THE AI THREAT IS INDUSTRIAL NOW

DATEC INCORPORATED

Date: May 11, 2026
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN. May be shared within your organization and with peers in your sector.
Previous briefing: April 27, 2026: The Collapsed Exploit Timeline

---

EXECUTIVE SUMMARY

The two weeks since the April 27 briefing make one thing concrete: AI is no longer the headline story sitting on top of the cyber landscape — it is the soil everything else is growing in. Highlights from the period:

- **AI threat goes formal — and Google says it's already "industrial-scale."** On May 11, Google's Threat Intelligence Group published a report concluding that AI-powered hacking has gone from a nascent problem to an industrial-scale threat in just three months. Google's chief analyst John Hultquist: *"There's a misconception that the AI vulnerability race is imminent. The reality is that it's already begun"* [36]. The IMF reached the same destination from the policy side at its spring meetings, naming AI-driven cyberattacks a financial-stability risk and citing Anthropic's Claude Mythos Preview as evidence the threat is moving faster than patching [1]. KnowBe4 says 86% of the phishing campaigns it tracked in the past six months involved AI [2].
- **Microsoft device-code phishing is hitting hundreds of organizations daily** with AI-generated, hyper-personalized lures. Microsoft reports 10–15 distinct campaigns launching every 24 hours since March 15, with finance personas the post-compromise focus. Tooling overlaps with the EvilTokens phishing-as-a-service kit, and a separate AiTM "code of conduct" campaign hit 35,000+ users across 13,000+ organizations in 26 countries in just 72 hours (April 14–16) [33, 34, 35].
- **Supply-chain attacks roll through dev and security tooling.** JDownloader's website was backdoored to deliver a Python RAT [3]; a TeamPCP / Mini Shai-Hulud worm hit SAP, Intercom, and PyTorch Lightning npm/PyPI packages [4]; a competing worm called PCPJack is hijacking TeamPCP victims [5]; and Kaspersky disclosed a monthlong Daemon Tools backdoor with a targeted-payload tail [6].
- **Edge devices take another beating.** A Palo Alto PAN-OS zero-day is under active state-backed exploitation **with no patch yet** [7]; an incomplete Windows fix left a zero-click NTLM credential-theft hole now under attack [8]; and "Dirty Frag" Linux LPE was released into the wild with no CVE, no patches, and a public root exploit [9].
- **State actors are operating openly.** Russia's GRU is still living in home routers [10]; China's hacker-for-hire ecosystem is, per the FBI, "out of control" [11]; ShinyHunters took 6.65 TB out of Canvas and threw US universities into final-exam chaos [12].

- **The Iran war hits operations.** The conflict that began February 28 is now producing what the IEA calls "the largest supply disruption in the history of the global oil market": Brent at $101, US gas at $4.52 with $5 "no longer dismissible" per JP Morgan, jet fuel doubled in Europe, Lufthansa cutting 20,000 flights, Qatar's Ras Laffan LNG offline, sulfuric acid tightening with second-order pressure on phosphate fertilizers, and China imposing export restrictions on both refined fuels and sulfuric products to protect its own food supply [25, 26, 27, 28, 30].
- **CMMC Phase 2 is six months out.** Of ~100,000 DIB contractors expected to need CMMC Level 2 certification, ~1% have it; only 103 C3PAOs are authorized; and Rev 3 is in DOW rule-making within 12–18 months [31, 32].
- **AI's memory appetite bends the IT supply chain.** Server DRAM is on track to double in price by year-end, Meta is extending server life from six to seven years, and AWS is openly saying the shortage is pushing customers off-prem [13].

The next 30 days are about four things:

1. Assume AI is involved with or behind every phishing message and every vulnerability scan that gets run against you.
2. Treat developer tooling and edge devices as actively contested territory.
3. Price the AI-memory squeeze into your 2026/2027 hardware plans.
4. Run a 6–12 month scenario for fuel, fertilizer, and chemical input exposure if your operations touch energy, food, manufacturing, logistics, or aviation.

SUMMARY OF IMMEDIATE ACTIONS

The one-pager view of immediate actions. Each row is expanded with rationale in the "What You Should Be Doing Right Now" section later in this briefing.

Priority	Action	Why Now
CRITICAL	Restrict Palo Alto PAN-OS Captive Portal (User-ID Authentication Portal) to trusted networks or disable it entirely	CVE-2026-0300 (CVSS 9.3) under active state-backed exploitation; **no patch yet**; CISA KEV-listed [7]
CRITICAL	Apply Windows updates for CVE-2026-32202; federal agencies have a May 12 deadline; block outbound SMB to untrusted destinations to limit Net-NTLMv2 hash leakage	Incomplete February patch left zero-click LNK auth-coercion live; APT28 toolkit territory; CISA KEV-listed [8]

Priority	Action	Why Now
CRITICAL	If anyone in your environment downloaded JDownloader from the official site between May 6 and May 7, treat those endpoints as compromised: reinstall the OS and reset credentials. Search EDR and firewall telemetry for downloads from `jdownloader.org` in that window, and for outbound connections to `parkspringshotel[.]com`, `auraguest[.]lk`, or `checkinnhotels[.]com`; users may have pulled JDownloader via embedded apps or packages IT does not centrally track	Site backdoored; signed-by check fails ("AppWork GmbH" is legit; "Zipline LLC" / "The Water Team" are not); Python RAT loader confirmed [3]
CRITICAL	Audit dev/CI environments for the compromised npm and PyPI packages: SAP CAP family (mbt, @cap-js/db-service, @cap-js/postgres, @cap-js/sqlite), intercom-client 7.0.4/7.0.5, PyTorch Lightning 2.6.2/2.6.3	Mini Shai-Hulud worm steals GitHub tokens, npm creds, AWS/Azure/GCP secrets, Kubernetes tokens, Actions secrets; exfiltrates via repos under your account [4]
CRITICAL	Block Microsoft Entra ID OAuth 2.0 device code authentication flow via Conditional Access wherever it is not operationally required; restrict device-code flow to specific user groups, devices, and locations where it is required (smart TVs, printers, kiosks, headless IoT)	Active campaign compromising hundreds of organizations daily since March 15; 10–15 new campaigns/day; finance personas targeted for email exfil; bypasses non-phishing-resistant MFA; EvilTokens PhaaS in active use by Storm-237, UTA032, UTA0355, UNK_AcademicFlare, TA2723, and ShinyHunters [33, 34]

Priority	Action	Why Now
CRITICAL	Hunt EDR, email gateway, and identity logs for the AiTM "code of conduct" campaign IOCs (April 14–16): domains `compliance-protectionoutlook[.]de` and `acceptable-use-policy-calendly[.]de`; sender domains `cocinternal[.]com`, `gadellinet[.]com`, `harteprn[.]com`; sender addresses `cocpostmaster@cocinternal.com`, `nationaladmin@gadellinet.com`, `nationalintegrity@harteprn.com`, `m365premiumcommunications@cocinternal.com`, `documentviewer@na.businesshellosign.de`; PDF SHA-256s `5DB1EC...AECBC6`, `B5A334...876C9EAD`, `11420D...BE1A49D`	35,000+ users across 13,000+ organizations in 26 countries hit in 72 hours; 92% US; Healthcare & life sciences (19%), Financial services (18%), Professional services (11%), Tech & software (11%); Paubox HIPAA-banner spoofing; uses CAPTCHA + image selection to gate against sandboxes [35]
HIGH	Refresh phishing training specifically for the device-code prompt and the "code of conduct review" lure family; teach users to refuse any request to enter a Microsoft device code unless they personally initiated the device-code flow on a known device (smart TV, printer, etc.)	Dynamic device-code generation places the 15-minute timer after the redirect chain, leaving ample time for users to comply; users are also seeing the legitimate microsoft.com/devicelogin page, so URL-based training fails here [33]
HIGH	Treat 86%-AI phishing as the new baseline: refresh training and tooling for AI-quality lures, calendar-invite phishing, and Microsoft Teams help-desk impersonation	KnowBe4: AI use in phishing 80% (2024) → 84% (2025) → 86% (2026); calendar-invite attacks +49%, Teams impersonation +41%; Microsoft says AI lures are 4.5× more effective [2]

Priority	Action	Why Now
HIGH	Patch or replace the named TP-Link SOHO router models still in use anywhere your remote workforce or branch offices touch the corporate network; disable remote management; rotate router admin credentials	GRU APT28 has been DNS-hijacking 23 named TP-Link models since 2024; 200+ orgs and 5,000 devices already affected; FBI took the unusual step of remote-resetting US devices under court order [10]
HIGH	Validate Linux server kernel posture in light of Dirty Frag: apply Hyunwoo Kim's temporary mitigation (disable xfrm-ESP and RxRPC modules, clear page cache) for sensitive systems pending patches	Public root exploit, no CVE, no patches; impacts Ubuntu, RHEL, CentOS Stream, Fedora, AlmaLinux, openSUSE Tumbleweed [9]
HIGH	Review hiring controls and contractor onboarding for the North Korean fake-IT-worker risk: ID verification, on-camera technical interviews, location-of-work attestations, no shipping company laptops to addresses you cannot tie to the named hire	Two more US "laptop farm" hosts were each sentenced to 18 months prison this week; the scheme is clearing $500M+/year for Pyongyang and has expanded into healthcare, finance, and professional services [14]
HIGH	Confirm the Microsoft Exchange Online TLS 1.0/1.1 cutoff (POP3/IMAP4) for July 2026 will not break legacy clients or appliances in your estate	Long-telegraphed deadline now firm; "minimal impact" messaging assumes you actually inventory legacy clients [15]

Priority	Action	Why Now
MEDIUM	Build the AI-driven memory squeeze into your 2026 and 2027 hardware refresh plans; lock in supply where you have leverage; consider extending server life and rebalancing on-prem vs. cloud only after running the math, not on FUD	Server DRAM on track to double in price by end of 2026; Samsung +60% on 32GB DDR5 modules; Meta extending server life 6→7 years; AWS publicly saying memory shortage is accelerating cloud migration [13]
HIGH	If your operations touch fuel, fertilizer, agricultural commodities, sulfuric acid / phosphates, plastics inputs, aviation, or shipping, build a 6–12 month price-and-supply contingency view. Lock in supply where you have leverage; review force majeure clauses on long-term fuel contracts; qualify alternate suppliers; consider strategic stockpiles for critical inputs	IEA: “largest supply disruption in the history of the global oil market”; jet fuel +100% in Europe; sulfuric acid tightening with phosphate fertilizer downstream; China restricting both fuel and sulfuric exports; recovery 1–6+ months even after Hormuz reopens [25, 26, 27, 28, 30]
MEDIUM	For aviation operators and large fuel buyers in Europe, evaluate Jet A acceptance per IATA/EASA guidance as a partial supply hedge; communicate fuel-grade handling carefully across the supply chain	EASA published guidance; EU confirmed no regulatory obstacle; Lufthansa already cut 20,000 flights citing fuel costs; Ireland reportedly down to 10 days of jet fuel stock cover [29]

Priority	Action	Why Now
HIGH	If you hold or supply DOW (Department of War) contracts touching CUI: review your most recent SPRS affirmation against what is actually deployed; book or confirm a C3PAO assessment for late 2026 / early 2027 if you have not already; begin a NIST SP 800-171 Rev 3 migration plan in parallel, implementing the Rev 2 Appendix E NFO controls as a head start	CMMC Phase 2 mandatory Level 2 begins 2026-11-10 (six months out); ~1% of the ~100,000 Level-2-required DIB are certified; only 103 C3PAOs are authorized; SMB assessment costs run $50K–$100K; Rev 3 expected in DOW rule-making within 12–18 months [31, 32]

WHAT'S CHANGED SINCE APRIL 27

The April 27 briefing called out AI-accelerated offense, the Mythos Preview unauthorized-access story, the worst crypto-theft month since Bybit, third-party vendor exposure, and CMMC Phase 2 compression. In the two weeks since, five currents are clearly visible:

- **The IMF made AI cybercrime an explicit financial-stability concern.** At its spring meetings, the IMF tied AI-driven cyberattacks to potential funding strains, solvency concerns, and macro-financial shock, and named Anthropic's Mythos Preview as evidence of how fast the offense is improving. Barclays' CEO publicly called Mythos "a serious issue" and noted "There will be a Mythos 2 and a Mythos 3" [1].
- **A Microsoft device-code phishing campaign went industrial.** Microsoft began reporting on April 7 that 10–15 distinct device-code phishing campaigns have been launching every 24 hours since March 15, compromising hundreds of organizations daily, with infrastructure overlapping the EvilTokens phishing-as-a-service kit [33, 34]. In parallel, Microsoft Defender Research disclosed a separate AiTM "code of conduct" credential-theft campaign that hit 35,000+ users across 13,000+ organizations in 26 countries between April 14–16, with US healthcare, finance, and professional services taking the heaviest hits [35].
- **The supply-chain attack tempo did not let up.** TeamPCP / Mini Shai-Hulud expanded from SAP-related npm packages (~572K weekly downloads) to Intercom and PyTorch Lightning [4]. JDownloader's website was compromised and serving a Python-RAT loader [3]. Kaspersky published findings on a monthlong Daemon Tools backdoor that quietly delivered a more complex QUIC RAT to a small set of government, scientific, manufacturing, and retail organizations [6]. And SentinelLabs found a competing worm, PCPJack, methodically taking over TeamPCP victims and harvesting cloud credentials at scale [5].
- **Edge devices entered another bad cycle.** Palo Alto PAN-OS got a state-backed unauthenticated-RCE-as-root zero-day with no patch [7]. Microsoft's February fix for an APT28-exploited Windows flaw turned

out to leave a zero-click NTLM hash-leak live, now under active exploitation [8]. Linux admins got "Dirty Frag": public exploit, no CVE, no patches [9]. And the FBI/NSA's April 7 disclosure on GRU/APT28 hijacking 23 named TP-Link SOHO router models continues to ripple, with the FBI having taken the rare step of remotely resetting thousands of US devices under court order [10].

- **The biggest single disruption hit education.** ShinyHunters claimed 6.65 TB of Canvas data covering 9,000 schools, threatened to leak unless paid by May 12, and forced US universities (Penn State, Illinois, UNLV, Mississippi State, Tennessee, Mount Saint Mary's, Rutgers, others) to cancel or postpone final exams [12].

THE AI THREAT EQUATION HARDENS

Two weeks ago we noted Anthropic's Mythos Preview, the unauthorized-access incident around it, and Unit 42's Zealot proof-of-concept doing end-to-end cloud compromise in 2–3 minutes. This period brought four reinforcing data points and one useful counterweight.

Google said it bluntly on May 11. The Google Threat Intelligence Group published a report concluding that AI-powered hacking has gone from a nascent problem to an industrial-scale threat in just three months [36]. Google's chief analyst John Hultquist: *"There's a misconception that the AI vulnerability race is imminent. The reality is that it's already begun. Threat actors are using AI to boost the speed, scale, and sophistication of their attacks. It enables them to test their operations, persist against targets, build better malware and make many other improvements"* [36]. Google's report names criminal groups and state-linked actors from China, North Korea, and Russia as widely using commercial AI models — Gemini, Claude, and OpenAI tools — to refine and scale attacks [36]. The threat is not concentrated in any single vendor's model. Critically: Google flagged that a criminal group was recently on the verge of leveraging a zero-day vulnerability for a "mass exploitation" campaign using an LLM that was **not** Mythos [36]. This is the broader-than-Anthropic framing the security press has been waiting for.

The IMF formalized it. Speaking at the spring meetings, the IMF said advanced AI models can "dramatically reduce the time and cost needed to identify and exploit vulnerabilities," and that attackers hold a structural advantage because "discovering and exploiting vulnerabilities can occur faster than patching and remediation" [1]. The framing matters. When the IMF makes systemic-risk language about a security topic, it lands in board rooms in a way the same words from a security vendor do not. Barclays' CEO calling Mythos "a serious issue" and predicting Mythos 2 and 3 reinforces that the conversation has reached the C-suite [1]. CrowdStrike's 2026 Global Threat Report (cited in the same coverage) puts AI-powered attacks up 89% year-over-year and state-actor cloud intrusions up 266% [1].

The phishing baseline jumped again. KnowBe4's seventh edition Phishing Threat Trends report says 86% of the phishing campaigns it tracked in the last six months made use of AI, up from 84% last year and 80% in 2024 [2]. More important than the headline number is *how* AI is being used: not just message generation, but reconnaissance and target enrichment, pivoting from email into calendar invites (+49%) and Microsoft Teams

help-desk impersonation (+41%), and generating polymorphic lures that no longer carry the misspellings users were trained to spot. Microsoft's own data has AI lures performing 4.5× better than human-crafted ones; the FBI's $20.87B 2025 cybercrime loss number includes ~$893M in AI-related fraud [2].

The "fear marketing" critique is worth reading even if you reject the conclusion. BBC Future ran a thoughtful counter-piece arguing AI vendors benefit from keeping the public fixated on civilizational risk, because it distracts from present harms and pushes regulators toward the position that only the labs themselves can be trusted to govern this [17]. The AI Now Institute's Heidy Khlaaf flagged a real and specific gap in Anthropic's Mythos materials: no false-positive rate, no comparison against existing static-analysis tools security engineers have used for decades [17]. Critically, Khlaaf does **not** say the underlying capability isn't real. Her summary is "Mythos might be capable" and "automatically finding security vulnerabilities is a real and pressing danger"; the marketing, in her reading, is doing more work than the verification [17]. Pair that with the May 9 Seattle Times feature on PNNL, where the federal lab's chief AI scientist describes a measured optimism, deployed guardrails, and a real concern about who holds the controls [18]. Steven Murdoch, professor of security engineering at University College London, frames the defender side of the same dynamic in the Google Guardian piece: *"In general we have reached a stage where the old way of discovering bugs is gone, and it will now all be LLM-assisted. It will take a little while before the consequences of this get shaken out"* [36].

What this means in practice. The vendor pitch for the next 24 months will be split between "AI is your defender" and "AI is your attacker." Both are partially true. What's actually changing is that the *defender* now has to assume the *attacker* is testing every exposed surface with a model that doesn't get tired and that costs less per scan than the cheapest contractor in your previous threat model. Plan for 86% of phishing using AI to be conservative; plan for "every exposed CVE is being inspected by something that can chain it" as your working assumption.

ACTIVE CAMPAIGN: DEVICE-CODE PHISHING AT INDUSTRIAL SCALE

This is the operationally hottest item in this briefing. Treat it that way.

The volume. Microsoft VP of security research Tanmay Ganacharya told The Register that "since March 15, 2026, we have observed 10 to 15 distinct campaigns launching every 24 hours. Each campaign is distributed at scale, targeting hundreds of organizations with highly varied and unique payloads, making pattern-based detection more challenging. We continue to observe high-volume activity, with hundreds of compromises occurring daily across affected environments" [33]. All sectors, globally; post-compromise focus is on finance-related personas with automated email exfiltration.

The mechanism. The attackers abuse OAuth 2.0 device code authentication, the flow originally designed for smart TVs, printers, and headless devices that cannot present a standard browser login. In that flow, a device shows a short code and instructs the user to type it into `microsoft.com/devicelogin` on a separate

device. Microsoft warns: "Because authentication is completed on a separate device, the session initiating the request is not strongly bound to the user's original context" [33]. An attacker who initiates the flow and tricks a user into entering the code completes authentication as the user, including bypassing non-phishing-resistant MFA.

The attack chain.

1. **Reconnaissance.** Attackers query Microsoft's `GetCredentialType` API endpoint to confirm a target email exists and is active in the tenant, typically 10–15 days before phishing [33].
2. **AI-generated lures.** Hyper-personalized emails aligned to the target's role: RFPs, invoices, manufacturing workflows, payroll notices, DocuSign / SharePoint share notifications [33, 34]. EvilTokens-specific lures impersonate Adobe Acrobat or DocuSign verification pages [34].
3. **Redirect chains on trusted infrastructure.** Compromised legitimate domains and serverless platforms (Railway, Cloudflare Workers, DigitalOcean, AWS Lambda) front the attacker infrastructure, helping the chain blend into normal enterprise cloud traffic and defeat URL scanners [33].
4. **Dynamic device-code generation.** The clever part. Device codes are valid only 15 minutes. Static phishing emails ship a pre-generated code, leaving a small window for the attack. This campaign defers code generation to the final stage of the redirect chain, so the 15-minute timer doesn't start until the victim is already on the final page [33].
5. **Real-time polling.** After presenting the code, the malicious script polls the attacker's `/state` endpoint every 3–5 seconds via `setInterval`, monitoring whether the user has completed authentication on the real Microsoft site [33].
6. **Token capture and persistence.** Once the user authenticates, the access token is sent to the attacker. Post-compromise, attackers have been observed registering new devices within 10 minutes to mint a Primary Refresh Token (PRT) for long-term persistence, or waiting hours before stealing email or creating inbox rules that forward messages whose subjects contain "payroll" or "invoice" [33].

EvilTokens phishing-as-a-service. EvilTokens has been sold over Telegram since mid-February 2026 and is under continuous development; the operators have announced plans to add Gmail and Okta phishing pages [34]. Sekoia attributes active use to multiple Russian-tracked groups (Storm-237, UTA032, UTA0355, UNK_AcademicFlare, TA2723) and to the ShinyHunters data-extortion crew that took down Canvas [34]. EvilTokens lures arrive as PDF, HTML, DOCX, XLSX, or SVG attachments with QR codes or hyperlinks; they impersonate financial documents, meeting invitations, logistics or purchase orders, payroll notices, and DocuSign / SharePoint shares; they are aimed at finance, HR, logistics, and sales roles [34]. Most-affected countries per Sekoia: US, Canada, France, Australia, India, Switzerland, UAE. EvilTokens advertises explicit BEC (business email compromise) automation features.

The "code of conduct" AiTM campaign (April 14–16). Microsoft Defender Research published a separate detailed write-up on May 4 documenting an adjacent campaign that targeted 35,000+ users across 13,000+ organizations in 26 countries in just 72 hours [35]. Distribution: 92% US. Industries hit hardest were Healthcare & life sciences (19%), Financial services (18%), Professional services (11%), and Technology &

software (11%). Lures posed as internal compliance communications ("Internal Regulatory COC," "Workforce Communications," "Team Conduct Report") with subjects like "Internal case log issued under conduct policy." Emails spoofed a Paubox HIPAA-compliance encryption banner to add legitimacy and included PDF attachments with names like `Awareness Case Log File – Tuesday 14th, April 2026.pdf`. The attack chain used Cloudflare CAPTCHA and a second image-selection CAPTCHA to gate against automated analysis, redirected mobile and desktop users to different final stages, and ultimately captured authentication tokens via an adversary-in-the-middle (AiTM) proxy of the Microsoft sign-in page. Microsoft notes the chain "has several hallmarks of device code phishing" but they could only confirm the AiTM portion [35]. Indicators of compromise for hunting are listed in the immediate-actions table above and in the Microsoft blog.

Why this matters. Three things make this campaign hard to defend against with standard awareness training:

- The final phishing destination is `microsoft.com/devicelogin` itself. Users *do* land on a legitimate Microsoft page. "Check the URL" training fails.
- AiTM and device-code attacks bypass non-phishing-resistant MFA (SMS, push, TOTP), defeating the most common second factor most organizations have deployed.
- AI-generated lures and platform-aware redirect chains defeat pattern-based email and URL detection.

What works.

- **Block or scope down device-code flow.** Microsoft's explicit guidance is "only allow device code flow where absolutely necessary" [33]. In Microsoft Entra ID Conditional Access, build a policy that blocks the OAuth 2.0 device code grant for all users by default, then add narrow exceptions for the specific user groups, devices, and locations that legitimately require it (digital signage, conference room hardware, IoT/headless devices).
- **Phishing-resistant MFA.** FIDO2 / WebAuthn / platform passkeys are not susceptible to AiTM proxying or device-code social engineering. Push and SMS are.
- **Conditional Access risk policies.** Microsoft Entra ID Protection signals such as "Anomalous Token," "Unfamiliar sign-in properties for session cookies," and "Impossible travel" are the right detections to elevate to block, not just to monitor [35].
- **Defender for Office 365 hardening.** Safe Links, Safe Attachments, Zero-hour Auto Purge (ZAP), and network protection in Defender for Endpoint all materially help here [35].
- **Targeted user training.** Specifically train users that "enter this device code on `microsoft.com/devicelogin`" is the new phishing prompt, and that the only valid reason to do so is when they personally initiated a device-code flow on a non-browser device they are physically holding. The 2021 Azure "Cancel / Continue" sign-in confirmation prompt that is missing from phishing flows is a useful tell to teach.

Operational priority. This belongs at the top of your immediate action list along with the unpatched Palo Alto zero-day. The volume is industrial, the bypass is real, and the post-compromise activity is monetizable inside hours.

SUPPLY CHAIN ATTACKS DON'T STOP

Four discrete compromises in the past two weeks paint a now-familiar picture: dev and security tooling is the wedge, and the attackers running it are organized enough to recycle infrastructure, propagate worm-style, and add targeted second stages on top of mass infection.

JDownloader (May 6–7). Attackers compromised the official JDownloader website via an unpatched CMS vulnerability, swapped the Windows "Alternative Installer" and Linux shell installer download links, and served a Python-RAT loader (Windows) plus a SUID-root persistence chain (Linux) [3]. Legitimate publisher is "AppWork GmbH"; malicious installers were signed "Zipline LLC" or "The Water Team." C2 hid behind hospitality-themed domains. JDownloader's incident response was responsible (site offline, public IR write-up, IOCs published), but the only safe path for affected endpoints is full OS reinstallation and credential reset [3].

TeamPCP / Mini Shai-Hulud (April 29 onward). Wiz and Socket attribute a coordinated worm-style npm/PyPI campaign to TeamPCP, the same crew linked to earlier Checkmarx, Bitwarden, Telnyx, LiteLLM, and Aqua Trivy compromises [4]. Compromised packages (four official SAP JavaScript/Cloud Application Development packages at ~572K weekly downloads, intercom-client at ~360K weekly downloads with 100+ dependent projects, and PyTorch Lightning) execute attacker code on every `npm install` (or import for Lightning), steal GitHub tokens, npm credentials, AWS/Azure/GCP secrets, Kubernetes tokens, GitHub Actions secrets, and exfiltrate via new GitHub repos created **under the victim's own account** [4]. This is no longer a single-package incident pattern; it is a propagation framework targeting the developer pipeline.

Daemon Tools / Kaspersky disclosure. A monthlong supply-chain attack on the Daemon Tools disk app pushed an info-stealer to roughly 100 organizations, with a more complex backdoor (QUIC RAT) quietly delivered to about a dozen systems at government, scientific, manufacturing, and retail organizations in Russia, Belarus, and Thailand [6]. QUIC RAT supports HTTP, UDP, TCP, WSS, QUIC, DNS, and HTTP/3 C2; injects into notepad.exe and conhost.exe. The Kaspersky language is precise: "deployment of the backdoor to a small subset of infected machines clearly indicates that the attacker had intentions to conduct the infection in a targeted manner" [6]. Mass infection plus targeted second stage is now an expected pattern.

PCPJack. SentinelLabs disclosed on May 8 a worm that hijacks TeamPCP infections. Its first action on a compromised host is to remove TeamPCP's tooling, then take that environment over for itself [5]. PCPJack spreads through exposed Docker, Kubernetes, Redis, MongoDB, and RayML services, harvests environment variables, config files, SSH keys, Docker secrets, Kubernetes tokens, and lengthy lists of finance/enterprise/

messaging/cloud credentials, and scans for new environments to infect [5]. No cryptominer is included, which SentinelLabs reads as either spam/fraud monetization or data resale. Whether PCPJack is a TeamPCP rival, a TeamPCP splinter, or just an opportunist riding the same vulnerable estate is unclear.

The Vidar campaign rounds out the picture. LevelBlue documented a multi-stage Vidar info-stealer campaign delivered via a fake Microsoft Toolkit hacktool [19]. Vidar (originally Arkei, 2018) is unremarkable in capability but exemplary in evasion: extension masquerading (.dot to .bat), tasklist/findstr enumeration, ZwQueryInformationProcess to detect debuggers and EDR, abuse of Telegram and Steam Community profiles for staging, and post-execution disk scrub via `RtlExitUserProcess` to delete its own footprint [19]. Targeted: browser passwords, cookies, crypto wallets. Telemetry pattern: financial threat actors and initial access brokers.

Operational implication. Treat your developer tooling, package managers, and CI/CD pipelines as actively contested territory. Pin versions, monitor preinstall scripts, alert on GitHub repo creation under service accounts, audit secrets stored as environment variables in CI runners, and assume any unsigned Windows installer downloaded from a vendor site this past two weeks needs IOC-level scrutiny.

EDGE & ENDPOINT UNDER SIEGE

Five separate edge-and-endpoint stories landed in this period. Three are urgent; two are housekeeping with a deadline.

Palo Alto PAN-OS: CVE-2026-0300, no patch yet. A memory-corruption flaw in the User-ID Authentication Portal (a.k.a. Captive Portal) on PA-Series and VM-Series firewalls allows unauthenticated remote code execution as root on internet-exposed devices [7]. Unit 42 attributes ongoing exploitation to a "likely state-sponsored" cluster (CL-STA-1132). First failed attempts began April 9; successful RCE about a week later; attackers cleared logs and crash reports, then moved deeper, including Active Directory probing. On April 29, attackers triggered an authentication-traffic flood that forced a secondary firewall to take over internet-facing duty, and they compromised that one too [7]. CISA put it in the Known Exploited Vulnerabilities catalog. There is **no patch yet**. Until there is, lock the User-ID Authentication Portal to trusted networks or disable it.

Windows zero-click: CVE-2026-32202, incomplete February patch. An Akamai researcher discovered, while testing Microsoft's February fix for CVE-2026-21510 (used by Russia's APT28 against Ukraine and the EU), that the patch left a zero-click authentication-coercion vulnerability live [8]. CVE-2026-32202 lets a malicious LNK file send a victim's Net-NTLMv2 hash to an attacker, who can then authenticate as the user, snoop the network, and exfiltrate. Microsoft marked it "exploitation detected" on April 28; CISA added it to KEV with a May 12 federal deadline [8].

"Dirty Frag" Linux LPE: no CVE, no patches, public exploit. Researcher Hyunwoo Kim disclosed a kernel privilege-escalation chain combining a January 2017 xfrm-ESP commit and a 2023 RxRPC change after the disclosure embargo broke [9]. Affected distributions: Ubuntu, RHEL, CentOS Stream, Fedora, AlmaLinux, openSUSE Tumbleweed. A separate GitHub project ("Copy Fail 2: Electric Boogaloo") weaponizes the ESP/

xfrm half independently. Kim published a temporary workaround (disable the affected ESP and RxRPC kernel modules and clear the system page cache), but as he put it, "turn bits of the kernel off and hope for the best" is not the guidance admins enjoy [9].

TP-Link SOHO routers: APT28 / Forest Blizzard / GRU. The April 7 FBI/NSA disclosure that GRU's APT28 has been DNS-hijacking SOHO routers since at least 2024 has become a longer-tail problem because the affected devices are end-of-life [20]. Microsoft Threat Intelligence cites 200+ organizations and 5,000 consumer devices already affected. The UK NCSC list of 23 TP-Link models is described as "likely not exhaustive." The FBI took the unusual step of remotely resetting US devices under a court order, but action by individual owners and IT teams is still needed to upgrade past the affected hardware, change default credentials, disable remote management, and enable automatic firmware updates [20].

Exchange Online: TLS 1.0/1.1 retirement July 2026. Microsoft will block TLS 1.0/1.1 connections to Exchange Online via POP3 and IMAP4 starting July 2026, ending an opt-in legacy endpoint kept alive since 2023 [15]. Microsoft expects "minimal impact"; that is true only if you actually have visibility into legacy clients, scanners, MFPs, and embedded appliances that may still be using the old protocols. Now is the time to inventory, not next month.

STATE ACTORS ACTING BOLDLY

The state-actor picture for the period is unusually crisp because all four major adversaries produced public moves.

China: hacker-for-hire ecosystem "out of control." The FBI's cyber assistant director, Brett Leatherman, briefed reporters that China's network of private hacker-for-hire firms operating at the behest of MSS and provincial security bureaus has gotten out of control, with contractors selling unwanted access and stolen data on dark-web markets when their PRC clients pass [11]. Xu Zewei, a Chinese national arrested in Italy last July and extradited to the US the weekend before, was charged with nine hacking-related crimes including roles in the 2021 Hafnium / Silk Typhoon Microsoft Exchange campaign that compromised hundreds of thousands of servers worldwide and 12,700 organizations in the US. He's also alleged to have targeted American universities and researchers working on COVID-19 vaccines and treatments [11]. Co-defendant Zhang Yu, a director at Shanghai Firetech, remains at large. Leatherman's message: "the protection you assume from operating inside China does not extend the moment you cross a border" [11].

Russia: APT28 still everywhere. In the past two weeks alone, Russia's GRU has been credibly linked to the Windows zero-click CVE-2026-32202 territory (incomplete patch for the APT28-exploited CVE-2026-21510 chain) [8] and to ongoing TP-Link SOHO router compromise [20]. This is an operational-tempo signal. Expect continued Ukraine-EU targeting and continued use of consumer/SMB networking gear as persistent recon infrastructure.

Iran: pro-Iran "313 Team" turning DDoS into extortion. The pro-Iran Islamic Cyber Resistance in Iraq, a.k.a. 313 Team, began a sustained DDoS against Canonical's Ubuntu.com infrastructure on the evening of April 30 and within hours pivoted to a Telegram extortion message: "There is a simple way out. We have emailed you with our Session Contact ID. If you fail to reach out, we will continue our assault." [21] 313 Team had previously claimed similar DDoS campaigns against eBay Japan and US, and BlueSky. The shift from hacktivist DDoS-as-message to DDoS-as-shakedown is the noteworthy part: it lowers the bar to monetize state-aligned disruption.

North Korea: the laptop-farm convictions continue. Two more US "laptop farm" hosts, Matthew Knoot of Nashville and Erick Ntekereze Prince of New York, were each sentenced to 18 months prison this week for hosting company-issued laptops used by North Korean IT workers to remotely infiltrate US firms [14]. Between them they generated >$1.2M in fraudulent revenue for Pyongyang, victimized ~70 US companies, and forced $1.5M in audit/remediation costs. The DPRK fake-IT-worker scheme is now estimated at $500M+/year and has expanded beyond big tech into healthcare, finance, and professional services [14]. Hire-process controls and laptop-shipping verification are no longer optional in any sector that touches sensitive data.

SECTOR SPOTLIGHT: EDUCATION HIT HARD

Canvas, the learning-management platform from Instructure used by 30M+ active users in K-12 schools and universities globally (including every Ivy League institution), was breached in late April, taken down on May 8, and used as a finals-week pressure point against US universities by ShinyHunters [12]. ShinyHunters claimed 6.65 TB of stolen data covering 9,000 schools and demanded "settlement" by May 12 or threatened a public dump. Instructure publicly confirmed unauthorized activity, called in outside forensics, and notified law enforcement; the platform began coming back online late May 8 [12].

The downstream chaos is what made the story. Penn State and the University of Illinois cancelled or postponed final exams. UNLV, Mississippi State, Tennessee, and Rutgers shifted finals. Mount Saint Mary's told students to print all reading material from Canvas as a precaution. The FBI issued a public reminder that parties claiming to hold stolen data may be lying and that students should await formal institutional guidance rather than respond to threats [12]. Universities issued near-uniform warnings about heightened phishing risk leveraging breach awareness.

There are two takeaways. First, Canvas is one of those SaaS platforms that schools have come to depend on the way hospitals depend on EHRs; when it goes down, the whole operation degrades. Second, ShinyHunters timing the threat-to-leak deadline to coincide with finals is an attack on the institutions' ability to negotiate, not just on the data itself. Sector defenders should expect this pattern (operationally inconvenient timing as an extortion lever) to spread.

THE IRAN WAR REACHES OPERATIONS: FUEL, FOOD, AND CHEMICALS

The Iran war that began on February 28 with US and Israeli strikes is now producing the kind of cascading supply-side effects that Russia's invasion of Ukraine produced for grain and natural gas — but at greater speed and across more product categories. The Strait of Hormuz, which handles roughly 25% of global seaborne oil trade and 20% of LNG, has seen tanker traffic plunge to a near halt. The IEA called this "the largest supply disruption in the history of the global oil market" [25]. The market had a grace period in March and April as pre-war shipments arrived; that grace period is over [26]. The cyber dimension of the conflict (313 Team DDoS, prior Iranian PLC campaigns) continues alongside the economic dimension and is increasingly the smaller of the two stories.

Oil and gasoline

Brent crude was $101.27/bbl on May 6 (down 7.8% on peace-talk progress); a Reuters poll has the 2026 average at $86.38, up from ~$62 in January [26]. Total stockdraw to date is roughly 600 million barrels per Rystad, with projected total losses of 1.2–2 billion barrels before recovery (between 16% and 27% of pre-war global inventories) [26]. US gasoline hit $4.52 on Sunday May 10 per AAA (+37¢ month-over-month), and JP Morgan now says the $5/gallon mark "can no longer be dismissed"; Energy Secretary Chris Wright, asked directly on Meet the Press, declined to rule it out [27]. Morgan Stanley projects US gasoline inventories will fall to ~198M barrels by late summer, the lowest level for that time of year in modern records; the May 1 reading of 220M was already the lowest for the date since 2014 [26]. Goldman Sachs has global inventories falling to 98 days by end of May vs 105 days at end of February [26]. Recovery is not measured in days: Exxon's Darren Woods says 1–2 months for oil flows to normalize after Hormuz reopens; Equinor's Anders Opedal says at least six months for the market to be normal even with peace [26].

Jet fuel: Asia first, then everyone

Pre-war, the Persian Gulf was the largest single source of jet fuel supply globally; Europe imported 20% of its jet fuel from the Gulf and Asian refineries (China, South Korea, India) depend on Gulf crude as feedstock [28]. Global jet fuel exports plunged 30% in April year-over-year (1.9M bpd to 1.3M bpd); tanker loadings fell 50% week-over-week [28]. European jet fuel prices have doubled to $187/barrel as of May 1 (IATA); Lufthansa cut 20,000 short-haul flights through October citing fuel costs [28]. Airports Council International Europe warned the EU on April 9 of a "systemic jet fuel shortage" if Hormuz did not reopen within three weeks; oil flows did not normalize in April. Ireland reportedly had only 10 days of jet fuel stock cover (Goldman) [26]. IATA has suggested European airlines accept US-grade Jet A as a partial workaround; EASA published safety guidance and the EU said there are no "regulatory obstacles" to its use, though it warned of the risks of mixing fuel grades [29]. US refiner exports to Europe surged more than 400% to 94,000 bpd in April; Valero raised jet fuel to 30% of total distillate, up from a typical 26% [28]. US West Coast vulnerability is concentrated: 93,000 bpd of jet fuel imports in 2025, more than 80% from South Korea, whose refineries

themselves lost ME crude feedstock [28]. Kpler's Matt Smith summarized the pattern: "It is a series of dominoes that are falling here. Jet is the first one to go. Asia is the first region, but it's going to spread across the globe, and it's also going to spread across the products" [28].

Natural gas and LNG

An Iranian drone attack halted Qatar's Ras Laffan LNG facility, which accounted for roughly a fifth of global LNG supply [25]. Total LNG loss to date is estimated at 30–50 million tonnes (7–11% of annual global supply) [26]. European gas futures nearly doubled in the days after the conflict began, reaching their highest levels since 2023; Europe is exiting winter with unusually low storage and needs to refill before next winter into a much tighter market [25]. US LNG producers stand to benefit but are already operating near full capacity; new US LNG facilities coming online this year can only partially replace Qatari gas, so some consumers will have to cut usage or find substitutes [25].

Fertilizer, food, and chemicals: the most underappreciated thread

Mark Preston's framing for the Guardian deserves to be quoted directly: "The concern is at least as much, if not more, around food and fertiliser than it is around oil, because there are alternative sources of oil. There aren't very many alternative sources of nitrogen, for the production of fertiliser." [16] UK farmer fertilizer costs are already up 50–70% per Grosvenor; Yara, the world's largest fertilizer firm, has warned of food shortages and price rises in Africa's most vulnerable communities. The mechanism is direct: natural gas (LNG) is the input for nitrogen-based fertilizers like urea, and the Hormuz closure cut LNG flows at scale [16, 25].

The fertilizer story has now widened beyond nitrogen. The Wall Street Journal reported (via Press TV's coverage on May 10) that sulfuric acid supply is tightening because Persian Gulf refineries and gas plants are a major sulfur source: "a large chunk of the world's sulfur comes from Persian Gulf oil refineries and gas plants and has been choked off at the Strait" [30]. Sulfuric acid is upstream of phosphate fertilizers, copper leaching, pulping wood, pickling steel, leather tanning, and rubber vulcanization [30]. Compounding the squeeze, China (the world's largest sulfuric-products manufacturer) imposed export restrictions on sulfuric acid this month to protect its own fertilizer and food supply. Acuity Commodities' Freda Gordon told the WSJ this is "boosting prices and further straining availability" [30]. China has separately told its biggest oil refiners to suspend exports of diesel and gasoline [25]. Naphtha (used to make plastics and road fuel) is also rising alongside other refined products [25].

Reserve building and policy responses

IEA member countries agreed to release more than 400 million barrels of crude and oil products from emergency reserves, more than double the volume released in response to Russia's 2022 invasion of Ukraine. These barrels will not all hit the market at once and will only cover a portion of daily lost Gulf supply [25]. Australia (which imports ~80% of its fuel and has been suffering shortages) announced $7.22 billion to build fuel reserves [26]. The European Commission is considering revising the EU's 90-day oil-stock requirement to add a specific jet fuel reserve mandate [26]. The US is providing limited naval escort capacity

(the Trump administration has called on Europe and Asia to share the protection burden); buyers across Asia have turned to US barrels, and India is taking Russian crude after the Trump administration eased sanctions on cargoes already at sea [25].

What this means for sectors

- **Aviation:** Lufthansa's flight cuts are likely a leading indicator; carriers exposed to Middle East refining or to Asian refining-via-Gulf-feedstock should plan for Q3 2026 fuel cost shocks and potential schedule reductions. Cargo carriers and freight-dependent operations should expect surcharges to widen.
- **Agriculture and food production:** Plan for elevated fertilizer prices through next planting season; UK is already +50–70% on nitrogen, and phosphate is now exposed via the sulfuric acid path. Grocery costs lag input shocks by months. Food-processor input contracts deserve a hard look.
- **Manufacturing:** Sulfuric acid is upstream of copper smelting, steel pickling, rubber, leather, and many specialty chemical processes. Where acid is critical to a process, lock in supply now; expect quotes to shorten and pricing to firm. Naphtha-dependent plastics manufacturing has parallel exposure.
- **Logistics and shipping:** Bunker fuel costs are rising; Asian fuel-oil hubs are tight (Singapore stocks at near-1-year low). Build pricing flexibility into freight contracts and consider reserves where feasible.
- **Critical infrastructure and public sector:** Diesel for backup generation and contracted fuel delivery deserve a fresh review. Agencies and utilities running on multi-year fuel contracts should assess force majeure clauses, alternate-supplier qualification timelines, and stockpile levels.
- **Insurance and finance:** Marine cargo, hull, and war-risk premiums for Gulf transit are repricing; commodity hedging desks should build sustained-disruption scenarios into their books rather than assuming a quick reopening.

CMMC PHASE 2 IN SIX MONTHS, WITH REV 3 ON DECK

The CMMC compliance picture has not improved since the April 27 briefing. Of the roughly 100,000 defense industrial base contractors expected to need CMMC Level 2 certification, approximately 1% have actually achieved it [31]. Only 103 C3PAOs (Cybersecurity Maturity Model Certification third-party assessors) are authorized by CyberAB to perform assessments [31]. Industry voices in recent reporting are split on whether this is a structural crisis. Trey Hodgkins of Hodgkins Consulting and AEI's Bill Greenwalt argue the Department of War (DOW, the renamed DoD) needs "thousands of C3PAOs" to bring fees and wait times down. Active C3PAOs counter that booking an assessment 6–10 months in advance is normal for a program of this scale and that the prep window is, for organizations that use it well, valuable rather than wasteful [31]. Both readings have merit: the program is operationally functional for organizations that started preparing early, and structurally squeezed for the long tail of small contractors who waited.

The cost picture is what matters most for SMB defenders. Hodgkins reports many small businesses are paying $50,000 to $100,000 combined for a C3PAO assessment and the consulting work required to be assessment-ready: a fee stack that is genuinely meaningful for a sixth- or seventh-tier subcontractor whose annual revenue may be $150,000 [31]. Industry consensus per ExecutiveGov is that companies do not become assessment-ready in fewer than three months in any case [31]. GovCon attorney Cherylyn Harley LeBon framed the strategic question bluntly: "Either you're going to play the game… and go along with it, or you're going to pivot to something else. But budgets have decreased in these other agencies and there are fewer opportunities. So where does that leave you? With commercial opportunities and state and local [governments]" [31].

Phase 2 timing reminder. Phase 2 (the point at which DOW can begin requiring Level 2 certification, via self-assessment or C3PAO, in individual contracts) begins November 10, 2026. Phase 3, which begins November 10, 2027, makes independent C3PAO assessment every three years mandatory [31].

Rev 3 is the next shoe to drop. CMMC currently rests on NIST SP 800-171 Rev 2 (110 controls). Rev 3, published by NIST in May 2024, adds three new security-control families emphasizing supply chain security, incident response, and countering advanced threats; aligns more closely with NIST SP 800-53 Rev 5 structure; introduces 88 organization-defined parameters (ODPs) where DOW has set the specific values (password length, session timeout duration, etc.) rather than allowing organizational flexibility; and formally incorporates non-federal organization (NFO) controls that Rev 2 listed in Appendix E but assumed organizations would satisfy by default [32]. Rev 3 has 13 fewer line-item requirements than Rev 2 on paper, but most withdrawn items were merged into others, and the NFO incorporation means there is more total work, not less. DOW has not formally announced the Rev 3 effective date; published memoranda indicate rule-making within the next 12–18 months [32].

The "major change" trap. DOW policy treats certain modifications to a CMMC-assessed environment as "major changes" that trigger re-certification. DOW has not defined what counts as a "major change", which means a Rev 2 → Rev 3 migration handled the wrong way could force re-payment for an assessment just completed [32]. Stillwater's recommendation: build current certification on Rev 2 using the NIST SP 800-171A assessment guide, and in parallel begin a Rev 3 migration plan that voluntarily implements the Rev 2 Appendix E NFO controls. Those steps will count toward Rev 3 requirements when the rule-making lands, and they are unlikely on their own to qualify as a "major change." Sequence and document the migration carefully; treat any environmental change as a question to evaluate against the eventual official "major change" definition, not an assumption to make.

For DIB-adjacent readers, the actions are unchanged from April 27 in priority but more urgent in tempo: review your most recent SPRS affirmation against what is actually deployed (32 CFR 170.22 makes the affirming senior official personally False Claims Act–exposed for the SPRS signature); book or confirm a C3PAO assessment now if you have Phase 2 contracts in your near pipeline; and start the Rev 3 prep work in parallel rather than sequentially. For the long-tail SMBs in the supply chain who are facing the genuine $50K–$100K decision: the answer is increasingly to either commit to compliance early (so the cost is amortized across multiple contract cycles) or to pivot deliberately into commercial, state, and local opportunities before Phase 2 closes the door.

The Stillwater Group provides CMMC readiness consulting, NIST SP 800-171 gap assessments, SPRS affirmation review, Rev 2 to Rev 3 migration planning, and pre-assessment preparation across DIB primes and subcontractors. Contact us if a Phase 2 contract is in your pipeline and you need a clear-eyed read on where you stand.

THE BROADER LANDSCAPE

Drones outpace defense at large public events

The Center for Internet Security published a paper warning that drone technology is outpacing the systems state and local governments rely on to secure large public gatherings, including the FIFA World Cup matches that begin in June across North American host cities [22]. Detection tools (radar, RF, cameras) struggle in dense environments and produce false positives. Federal counter-drone authority is concentrated at four agencies (DOW, DoJ, DoE, DHS); state, local, and private operators including airport authorities are prohibited from jamming or disabling drones. Bills in Congress (HR 7525, Burlison R-MO) would extend counter-drone authority to state and local law enforcement after a three-year pilot [22]. CIS recommends a layered approach pairing detection tools with stronger interagency coordination and clearer governance. For sectors hosting large public events or operating high-value facilities, the operational gap is real; for correctional facilities, drone-delivered contraband is already a measurable trend (DoJ recorded 130 federal-prison incidents 2015–2019; Federal Bureau of Prisons documented incidents nearly doubled after 2018) [22].

Hardware stress becomes a business story

The story we used to call "RAMageddon" has crossed from PC-enthusiast Twitter into IT capex planning [23, 13]. Counterpoint Research projects DDR5 64GB RDIMM modules used in enterprise data centers will cost roughly twice as much by end of 2026 as they did in early 2025. Samsung raised 32GB DDR5 prices to $239 from $149 (a 60% jump); SK Hynix sold out HBM, DRAM, and NAND through 2026 on its October earnings call; Micron stopped quoting some products entirely [23]. Nvidia's Grace CPU Superchip uses up to 960GB of LPDDR5X, a smartphone-class memory category that one customer can now move all by itself. The price inversion is real: DDR4 trades at $2.10/Gb while server-grade DDR5 trades at $1.50/Gb [23]. Gartner's Tony Harvey: "When an on-premises server costs 4x what it did a year ago that changes the comparison to cloud" [13]. AWS chief Andy Jassy used his Q1 earnings call to tell analysts the memory shortage is accelerating customer migration to AWS, with Omdia's Roy Illsley pushing back with a useful caveat: "most on-premises datacenters already have servers with memory, so it just means they delay a refresh or upgrade and wait for a server to be delivered" [13]. Meta is extending server life from six to seven years in response to the deficit and expects DRAM and hard-drive constraints through 2027 [13]. The implication for everyone except hyperscalers is straightforward: less leverage with suppliers, longer refresh cycles, harder math on cloud-vs-on-prem, and pressure to lock in supply ahead of need.

China's "AI as infrastructure" play

A New York Times opinion piece (Jacob Dreyer, May 9) makes a useful long-arc argument: the US and China are racing toward different finish lines [24]. US strategy is bet-the-farm on superintelligence; Chinese strategy ("AI+") treats AI as infrastructure to embed into public services: schools, hospitals, transit, urban management. Chinese A.I. is integrated into supply chains that dominate world trade; as China exports those systems to emerging markets (energy, telecoms, transportation, surveillance), "it will be exporting Chinese governance as well, with all of the safety, abundance, surveillance and embedded hierarchies that entails" [24]. Whether or not you accept the framing, the strategic point matters for sectors that operate internationally: the choice of "good enough AI infrastructure that comes with governance assumptions" is now a procurement and risk decision, not a hypothetical.

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Mitigate Palo Alto PAN-OS CVE-2026-0300.** Restrict the User-ID Authentication Portal to trusted networks or disable it. No patch yet. Watch for one and apply when released.
2. **Apply CVE-2026-32202 Windows updates** ahead of the May 12 federal deadline. Block outbound SMB to untrusted destinations as a defense-in-depth.
3. **Audit JDownloader endpoints.** Anyone who downloaded between May 6–7 from the official site should treat their workstation as compromised: full reinstall + credential reset. Verify Digital Signatures of any installer in scope: legit is "AppWork GmbH."
4. **Pull the compromised package versions out of your dev/CI environment.** SAP CAP family (mbt 1.2.48, @cap-js/db-service 2.10.1, @cap-js/postgres 2.2.2, @cap-js/sqlite 2.2.2), intercom-client 7.0.4 and 7.0.5, PyTorch Lightning 2.6.2 and 2.6.3. Audit GitHub for unexpected repo creation under service accounts; rotate all secrets touched by CI runners.
5. **Validate Linux kernel posture against Dirty Frag.** Apply Kim's mitigation on sensitive systems pending patches. Watch for vendor advisories.
6. **Inventory and replace named TP-Link SOHO models.** Disable remote management. Rotate router admin credentials. Assume DNS-level traffic visibility loss on any device that has not been firmware-updated in two years.
7. **Refresh phishing training and tooling for the 86%-AI baseline.** Specifically cover calendar-invite phishing, Microsoft Teams help-desk impersonation, and AI-quality lures that no longer have spelling-error tells.

Strategic Actions (This Month)

1. **Microsoft Entra ID device-code flow lockdown.** Build a Conditional Access policy that blocks OAuth 2.0 device-code authentication by default, with explicit narrow exceptions for the hardware that legitimately requires it. Migrate identity-sensitive users (executives, finance, legal, HR, IT admins) to phishing-resistant MFA (FIDO2, passkeys, Windows Hello, Microsoft Authenticator) ahead of the broader rollout. Enable Defender for Office 365 Safe Links, Safe Attachments, ZAP, and Entra ID Protection risk-based blocking policies for Anomalous Token and session-cookie sign-in anomalies.
2. **Hardening reviews for developer tooling and supply chain.** Pinned versions, preinstall-script monitoring, restricted GitHub repo-creation permissions for service accounts, secrets-in-CI auditing, and IOC monitoring against the TeamPCP / Mini Shai-Hulud / PCPJack / Daemon Tools campaigns.
3. **Hire-process review for fake-IT-worker risk.** ID verification, on-camera technical interviews, location-of-work attestations, no shipping company laptops to addresses that cannot be tied to the named hire. Apply across all sectors; healthcare, finance, professional services are now active targets.
4. **Inventory Exchange Online TLS 1.0/1.1 dependencies** ahead of the July cutoff. Legacy clients, scanners, MFPs, and embedded appliances are the typical surprises.
5. **2026/2027 hardware planning under the memory-supply squeeze.** Run cloud-vs-on-prem math with realistic 2026 server prices, not 2024 numbers. Lock in supply where you have leverage; accept longer refresh cycles where you do not. Consider extending server life judiciously.
6. **For institutions that depend on critical SaaS** (LMS, EHR, ERP, identity): treat ShinyHunters' Canvas timing as a template. Operationally inconvenient breach windows (finals, fiscal close, surgery scheduling) are now an extortion lever. Build an institutional response plan that does not assume the SaaS provider is the sole respondent.
7. **For sectors exposed to Iran/Hormuz second-order effects:** build a 6–12 month price/supply contingency view for fuel, fertilizer (nitrogen and phosphate paths), sulfuric acid, plastics inputs (naphtha), aviation fuel, and shipping-dependent operations. Lock in supply where you have leverage; assess force majeure provisions on long-term contracts; qualify alternate suppliers; review reserve and stockpile policies. Aviation operators in Europe should specifically evaluate IATA/EASA Jet A guidance as a partial hedge.
8. **For C-suite and board reporting:** the IMF's framing of AI cyber risk as a financial-stability issue gives you the language you need to elevate AI security investment beyond IT. Use it.

REFERENCES

[1] *AI Is Supercharging Cybercrime — And IMF Says Finance May Not Be Ready* (Benzinga via MSN, May 2026). https://www.msn.com/en-us/money/news/ai-is-supercharging-cybercrime-and-imf-says-finance-may-not-be-ready/ar-AA22Lbbv

[2] *Bot her emails: most modern phishing campaigns are AI-enabled* (The Register, 2026-04-30). https://www.theregister.com/security/2026/04/30/most-phishing-now-uses-ai-says-knowbe4/5220579

[3] *JDownloader site hacked to replace installers with Python RAT malware* (BleepingComputer, 2026-05-09). https://www.bleepingcomputer.com/news/security/jdownloader-site-hacked-to-replace-installers-with-python-rat-malware/

[4] *The never-ending supply chain attacks worm into SAP npm packages, other dev tools* (The Register, 2026-05-01). https://www.theregister.com/security/2026/05/01/ongoing-supply-chain-attacks-worm-into-sap-npm-packages/5228837

[5] *Worm rubs out competitor's malware, then takes control* (The Register, 2026-05-08). https://www.theregister.com/security/2026/05/08/worm-rubs-out-competitors-malware-then-takes-control/5237389

[6] *Widely used Daemon Tools disk app backdoored in monthlong supply-chain attack* (Ars Technica, 2026-05). https://arstechnica.com/security/2026/05/widely-used-daemon-tools-disk-app-backdoored-in-monthlong-supply-chain-attack/

[7] *State-backed hackers hammer Palo Alto firewall zero-day before patch lands* (The Register, 2026-05-07). https://www.theregister.com/cyber-crime/2026/05/07/state-backed-hackers-hammer-palo-alto-firewall-zero-day-before-patch-lands/5234737

[8] *Microsoft's patch for a 0-day exploited by Russian spies fell short. Another Windows flaw is under attack* (The Register, 2026-04-29). https://www.theregister.com/security/2026/04/29/microsoft-patch-fell-short-new-windows-flaw-exploited/5227153

[9] *'Dirty Frag' Linux flaw one-ups CopyFail with no patches and public root exploit* (The Register, 2026-05-08). https://www.theregister.com/security/2026/05/08/dirty-frag-linux-flaw-one-ups-copyfail-with-no-patches-and-public-root-exploit/5237230

[10] *5 steps the FBI wants you to take to secure your router right now* (CNET). https://www.cnet.com/home/internet/5-steps-the-fbi-wants-you-to-take-to-secure-your-router-right-now/

[11] *FBI cyber boss: China's hacker-for-hire ecosystem 'out of control'* (The Register, 2026-04-30). https://www.theregister.com/security/2026/04/30/fbi-chinas-hacker-for-hire-ecosystem-out-of-control/5227748

[12] *How a massive hack on school software disrupted classes across America* (NBC News, 2026-05-08/09): https://www.nbcnews.com/tech/security/canvas-software-hacked-disrupted-classes-america-shinyhunters-rcna344199 ; *Hackers ate my homework: Educational SaaS Canvas down after cyberattack* (The Register, 2026-05-08): https://www.theregister.com/security/2026/05/08/hackers-ate-my-homework-educational-saas-canvas-down-after-cyberattack/5235561

[13] *AWS says acute server memory shortage is driving customers to the cloud* (The Register, 2026-04-30). https://www.theregister.com/2026/04/30/server_memory_shortage_pushing_you/

[14] *Fake IT workers rented laptops to Nork scammers, got prison time* (The Register, 2026-05-07). https://www.theregister.com/cyber-crime/2026/05/07/fake-it-workers-rented-laptops-to-nork-scammers-got-prison-time/5235342

[15] *Legacy TLS tour continues with Exchange Online blocking old versions from July 2026* (The Register, 2026-04-29). https://www.theregister.com/security/2026/04/29/exchange-online-blocks-legacy-tls-from-july-2026/5227378

[16] *Fertiliser shortages caused by Iran war drive up costs for UK farmers by up to 70%* (The Guardian, 2026-05-06). https://www.theguardian.com/business/2026/may/06/fertiliser-shortages-iran-war-global-food-prices-farming

[17] *AI companies want you to be afraid of them* (BBC Future, 2026-04-29). https://www.bbc.com/future/article/20260428-ai-companies-want-you-to-be-afraid-of-them

[18] *Seeking reassurance at a federal lab in Richland where AI is booming* (The Seattle Times, 2026-05-09). https://www.seattletimes.com/pacific-nw-magazine/seeking-reassurance-at-a-federal-lab-in-richland-where-ai-is-booming/

[19] *Vidar Malware Campaign Targets Login Credentials, Session Cookies, and Wallet Files* (Cyberpress / LevelBlue, 2026-05-09). https://cyberpress.org/vidar-malware-campaign-targets-login-credentials/

[20] CNET *5 steps the FBI wants you to take to secure your router right now*: see [10]. See also FBI/NSA disclosure 2026-04-07 and UK NCSC TP-Link advisory.

[21] *Pro-Iran crew turns DDoS into shakedown as Ubuntu.com stays down* (The Register, 2026-05-01). https://www.theregister.com/security/2026/05/01/pro-iran-group-turns-ubuntu-ddos-into-shakedown/5224575

[22] *Drones outpace security at large public gatherings, CIS warns* (StateScoop): https://statescoop.com/drones-security-risks-large-public-gatherings-cis-report/ ; CIS report: https://www.cisecurity.org/insights/white-papers/uas-evolving-risks-to-large-scale-public-gatherings

[23] *Server memory prices could double by 2026 as AI demand strains supply* (Network World citing Counterpoint Research). https://www.networkworld.com/article/4093752/server-memory-prices-could-double-by-2026-as-ai-demand-strains-supply.html

[24] *Why China Is So Much Less Scared of A.I.* (Jacob Dreyer, NYT Opinion, 2026-05-09). https://www.nytimes.com/2026/05/09/opinion/ai-china-america-race.html

[25] *How the Iran War Is Disrupting Global Oil and Gas Supply* (energynow.ca / Bloomberg, 2026-03). https://energynow.ca/2026/03/how-the-iran-war-is-disrupting-global-oil-and-gas-supply/

[26] *Why a US-Iran peace deal won't immediately solve the oil supply crisis* (Baird Maritime / Reuters, 2026-05-07). https://www.bairdmaritime.com/shipping/tankers/feature-why-a-us-iran-peace-deal-wont-immediately-solve-the-oil-supply-crisis

[27] *Energy Secretary Chris Wright won't rule out $5 gas due to Iran war* (Washington Examiner, 2026-05): https://www.washingtonexaminer.com/policy/energy/4562203/chris-wright-5-dollar-gas-iran-war/ ; JPMorgan via Bloomberg: https://www.bloomberg.com/news/articles/2026-05-08/risk-of-5-gasoline-can-no-longer-be-dismissed-jpmorgan-says

[28] *Jet fuel shortages threaten summer travel as Iran war ripples through Asia and Europe* (CNBC, 2026-05-06). https://www.cnbc.com/2026/05/06/iran-war-jet-fuel-europe-asia-summer-flights.html

[29] *European airlines could use US-grade jet fuel to ease shortages from Iran war* (BBC News, Theo Leggett, 2026-05-08). https://www.bbc.com/news/articles/cp8pk2m4nlxo

[30] *West Asia war triggers global sulfuric acid supply shortage* (Press TV citing Wall Street Journal, 2026-05-10). https://www.presstv.ir/Detail/2026/05/10/768359/west-asia-war-sulfuric-acid-supply-shortage (NOTE: original WSJ source 2026-05-09 preferred for production briefing)

[31] *CMMC: Low Compliance Rate, Few C3PAOs Hamper Pentagon Program* (ExecutiveGov, 2026-05). https://www.executivegov.com/articles/cmmc-dow-cybersecurity-c3pao-cio

[32] *Rev. 3 is coming: Start preparing for the next CMMC requirement* (Ned Butler, Redspin, in Federal News Network, 2026-04-24). https://federalnewsnetwork.com/commentary/2026/04/rev-3-is-coming-start-preparing-for-the-next-cmmc-requirement/

[33] *Hundreds compromised daily in Microsoft device code phishes* (The Register, 2026-04-07). https://www.theregister.com/security/2026/04/07/hundreds-compromised-daily-in-microsoft-device-code-phishes/5222742

[34] *New EvilTokens service fuels Microsoft device code phishing attacks* (BleepingComputer, Bill Toulas, citing Sekoia research). https://www.bleepingcomputer.com/news/security/new-eviltokens-service-fuels-microsoft-device-code-phishing-attacks/

[35] *Breaking the code: Multi-stage 'code of conduct' phishing campaign leads to AiTM token compromise* (Microsoft Defender Security Research Team, 2026-05-04). https://www.microsoft.com/en-us/security/blog/2026/05/04/breaking-the-code-multi-stage-code-of-conduct-phishing-campaign-leads-to-aitm-token-compromise/

[36] *AI-powered hacking has exploded into industrial-scale threat, Google says* (Aisha Down and Dan Milmo, The Guardian, citing Google Threat Intelligence Group report, 2026-05-11). https://www.theguardian.com/technology/2026/may/11/ai-powered-hacking-industrial-scale-threat-three-months-google

Additional Resources

- CIS UAS report: https://www.cisecurity.org/insights/white-papers/uas-evolving-risks-to-large-scale-public-gatherings
- HR 7525 (Burlison counter-drone bill): https://www.congress.gov/bill/119th-congress/house-bill/7525
- JDownloader incident report: https://jdownloader.org/incident_8.5.2026.html

- Yara warning on African food security: https://www.theguardian.com/business/2026/may/01/iran-war-may-cause-food-shortages-in-africa-world-largest-fertiliser-firm-yara-says

---

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net