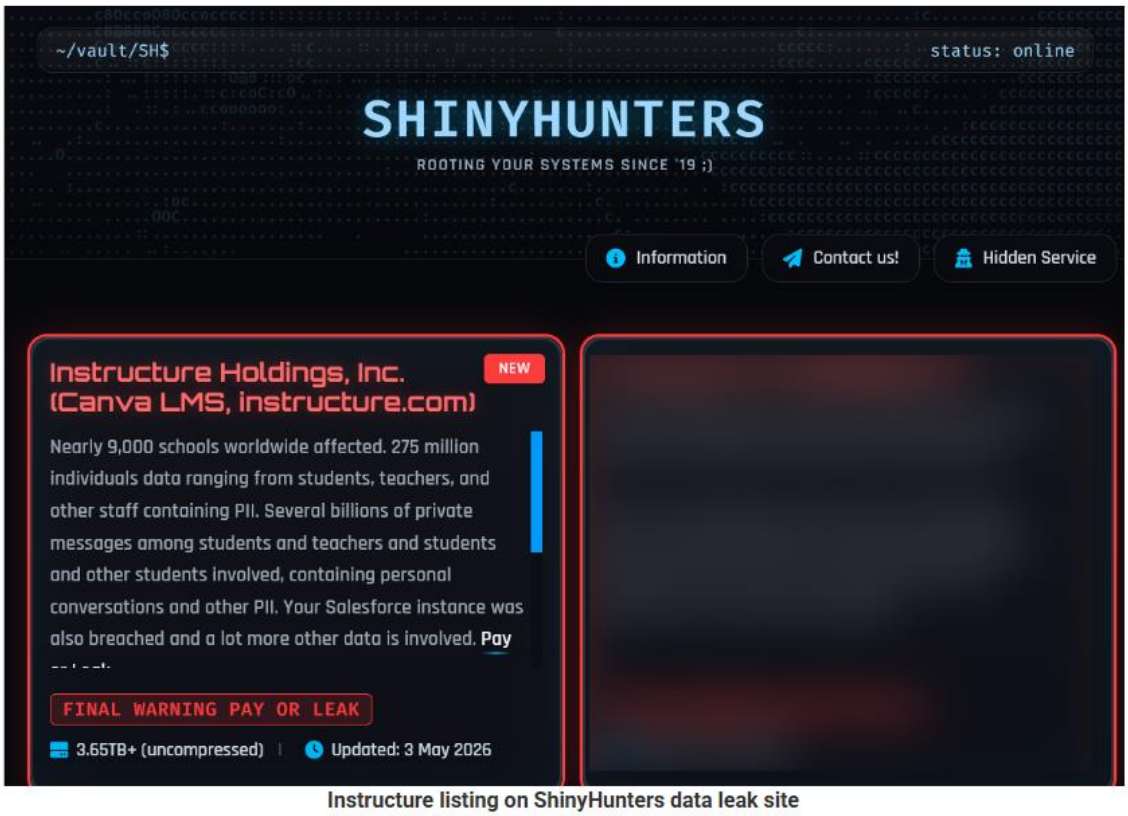
Global Senior Security Engineer

Executive Summary

In May 2026, the Canvas learning management system (LMS), operated by **Instructure**, was the victim of a massive, multi-stage cybersecurity and extortion campaign orchestrated by the criminal group **ShinyHunters**. The group claims to have exfiltrated 3.65 TB of data belonging to approximately 275 million users across 9,000 schools and 15,000 institutions worldwide. The attack has caused global operational disruptions, including platform-wide outages and the defacement of institutional login portals with ransom demands.

3.65 TB OF EXFILTRED DATA	275M INDIVIDUALS AFFECTED
~9k / ~15k SCHOOLS / INSTITUTIONS IMPACTED	2nd BREACH IN 2026

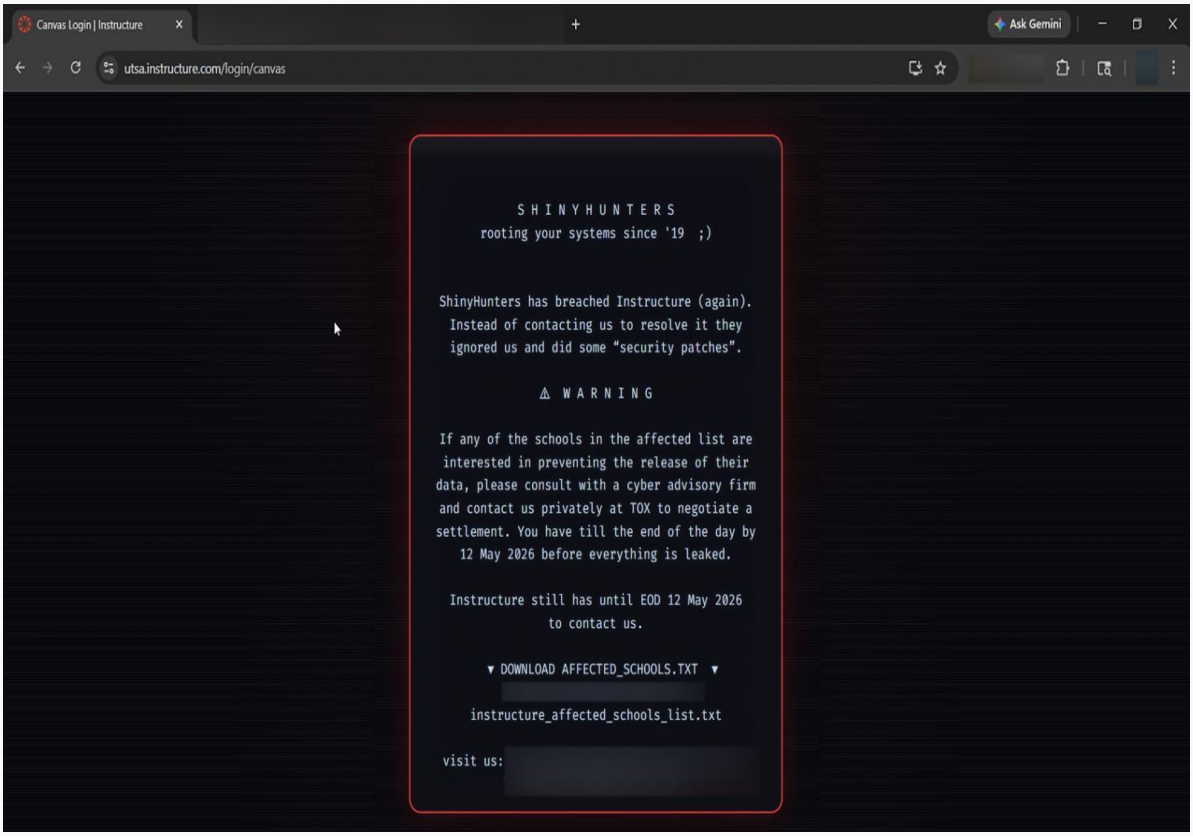
The defacement wasn't the start of the attack. It was a second move in an extortion campaign that began days earlier. On May 3, 2026, ShinyHunters added Instructure to its dark-web leak site under a "PAY OR LEAK" headline and posted 3.65 TB of data as proof. The group threatened to release billions of private messages between students and teachers if Instructure didn't pay by May 6.



Instructure listing on ShinyHunters data leak site

Executive Summary

Instructure refused to negotiate and rolled out security patches instead. ShinyHunters responded by exploiting a different vulnerability and defacing the Canvas login pages of hundreds of universities on May 7. Instructure quickly took Canvas, Canvas Beta, and Canvas Test offline for maintenance, but the defacement was visible for about 30 minutes before that happened. The message on the login pages read: *"ShinyHunters has breached Instructure (again). Instead of contacting us to resolve it they ignored us and did some 'security patches'."* The group also extended the deadline to end of day on May 12, after which they said the full dataset would be leaked.



Defacing public login pages and reaching out directly to journalists at TechCrunch shows a clear shift in tactics. ShinyHunters moved from quiet data theft to loud public pressure, using Instructure's own customers (schools, faculty, and students) as leverage against the company.

Incident Overview

Breached Entity

Instructure (Canvas LMS)

Attribution

ShinyHunters (aka UNC6240, UNC6040, UNC6661)

Incident Type

Data theft extortion utilizing SaaS misconfigurations and identity compromise.

Data Compromised

- Names
- Institutional email addresses (.edu)
- Student identification numbers
- Private messages between students and faculty

Timeline

- **April 30:** Initial disruption detected; Instructure identifies failures in API-dependent tools.
- **May 1:** Official confirmation of a cybersecurity incident; forensic experts engaged.
- **May 3:** ShinyHunters lists Instructure on their "Scattered LAPSUS$ Hunters" Data Leak Site (DLS).
- **May 7:** Massive escalation; approximately 330 institutional login portals are defaced with ransom messages

Attack Methodology

The attack chain follows a pattern ShinyHunters has refined throughout 2025 and 2026 across victims like Cisco, Allianz Life, Odido, and Wynn Resorts. The same playbook keeps working because it bypasses the controls most organizations rely on (MFA, EDR, perimeter defenses) by abusing legitimate authentication flows instead of breaking them.

NOTE: Instructure has not published a forensic report, so parts of this section are inferred from ShinyHunters' documented operations against similar SaaS environments.

1

Initial Access

Attackers likely gained entry by exploiting a combination of misconfigured "Free-For-Teacher" accounts and API key vulnerabilities. Evidence suggests the group leveraged vishing (voice phishing) to compromise internal administrative accounts, allowing them to register their own Multi-Factor Authentication (MFA) devices and bypass perimeter security.

T1566.004 · T1078.004 · T1556.006 · T1528

2

Lateral Movement & Exfiltration

Once inside, the actors pivoted to Instructure's Salesforce instance to harvest customer records and metadata. They used tools like AuraInspector (internally dubbed "RapeForce") to identify misconfigured Salesforce Experience Cloud guest profiles and programmatically exfiltrate data via Salesforce Object Query Language (SOQL) queries.

T1538 · T1526 · T1213.005 · T1098.001

3

Extortion & Pressure Tactics

The May 7 defacement campaign utilized HTML injection to replace legitimate login pages with a ransom demand. The message set a final deadline of May 12, 2026, for settlement negotiations. The timing was strategically chosen to maximize chaos during the examination period, increasing the likelihood of institutional pressure on the vendor.

T1491.002 · T1657 · T1485

Who is ShinyHunters?

ShinyHunters (aka UNC6240, Bling Libra, and Scattered LAPSUS$ Hunters) is a prolific, financially motivated cybercriminal group active since early 2020. The group specializes in mass data exfiltration and high-pressure extortion, primarily targeting enterprise Software-as-a-Service (SaaS) and cloud environments.
The group is sector-agnostic but prioritizes high-value datasets. Some industries impacted by the group: Education, Technology & SaaS, Finance, Insurance and Entertainment.

Operational Methodology

ShinyHunters operates through a highly specialized ecosystem, often outsourcing initial access to "contractor" clusters while retaining control over the final exfiltration and negotiation phases.

- **Identity-Centric Targeting:** Rather than exploiting infrastructure zero-days, they focus on compromising the identity layer: Single Sign-On (SSO) and Multi-Factor Authentication (MFA).
- **Vishing & Social Engineering:** They frequently employ "voice phishing" (vishing), where operators impersonate IT help desk staff to trick employees into providing MFA codes or authorizing malicious applications.
- Supply Chain & Third-Party Abuse: They aggressively target third-party SaaS integrations (e.g., Gainsight, Salesloft, Snowflake) to gain cascading access to hundreds of downstream customer environments.
- **Extortion Model:** Operating under a "Pay or Leak" model, they maintain the Scattered LAPSUS$ Hunters Data Leak Site (DLS) to shame victims. Negotiations typically occur via Tox, and they use file-sharing sites like LimeWire to host proof-of-breach data.

Technical Tactics & Tooling

Initial Access & Persistence

- MFA Bypass: Once a target is on a phishing site, attackers capture SSO credentials and real-time MFA codes to register their own devices for persistent access.
- Malicious Connected Apps: They often register fake or modified applications (e.g., a malicious version of *Salesforce Data Loader) to maintain programmatic access to CRM data.

Exfiltration & Reconnaissance

- Cloud Enumeration: The group uses tools like AuraInspector (internally called "RapeForce") to scan for misconfigured Salesforce Experience Cloud sites and query API limits.
- Data Aggregation: Legitimate administrative tools like Rclone, Amazon S3 Browser, and WinSCP are used to exfiltrate massive datasets from cloud storage.

Custom Malware

- SHINYSPIDER: A Go-based ransomware family in development as of late 2025, capable of encrypting local/network drives and specifically targeting VMware ESXi environments.

Impact Assessment

Global disruption of academic operations has been confirmed. Major institutions including Harvard, Stanford, Oxford, and Cambridge are on the group's alleged victim list. In the U.S., universities such as UMass Lowell and Brown University were forced to postpone final exams.

For Impacted Schools and Institutions

Operational: The Canvas outage hit during spring finals, blocking assignment submissions and exams at thousands of institutions. Every Canvas integration (gradebooks, plagiarism tools, library systems) needs to be re-authorized using Instructure's new timestamped API keys, which is days of cleanup even when it goes smoothly.
Security: The exposed dataset (names, emails, student IDs, Canvas messages) is a phishing goldmine. Attackers now have real student names, teacher names, course titles, and internal messages to build convincing lures. Expect a sustained spike in targeted social engineering. Canvas messaging often contains grade disputes, accommodation requests, mental health check-ins, and safeguarding conversations, most of which had no retention policy. Whatever lived there for years is now potentially leaked.
Compliance: The breach likely triggers reporting requirements under FERPA (US), GDPR (EU/UK), and similar student data protection laws. Institutions that used Canvas messaging for safeguarding-related conversations may have additional obligations under child protection laws.
Financial and Reputational: Direct costs include incident response, legal review and identity protection services. Indirect costs include staff time pulled from other priorities, higher insurance premiums, and trust damage with parents and faculty asking why sensitive messages were retained at all.

For Parents and Students

What was exposed: your name, email, student ID, and Canvas messages. What was not (per Instructure): passwords, date of birth, government ID, or financial information.
What to watch for: emails claiming to be from your school, messages pretending to be from a teacher, phone calls from "IT helpdesk" asking for codes, and scams referencing real classes, assignments, or grades. If anything feels off, slow down. Go directly to the official site and call the school using a number you already trust.
Privacy: Anything you wrote in Canvas messages may be in the leaked data. If you're worried about specific conversations, contact your school's privacy officer.
For parents of younger students: Children are easy phishing targets, especially when scams reference real teachers. Tell your kids not to click links, not to share codes, and to come to you when something feels weird. If the school used Canvas for counseling or special education communications, reach out directly.

Recommendations

A note before we get to recommendations: do not pay the ransom. Paying does not guarantee the data is deleted, does not prevent it from being resold to other criminal groups, and directly funds the next attack Law enforcement agencies in the US, UK, EU, and most other jurisdictions consistently advise against payment, and in some cases payment may itself violate sanctions law.

For Impacted Schools and Institutions

Immediate :

- Force password reset and revoke active session tokens across Canvas and connected SaaS apps (Salesforce, Google Workspace, Microsoft 365).
- Revoke all privileged API keys and OAuth tokens, including those tied to the "Free-For-Teacher" ecosystem. Re-authorize integrations using Instructure's new timestamped keys.
- Block OAuth Device Code Flow in Microsoft Entra ID via Conditional Access for any user not on shared meeting-room hardware. Salesforce admins should do the same on connected apps.

Short-Term:

- Send phishing alerts to staff and students. Attackers have real course names and identities to build convincing lures.
- Lock down the helpdesk: managed devices only, phishing-resistant MFA, and out-of-band verification for password and MFA reset calls.

Long-Term:

- Move all admin and high-value accounts to FIDO2 hardware keys or passkeys.
- Build a full API key inventory (owner, scope, last-used date) with automate rotation,.
- Set retention policies on Canvas messages and audit free-text fields for sensitive content. The data you don't store is the data ShinyHunters can't leak.
- Run a vishing tabletop exercise. Walk through the scenario where a fluent caller asks an employee to enter a code at microsoft.com/devicelogin.

For Parents and Students

Immediate: Change your Canvas password and use a unique one. Turn on multi-factor authentication, preferably an authenticator app over SMS. Review recent logins and messages for anything unfamiliar.

Short-Term: Treat any unexpected school-related email, text, or call as suspicious until verified through official channels. Avoid sending sensitive information through Canvas messages or school email until things stabilize. Ask your school what specific data of yours was affected.

Long-Term: Sign up for Have I Been Pwned (haveibeenpwned.com) using both your school and personal emails. Be skeptical of phone calls claiming to be from IT, especially ones asking you to enter codes on a Microsoft or Google login page. **For parents:** if your child used Canvas for sensitive conversations (counseling, accommodations, safeguarding), check in with the school about what was exposed.

stealthcyber

HACKERS | DEFENDERS | ADVISORS

Thank you

For questions or further clarification,
please contact us at:

Stealth Cyber Pty Ltd
contact@stealthcyber.io

Gold Coast AU | SP Brazil | Texas USA

END OF REPORT