Executive Summary

This edition covers active threat campaigns relevant to Healthcare and Technology sectors. One new campaign to be reported this week. **The most critical ongoing threat remains the Iran-nexus Handala/UNC5203 wiper activity following the March 11 Stryker attack — healthcare and technology organizations should treat Iran-linked threats as severely elevated while U.S.-Iran tensions persist.**

Note: This edition adds a new standing section — **Medical Device & IoT Security** covering threats specific to connected clinical devices, and FDA/CISA medical device advisories. The Regulatory and Compliance section is also in this edition but will be added ad-hoc as needed.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
Amatera AI-Lure Infostealer (CAMP.26.032)	Credential Theft / Espionage	Fake AI tool install pages (InstallFix/ClickFix); deploys Amatera MaaS stealer via mshta.exe; harvests browser creds, cookies, session tokens	Healthcare, Tech, IFinance — US, EU, AU	HIGH — Block mshta.exe execution in non-dev envs; alert on sponsored search ads for AI tools; train developers on download verification

Top Action This Week

[HIGH] 1. Block Amatera AI-Lure Infostealer (CAMP.26.032) — Developer Credential Theft

Active through at least March 31, 2026, this campaign uses sponsored Google and Bing search results to serve pixel-perfect fake installation pages for popular AI developer tools — including Claude Code, OpenClaw, and Doubao. On Windows, execution of the fake install command deploys Amatera Stealer via mshta.exe; on macOS, a base64-obfuscated script delivers AMOS. Both steal browser-stored credentials, session cookies, crypto wallets, and system metadata. For healthcare organizations, compromised developer credentials can directly expose EHR API integrations, cloud-hosted clinical data, and medical device management platforms.

- Block or alert on mshta.exe execution in any environment where it is not a standard tool
- Deploy DNS filtering to block known Amatera C2: 144.124.235.102 and associated CDN-hosted infrastructure
- Train developers: verify all AI tool downloads go to official vendor domains (anthropic.com for Claude Code); do not trust search ads
- Review browser-stored credentials on developer workstations; rotate any credentials that may have been exposed
- Enforce endpoint detection coverage on both Windows and macOS developer endpoints

Medical Device and IoT Security

Connected medical devices represent one of the most rapidly growing attack surfaces in healthcare. Industry research shows that 53% of connected medical devices in hospitals carry known critical vulnerabilities, and 89% of healthcare organizations have high-risk IoMT devices with active CISA KEVs and insecure internet connections on their networks.

CISA MEDICAL DEVICE ALERT: CVE-2026-3650 — Grassroots DICOM (GDCM) Memory Leak

Severity: HIGH (CVSS v3.1: 7.5 | CVSS v4.0: 8.7) | No Patch Available | Reported: March 26-27, 2026

CISA issued ICS Medical Advisory ICSMA-26-083-01 on March 26, 2026 for a memory leak vulnerability in the Grassroots DICOM (GDCM) open-source library (version 3.2.2). A maliciously crafted DICOM file of just ~150 bytes can cause the affected system to allocate up to 4.2 GB of memory without releasing it, triggering a full denial-of-service condition. Grassroots DICOM has not responded to CISA remediation requests — no patch is currently available.

WHO IS AFFECTED: Any hospital, radiology department, or clinical facility using PACS servers, imaging workstations, DICOM viewers, or research tools (including 3D Slicer, surgical planning tools) built on GDCM. Affected vendors include products from Dentsply Sirona and Zimmer Biomet. GDCM runs on thousands of clinical systems, often without administrator awareness.

PATIENT SAFETY RISK: Imaging system denial-of-service can delay critical diagnosis (radiology, cardiology). Researchers note the attack can also serve as a diversion — crashing imaging systems to draw attention while a separate intrusion occurs elsewhere on the hospital network.

Immediate Actions for CVE-2026-3650

- Inventory all PACS servers, DICOM viewers, radiology workstations, and surgical planning tools — identify any using GDCM version 3.2.2
- Apply network segmentation to imaging systems — restrict DICOM file ingestion to trusted, authenticated sources only
- Block inbound DICOM files from unauthenticated external sources at the network perimeter
- Implement file integrity monitoring on DICOM-processing systems to detect unexpected resource consumption
- Prepare clinical downtime procedures for imaging systems — know your manual workflow if PACS goes offline
- Contact your PACS, imaging workstation, and surgical planning software vendors to determine if their product uses GDCM and request patching timelines
- Monitor the CISA ICSMA-26-083-01 advisory page for patch availability

Broader IoMT Risk Context

Healthcare organizations should be aware of the following systemic IoMT risk factors, which elevate the impact of every campaign in this brief:

- 52% of IoMT devices run on Windows, but only 10% have active anti-malware protection (Forescout/Censinet, 2026)
- Authentication failures and code defects account for 59.8% of all medical device security flaws — default credentials and hardcoded passwords remain the primary entry points
- Legacy DICOM systems frequently run on unsupported OS versions and lack encrypted transport, making them trivially exploitable by actors such as Handala/UNC5203
- Vendor remote access for medical device maintenance commonly bypasses standard security controls — all vendor remote access sessions should be logged, time-limited, and monitored
- FDA now requires manufacturers submitting new devices to include cybersecurity lifecycle plans — for legacy devices, hospitals should request SBOMs (Software Bills of Materials) from vendors

Recommended IoMT Security Baseline

- Maintain a complete, current inventory of all connected medical devices on your network (device type, OS version, patch level, network segment)
- Segment medical devices onto a dedicated, monitored VLAN with least-privilege firewall rules — no direct clinical device-to-internet connectivity
- Enroll all manageable medical devices in your MDM or device management platform
- Participate in Health-ISAC and CISA's HC3 intelligence sharing programs to receive device-specific threat notifications
- Subscribe to CISA ICS Medical Advisories (ICSMA) at cisa.gov/news-events/ics-medical-advisories for ongoing device-specific vulnerability notifications

Regulatory and Compliance Update

CIRCIA Rulemaking — Healthcare Town Hall (March 17, 2026)

CISA hosted a CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act) town hall session for the Healthcare and Public Health sector on March 17, 2026. The rulemaking is expected to be finalized by May 2026, though timeline slippage is anticipated. Healthcare organizations should begin preparing for mandatory cyber

incident reporting workflows now, including identifying who will be responsible for CIRCIA submissions and establishing what constitutes a 'substantial' reportable incident under HIPAA + CIRCIA alignment requirements.

FDA Medical Device Cybersecurity Guidance — Updated Requirements

FDA has tightened medical device cybersecurity guidance for premarket submissions, now requiring manufacturers to demonstrate security considerations throughout the entire product lifecycle, including postmarket vulnerability monitoring and patching protocols. Notably, FDA has introduced a risk framework distinguishing 'controlled risk' (security flaw exists but patient harm is low) from 'uncontrolled risk' (security issue poses significant patient safety or data risk). Healthcare organizations should request updated security risk assessments from all medical device vendors against this new framework — and should specifically ask whether any currently-deployed devices would fail the new FDA standard.

HIPAA Security Rule Update

OCR is moving to finalize an updated HIPAA Security Rule in 2026, expected to make ongoing, system-level risk analysis a baseline requirement rather than a periodic task. Organizations should begin treating continuous monitoring as a compliance expectation, not just a best practice. The new rule will likely increase scrutiny of IoMT device inventory, medical device risk assessments, and third-party vendor access controls.

Threat Metrics

Activity Trends

▲ Iran-nexus wiper ops: sustained high threat
▲ AI-lure credential theft campaigns: +60% vs. prior
▲ Developer/supply chain attacks: +40% vs. prior
▼ Ransomware incidents: -12% vs. prior week
▲ Medical device CVEs: 27 new KEV additions (Feb–Mar)

Cumulative IOC Count: : 230+ (new this week)

File hashes: 72+
IP addresses: 8+
Domains: 24+ (incl. CDN-hosted Amatera infrastructure)
URLs: 49+