IAM & SECURITY BRIEFING

IAM & Security Weekly Briefing

WEEK OF 2026-05-03 to 2026-05-09

Reporting window: Sunday–Saturday of the prior calendar week (does not include the current in-progress week).

---

1. Executive Summary (TL;DR)

- **Identity-driven SaaS extortion went mainstream.** ShinyHunters (UNC6040) deepened a months-long Salesforce-via-vishing campaign — Instructure's Canvas LMS (275M records / 3.65 TB / ~8,800 institutions) and Cushman & Wakefield (500K+ Salesforce records, May 6 extortion deadline) were named the same week, both traced back to OAuth/SSO abuse following voice phishing of help-desk and support staff. (The Hacker News, Bitdefender)
- **Cisco bought its way into the agentic-identity race.** On May 4, Cisco announced its ~$400M acquisition of Astrix Security to fold non-human identity (NHI) and AI-agent discovery, governance, and threat detection into Cisco Identity Intelligence, Secure Access, and Duo. (Cisco Blogs, SiliconANGLE)
- **Two actively-exploited identity-edge CVEs hit KEV.** CISA added Palo Alto Networks PAN-OS CVE-2026-0300 (unauthenticated buffer overflow → root RCE in the User-ID Authentication / Captive Portal, CVSS 9.3) on May 6, and an Ivanti EPMM improper-input-validation flaw on May 7. Patches for PAN-OS don't start shipping until May 13. (Palo Alto PSIRT, BleepingComputer)
- **State-sponsored vishing through Teams.** Rapid7 attributed a "Chaos ransomware" intrusion to Iran's MuddyWater — the attackers used external Microsoft Teams chats and screen-shares to harvest credentials, manipulate MFA, then planted ransomware artifacts as a false flag. (The Hacker News, SecurityWeek)
- **Passkeys crossed a real milestone.** On World Passkey Day (May 7) the FIDO Alliance reported ~5 billion passkeys in use globally; Microsoft simultaneously rolled out Entra passkeys for Windows sign-in and declared passwords a security risk. (FIDO Alliance / BusinessWire, Microsoft)
- **Supply chain ≠ just open-source.** Kaspersky disclosed a trojanized DAEMON Tools Lite installer signed with the vendor's legitimate certificate (active since April 8; v12.6 clean build shipped May 5), affecting thousands across 100+ countries with a likely China-nexus actor. (The Hacker News, Help Net Security)
- **Strategic signal:** identity is now the control plane. Okta Ventures' May 4 "2026 Identity 25" framed AI agents and deepfakes as the dominant threat model, and Keeper Security's "Identity Security at Machine Speed" report (published this week) found 72% of orgs can't detect credential misuse in real time. (Okta, PRNewswire / Keeper)

---

2. Top IAM & Security News

1. SHINYHUNTERS EXTORTS INSTRUCTURE / CANVAS — 275M EDUCATION RECORDS VIA SSO + SALESFORCE

On May 1 Instructure detected unauthorized activity on its Canvas LMS; by mid-week, ShinyHunters (UNC6040) had added Instructure to its leak site claiming exfiltration of 3.65 TB covering ~275M students, teachers, and staff at ~8,800 institutions. Reporting through the week (CNN, NPR, Bitdefender) confirmed exposure of names, school email addresses, student IDs, and private message content, plus a compromised Salesforce tenant. Initial access reportedly came via vishing of help-desk staff to abuse an Okta SSO account. - **Why it matters:** This is the second ShinyHunters hit on Instructure in eight months and a near-perfect case study of identity-led SaaS supply chain risk: one social-engineered SSO account → trusted OAuth scope → Salesforce data plane → 275M downstream identities. It also took finals week offline at thousands of US schools, an operational-impact dimension regulators have been waiting to see in an identity breach. - **Source:** CNN — Canvas hack stranded college students at finals week, Bitdefender technical advisory, Sentra governance analysis

2. CISCO TO ACQUIRE ASTRIX SECURITY (~$400M) — FIRST MAJOR TIER-1 BET ON AGENTIC IDENTITY

Announced May 4. Astrix specializes in discovery and governance of NHIs — service accounts, API keys, OAuth tokens, and AI agents. Cisco will fold it into Cisco Identity Intelligence and extend the capabilities into Cisco Secure Access and Duo IAM, covering agent lifecycle, just-in-time access, secrets management, and runtime threat detection. - **Why it matters:** This is the first nine-figure consolidation move specifically aimed at AI-agent identity, signaling that hyperscalers and security platforms now view NHI/agent identity as a primary control plane — not an add-on to human IAM. Expect competing platform plays from Palo Alto/CyberArk, Okta, and Microsoft Entra in Q3. - **Source:** Cisco Blogs, SiliconANGLE, SecurityWeek

3. CVE-2026-0300: PAN-OS USER-ID AUTHENTICATION PORTAL — UNAUTH RCE, EXPLOITED IN THE WILD

On May 6 Palo Alto Networks PSIRT disclosed a buffer-overflow flaw in the User-ID / Captive Portal of PA-Series and VM-Series firewalls (CVSS 9.3) that allows unauthenticated root RCE via crafted packets. CISA added it to KEV the same day. Patches are scheduled to roll out starting May 13 through May 28. - **Why it matters:** The User-ID authentication portal is where most identity-aware policy gets enforced at the perimeter; an unauthenticated takeover gives an attacker the box that authenticates everyone else. Restrict portal exposure to trusted IPs or disable it until patched — there is no signed fix yet. - **Source:** Palo Alto PSIRT — CVE-2026-0300, BleepingComputer, Help Net Security, Wiz

4. MUDDYWATER (IRAN) WEAPONIZES MICROSOFT TEAMS EXTERNAL CHAT FOR CREDENTIAL & MFA THEFT

Rapid7 published a write-up this week describing an intrusion at a US-based victim that masqueraded as a Chaos ransomware affiliate but had no encryption payload. The kill chain: external Microsoft Teams chat request → screen-share session → coached "support" walkthrough → credential and MFA-code capture → DWAgent / AnyDesk persistence → lateral movement → data exfil. Attribution tied to MuddyWater via a "Donald Gay" code-signing certificate. - **Why it matters:** Microsoft Teams external messaging is enabled by default in most tenants; this is the second high-profile cluster (after Storm-1811) to weaponize it. The intrusion shows nation-state actors are mimicking eCrime to muddy attribution while still focused on identity theft, not encryption. - **Source:** The Hacker News, Rapid7 blog, SecurityWeek

5. SHINYHUNTERS THREATENS CUSHMAN & WAKEFIELD — 500K+ SALESFORCE RECORDS, MAY 6 DEADLINE

Continuing the UNC6040 streak, ShinyHunters posted a final-warning leak countdown against Cushman & Wakefield, claiming over 500,000 Salesforce records (PII + internal corporate data) and demanding payment by May 6, 2026. Reported initial access mirrors the Instructure pattern: vishing → compromised SaaS SSO → Salesforce exfil. - **Why it matters:** Same TTPs, different industry. The Salesforce-via-vishing playbook is now a repeatable, multi-victim campaign — every Salesforce tenant with a help-desk reset workflow and an Okta/Entra SSO integration is in scope. - **Source:** Netcrook coverage, Computer Weekly — ShinyHunters Salesforce explainer

6. WORLD PASSKEY DAY 2026 (MAY 7) — ~5B PASSKEYS IN CIRCULATION; MICROSOFT RETIRES LEGACY PASSWORD FALLBACK

FIDO Alliance's *State of Passkeys 2026* (research across 11,000 consumers and 1,400 enterprise decision-makers in 10 countries) puts global passkeys at ~5 billion, with 75% of consumers having enabled at least one, 68% of organizations deploying for workforce, and 82% naming fully passwordless workforce sign-in as a goal. Microsoft used the day to declare passwords a security risk and roll Entra passkeys onto Windows (GA mid-June). The FIDO Alliance separately announced a workstream on "trusted AI agent interaction" standards. - **Why it matters:** Passkeys cleared the inflection point on adoption, but enterprise deployment is now the gating problem (recovery, device binding, cross-platform sync). The agent-interaction standards work is the more strategic signal — FIDO is moving to standardize how AI agents authenticate, not just humans. - **Source:** FIDO Alliance / BusinessWire, Microsoft Security blog, FIDO — AI agent interaction standards

7. OKTA UNVEILS THE "2026 IDENTITY 25" — IDENTITY REFRAMED AS THE CONTROL PLANE

On May 4 Okta Ventures published the third edition of its Identity 25, themed *identity is the control plane*. The report names the 25 builders shaping post-AI-agent identity and bluntly states that authentication alone — even strong MFA — is no longer enough as agentic AI and deepfake-driven impersonation scale. - **Why it matters:** It's a vendor list, but the strategic positioning is the news: Okta is publicly arguing that identity-security buyers should expect continuous verification + agent identity governance to become non-negotiable line items in 2026 RFPs. - **Source:** Okta press release, LV Sun mirror

8. CISA KEV ADDITIONS: IVANTI EPMM RCE (MAY 7)

CISA added an Ivanti Endpoint Manager Mobile (EPMM) improper-input-validation vulnerability to the Known Exploited Vulnerabilities catalog on May 7. The flaw lets a remotely authenticated admin achieve RCE on the EPMM server — a high-impact secondary path once an admin credential is phished. Federal agencies have the standard 21-day remediation clock. - **Why it matters:** EPMM manages corporate mobile identity and configuration profiles; an admin RCE means push-down of malicious configuration policies to every enrolled device. Pair the EPMM and PAN-OS KEV additions and the week's KEV story is: identity-aware appliances are the active battleground. - **Source:** CISA KEV catalog

---

3. AI, Identity & Emerging Tech

CISCO–ASTRIX AND THE FORMALIZATION OF "AGENT IDENTITY"

The Cisco/Astrix deal (above) cleanly maps onto a new product category: discover every AI agent, map its NHIs and excessive scopes, govern its lifecycle (creation → rotation → decommission), and detect runtime drift like out-of-policy actions or compromised credentials. Expect the language of *agent identity* to start showing

up in Gartner Magic Quadrants and federal procurement. - **Implications:** SOC teams need a single inventory of human + non-human + agent identities or risk drift across three parallel governance models. Most CIAM / IGA stacks today only cover one. - **Source:** Cisco announcement

FIDO ALLIANCE TO DEVELOP "TRUSTED AI AGENT INTERACTION" STANDARDS

Announced April 27 but the workstream officially picked up momentum on World Passkey Day. FIDO is positioning to define how AI agents authenticate to APIs and SaaS the way it defined how humans authenticate to phones and laptops. - **Implications:** If this lands, the era of agents authenticating via long-lived API keys ends. Enterprises should start cataloging which automated workflows currently rely on bearer tokens — those become migration targets within ~18 months. - **Source:** FIDO Alliance / BusinessWire

GOOGLE CLOUD + WIZ: AI-AWARE EXTENSION THREAT DETECTION AND SHADOW-AI REPORTING (PREVIEW)

Google Cloud Next '26 messaging extended into the week with previews of *AI-aware extension threat detection* in Security Command Center and *shadow AI reporting* surfacing unsanctioned employee AI/SaaS use. Wiz announced agent-platform coverage for AWS Agentcore, Gemini Enterprise Agent Platform, Azure Copilot Studio, and Salesforce Agentforce. - **Implications:** Detection vendors are racing to instrument agent-platform telemetry. If you've already deployed any agent platform, lean on the platform's native telemetry rather than waiting for a single-pane-of-glass — fragmentation is the realistic 2026 state. - **Source:** Google Cloud blog

KEEPER SECURITY: 89% OF IT LEADERS LOSING THE IDENTITY-FOOTPRINT RACE

Identity Security at Machine Speed (released this week) surveyed global IT/security leaders. Headline numbers: 89% report difficulty managing the growing identity footprint as AI expands; 72% can't detect credential misuse in real time; 46% say AI-powered tools have access to critical systems and 76% of those identities are not consistently governed under PAM policies. - **Implications:** If you can't answer "what AI/automation has prod-database access and when was its credential last rotated" in under 5 minutes, you're in the 76%. - **Source:** PRNewswire — Keeper Security release, Yahoo Finance mirror

---

4. Cyber Threats & Attack Trends

A) VISHING → SSO → SAAS DATA PLANE (UNC6040 / SHINYHUNTERS)

The Instructure and Cushman & Wakefield breaches share an identity-centric kill chain: voice-phishing of help-desk or support staff → password / MFA reset of an SSO account (most often Okta) → privileged Salesforce or LMS access via OAuth → mass data exfil → leak-site extortion. Vishing now accounts for ~23% of cloud-related initial compromises, ahead of stolen credentials, email phishing, and exploits. - **Source:** Varonis on UNC6040 vishing, Halcyon ShinyHunters extortion analysis

B) MICROSOFT TEAMS EXTERNAL-CHAT SOCIAL ENGINEERING (MUDDYWATER + STORM-1811 LINEAGE)

Adversaries are moving social engineering off email and into Teams because it bypasses the bulk of email security and inherits Microsoft's trust UI. The MuddyWater intrusion (above) used external chat → screen share → live coaching to defeat MFA — same pattern Storm-1811 used in 2024–25. - **Source:** The Hacker News on MuddyWater, CybersecurityNews — MFA manipulation via Teams

C) IDENTITY-EDGE APPLIANCE EXPLOITATION (PAN-OS, IVANTI EPMM)

Two KEV additions this week target the very appliances enterprises trust to enforce identity at the perimeter and on mobile devices. Both fit a longer pattern of edge-device privilege escalation that, once chained, yields persistent identity-context access (User-ID mappings, MDM policy push, certificate stores). - **Source:** Palo Alto PSIRT, CISA KEV

D) SIGNED-INSTALLER SUPPLY CHAIN ATTACKS (DAEMON TOOLS)

DAEMON Tools Lite installers signed with the vendor's legitimate certificate distributed backdoors from April 8 through early May 2026. Telemetry across 100+ countries; targeting included government and scientific entities. Code signing failed as a trust anchor because the signing key itself was the compromised identity. - **Source:** The Hacker News, TechCrunch — China-nexus attribution

E) STOLEN-TOKEN PERSISTENCE AFTER SSO COMPROMISE

The Bitdefender and Sentra writeups on Instructure both flagged that even after detecting unauthorized SSO activity on May 1, Instructure's incident timeline shows attackers continuing to operate via valid OAuth tokens — a reminder that revocation must include OAuth/refresh tokens, not just user sessions. - **Source:** Sentra governance analysis, Obsidian — OAuth token abuse attack surface

---

5. Product Updates & Vendor News

- **Microsoft Entra — Entra passkeys on Windows (rolling out late April → GA mid-June 2026).** Phishing-resistant passwordless sign-in to Windows + Entra resources, announced/expanded for World Passkey Day. (BleepingComputer, Microsoft)
- **Microsoft Entra — workload-identity auth for SAP SuccessFactors (May 2026).** Replaces basic auth in SuccessFactors provisioning apps; matters because workload-identity auth removes a long-lived secret. (Microsoft Learn)
- **Microsoft Defender for Cloud — broader multicloud posture for AWS + GCP (May 2026 release wave).** Adds discovery/posture for identity, secrets, AI/ML, analytics, DevOps. (Microsoft Learn)
- **Google Cloud — simplified IAM predefined roles, role picker UX, re-auth for sensitive actions, AI-aware extension detection, shadow-AI reporting (Next '26 follow-on).** (Google Cloud Blog)
- **Cisco — announces intent to acquire Astrix Security (~$400M) for NHI/agent identity; integrates into Cisco Identity Intelligence, Secure Access, Duo.** (Cisco Blogs)
- **Okta — Identity 25 (May 4) and Business at Work 2026 APAC findings; agentic-identity positioning ahead of Q4 FY26 earnings.** (Okta press release, Futurum — Okta Q4 FY26 agentic positioning)
- **DAEMON Tools Lite v12.6 (May 5) — first clean build after April 8 supply chain compromise.** (Help Net Security)

---

6. Notable Research & Reports

FIDO ALLIANCE — *STATE OF PASSKEYS 2026* (MAY 7)

Surveys of 11,000 consumers + 1,400 enterprise decision-makers across 10 countries. Headline stats: 90% passkey awareness, 75% of consumers enabled at least one, 49% use regularly when available, 68% of orgs deploying for workforce, 82% naming fully passwordless as a goal. Strategic implication: passkey adoption is

no longer the question — *workforce* and *agent* passkey strategy is. - **Source:** BusinessWire — FIDO Alliance release

KEEPER SECURITY — *IDENTITY SECURITY AT MACHINE SPEED* (MAY 2026)

89% of IT leaders struggling with identity-footprint expansion under AI. 72% can't detect credential misuse in real time. 43% globally (51% in US) name AI-related NHI management as a top identity governance gap. 46% of respondents report AI tools have access to critical systems; 76% of those identities not consistently governed. - **Source:** PRNewswire — Keeper Security release

OKTA — *2026 IDENTITY 25* (MAY 4)

Theme: *identity is the control plane*. Frames deepfakes and agentic AI as the new dominant threat model and pushes "continuous identity verification" past static MFA. - **Source:** Okta press release

IBM — *X-FORCE THREAT INTELLIGENCE INDEX 2026* (MOST-CITED CARRYOVER)

Public-facing app exploitation surged 44%, overtaking stolen credentials as the top entry vector (40% vs 32%) — but stealer-driven credential theft and infostealer logs remain a foundational secondary path (300K+ ChatGPT credentials observed on dark web markets). 109 extortion groups tracked in 2025 (up from 73). - **Source:** IBM Think — X-Force 2026 identity recap

---

7. Practical Security Takeaways

1. **Patch / mitigate CVE-2026-0300 today.** No PAN-OS fix until May 13. Until then: restrict User-ID Authentication Portal to trusted internal IPs only, or disable it where not strictly required.
2. **Disable Microsoft Teams external chat by default** (or restrict to allow-listed domains). The MuddyWater intrusion proves the Teams attack pattern is now nation-state grade — not just eCrime.
3. **Treat help-desk identity reset as a critical attack path.** Require callback to verified channels + at least one out-of-band factor before resetting MFA or SSO credentials; ban screen-shared MFA workflows; deploy verifiable caller-ID for IT/help-desk reset calls.
4. **Inventory and revoke OAuth tokens after any SSO compromise.** Session revocation is not enough — Instructure's timeline shows attackers running on valid OAuth tokens after the user account was already flagged. Build a runbook that revokes app-grant + refresh tokens, not just the session.
5. **Pin and rotate code-signing keys; verify reproducible builds for installers.** The DAEMON Tools attack used a valid signature — codesign on its own is no longer a trust anchor.
6. **Build a single NHI / agent identity inventory.** Discover every API key, service account, OAuth grant, and AI agent; tag with owner, scope, last-used, and last-rotated. Cisco/Astrix, Okta, and Microsoft will all be selling this in Q3 — but you can start with a spreadsheet now.
7. **Start the Entra passkeys on Windows pilot before June.** Phishing-resistant workforce sign-in is the highest-leverage control against the Teams-vishing + Salesforce-vishing pattern dominating Q2 2026 — and the GA window is six weeks away.
8. **Adopt phishing-resistant MFA, not just "any MFA."** Per CISA/NSA guidance: FIDO2/WebAuthn / passkeys or PIV/CAC. Push-based MFA and OTP are now actively defeated by vishing + screen-share coaching.
9. **Patch Ivanti EPMM immediately** and audit admin sign-in events for the last 14 days for any unusual geos / impossible travel.

10. **Add a SaaS-tenant "blast radius" exercise to your tabletop.** Specifically: "if our help desk gets vished and a single Okta admin is compromised, what data — across every SaaS app — is reachable in 60 minutes?" This is now a board-level question.

---

8. Trends to Watch

- **Agent identity becomes a first-class product category.** Cisco/Astrix is the catalyst; expect Microsoft, Okta, Palo Alto/CyberArk, and HashiCorp/IBM to all stake claims by end of Q3 2026. CISOs should resist single-vendor lock-in until the category stabilizes.
- **Continuous identity verification displaces "just MFA."** Vishing + deepfakes have collapsed the trust we used to put in successful authentication — risk-scored, ongoing verification (behavior, device posture, session anomalies) becomes the new floor.
- **FIDO standards for AI agents.** The FIDO Alliance's *Trusted AI Agent Interactions* workstream could end long-lived API keys for agents within 18–24 months. Start tagging which workflows would need to migrate.
- **Salesforce / SaaS-tenant breaches become the new "datacenter breach."** The Salesforce-via-vishing playbook now has 760+ confirmed victims across the 2025–26 ShinyHunters/Scattered Spider arc — every SaaS tenant with help-desk-driven SSO is exposed.
- **Identity-edge appliances are the active battleground.** PAN-OS User-ID, Ivanti EPMM, SonicWall SSL VPN, Citrix NetScaler — anything that sits at the intersection of identity and the network edge is being actively exploited or chained. Expect a steady drumbeat of KEV additions through Q2.

---

9. Tool / Resource of the Week

CISA + NIST IR 8597 — *Protecting Tokens and Assertions from Forgery, Theft, and Misuse* (initial public draft). - **What it does:** Provides implementation guidance for federal agencies and CSPs on protecting OAuth, SAML, and OIDC tokens — exactly the artifacts at the center of this week's Instructure / Cushman & Wakefield breaches. - **Why it's useful:** It's the most concrete public guidance currently available on token theft / replay defenses (binding, lifetime, revocation, monitoring) and is becoming a de-facto enterprise baseline even outside federal. - **Source:** CISA — NIST IR 8597 draft announcement, CISA resource page

---

10. Sources

- Canvas hack strands college students at finals week — CNN
- Canvas is back online, but questions linger — NPR
- Technical Advisory: ShinyHunters Breach of Instructure Canvas LMS — Bitdefender
- ShinyHunters Launches Second Major Attack on Instructure Canvas LMS — Rescana
- How the Instructure Salesforce Breach Exposed a Major Data Governance Gap — Sentra
- Education Sector in the Crosshairs: ShinyHunters' Extortion Campaign — Halcyon
- ShinyHunters Salesforce cyber attacks explained — Computer Weekly
- ShinyHunters Breach: Cushman & Wakefield Salesforce Data Leak Threat — Netcrook
- What Salesforce Organizations Need to Know About ShinyHunters and Vishing — Varonis

- The new attack surface: OAuth Token Abuse — Obsidian Security
- Securing the Agentic Workforce: Cisco to Acquire Astrix Security — Cisco Blogs
- Cisco buys Astrix Security to strengthen AI agent discovery and governance — SiliconANGLE
- Cisco Moves to Acquire Astrix Security to Tackle Non-Human Identity Risks — SecurityWeek
- Cisco to Acquire Astrix Security — Cybersecurity News
- CVE-2026-0300 PAN-OS Buffer Overflow in User-ID Authentication Portal — Palo Alto Networks PSIRT
- Palo Alto PAN-OS Flaw Under Active Exploitation — The Hacker News
- Palo Alto Networks warns of firewall RCE zero-day — BleepingComputer
- Root-level RCE in Palo Alto firewalls (CVE-2026-0300) — Help Net Security
- Critical Buffer Overflow in PAN-OS Exploited In-the-Wild — Wiz
- MuddyWater Uses Microsoft Teams to Steal Credentials — The Hacker News
- Muddying the Tracks: State-Sponsored Shadow Behind Chaos Ransomware — Rapid7
- Iranian APT Intrusion Masquerades as Chaos Ransomware — SecurityWeek
- Hackers Use Microsoft Teams to Steal Credentials and Manipulate MFA — CybersecurityNews
- DAEMON Tools Supply Chain Attack Compromises Official Installers — The Hacker News
- DAEMON Tools compromised backdoors supply chain attack — Help Net Security
- Kaspersky suspects Chinese hackers planted backdoor in Daemon Tools — TechCrunch
- Government, Scientific Entities Hit via Daemon Tools — SecurityWeek
- FIDO Alliance Reports Accelerating Global Passkey Adoption — BusinessWire
- FIDO Alliance to Develop Standards for Trusted AI Agent Interactions — BusinessWire
- World Passkey Day: Advancing passwordless authentication — Microsoft Security Blog
- Microsoft Entra brings phishing-resistant sign-in to Windows — BleepingComputer
- Microsoft Entra releases and announcements — Microsoft Learn
- Microsoft Defender for Cloud release notes — Microsoft Learn
- Next '26: Redefining security for the AI era with Google Cloud and Wiz — Google Cloud Blog
- Okta Ventures Unveils 2026 Identity 25 — Okta Newsroom
- Okta Q4 FY 2026 Earnings — Agentic Identity Positioning — Futurum
- Keeper Security Research: 89% of IT Leaders Struggle to Manage Identity Footprint — PRNewswire
- Keeper Security Exposes Critical Gaps in Securing AI Agents and NHIs — Yahoo Finance
- 2026 X-Force Threat Intelligence Index: Securing identities, AI detection, risk management — IBM Think
- NIST/CISA Draft IR 8597 — Protecting Tokens and Assertions — CISA
- CISA Known Exploited Vulnerabilities Catalog — CISA KEV
- ThreatsDay Bulletin (week of May 5, 2026) — The Hacker News
- Weekly Intelligence Report — 08 May 2026 — CYFIRMA
- May 2026 Data Breaches: List Major Incidents & Latest Updates — SharkStriker
- Millions of students' personal data stolen in major education breach — Malwarebytes