Executive Summary

Three new campaigns to be reported this week, all sourced from Google Threat Intelligence (GTI). The most critical is the China-nexus exploitation of **CVE-2026-1731 in BeyondTrust Remote Support (GLOBAL.26.004)** — a CVSS 9.9 pre-auth RCE now linked to Medusa ransomware operations by threat actor Storm-1175, with confirmed healthcare sector targeting and an EPSS score of 0.796. Also new this week: a **DPRK supply chain attack via the compromised Axios NPM package (CAMP.26.042)** hitting healthcare DevOps environments globally, and a **LOOKTOWER malvertising campaign (CAMP.26.048)** using Google Ads to deploy persistent downloaders across healthcare and technology organizations. **Ransomware pressure on healthcare remains elevated — three of this week's active campaigns directly enable or deliver ransomware against clinical environments.**

Medical Device & IoT Security: CVE-2026-3650 (GDCM DICOM Memory Leak) — no patch available, compensating controls remain in effect. Contec CMS8000 (CVE-2024-12248/CVE-2025-0626) FDA disconnect recommendation unchanged. No new medical device CVEs this week.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
BeyondTrust RCE — Storm-1175 / Medusa Ransomware (GLOBAL.26.004)	Espionage / Financial	Pre-auth OS command injection via WebSocket (CVE-2026-1731, CVSS 9.9); LOTL using curl/wget/python; deploys SNOWLIGHT, SparkRAT, VShell backdoors; PostgreSQL credential dump; ends in Medusa ransomware	Healthcare, Technology, Manufacturing — US, EU, AU, CA	CRITICAL — Patch BeyondTrust RS/PRA immediately; isolate from internet; assume compromise if unpatched before Feb 9; hunt for SparkRAT and webshells
DPRK Axios NPM Supply Chain (CAMP.26.042)	Financial / Supply Chain	Hijacked Axios NPM maintainer account publishes malicious version with PLAIN-CRYPTO-JS; SETUP.JS dropper delivers platform-specific backdoor; anti-forensic measures; registry persistence	Healthcare, Technology, Government — US, UK, AU, JP, KR, CH, FR + 6 others	HIGH — Audit Axios NPM versions immediately; pin to known-good commit hash; rotate all secrets from affected CI/CD environments; scan for SETUP.JS artifacts
LOOKTOWER Malvertising — Fake Software Installers (CAMP.26.048)	Espionage / Financial	Google Ads masquerade as legitimate software; malicious installers deploy LOOKTOWER downloader; retrieves ZIP-packaged secondary payloads; 59 domains tracked as C2/distribution infrastructure	Healthcare, Technology, Education, Energy, Manufacturing — US	HIGH — Block ad-delivered executable downloads at proxy/endpoint; alert on ZIP execution from browser download paths; review software procurement policy

Top 3 Actions This Week

1. [CRITICAL] Patch BeyondTrust CVE-2026-1731 — Storm-1175 / Medusa Ransomware (GLOBAL.26.004)

GTI confirms China-nexus threat actor Storm-1175 (EPSS 0.796, Priority P0, CISA KEV deadline Feb 16, 2026 — already past) is actively exploiting CVE-2026-1731, a pre-authentication OS command injection in BeyondTrust Remote Support and Privileged Remote Access. Post-exploitation activity includes SparkRAT/VShell backdoor deployment, PostgreSQL credential dumping, and Medusa ransomware delivery. Healthcare organizations using BeyondTrust for remote support — including clinical helpdesks, vendor access portals, and managed service provider connections — are confirmed targets.

- Patch BeyondTrust Remote Support to v25.3.2+ and Privileged Remote Access to v25.1+ immediately — this is a pre-auth RCE with no interaction required
- If unpatched before Feb 9, 2026: assume compromise — hunt for webshells in web directories, SparkRAT/VShell processes, and new domain admin accounts created after Jan 31

- Isolate BeyondTrust appliances from internet-facing exposure pending patching; firewall rule restricting inbound WebSocket connections is a viable temporary workaround
- Hunt for LOTL indicators: anomalous curl/wget/python execution from the BeyondTrust service account, /tmp directory staging, and PostgreSQL or SQLite database exports
- Review all remote support sessions since Feb 6, 2026 — check for unauthorized admin account creation and Active Directory reconnaissance activity (ADRecon tool)

2. [HIGH] Audit Axios NPM Package — DPRK Supply Chain Attack (CAMP.26.042)

Since March 30, 2026, a DPRK-nexus actor hijacked a maintainer account for the widely-used Axios HTTP library on NPM and published malicious versions containing the PLAIN-CRYPTO-JS dependency. Upon installation, the SETUP.JS dropper delivers platform-specific backdoor payloads with credential theft, arbitrary code execution, anti-forensic measures, and registry-based persistence. Healthcare organizations using Axios in EHR integrations, API clients, or clinical data pipeline tooling are at direct risk. This is distinct from the earlier PyPI campaign (CAMP.26.029) — this targets the NPM ecosystem.

- Immediately audit all projects using Axios NPM — check installed version against the known-safe pinned commit hash; any version published between March 30 and April 6 should be treated as suspect
- Check npm audit logs and package-lock.json files for unexpected PLAIN-CRYPTO-JS dependency additions
- Rotate all secrets, tokens, and credentials accessible from any environment where the compromised Axios version may have been installed — including cloud API keys, EHR integration tokens, and CI/CD pipeline credentials
- Scan developer workstations and build servers for SETUP.JS artifacts, unexpected registry run keys, and anomalous outbound connections

3. [HIGH] Block LOOKTOWER Malvertising — Fake Software Installer Campaign (CAMP.26.048)

Active since January 7, 2026 and confirmed through April 9, an unknown actor is using Google Ads to serve convincing fake software installer pages. When users download and execute these installers, a downloader deploys LOOKTOWER, which retrieves ZIP-archived secondary payloads from C2 infrastructure. The campaign has 59 confirmed C2/distribution domains and targets Healthcare, Technology, Education, Energy, and Manufacturing in the US. The technique mirrors prior AI-lure campaigns (CAMP.26.032/CAMP.26.048) but uses a broader software category lure set.

- Block executable file downloads (.exe, .msi, .zip containing executables) originating from ad-served URLs at your web proxy or endpoint — flag any installer downloads where the referring page is a Google Ad
- Alert on ZIP archive extraction followed immediately by executable launch from browser download directories
- Review and enforce software procurement policy: all software installations should originate from verified vendor portals or an approved internal repository, never from search ad results
- Train staff to recognize that sponsored search results are a primary malware delivery vector in 2026 — reinforce this specifically for IT and clinical engineering staff who frequently download tools

Medical Device and IoT Security

Status Update — No New CVEs This Week

CVE-2026-3650 (GDCM DICOM): No patch available as of April 17, 2026. CISA ICSMA-26-083-01 remains open. Continue network segmentation of PACS/imaging systems and monitor vendor communications.

Contec CMS8000 / Epsimed MN-120 (CVE-2024-12248, CVE-2025-0626): GTI EPSS score 0.0068 — no known active exploitation as of April 17. FDA disconnect recommendation remains in force. Texas HHSC April 17 agency reporting deadline is today — Texas-based facilities should confirm submission.

BeyondTrust (CVE-2026-1731) and IoMT: Healthcare organizations using BeyondTrust for vendor remote access to medical devices and clinical systems should treat this as a medical device security issue, not only an IT issue. Remote access tools used for medical device maintenance are a primary exploitation vector — all vendor remote sessions should be logged, time-limited, and reviewed for anomalous activity following this week's disclosure.

Activity Trends

- ▲ China-nexus RCE exploitation: CRITICAL escalation
- ▲ DPRK NPM/supply chain attacks: +2 active campaigns
- ▲ Ransomware-enabling campaigns: 3 active this week
- ▲ Malvertising / fake installer lures: sustained vector
- ▲ Iran-nexus wiper posture: sustained, no new incidents

Cumulative IOC Count: 450+ (new this week)

File hashes: 10+ (new)
IP addresses: 47+ (new)
Domains: 59+ (new, led by LOOKTOWER)
URLs: 25+ (new)
CVE-2026-1731: EPSS 0.796, P0, CISA KEV

Sources: Google Threat Intelligence (GTI), CISA, FDA, MITRE ATT&CK, RSAC 2026, Health-ISAC, Cybersecurity Dive

Report suspicious activity to your IT security team immediately