PROTOS LABS

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

ShinyHunters / Instructure (Canvas) Incident

Technical Details: 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 document

This technical details document is structured for the security team for action and is built from Protos AI investigation work plus open-source corroboration as of 10 May 2026.

This document covers the following:

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. **Recommended actions and supporting technical material** — prioritised remediation, detection guidance, and TTP/IOC references for security teams.
4. **Threat actor context** — who ShinyHunters are, how they have evolved, and why the education sector is a recurring target.

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.**

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. 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.

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

3. Recommended actions

Priority 1 — This week

#	Action	Why	Owner
1	Validate vendor guidance and subscribe to official Instructure status updates	Avoid amplifying unverified actor claims; align actions with forensic findings	IT Security & Leadership
2	Inventory developer keys, LTI apps, and Canvas integrations; identify keys with reissue timestamps from the vendor; check any Free-For-Teacher account exposure	Cannot prioritise rotation without knowing what is in scope	Platform Admins
3	Rotate or reauthorise affected application keys, OAuth secrets, and service-account credentials; revoke obsolete keys	Vendor remediation patterns indicate credentials/tokens were likely abused	Platform Admins
4	Brief IT helpdesk and admin staff on the vishing technique described in section 3, including a verbal verification protocol (call back via the directory, not a number provided on the call)	Vishing is the primary 2026 initial-access technique; helpdesk staff are the primary target	IT Security
5	Harden privileged accounts: verify MFA, review recent privileged activity, temporarily restrict unnecessary privileged API access	Limits potential secondary abuse and lateral movement	IT Security
6	Require out-of-band approval (manager or IT Security) for any new MFA device enrollment; alert on deletion of "Security method enrolled" notifications	Single control that breaks the documented Mandiant-reported persistence pattern	IT Security
7	Audit your Salesforce instance and any other SaaS connected to your IdP for anomalous OAuth grants, new connected apps, and bulk-export jobs in the last 30 days	Salesforce is the recurring SLSH infrastructure target across this campaign series	Platform Admins & IT Security
8	Preserve logs (API, access, messages, audit trails, IdP logs) and coordinate with Legal/Privacy on retention	Required for forensic investigation and regulatory notification obligations	IT Security & Legal
9	Issue user notification focused on confirmed facts, currently known affected data types, the absence of confirmed password/financial exposure (if vendor position holds), and concrete anti-phishing guidance	Calm, accurate, actionable communication reduces panic and improves user vigilance	Communications & Legal

Priority 2 — Next 30 days

- Coordinate with third-party LTI vendors integrated with your Canvas tenant to confirm integration status and reauthorisation steps. Common categories include content publishers, video platforms, plagiarism-detection services, proctoring tools, and external authoring tools.
- Hunt for anomalous bulk exports from Canvas Data 2, analytics connectors, and Salesforce. A single account generating multiple full-dataset exports in a 24-hour window is the canonical signal.
- Reset OAuth client secrets where advised and adopt least-privilege/scoped credentials where the vendor supports them.
- Scan all code repositories — including private ones — for exposed AWS keys, OAuth tokens, API secrets, and service-account credentials. Tools: GitGuardian, truffleHog, GitHub native secret scanning. Rotate anything found, including historical exposures.

- Increase monitoring for phishing, enrollment changes, grade changes, and anomalous API activity for 60–90 days.
- Search dark-web feeds (via vetted partners or law enforcement) for leak-post metadata, sample files, and negotiation contacts.
- Assess your exposure to any other ShinyHunters-targeted edtech vendor (McGraw Hill, Infinite Campus) and request their post-incident control attestations.

Priority 3 — Strategic improvements

- **Phishing-resistant MFA.** Move from TOTP and SMS to FIDO2/WebAuthn passkeys or certificate-based authentication for privileged users at minimum. AiTM proxies can relay TOTP and SMS in real time; they cannot relay cryptographically domain-bound authenticators.
- **Automated app-consent inventory and expiry** for third-party integrations, particularly OAuth grants into Salesforce and your IdP.
- **Session limits and anomaly scoring** on API usage patterns for high-value data endpoints.
- **Network segmentation and Zero Trust access** between research data, student records, financial systems, and administrative systems.
- **Data minimisation on SaaS platforms** — audit what data each vendor actually needs and stop sending what is not operationally necessary.
- **Backup integrity for research data.** With ShinySp1d3r in development and a Linux variant announced, confirm offline or immutable backups exist for HPC and research-computing assets, and test restoration end-to-end.
- **Tabletop exercises** specifically simulating third-party SaaS-vendor incidents and vishing-driven account takeover.
- **Vendor concentration review.** This incident is, structurally, a vendor-concentration failure — a single SaaS provider holding records on hundreds of millions of users across thousands of institutions, compromised through one path, exposes every dependent institution simultaneously. Map your critical SaaS vendors and the blast radius of a compromise of each.
- **Threat intelligence subscriptions** covering ShinyHunters / Bling Libra / SLSH IOCs; establish direct channels with Palo Alto Unit 42, Mandiant, and (for Singapore institutions) CSA SingCERT.

4. Detection and hunt guidance

Priority hunt areas

- **OAuth and API token abuse.** Anomalous token refreshes, unexpected application consents, service principal activity outside maintenance windows.
- **Identity provider anomalies.** New device enrollments, especially from unfamiliar IPs or outside business hours; impossible-travel events; token replay indicators.
- **Notification suppression.** Email rules created or login-notification emails (particularly Okta "Security method enrolled" emails) deleted within 10 minutes of a new authentication event from an unfamiliar IP — documented ShinyHunters post-compromise behaviour from Mandiant's UNC6661 analysis.
- **Bulk data movement.** Compressed export jobs, elevated bytes_out, repeated full-dataset pulls — particularly for education-related datasets.
- **User-facing defacement / extortion artifacts.** Login-page text injection, HTTP 200 responses serving anomalous messages, maintenance-page modifications. The 7 May Canvas wave used login-page defacement specifically.

Detection rules (adapt to your environment)

These map directly to Mandiant- and Unit 42-published TTPs:

1. **AiTM MFA bypass:** Successful MFA authentication followed within 5 minutes by a new MFA device enrollment, from an IP not previously seen for that user.
2. **Notification suppression post-login:** Email rule created or login-notification email deleted within 10 minutes of authentication from an unfamiliar IP.
3. **OAuth token anomaly:** OAuth token used from an IP or user-agent inconsistent with the token's registration context.
4. **Bulk export from LMS/CRM:** Single account generating more than 3 full-dataset exports in 24 hours, or any export exceeding a defined row/size threshold.
5. **GitHub secret exposure:** Any commit to an institution-affiliated repository containing patterns matching AKIA[0-9A-Z]{16}, private key headers, or OAuth token formats.
6. **Vishing-correlated authentication:** Authentication event from an unfamiliar IP within 30 minutes of an inbound call to an IT-helpdesk number, where the helpdesk ticketing system shows no corresponding ticket. Requires phone-system + ticketing + IdP correlation.
7. **Linux mass file modification:** Process on a Linux server modifying more than 500 files within 60 seconds — pre-encryption signal in case ShinySp1d3r Linux variant is released.

Platform-specific guidance

- **Splunk:** Build searches for OAuth/API dark-signal patterns and large-export detection.
- **Microsoft Sentinel (KQL):** Monitor SigninLogs and AuditLogs for suspicious app changes and new credentials being added or rotated.
- **Sigma:** High-level rules for suspicious SaaS token or application credential changes (rotate key, add credentials, authorize application).

Monitoring tier order

Given that most education-sector security teams are capacity-constrained, prioritise in this order:

- **Tier 1 (continuous):** SSO/IdP authentication logs, MFA device enrollment events, Salesforce admin/audit logs, GitHub and code-repository activity.
- **Tier 2 (daily review):** LMS and CRM bulk-export logs, VPN authentication from new devices, outbound data-transfer volumes.
- **Tier 3 (weekly review):** Staff credential exposure in breach databases, Linux server cron/systemd changes, network connections to low-reputation domains.

5. Indicators of compromise (with caveats)

Most ShinyHunters tradecraft this campaign series is identity-led rather than network-led, so behavioural detections (section 6) are higher-yield than network-blocking IOCs. Investigators should rely on vendor-reported developer-key timestamps, integration inventories, IdP logs, and Salesforce audit trails first.

Observable artifacts from the Canvas incident

Type	Indicator	Context	Risk
Login-page defacement message (7 May wave)	"ShinyHunters has breached Instructure (again)... contact us privately at TOX" with 12 May 2026 deadline	Reproduced by TechCrunch, CNN, Time, NBC, Harvard Crimson, Duke Chronicle	High — confirms compromise visibility
Negotiation channel	Tox messaging protocol; specific Tox ID associated with UNC6240/ShinyHunters	Tox is a peer-to-peer encrypted chat protocol — *not* a token. The actionable	Medium

		indicator is the specific Tox ID string	
Claimed dataset size (actor claim)	"3.65 TB / ~275M records / ~8,809 schools" — one ShinyHunters representative later cited ~231M unique emails	Actor leak-site claim, **unverified**	Low–Medium
Leak site	Listed on Tor-based "SHINYHUNTERS" DLS that emerged in late January 2026	Reproduced by Ransomware.live	Reference only

ShinyHunters / UNC6240 contact addresses (Mandiant-published)

- shinycorp@tutanota[.]com
- shinygroup@onionmail[.]com

These have been associated with UNC6240 / ShinyHunters extortion in Mandiant reporting. They are not tied to one specific incident; their appearance in inbound communications is a strong signal.

ShinySp1d3r ransomware family (Unit 42, November 2025)

- Embedded Tor stub URL (defanged):
  - hxxp://sh1nysp1d3rxyz123456789abcdefghijklmnopqrstuvwxyz[.]onion/
- **Current observed samples are Windows PE; a Linux variant has been announced but not yet observed in samples.**
- ELF binaries on Linux exhibiting mass file rename / extension append behaviour (forward-looking signature for the announced Linux variant)
- Unusual cron job creation or systemd service installation on Linux servers (forward-looking)
- README filename: README_SH1NYSP1D3R.txt

Sample SHA-256 hashes from Unit 42's published IOC feed (November 2025):

- d12e44a6c04ab4cafda1471a1204fbe3b6f0d01ca4017e3d8ae13fa8870c7689
- e41dd341f317cb674ff12c83a17365e5c5aa3240d912ab3801ff4cf09a00ccb2
- 50d18f4b11c5d9de7fc16cbc6ca71e65c5e8e9df7d8f3fb192565f035e5adf8a

(Full Unit 42 IOC list at: github.com/PaloAltoNetworks/Unit42-timely-threat-intel)

6. User-facing notification guidance

What to include in a notification to your community:

- The confirmed incident (Instructure / Canvas, late April / early May 2026, with the Free-For-Teacher account program identified as the vector and now permanently shut down by the vendor) and that your institution is investigating its specific exposure.
- The currently known affected data categories (names, email addresses, student IDs, Canvas inbox messages), framed as "based on the vendor's current findings, which may be revised."
- The absence of confirmed password or financial-data exposure as of the reporting date — if Instructure's position still holds when you publish.
- The FBI's public guidance: do not engage with anyone claiming to have your data, do not respond to demands or send payments, and verify any unsolicited communication that references your school or Canvas through known channels before responding.

- Practical anti-phishing guidance: verify any email referencing course or instructor names, never act on urgent payment or credential requests without independent verification, report suspicious calls to IT.
- A clear contact channel for questions and for reporting suspicious messages.
- A commitment to provide updates as the investigation continues.

What to avoid:

- Repeating the actor's unverified scope claims (record counts, terabytes, number of institutions). These figures are actor-supplied and amplifying them aids the extortion strategy.
- Categorical reassurances about exposure that the vendor has not confirmed.
- Direct linking or referencing of the leak portal or Tox contact details.

7. 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.

MITRE ATT&CK mapping (Instructure/Canvas May 2026 campaign)

Tactic	Technique	Confidence	Evidence

Initial Access	T1190 — Exploit Public-Facing Application	High	Vendor-confirmed exploitation of an issue in the Free-For-Teacher account program
Initial Access	T1078 — Valid Accounts	High	Privileged credentials revoked; API keys rotated
Defense Evasion / Discovery	T1671 — Cloud Application Abuse	High	Abuse of legitimate Canvas APIs and connected applications
Collection	T1530 — Data from Cloud Storage	Medium	Bulk extraction from Canvas tenant data
Exfiltration	T1567 — Exfiltration over Web Services	High	Aligned to ShinyHunters Campaign C0059 reference profile
Exfiltration	T1020 — Automated Data Extraction	Medium	Scale of extraction implies automated tooling

Kill chain status: the operation reached **Actions on Objectives** — public extortion, login-page defacement, and likely data monetisation. There is no public evidence of persistent endpoint malware, backdoors, or ransomware deployment in the Canvas incident.

8. Evidence gaps and confidence assessment

Confidence	Findings
High	Vendor-confirmed incident; Free-For-Teacher account exploitation as the access vector; exposed data categories (names, emails, student IDs, Canvas messages); ShinyHunters' extortion behaviour and leak-site tactics; SLSH alliance and UNC cluster mapping; vishing-led initial access via AiTM phishing kits; ShinySp1d3r Windows samples confirmed by Unit 42
Medium	Tenant-by-tenant scope; whether the 7 May login-page defacement campaign yielded additional data beyond the original intrusion; ShinySp1d3r Linux variant status (announced, not observed)
Low / Unverified	Actor-supplied numeric claims (3.65 TB / 275M records / 8,809 schools); the alternative ~231M unique email figure cited to TechCrunch; whether the same Free-For-Teacher issue exposed any additional Canvas tenant boundaries

Information gaps:

- Final dataset scale will only be known if and when ShinyHunters leaks (deadline 12 May 2026) or an independent forensic accounting is published.
- Tenant-specific exposure varies; each Canvas customer must independently confirm scope with Instructure.
- Whether further legal action follows similar to the 2024 DoJ prosecution of Sebastien Raoult.

Methodology note: This pack is built on open-source reporting, vendor statements, and Protos AI investigation work as of 10 May 2026. Update this pack as Instructure publishes further findings beyond the reporting window — particularly any post-12-May leak activity.

9. 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.