SOL THREAT INTELLIGENCE

June 2026 Higher Education Regional Sector Brief

- 1 JUN TO 30 JUN 2026
- 3 REGIONS
- 4 PAGES PER REGION
- PREPARED BY KAARTHEESWARAN RAVICHANDRAN

AMERICAS

EXECUTIVE SUMMARY

Higher education was the primary victim concentration in the PeopleSoft campaign

Americas higher education had the strongest sector-region evidence in the source set. More than 100 organizations were targeted through CVE-2026-35273 and 68 percent were reported as U.S. higher education institutions. The campaign operated as a zero-day from 27 May through 9 June, with victim data published on 9 June and Oracle issuing its advisory on 10 June. This was a systematic mass-exploitation event against a shared university ERP platform, not an isolated breach.

KEY INSIGHTS

1	**About 68 percent of more than 100 targets were U.S. higher education institutions**, making American universities the principal victim concentration.
2	**PeopleSoft Campus Solutions, HCM and Financials** created a common attack surface across universities and colleges.
3	**ShinyHunters used a custom fan-out script** to spray SSH credentials and move across internal PeopleSoft nodes.
4	**Canvas, Okta, Microsoft 365 and Salesforce** formed parallel supply chain and identity attack surfaces.
5	**AI vishing targeted helpdesk processes** and real-time MFA interception through malicious connected-app approvals.

6	**The United States also carried the highest ransomware victim share globally** across June, increasing the secondary opportunistic threat to universities.

Top threat entities and June trend shifts

- **ShinyHunters, UNC6240** PRIMARY ACTOR

Mass exploitation of PeopleSoft, cloud data theft, AI vishing and insider recruitment against university environments.

- **Oracle PeopleSoft campaign** MASS EXPLOITATION

Approximately 68 U.S. university targets, MeshCentral C2, SSH fan-out, zstd staging and extortion.

- **Canvas LMS compromise** SUPPLY CHAIN

Risk to the dominant LMS ecosystem across U.S. and Canadian institutions.

- **Securotrop, Qilin affiliate** RANSOMWARE

GPO-based Chrome credential theft and domain-wide ransomware techniques relevant to university AD environments.

- **3AM ransomware** HELPDESK SOCIAL ENGINEERING

Email bombing, Quick Assist abuse, QEMU EDR bypass and long dwell time, all applicable to university support environments.

Trend shifts versus May 2026

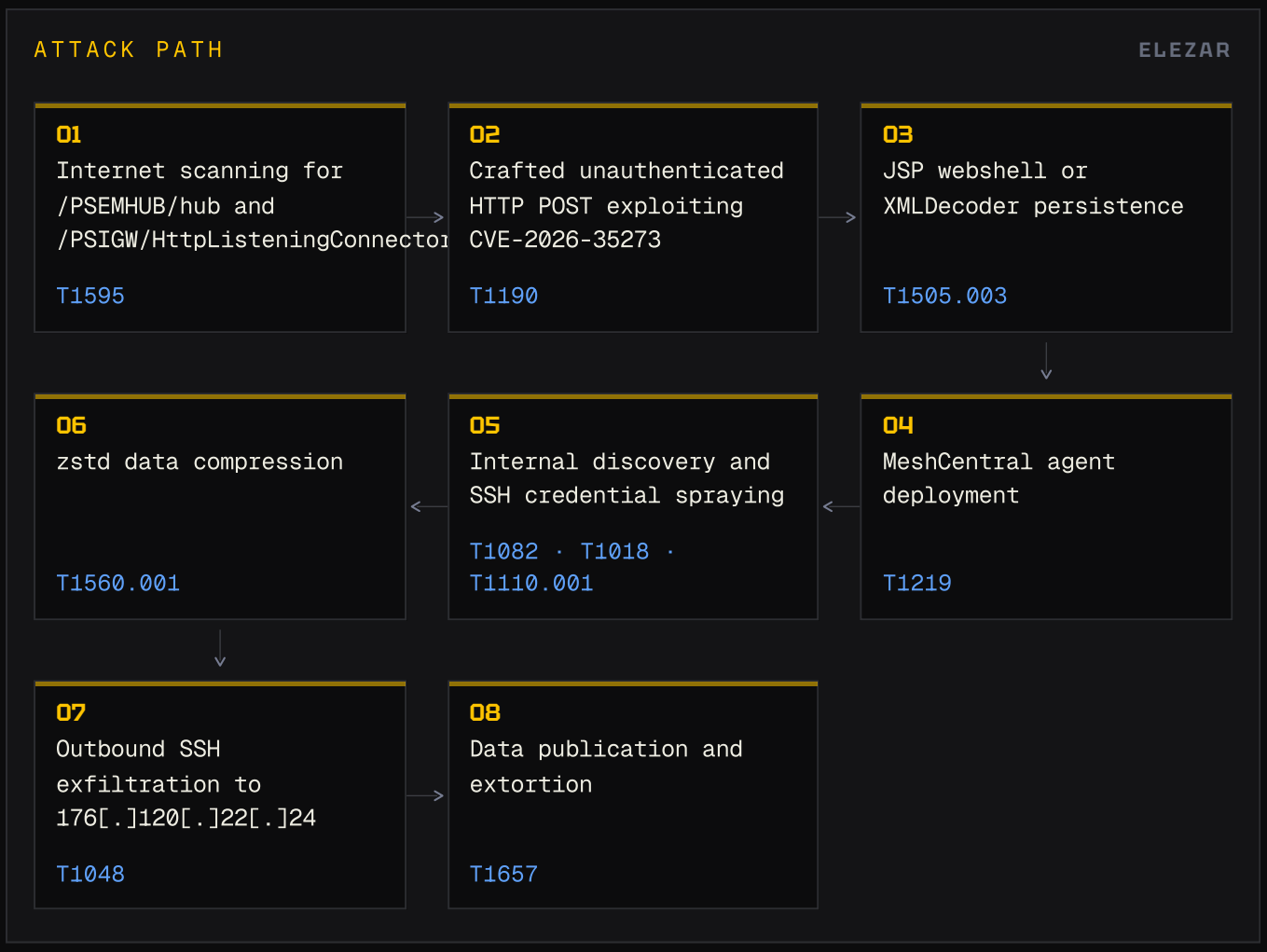
1	**Mass zero-day exploitation produced the first large confirmed university victim cluster** in the tracked dataset.
2	**Shared ERP infrastructure became the force multiplier**, allowing one vulnerability to affect dozens of institutions.

3	**AI vishing became an operational identity attack method** rather than an emerging concept.
4	**Canvas compromise broadened risk from on-premises ERP to SaaS learning platforms.**

Attack chains, vulnerabilities and indicators

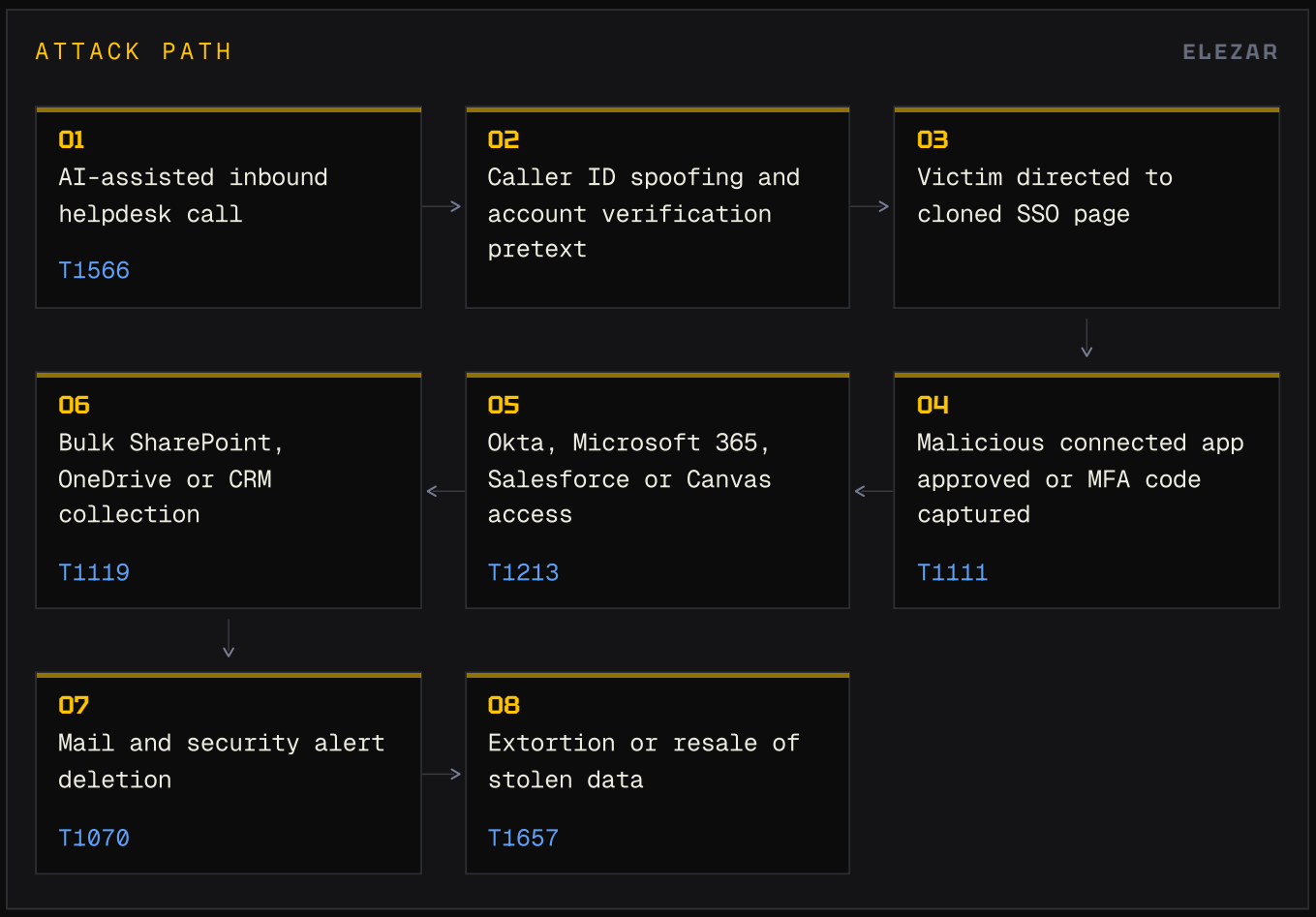
CVE	PRODUCT	CVSS	JUNE CONTEXT
CVE-2026-35273	Oracle PeopleSoft PeopleTools 8.61 and 8.62	9.8	Zero-day; about 68 percent of targets were U.S. higher education
CVE-2026-20253	Splunk Enterprise	9.8	Risk to university SIEM infrastructure
CVE-2026-48907	Joomla Widget Factory	9.8	Risk to university web portals
CVE-2021-44228	Apache Log4j	10.0	Actively exploited by DragonForce in June reporting
CVE-2024-57726, 57727, 57728	SimpleHelp RMM	High	Relevant to outsourced university IT and MSP access

Attack Chain 1: PeopleSoft zero-day to extortion



Source reports: ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit; Oracle PeopleSoft zero-day analyses

Attack Chain 2: AI vishing to cloud data theft



Source report: The ShinyHunters Domino Effect: One Breach, Hundreds of Victims

Selected high-value indicators

TYPE	INDICATOR	ASSOCIATION
IP	142[.]11[.]200[.]186 through 142[.]11[.]200[.]190	ShinyHunters staging infrastructure
IP	176[.]120[.]22[.]24	Data leak site mirror and exfiltration destination
Domain	azurenetfiles[.]net	MeshCentral C2 masquerading as Azure infrastructure
URL	wss://azurenetfiles[.]net:443/agent.ashx	MeshCentral WebSocket C2
Domain	bless-invite[.]com	SSO and invitation phishing lure
File	meshagent64-azure-ops.exe, meshagent32-azure-ops.exe, meshagent64-v2.exe	Customized MeshCentral agents
Path	/PSEMHUB/hub and /PSIGW/HttpListeningConnector	PeopleSoft exploitation endpoints
File	README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT	Extortion marker
SHA256	2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35	MeshCentral agent sample

Prioritized defensive guidance

Scoped to the typical higher education environment: PeopleSoft, Canvas or other LMS platforms, federated SSO, Microsoft 365, open research networks, decentralized IT and high staff and student turnover.

IMMEDIATE: ACT WITHIN 72 HOURS

1. Assume possible PeopleSoft compromise until cleared

Check every externally exposed PeopleTools 8.61 or 8.62 environment used between 27 May and 9 June. Preserve evidence and hunt for the documented persistence, C2 and exfiltration artifacts.

2. Remove PSEMHUB and PSIGW from the internet

Place management endpoints behind VPN or internal network controls.

3. Patch and deploy the full IOC set

Apply Oracle's fix after evidence preservation and push domain, IP and hash indicators to EDR, SIEM, proxy and firewall tooling.

URGENT: ACT WITHIN 1 TO 2 WEEKS

4. Harden helpdesk and account-recovery workflows

Require callback verification and never approve connected apps or MFA changes from unsolicited calls.

5. Rotate Canvas, Salesforce and SSO integrations

Revoke dormant grants, verify vendor scope and isolate CI or administrative credentials from SaaS compromise paths.

6. Enforce phishing-resistant MFA

Prioritize FIDO2 or WebAuthn for PeopleSoft, registrar, finance, HR and research administrators.

7. Address insider recruitment

Deploy UBA for bulk downloads, automate offboarding and monitor high-risk changes involving VPN, Git and SSO.

INVESTIGATE AND TUNE DETECTIONS

8. Build a FERPA-focused breach playbook

Pre-approve evidence preservation, legal review, regulator coordination and affected-person communication for student data exposure.

9. Detect QEMU-based EDR evasion

Alert on qemu-system executables, ACOW2 or QCOW2 files in ProgramData and the WindowsSensor15 scheduled task.

10. Add PeopleSoft, SaaS and helpdesk correlation rules

Correlate inbound support calls, connected-app approvals, bulk cloud downloads and new authentication methods within short time windows.

June source reports: ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit · ShinyHunters Exploits Oracle PeopleSoft Zero-Day to Breach Universities · Oracle PeopleSoft 0-Day RCE Flaw Under Active Exploitation by ShinyHunters · The ShinyHunters Domino Effect: One Breach, Hundreds of Victims · June 2026 weekly threat intelligence reports

EMEA

EXECUTIVE SUMMARY

A named university breach confirms direct sector impact

EMEA higher education experienced the clearest named victim evidence in the source set. The University of Nottingham was compromised through ShinyHunters exploitation of CVE-2026-35273 in Oracle PeopleSoft, with about 455,000 unique email addresses and personal records, including passport data, published on 9 June 2026. The global campaign affected more than 100 organizations and 68 percent were higher education institutions. This confirms that PeopleSoft exposure was not theoretical for European universities.

KEY INSIGHTS

1	**The University of Nottingham** was the only named EMEA higher education victim in the source reports.
2	**Data publication preceded Oracle's advisory by one day**, leaving affected institutions without official patch guidance before disclosure.
3	**CVE-2026-35273 required no credentials or user interaction** and targeted PeopleTools 8.61 and 8.62.
4	**ShinyHunters' SaaS domino-effect model** also affected Canvas-related ecosystems and cloud integrations used across universities.
5	**AI vishing and insider recruitment** created identity risk across Okta, Microsoft SSO, Citrix VPN and Git environments.
6	**GDPR pressure increased extortion risk**, both for confirmed data theft and for opportunistic ransomware operators active across EMEA.

Top threat entities and June trend shifts

- ShinyHunters, UNC6240 CONFIRMED ACTOR

Confirmed University of Nottingham breach and broader higher education targeting through PeopleSoft, SaaS compromise and identity attacks.

- **Oracle PeopleSoft campaign** ZERO-DAY CAMPAIGN

  Unauthenticated RCE, persistence, MeshCentral deployment, SSH fan-out and data publication.

- **Brain Cipher** RANSOMWARE

  Opportunistic EMEA ransomware using exposed remote access, credential theft and GDPR notification pressure.

- **AiLock** RANSOMWARE

  RaaS with aggressive data-protection notification threats and post-quantum key encapsulation.

- **Canvas LMS compromise** SUPPLY CHAIN

  A shared-platform risk for European, Middle Eastern and African universities using Canvas.

Trend shifts versus May 2026

1	**A named European university victim was confirmed**, moving sector risk from inferred to directly evidenced.
2	**University ERP systems became a zero-day target class**, replacing the prior month's more routine credential and phishing activity.
3	**AI vishing broadened beyond email security controls**, especially in multilingual helpdesk environments.
4	**GDPR notification pressure became part of the threat model** for both data theft and ransomware extortion.

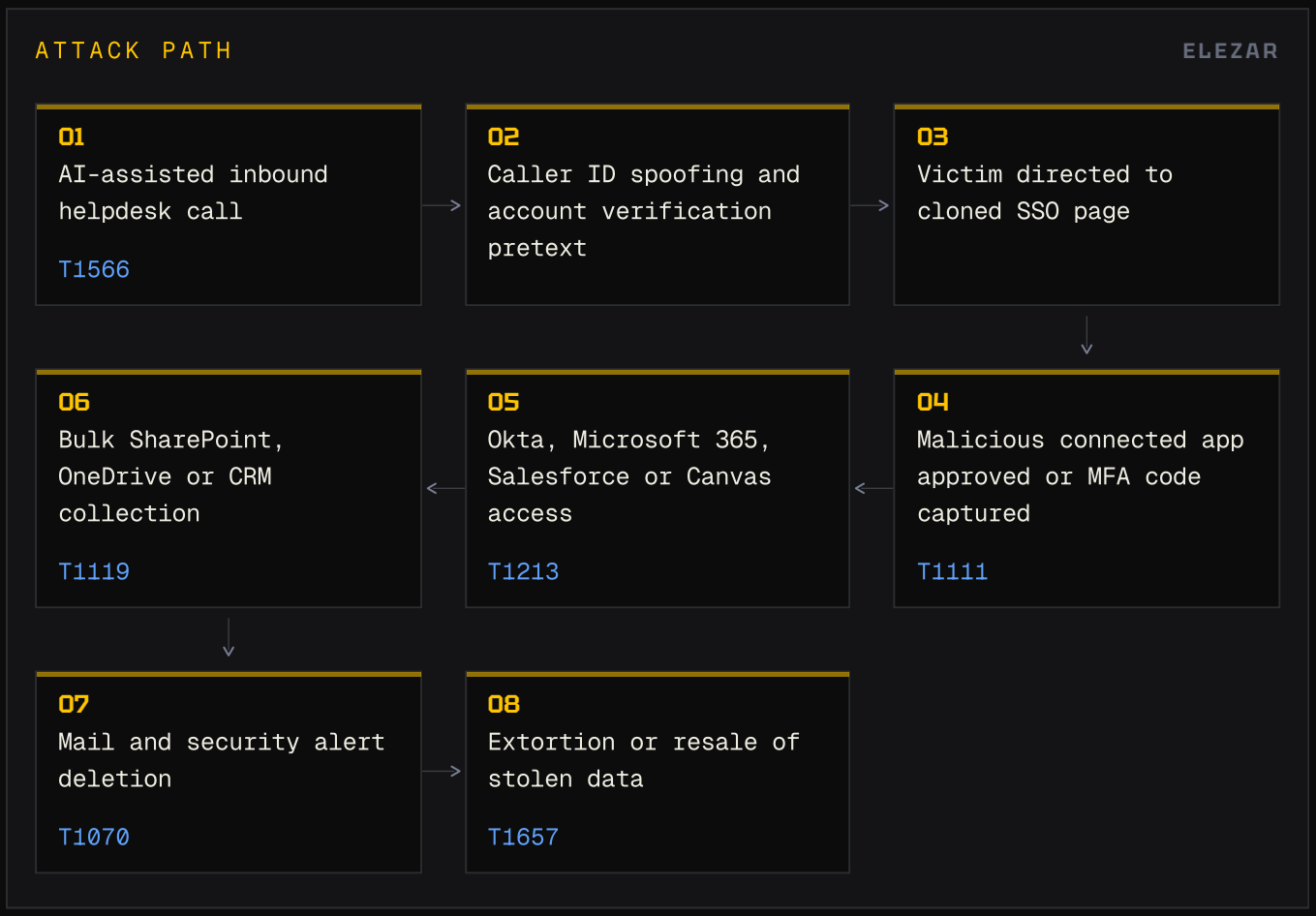
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	CVSS	JUNE CONTEXT
CVE-2026-35273	Oracle PeopleSoft PeopleTools 8.61 and 8.62	9.8	Actively exploited; University of Nottingham confirmed victim
CVE-2026-20253	Splunk Enterprise	9.8	Risk to university SIEM and logging systems
CVE-2026-48907	Joomla Widget Factory	9.8	Risk to public-facing university sites
CVE-2023-28252	Windows CLFS driver	7.8	Actively used by Brain Cipher
CVE-2026-0257	Palo Alto PAN-OS	9.1	Network perimeter authentication bypass risk

Attack Chain 1: PeopleSoft zero-day to extortion

Source reports: ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit; Oracle PeopleSoft zero-day analyses

Attack Chain 2: AI vishing to cloud data theft



Source report: The ShinyHunters Domino Effect: One Breach, Hundreds of Victims

Selected high-value indicators

TYPE	INDICATOR	ASSOCIATION
IP	142[.]11[.]200[.]186 through 142[.]11[.]200[.]190	ShinyHunters staging infrastructure
IP	176[.]120[.]22[.]24	Data leak site mirror and exfiltration destination
Domain	azurenetfiles[.]net	MeshCentral C2 masquerading as Azure infrastructure
URL	wss://azurenetfiles[.]net:443/agent.ashx	MeshCentral WebSocket C2
Domain	bless-invite[.]com	SSO and invitation phishing lure
File	meshagent64-azure-ops.exe, meshagent32-azure-ops.exe, meshagent64-v2.exe	Customized MeshCentral agents
Path	/PSEMHUB/hub and /PSIGW/HttpListeningConnector	PeopleSoft exploitation endpoints
File	README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT	Extortion marker
SHA256	2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35	MeshCentral agent sample

Prioritized defensive guidance

Scoped to the typical higher education environment: PeopleSoft, Canvas or other LMS platforms, federated SSO, Microsoft 365, open research networks, decentralized IT and high staff and student turnover.

IMMEDIATE: ACT WITHIN 72 HOURS

1. Investigate and patch PeopleSoft immediately

Preserve evidence while checking for JSP webshells, XMLDecoder persistence, MeshCentral agents, zstd staging, sshpass and outbound SSH. Patch without delaying containment.

2. Restrict PSEMHUB and PSIGW to internal access

Remove public exposure and require VPN or management-network access.

3. Block known infrastructure and review historic logs

Hunt for azurenetfiles[.]net, the five staging IPs and 176[.]120[.]22[.]24 across the prior 60 to 90 days.

URGENT: ACT WITHIN 1 TO 2 WEEKS

4. Rework helpdesk identity verification

Do not approve connected apps, MFA resets or account recovery from inbound calls without callback and ticket verification.

5. Rotate Canvas and OAuth credentials

Verify breach scope, rotate Canvas API tokens and remove dormant SaaS grants.

6. Enforce phishing-resistant MFA

Use FIDO2 or WebAuthn for administrative, registry, HR, finance and research-data roles.

7. Prepare GDPR and UK GDPR response playbooks

Pre-approve supervisory authority and affected-person notification workflows for PeopleSoft data exposure.

INVESTIGATE AND TUNE DETECTIONS

8. Add PeopleSoft-specific SIEM rules

Alert on external PSEMHUB access, WebLogic child shells, JSP creation, sshpass and unusual zstd operations.

9. Prepare for GDPR-aware ransomware extortion

Create a pre-approved response for threats to notify regulators inside the 72-hour reporting window.

10. Improve offboarding and insider-risk visibility

Revoke all SSO, API and VPN credentials at departure and alert on bulk downloads by users with changing roles.

June source reports: ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit · ShinyHunters Exploits Oracle PeopleSoft Zero-Day to Breach Universities · Oracle PeopleSoft 0-Day RCE Flaw Under Active Exploitation by ShinyHunters · The ShinyHunters Domino Effect: One Breach, Hundreds of Victims · June 2026 weekly threat intelligence reports

APAC

EXECUTIVE SUMMARY

PeopleSoft zero-day exposure defines the June threat picture

APAC higher education faced a defining June 2026 threat through ShinyHunters exploitation of CVE-2026-35273 in Oracle PeopleSoft PeopleTools. The campaign operated from 27 May to 9 June before Oracle published its advisory on 10 June. More than 100 organizations were notified globally and 68 percent were higher education institutions. The only named university victim in the source set was the University of Nottingham, so APAC risk is assessed from the campaign's global scanning model, ShinyHunters' documented targeting history in Australia, Japan and India, and the broad use of PeopleSoft across the region.

KEY INSIGHTS

1	**CVE-2026-35273**, CVSS 9.8, enabled unauthenticated remote code execution against PeopleTools 8.61 and 8.62 through exposed PSEMHUB and PSIGW endpoints.
2	**ShinyHunters, tracked as UNC6240**, used MeshCentral agents, SSH credential spraying, zstd compression and outbound SSH exfiltration after exploitation.
3	**Sixty-eight percent of more than 100 targeted organizations were higher education institutions**, making this the most consequential sector campaign in the source set.
4	**Canvas LMS compromise and OAuth abuse** reinforced a SaaS domino-effect model in which one upstream breach can affect many universities.
5	**AI-powered vishing** using Bland AI and Vapi targeted helpdesk workflows, Okta or Microsoft SSO approvals and real-time MFA interception.
6	**No named APAC university ransomware victim was confirmed** in the source reports for June, so ransomware is treated as a secondary opportunistic risk rather than a confirmed regional incident trend.

Top threat entities and June trend shifts

- **ShinyHunters, UNC6240** CRIMINAL EXTORTION

PeopleSoft zero-day exploitation, Canvas-related supply chain activity, cloud data theft, AI vishing and insider recruitment.

- **Oracle PeopleSoft campaign** CAMPAIGN

Global scanning and exploitation of PSEMHUB and PSIGW endpoints, followed by MeshCentral deployment, SSH fan-out and data publication.

- **Canvas LMS compromise** SUPPLY CHAIN

A vendor-level breach pattern with potential downstream exposure for institutions relying on Canvas for course delivery and student data.

- **MeshCentral** REMOTE ACCESS TOOL

Customized agents named to resemble Azure operations software and beaconing to azurenetfiles[.]net over WebSocket TLS.

- **CryptoBandits** USB MALWARE

USB and LNK-based propagation relevant to shared computer labs and library workstations, with clipboard hijacking and cryptocurrency theft.

Trend shifts versus May 2026

1	**Zero-day exploitation replaced routine phishing as the defining sector event**, with direct targeting of university ERP infrastructure.
2	**AI voice social engineering entered the operational playbook**, creating a gap in standard phishing-awareness programs.
3	**SaaS concentration became a structural risk multiplier** across PeopleSoft, Canvas, Salesforce, Okta and Microsoft 365.

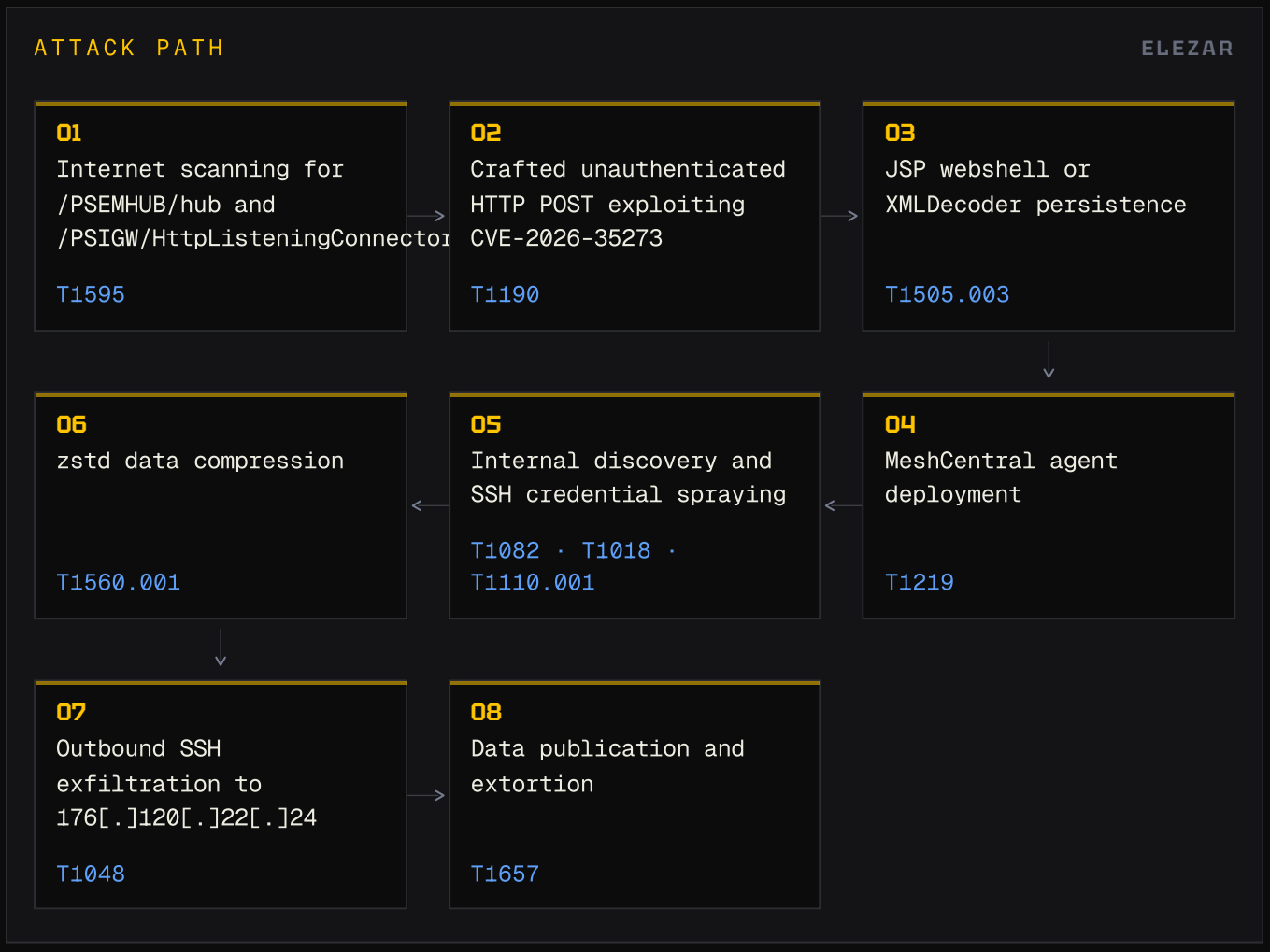
4

June report volume increased from 164 to 455, indicating a materially more active intelligence environment than May.

Attack chains, vulnerabilities and indicators

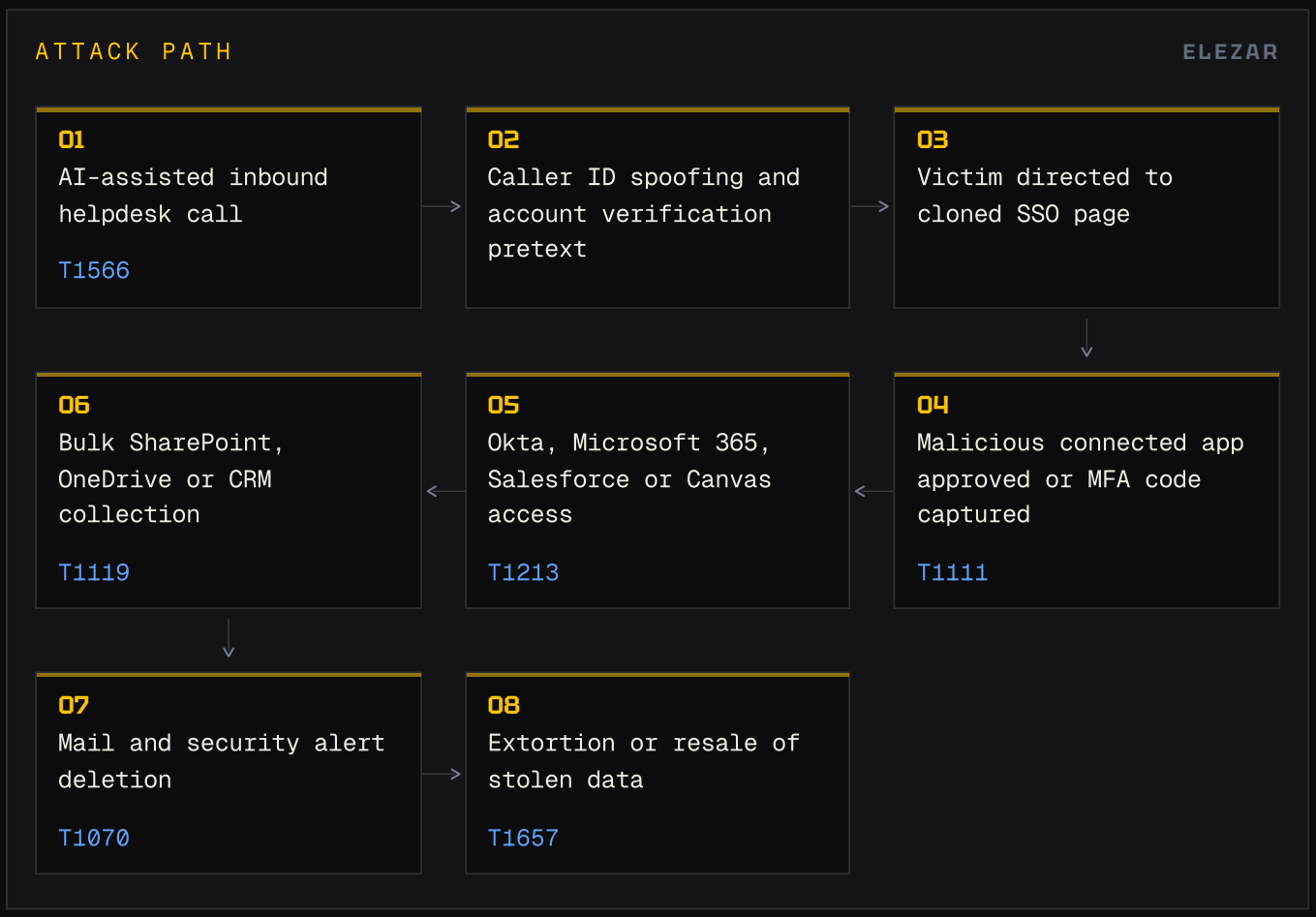
CVE	PRODUCT	CVSS	JUNE CONTEXT
CVE-2026-35273	Oracle PeopleSoft PeopleTools 8.61 and 8.62	9.8	Zero-day RCE actively exploited against higher education
CVE-2026-20253	Splunk Enterprise	9.8	Risk to university SIEM infrastructure
CVE-2026-48907	Joomla Widget Factory	9.8	Risk to public-facing university web portals
CVE-2024-6387	OpenSSH RegreSSHion	Critical	Relevant to university Linux and SSH infrastructure

Attack Chain 1: PeopleSoft zero-day to extortion



Source reports: ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit; Oracle PeopleSoft zero-day analyses

Attack Chain 2: AI vishing to cloud data theft



Source report: The ShinyHunters Domino Effect: One Breach, Hundreds of Victims

Selected high-value indicators

TYPE	INDICATOR	ASSOCIATION
IP	142[.]11[.]200[.]186 through 142[.]11[.]200[.]190	ShinyHunters staging infrastructure
IP	176[.]120[.]22[.]24	Data leak site mirror and exfiltration destination
Domain	azurenetfiles[.]net	MeshCentral C2 masquerading as Azure infrastructure
URL	wss://azurenetfiles[.]net:443/agent.ashx	MeshCentral WebSocket C2
Domain	bless-invite[.]com	SSO and invitation phishing lure
File	meshagent64-azure-ops.exe, meshagent32-azure-ops.exe, meshagent64-v2.exe	Customized MeshCentral agents
Path	/PSEMHUB/hub and /PSIGW/HttpListeningConnector	PeopleSoft exploitation endpoints
File	README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT	Extortion marker
SHA256	2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35	MeshCentral agent sample

Prioritized defensive guidance

Scoped to the typical higher education environment: PeopleSoft, Canvas or other LMS platforms, federated SSO, Microsoft 365, open research networks, decentralized IT and high staff and student turnover.

IMMEDIATE: ACT WITHIN 72 HOURS

1. Forensically assess all PeopleTools 8.61 and 8.62 systems

Treat any externally exposed PSEMHUB or PSIGW deployment present between 27 May and 9 June as potentially compromised. Hunt for unexpected JSP files, modified XML under envmetadata/data/environment, MeshCentral agents, sshpass use, zstd staging and outbound SSH.

2. Remove PSEMHUB and PSIGW from public exposure

Restrict /PSEMHUB/hub and /PSIGW/HttpListeningConnector to trusted internal ranges or VPN access only.

3. Block and retrospectively hunt ShinyHunters infrastructure

Block azurenetfiles[.]net, 142[.]11[.]200[.]186 through 142[.]11[.]200[.]190 and 176[.]120[.]22[.]24. Review at least 60 days of proxy, firewall and endpoint telemetry.

URGENT: ACT WITHIN 1 TO 2 WEEKS

4. Harden university helpdesks against AI vishing

Require callback verification and ticket-bound out-of-band codes for MFA resets, connected-app approvals and account recovery.

5. Audit OAuth and SaaS integrations

Revoke dormant or unexplained tokens across Canvas, Okta, Microsoft 365 and Salesforce. Verify vendor breach scope and rotate exposed API credentials.

6. Move privileged users to phishing-resistant MFA

Prioritize FIDO2, WebAuthn or passkeys for PeopleSoft administrators, finance, HR, registry and research data custodians.

7. Address insider recruitment risk

Use UBA for bulk downloads, tighten offboarding and monitor high-risk access changes involving SSO, VPN and Git platforms.

INVESTIGATE AND TUNE DETECTIONS

8. Deploy PeopleSoft-specific detections

Alert on external POSTs to PSEMHUB, WebLogic spawning shell tools, JSP creation in application directories, sshpass on application hosts and outbound SSH to unapproved destinations.

9. Reduce USB malware exposure

Disable or tightly control USB storage on shared lab systems and detect LNK execution from removable media.

10. Establish vendor breach notification SLAs

Require rapid disclosure, OAuth rotation support and annual token hygiene reviews from core SaaS vendors.

June source reports: ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit · ShinyHunters Exploits Oracle PeopleSoft Zero-Day to Breach Universities · Oracle PeopleSoft 0-Day RCE Flaw Under Active Exploitation by ShinyHunters · The ShinyHunters Domino Effect: One Breach, Hundreds of Victims · June 2026 weekly threat intelligence reports