ultraviolet

THREAT ADVISORY

ShinyHunters Canvas Attack

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
May 13, 2026
TLP:GREEN

Executive Snapshot

In May 2026, the cybercriminal extortion collective ShinyHunters breached Instructure's Canvas learning management system twice within ten days, exploiting cross-site scripting vulnerabilities in the platform's Free-for-Teacher accounts to escalate to administrative access and exfiltrate approximately 3.6 terabytes of data belonging to an estimated 275 million users across nearly 9,000 educational institutions worldwide. The group, active since 2019 and responsible for prior breaches at AT&T, Ticketmaster, Salesforce customer environments, and others, operates as a loosely affiliated network of predominantly young, English-speaking operators with documented ties to Scattered Spider and the broader "Com" ecosystem. After Instructure remediated the initial vulnerability without paying, ShinyHunters re-entered the environment through the same exploit class and injected ransom demands into hundreds of institutional login portals, forcing a platform-wide outage during final examinations. Instructure ultimately reached a financial agreement with the group in exchange for digital confirmation of data destruction, though cybersecurity experts have widely cautioned that such assurances from criminal actors carry no enforceable guarantee.

The incident underscores the outsized blast radius that a single vulnerability in a shared SaaS platform can produce and highlights the need for the following defensive priorities:

- **Harden web application attack surfaces.** Conduct regular penetration testing and static/dynamic code analysis across all customer-facing portals, with particular scrutiny on ancillary product tiers (such as freemium or trial environments) that may share infrastructure with the core platform but receive less security attention.

- **Enforce least-privilege controls on SaaS integrations.** Inventory all OAuth grants, API tokens, and third-party integration credentials; scope each to the minimum required permissions; and implement continuous monitoring for anomalous bulk data export or access patterns that could indicate exfiltration in progress.

- **Deploy phishing-resistant MFA and harden identity infrastructure.** Adopt FIDO2/WebAuthn hardware keys for privileged accounts, enforce conditional access policies tied to device posture and location, and train helpdesk and IT support staff to verify caller identity through out-of-band channels before processing credential or MFA resets, given ShinyHunters' documented use of AI-powered voice phishing.

- **Test incident response playbooks against multi-phase extortion scenarios.** Ensure response plans account for attackers who re-enter environments after initial remediation, segment sensitive data stores to contain blast radius, and validate that backup and recovery procedures enable service restoration without dependence on attacker cooperation or ransom payment.

TIDE Team Analysis

In late April and early May 2026, the financially motivated cybercriminal collective known as ShinyHunters conducted a two-phase intrusion against Instructure, the Utah-based company that operates Canvas, the most widely adopted learning management system in North American higher education. Instructure detected unauthorized activity on April 29, 2026, immediately revoked access, and engaged external forensic investigators. During the first intrusion, the attackers claimed to have exfiltrated approximately 3.6 terabytes of uncompressed data, including usernames, email addresses, course names, enrollment information, and private messages exchanged between students and educators. When Instructure patched the initial vulnerability rather than negotiate, ShinyHunters re-entered the environment on May 7 via the same exploit path and injected JavaScript containing ransom demands directly into hundreds of Canvas login portals, forcing the platform offline during final exams and Advanced Placement testing at institutions across the United States, Canada, Australia, New Zealand, and parts of Europe and Asia.

ShinyHunters is a criminal data extortion collective that has been active since approximately 2019, gaining public notoriety in May 2020 when it appeared on dark web forums offering millions of stolen user records from more than a dozen companies in a single two-week burst. The group operates under a consistent "pay or leak" model: after exfiltrating high-volume datasets, it demands ransom and threatens to publish or auction the data if payment is not received. Security researchers and law enforcement describe the group not as a monolithic organization but as a loosely affiliated brand encompassing multiple threat clusters, with operational overlap with Scattered Spider and members of "The Com," a broader English-speaking cybercriminal ecosystem. Members are believed to be predominantly teenagers and young adults based in the United States and the United Kingdom, though the group's international reach and use of hired operators complicate precise attribution.

The group has a well-documented history of high-profile breaches spanning multiple sectors. Early operations in 2020 targeted Tokopedia, Wattpad, and Microsoft's private GitHub repositories. Subsequent campaigns struck AT&T Wireless in 2024, from which over 110 million customer records were stolen and a ransom was ultimately paid. In 2025 and 2026, ShinyHunters-branded operations escalated to target enterprise SaaS platforms including Salesforce, Workday, and Snowflake customer environments, as well as consumer-facing companies such as Ticketmaster, Santander, Pizza Hut Australia, Coinbase, and Qantas. The progression reflects a deliberate strategic shift from database-level theft toward exploiting cloud identity layers and third-party integrations, where a single compromised access path can yield data from thousands of downstream organizations.

The victimology in the Canvas incident is particularly notable for its breadth and the sensitivity of the population affected. ShinyHunters claimed the breach impacted approximately 8,809 universities, educational ministries, and other institutions worldwide, with data on roughly 275 million users compromised, including billions of private messages. Affected institutions ranged from Ivy League universities such as Columbia, Princeton, Harvard, and Georgetown to K-12 school districts and international educational bodies. The timing of the attack, during final examination periods, amplified operational disruption and reputational damage, forcing institutions to extend deadlines, alter exam schedules, and revert to paper-based processes. The incident drew comparisons to the 2024-2025 PowerSchool breach, in which a similar extortion-and-ransom cycle targeting the education sector ultimately led to criminal charges against a Massachusetts college student.

The technical attack path in this case centered on a web application vulnerability rather than the group's more recently publicized vishing campaigns. Investigators determined that ShinyHunters exploited cross-site scripting (XSS) vulnerabilities in Canvas's Free-for-Teacher accounts, which allowed the attackers to escalate to administrative access within the broader Canvas environment. This access enabled bulk data exfiltration during the first phase and, when the same vulnerability class was not fully remediated, permitted the second intrusion on May 7

in which the group defaced login portals with ransom messaging. Separately, the group's broader 2025-2026 toolkit includes AI-powered voice phishing using platforms such as Bland AI and Vapi, abuse of OAuth token flows and SaaS integration tools like Salesforce Data Loader, supply chain compromise through CI/CD pipeline infiltration via BrowserStack and JFrog, and SIM swapping to defeat multi-factor authentication. The Canvas operation demonstrates that even as the group adopts increasingly sophisticated social engineering techniques, it remains opportunistic about exploiting conventional web application flaws when they present themselves.

The incident concluded on May 12, 2026, when Instructure announced it had reached an agreement with ShinyHunters under which the company received digital confirmation of data destruction via shred logs, along with assurances that no customers would be further extorted. The U.S. House Homeland Security Committee summoned Instructure's CEO to Capitol Hill for a briefing on the circumstances of both intrusions, the volume and nature of data accessed, the adequacy of coordination with federal law enforcement and CISA, and the company's remediation steps. The FBI mobilized resources in multiple states to assist affected institutions. Cybersecurity experts publicly cautioned that paying ransoms provides no reliable guarantee that attackers have truly destroyed exfiltrated data, and the decision to pay may incentivize future targeting of the education sector.

Organizations seeking to defend against ShinyHunters and similarly structured extortion groups should prioritize several overlapping controls. First, rigorous web application security testing, including regular penetration testing and static/dynamic analysis of customer-facing portals, is essential, as the Canvas breach was enabled by an XSS vulnerability in a peripheral product tier that provided a pathway into the core platform. Second, all SaaS integrations, OAuth grants, and third-party API tokens should be inventoried, scoped to least privilege, and continuously monitored for anomalous bulk data access patterns. Third, given ShinyHunters' documented use of AI-powered vishing and social engineering to compromise SSO and MFA, organizations should deploy phishing-resistant MFA (such as FIDO2/WebAuthn hardware keys), enforce conditional access policies, and train helpdesk staff to verify identity through out-of-band channels before resetting credentials or MFA tokens. Finally, organizations should maintain tested incident response playbooks that account for multi-phase extortion scenarios, segment sensitive data stores to limit blast radius, and ensure that backup and recovery procedures allow rapid restoration of services without dependence on attacker cooperation.

Why It Matters

The Canvas breach represents the largest known cybersecurity incident in the education sector to date, and its implications extend well beyond Instructure's customer base. Canvas holds a 41% market share among North American higher education institutions and serves over 30 million active users globally, meaning the platform functions as critical infrastructure for academic operations at scale. When ShinyHunters forced the platform offline on May 7, thousands of institutions simultaneously lost access to course materials, grading systems, and communication tools during one of the most operationally sensitive periods of the academic calendar. The incident demonstrated that a single vulnerability in a dominant SaaS provider can cascade into disruption across an entire sector, a risk model that applies equally to any industry with heavy concentration in a small number of cloud platforms.

The nature of the compromised data carries long-tail risk that organizations and individuals should not underestimate. While Instructure confirmed that passwords, financial information, and government identifiers were not accessed, the exfiltrated dataset reportedly included billions of private messages between students and educators, enrollment records, and student identification numbers. This type of data is particularly valuable for social engineering, identity fraud, and targeted phishing campaigns, and its sensitivity is compounded by the fact that a significant portion of the affected population includes minors enrolled in K-12 institutions. Even if the attackers' claims of data destruction are taken at face value, the possibility that copies were retained or distributed before the agreement cannot be independently verified.

The incident also highlights a troubling trend in threat actor economics. Instructure's decision to reach a financial agreement with ShinyHunters, following a nearly identical playbook to AT&T's ransom payment to the same group in 2024, reinforces a cycle in which paying extortion demands validates the business model and signals to other criminal operators that the education sector is both vulnerable and willing to pay. The PowerSchool breach in late 2024, which followed the same pattern and ultimately saw re-extortion of individual school employees months after the initial ransom was paid, offers a concrete case study in why ransom payments rarely produce durable resolution. Each payment funds further operational capability and recruitment within the ShinyHunters ecosystem and the broader cybercriminal underground it draws from.

Finally, the breach should prompt security leadership across all sectors to reassess third-party and supply chain risk with renewed urgency. The attack vector was not a sophisticated zero-day exploit or an advanced social engineering campaign; it was a cross-site scripting flaw in a peripheral product tier that shared access with the core platform. This is a class of vulnerability that is well understood, detectable through standard application security practices, and preventable with disciplined secure development lifecycles. The gap between what was technically preventable and what actually occurred points to a broader governance failure: organizations that delegate critical operations to SaaS providers must hold those providers to contractual security standards, demand evidence of regular independent testing, and maintain contingency plans for platform-level outages that assume the worst-case scenario rather than the vendor's best-case assurances.

How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure third party vendor services are adequately segmented from production and mission critical systems.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---