



Executive Summary

Three GTI-verified campaigns are reported this week, sourced from Google Threat Intelligence (GTIG). The most critical is **CAMP.26.081**, a Russia-nexus actor conducting AI-assisted cloud-native intrusions targeting **AWS, Azure, and Bitbucket environments — actively targeting Healthcare, Pharmaceuticals, and Technology** as recently as June 11, 2026. Also new: **CAMP.26.080**, a financially motivated actor deploying malicious LNK payloads via fake browser update lures (first observed June 1), and a newly disclosed medical device vulnerability, **CVE-2026-0611**, an unauthenticated RCE (CVSS 9.8) in Spacelabs Healthcare Cardiac monitoring software.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
Russia-Nexus Cloud Intrusion — Slack C2 + AI-Assisted (CAMP.26.081)	Espionage / Financial	Multi-vector cloud-native intrusion via compromised third-party credentials; AWS Lambda reconfiguration; privilege escalation; Slack used as C2; AI-assisted scripting for reconnaissance; targets AWS, Azure, Bitbucket	Healthcare, Pharma, Manufacturing, Tech — US (active as of June 11, 2026)	CRITICAL — Audit third-party cloud credentials; rotate AWS/Azure tokens; monitor Slack for anomalous API calls; enable CloudTrail and Defender for Cloud alerting
Fake Browser Update / Malicious LNK Payloads (CAMP.26.080)	Financial / Malware Delivery	Deceptive websites mimic Chrome update pages; user downloads weaponized ZIP with malicious LNK; LotL string-concatenation spawns hidden PowerShell; in-memory secondary payload; scheduled task persistence with SYSTEM privileges; C2 via randomized staging infrastructure	Financial, Manufacturing, Media, Retail — US, Belgium (first seen June 1, 2026)	HIGH — Block LNK execution from ZIP/browser downloads; alert on PowerShell spawning hidden processes; enforce AppLocker; train users to verify software update sources
Spacelabs Sentinel Cardiac Monitor RCE — CVE-2026-0611 (Medical Device)	Vulnerability / Medical Device RCE	Unauthenticated RCE via deprecated .NET Remoting HTTP channel on port 8989 in Spacelabs Healthcare Sentinel v10.5.x–11.5.x; attacker writes ASPX webshell to IIS wwwroot; exploits if port 8989 is network-accessible; CVSS 9.8; CISA ICSMA advisory; affects Sentinel cardiac monitoring and connectivity software	Healthcare — Cardiac monitoring & connectivity environments globally (Dentsply Sirona, Zimmer Biomet also impacted)	HIGH — Upgrade to Sentinel v11.6.0+; disable or firewall port 8989 from network access; verify IIS wwwroot for unexpected ASPX files; treat as OT/IoMT asset requiring clinical continuity planning

[CRITICAL] Harden Cloud Credential Controls — Russia-Nexus AI-Assisted Cloud Intrusion (CAMP.26.081)

GTIG's most recent campaign intelligence, with activity confirmed as recently as June 11, 2026, tracks **CAMP.26.081** — a Russia-nexus financially motivated actor conducting multi-vector cloud-native intrusions against AWS, Azure, and Bitbucket environments. The actor gains initial access by exploiting compromised third-party credentials, then performs API-driven reconnaissance and escalates privileges by reconfiguring AWS Lambda functions to assume higher-privileged execution roles. Uniquely, this actor uses Slack as a command-and-control channel — blending malicious traffic into legitimate enterprise communication flows — and employs AI tools to automate scripting and accelerate reconnaissance. GTI confirms active targeting of Healthcare, Pharmaceuticals, Manufacturing, and Technology organizations in the US.

This campaign is a direct threat to healthcare organizations that rely on cloud-hosted EHR integrations, clinical data warehouses, and third-party health IT vendors with shared cloud



infrastructure. The use of Slack C2 means traditional network-based C2 detection will miss activity unless Slack API audit logging is explicitly monitored.

- Immediately audit all third-party vendor credentials with access to your AWS, Azure, and Bitbucket environments — rotate any that have not been rotated in the past 90 days or that lack MFA enrollment
- Enable CloudTrail (AWS) and Azure Monitor / Defender for Cloud audit logs; alert on Lambda function policy changes, IAM role assumption anomalies, and privilege escalation events
- Audit Slack workspace OAuth applications and bot tokens — review for unauthorized API access patterns; Slack Enterprise Grid organizations should enable DLP and API activity logging
- Healthcare-specific: third-party health IT vendors with cloud access to your environment (EHR integrators, clinical analytics platforms, cloud imaging vendors) are a primary attack surface — require attestation of MFA enforcement and credential rotation logs from all cloud-connected BAs
- Implement just-in-time access for AWS Lambda execution roles and Bitbucket CI/CD service accounts — remove standing elevated permissions

[HIGH] Block Malicious LNK + Fake Browser Update Lures (CAMP.26.080)

Beginning June 1, 2026, GTIG has tracked CAMP.26.080 — a financially motivated actor distributing malicious LNK files through websites that convincingly impersonate Google Chrome update pages. When a user visits one of these sites, they are prompted to download a ZIP archive containing a weaponized Windows shortcut (LNK) file. On execution, the LNK file leverages living-off-the-land techniques — using native string concatenation and filtering utilities — to spawn a hidden PowerShell process that evades basic command-line monitoring. That hidden process assembles download URLs using character-encoded arrays, pulls down in-memory script blocks from C2 infrastructure, profiles the local system, and downloads a final executable payload that installs itself with a scheduled task configured to run with SYSTEM privileges on every user login.

GTI records 22 IOCs for this campaign (13 malicious files, 7 domains, 1 IP, 1 URL) with confirmed targeting in the United States and Belgium. While the campaign's confirmed targeted industries are Financial Services, Manufacturing, Media, and Retail, the fake browser update delivery method is industry-agnostic and has repeatedly been observed as a precursor to healthcare-sector ransomware intrusions. The 22-second median access-broker handoff documented in M-Trends 2026 remains operative — any fake update lure detection should be treated as imminent-ransomware.

- Configure AppLocker or WDAC to block LNK file execution from user download directories and ZIP extraction paths — this is the single highest-leverage control against this delivery chain
- Alert on PowerShell processes spawned with hidden window flags (-WindowStyle Hidden) or with obfuscated encoded command arguments from non-standard parent processes
- Deploy web content filtering to block lookalike browser update pages — verify Chrome/Edge update mechanisms enforce only Google/Microsoft delivery (e.g., via enterprise update policies)
- Train clinical and administrative staff to recognize browser update lures — genuine browser updates are delivered silently through the browser itself, never via a website download prompt

**[HIGH] Patch or Firewall Spacelabs Sentinel Cardiac Monitor — CVE-2026-0611 (CVSS 9.8)**

CVE-2026-0611, disclosed May 29, 2026 and cataloged by CISA, is an unauthenticated remote code execution vulnerability in Spacelabs Healthcare Sentinel versions 10.5.x through 11.5.x — software used for cardiac monitoring connectivity and telemetry integration in hospitals and ambulatory care settings. The flaw stems from a deprecated .NET Remoting HTTP channel exposed on port 8989. An unauthenticated attacker who can reach that port over the network can write arbitrary ASPX webshell files to the IIS web root directory, achieving full unauthenticated RCE with the privileges of the IIS application pool. CVSS base score is 9.8; the CISA ICSMA advisory notes the vulnerability affects OT/IoMT systems. A patch is available: Sentinel version 11.6.0.

Critical context: the vulnerability is only exploitable if port 8989 has been explicitly made network-accessible through deliberate configuration or network policy changes. However, in clinical environments where default configurations are sometimes overridden for vendor remote access or integration purposes, this is a real risk. No active exploitation has been confirmed as of June 12, 2026, but the unauthenticated attack path and CVSS 9.8 score make this a high-priority remediation target.

- Upgrade all Spacelabs Healthcare Sentinel installations to version 11.6.0 — contact Spacelabs or your biomedical engineering vendor for patch deployment guidance
- As an immediate compensating control: verify that port 8989 is not accessible from any network segment other than the dedicated biomedical device VLAN or vendor-managed access zone — implement firewall rules to block external access if upgrade has not yet occurred
- Inspect the IIS wwwroot directories of all Spacelabs Sentinel servers for unexpected .aspx or .asmx files that could indicate prior exploitation
- Engage your biomedical engineering team to validate that no other .NET Remoting channels are exposed on Spacelabs or similarly architected clinical monitoring systems
- Document this CVE in your IoMT risk register and flag to your HIPAA Security Rule risk analysis — an unpatched RCE in cardiac monitoring infrastructure is a direct ePHI and patient safety risk

Medical Device and IoT Security

New Medical Device CVE This Week:

CVE-2026-0611 (Spacelabs Healthcare Sentinel — Unauthenticated RCE via .NET Remoting): Disclosed May 29, 2026. CVSS 9.8 (v3.1). Affects Sentinel versions 10.5.x and higher through 11.5.x. Patch: upgrade to v11.6.0. CISA ICSMA advisory issued. No active exploitation confirmed. Compensating control: firewall port 8989 immediately. Full detail in Top 3 Actions above.

Persistent Medical Device Status Updates:

- CVE-2026-3650 (GDCM DICOM Memory Leak): No patch available as of June 12, 2026. CISA ICSMA-26-083-01 remains open — now week 11 of the open advisory. Continue network segmentation of PACS and imaging systems; block unauthenticated DICOM file ingestion; monitor imaging workstations for resource exhaustion anomalies. Vendor (Grassroots DICOM) has not responded to CISA.



- Contec CMS8000 / Epsimed MN-120 (CVE-2024-12248, CVE-2025-0626): GTI EPSS 0.0068 — no known active exploitation as of June 12. FDA disconnect recommendation remains in force. Do not connect these devices to networks without compensating controls.
- BeyondTrust CVE-2026-1731: CISA KEV deadline (Feb 16) has long passed. Confirm patching is complete across all BeyondTrust RS and PRA platforms used for medical device vendor remote maintenance access. Any unpatched appliance should be treated as potentially compromised.

IoMT Risk Context:

The Spacelabs Sentinel vulnerability (CVE-2026-0611) is a reminder that clinical monitoring infrastructure carries the same vulnerability lifecycle risks as enterprise IT — and often with slower patch adoption cycles. Organizations should apply the CISA/RSAC 2026 IoMT Exploitability Management Framework: prioritize CVEs by EPSS score and KEV status, not CVSS alone, and focus on making unpatchable devices unexploitable through network isolation and traffic inspection rather than waiting for vendor patches.

Activity Trends	Key Numbers This Week
▲ Russia-nexus AI-assisted cloud intrusion: escalating — active June 11, 2026 ▲ Fake browser update lures: persistent, industry-agnostic delivery vector ▲ Medical device / IoMT RCE vulnerabilities: new CVE-2026-0611 joins persistent GDCM CVE-2026-3650 ▲ Ransomware healthcare targeting: sustained — Lynx, SPHINXLOCKER, INC Ransom remain active ▲ Vishing / social engineering of IT help desks: active UNC3944 activity ▼ Email phishing as primary initial access vector: continued decline (M-Trends 2026)	3 New GTI-verified campaigns this week CAMP.26.081 last seen: June 11, 2026 (Russia-nexus cloud) CAMP.26.080 first seen: June 1, 2026 (LNK lure) CVE-2026-0611 CVSS 9.8 — Spacelabs Sentinel RCE (patch: v11.6.0) CVE-2026-3650 (GDCM): NO PATCH — week 11 of open advisory HIPAA 90 FR 800: UNFINALIZED — May 2026 window passed with no final rule 22 seconds — median access-broker-to-ransomware handoff (M-Trends 2026, still operative)

Sources: Google Threat Intelligence (GTI / GTIG), CISA, CISA ICSMA advisories, National Vulnerability Database (NVD), Spacelabs Healthcare Security Advisory 079-0273-00, MITRE ATT&CK, Mandiant M-Trends 2026, OCR / HHS Regulatory Agenda, HIPAA Journal (June 2026), Medcurity (June 2026), Alston & Bird (Nov 2025)