ShinyHunters Compromise of Canvas LMS

08 May 2026

Executive Summary

In May 2026, the cyber-criminal collective ShinyHunters (also known as Scattered LAPSUS$ Hunters, UNC6661, UNC6671, and UNC6240) targeted Instructure which is an educational technology company and the developer and publisher of Canvas, a web-based learning management system. The group has claimed responsibility for the exfiltration of 3.65 terabytes of data belonging to over 9,000 global institutions, including the vast majority of California's higher education and K-12 systems. This is a one-to-many attack: by hitting the Software as a service (SaaS) they've compromised thousands of downstream campuses.

Timeline of Events

29 April 2026: Initial compromise detected by Instructure, revoked access and started an investigation.

07 May 2026-01: A second compromise occurred and Canvas was taken offline after defacements were made with a ransomware message.

12 May 2026: A hard deadline for public data release.

Typical Targets

ShinyHunters prioritize high-value, low-friction targets—organizations that hold massive amounts of sensitive data but have complex SaaS (Software as a Service) ecosystems that are easy to misconfigure.

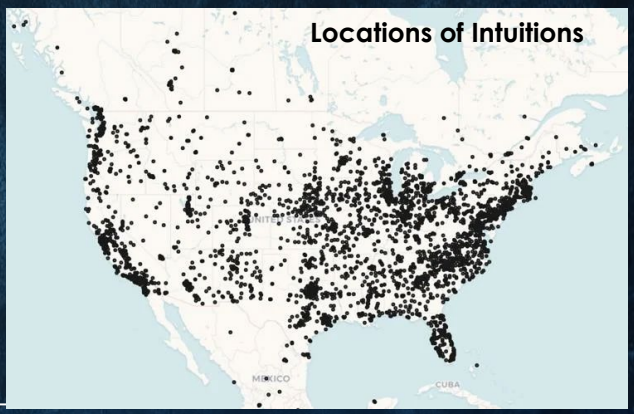
- SaaS-Heavy Enterprises: Any company that relies heavily on Salesforce, Google Workspace, or Workday.
- The Luxury & High-Net-Worth Sector: Specifically, to harvest records of wealthy individuals, as this data sells for a premium on the dark web.
- Supply Chain "Connectors": They target the "middlemen" of the internet - By breaching one of these, they gain automated access to thousands of downstream customers.

Information taken

Identified: Full names, institutional emails, and Student ID numbers.

High Risk: Billions of private messages exchanged between students and faculty.

Verified Safe: Instructure has confirmed that passwords, government IDs (SSNs), and financial data remain uncompromised in this specific cloud environment.



ShinyHunters Compromise of Canvas LMS

08 May 2026

Technical Specifications TTPs and IOCs

Tactics, Techniques, and Procedures

ShinyHunters' 2026 tradecraft is defined by Identity Persistence.

- **Vishing for Initial Access (T1566.004):** Attackers call IT help desks using AI-voice cloning or high-pressure scripts to reset passwords or "fix" MFA issues for high-privilege accounts.
- **MFA Manipulation & Bypass (T1556):** After obtaining a password, they immediately register a new MFA device. They frequently use Genymobile emulators to appear as legitimate mobile devices during enrollment.
- **SaaS/SSO Enumeration:** Once inside an SSO (Single Sign-On) environment like Okta, they rapidly move through all connected apps (Slack, Salesforce, Google Drive) within minutes.
- **Automated Exfiltration:** Data is not browsed manually; the group uses scripts to query cloud APIs and download data at speeds that often evade standard rate-limiting controls.

Indicators of Compromise

Defenders should monitor for the following specific 2026 signals:

- Enrollment Artifacts: New MFA devices named "Passkey", "Phone", or any device linking to Genymobile.
- User Agents: com.okta.android.auth/8.19.0, Android/16.
- Anomalous API Traffic: Spikes in traffic to /api/v1/conversations (Canvas messaging) or Salesforce bulk export endpoints.
- Authentication Deviations: Lengthy authentication flows with multiple failures followed by a sudden, successful device enrollment.

ShinyHunters Compromise of Canvas LMS

08 May 2026

IOC list

Historical ShinyHunters IOCs

IP Addresses

24.242.93.122
23.234.100.107
23.234.100.235
73.135.228.98
157.131.172.74
149.50.97.144
67.21.178.234
142.127.171.133
76.64.54.159
76.70.74.63
206.170.208.23
68.73.213.196
37.15.73.132
104.32.172.247
85.238.66.242
199.127.61.200
209.222.98.200
38.190.138.239
198.52.166.197
23.162.8.66
23.234.69.167
23.94.126.63
31.58.169.85
31.58.169.92
31.58.169.96
34.86.51.128
35.186.181.1
37.19.200.132
37.19.200.141
37.19.200.154
37.19.200.167
37.19.221.179
38.22.104.226
45.83.220.206
51.89.240.10
64.95.11.225
64.95.84.159
66.63.167.122
67.217.228.216
68.235.43.202
68.235.46.22
68.235.46.202
68.235.46.151
68.235.46.208
68.63.167.122
69.246.124.204
72.5.42.72
79.127.217.44
83.147.52.41
87.120.112.134
94.156.167.237
96.44.189.109
96.44.191.141
96.44.191.157
104.223.118.62
104.193.135.221
141.98.252.189
146.70.165.47
146.70.168.239
146.70.173.60
146.70.185.47
146.70.189.47
146.70.189.111
146.70.198.112
146.70.211.55
146.70.211.119
146.70.211.183
147.161.173.90
149.22.81.201
151.242.41.182
151.242.58.76
163.5.149.152
185.141.119.136
185.141.119.138
185.141.119.151
185.141.119.166
185.141.119.168
185.141.119.181
185.141.119.184
185.141.119.185
185.209.199.56
191.96.207.201
198.44.129.56
198.44.129.88
195.54.130.100
196.251.83.162
198.244.224.200
198.54.130.100
198.54.130.108
198.54.133.123
205.234.181.14
206.217.206.14
206.217.206.25
206.217.206.26
206.217.206.64
206.217.206.84
206.217.206.104
206.217.206.124
208.131.130.53
208.131.130.71
208.131.130.91
31.58.169.96
64.94.84.78
192.198.82.235
23.145.40.165
208.68.36.90
44.215.108.109
154.41.95.2
176.65.149.100
179.43.159.198
185.130.47.58
185.207.107.130
185.220.101.133
185.220.101.143
185.220.101.164
185.220.101.167
185.220.101.169
185.220.101.180
185.220.101.185
185.220.101.33
192.42.116.179
192.42.116.20
194.15.36.117
195.47.238.178
195.47.238.83

URLs

- Login[.]salesforce[.]com/setup/connect?user_code=aKYF7V5N
- Login.salesforce.com/setup/connect?user_code=8KCQGTVU
- https://help[victim][.]com
- https://login[.]salesforce[.]com/setup/connect
- http://64.95.11[.]112/hello.php
- 91.199.42.164/login

User-Agent Strings:

- Salesforce-Multi-Org-Fetcher/1.0
- Salesforce-CLI/1.0
- python-requests/2.32.4
- Python/3.11 aiohttp/3.12.15

ShinyHunters Compromise of Canvas LMS

08 May 2026

Mitigation and Recommendations

For Network Defenders (SaaS/Cloud)

- FIDO2 Hardware Keys: Transition administrators to hardware security keys (e.g., YubiKey). ShinyHunters' current TTPs easily bypass SMS, Email, and Push-based MFA.
- Zero-Dwell Auditing: Audit for "SSO Bursts"—where a user accesses more than 10 connected applications within a 5-minute window.
- API Token Rotation: Rotate all Salesforce OAuth and Gainsight integration tokens immediately.

For User Groups (Students/Faculty)

- Extortion Awareness: Do not respond to "Tox" or "Telegram" links sent via email. These are psychological tactics.
- Minor Protection: Parents in K-12 districts should proactively freeze the credit of minors. Student IDs, while not as sensitive as SSNs, are the first step in long-term identity theft.
- Password Hygiene: While passwords were not stolen, the actor is using leaked names to attempt "Credential Stuffing" on personal accounts. Change passwords on any site that shared a password with your school account.

Sharing, Reporting, and Support

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

833-REPORT-1 or 916.636.2997

calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:

Federal Officials at CISA and/or the FBI as applicable

Coordinate with your regional Fusion Center

SHARE information, intelligence, and IOCs with ISACs