



Executive Summary

One new GTI-verified campaign and one major multinational advisory anchor this week. The most significant development is joint Cybersecurity Advisory AA26-194A, released July 13, 2026 by the NSA, CISA, FBI, and DC3 with international partners (19 allied agencies in total): Russian FSB Center 16 cyber actors are exploiting poorly configured and vulnerable networking devices worldwide, opportunistically compromising critical infrastructure networks — and Healthcare and Public Health is explicitly named among the six sectors most at risk. The tradecraft is unglamorous and highly effective: scanning for internet-exposed routers with weak or default credentials, abusing SNMP with default community strings to pull configuration files and credentials, and exploiting Cisco Smart Install and known Cisco CVEs. Because most of the exploited weaknesses are configuration-based rather than unpatched software, router hygiene audits alone meaningfully reduce exposure.

The GTI campaign, CAMP.26.095 (intelligence released July 14), closes the loop on a story this series has tracked since July 3: the FLUTECLICK web-compromise reconnaissance chain has now been observed completing its full lifecycle — ClickFix lures on compromised websites, in-memory FLUTECLICK/CORNFLAKE deployment with Node.js persistence, handoff to the RHYSIDA-linked group, offline extraction of Active Directory ntds.dit via virtual disk snapshot cloning to evade EDR, and final deployment of INTERLOCK ransomware with data extortion. GTI confirms Government targeting; healthcare is not yet confirmed for this campaign, but it is the direct continuation of the healthcare-confirmed CAMP.26.092, and INTERLOCK is the group behind the Kettering Health breach (1.69M individuals).

The vendor-side pressure showed up in-window: on July 16, Abbott disclosed a cyber incident involving unauthorized access to a limited number of internal systems in its Cancer Diagnostics business (which includes the recently acquired Exact Sciences), alongside a second, apparently unrelated claimed intrusion at its LabCentral laboratory portal — details in the incident section below. Medical Device: no new CISA medical advisory this week; the three open DICOM library advisories carry forward (GDCM enters week 17 without a patch). Regulatory: the HIPAA Security Rule delay to at least July 2027 (reported in the July 10 brief) is re-verified and unchanged.

Active Threat Campaigns- Healthcare & Technology

Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
Russian FSB Center 16 — Networking Device Exploitation (Joint CSA AA26-194A, July 13)	Nation-State / Espionage (Russia — FSB Center 16)	Scanning for internet-exposed routers and networking devices that are unpatched, misconfigured, or using weak/default credentials; abuse of SNMP with default or common community strings to pull device configuration files and harvest credentials; exploitation of Cisco Smart Install and known Cisco CVEs; exfiltration of configurations to actor-controlled infrastructure; opportunistic compromises confirmed across multiple critical infrastructure sectors; decade-plus activity, expanded TTPs published July 13, 2026	Healthcare and Public Health explicitly named among six most-at-risk sectors, alongside communications, defense industrial base, energy, financial services, government — US + allied nations	CRITICAL — Audit every internet-exposed router/edge device now; disable SNMP v1/v2 or replace default community strings; disable Cisco Smart Install; patch known Cisco CVEs; hunt for unauthorized config pulls per AA26-194A TTPs
ClickFix → FLUTECLICK/CORNFLAKE → INTERLOCK Ransomware Chain (CAMP.26.095)	Financial / Ransomware + Data Extortion	Compromised legitimate websites host ClickFix lures (fake CAPTCHAs/system updates) driving obfuscated PowerShell execution; in-memory deployment of the FLUTECLICK JavaScript profiler and CORNFLAKE JavaScript backdoor with	GTI-confirmed: Government — US. Healthcare NOT yet GTI-confirmed; included as the direct completion of	HIGH — Treat any FLUTECLICK/CORNFLAKE/ClickFix detection as a Priority-1 pre-ransomware incident; alert on VM snapshot mounting and offline ntds.dit access; alert on unexpected Node.js



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
		persistence via local Node.js environments and scheduled tasks; handoff to a financially motivated group with historical RHYSIDA ties; recon via native admin tools and port scanners for domain controllers and hypervisors; snapshot mounting to clone virtual disks and extract Active Directory ntds.dit offline (EDR evasion); credential harvesting, event log purging, INTERLOCK ransomware deployment with multifaceted data extortion; active June 3–30, 2026, intelligence released July 14	the healthcare-confirmed CAMP.26.092 FLUTECLICK chain (July 3 brief), ending in INTERLOCK — the group behind the 1.69M-record Kettering Health breach	runtimes; monitor event-log clearing

Top 2 Priority Actions This Week

1. [CRITICAL] Audit Network Edge Devices Against FSB Center 16 Targeting (AA26-194A)

On July 13, 2026, the NSA — joined by CISA, FBI, DC3, and international partners including the UK NCSC, Australia's ACSC, and Canada's Cyber Centre (19 agencies in total) — released joint advisory AA26-194A, 'Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting.' It attributes a decade-plus of ongoing activity to Russian FSB Center 16 and documents opportunistic compromises across multiple critical infrastructure sectors, with Healthcare and Public Health explicitly listed among the six sectors most at risk. The actors scan for internet-exposed routers and networking devices that are unpatched, misconfigured, or protected by weak or default administrative credentials; abuse SNMP agents configured with default or common community strings to pull device configuration files and harvest credentials; and have exploited Cisco Smart Install and known Cisco CVEs. Exfiltrated configurations flow to actor-controlled infrastructure and enable deeper pivots. For hospitals, a compromised perimeter or clinical-edge router can expose authentication infrastructure and provide a path toward clinical and medical device VLANs. The advisory maps activity to MITRE ATT&CK v19 and stresses that most of the exploited weaknesses are configuration-based — meaning remediation is largely within reach of routine maintenance, not emergency patching.

- Inventory every internet-exposed router, switch, and edge device — including branch clinics, imaging centers, and vendor-managed circuits — and verify firmware currency
- Disable SNMP v1/v2c where possible; where SNMP is required, eliminate default/common community strings and restrict SNMP to management networks
- Disable Cisco Smart Install on all Cisco devices and confirm known exploited Cisco CVEs are patched
- Replace default and shared administrative credentials on all network devices; require MFA on device management planes
- Hunt retrospectively using the AA26-194A TTP appendices: unauthorized configuration pulls, TFTP/FTP config transfers to unknown hosts, and logins to device management interfaces from unexpected sources

2. [HIGH] Detect the Full ClickFix → FLUTECLICK/CORNFLAKE → INTERLOCK Kill Chain (CAMP.26.095)

GTI released intelligence on July 14 documenting the completed lifecycle of the FLUTECLICK operation first covered in the July 3 brief. The chain: compromised legitimate websites host ClickFix lures (fake CAPTCHA and system-update prompts) that trick users into executing obfuscated PowerShell; the FLUTECLICK JavaScript profiler and, subsequently, the CORNFLAKE JavaScript backdoor deploy in memory, persisting through local Node.js environments and scheduled tasks; access is handed off to a financially motivated group with historical RHYSIDA ransomware ties; the



post-handoff actor performs rapid reconnaissance with native admin tools and port scanners to locate domain controllers and hypervisors; and — notably — rather than touching the domain controller directly, the actor mounts virtual disk snapshots to clone and extract the Active Directory ntds.dit database offline, evading EDR entirely. The operation culminates in credential harvesting, event log purging, and INTERLOCK ransomware deployment with multifaceted data extortion. Activity ran June 3–30, 2026 against US organizations; GTI confirms Government targeting. Healthcare is not yet GTI-confirmed for this campaign, but the lineage matters: CAMP.26.092 (healthcare-confirmed) is the front half of this same operation, and INTERLOCK carried out the Kettering Health attack that exposed 1,695,382 individuals' records — every hospital security team should treat this kill chain as directly applicable.

- Escalate any FLUTECLICK, CORNFLAKE, or ClickFix detection to Priority-1 incident handling — this campaign proves the handoff ends in ransomware, not just profiling
- Alert on VM snapshot creation/mounting outside backup windows and on any offline access to ntds.dit or volume shadow copies of domain controllers — the EDR-evasion step is itself detectable at the hypervisor layer
- Alert on unexpected Node.js runtime installation or execution on endpoints where Node is not a sanctioned tool
- Treat event-log clearing (Security log 1102) as a high-fidelity signal requiring immediate response
- Ingest the 22 GTI-verified domains into web filtering and SIEM watchlists; re-verify the July 3 CAMP.26.092 controls (WordPress scanning, .xyz/.lol blocking) are in place

Medical Device and IoT Security

No New Medical Device Advisories This Week

CISA published no new ICS Medical Advisory during the July 11–17 window — the most recent remains ICSMA-26-181-01 (OFFIS DCMTK, June 30), covered in the July 10 brief. The standing priority is unchanged: three open-source DICOM library advisories remain open simultaneously, and DCMTK is the only one with a patch path — completing DCMTK remediation (standalone installs plus vendor-embedded copies) is the fastest available risk reduction in the imaging ingestion chain. GDCM (CVE-2026-3650) enters week 17 without a patch and pydicom/pynetdicom (CVE-2026-56445) remains without a vendor fix; the shared compensating controls — blocking DICOM ingestion from unauthenticated sources, imaging network segmentation, and boundary file validation — cover all three. Additionally, the FSB Center 16 advisory (Action 1) has a direct medical device dimension: compromised edge routers are a documented pivot path into clinical and medical device VLANs, making router hygiene a medical-device-security control, not just an IT one. The persistent CVE tracker from last week stays and is not repeated in this week's threat brief. Please refer to the July 10th brief.

Major Incident Development — Abbott Cancer Diagnostics Cyberattack

On Thursday, July 16, 2026, Abbott disclosed in a statement on its website that a cyber incident resulted in unauthorized access to a limited number of internal systems in its Cancer Diagnostics business — the unit that includes Exact Sciences, acquired by Abbott in a \$21 billion deal earlier this year. Abbott states there is no impact on business operations, product availability, manufacturing or lab operations, or its ability to serve patients; that no other Abbott businesses, sites, or systems were affected; and that the legacy Exact Sciences systems are separate from Abbott's. The company has engaged third-party cybersecurity experts and law enforcement, is still investigating what information was accessed, and does not currently expect a material impact on business or financial results. It has not disclosed what type of information was accessed or when the intrusion was discovered.

HIPAA Security Rule Regulatory Update: 90 FR 800 — Re-verified: Final Action Remains Delayed to At Least July 2027.

Refer to July 10th brief for a note on this topic.



Threat Metrics

Activity Trends	Key Numbers This Week
▲ Nation-state targeting of network edge devices: CRITICAL — FSB Center 16, healthcare named at-risk (AA26-194A) ▲ Healthcare ransomware H1 2026: +14% vs H2 2025 (Comparitech) — 2.3 attacks/day ▲ Attacks on healthcare businesses/vendors: +35% vs H2 2025 — outpacing provider attacks (+3%) ▲ ClickFix-to-ransomware completion: FLUTECLICK recon (July 3 brief) now confirmed ending in INTERLOCK deployment ▲ Medtech vendor incident disclosures: Abbott (July 16) joins Stryker, Intuitive, Medtronic, iRhythm, AdaptHealth in recent months ► Medical device advisories: no new ICSMA this week; three DICOM library advisories remain open ► HIPAA Security Rule: July 2027 delay re-verified — unchanged	410 healthcare ransomware attacks in H1 2026 (247 providers / 163 businesses) — Comparitech Top strains claiming healthcare victims H1 2026: DragonForce (14), The Gentlemen (13), INC (12), Qilin (10) Median ransom demand: \$310K (providers) / \$300K (healthcare businesses) 22 new GTI-verified IOCs (CAMP.26.095) 2 apparently unrelated cyber incidents under investigation at Abbott (Cancer Diagnostics + LabCentral); extortion claims unverified 19 allied agencies co-sealed AA26-194A (July 13) CVE-2026-3650 (GDCM): NO PATCH — week 17; CVE-2026-56445 (pynetdicom): NO PATCH

Source: Google Threat Intelligence (GTI), NSA / CISA / FBI / DC3 Joint Cybersecurity Advisory AA26-194A (cisa.gov), UK NCSC, CISA ICS Medical Advisories (ICSMA-26-181-01; -176-01; -083-01), Abbott Newsroom (official statement), Cybersecurity Dive / MedTech Dive, Reuters, Cybernews, DataBreaches.net, SC Media, Comparitech H1 2026 Healthcare Ransomware Roundup, TechTarget HealthTech Security, HIPAA Journal, GovInfoSecurity (ISMG), Davis Wright Tremaine, Clearwater, BleepingComputer