Executive Summary

Four new campaigns are reported this week. The most critical is a **confirmed Lynx ransomware attack on a U.S. regional hospital — with EHR and scheduling systems encrypted and patient data exfiltrated.** Also new this week: CVE-2026-38125, a critical unauthenticated RCE in Ivanti Endpoint Manager Mobile (EPMM) added to the CISA KEV catalog; a DPRK-linked spear-phishing campaign targeting healthcare and biotech researchers (CAMP.26.058) deploying the TOUCHMOVE macOS backdoor via trojanized academic PDF lures; and a WordPress plugin supply chain compromise (CAMP.26.061) affecting patient portal and appointment booking infrastructure at dozens of healthcare organizations. The dominant theme this week: ***healthcare ransomware incidents continue to spike, CISA's April 28 SharePoint deadline has now passed and compliance must be verified, and the DPRK continues to expand multi-front attacks across the healthcare and life sciences ecosystem***.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Targets	Key Technique	Priority Action
Lynx Ransomware — Regional Hospital Attack	Financial / Ransomware (RaaS)	Healthcare — US	Double extortion via Lynx RaaS; EHR and scheduling systems encrypted; patient data exfiltrated prior to encryption; uses Intermittent Encryption for speed; affiliate leveraged unpatched Citrix NetScaler as initial access	**CRITICAL — Validate EDR on all clinical endpoints; verify Citrix NetScaler patch status; confirm offline backups; exercise downtime procedures now**
Ivanti EPMM Unauthenticated RCE *CVE-2026-38125*	Vulnerability / RCE	Healthcare, Government, Tech — Global	Pre-auth RCE in Ivanti Endpoint Manager Mobile (EPMM) CVSS 9.8; exploited in wild before patch; CISA KEV added April 29; targets MDM infrastructure managing clinical mobile devices; 800+ internet-exposed EPMM instances per Shadowserver	**HIGH — Patch EPMM to 12.4.0.1 or later immediately; isolate EPMM from internet; audit mobile device management logs for unauthorized changes**
DPRK TOUCHMOVE macOS Backdoor via PDF Lures	Espionage / Financial	Healthcare, Biotech, Education — US, UK, JP, KR	DPRK-nexus (UNC4899) spear-phishes researchers with trojanized academic PDFs; macOS TOUCHMOVE backdoor deployed in-memory via Python stager; exfiltrates research data and credentials; C2 rotates via Cloudflare Workers	**HIGH — Alert on Python stager execution from PDF viewer processes; audit macOS EDR coverage for research workstations; train biomedical researchers on targeted PDF lure campaigns**
WordPress Plugin Supply Chain — Patient Portal Compromise	Financial / Supply Chain	Healthcare, SMB — US, CA, AU	Unknown actor compromised three widely-used WordPress scheduling/booking plugins; malicious update injected PHP webshell and credential-harvesting overlay; 40+ healthcare patient portals confirmed affected; harvested credentials sold on dark web	**HIGH — Audit WordPress plugin versions on all patient portal sites; remove or rollback affected plugins (HealthBook Pro, BookMe+, CareScheduler); scan for webshells; rotate credentials for any affected portals**

Top 4 Actions This Week

1. [CRITICAL] Respond to Lynx Ransomware Healthcare Targeting (CAMP.26.062)

On April 29, 2026, a U.S. regional hospital (name withheld pending disclosure) confirmed a cybersecurity incident attributed to the Lynx ransomware-as-a-service group. Lynx affiliates encrypted the hospital's EHR and patient scheduling systems and claimed exfiltration of patient records. The affiliate leveraged an unpatched Citrix NetScaler appliance as the initial access vector — consistent with INC Ransom TTPs reported in the April 10 brief, but confirmed as a distinct Lynx affiliate operation. Lynx uses Intermittent Encryption (encrypting only partial file blocks) to maximize infection speed and outrun detection windows. The group operates a double-extortion model with a

dark-web leak site. GTI confirms Healthcare as a primary targeted sector for this group, with confirmed incidents across US and EU in Q1 2026.

- Validate EDR deployment and alerting on all clinical endpoints immediately
- Verify Citrix NetScaler / ADC patch status — Citrix Bleed (CVE-2023-4966) and related appliance vulnerabilities remain the dominant initial access vector for healthcare ransomware in 2026
- Confirm offline or immutable backup integrity for EHR, PACS, and pharmacy systems. Lynx targets backup infrastructure first; air-gapped copies must be verified as restorable
- Exercise downtime procedures this week: run a tabletop or walkthrough with nursing and clinical informatics staff; identify which workflows require paper-based fallback and who authorizes the switch. Review Breach notification procedures as well.
- Review ambulance diversion and care diversion decision authority and confirm communication chain with EMS dispatch, receiving facilities, and clinical leadership is documented and current

2. [HIGH] Patch Ivanti EPMM CVE-2026-38125 — Pre-Auth RCE on Clinical MDM Infrastructure

On April 27, 2026, Ivanti disclosed CVE-2026-38125, a pre-authentication remote code execution vulnerability in Ivanti Endpoint Manager Mobile (EPMM, formerly MobileIron Core). The vulnerability carries a CVSS score of 9.8 and was exploited in the wild prior to disclosure. CISA added it to the Known Exploited Vulnerabilities catalog on April 29. Shadowserver identifies approximately 800 internet-exposed EPMM instances. For healthcare organizations, EPMM is commonly used to manage clinical mobile devices, including physician smartphones, nursing tablets, and connected bedside devices. A compromised EPMM server gives an attacker the ability to push malicious profiles to every enrolled device in the fleet, equivalent in scope to the Intune wiper scenario discussed in the March 23 brief.

- Patch Ivanti EPMM to version 12.4.0.1 or later immediately as this is a pre-auth RCE with no workaround; the only remediation is patching
- Isolate EPMM management interfaces from internet-facing networks pending patching as no MDM console should be directly internet-accessible
- Audit mobile device management logs for unauthorized profile pushes, new enrollment tokens, or configuration policy changes made in the past 30 days
- Review which clinical devices are enrolled in EPMM and confirm none have received unexpected configuration changes
- If unpatched EPMM is confirmed exposed to the internet: assume compromise, initiate IR, and audit all enrolled device profiles for unauthorized modifications

3. [HIGH] Block DPRK TOUCHMOVE macOS Backdoor — Academic PDF Lure Campaign (CAMP.26.058)

Active since April 24, 2026, a DPRK-nexus actor tracked as UNC4899 is conducting targeted spear-phishing attacks against biomedical researchers, clinical trial coordinators, and healthcare-sector academics in the US, UK, Japan, and South Korea. The campaign delivers trojanized academic PDF documents often citing real conference papers or clinical trial data that execute a Python stager when opened in macOS Preview or Adobe Acrobat. The stager deploys the TOUCHMOVE backdoor entirely in memory, communicating with C2 infrastructure hosted on Cloudflare Workers to evade domain-based blocking. TOUCHMOVE exfiltrates research files, credentials, and genomic/clinical trial data. This campaign is distinct from DPRK's prior NPM supply chain and GitHub tampering operations as it specifically targets individual researchers rather than developer infrastructure.

- Alert on Python stager processes spawned from macOS PDF viewer applications (Preview, Acrobat) as this is an anomalous parent-child process relationship that behavioral EDR should flag
- Ensure all macOS research workstations are enrolled in MDM and covered by EDR with behavioral detection as signature-based tools will not detect TOUCHMOVE's in-memory execution

- Brief biomedical researchers, clinical trial staff, and academic collaborators on this campaign specifically as targeted PDF lures are highly convincing; awareness of this active campaign is a primary defensive control
- Block outbound connections from research workstations to Cloudflare Workers subdomains that do not correspond to approved SaaS services and review proxy logs for unusual workers.dev traffic

4. [HIGH] Audit WordPress Patient Portal Plugins — Supply Chain Compromise (CAMP.26.061)

Between April 26 and April 29, 2026, an unknown threat actor compromised three widely-used WordPress plugins deployed on healthcare patient portal and appointment scheduling websites: HealthBook Pro (v3.4.1–3.4.3), BookMe+ (v5.1.0–5.1.2), and CareScheduler (v2.8.7). Malicious updates pushed to the WordPress plugin repository injected a PHP webshell and a credential-harvesting overlay that intercepted patient login submissions before displaying the legitimate portal. GTI has confirmed at least 40 healthcare organizations are affected, with stolen credentials actively being sold on dark-web marketplaces. This campaign is entirely distinct from prior NPM (Shai-Hulud, Axios) and PyPI supply chain attacks as it targets the WordPress ecosystem and directly exposes patient-facing web infrastructure.

- Immediately audit all WordPress installations hosting patient portals or appointment booking and check installed plugin versions against the affected version ranges above
- If any affected plugin versions are found: take the portal offline, remove the malicious plugin versions, scan all PHP files for webshells (look for eval/base64_decode patterns), and force-reset all patient credentials
- Review web server access logs for the past 10 days for unexpected POST requests to wp-admin paths or PHP files not in your plugin directory
- Rotate all WordPress admin credentials and database credentials on affected systems as the webshell provides persistent access even after plugin removal if credentials are not changed
- For organizations that do not use these specific plugins: audit all third-party WordPress plugins for unexpected recent updates and verify plugin integrity against the official WordPress.org repository checksums

Medical Device and IoT Security

Claroty Team82 — State of CPS Security: Healthcare Exposures 2025:

- An analysis of 2.25 million IoMT devices across 351 healthcare organizations found that 99% of HDOs have IoMT devices with confirmed KEVs, 96% carry KEVs linked to active ransomware campaigns, and 89% have ransomware-linked KEVs combined with insecure internet connectivity. Imaging systems are the highest-risk individual device category — 8% carry ransomware-linked KEVs and insecure connectivity, affecting 85% of HDOs. Healthcare organizations should use this data to reframe their IoMT remediation priority away from CVSS scores alone and toward the three-factor model: KEVs + ransomware linkage + insecure connectivity.

Medtronic Data Breach (Confirmed April 24)

- ShinyHunters claimed on April 18 to have exfiltrated over 9 million PII records and terabytes of internal corporate data from Medtronic, setting an April 21 ransom deadline; Medtronic confirmed unauthorized access to corporate IT systems via an SEC Form 8-K on April 24, stating no impact to products, patient safety, or operational networks. The company has not verified the 9 million record figure, the investigation is ongoing, and Medtronic has been removed from ShinyHunters' leak site — with no ransom payment confirmed.
- Monitor Medtronic vendor communications — if your organization uses Medtronic devices or services, watch for breach notification correspondence; PHI exposure will trigger a HIPAA 60-day notification clock if confirmed.

Activity Trends	Key Numbers This Week
▲ Healthcare ransomware (Lynx, Anubis, Medusa, Qilin): sustained critical high ▲ DPRK multi-vector targeting: GitHub, NPM, macOS, spear-phish — expanding ▲ MDM/device management infrastructure attacks: new vector (EPMM) ▲ WordPress / web supply chain compromises: emerging as healthcare vector ▲ Citrix / VPN exploitation as ransomware initial access: sustained high ▲ Vishing as initial access: #2 per M-Trends 2026 (11%) — ongoing	**CVSS 9.8 — Ivanti EPMM CVE-2026-38125 (pre-auth RCE)** 800+ EPMM instances internet-exposed (Shadowserver) 40+ healthcare patient portals affected by WordPress compromise 14 new CVEs in bedside patient monitors (Claroty ThreatBridge) 22 seconds — median access-broker handoff (M-Trends 2026) **CISA KEV deadline April 28 — SharePoint CVE-2026-32201: VERIFY NOW**

Sources: *Google Threat Intelligence (GTI), Mandiant M-Trends 2026, CISA, FDA, MITRE ATT&CK, Microsoft Security Response Center, Shadowserver Foundation, Claroty Team82 — State of CPS Security: Healthcare Exposures 2025:*