PROTOS LABS

75 Ayer Rajah Crescent,
#02-06, Singapore 139953.

ShinyHunters / Instructure (Canvas) Incident

CISO Information Pack — Education Sector

Classification	TLP:CLEAR
Prepared by	Protos AI Threat Intelligence
Version	v2 — 10 May 2026
Reporting window	29 April 2026 → 10 May 2026 (incident); broader actor profile draws on 2020–2026 reporting
Audience	CISOs and security leaders in the education sector

How to use this pack

This pack is structured so a CISO can read the first two sections in five minutes and brief the executive team, then hand the rest to their security team for action. It is built from Protos AI investigation work plus open-source corroboration as of 10 May 2026. Where claims are based on actor statements rather than vendor or independent confirmation, that distinction is preserved.

The pack covers four things:

1. **Latest position** — what is confirmed, what is claimed but unverified, and what changed in the last 72 hours.
2. **What this means for your institution** — risk framing for non-Instructure customers as well as direct ones.
3. **Threat actor context** — who ShinyHunters are, how they have evolved, and why the education sector is a recurring target.
4. **Recommended actions and supporting technical material** — Contained in accompanying technical details document.

1. Latest position (as of 10 May 2026)

Timeline of the incident

Date	Event
25 April 2026	Initial intrusion (Instructure-stated incident date)
29 April 2026	Instructure detects unauthorized activity in Canvas; revokes attacker access
30 April 2026	Additional suspicious access discovered; further revocations and "underlying vulnerability" addressed; Canvas Data 2 and Canvas Beta placed under maintenance after disruption to API-key-dependent tools
1 May 2026	Instructure CISO Steve Proud publicly confirms a "cybersecurity incident perpetrated by a criminal threat actor"; outside forensics engaged; Canvas Test also enters maintenance
2 May 2026	Vendor states the incident is "contained"; exposed data categories disclosed
3 May 2026	ShinyHunters lists Instructure on its Tor-based leak site with "PAY OR LEAK" and an initial 6 May deadline
5 May 2026	Instructure begins notifying impacted schools
6 May 2026	Instructure states it is "not seeing any ongoing unauthorized activity"

Confirmed Exposed Data:

- **Names, email addresses (mostly institutional .edu addresses), student ID numbers, and Canvas inbox messages between users.**

75 Ayer Rajah Crescent,
#02-06, Singapore 139953.

Canvas Breach Confirmed by Instructure

- Instructure, the company behind SaaS platform Canvas, stated the cyber incident date as 25 April 2026, with detection on 29 April.
- The unauthorized actor exploited an issue related to Instructure's **Free-For-Teacher account program** — the same issue that enabled the second-wave 7 May intrusion. The program has now been permanently shut down.
- Privileged credentials were revoked, API keys rotated, and law enforcement engaged.
- Instructure confirmed only the following exposed data: **names, email addresses (mostly institutional .edu addresses), student ID numbers, and Canvas inbox messages between users.**
- Per their most recent statement, no evidence that passwords, dates of birth, government identifiers, or financial information were exposed. This may be revised as the investigation continues.
- Canvas was fully restored on 8 May 2026 following the Free-For-Teacher shutdown.
- **As of 8 May, Instructure had been removed from the ShinyHunters leak site.** Threat analysts note this typically indicates either ongoing negotiation or payment, though Instructure has not publicly confirmed either. CISOs should factor this uncertainty into user-notification language.

Claimed by the threat actor (unverified)

- An actor using the ShinyHunters name claimed responsibility on 3 May 2026 via its Tor-based leak site; the listing was reproduced by Ransomware.live.
- The claim references approximately 3.65 TB of data, ~275 million records, and ~8,809 schools/institutions. **These figures are actor-supplied and have not been independently verified.** Historical ShinyHunters claims have frequently been inflated; one ShinyHunters representative subsequently told TechCrunch the unique email count is closer to 231 million.
- The 7 May login-page defacement messages instructed schools to "contact us privately at TOX" — referring to Tox, a peer-to-peer encrypted messaging protocol used by the group for negotiation. The specific Tox ID is the actionable indicator; "TOX" itself is the channel, not a token.

Confirmed second breach in eight months

This is **Instructure's second ShinyHunters breach in eight months**, but the attack surfaces differ:

- **September 2025**: Vishing-led social engineering against Instructure's Salesforce instance — peripheral business infrastructure, no Canvas product data. Part of a broader campaign that allegedly exfiltrated ~1.5 billion Salesforce records from ~760 organisations via the Salesloft Drift supply-chain attack.
- **May 2026**: Direct exploitation of the Free-For-Teacher program in the Canvas platform itself — institutional course data, student information, and private communications.

CISOs evaluating Instructure (or any SaaS vendor) on this campaign should request documentation on what changed after September 2025 and why those controls did not prevent the May 2026 incident.

What is not yet known

- Tenant-by-tenant scope. Each Canvas customer must confirm with Instructure which of its specific data, integrations, and users were affected.
- Final dataset scale. The actor's 275M / 8,809-schools figures have not been independently corroborated.
- Whether further data was taken from the second-wave (7 May) login-page activity beyond the original intrusion.

75 Ayer Rajah Crescent,
#02-06, Singapore 139953.

2. Executive summary for non-technical stakeholders

The headline. Canvas — the learning management system used by 41% of higher-education institutions in North America and over 8,000 institutions globally — has been hit by a data-extortion group called ShinyHunters. Identity data and private messages are confirmed exposed. The most realistic near-term threat to your institution is not encryption of your systems but a wave of highly credible phishing emails and phone calls aimed at your students, faculty, and IT staff, using context stolen from Canvas.

Why it matters even if you are not an Instructure customer. ShinyHunters has spent the last 18 months systematically targeting the education and edtech sector, and the broader SaaS ecosystem the sector depends on. Confirmed victims in this campaign series include Instructure (twice), McGraw Hill (April 2026, ~13.5M emails confirmed by Have I Been Pwned), Infinite Campus (March 2026, via its Salesforce instance), and individual universities including the University of Pennsylvania, Princeton, and Harvard (late 2025). The recurring infrastructure target is Salesforce — many edtech vendors run customer data on Salesforce, and a single Salesforce or analytics-vendor compromise has cascaded across the sector multiple times.

What to do this week. Brief your IT helpdesk and admin staff on a specific phone-based social-engineering technique (vishing) the group is using to bypass MFA. Inventory and rotate developer keys, OAuth tokens, and service-account credentials tied to Canvas and Salesforce. Scan code repositories for exposed credentials. Preserve logs. Issue a measured user notification that focuses on what is confirmed, not what the actor claims.

Risk level: High. This is driven by the combination of personally identifiable information, private message content, and educational context — not by ransomware. The follow-on phishing risk is the live threat.

75 Ayer Rajah Crescent,
#02-06, Singapore 139953.

3. What does this mean for your institution

If you are an Instructure customer

You are a directly affected party. Your immediate priorities are validating vendor guidance, inventorying your Canvas developer keys and LTI integrations, rotating or reauthorising affected credentials / tokens, hardening privileged access, preserving logs for forensic and regulatory needs, and preparing a measured user notification. See section 5 for sequenced actions.

You should also specifically check whether your tenant ever used or interacted with Free-For-Teacher accounts — these have now been permanently shut down, and any data flows dependent on them need to be unwound.

If you are not an Instructure customer

You are still affected by the broader campaign in three ways:

1. **Adjacent vendor exposure.** Confirmed ShinyHunters victims also include McGraw Hill (April 2026), and Infinite Campus (March 2026, via its Salesforce instance). Most institutions hold student or staff data with at least one of these. Run the same key-rotation and integration-audit process against any edtech vendor that has disclosed an incident in the past 18 months, and pay particular attention to anything that touches Salesforce.
2. **Indirect data exposure via partners.** Affiliated schools, alumni systems, research partners, and third-party tutoring/proctoring services may be Canvas customers whose breach exposes your population indirectly.
3. **Sector-wide phishing risk.** The data exposed in this campaign — names, emails, student IDs, message content — fuels phishing campaigns targeted at the education sector generally, not just Canvas users. Expect attempts that reference plausible course names, instructor names, or message threads to surface across the sector for the next several months.

What will probably happen next

In the order of likelihood:

- Targeted phishing emails referencing internal course or instructor names, sent to students and staff, attempting credential harvest or fraudulent payment requests.
- Vishing calls to IT helpdesks and finance/admin staff, using context from leaked data to appear legitimate.
- Impersonation of faculty in messages to students requesting urgent action (grade changes, fee payments, gift-card requests).
- Further leak-site postings or sample releases as negotiation pressure escalates beyond 12 May.
- (Lower probability, longer time horizon) Follow-on intrusions where credentials harvested in this campaign are used to access other systems, particularly cloud services where the victim reused passwords.

FBI guidance

The FBI has publicly advised anyone who may be affected: do not engage with anyone claiming to have your data, do not respond to demands or send payments, and verify any unsolicited email, call, or text claiming to be from your school or learning management system through known channels before responding. This is useful framing to incorporate into your own user notifications.

4. Threat actor context: who ShinyHunters are

Behavioural profile

ShinyHunters is a financially motivated data-extortion actor that emerged in 2020. The operating model emphasises public coercion rather than encryption: leak-site listings, staged sample releases, deadline-based negotiation pressure, and login-page defacement to amplify visibility. Until late 2025 ransomware was not part of the playbook (see "evolution" below).

The group has demonstrated effective tradecraft against SaaS and cloud-hosted environments, with particular skill at exploiting integration pathways — OAuth tokens, API keys, third-party connectors — rather than compromising endpoints.

Description of the actor in current reporting: a loose affiliation of teenagers and young adults based in the US and UK. Sebastien Raoult, an alleged member, was sentenced to three years' prison and over $5 million in restitution by the US Department of Justice in 2024.

The SLSH alliance — important context

ShinyHunters now operates within **Scattered LAPSUS$ Hunters (SLSH)**, a situational alliance fusing ShinyHunters, LAPSUS$, and Scattered Spider tradecraft. The umbrella sits inside the broader "Com" cybercrime ecosystem.

Mandiant currently tracks the activity across multiple UNC clusters that overlap with or feed ShinyHunters-branded extortion: **UNC6040, UNC6240, UNC6661, and UNC6671**. The Bling Libra cluster (Unit 42's designation for the same actor) is also part of this picture.

For CISOs, that means when you read about "ShinyHunters" in the press, you may be reading about several overlapping or affiliated clusters using shared infrastructure, branding, and extortion tooling. Defences calibrated to the brand alone may miss adjacent activity.

Targeting pattern

Recent ShinyHunters and SLSH activity shows recurring overlap with:

- **Salesforce** — the central recurring infrastructure target. The Salesloft Drift supply-chain attack (August 2025), the Salesforce Aura campaign, and direct vishing-driven Salesforce intrusions are all linked to this group. The actor claims ~1.5 billion Salesforce records across ~760 organisations; independent reporting confirms at least ~400 affected Salesforce customers in the campaign cluster. The McGraw Hill, Infinite Campus, and ADT intrusions are Salesforce-rooted. ShinyHunters has also claimed that Instructure's Salesforce instance was breached in May 2026, but Instructure has not confirmed this; the vendor-confirmed vector is the Canvas Free-For-Teacher account program (see Section 1).
- **Analytics and data-pipeline supply-chain pivots.** In April 2026 ShinyHunters compromised **Anodot** (a third-party analytics provider) and used stolen authentication tokens to pivot into customers' **Snowflake** and **BigQuery** environments. Vimeo is the publicly named victim of that pivot (~119,200 unique emails, 106GB leaked after extortion failed). ShinyHunters told BleepingComputer it had stolen data from "dozens of companies" via Anodot tokens. The earlier 2024 Snowflake customer campaign (Ticketmaster ~560M records, AT&T call/text metadata, Santander 30M, Neiman Marcus, and others) is also attributed to ShinyHunters.

- **Identity providers.** Okta is the primary identity-provider target via vishing-driven AiTM attacks; the group has also moved laterally into Microsoft 365 and Google Workspace environments via stolen SSO sessions.
- **Education and edtech.** Confirmed ShinyHunters victims: Instructure (September 2025 + May 2026), Infinite Campus (March 2026, via Salesforce), McGraw Hill (April 2026, via a Salesforce misconfiguration), and the late-2025 university intrusions at Penn, Princeton, and Harvard.
- **Datasets containing PII and communications content** — the mix that makes downstream phishing more credible.

The overlap is at the level of *shared target platforms and integration pathways*, not shared C2 infrastructure. This means defences focused on Salesforce hygiene, analytics-vendor token management, identity-provider controls, and integration least-privilege transfer well across incidents.

Evolution: three phases

The threat has changed materially over the last 24 months. Defences calibrated to the 2024 version of this group will miss the 2026 version.

Phase 1 (historical, 2020–2024): Stealing OAuth keys and AWS credentials from public GitHub repositories, using them to bulk-export cloud databases, and reselling on underground markets. The Tokopedia and Microsoft GitHub incidents are early examples. By mid-2024 the credential-theft model expanded into the Snowflake customer campaign (Ticketmaster, AT&T, Santander and others), using credentials harvested from infostealer logs rather than GitHub.

Phase 2 (current, 2025–2026): A shift in initial access from technical exploitation to phone-based social engineering. The primary entry technique is now a vishing call: an attacker impersonates IT, creates urgency around an SSO reset or MFA update, and uses a real-time adversary-in-the-middle (AiTM) phishing kit to relay credentials and MFA codes. Documented post-compromise behaviour includes registering an attacker-controlled device for MFA, then immediately deleting the "Security method enrolled" notification email from the victim's mailbox to avoid detection. Mandiant, Okta, and Sophos have all published detailed analyses of this technique throughout late 2025 and early 2026.

Phase 3 (emerging): A purpose-built ransomware family, **ShinySp1d3r** (also written Sh1nySp1d3r), tracked by Unit 42 under the Bling Libra cluster name, was first observed in November 2025. **Discovered samples to date are Windows PE binaries**; a Linux variant has been announced by the group but not yet observed in samples. The encryptor was reportedly built from scratch and is still under active development. This means the group is moving toward combined data-theft *and* encryption, which expands the relevant attack surface beyond pure SaaS data exfiltration.

5. Sources

Vendor: Instructure status communications, CISO Steve Proud's update log, application-key timestamp notice, community posts.

Vendor research / threat intelligence:

- Mandiant / Google Threat Intelligence Group — vishing campaign analysis, UNC cluster tracking (UNC6040, UNC6240, UNC6661, UNC6671), defensive guidance for ShinyHunters-branded data theft
- Palo Alto Networks Unit 42 — Bling Libra coverage, ShinySp1d3r ransomware IOC feed (21 November 2025), Scattered LAPSUS$ Hunters updates
- Okta Threat Intelligence — vishing-enabled phishing-kit analysis

- Sophos Counter Threat Unit — campaign attribution and infrastructure analysis
- Bitdefender — technical advisory on Free-For-Teacher account compromise

News reporting: CNN, Time, BleepingComputer, TechCrunch, Inside Higher Ed, KSL, WRAL, NBC, ABC News (Australia), CBS Sacramento, ABC15. Coverage from student newspapers including the Harvard Crimson, the Duke Chronicle, and the Daily Pennsylvanian.

OSINT and analysis: SOCRadar, Memeburn, Ogun Security, Ransomware.live, Have I Been Pwned breach ingestion records, the Wikipedia 2026 Canvas security incident article (which compiles primary sources).

Underlying Protos AI investigations:

1. *ShinyHunters / Instructure (Canvas) Incident — May 3–6, 2026*
2. *ShinyHunters — Threat Actor Dossier: Instructure/Canvas Campaign (Apr 06 → May 06 2026)*
3. *ShinyHunters Defense Advisory* (university defensive layering)
4. *ShinyHunters / Bling Libra — TTP & IOC Monitoring Reference*

Prepared by Protos AI Threat Intelligence. TLP:CLEAR — share freely within and between organisations to support sector defence. Update as Instructure publishes additional forensic findings, particularly after the 12 May 2026 leak deadline.