# AI CYBER RISK IS A FINANCIAL STABILITY ISSUE 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
**Sector:** Financial Services

---

## EXECUTIVE SUMMARY

The two weeks since the April 27 briefing produced the first time a multilateral financial institution put AI cybercrime on the financial-stability shelf, and they did it the same week an industrial-scale phishing campaign targeting finance personas was hitting hundreds of organizations daily. Highlights for financial services:

- **The IMF named AI cybercrime a financial-stability concern** at its spring meetings, warning that AI-driven attacks could trigger funding strains, solvency concerns, and broader market disruption — and citing Anthropic's Claude Mythos Preview as evidence the threat is moving faster than patching [1]. Barclays' CEO C.S. Venkatakrishnan publicly called Mythos "a serious issue" and noted "There will be a Mythos 2 and a Mythos 3." CrowdStrike's 2026 Global Threat Report puts AI-powered attacks up 89% year-over-year [1]. **Google's Threat Intelligence Group reached the same conclusion from the security-operations side on May 11**, concluding AI-powered hacking has gone from a nascent problem to an industrial-scale threat in just three months, with criminal groups and state-linked actors from China, North Korea, and Russia widely using Gemini, Claude, and OpenAI tools to scale attacks. Google's chief analyst John Hultquist: *"the AI vulnerability race … has already begun"* [36].
- **An active Microsoft device-code phishing campaign is targeting finance personas specifically.** Since March 15, 10–15 distinct campaigns are launching every 24 hours; "post-compromise activity shows a consistent focus on finance-related personas, with automated email exfiltration observed in those accounts" (Microsoft VP Tanmay Ganacharya) [33]. Tooling overlaps with the EvilTokens phishing-as-a-service kit, which is actively used by Russian groups and the ShinyHunters data-extortion crew [34]. A parallel AiTM "code of conduct" campaign hit financial services at 18% of victims (35,000+ users across 13,000+ organizations in 26 countries between April 14–16) [35].
- **The phishing baseline jumped to 86% AI-enabled** (KnowBe4); calendar-invite phishing up 49%; Microsoft Teams help-desk impersonation up 41%; Microsoft says AI lures are 4.5× more effective than human-crafted [2]. FBI: 2025 US cybercrime losses hit $20.87B, with ~$893M in AI-related fraud [2].
- **Vidar is back at scale** as the favored info-stealer of financial threat actors and initial access brokers, harvesting browser passwords, cookies, and crypto wallets via Microsoft Toolkit hacktool delivery [19].

- **Edge-device cluster.** Palo Alto PAN-OS zero-day under active state-backed exploitation with **no patch yet** [7]; incomplete Windows fix left a zero-click NTLM credential-theft hole live [8]; "Dirty Frag" Linux LPE released with no CVE, no patches, and a public root exploit [9]. Russia's GRU continues DNS-hijacking SOHO routers used by remote workforce [10].
- **The Iran war reaches commodity exposure.** IEA: "largest supply disruption in the history of the global oil market"; Brent $101; jet fuel doubled in Europe; marine cargo, hull, and war-risk premiums for Gulf transit are repricing; commodity hedging desks need to build sustained-disruption scenarios, not assume quick reopening [25, 26, 28].
- **Server DRAM on track to double by year-end** as AI demand bends the IT supply chain [13, 23].

The next 30 days for finance are about five things:

1. Lock down Microsoft Entra ID device-code authentication flow; migrate identity-sensitive users (executives, finance, treasury, audit, IT admins) to phishing-resistant MFA (FIDO2, passkeys, Microsoft Authenticator).
2. Treat 86%-AI phishing as the new baseline and refresh both training and email/identity controls accordingly.
3. Apply the urgent edge/endpoint patches and mitigations (Palo Alto, Windows CVE-2026-32202, Dirty Frag).
4. Use the IMF framing in board reporting to elevate AI security investment beyond IT.
5. Run a 6–12 month commodity / energy / shipping scenario across hedging desks and revisit Gulf-transit insurance.

---

## SUMMARY OF IMMEDIATE ACTIONS

| Priority | Action | Why Now |
|---|---|---|
| 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 | Active campaign compromising hundreds of organizations daily since March 15; **finance personas specifically targeted for post-compromise email exfil**; bypasses non-phishing-resistant MFA; EvilTokens PhaaS in active use [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`; PDF SHA-256s `5DB1EC...AECBC6`, `B5A334...876C9EAD`, `11420D...BE1A49D` | Financial services was 18% of victims across 13,000+ organizations in 72 hours; full IOC list in [35] |
| CRITICAL | Migrate executives, finance/treasury, audit, payments, AP/AR, and IT admin users to phishing-resistant MFA (FIDO2, passkeys, Windows Hello, Microsoft Authenticator); disable SMS and push as second factor for these populations | AiTM and device-code attacks bypass non-phishing-resistant MFA; this is the only durable control [33, 35] |
| 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] |
| CRITICAL | If anyone in your environment downloaded JDownloader from the official site between May 6 and May 7, treat those endpoints as compromised; search EDR/firewall telemetry for downloads from `jdownloader.org` in that window and for outbound connections to `parkspringshotel[.]com`, `auraguest[.]lk`, `checkinnhotels[.]com` | Site backdoored; Python RAT loader confirmed [3] |
| HIGH | Audit dev/CI environments for the compromised npm and PyPI packages (SAP CAP family, intercom-client 7.0.4/7.0.5, PyTorch Lightning 2.6.2/2.6.3); rotate cloud, Kubernetes, and GitHub Actions secrets touched by CI runners | Mini Shai-Hulud worm exfiltrates secrets via repos under your account [4] |

| Priority | Action | Why Now |
|---|---|---|
| HIGH | Refresh phishing training for the device-code prompt, the "code of conduct review" lure family, calendar-invite phishing, and Microsoft Teams help-desk impersonation; specifically warn finance teams that invoice / payroll / RFP / wire-instruction lures are now AI-personalized | KnowBe4: 86% AI use in phishing; Microsoft: AI lures 4.5× more effective; calendar invites +49%, Teams impersonation +41% [2, 33] |
| 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 [9] |
| HIGH | Patch or replace the named TP-Link SOHO router models still in use by remote workforce and branch offices; disable remote management; rotate router admin credentials | GRU APT28 DNS-hijacking 23 named TP-Link models since 2024 [10] |
| HIGH | Review hiring controls and contractor onboarding for the North Korean fake-IT-worker scheme (now explicitly targeting financial services per DoJ) | DoJ confirms scheme expanded into finance; $500M+/year for Pyongyang; data theft alongside revenue [14] |
| HIGH | Vet your inbox-rule and email-forwarding governance: alert on creation of rules that auto-forward messages with "payroll," "invoice," "wire," or "ACH" in the subject; require admin review for any new outbound forwarding rule | Post-compromise device-code attackers observed creating exactly these inbox rules to siphon financial communications [33] |
| HIGH | Use the IMF systemic-risk framing in your next board cyber report; pair it with CrowdStrike's 2026 numbers (AI attacks +89%, state-actor cloud intrusions +266%) to elevate AI security investment | IMF position lands in board rooms in a way vendor warnings do not [1] |
| MEDIUM | Build the AI-driven memory squeeze into 2026 and 2027 hardware refresh plans (core banking, fraud platforms, data lake); lock in supply where you have leverage | Server DRAM on track to double; SK Hynix sold out HBM/DRAM/ NAND through 2026; Meta extending server life 6→7 years [13, 23] |
| HIGH | Run a sustained Gulf-disruption scenario across commodity, marine, energy, and aviation hedging books; review war-risk and hull premiums for vessel exposure; revisit force majeure language on multi-year fuel contracts and refined-product supply agreements | IEA: largest supply disruption in oil market history; Brent $101; 1.2–2B barrel projected loss; recovery 1–6+ months after Hormuz reopens [25, 26, 28] |

| Priority | Action | Why Now |
|---|---|---|
| HIGH | If you hold or supply DOW (Department of War) contracts touching CUI (e.g., defense banking, prime contractor financing, defense-sector M&A advisory): review SPRS affirmation and begin Rev 3 prep | CMMC Phase 2 mandatory Level 2 begins 2026-11-10; ~1% certified; Rev 3 in DOW rule-making within 12–18 months [31, 32] |

## WHAT'S CHANGED SINCE APRIL 27

- **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. Barclays' CEO publicly called Mythos "a serious issue" and predicted Mythos 2 and 3. The IMF specifically warned that financial systems built on decades-old legacy infrastructure may not withstand AI-enabled attack speed [1].
- **Microsoft device-code phishing went industrial against finance personas.** Microsoft reported on April 7 that 10–15 distinct device-code phishing campaigns launch every 24 hours, with post-compromise focus on finance-related personas and automated email exfiltration [33]. EvilTokens PhaaS use is widespread and adversaries include the ShinyHunters crew that took down Canvas [34]. Microsoft Defender Research disclosed a separate AiTM "code of conduct" campaign in which financial services were 18% of the 13,000+ affected organizations [35].
- **The supply-chain attack tempo did not let up.** TeamPCP / Mini Shai-Hulud expanded across SAP, Intercom, and PyTorch Lightning packages [4]; JDownloader's website was backdoored [3]; Kaspersky disclosed a monthlong Daemon Tools backdoor with targeted QUIC RAT payload [6]; SentinelLabs found a competing worm (PCPJack) explicitly harvesting finance, enterprise, and cloud credentials [5].
- **Edge devices entered another bad cycle** (Palo Alto, Windows, Dirty Frag, TP-Link), and **ShinyHunters used a Canvas / Instructure breach against the education sector** to test a finals-timed extortion model that financial-services SaaS users (core banking, payment processors, identity, treasury management) should treat as a template [7, 8, 9, 10, 12].

## THE IMF FRAMING AND WHAT IT MEANS FOR FINANCE

The headline financial-stability framing matters and is worth understanding at the board level.

**What the IMF said.** Speaking at the spring meetings, the IMF warned that AI-driven cyberattacks pose a growing threat to financial stability, with "extreme cyber-incident losses potentially triggering funding strains, solvency concerns and broader market disruption" [1]. The IMF cited two structural facts. First, advanced AI

models can “dramatically reduce the time and cost needed to identify and exploit vulnerabilities,” and “discovering and exploiting vulnerabilities can occur faster than patching and remediation” [1]. Second, the financial system relies on shared digital infrastructure (software, cloud services, payment networks) also used by energy, telecom, and public services; dependence on a small number of platforms could turn a localized breach into a system-wide macro-financial shock [1].

**What this changes.** Cyber stress testing, scenario analysis, and board-level oversight are now framed by the IMF as “indispensable components of financial stability frameworks” [1]. For financial institutions, that is regulator language. Expect Federal Reserve, OCC, FDIC, FINRA, FCA, and ECB supervisory programs to reflect this framing in 2026–2027 examinations.

**Barclays’ framing.** C.S. Venkatakrishnan, speaking at the G30 consultancy group meeting during the IMF spring gatherings, called Mythos “a serious issue” and warned that it could identify vulnerabilities in financial systems and suggest ways to exploit them. “There will be a Mythos 2 and a Mythos 3” [1]. This is a publicly traded global bank CEO saying the AI vulnerability-discovery curve is a strategic issue, not a SOC issue.

**What to do.** Use this material in your next board cyber report. Pair the IMF systemic-risk language with CrowdStrike’s 2026 Global Threat Report numbers (AI-powered attacks +89% year-over-year, state-actor cloud intrusions +266%) [1]. Pair it with KnowBe4’s 86% AI-in-phishing baseline and Microsoft’s data that AI lures are 4.5× more effective than human-crafted [2]. Pair it with Google’s Threat Intelligence Group concluding on May 11 that AI-powered hacking has crossed from nascent to industrial-scale in three months [36]. When the IMF, the leading commercial threat-intel publisher (CrowdStrike), Microsoft, and Google all converge on the same characterization within a single quarter, the conversation has shifted. This is the language you need to elevate AI security investment beyond IT.

---

## ACTIVE CAMPAIGN: DEVICE-CODE PHISHING TARGETING FINANCE PERSONAS

**The volume and the focus.** Microsoft’s Ganacharya: “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. We continue to observe high-volume activity, with hundreds of compromises occurring daily across affected environments” [33]. Critically for this sector: “post-compromise activity shows a consistent focus on finance-related personas, with automated email exfiltration observed in those accounts” [33].

**The mechanism.** The attackers abuse OAuth 2.0 device-code authentication, the flow originally designed for smart TVs, printers, and headless devices. An attacker initiates the flow, tricks a finance, treasury, AP/AR, or executive user into entering the code on `microsoft.com/devicelogin`, and completes authentication as the user. Non-phishing-resistant MFA (SMS, push, TOTP) does not stop this [33].

**The clever part.** The campaign uses dynamic device-code generation. Static phishing emails ship a pre-generated code, leaving a small 15-minute window for the attack. This campaign defers code generation to the final stage of the redirect chain (Railway, Cloudflare Workers, DigitalOcean, AWS Lambda fronting), so the 15-minute timer doesn't start until the victim is already on the final page [33].

**The post-compromise pattern for finance.** 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 and creating inbox rules that forward messages whose subjects contain "payroll" or "invoice" [33]. For financial institutions, expand the watch list: alert on rule creation containing "wire," "ACH," "treasury," "settlement," "FedWire," "SWIFT," "trade," and counterparty names.

**EvilTokens and the actor set.** EvilTokens phishing-as-a-service is sold on Telegram and used by multiple Russian groups (Storm-237, UTA032, UTA0355, UNK_AcademicFlare, TA2723) and ShinyHunters [34]. EvilTokens lures impersonate financial documents, meeting invitations, logistics or purchase orders, payroll notices, and DocuSign / SharePoint shares; aimed at finance, HR, logistics, and sales [34]. Sekoia: most-affected countries are US, Canada, France, Australia, India, Switzerland, UAE. Operators have advertised plans to add Gmail and Okta phishing pages [34].

**The "code of conduct" AiTM campaign.** April 14–16: 35,000+ users across 13,000+ organizations in 26 countries hit in 72 hours. 92% US. Financial services was 18% of the victim set, second only to healthcare [35]. Lures spoofed internal compliance and a Paubox HIPAA-compliance encryption banner. Cloudflare CAPTCHA + image-selection second CAPTCHA gated against sandboxes. Ultimate token capture via AiTM proxy of the Microsoft sign-in page.

**Why standard awareness training fails.**

- The final destination is `microsoft.com/devicelogin` itself. "Check the URL" training fails.
- AiTM and device-code attacks bypass non-phishing-resistant MFA (SMS, push, TOTP).
- AI-generated lures and platform-aware redirect chains defeat pattern-based detection.

**What works.**

- Block or scope down OAuth 2.0 device-code flow via Entra ID Conditional Access. Microsoft's explicit guidance is "only allow device code flow where absolutely necessary" [33].
- Migrate executives, finance, treasury, audit, AP/AR, payments, IT admin, and any privileged role to phishing-resistant MFA (FIDO2 / passkeys / Windows Hello / Microsoft Authenticator). Disable SMS and push as second factor for these populations.
- Enable Entra ID Protection risk-based blocking for "Anomalous Token," "Unfamiliar sign-in properties for session cookies," and "Impossible travel" — and elevate from monitor to block for high-value identities [35].
- Defender for Office 365: Safe Links, Safe Attachments, Zero-hour Auto Purge, network protection in Defender for Endpoint [35].

- Inbox-rule governance: alert on creation of forwarding rules that match financial subject keywords; require admin review for any new outbound forwarding rule.

---

## SUPPLY CHAIN AND EDGE RISK FOR FINANCIAL INSTITUTIONS

**Supply-chain attacks against developer tooling.** Four discrete compromises in this period directly affect any financial institution running a non-trivial software development organization: JDownloader (May 6–7, Python RAT loader) [3]; TeamPCP / Mini Shai-Hulud (SAP CAP, Intercom, PyTorch Lightning npm/PyPI; steals GitHub tokens, npm credentials, AWS/Azure/GCP secrets, Kubernetes tokens, GitHub Actions secrets; exfiltrates via repos under your account) [4]; Daemon Tools (monthlong Kaspersky-disclosed campaign with QUIC RAT to government, scientific, manufacturing, and retail targets) [6]; PCPJack (SentinelLabs-disclosed worm that hijacks TeamPCP victims and harvests finance / enterprise / messaging / cloud credentials) [5]. For financial institutions, the supply-chain wedge is your developer pipeline. Pin versions, monitor preinstall scripts, alert on GitHub repo creation under service accounts, audit secrets stored as environment variables in CI runners.

**Vidar back at scale.** LevelBlue documented a multi-stage Vidar info-stealer campaign delivered via fake Microsoft Toolkit hacktool [19]. Vidar (originally Arkei, 2018) is the long-running info-stealer favored by financial threat actors and initial access brokers. Defense evasion is exemplary: 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`. Targets: browser passwords, cookies, crypto wallets. If you operate any crypto-adjacent business (custody, exchange relationships, treasury operations involving stablecoins, customer wallet support), Vidar should be in your hunting queries.

**Edge & endpoint vulnerabilities affecting bank perimeters and remote workforces.**

- **Palo Alto PAN-OS CVE-2026-0300** (CVSS 9.3, no patch): unauthenticated remote code execution as root on internet-exposed PA-Series and VM-Series firewalls. State-backed cluster CL-STA-1132 active since April 9; attackers cleared logs, moved into Active Directory, and on April 29 forced a secondary firewall to take over and compromised that too [7]. Until Palo Alto ships a patch, restrict User-ID Authentication Portal to trusted networks or disable it.
- **Windows CVE-2026-32202** (zero-click NTLM hash leak via auto-parsed LNK files): incomplete February fix. Microsoft marked “exploitation detected” April 28; CISA KEV with May 12 federal deadline [8].
- **“Dirty Frag” Linux LPE** (no CVE, no patches, public root exploit): affects Ubuntu, RHEL, CentOS Stream, Fedora, AlmaLinux, openSUSE Tumbleweed. Apply researcher’s temporary mitigation pending vendor patches [9].

- **TP-Link SOHO routers** (GRU APT28 DNS hijacking since 2024): 23 named models, list likely incomplete. For financial institutions with remote workforce, branch offices, or BYO-network executives, this is an authentication-bypass vector for the home perimeter [10].

**Exchange Online TLS 1.0/1.1 cutoff July 2026.** Microsoft will block legacy TLS for POP3 and IMAP4 starting July. Inventory legacy mail clients, scanners, MFPs, and embedded appliances now; these are the typical surprise dependencies [15].

---

## THE IRAN WAR AND FINANCIAL EXPOSURE

The Iran war that began February 28 is producing what the IEA called "the largest supply disruption in the history of the global oil market" [25]. For financial services, three exposures matter: commodity hedging, marine insurance, and counterparty credit on energy-exposed and food-exposed operating companies.

**Commodity hedging.** Brent at $101.27/bbl on May 6 (Reuters poll: 2026 average $86.38, up from ~$62 in January). Rystad: 600M barrels lost so far, projected total losses 1.2–2 billion barrels (16–27% of pre-war global inventories). LNG loss 30–50 million tonnes (7–11% of annual global supply) following Iranian drone strike on Qatar's Ras Laffan facility [25, 26]. Hedging desks should build sustained-disruption scenarios rather than assume a quick reopening. Equinor's CEO says it will take six months minimum to normalize even with peace; Exxon says 1–2 months for oil flows to clear after Hormuz reopens (30-day ME→EU shipping, 40-day ME→US) [26].

**Marine and war-risk premiums.** Marine cargo, hull, and war-risk premiums for Gulf transit are repricing. Underwriters should be modeling sustained vessel exposure, not the brief shock pattern. Australia announced $7.22B to build fuel reserves; EU is considering revising the 90-day oil-stock requirement to add a specific jet-fuel reserve mandate [26].

**Counterparty credit exposure to second-order effects.**

- **Aviation:** Lufthansa cut 20,000 short-haul flights through October; carriers exposed to Middle East refining or Asian refining-via-Gulf-feedstock should be in your watch. Ireland reportedly down to 10 days of jet-fuel stock cover [26, 28].
- **Agriculture and food processors:** UK farmer fertilizer costs up 50–70%; sulfuric acid (input to phosphate fertilizers, copper leaching, steel pickling) tightening as Persian Gulf refineries are choked off; China imposed sulfuric acid export restrictions in May [16, 30].
- **Manufacturing:** Naphtha (plastics, road fuel) rising alongside other refined products; sulfuric acid upstream of copper smelting, steel pickling, rubber, leather [25, 30].
- **Shipping and freight:** Bunker fuel costs rising; Singapore fuel-oil stocks at near-1-year low [26].

**The cyber dimension.** Pro-Iran "313 Team" (Islamic Cyber Resistance in Iraq) shifted from DDoS-as-hacktivism to DDoS-as-extortion against Canonical's Ubuntu.com starting April 30, demanding payment in a Telegram message [21]. Financial-services targets are not yet named but the precedent is established; treat sustained DDoS combined with a Telegram demand as a recognizable pattern.

---

## CMMC AND DEFENSE-ADJACENT FINANCIAL SERVICES

Financial institutions providing services to DOW primes, defense-sector M&A advisory, defense banking, or prime-contractor receivables financing are increasingly being asked about CMMC posture by their clients. The picture has not improved. Of roughly 100,000 DIB contractors expected to need CMMC Level 2 certification, approximately 1% have achieved it [31]. Only 103 C3PAOs are authorized. Phase 2 (the point at which DOW can begin requiring Level 2 certification in individual contracts) begins November 10, 2026. Phase 3, requiring independent C3PAO assessment every three years, begins November 10, 2027. SMB total cost of compliance and prep runs $50K–$100K [31].

NIST SP 800-171 Rev 3 is the next shoe to drop; DOW rule-making expected within 12–18 months. Rev 3 adds three new control families (supply chain security, incident response, advanced threat counter), introduces 88 organization-defined parameters where DOW sets the values, and formally incorporates the Rev 2 Appendix E NFO controls [32]. A "major change" to an assessed environment triggers re-certification, and DOW has not yet defined what counts as a major change. For institutions touching CUI through their defense-sector book, the recommended path is to build current certification on Rev 2 and in parallel begin a Rev 3 migration plan that voluntarily implements the Rev 2 Appendix E NFOs.

*The Stillwater Group provides CMMC readiness consulting, NIST SP 800-171 gap assessments, and SPRS affirmation review for financial institutions providing services to the DIB.*

---

## WHAT YOU SHOULD BE DOING RIGHT NOW

### This Week

1. **Block or scope-down Entra ID OAuth 2.0 device-code flow** via Conditional Access; allow only for specific user groups, devices, and locations that legitimately need it.
2. **Migrate finance, treasury, AP/AR, payments, audit, executive, and IT admin populations to phishing-resistant MFA** (FIDO2 / passkeys / Microsoft Authenticator). Disable SMS and push as second factor for these populations.
3. **Hunt the AiTM "code of conduct" campaign IOCs** in EDR, email gateway, and identity logs. Full IOC list in [35] and in the immediate-actions table above.

4. **Apply the urgent patches and mitigations:** Palo Alto Captive Portal lockdown (no patch yet); Windows CVE-2026-32202 (May 12 federal deadline); Dirty Frag Linux mitigation.
5. **Audit JDownloader exposure** in the May 6–7 window; reinstall and rotate credentials on affected endpoints.
6. **Refresh phishing training** for the device-code prompt, the "code of conduct" lure family, calendar-invite phishing, and Teams help-desk impersonation. Specifically warn finance teams that invoice / wire / RFP / payroll lures are now AI-personalized.
7. **Inbox-rule governance:** alert on creation of forwarding rules matching financial subject keywords (wire, ACH, payroll, invoice, FedWire, SWIFT, settlement, treasury, counterparty names).

## This Month

1. **Use the IMF systemic-risk framing in your next board cyber report.** Pair with CrowdStrike's 2026 numbers and KnowBe4's 86% AI-in-phishing baseline. This is the language to elevate AI security beyond IT.
2. **Developer-pipeline hardening.** Pinned versions, preinstall-script monitoring, restricted GitHub repo-creation permissions for service accounts, secrets-in-CI auditing. Add IOC monitoring against TeamPCP / Mini Shai-Hulud / PCPJack / Daemon Tools.
3. **Sustained Gulf-disruption scenario** across commodity, marine, energy, and aviation hedging books. Review war-risk and hull premiums. Revisit force majeure clauses on multi-year fuel contracts and refined-product supply agreements. Stress-test counterparty credit on aviation, agriculture / food processors, manufacturing, and shipping operating companies.
4. **Hire-process review for North Korean fake-IT-worker risk** now that the scheme has expanded into financial services. ID verification, on-camera technical interviews, location-of-work attestations, no shipping company laptops to unverifiable addresses.
5. **Exchange Online TLS 1.0/1.1 inventory** ahead of the July cutoff.
6. **2026/2027 hardware planning under the memory-supply squeeze.** Core banking, fraud platforms, data lake, and recovery infrastructure all assume specific DRAM cost curves; redo the math at 2026 server prices.
7. **For institutions providing SaaS to your own customers** (treasury management, payments, identity, fraud platforms): the Canvas / ShinyHunters timing pattern (extortion deadline aligned with fiscal close, settlement window, or regulator filing deadline) is now an extortion lever to plan for.
8. **For institutions providing services to DOW / DIB contractors:** SPRS affirmation review and Rev 3 prep are increasingly relevant to your client conversations.

---

# 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* (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/

[12] *How a massive hack on school software disrupted classes across America* (NBC News): 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

[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/

[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

[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

[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

[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

[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

[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* (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, citing Sekoia). 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, 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, 2026-05-11). https://www.theguardian.com/technology/2026/may/11/ai-powered-hacking-industrial-scale-threat-three-months-google

---

*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*