ZEROFOX INTELLIGENCE

Flash

ShinyHunters' Campaign Against the Education Sector

F-2026-05-13a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Threat Actor, Phishing

May 13, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:30 AM (EDT) on May 13, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | ShinyHunters' Campaign Against the Education Sector

| Key Findings

- ShinyHunters is very likely in the midst of an ongoing campaign of escalatory attacks. This campaign almost certainly includes intentional targeting of the education sector—most recently Canvas and Houghton Mifflin Harcourt.
- The group's targeting of the education sector is almost certainly due to the large amount of user, employee, and customer data housed by educational institutions and within learning management systems.
- Data retrieved from the attack on Canvas is very likely to be used for further attacks against companies and institutions that use the learning management system for corporate and online training.
- ShinyHunters is very likely employing escalatory tactics: using data stolen in one breach to attack the next organization in a ladder of escalation. Further attacks exploiting lax access token protocols—and empowered by sophisticated phishing attacks—will almost certainly occur in the coming weeks and months.

Details

Beginning on April 30, 2026, ShinyHunters breached the web-based learning management system Canvas. Subsequently, on May 7, the group stated that Instructure, the company that owns and operates Canvas, had not negotiated and instead simply performed "security patches."[1] ShinyHunters subsequently gave affected educational institutions and companies that use Canvas until May 12 to negotiate ransoms individually.[2]

- Canvas is a cloud-based learning management system used by hundreds of educational institutions around the world. Additionally, it is used by major companies to manage and administer corporate training.[3] It is a comprehensive platform for online learning, course management, and student engagement.[4]

According to ShinyHunters, the breach could affect up to 275 million people across 8,809 institutions—including students, educators, and administrators; given the scope of the breach, ZeroFox assesses it is likely these claims are fairly accurate. Some of the most prominent universities in the world were listed among the victims, including:

- Harvard University
- Stanford University
- University of Oxford
- Massachusetts Institute of Technology (MIT)
- Princeton University
- Columbia University
- University of Cambridge (access was gained via Cambridge University Press)
- Cornell University
- Georgetown University
- University of California, Berkeley

[1] hXXps://www.wral[.]com/news/education/canvas-shinyhunters-ransom-instructure-hack-data-breach-may-2026/
[2] hXXps://databreaches[.]net/2026/05/07/developing-shinyhunters-hacks-instructure-again-canvas-down/
[3] hXXps://www.timeshighereducation[.]com/campus/sponsor/canvas
[4] *Ibid.*

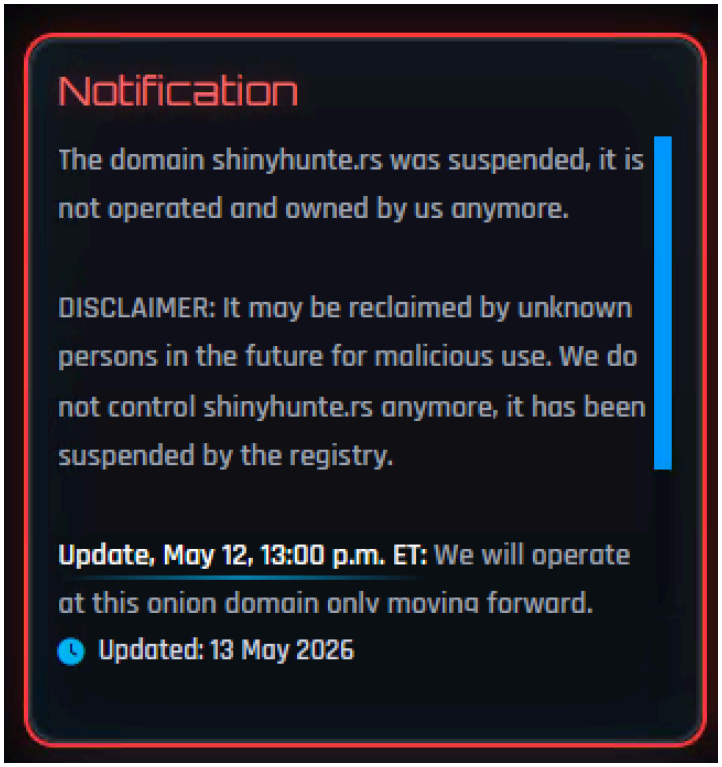
On May 12, 2026, Instructure posted a statement online indicating it had come to an agreement with ShinyHunters, who reportedly agreed to delete data stolen in the breach.[5] Instructure did not publicly give details but likely paid ShinyHunters a ransom for the release of data. It is also likely that ShinyHunters—despite reportedly presenting Instructure with shred logs—maintained a copy of essential data needed for future attacks.

Additionally, on May 11, 2026, ShinyHunters claimed an attack against academic textbook publisher Houghton Mifflin Harcourt Company (HMH) on its leak site. The group stated HMH's data was breached in several campaigns conducted over the past several months. ShinyHunters gave the publisher until May 12, 2026, to contact the group and negotiate the ransom or the data would be released. There has been no indication of release as of the time of writing.

ShinyHunters' claim of HMH breach
Source: ZeroFox Intelligence

[5] hXXps://abc7[.]com/post/deal-reached-hackers-delete-data-stolen-canvas-educational-platform/19086610/

On May 12, 2026, ShinyHunters announced that its clear net site has been suspended and that the group will continue operating its dark web site. It is unclear at this time if the suspension is the result of law enforcement action or a service provider decision.



ShinyHunters' web site suspension announcement

Source: ZeroFox Intelligence

ShinyHunters is a financially motivated ransomware and digital extortion (R&DE) collective that has been active since at least 2020. The group operates on a "pay or leak" model; they do not lock victims out of their data or encrypt servers. Instead, a ShinyHunters attack simply copies user, employee, and customer data from the victim and issues a ransom demand; failure to negotiate results in a leak of sensitive data.[6]

Since late 2024, ZeroFox has observed ShinyHunters conducting a campaign against the education sector, including educational institutions and companies that provide platforms for online learning and corporate training.

[6] hXXps://www.mayhemcode[.]com/2026/03/shinyhunters-hacking-group-explained.html

- Since November 1, 2024, the education sector has accounted for at least 10 percent of all ShinyHunters R&DE attacks.
- This relatively high level of targeting education companies and institutions suggests that ShinyHunters (despite its protestations to the contrary) is likely conducting an intentional campaign against the sector—almost certainly due to the large amount of user data to which these entities have access.

ShinyHunters likely uses phishing and social engineering to gain initial access to target networks. In the case of Canvas, it is likely that the group used credentials stolen in previous attacks against educational institutions, such as Harvard University and the University of Pennsylvania in 2025.[7] Reportedly, ShinyHunters specifically targets Salesforce Experience Cloud instances with misconfigured user permissions.[8]

- ShinyHunters very likely then exploits lax access protocols and applies contextual intelligence, knowing which organizations to attack next because the previous victim's data revealed the relationship.

This methodology likely allows ShinyHunters to continue attacking the education sector via climbing a "credentials ladder": using credentials, access tokens, and hashed passwords stolen from one institution to attack software, platforms, and associated organizations in an escalatory campaign.

[7] hXXps://www.yahoo[.]com/news/articles/personal-data-stolen-during-harvard-132500693.html?guccounter=1
[8] hXXps://www.mayhemcode[.]com/2026/03/shinyhunters-hacking-group-explained.html

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%