IAM & SECURITY BRIEFING

IAM & Security Weekly Briefing

WEEK OF 2026-04-26 to 2026-05-02

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

---

1. Executive Summary (TL;DR)

- **Identity-led breach goes mainstream:** ADT confirmed a ShinyHunters intrusion that began with a vishing call against a help desk, ended with a hijacked **Okta SSO** account, and exfiltrated **5.5 million** customer records from Salesforce — a textbook identity-first kill chain that did not need a single zero-day. (BleepingComputer)
- **CISA forces a national auth-bypass patch sprint:** CISA added **CVE-2026-41940** (pre-auth bypass in cPanel & WHM, CVSS 9.8) to the KEV catalog after evidence of active exploitation against government and MSP targets. Roughly **1.5 million** internet-exposed cPanel hosts are in scope. (CyberScoop, Picus)
- **Zero Trust crosses the IT/OT line:** CISA, FBI, DOE, DOS, and DoW jointly released "Adapting Zero Trust Principles to Operational Technology," explicitly mandating continuous identity validation for both human and machine identities in OT. (CISA)
- **Microsoft pushes phishing-resistant auth to every Windows endpoint:** Entra ID passkeys started rolling out to corporate, personal, and **shared/unmanaged** Windows devices, stored in the Windows Hello container and never sent over the wire. (BleepingComputer)
- **Identity telemetry is going multi-cloud, multi-IdP:** Microsoft Sentinel UEBA expanded to ingest behavioral signals from AWS, GCP, and **Okta**, narrowing the gap between IT estate detection and identity-provider detection. (Microsoft Security Blog)
- **OAuth supply-chain risk keeps compounding:** Reporting throughout the week traced the Vercel incident back to **Context.ai** OAuth tokens harvested by Lumma Stealer two months earlier — a single infostealer infection that became a cross-tenant SaaS compromise. (The Hacker News, Trend Micro)
- **Strategic implication:** Every major story this week — ADT, cPanel, Vercel, OT Zero Trust — converges on the same point: identity (human, machine, and AI agent) is now the primary control plane and the primary attack surface. Patch cadence still matters, but identity hygiene is what determines blast radius.

---

2. Top IAM & Security News

ADT Confirms 5.5M-Record Breach After Vishing → Okta SSO → Salesforce Chain - ADT confirmed unauthorized access first detected on April 20 after ShinyHunters set a public extortion deadline of April 27. Reporting throughout the window detailed the full attack path: a voice-phishing call against an employee, takeover of that employee's **Okta SSO** account, and exfiltration of customer data from the connected

Salesforce instance. The leak ultimately exposed names, phone numbers, addresses, and a smaller subset of DOBs and partial SSN/tax IDs for 5.5M people. - **Why it matters:** This is the prototypical 2026 identity breach — no malware on ADT's network, no exploit, no zero-day. A single help-desk-style social engineering call against a federated identity owner produced enterprise-wide impact via a downstream SaaS. Service desks remain the soft underbelly of even mature IAM programs. - **Source:** BleepingComputer, SC Media

CISA Adds cPanel/WHM Authentication Bypass (CVE-2026-41940) to KEV Catalog - On April 30, CISA added CVE-2026-41940 — a pre-authentication remote auth bypass in cPanel & WHM (CVSS 9.8) — to its Known Exploited Vulnerabilities catalog after Ctrl-Alt-Intel and others reported active exploitation. The flaw chains a CRLF injection in the session writer with a malformed-cookie encryption skip to "promote" an injection into a privileged login. Exploitation has been observed since approximately late February, meaning this was a true zero-day for two months before cPanel's emergency patch on April 28. - **Why it matters:** Roughly **1.5 million** cPanel instances are exposed to the internet, and the early targeting profile (Philippines `*.mil.ph` / `*.gov`, Laos `*.gov.la`, MSPs, hosting providers) suggests state-aligned interest. A pre-auth bypass on a hosting management plane is effectively a privileged identity, granting attackers "first user" status without needing to compromise a credential at all. - **Source:** CyberScoop, The Hacker News, watchTowr Labs

CISA, FBI, DOE, DOS, and DoW Publish Joint Zero Trust Guidance for OT - On April 30, CISA and four federal partners released "Adapting Zero Trust Principles to Operational Technology," the first joint federal guide focused on translating Zero Trust into OT and ICS environments. The document mandates **continuous validation of both human and machine identities**, recommends MFA wherever technically feasible, and emphasizes asset inventory, behavioral baselining, and micro-segmentation between IT and OT networks. - **Why it matters:** This shifts identity-centric security from an IT-only discipline to a federally endorsed expectation for critical infrastructure. Expect this guide to anchor future regulator and insurer expectations for utilities, manufacturing, water, and pipelines. - **Source:** CISA, Infosecurity Magazine, Industrial Cyber

Microsoft Begins Rolling Entra Passkeys to All Windows Devices - Microsoft started rolling Entra ID passkeys to Windows devices for phishing-resistant passwordless sign-in to any Entra-protected resource, with general availability targeted by mid-June 2026. The rollout includes corporate-managed, personal, and **shared/unmanaged** Windows devices, with admin controls via Conditional Access and Authentication Methods policies. Passkeys are stored in the Windows Hello container, are device-bound, and are never transmitted across the network. - **Why it matters:** This is the largest single expansion of phishing-resistant authentication for the Microsoft ecosystem to date. Combined with Microsoft pushing **external MFA** support in Entra ID to GA at RSAC, the legacy "username + OTP" pattern now has a vendor-supported, default replacement for the world's largest enterprise identity estate. - **Source:** BleepingComputer, TechRadar

Microsoft Sentinel UEBA Expands to AWS, GCP, and Okta - On April 28, Microsoft announced an expanded UEBA footprint that ingests behavioral signals from AWS (and AWS defense scenarios specifically), GCP, and Okta authentication logs alongside existing Entra signal. This brings cross-IdP behavioral detection — failed logins, atypical resource access, anomalous role assumptions — under a single analytics layer. - **Why it matters:** Most enterprises run more than one IdP and more than one cloud. Until this update, identity-anomaly detection was largely siloed by vendor. Bringing Okta into Sentinel UEBA shrinks the gap that ADT-style help-desk takeovers exploit, and it lays groundwork for cross-cloud session-risk scoring. - **Source:** Microsoft Security Blog

Vercel Incident Traced to Context.ai OAuth Supply Chain - New reporting during the window connected Vercel's April 19 disclosure to a stolen OAuth token issued by **Context.ai**, a third-party AI Office Suite. The original compromise has been traced to a Lumma Stealer infection on a Context.ai employee in approximately February 2026; the attacker then pivoted through OAuth into Vercel two months later. - **Why it matters:** A second-degree SaaS supply chain breach where the trigger was a single infostealer log from a small AI vendor. OAuth grants long-lived, broad-scope access by default, and most enterprises do not maintain inventory of

third-party OAuth grants. Expect "OAuth grant inventory" to move up the audit checklist this quarter. - **Source:** The Hacker News, Trend Micro, Cloud Security Alliance

---

3. AI, Identity & Emerging Tech

AI Agents Get First-Class Identity Treatment From Hyperscalers - Following the Google Cloud Next '26 announcements that anchored attention earlier in the month, vendor messaging through this week reinforced that AI agents now require their own scoped identities, authentication flows, and human-delegation models — not reused service accounts. Okta has expanded its support for registering, securing, and governing AI agent identities directly within the platform. - **Security implications:** Agent identity is moving out of the "research" bucket and into mainstream IAM roadmaps. Treating an agent as just another OAuth client is no longer adequate; agents need an audit trail back to a human owner, scoped delegation, and revocable credentials. (Google Cloud, Okta)

Non-Human Identities Outnumber Humans by 40:1 to 100:1 - New analysis circulating during the window reaffirmed that NHIs (service accounts, API keys, workload identities, agentic identities) outnumber human identities by ratios of 40:1 to over 100:1, reaching 500:1 in hyper-automated environments. Roughly **78%** of organizations report having no formal policy for creating or removing AI identities, and **92%** lack confidence that legacy IAM tooling can manage AI/NHI risk. - **Security implications:** The legacy NHI playbook (rotate keys, audit service accounts) does not scale to ephemeral, autonomous agents. Identity governance vendors that can track agent provenance and lineage will see acceleration; legacy IGA is increasingly insufficient on its own. (CSO Online, Cyber Strategy Institute)

AI-Powered Vishing Becomes a Repeatable Breach Pattern - The ADT incident this week is not an outlier. Across the security press, AI-generated voice scams have escalated from "novelty risk" to repeatable enterprise breach pattern; help desks and SSO admins are the most exploited choke points. Group-IB and others continue to report fully automated AI scam call centers combining synthetic voice, LLM coaching, and inbound AI responders. - **Security implications:** Voice cannot be trusted as a verification channel. Help-desk and IT-support workflows must require an out-of-band, phishing-resistant identity proof before any password reset, MFA reset, or session re-issuance — the same controls used for high-risk transactions. (Group-IB)

---

4. Cyber Threats & Attack Trends

Vishing → Federated SSO Takeover (ADT pattern) - **Attack description:** Threat actor calls a help desk or employee, impersonates internal staff, and convinces the target to reset MFA or share a session token. - **How identity was exploited:** Compromised Okta SSO account → blanket access to every federated SaaS the user could reach. - **Techniques used:** Voice phishing (vishing), MFA fatigue/bypass, downstream SaaS pivoting. - **Real-world example:** ADT (5.5M records via Okta + Salesforce, this week). - **Source:** BleepingComputer

Pre-Auth Bypass for Privileged Hosting Identity (cPanel CVE-2026-41940) - **Attack description:** Pre-auth, network-reachable bypass in cPanel/WHM allowing attackers to assume privileged session state without credentials. - **How identity was exploited:** The flaw effectively grants attacker-controlled "first user" identity on the hosting management plane. - **Techniques used:** CRLF injection in session writer, malformed-cookie encryption skip, session cache abuse. - **Real-world example:** Targeting of `.mil.ph`, `.ph`, `.gov.la` and MSP/hosting plane infrastructure observed May 2. - **Source:** Picus Security, The Hacker News

OAuth Supply Chain Pivoting - **Attack description:** Compromise of a small SaaS vendor leads to OAuth token theft, then long-dwell pivoting into much larger downstream tenants. - **How identity was exploited:**

Stolen OAuth grant ≈ stolen identity, with broad scopes that survive password rotation and (often) MFA. - **Techniques used:** Lumma Stealer infection → OAuth token theft → cross-tenant SaaS access. - **Real-world example:** Vercel ↔ Context.ai chain, with reporting filling in details across the window. - **Source:** Trend Micro

Infostealer-Fueled Identity Takeover - **Attack description:** Commodity infostealers (Lumma, RedLine, etc.) silently harvest cookies, OAuth tokens, and saved credentials from compromised endpoints, then sell them in bulk. - **How identity was exploited:** Stolen sessions reused to bypass MFA via cookie replay; stolen OAuth tokens reused across hundreds of victim tenants. - **Techniques used:** Endpoint malware, credential/cookie theft, token replay, AiTM relay. - **Real-world example:** The same Lumma Stealer pattern that drove the Vercel/Context.ai chain; F5 reporting on the multi-billion credential leak underscores the scale. - **Source:** F5 Labs

---

5. Product Updates & Vendor News

Microsoft Entra - **What changed:** Phishing-resistant Entra ID passkeys rolling to Windows (corporate, personal, shared/unmanaged), stored in Windows Hello container; targeted GA mid-June 2026. - **Why it matters:** Removes most credential-replay and AiTM token-theft attack surface for Entra-protected apps when adopted broadly. - **Source:** BleepingComputer

Microsoft Sentinel - **What changed:** UEBA expanded to AWS, GCP, and Okta, with an explicit AWS-defense scenario blog on April 28. - **Why it matters:** Cross-IdP, cross-cloud behavioral analytics under one detection layer reduces the seam attackers like ShinyHunters exploit when an Okta-only signal is invisible to AWS-only tooling. - **Source:** Microsoft Security Blog

Okta - **What changed:** April release notes (2026.04.0) include AI agent identity registration/governance inside Okta, search-enabled IdP picker for >10 IdPs, and Express Submission for OIN/Auth0 SaaS apps. Okta Privileged Access (April 15) now resumes AD account discovery from the last successful stage on timeout, reducing processing time. - **Why it matters:** Okta is moving agent identity into the standard IAM control plane rather than treating it as an out-of-band capability — relevant given ADT-style attacks specifically targeted Okta SSO this week. - **Source:** Okta Release Notes, Okta PAM Release Notes

cPanel (WebPros) - **What changed:** Emergency patch released on April 28 for CVE-2026-41940; CISA forced federal patching deadlines through KEV inclusion on April 30. - **Why it matters:** Roughly 1.5M instances are in scope, and a pre-auth bypass on a hosting plane is effectively unauthenticated identity escalation. Patch is mandatory. - **Source:** Rapid7, CISA KEV alert

Google Cloud / Wiz - **What changed:** Continued reinforcement of the Next '26 Agent Identity model (unique agent identities, scoped human delegation) and the Agentic Defense partnership between Google Security Operations and Wiz. - **Why it matters:** Agent Identity is becoming a first-class concept in cloud IAM rather than a research artifact, aligning with the Microsoft/Okta direction this week. - **Source:** Google Cloud Blog

---

6. Notable Research & Reports

CISA Joint Guide — "Adapting Zero Trust Principles to Operational Technology" (April 30, 2026) - **Key findings:** OT environments cannot inherit IT-centric Zero Trust patterns wholesale; the guide prioritizes asset visibility, continuous identity validation for human and machine identities, MFA where feasible, and aggressive micro-segmentation between IT and OT. - **Strategic implications:** This is now the de facto federal reference architecture for OT identity. Expect insurer and regulator alignment, especially in water, energy, manufacturing, and pipelines. - **Source:** CISA

Verizon 2026 DBIR — Identity-Centric Findings - **Key findings:** Stolen credentials remain the most common initial-access vector at **22%** of breaches; **88%** of basic web app attacks involve stolen credentials; infostealers compromised **30%** of corporate and **46%** of unmanaged devices holding company credentials; **15%** of staff accessed GenAI tools, with **72%** doing so via personal email accounts. - **Strategic implications:** Identity is the modal attack surface, and personal-account GenAI usage is creating credential bleed-through that few enterprises have visibility into. - **Source:** Verizon DBIR

State of NHI and AI Security (referenced this week) - **Key findings:** NHI-to-human ratios of 40:1 to 100:1; 78% of organizations have no formal AI-identity lifecycle policy; 92% lack confidence in legacy IAM for AI/NHI. - **Strategic implications:** AI identity governance is the next big audit and tooling category — and a clear gap in most current IGA programs. - **Source:** Cloud Security Alliance

---

7. Practical Security Takeaways

1. **Treat the help desk as Tier 0 identity infrastructure.** Mandate phishing-resistant, out-of-band proof (FIDO2/passkey or video-call with verified ID) before any MFA reset, password reset, or SSO recovery. The ADT attack chain dies at this control.
2. **Patch CVE-2026-41940 today.** If you run cPanel/WHM directly or via a hosting provider, confirm the April 28 patch is applied, audit for indicators of compromise back to late February, and rotate any administrative credentials and API tokens that traversed those hosts.
3. **Inventory and prune third-party OAuth grants.** Pull the list of SaaS-to-SaaS OAuth grants in Microsoft 365, Google Workspace, Salesforce, Snowflake, and your code/CI platforms. Revoke anything unused, scope down anything broader than needed, and add OAuth grant changes to your monitoring.
4. **Roll passkeys to Windows now, not "later this year."** Microsoft has removed the last excuses by extending Entra passkeys to shared and unmanaged Windows devices. Stage rollout to high-risk roles (admins, finance, exec assistants, help desk) first.
5. **Fold Okta (and any non-Microsoft IdP) into your UEBA.** Sentinel UEBA now ingests Okta; if you use a different SIEM/XDR, ensure Okta system logs feed it with the same anomaly rules you run on Entra. Cross-IdP correlation is what would have flagged the ADT session takeover earlier.
6. **Establish an AI-agent identity policy before agents proliferate.** Define how agents get created, who owns them, what scopes they can hold, how their actions are logged, and how they are revoked. 78% of organizations have no such policy — do not be one of them.
7. **Assume infostealer compromise of contractors and small SaaS vendors.** Vercel/Context.ai shows that a Lumma infection on a vendor's laptop two months ago can become your incident this week. Require that vendors with OAuth into your tenant maintain endpoint detection and rotate refresh tokens regularly.
8. **Apply CISA's Zero Trust OT guidance to your OT roadmap.** Even if you are not directly mandated, the document is now the reference text — adopting it preempts insurer and regulator pressure.
9. **Monitor for vishing precursors.** Pretexting reconnaissance against help desks and finance often precedes the actual call. Detect rising volumes of failed verification questions, repeated callback requests, and out-of-hours HR/IT impersonation attempts.
10. **Reduce overprivileged Okta admin and Salesforce profile counts.** ADT lost 5.5M records because a single SSO identity could reach the customer dataset in Salesforce. Apply least-privilege at the IdP and within each major SaaS app simultaneously.

---

8. Trends to Watch

- **Identity is the new "patch Tuesday."** Three of this week's biggest stories (ADT, Vercel, cPanel) all came down to identity — stolen, hijacked, or unauthenticated. Expect identity-incident frequency to surpass classic CVE incidents in board-level reporting within 12 months.
- **Phishing-resistant authentication becomes default, not optional.** Microsoft's Entra passkey rollout to shared/unmanaged Windows + Japan FSA's April pivot to mandating phishing-resistant MFA for high-risk financial flows signal that "MFA" without the "phishing-resistant" qualifier will soon read as audit findings, not adequate control.
- **OAuth grants become the next attack surface to inventory.** Following Drift, Anodot/Snowflake, and now Vercel/Context.ai, OAuth-grant inventory and lifecycle management will become standard line items in audits and SaaS security reviews.
- **Agent identity moves into the IAM control plane.** Okta, Microsoft, and Google all moved agent-identity capabilities into mainstream IAM products this month rather than separate products. The market is consolidating around "agents are identities," not "agents are integrations."
- **Cross-IdP behavioral analytics become table stakes.** Sentinel UEBA's expansion to Okta is one example; expect every major SIEM/XDR to follow. If your detection only sees one IdP, you are blind to the realistic attack path.

---

9. Tool / Resource of the Week

CISA — "Adapting Zero Trust Principles to Operational Technology" (joint guidance, April 30, 2026) - **What it does:** Provides a federally backed roadmap for applying Zero Trust to OT/ICS, including identity, asset visibility, and segmentation guidance tailored to legacy and safety-critical systems. - **Why it's useful:** It is currently the most authoritative single reference for IT-OT identity convergence and will be cited in audits, insurance underwriting, and regulator communications going forward. Use it as the framework backbone for OT Zero Trust roadmaps even if you are not in a federally regulated sector. - **Link:** Adapting Zero Trust Principles to Operational Technology — CISA

---

10. Sources

- ADT confirms data breach after ShinyHunters leak threat — https://www.bleepingcomputer.com/news/security/adt-confirms-data-breach-after-shinyhunters-leak-threat/
- ADT confirms data breach after ShinyHunters threatens data leak (SC Media) — https://www.scworld.com/brief/adt-confirms-data-breach-after-shinyhunters-threatens-data-leak
- ADT Breach Exposes Data of 5.5 Million Customers (Security Boulevard) — https://securityboulevard.com/2026/04/adt-breach-exposes-data-of-5-5-million-customers-shinyhunters-likely-behind-attack/
- ShinyHunters leak ADT data from 5.5 million accounts (MSN) — https://www.msn.com/en-us/news/insight/shinyhunters-leak-adt-data-from-5-5-million-accounts/gm-GMDC192A6C
- cPanel's authentication bypass bug is being exploited in the wild, CISA warns (CyberScoop) — https://cyberscoop.com/cpanel-authentication-bypass-vulnerability-cve-2026-41940-exploited/

- CVE-2026-41940 Explained: The cPanel & WHM Authentication Bypass That Hit 1.5M Servers (Picus) — https://www.picussecurity.com/resource/blog/cve-2026-41940-explained-cpanel-whm-authentication-bypass-hit-1-5m-servers
- CVE-2026-41940: cPanel & WHM Authentication Bypass (Rapid7) — https://www.rapid7.com/blog/post/etr-cve-2026-41940-cpanel-whm-authentication-bypass/
- The Internet Is Falling Down (watchTowr Labs) — https://labs.watchtowr.com/the-internet-is-falling-down-falling-down-falling-down-cpanel-whm-authentication-bypass-cve-2026-41940/
- Critical cPanel Vulnerability Weaponized to Target Government and MSP Networks (The Hacker News) — https://thehackernews.com/2026/05/critical-cpanel-vulnerability.html
- CISA Adds Eight Known Exploited Vulnerabilities to Catalog — https://www.cisa.gov/news-events/alerts/2026/04/20/cisa-adds-eight-known-exploited-vulnerabilities-catalog
- CISA, Federal Partners Unveil Guide to Accelerate Zero Trust Adoption in Operational Technology — https://www.cisa.gov/news-events/news/cisa-and-us-government-partners-unveil-guide-accelerate-zero-trust-adoption-operational-technology
- Adapting Zero Trust Principles to Operational Technology (CISA resource page) — https://www.cisa.gov/resources-tools/resources/adapting-zero-trust-principles-operational-technology
- CISA and Partners Publish Zero Trust Guidance For OT Security (Infosecurity Magazine) — https://www.infosecurity-magazine.com/news/zero-trust-guidance-operational/
- New CISA guidance outlines zero trust roadmap for OT environments (Industrial Cyber) — https://industrialcyber.co/zero-trust/new-cisa-guidance-outlines-zero-trust-roadmap-for-ot-environments-facing-legacy-constraints-and-growing-attack-surfaces/
- Microsoft to roll out Entra passkeys on Windows in late April (BleepingComputer) — https://www.bleepingcomputer.com/news/microsoft/microsoft-to-roll-out-entra-passkeys-on-windows-in-late-april/
- Microsoft is introducing Entra passkeys to Windows (TechRadar) — https://www.techradar.com/pro/security/microsoft-is-introducing-entra-passkeys-to-windows-so-tough-luck-if-your-device-is-jailbroken-as-your-credentials-will-soon-be-gone-forever
- Simplifying AWS defense with Microsoft Sentinel UEBA (Microsoft Security Blog, April 28, 2026) — https://www.microsoft.com/en-us/security/blog/2026/04/28/simplifying-aws-defense-microsoft-sentinel-ueba/
- Vercel Breach Tied to Context AI Hack Exposes Limited Customer Credentials (The Hacker News) — https://thehackernews.com/2026/04/vercel-breach-tied-to-context-ai-hack.html
- The Vercel Breach: OAuth Supply Chain Attack (Trend Micro) — https://www.trendmicro.com/en_us/research/26/d/vercel-breach-oauth-supply-chain.html
- AI SaaS as Enterprise Attack Vector: The Vercel–Context.ai Breach (Cloud Security Alliance) — https://labs.cloudsecurityalliance.org/research/csa-research-note-ai-saas-supply-chain-vercel-contextai-2026/
- Vercel April 2026 security incident (Vercel KB) — https://vercel.com/kb/bulletin/vercel-april-2026-security-incident
- Anodot SaaS Breach: ShinyHunters Stole OAuth Tokens (MINE2) — https://mine2.io/blog/2026-04-10-saas-integration-token-theft-anodot-snowflake-credential-mines/
- Okta Identity Engine release notes (2026) — https://help.okta.com/oie/en-us/content/topics/releasenotes/archive/oie-relnotes-2026.htm

- Okta Privileged Access Platform release notes — https://help.okta.com/oie/en-us/content/topics/releasenotes/privileged-access/opa-release-notes-platform.htm
- Next '26: Redefining security for the AI era with Google Cloud and Wiz — https://cloud.google.com/blog/products/identity-security/next26-redefining-security-for-the-ai-era-with-google-cloud-and-wiz
- Verizon 2026 Data Breach Investigations Report — https://www.verizon.com/business/resources/reports/dbir/
- Why non-human identities are your biggest security blind spot in 2026 (CSO Online) — https://www.csoonline.com/article/4125156/why-non-human-identities-are-your-biggest-security-blind-spot-in-2026.html
- 2026 NHI Reality Report (Cyber Strategy Institute) — https://cyberstrategyinstitute.com/2026-nhi-reality-report/
- The State of NHI and AI Security (Cloud Security Alliance) — https://cloudsecurityalliance.org/artifacts/state-of-nhi-and-ai-security-survey-report
- The Anatomy of a Deepfake Voice Phishing Attack (Group-IB) — https://www.group-ib.com/blog/voice-deepfake-scams/
- 16 Billion Credentials Exposed: Why This Infostealer Leak Demands a Rethink (F5 Labs) — https://www.f5.com/company/blog/16-billion-credentials-exposed-why-this-infostealer-leak-demands-a-rethink-of-bot-defense
- Japan FSA Passkeys: Push for Phishing-Resistant MFA (2026) — https://www.corbado.com/blog/japan-fsa-passkeys-phishing-resistant-mfa
- Netizen: Monday Security Brief (5/4/2026) — https://blog.netizen.net/2026/05/04/netizen-monday-security-brief-5-4-2026/