HEALTHCARE WAS THE #1 TARGET OF THE AITM CAMPAIGN

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: Healthcare and Life Sciences (hospitals, health systems, medical devices, payers, life sciences, research)

EXECUTIVE SUMMARY

The two weeks since the April 27 briefing produced a number that should stop the room: when Microsoft Defender Research disclosed a three-day AiTM credential-theft campaign that hit 13,000+ organizations in 26 countries, **Healthcare and life sciences was the most-affected industry at 19% of victims** — and the lures spoofed a Paubox HIPAA-compliance encryption banner to enhance legitimacy [35]. Healthcare was the headline target. Highlights for the sector:

- **An active Microsoft device-code phishing campaign and a parallel AiTM "code of conduct" campaign are hitting healthcare hard.** Microsoft reports 10–15 distinct device-code campaigns launching every 24 hours since March 15, with hundreds of organizations compromised daily; post-compromise activity targets finance personas [33]. The AiTM campaign (April 14–16) hit 35,000+ users across 13,000+ organizations in 72 hours, with healthcare leading at 19% [35]. The Paubox spoof is the critical detail: healthcare staff are trained to trust encryption banners on regulated messages. EvilTokens phishing-as-a-service is in active use by Russian groups and the ShinyHunters crew that took down Canvas [34].
- **The North Korean fake-IT-worker scheme has expanded into healthcare.** Two more US "laptop farm" hosts were sentenced to 18 months prison this week; the DoJ explicitly named healthcare as a current expansion target alongside finance and professional services [14].
- **Phishing is now 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].
- **The Canvas / ShinyHunters breach is a template for healthcare SaaS extortion.** ShinyHunters timed the threat-to-leak deadline to coincide with university finals; the same pattern aimed at an EHR, scheduling, or PACS platform during surgery scheduling, billing close, or accreditation review would be operationally devastating [12].
- **Edge devices took another beating.** Palo Alto PAN-OS zero-day (CVE-2026-0300) under active state-backed exploitation with **no patch yet** [7]; incomplete Windows fix left a zero-click NTLM credential-theft

hole live (CISA KEV, May 12 federal deadline) [8]; "Dirty Frag" Linux LPE with no CVE and a public root exploit [9]. Russia's GRU continues DNS-hijacking SOHO routers used by remote workforce and home-based clinical staff [10].

- **The Iran war reached operations.** IEA: "largest supply disruption in the history of the global oil market." Diesel for backup generation at hospitals; aviation fuel for medical transport; and the sulfuric acid story matters for chemistry-supply downstream (pharma manufacturing, lab reagents) [25, 26, 28, 30].
- **The IMF named AI cybercrime a financial-stability concern** — important context for health-system board reporting now that healthcare is named as the leading target of a major credential-theft campaign [1].

The next 30 days for healthcare are about five things:

1. Hunt the AiTM "code of conduct" campaign IOCs across email gateway, EDR, and identity logs — the Paubox-spoofing template is most likely to convert against healthcare users.
2. Block Microsoft Entra ID device-code authentication flow for any role that does not legitimately need it; migrate physicians, executives, finance, IT admins, and revenue cycle to phishing-resistant MFA.
3. Apply the urgent edge/endpoint patches and mitigations.
4. Tighten hiring controls for the North Korean fake-IT-worker scheme now that DPRK is named as a healthcare-targeting actor.
5. Plan for diesel-backup, aviation, and pharma chemistry-supply pressure as the Iran war reaches operations.

SUMMARY OF IMMEDIATE ACTIONS

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`, `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`	**Healthcare & life sciences was 19% of victims** (highest industry); 35,000+ users / 13,000+ orgs / 26 countries / 72 hours; emails spoofed Paubox HIPAA-compliance encryption banner to enhance legitimacy with healthcare staff [35]

Priority	Action	Why Now
CRITICAL	Block Microsoft Entra ID OAuth 2.0 device code authentication flow via Conditional Access wherever not operationally required; restrict to specific user groups, devices, and locations where needed (digital signage in lobbies, conference room hardware, IoT/headless medical devices that use it)	Active campaign compromising hundreds of organizations daily since March 15; bypasses non-phishing-resistant MFA; EvilTokens PhaaS in active use by Russian groups and ShinyHunters [33, 34]
CRITICAL	Migrate physicians, executives, finance, revenue cycle, billing, HIM, IT/SOC admins, and any clinical leader with PHI access 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 on PA-Series and VM-Series firewalls (including any deployed at biomedical/clinical network boundaries)	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	Incomplete February patch left zero-click LNK auth-coercion live; APT28 toolkit territory [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 outbound connections to `parkspringshotel[.]com`, `auraguest[.]lk`, `checkinnhotels[.]com`	Site backdoored; Python RAT loader confirmed [3]

Priority	Action	Why Now
CRITICAL	Tighten hiring controls and contractor onboarding for the North Korean fake-IT-worker scheme: ID verification, on-camera technical interviews, location-of-work attestations, no shipping company laptops to addresses you cannot tie to the named hire	DoJ confirms scheme has expanded into healthcare; $500M+/ year for Pyongyang; data theft alongside revenue [14]
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; SAP heavily used in healthcare ERP/supply [4]
HIGH	Validate Linux server kernel posture in light of Dirty Frag — apply Hyunwoo Kim's temporary mitigation for sensitive systems pending patches (EHR back-end, PACS, lab informatics, revenue cycle, research compute)	Public root exploit, no CVE, no patches [9]
HIGH	Patch or replace the named TP-Link SOHO router models still in use at remote clinics, satellite offices, telehealth clinician home networks; disable remote management; rotate router admin credentials	GRU APT28 DNS-hijacking 23 named TP-Link models since 2024; remote clinicians are a prime exposure [10]
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 address the Paubox-spoofing template that targeted healthcare	KnowBe4: 86% AI use in phishing; Microsoft: AI lures 4.5× more effective; calendar invites +49%, Teams impersonation +41% [2, 35]

Priority	Action	Why Now
HIGH	Treat the Canvas / ShinyHunters timing pattern as a template for healthcare SaaS extortion: pre-stage IR for EHR / scheduling / PACS / RCM platform outages timed to surgery scheduling, accreditation, or month-end close; pre-decide ransom posture	ShinyHunters' Canvas attack timed leak deadline to finals week; same pattern aimed at clinical SaaS during operationally critical windows is the next inevitable variation [12]
HIGH	Review hiring controls for clinical informatics, telehealth, RCM-outsourced, and biomedical-engineering remote staff under the North Korean fake-IT-worker scheme (now explicitly targeting healthcare)	$500M+/year scheme; healthcare named as expansion target alongside finance and professional services [14]
HIGH	Plan for sustained pressure on diesel-for-backup generation, contracted refined-product delivery, aviation fuel for medical transport, and lab/pharma chemistry-supply downstream of the Iran war	IEA: largest supply disruption in oil market history; jet fuel +100% in Europe; sulfuric acid tightening with phosphate/ pharmaceutical chemistry downstream; China restricting both fuel and sulfuric exports [25, 26, 28, 30]
HIGH	Confirm the Microsoft Exchange Online TLS 1.0/1.1 cutoff (POP3/ IMAP4) for July 2026 will not break legacy clinical systems, fax-to-email gateways, scanners, MFPs, or embedded medical devices	Long-telegraphed deadline; legacy clinical estate is the typical surprise [15]
MEDIUM	Build the AI-driven memory squeeze into 2026/2027 hardware refresh plans for EHR, PACS, lab informatics, and clinical data lake	Server DRAM on track to double; SK Hynix sold out HBM/DRAM/ NAND through 2026 [13, 23]

WHAT'S CHANGED SINCE APRIL 27

- **Healthcare was named the #1 target of the AiTM "code of conduct" credential-theft campaign.** 19% of 13,000+ organizations affected, with lures spoofing the Paubox HIPAA-compliance encryption banner [35]. This is the most important sector-specific datapoint in the period.
- **Microsoft device-code phishing went industrial.** 10–15 campaigns launching every 24 hours since March 15; post-compromise activity targets finance personas; EvilTokens PhaaS in active use by Russian groups and ShinyHunters [33, 34].
- **The North Korean fake-IT-worker scheme has expanded into healthcare** per DoJ; two more US "laptop farm" hosts were sentenced to 18 months prison this week [14].
- **Edge-device cycle continued** with Palo Alto PAN-OS no-patch zero-day [7], incomplete Windows patch leaving zero-click NTLM credential theft live [8], "Dirty Frag" Linux LPE with no CVE and a public root exploit [9], and ongoing GRU TP-Link SOHO router hijacking [10].
- **The Canvas / ShinyHunters breach** showed how a critical SaaS dependency can be turned into an extortion lever via timing pressure (finals week). The healthcare analog is EHR, surgery scheduling, RCM, or PACS during an accreditation, fiscal close, or major service-line launch [12].
- **The Iran war reached operations.** IEA called the supply disruption "the largest in the history of the global oil market"; diesel, aviation, and chemistry-supply implications follow [25].

ACTIVE CAMPAIGN: HEALTHCARE WAS THE LEAD AITM TARGET

Microsoft Defender Research disclosed on May 4 a detailed analysis of a sophisticated phishing campaign that ran April 14–16 [35]. 35,000+ users across 13,000+ organizations in 26 countries, 92% US. Industry distribution: **Healthcare & life sciences 19% (highest)**, Financial services 18%, Professional services 11%, Technology & software 11% [35].

The lure pattern is built for healthcare staff.

- Emails posed as internal compliance / regulatory communications. Display names: "Internal Regulatory COC," "Workforce Communications," "Team Conduct Report." Subjects: "Internal case log issued under conduct policy," "Reminder: employer opened a non-compliance case log" [35].
- Messages claimed a "code of conduct review" had been initiated, referenced organization-specific names embedded in the text, and instructed recipients to "open the personalized attachment" to review case materials.

- A notice at the top of each message stated that the message had been "issued through an authorized internal channel" and that links and attachments had been "reviewed and approved for secure access" [35].
- **Critically for healthcare:** the end of each message contained a green banner stating that contents had been "encrypted using Paubox" — a legitimate service associated with HIPAA-compliant communications [35]. Paubox banners are common in healthcare; staff are trained to trust them.

PDF attachment names included `Awareness Case Log File – Tuesday 14th, April 2026.pdf` and `Disciplinary Action – Employee Device Handling Case.pdf`. Recipients were directed to click "Review Case Materials" inside the PDF.

The attack chain. Click → attacker domain (`acceptable-use-policy-calendly[.]de` or `compliance-protectionoutlook[.]de`) → Cloudflare CAPTCHA (gating sandboxes) → intermediate site asking users to click "Review & Sign" → email entry → image-selection CAPTCHA → "verification successful" message → final page directing user to schedule a time to discuss the case → "Sign in with Microsoft" → AiTM proxy of the real Microsoft authentication page → token capture [35]. Microsoft notes the chain "has several hallmarks of device code phishing" but they could only confirm the AiTM portion.

Why this template converts so well in healthcare.

- Healthcare staff are conditioned to take compliance, HIPAA, and code-of-conduct communications seriously. Disciplinary processes are a high-stakes, time-sensitive class of internal message.
- The Paubox banner is a recognized trust signal in clinical environments.
- PDF attachments are a common attestation / training format.
- "Review & Sign" workflows are standard for HR, ethics, and compliance attestations.

Why standard awareness training fails.

- The final destination is `microsoft.com` itself — an AiTM proxy of the legitimate Microsoft sign-in page. "Check the URL" training fails.
- AiTM attacks bypass non-phishing-resistant MFA (SMS, push, TOTP).
- AI-generated lures and platform-aware redirect chains defeat pattern-based email and URL detection.

Parallel: the Microsoft device-code phishing campaign

Separately and concurrently, Microsoft VP Tanmay Ganacharya told The Register: "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. We continue to observe high-volume activity, with hundreds of compromises occurring daily" [33]. Post-compromise activity targets finance personas with automated email exfiltration. In healthcare organizations, that maps to revenue cycle, accounts payable, contracting, accounts receivable, and finance teams handling vendor invoices and payer remittances.

EvilTokens phishing-as-a-service (sold on Telegram, plans to add Gmail and Okta) is used by Russian groups (Storm-237, UTA032, UTA0355, UNK_AcademicFlare, TA2723) and the ShinyHunters crew that took down Canvas [34]. EvilTokens lures impersonate financial documents, meeting invitations, logistics or purchase orders, payroll notices, DocuSign / SharePoint shares — all standard healthcare staff inbox content.

What works

- **Block or scope down OAuth 2.0 device-code flow** via Entra ID Conditional Access. Microsoft's explicit guidance: "only allow device code flow where absolutely necessary" [33].
- **Migrate physicians, executives, finance, revenue cycle, billing, HIM, IT/SOC admins, clinical informatics, and ethics/compliance leaders to phishing-resistant MFA** (FIDO2, passkeys, Windows Hello, Microsoft Authenticator). Disable SMS and push for these populations.
- **Enable Entra ID Protection risk-based blocking** for "Anomalous Token," "Unfamiliar sign-in properties for session cookies," and "Impossible travel" — elevate from monitor to block for high-PHI-access populations [35].
- **Defender for Office 365 hardening:** Safe Links, Safe Attachments, Zero-hour Auto Purge, network protection in Defender for Endpoint [35].
- **Targeted training** that names the Paubox-spoofing template as a healthcare-specific lure and the device-code prompt as the new phishing tell.

NORTH KOREA NOW TARGETS HEALTHCARE

Matthew Knoot (Nashville TN) and Erick Ntekereze Prince (NY) 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]. Combined: >$1.2M for Pyongyang, ~70 US companies victimized, $1.5M in audit/remediation costs.

The DoJ explicitly named healthcare as a current scheme expansion target alongside finance and professional services [14]. The scheme is now $500M+/year for Pyongyang.

For healthcare and life sciences, the implications are practical and immediate.

- Health systems with significant remote IT staffing (clinical informatics, EHR build, RCM, biomedical engineering) need rigorous identity verification.
- Life sciences and pharma R&D, which routinely hire remote technical staff for data engineering and bioinformatics, are obvious targets given the IP value.
- Telehealth and digital-health vendors have a large remote technical workforce; downstream client risk is real.

The action set.

- **ID verification beyond a video call** — government ID + biometric verification + cross-reference against the candidate's claimed location.
- **On-camera technical interviews**, not narrative interviews. Have the candidate share their screen and write code or work through architecture, not just answer questions.
- **Location-of-work attestations** with location verification — IP geolocation, MFA device geolocation, badge / access-log location. Compare claimed location to where their MFA actually authenticates.
- **No shipping company laptops to addresses you cannot tie directly to the named hire.** Period. This is the entire mechanism behind the laptop-farm convictions.
- **Audit existing remote IT contractor accounts** for telltales: travel during US off-hours, IP geolocation drift, MFA device location inconsistencies, simultaneous logins from disparate locations.

This applies to outsourced services as well as direct hires. If your RCM is offshored or your bioinformatics support is contracted, your supplier's hire process is part of your control surface.

EDGE & ENDPOINT UNDER SIEGE IN HEALTHCARE

Palo Alto PAN-OS: CVE-2026-0300, no patch yet. Memory-corruption flaw in the User-ID Authentication Portal on PA-Series and VM-Series firewalls; unauthenticated RCE as root on internet-exposed devices [7]. Unit 42 attributes ongoing exploitation to state-sponsored cluster CL-STA-1132. Attackers cleared logs, moved into Active Directory, and on April 29 forced a secondary firewall to take over and compromised that too [7]. Palo Alto firewalls are heavily deployed in healthcare at biomedical/clinical network boundaries, hospital DMZ between corporate IT and patient-care VLANs, and at multi-site MAN/WAN edges. Lock the User-ID Authentication Portal to trusted networks or disable it until a patch ships.

Windows zero-click: CVE-2026-32202. Incomplete February patch left a zero-click NTLM hash-leak live via auto-parsed LNK files [8]. CISA KEV with May 12 federal deadline. Patch clinical workstations, EHR thin/thick clients, finance/RCM workstations, and any Windows endpoint in the patient-care network promptly.

"Dirty Frag" Linux LPE. Public root exploit, no CVE, no patches; affects all major distributions [9]. Apply researcher's temporary mitigation to EHR back-ends, PACS, lab informatics, research compute, and revenue-cycle infrastructure pending vendor patches.

TP-Link SOHO routers: APT28 / GRU. DNS-hijacking 23 named TP-Link models since at least 2024 [10]. For health systems with remote clinicians (telehealth), satellite clinic networks, or home-based RCM / coding / billing staff: this is an authentication-bypass vector for the home perimeter and a direct PHI-disclosure risk. Inventory and replace; disable remote management; rotate credentials.

Exchange Online: TLS 1.0/1.1 retirement July 2026. Microsoft blocks legacy TLS for POP3 and IMAP4 [15]. Healthcare estates often contain legacy fax-to-email gateways, scanners, MFPs, lab interfaces, and embedded medical devices that may still be using the old protocols. Inventory now.

SAAS EXTORTION TIMING — THE HEALTHCARE LESSON FROM CANVAS

ShinyHunters took 6.65 TB of Canvas data covering 9,000 schools and demanded "settlement" by May 12 or threatened a public dump. Universities were forced to cancel or postpone final exams across the US [12]. The operational pressure was the point: ShinyHunters timed the threat-to-leak deadline to coincide with the moment when the institution's ability to negotiate was at its lowest.

The healthcare analog is direct and worth pre-planning for.

- **EHR (Epic, Cerner, Meditech, Athena, etc.) extortion timed to a major service-line launch, accreditation visit, or month-end billing close.**
- **Surgery / OR scheduling platform extortion timed to a peak surgical block week.**
- **RCM platform extortion timed to a payer-cycle close or quarter-end revenue recognition.**
- **PACS extortion timed to a service-line dependency window** (cardiology, oncology, radiology).
- **Clinical labs platform extortion timed to a regulatory filing deadline** (CLIA, CAP, FDA).

ShinyHunters is using device-code phishing tooling that overlaps EvilTokens [34], meaning the same actor set has both initial-access capability and the SaaS-extortion playbook.

Build the IR plan now.

- For each critical SaaS dependency, identify the operationally critical windows (accreditation, billing close, service-line launches).
- Pre-decide ransom posture as an executive decision, documented, not made under deadline pressure.
- Identify the manual / paper-based / alternate-vendor fallback for the platform. EHR downtime procedures, manual scheduling, paper charge capture — exercise these annually, not theoretically.
- Pre-draft patient and clinician communication templates.
- Coordinate with state HHS, HSCC (Health Sector Coordinating Council), HHS HC3 (Health Sector Cybersecurity Coordination Center), and your malpractice insurer.

THE IRAN WAR REACHES HEALTHCARE OPERATIONS

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]. Three exposures matter most for healthcare: diesel for backup generation, aviation fuel for medical transport, and chemistry-supply downstream pressure on lab and pharma manufacturing.

Diesel for backup generation. US gasoline at $4.52 on May 10 (+37¢ month-over-month per AAA); JP Morgan: $5/gallon “can no longer be dismissed”; Wright declined to rule it out [27]. Morgan Stanley projects US gasoline inventories will fall to ~198M barrels by late summer (lowest in modern records) [26]. Hospitals, surgery centers, and clinical-research facilities rely on contracted diesel for backup generation supporting life-safety systems, surgical cases, neonatal intensive care, dialysis, and EHR/clinical IT. Review force majeure language on diesel contracts; confirm stockpile levels are at or above policy and regulatory minimums (Joint Commission requires testing; some state regs specify minimum on-site fuel supply duration). Many multi-year hospital fuel contracts are not priced for sustained 6–12 month supply disruption — revisit pricing terms now.

Aviation fuel for medical transport. 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]. Health systems operating medical helicopter / fixed-wing transport, organ procurement networks, and patient-transport contracts on the US West Coast should plan for both price and availability pressure through Q3 2026. Lufthansa cut 20,000 short-haul flights through October citing fuel costs [28]; Ireland reportedly down to 10 days of jet fuel stock cover [26].

Chemistry-supply pressure on labs and pharma manufacturing. Sulfuric acid supply is tightening because Persian Gulf refineries and gas plants are a major sulfur source, and China imposed sulfuric acid export restrictions in May to protect its own food / fertilizer supply [30]. Sulfuric acid is upstream of pharmaceutical chemistry, lab reagent manufacturing, and clinical chemistry workflows. Naphtha (plastics, road fuel) is also rising — relevant to medical-device manufacturing and lab consumables [25, 30]. Life sciences and pharma manufacturers should be auditing chemistry-supply contracts and lab-reagent inventory now.

Marine cargo, hull, and war-risk premiums for Gulf transit are repricing. Medical device manufacturers, pharma supply chains, and lab consumable suppliers with ocean-shipping exposure should review insurance terms and qualify alternate routing.

SUPPLY CHAIN AND AI THREAT CONTEXT

Supply-chain attacks against developer tooling and SaaS.

- **JDownloader (May 6–7):** official website backdoored to deliver Python RAT loader [3]. Full reinstall and credential reset for affected endpoints; hunt the IOCs listed in immediate actions.
- **TeamPCP / Mini Shai-Hulud (April 29 onward):** SAP CAP family, intercom-client, and PyTorch Lightning npm/PyPI packages compromised; steals GitHub tokens, cloud secrets, Kubernetes tokens [4]. Healthcare ERP and analytics environments running SAP or pulling from npm/PyPI are in scope.
- **Daemon Tools / Kaspersky disclosure:** monthlong campaign with QUIC RAT targeting government, scientific, manufacturing, and retail [6].
- **PCPJack (SentinelLabs, May 8):** worm hijacking TeamPCP victims; harvests cloud credentials, SSH keys, Kubernetes tokens [5].

AI threat baseline. KnowBe4: 86% of phishing campaigns in past six months used AI [2]. Microsoft: AI lures 4.5× more effective. FBI: 2025 US cybercrime losses $20.87B, with ~$893M in AI-related fraud [2]. CrowdStrike's 2026 Global Threat Report puts AI-powered attacks up 89% year-over-year [1].

Vidar. LevelBlue documented a Vidar info-stealer campaign via fake Microsoft Toolkit hacktool [19]. Targets browser passwords, cookies, crypto wallets. Relevant to any healthcare staff who use personal devices for any work activity.

IMF systemic-risk framing. At the spring meetings, the IMF named AI-driven cyberattacks a financial-stability risk. For health-system boards, this is regulator-tier language to bring to leadership for AI security investment decisions [1].

WHAT YOU SHOULD BE DOING RIGHT NOW

This Week

1. **Hunt the AiTM "code of conduct" campaign IOCs** in EDR, email gateway, and identity logs. Healthcare was 19% of victims; the Paubox spoof was designed for healthcare conversion. Full IOC list in [35] and in the immediate-actions table.
2. **Block or scope-down Entra ID OAuth 2.0 device-code flow** via Conditional Access.
3. **Migrate physicians, executives, finance, revenue cycle, billing, HIM, IT/SOC admins, and clinical informatics leaders to phishing-resistant MFA.** Disable SMS and push for these populations.
4. **Apply the urgent patches and mitigations:** Palo Alto Captive Portal lockdown (no patch yet); Windows CVE-2026-32202; Dirty Frag Linux mitigation on EHR back-ends, PACS, lab informatics, research compute, revenue cycle.
5. **Audit JDownloader exposure** in the May 6–7 window; reinstall and rotate credentials.

6. **Refresh phishing training** specifically for the Paubox-spoofing template, the device-code prompt, calendar-invite phishing, and Teams help-desk impersonation.
7. **Tighten hire-process and remote-contractor onboarding** now that the DPRK fake-IT-worker scheme is explicitly targeting healthcare.

This Month

1. **Pre-stage IR for healthcare SaaS extortion-timing attacks** (EHR, scheduling, RCM, PACS, lab). Identify operationally critical windows; pre-decide ransom posture; exercise downtime procedures; pre-draft communications.
2. **Inventory and replace named TP-Link SOHO models** at remote clinics, satellite offices, and telehealth clinician home networks. Disable remote management; rotate router credentials.
3. **Developer-pipeline and ERP supply-chain hardening.** Pinned versions, preinstall-script monitoring, restricted GitHub repo-creation for service accounts, secrets-in-CI auditing.
4. **Iran war contingency.** Diesel-backup fuel contracts and stockpile review; West Coast aviation fuel exposure for medical transport; chemistry-supply audit for lab and pharma manufacturing; marine and war-risk insurance review for global pharma / device supply.
5. **Exchange Online TLS 1.0/1.1 inventory** ahead of July cutoff. Watch for legacy fax-to-email gateways, scanners, MFPs, lab interfaces, and embedded medical devices.
6. **2026/2027 hardware planning** under the memory-supply squeeze. EHR, PACS, lab informatics, clinical data lake, and recovery infrastructure all need fresh cost math.
7. **Use the IMF systemic-risk framing in board cyber reporting** alongside the 19% AiTM-victim statistic for healthcare. This is the language to elevate AI security investment beyond 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* (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

[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/

[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

[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/

[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

[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/

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