



Executive Summary

The most consequential item this week is a threat to staff who travel. GTI campaign CAMP.26.107, released August 3, documents a suspected Russian espionage actor compromising public Wi-Fi gateway infrastructure and redirecting browsing sessions to rogue captive portal pages that spoof Microsoft authentication domains — with Healthcare GTI-confirmed among nine targeted industries and United States targeting confirmed. Microsoft Threat Intelligence published closely matching findings in the same window under the campaign name CaptiveCrunch, attributing the activity to Storm-2945, which it assesses to be an operational sub-cluster of Midnight Blizzard (APT29 / Cozy Bear), an actor the US and UK governments have attributed to Russia's SVR. The operational detail that matters most: since July 16, some landing pages redirect victims into Microsoft's genuine device code authentication flow, so a traveller who enters an attacker-supplied code on the real Microsoft sign-in page hands over an MFA-satisfied session. With autumn conference season approaching, this is a control gap that clinical and administrative travel exposes directly.

Medical device intelligence resumed after a three-week gap, with two new CISA medical advisories inside the window. ICSMA-26-216-01 (August 4) covers CVE-2026-17583 in Thermo Fisher Applied Biosystems genetic analyzer software — CVSS v4.0 8.2, and unusual in that it is an integrity attack rather than a confidentiality one: the analysis software does not verify the authenticity of instrument-generated .fsa and .hid files, so DNA data can be altered before analysis in a way the software will not flag. ICSMA-26-218-01 (August 6) covers CVE-2026-17264 in the Medixant RadiAnt DICOM Viewer, a widely deployed clinical imaging viewer, where a crafted DICOM file with malicious JPEG-compressed pixel data triggers an attacker-controlled heap out-of-bounds write. RadiAnt is the fourth distinct DICOM product line to draw an advisory in the current run after GDCM, pydicom/pynetdicom, and DCMTK — and unlike the first two, it has a fix.

Also this week: Palo Alto Networks Unit 42 published research on August 3 describing three techniques — Pass-ta-key, Silver Pass-ta-key, and Golden Pass-ta-key — by which malware already resident on a Windows endpoint can abuse Google-synced passkeys to authenticate without any biometric or PIN prompt, install an attacker-controlled user-verification key, or extract the master secret that decrypts every synced passkey. This matters to this readership specifically because phishing-resistant passkey and FIDO2 authentication is the control this series has recommended repeatedly against help-desk reset abuse and identity takeover. The finding does not overturn that recommendation — passkeys remain materially safer than passwords, and every technique requires prior endpoint compromise — but it does change the supporting assumptions, and Priority Action 3 sets out what to adjust.

Active Threat Campaigns- Healthcare & Technology

Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
Hospitality Wi-Fi Captive Portal Compromise (CAMP.26.107; Microsoft "CaptiveCrunch" / Storm-2945)	Nation-State / Espionage (Russia-nexus)	Compromised public Wi-Fi gateway infrastructure at hotels, conference centres, and airports is used to intercept and manipulate user network connections; DNS and HTTP traffic is manipulated so browsing sessions are redirected to rogue captive portal pages spoofing Microsoft authentication domains hosted on external infrastructure. Two distinct outcomes are reported: (a) fake verification checks, sign-in prompts, and software/driver update prompts that deliver malware capable of harvesting browser cookies, passwords, and documents, capturing keystrokes, screenshots, audio and video, monitoring the clipboard, and operating the device remotely; and (b)	GTI-confirmed for CAMP.26.107: Healthcare among nine industries (also Financial Services, Insurance, Legal & Professional Services, Manufacturing, Retail, Transportation, Construction & Engineering, Chemicals & Materials) — United States, Canada, India, Belgium confirmed. Microsoft describes worldwide	CRITICAL — Treat hotel, conference, and airport Wi-Fi as untrusted for clinical and administrative staff; block device code authentication via Conditional Access where not required; mandate cellular hotspot or always-on full-tunnel VPN for travel; never install updates, certificates, or tools offered by a captive portal



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
		credential, OAuth token, and device-code harvesting leading to Microsoft 365 mailbox and OneDrive access. Since July 16, 2026, some landing pages redirect victims into Microsoft's legitimate device code authentication flow — entering the attacker-supplied code on the real Microsoft sign-in page grants the attacker an MFA-satisfied session. GTI activity window: June 30 – July 29, 2026; Microsoft reports observation since early May 2026	targeting of business travellers	
"Pass-ta-key" — Synced Passkey Abuse (Unit 42 research, August 3)	Security Research Disclosure (no in-the-wild exploitation reported)	Palo Alto Networks Unit 42 disclosed three attack techniques against Google-synced passkeys. Precondition in all three is malware already running on a compromised Windows device using Chrome. Chrome stores synced passkey metadata locally in an unencrypted, readable database, giving malware a map of every service where the victim uses passkey login without needing elevated privileges. Pass-ta-key: malware silently asks Chrome and Google's cloud to mint a valid passkey assertion with no biometric or PIN prompt. Silver Pass-ta-key: the malware invalidates the existing user-verification key and, during the re-enrolment window, registers its own key — the cloud authenticator does not validate that key's attestation, so every subsequent assertion carries a fraudulent "user verified" flag, and the attacker can authenticate from their own environment. Golden Pass-ta-key: extraction of the 32-byte Security Domain Secret, the master key that decrypts every synced passkey private key; Unit 42 reports no mechanism exists to rotate or revoke it	Not industry-targeted. Healthcare relevance is direct: phishing-resistant passkey and FIDO2 authentication is the control this brief series has recommended repeatedly for help-desk reset abuse and identity takeover	HIGH — Do not abandon passkeys; they remain materially safer than passwords. Require and validate the returned user-verification bit on relying parties you control; prefer hardware security keys for privileged clinical and administrative accounts; treat endpoint malware prevention as a passkey control

Top 3 Priority Actions This Week

1. [CRITICAL] Harden Travel and Guest-Network Access for Clinical and Administrative Staff

GTI released CAMP.26.107 on August 3, describing a suspected Russian espionage actor that compromises public Wi-Fi gateway infrastructure to intercept and manipulate user network connections, redirecting browsing sessions to rogue captive portal pages that spoof Microsoft authentication domains hosted on external infrastructure. Healthcare is GTI-confirmed among nine targeted industries, with confirmed targeting in the United States, Canada, India, and Belgium; the GTI activity window runs June 30 to July 29, 2026, with 13 indicators and 31 mapped ATT&CK techniques. Microsoft Threat Intelligence published closely matching findings in the same window as CaptiveCrunch, attributed to Storm-2945, reporting observation of the traffic manipulation since early May 2026 across hospitality networks in several countries, and noting common equipment and management systems across affected networks that may indicate a shared upstream access route. Two outcomes are documented. In the malware route, the portal presents fake verification checks, sign-in prompts, or software and driver update prompts; the resulting implant harvests browser



cookies, passwords, and documents, and can capture keystrokes, screenshots, audio, and video, monitor the clipboard, and operate the device remotely. In the credential route, victims are redirected to spoofed Microsoft sign-in pages that harvest credentials, OAuth tokens, and device codes, yielding mailbox and OneDrive access. Since July 16, some landing pages route victims into Microsoft's legitimate device code authentication flow — the victim enters an attacker-supplied code on the genuine Microsoft page, and the attacker receives a session that satisfies MFA. For healthcare, the exposure is concrete: clinicians and executives travel to conferences, and a compromised session in a healthcare tenant reaches clinical SharePoint, mail, and OneDrive.

- Block device code authentication through Conditional Access wherever it is not required — this single policy closes the route that defeats MFA, and Microsoft recommends it explicitly
- Issue guidance and provisioning for travel connectivity: cellular hotspots or an always-on, full-tunnel VPN that resolves DNS through corporate resolvers before the venue gateway can answer
- Instruct staff never to install software updates, drivers, certificates, browser updates, or “troubleshooting” tools presented by a captive portal — no legitimate venue network requires this
- Ingest the 13 GTI indicators (1 file hash, 7 IP addresses, 5 domains) into DNS monitoring, web filtering, and SIEM watchlists
- Hunt retrospectively for travel-window anomalies since early May: impossible-travel sign-ins, new device registrations from hotel or conference IP ranges, unexpected device code grants, and OAuth consent events tied to travelling users
- Brief anyone attending an autumn conference before they leave, and consider issuing loaner devices for high-risk travel by executives and staff with privileged clinical system access

2. [HIGH] Remediate the Two New Medical Device Advisories — Thermo Fisher and RadiAnt

CISA published two medical advisories inside this window, ending a three-week gap. ICSMA-26-216-01 (August 4) addresses CVE-2026-17583, rated CVSS v4.0 8.2, in Thermo Fisher Applied Biosystems genetic analyzer and Human Identification software. The flaw is a data integrity issue: the analysis software does not verify the integrity or authenticity of the .fsa and .hid output files produced by the instruments, so if surrounding laboratory controls are circumvented an instrument-generated file can be altered before it is loaded and the application will process the altered data without raising an integrity warning. CISA states the vulnerability is not remotely exploitable and reports no known public exploitation, and it is not on the KEV catalog. Thermo Fisher's July 31 bulletin ships updates for five supported product lines that add digital signatures to newly generated files; per that reporting, three end-of-life data collection products will receive no vendor update, so laboratories running older instruments must fall back to file custody and access controls. The disclosure was coordinated with CISA and credited to researchers Nathan Adams, Kevin Dyer, and Laura Gaydosh Combs; one outlet reports that the demonstration used a commercial AI assistant to merge two DNA profiles into a single file that appeared unaltered since 2015, which if accurate speaks to how little specialist skill the manipulation requires.

ICSMA-26-218-01 (August 6) addresses CVE-2026-17264 in the Medixant RadiAnt DICOM Viewer, versions 2025.2 and earlier. Opening a crafted DICOM file containing malicious JPEG-compressed pixel data triggers an attacker-controlled heap out-of-bounds write (CWE-787). Read the advisory carefully rather than the headline: the vulnerability description says remote arbitrary code execution may be possible, while CISA's own summary line and both CVSS vectors (5.3 v4.0, 4.3 v3.1) reflect only an application crash and availability impact, and CISA notes the binary is compiled with Control Flow Guard, Data Execution Prevention, and ASLR enabled, which it says significantly reduces practical exploitability. Treat it as a real but moderate issue with an easy fix. RadiAnt is the fourth distinct DICOM product line to draw an advisory in the current run, after GDCM, pydicom/pynetdicom, and DCMTK — and notably it is a clinical viewer used at the point of care rather than a developer library, which widens who needs to act.



- Inventory Applied Biosystems instruments and analysis software across pathology, genetics, molecular diagnostics, and any forensic or research laboratory, and apply the vendor updates that add file digital signatures
- For end-of-life Applied Biosystems products with no available update, document compensating controls: restricted file system permissions on instrument output directories, chain-of-custody logging, and hash verification of files between instrument and analysis workstation
- Update RadiAnt DICOM Viewer to 2026.1 across all clinical workstations, including radiologist home-reading setups and any instances installed outside the managed software catalogue
- Reinforce the standing DICOM control set — open imaging files only from trusted sources, block DICOM ingestion from unauthenticated sources, segment imaging networks, and validate files at the boundary — which now covers four concurrent advisories
- Record the integrity-attack pattern in your risk register: CVE-2026-17583 produces wrong clinical or forensic results rather than stolen data, and detection depends on file custody controls, not on data-loss monitoring

3. [HIGH] Re-validate Passkey Assumptions Without Abandoning Passkeys

On August 3, Palo Alto Networks Unit 42 published research describing three attack techniques against Google-synced passkeys, collectively named Pass-ta-key. All three assume malware is already running on a compromised Windows device using Chrome, which is the essential context for interpreting them. Unit 42 found that Chrome stores synced passkey metadata locally in an unencrypted, readable database, giving malware an inventory of every service where the victim uses passkey authentication without requiring elevated privileges. In the base Pass-ta-key technique, malware silently asks Chrome and Google's cloud authenticator to produce a valid passkey assertion with no biometric or PIN prompt. In Silver Pass-ta-key, the malware invalidates the existing user-verification key and, during the brief re-enrolment window, registers its own key; because the cloud authenticator does not validate that key's attestation, every subsequent assertion carries a fraudulent user-verified flag, and the attacker can authenticate from their own environment without further access to the victim machine. In Golden Pass-ta-key, the malware extracts the 32-byte Security Domain Secret, the master key that decrypts every synced passkey private key — and Unit 42 reports Google currently provides no mechanism to rotate or revoke it, so current and future synced passkeys remain protected by the same compromised secret. Unit 42 also found that some relying parties trusted a user-verified flag without confirming a real verification event; eBay corrected this after being notified. Google removed the secret from Chrome's logging output following the report, but Unit 42 states it still reaches the client and remains accessible in Chrome process memory. No CVEs have been assigned to the three techniques, and no in-the-wild exploitation has been reported. The honest conclusion for a healthcare security program is that passkeys remain significantly safer than passwords and the recommendation to move away from SMS and password-based recovery stands — but the assumption that a passkey assertion proves a human was present does not, and the chain that gets malware onto the endpoint in the first place is exactly the ClickFix-to-infostealer pattern this series has tracked all summer, including the LUMMAC and VIDAR delivery in CAMP.26.102 reported last week.

- On any relying party your organization controls — patient portals, staff applications, custom clinical software — set userVerification to required and validate the returned user-verification bit rather than trusting the request setting alone
- Prefer hardware security keys over synced software passkeys for privileged accounts: domain and tenant administrators, EHR super-users, finance approvers, and help-desk staff who can reset others' credentials
- Reframe endpoint malware prevention as an authentication control — these techniques are only reachable after endpoint compromise, so EDR coverage and ClickFix-focused user training now protect your passkeys as well as your data
- Add the published forensic signals to detection engineering: unexpected reads of Chrome's synchronization database by non-browser processes, deletion or re-creation of the passkey



enclave state file outside a normal update cycle, and cross-process memory access to chrome.exe from unsigned or unusual binaries (Sysmon event IDs 10 and 11 map to these)

- Do not pause a passkey rollout on the strength of this research; document the residual risk, prioritise hardware keys where impact is highest, and revisit if CVEs or in-the-wild exploitation are reported

Medical Device and IoT Security

Both new advisories are covered in full in Priority Action 2. The tracker view: CVE-2026-17583 (Thermo Fisher, CVSS v4.0 8.2, patches available for supported lines, no update for three end-of-life products) and CVE-2026-17264 (Medixant RadiAnt DICOM ≤ 2025.2, fixed in 2026.1). Neither has known public exploitation and neither is on the KEV catalog. With these additions, four distinct DICOM-handling products now carry open or recently-closed advisories in this run: GDCM (no patch, week 20), pydicom/pynetdicom (no vendor fix, maintainer unresponsive to CISA), DCMTK (patched), and RadiAnt (patched). Two of the four have fixes and two do not, which makes the split worth stating plainly to clinical leadership: the patchable items are a maintenance task and should be closed quickly, while GDCM and pynetdicom will remain compensating-control problems for the foreseeable future. The shared control set — blocking DICOM ingestion from unauthenticated sources, imaging network segmentation, boundary file validation, and opening imaging files only from trusted sources — covers all four at once.

One theme worth flagging to biomedical and laboratory leadership. The Thermo Fisher advisory is an integrity vulnerability, not a data-theft vulnerability: successful exploitation produces inaccurate test results rather than exposed records. That failure mode does not appear in most healthcare risk registers, which are built around confidentiality and availability, and it is not detected by data-loss monitoring. Laboratory and genomics environments should be assessed for whether instrument output files have any integrity assurance between generation and analysis — for many workflows the answer will be that they do not.

Persistent CVE and KEV Tracker

CVE	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-17583 (NEW)	Thermo Fisher Applied Biosystems genetic analyzers / Human Identification software	8.2 (v4.0)	CISA ICSMA-26-216-01 (Aug 4); vendor bulletin Jul 31	Partial	Analysis software does not verify the integrity or authenticity of instrument-generated .fsa/.hid files, allowing near-undetectable tampering with DNA data before analysis and producing inaccurate results. NOT remotely exploitable; no known public exploitation; not on KEV. Five supported product lines received updates adding digital signatures (3500/3500xL Data Collection 4.0.3; 3730/3730xL 5.0.3; SeqStudio Genetic Analyzer 1.2.6; SeqStudio Flex 1.2.1; GeneMapper ID-X updated per vendor bulletin). Per vendor reporting, three end-of-life data collection products will receive NO update — confirm your exact products against the advisory.
CVE-2026-17264 (NEW)	Medixant RadiAnt DICOM Viewer ≤ 2025.2	5.3 (v4.0) / 4.3 (v3.1)	CISA ICSMA-26-218-01 (Aug 6)	Yes	Crafted DICOM file with malicious JPEG-compressed pixel data triggers an attacker-controlled heap out-of-bounds write (CWE-787). Update to RadiAnt 2026.1 and open DICOM files only from trusted sources. Note the scoring tension:



CVE	System / Component	CVSS	Advisory	Patch	Status & Action
					the description states remote arbitrary code execution may be possible while CISA's summary and the CVSS vectors reflect application crash / availability impact only; CISA also notes the binary ships with CFG, DEP, and ASLR enabled, which significantly reduces practical exploitability. No known public exploitation.
CVE-2026-50003 (+4 high)	OFFIS DCMTK Toolkit ≤ 3.7.0 (DICOM library)	9.8	CISA ICSMA-26-181-01	Yes	Path traversal via bit-preserving C-GET, plus CVE-2026-50254, -35505, -52868, -44628. Confirm the patched snapshot is deployed and continue pressing imaging vendors on embedded DCMTK timelines.
CVE-2026-56445	pydicom / pynetdicom qrscp (DICOM C-STORE)	9.1	CISA ICSMA-26-176-01	NO	Unauthenticated path traversal / arbitrary file write; pynetdicom ≥v1.0.0 to <v3.0.4 affected. Maintainer still unresponsive to CISA. Restrict DICOM port access, segment, monitor the GitHub project.
CVE-2026-3650	Grassroots DICOM (GDCM) 3.2.2	7.5	CISA ICSMA-26-083-01 (Mar 24)	NO	Week 20 with no patch. Memory leak parsing malformed DICOM files with non-standard VR types in file meta information, causing resource depletion and denial of service. Maintain PACS segmentation and block unauthenticated DICOM ingestion.
CVE-2026-22879 / CVE-2026-12473	vtk-dicom 9.5.2; OHIF DICOM Web Viewer	8.1 / 8.2	Talos TALOS-2026-2366; CISA ICSMA-26-176-02	Yes	Heap overflow via crafted DICOM file (vtk-dicom) and SSRF (OHIF, patched v3.12.2). Confirm distribution packages and OHIF deployments are current; remove unused OHIF DicomWebProxy/DicomJSON data sources.
CVE-2025-66376	Zimbra Collaboration Suite — Classic UI webmail	See note	Joint CSA AA26-204A (Jul 23)	Yes	Zero-click XSS exploited by LAUNDRY BEAR since at least July 2025; patched by Synacor November 2025. Not found in the CISA KEV catalog on review; the joint advisory is the authority. Confirm ZCS patch level and hunt with the advisory STIX packages.
CVE-2026-25089 / CVE-2026-39808	Fortinet FortiSandbox (incl. Cloud and PaaS)	9.8 / 9.1	CISA KEV (Jul 16)	Yes	Two actively exploited unauthenticated OS command injection flaws. Fixed in 4.4.9+, 5.0.6+, Cloud/PaaS 5.0.6+. Exploitation predates the KEV listing, so hunt internet-exposed instances rather than assuming patching is sufficient.
CVE-2026-58644 / CVE-2026-48558	Microsoft SharePoint Server; SimpleHelp RMM	9.8 / KEV	CISA KEV (Jul 16 / Jun 29)	Yes	SharePoint deserialization (CISA describes network code execution; Microsoft's FAQ states Site Owner rights are needed — model both) and SimpleHelp authentication



CVE	System / Component	CVSS	Advisory	Patch	Status & Action
					bypass. Re-check Site Owner assignments on clinical policy libraries; verify no vendor remote-access path uses an unpatched SimpleHelp instance.
CVE-2026-0611 / CVE-2026-43994	Spacelabs Sentinel; coturn TURN/STUN (telehealth)	9.8 / 8.1	June 12 / June 19 briefs	Yes	Both patched (Sentinel v11.6.0; coturn 4.10.0). Confirm deployment complete across cardiac monitoring and telehealth stacks.
CVE-2024-12248 / CVE-2025-0626	Contec CMS8000 patient monitors	9.8	FDA / CISA	N/A	FDA disconnect recommendation remains in force; no active exploitation observed.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Nation-state targeting of travellers via untrusted network infrastructure: CRITICAL — healthcare GTI-confirmed (CAMP.26.107 / CaptiveCrunch) ▲ Device code authentication abuse: new route observed from July 16 — yields MFA-satisfied Microsoft 365 sessions ▲ Medical device advisories: 2 new ICSMA in one week, ending a three-week gap ▲ DICOM software advisories: fourth distinct product line in the current run (GDCM, pynetdicom, DCMTK, now RadiAnt) ▲ Attacks on data integrity rather than confidentiality: DNA analysis file tampering (CVE-2026-17583) ► Passkey security: first substantive research showing endpoint malware can defeat synced-passkey verification	2 new CISA ICS Medical Advisories in the Aug 1-7 window: ICSMA-26-216-01 (Aug 4) and ICSMA-26-218-01 (Aug 6) 13 new GTI-verified IOCs (CAMP.26.107) — 1 file, 7 IPs, 5 domains CAMP.26.092 IOC set grew from 14 to 275 indicators since the July 3 brief — refresh required 3 Pass-ta-key techniques disclosed; 0 CVEs assigned and no in-the-wild exploitation reported as of Aug 3 Microsoft reports hospitality Wi-Fi compromise observed since early May 2026 — roughly three months before public disclosure CVE-2026-3650 (GDCM): NO PATCH — week 20; CVE-2026-56445 (pynetdicom): NO PATCH

Sources: Google Threat Intelligence (GTI, including the Industry Snapshot: Healthcare profile), CISA ICS Medical Advisories ICSMA-26-216-01 and ICSMA-26-218-01 (plus -181-01, -176-01, -176-02, -083-01), CISA KEV Catalog, Joint Cybersecurity Advisory AA26-204A, Microsoft Threat Intelligence (CaptiveCrunch), Palo Alto Networks Unit 42 ("Pass the Passkey", August 3, 2026), Thermo Fisher Scientific security bulletin (July 31, 2026), Medixant, NVD / CVE Program / MITRE, Fortinet PSIRT, Microsoft Security Response Center, The Hacker News, BleepingComputer, SecurityWeek, Cybernews, Malwarebytes, Forbes, ABC News, PCWorld, ReliaQuest, Rescana, CyberSecurityNews, GBHackers