



Executive Summary

Two GTI-confirmed healthcare threats lead this week, and both turn on the abuse of legitimate remote-access tooling rather than on exploits. CAMP.26.154 documents a financially motivated campaign, tracked by GTIG since August 2026 and carrying 65 mapped ATT&CK techniques, in which initial access is achieved through MICROSOFT TEAMS VISHING — the attacker calls or messages a user over Teams and talks them into granting remote control through QUICK ASSIST, Microsoft’s built-in remote assistance tool. The TAILGLOW backdoor is then deployed, with persistence and command and control spread across CURL, Python, SharePoint Online dead-drop signalling, and the commercial remote tools AnyDesk, GetScreen and DWAgent. Escalation runs through Active Directory Certificate Services template abuse, NTDS.dit extraction using the Windows Server Backup utility WBADMIN, and lateral movement with Impacket WMIEXEC. Exfiltration goes to Azure Blob Storage via S3 Browser and WebRTC tunnelling. Healthcare is GTI-confirmed alongside Legal & Professional Services, with targeting in Canada and the United Kingdom and GTI describing the victim set as North America and Northern Europe.

The second is a scale event in a thread this series has followed since September 11. GTI published eight UNC7072 operation records covering a single sustained CLOUDHAZE campaign, all linked to CAMP.26.125 — the invoice-themed malvertising campaign reported in the September 18 brief — and to the same threat actor record. THREE of the eight are healthcare victims: two in the United States with activity running October 1 to 9 and October 2 to 9, and one in the United Kingdom spanning healthcare and education with activity from September 8 through October 13 using AWS S3 infrastructure and the domain westbeavers.com. The remaining five cover legal services in the US and UK, government in the US, and a manufacturing victim where data was exfiltrated to AWS S3 through a domain masquerading as a browser history backup service. This is the clearest picture yet of UNC7072’s operational tempo, and healthcare is a recurring rather than incidental target.

On breaches, the Oracle Health incident reported in the October 2 brief now has a scale figure. Bloomberg reports that the Texas Attorney General released information suggesting the protected health information of almost 20 million individuals was compromised when a hacker accessed two legacy Cerner servers in 2025. HIPAA Journal states plainly that the figure is not independently verified. Oracle Health has not made a public announcement but has begun notifying affected healthcare providers, and the HHS OCR breach portal still carries a placeholder total of 501 individuals. CISA published no new medical advisory in this window — confirmed against the full ICSMA index — leaving the two September 10 advisories open for a fourth consecutive week.

Active Threat Campaigns- Healthcare & Technology

Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
Microsoft Teams Vishing → Quick Assist → TAILGLOW Backdoor (CAMP.26.154)	Financially motivated intrusion — large-scale data exfiltration	A full-lifecycle intrusion campaign tracked by GTIG since August 2026, carrying 65 mapped ATT&CK techniques. Initial access is social engineering via MICROSOFT TEAMS VISHING, with the victim talked into granting remote control through QUICK ASSIST, after which the actor deploys the TAILGLOW backdoor. Command and control and persistence use CURL, Python, SharePoint Online dead-drop signalling, and the legitimate remote tools ANYDESK, GETSCREEN and DWAGENT. Escalation is via Active Directory Certificate Services template abuse, followed by NTDS.dit extraction using WBADMIN — the Windows Server Backup utility — and lateral movement with Impacket WMIEXEC and	Healthcare GTI-confirmed, alongside Legal & Professional Services — Canada and United Kingdom confirmed. GTI describes targeting as North America and Northern Europe in the Healthcare and Business Services industries	CRITICAL — Disable or tightly restrict Quick Assist; require out-of-band verification before any remote-control session. Alert on ADCS template abuse, on WBADMIN invoked against a domain controller, and on AnyDesk, GetScreen and DWAgent outside the sanctioned RMM set



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		OVERGROW. The actor enumerates file shares with custom Java tooling and exfiltrates to Azure Blob Storage using S3 Browser and WebRTC tunnelling. Activity observed August 10 to September 16, 2026		
UNC7072 CLOUDHAZE — Eight-Victim Cluster, Three in Healthcare (OP.26.1675, .1676, .1677 and five related)	Multi-victim intrusion set (motivation unknown)	GTI published eight UNC7072 operation records covering a single sustained CLOUDHAZE campaign, all linked to CAMP.26.125 — the invoice-themed malvertising campaign reported in the September 18 brief — and to the same threat actor record. THREE are healthcare: OP.26.1675 (US, activity October 1–9, CLOUDHAZE with WHOAMI reconnaissance), OP.26.1676 (US, activity October 2–9) and OP.26.1677 (UK, healthcare and education, activity September 8 to October 13, using AWS S3 infrastructure and the domain westbeavers.com). The remainder cover Legal & Professional Services in the US and UK, Government in the US including the domain motherotters.com, and a US manufacturing victim where the actor exfiltrated data to AWS S3 THROUGH A DOMAIN MASQUERADING AS A BROWSER HISTORY BACKUP SERVICE. Technique counts range from 13 to 30 per operation	Healthcare GTI-confirmed for three operations — United States (two) and United Kingdom (one). Same actor and malware family as the US healthcare victim reported in the September 11 brief (OP.26.1312)	CRITICAL — Block and retro-hunt westbeavers.com and motherotters.com alongside the previously reported apexesmasters.com and familypenguins.com. Alert on CLOUDHAZE file hashes and on AWS S3 egress to buckets with no business relationship
Oracle Health / Cerner Breach — Scale Emerges at Nearly 20 Million (reported Oct 8; Texas AG updated Oct 2)	Healthcare IT vendor / EHR platform breach	More than a year and a half after a hacker accessed two legacy Cerner servers, the scale of the 2025 breach is becoming clearer. Bloomberg reports that the Texas Attorney General released information suggesting the protected health information of almost 20 million individuals was compromised; the Texas AG was provided with an updated total on October 2, 2026. HIPAA Journal states explicitly that the figure is NOT independently verified. Compromised data reportedly includes names, Social Security numbers, and medical record-related health information — diagnoses, care and treatment information, medications, test results, medical images, medical record numbers and physician names. Oracle Health, which acquired Cerner in 2022, has not made a public announcement but has begun notifying affected healthcare providers. The HHS OCR breach portal still carries a PLACEHOLDER TOTAL OF 501 individuals and has yet to be updated	US health systems on Oracle Health / legacy Cerner platforms. Follows the 29 named health systems reported in the October 2 brief — this is the scale figure for that same incident	CRITICAL (if applicable) — Do not wait for the OCR portal to update; it is three orders of magnitude out of date. Request written confirmation from Oracle Health of whether your patient population is in scope and what categories were involved
ScreenConnect Backdoors via Phishing Lures (CAMP.26.156)	Remote access tool abuse (motivation unknown)	An email phishing campaign delivering VBScript and JavaScript files masquerading as legitimate documents or invitations. The scripts use WScript and PowerShell to download follow-on payloads, specifically ScreenConnect MSI installers retrieved from DROPBOX and from actor-controlled	GTI-confirmed: Chemicals & Materials, Construction & Engineering, Government, Legal & Professional	HIGH — Inventory sanctioned ScreenConnect instances and relay endpoints, then alert on any ScreenConnect



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		domains. The ScreenConnect ClientService then establishes persistent remote access to external relay infrastructure. The actor manipulates the registry to secure persistence and deploys the utility HideUL_x64.exe to CONCEAL THE SCREENCONNECT INSTALLATION from the user. Activity observed July 28 through October 8, 2026 — running into this coverage window; 42 mapped ATT&CK techniques	Services, Manufacturing, Technology — United States, Canada, South Korea. Healthcare NOT confirmed. Carried because ScreenConnect is widely deployed in healthcare IT and by vendors, so a malicious instance blends with legitimate use	ClientService connecting to an unlisted relay. Alert on HideUL_x64.exe and on MSI downloads from Dropbox by scripting engines

Top 4 Priority Actions This Week

1. [CRITICAL] Break the Teams Vishing and Quick Assist Chain (CAMP.26.154)

GTIG has tracked this financially motivated campaign since August 2026, and it is the most completely mapped healthcare-confirmed intrusion chain this series has reported, with 65 ATT&CK techniques. The entry point deserves attention because it bypasses every email control: the actor contacts a user through Microsoft Teams, conducts a voice-based social engineering call, and persuades the victim to grant remote control via QUICK ASSIST — a tool built into Windows, signed by Microsoft, and frequently allowed by default. There is no attachment, no link, no exploit. From that foothold the actor deploys the TAILGLOW backdoor and establishes redundant persistence through CURL, Python, SharePoint Online dead-drop signaling, and three separate commercial remote tools: AnyDesk, GetScreen and DWAgent. Escalation abuses Active Directory Certificate Services templates — the same ADCS weakness CISA demonstrated in its red team advisory AA26-237A covered in the August 28 brief, and seen again in CAMP.26.077. The actor then extracts NTDS.dit using WBADMIN, the legitimate Windows Server Backup utility, which is a notably quiet alternative to the usual shadow-copy or credential-dumping routes. Lateral movement uses Impacket WMIEXEC and OVERGROW, share enumeration uses custom Java tooling, and exfiltration goes to Azure Blob Storage via S3 Browser and WebRTC tunnelling.

The defensive implication is that almost every stage uses something legitimate. Quick Assist is a Microsoft tool. WBADMIN is a Windows feature. AnyDesk and ScreenConnect are in many healthcare environments already. Azure Blob Storage is a sanctioned destination for most organizations. Detection has to be built on context and baseline rather than on inherently malicious artefacts.

- Disable Quick Assist through policy where there is no business need, or restrict it so that a remote-control session cannot be initiated without out-of-band verification through a known-good channel
- Review Microsoft Teams external access and federation settings — this is the second consecutive week a GTI campaign has used Teams as the initial access channel, after CAMP.26.148 in the October 2 brief
- Alert on ADCS certificate template abuse and audit templates for the ESC1 misconfiguration (requester-supplied subject alternative names plus client authentication EKU and low enrolment requirements); set Machine Account Quota to zero if you have not already



- Alert on WBADMIN executed against a domain controller or against the volume containing NTDS.dit — a backup utility invoked interactively on a domain controller is a high-fidelity signal
- Inventory and allowlist remote access tooling, then alert on AnyDesk, GetScreen and DWAgent anywhere outside the sanctioned set; this single control also covers the ScreenConnect campaign in Priority Action 4
- Monitor for bulk uploads to Azure Blob Storage and for S3 Browser execution on endpoints that have no cloud storage administration role

2. [CRITICAL] Hunt the UNC7072 CLOUDHAZE Infrastructure — Three Healthcare Victims

GTI published eight UNC7072 operation records covering a single sustained CLOUDHAZE campaign, and the healthcare concentration is the headline. OP.26.1675 documents a US healthcare organization with activity from October 1 to 9, using CLOUDHAZE with the WHOAMI utility for host reconnaissance across 24 mapped techniques. OP.26.1676 documents a second US healthcare organization with activity from October 2 to 9. OP.26.1677 documents a UK organization spanning healthcare and education, with activity from September 8 through October 13, where the actor used AWS S3 infrastructure and the domain westbeavers.com for command and control. The remaining records cover other types of industry in the US and UK, two government victims in the US — one using the domain motherotters.com — and a US manufacturing and engineering victim where the actor exfiltrated data to AWS S3 through a domain deliberately masquerading as a browser history backup service. All eight are linked by GTI to CAMP.26.125, the invoice-themed malvertising campaign reported in the September 18 brief, and to the same threat actor record as OP.26.1312, the US healthcare victim reported on September 11.

Two operational points. First, the use of AWS S3 for both delivery and exfiltration means egress to a major cloud provider is doing double duty, and generic cloud-storage allowlisting will not catch it — the control has to be bucket-level or account-level. Second, the browser-history-backup masquerade is a deliberate choice: a domain name that sounds like a benign browser utility is unlikely to be challenged by a user or a tier-one analyst reviewing proxy logs.

- Block and retro-hunt westbeavers.com and motherotters.com across DNS, proxy and firewall logs, alongside the previously reported apexesmasters.com and familypenguins.com from the September 11 brief
- Ingest the 15 CLOUDHAZE file hashes published across the eight operation records into EDR blocklists and retro-hunt endpoint telemetry back to early September
- Review AWS S3 egress: alert on connections to S3 buckets outside your organization's known accounts, and treat S3 as an exfiltration channel rather than a trusted destination
- Alert on WHOAMI execution immediately following process creation from a browser or download path — it appears across most of these operations as the first reconnaissance step
- Re-apply the CAMP.26.125 controls from the September 18 brief: brief revenue cycle, accounts payable and procurement staff on invoice-site malvertising, and review ad-network web filtering

3. [CRITICAL] Act on the Oracle Health Scale Figure Without Waiting for OCR

The Oracle Health incident covered in the October 2 brief, where reporting named 29 affected health systems, now has a scale figure attached. According to Bloomberg, the Texas Attorney



General released information suggesting the protected health information of almost 20 million individuals was compromised when a hacker accessed two legacy Cerner servers in 2025. The Texas Attorney General was provided with an updated total on October 2, 2026 of about 3 million Texans. HIPAA Journal, reporting on October 8, states explicitly that the figure is not independently verified, and this brief presents it on the same basis — as reported, not as established. The data reportedly compromised is unusually complete for a healthcare breach: names, Social Security numbers, and medical record-related health information including diagnoses, care and treatment information, medications, test results, medical images, medical record numbers and physician names. Oracle Health, which acquired Cerner in 2022, has not made a public announcement but has begun notifying affected healthcare providers.

One detail deserves to be put in front of compliance and legal leadership. The HHS OCR breach portal still lists this incident with a placeholder total of 501 individuals. If your organization monitors the OCR portal as its primary source for vendor breach scale — as many do — then for this incident that source is currently understating the reported figure by roughly four orders of magnitude. The portal is expected to be updated in the coming weeks, but the gap between a placeholder filing and a confirmed total is a structural blind spot in vendor risk monitoring, not a one-off.

- If you run Oracle Health or legacy Cerner platforms, request written confirmation of whether your patient population is in scope, the data categories involved, and the notification timeline — Oracle is notifying providers directly rather than announcing publicly
- Given that Social Security numbers and medical images are reportedly in scope, prepare patient notification and credit monitoring planning now rather than after a confirmed count
- Record this as a Business Associate event with the reported figure, its sourcing chain (Texas AG via Bloomberg via HIPAA Journal) and the explicit non-verification caveat, keeping reported and confirmed facts separate in any internal or patient-facing communication

4. [HIGH] Bring Remote Access Tooling Under Inventory and Alerting (CAMP.26.156)

GTIG released CAMP.26.156 documenting an email phishing campaign that delivers VBScript and JavaScript files masquerading as legitimate documents or invitations. The scripts use WScript and PowerShell to download ScreenConnect MSI installers from Dropbox and from actor-controlled domains; the ScreenConnect ClientService then establishes persistent remote access to external relay infrastructure. The actor manipulates the registry for persistence and deploys a utility named HideUL_x64.exe specifically to conceal the ScreenConnect installation from the user. Activity ran from July 28 through October 8, 2026 — into this coverage window — across 42 mapped techniques, with GTI-confirmed targeting in Chemicals & Materials, Construction & Engineering, Government, Legal & Professional Services, Manufacturing and Technology across the United States, Canada and South Korea. Healthcare is not confirmed. It is carried because ScreenConnect is widely deployed in healthcare IT departments and by third-party vendors for support, which means a malicious instance does not look anomalous by its presence alone — only by where it connects.

Taken together with CAMP.26.154, this is the week's structural theme: four separate legitimate remote-access products (Quick Assist, AnyDesk, GetScreen, DWAgent) in one campaign and a fifth (ScreenConnect) in another, all used as the persistence layer. The federal Medusa advisory covered in the August 21 brief made the same point about RMM tooling selected to match what is already present in the victim environment. The control that addresses all of it is an inventory plus an allowlist, not signature detection.

- Build or refresh the inventory of sanctioned remote access tools AND their legitimate relay or cloud endpoints, then alert on any instance connecting somewhere not on that list — for ScreenConnect specifically, the relay endpoint is the discriminator



- Alert on HideUL_x64.exe and on any utility whose function is to hide installed software from the user interface
- Alert on MSI installers downloaded by WScript, cscript or PowerShell, and on MSI retrieval from consumer file-sharing services including Dropbox
- Extend the same allowlist to vendor-operated remote access: ask medical device and IT vendors which remote support product they use and which endpoints it contacts, then alert on everything else
- Note the third-party credential lesson from the Denmark Central Register breach disclosed October 5, where reporting attributes access to an IT supplier account protected by the password “123456” and 14 million automated searches ran for ten days before detection — vendor access accounts need the same authentication standards as your own privileged accounts

Healthcare Sector Incident Watch

Alongside the Oracle Health development, several provider-side incidents surfaced. A ransomware attack on Hospital Caribbean Medical Center in Puerto Rico affected up to 92,000 individuals. Tennessee-based Artemis Healthcare experienced a ransomware attack involving data theft. Notifications began on October 6 from Secure Healthcare Information Management, an Allentown, Pennsylvania medical management and billing service provider, and in early October from Desert Orthopedic Center in Nevada; neither incident yet appears on the OCR breach portal, so affected counts are not established. Internationally, Denmark confirmed on October 5 a breach of its Central Register of Persons affecting 8.8 million people. The access route is the instructive part: reporting indicates the attacker used a Danish IT company's legitimate access to the national register, through an account protected by the password “123456”, ran roughly 14 million automated searches between September 10 and 20, and was not detected until October 2 — twelve days after the last searches. That is a third-party access failure rather than a technical exploit, and it maps directly onto the vendor and business associate access that healthcare organizations grant routinely.

- Audit third-party and vendor accounts that hold standing access to patient data systems or registries for password strength, MFA enforcement, and whether bulk query activity would be detected
- Set volumetric alerting on record lookups by service and vendor accounts — the Denmark case ran 14 million queries over ten days without triggering a response
- Track the Secure Healthcare Information Management and Desert Orthopedic Center filings on the OCR portal for eventual counts if either is in your referral or billing network

Medical Device and IoT Security

No New Advisory Surfaced — Open Actions Carried

A direct review of the CISA ICS Medical Advisory index confirms no new medical advisory was published between October 3 and 9, 2026. The most recent remain ICSMA-26-253-01 (NextGen Healthcare Mirth Connect) and ICSMA-26-253-02 (Orthanc DICOM Server), both from September 10 and both carrying available vendor fixes, now open for a fourth consecutive reporting cycle. CISA did publish general ICS advisories in the window — ICSA-26-279-01 covering Johnson Controls EasyIO FG and ICSA-26-279-02 covering the Savannah lwIP SMTP client on October 6, and ICSA-26-281-03 covering Hitachi Energy Asset Suite on October 8 — none of which is a medical advisory. Johnson Controls EasyIO FG is worth a note for facilities and biomedical engineering because it is a building automation controller, and the hospital-campus OT exposure raised in joint advisory AA26-231A (August 21 brief) applies to building automation platforms as directly as it does to PLCs.



The unpatched standing set is unchanged and has now been open long enough to warrant a governance decision rather than continued tracking. Grassroots DICOM reaches week 29 without a patch and pydicom/pynetdicom remains unfixed, both with maintainers CISA records as unresponsive; the Pulsetto Vagus Nerve Stimulator has no vendor fix and no vendor response, leaving undisclosed Bluetooth commands capable of disabling electrical safety mechanisms exploitable within radio range. For these three, compensating controls are permanent, and the risk acceptance should be documented and signed rather than carried indefinitely as an open finding.

Persistent CVE and Advisory Tracker

CVE / Advisory	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-88771 / -88772 / -88779	Citrix NetScaler ADC and NetScaler Gateway	9.5 (v4) for -88771 and -88772	CISA KEV (Sep 27); Citrix CTX697096	Yes	CARRIED — HUNT REQUIRED. Exploitation preceded disclosure by roughly 18 days, so any appliance exposed during September should be hunted, not just patched: check httpd.conf for injected directives, the GUI directory for .sig web shells, /bin/sh for SUID root, and /etc/crontab for removed entries. CVE-2026-88779, an exploited denial-of-service flaw affecting SAML deployments, was disclosed October 3 — confirm it is covered by your patch level.
CVE-2026-82583 / -78224 / -82578	NextGen Healthcare Mirth Connect ≤ v4.7.1	8.3 / 7.5 (v3.1); 8.7 (v4.0)	CISA ICSMA-26-253-01	Yes	OPEN ACTION — FOURTH WEEK. CVE-2026-82583 permits an authenticated user to execute arbitrary SQL via a Database Connector API, enabling disclosure of stored credentials for connected systems; CVE-2026-82578 requires no privileges. Update to v4.7.2+ AND rotate every downstream integration credential.
CVE-2026-87020	Orthanc DICOM Server < 1.13.0	8.1 (v3)	CISA ICSMA-26-253-02	Yes	OPEN ACTION — FOURTH WEEK. Integer overflow in pitch and buffer-size computation leads to a heap out-of-bounds write when Orthanc decodes an attacker-supplied PNG. Upgrade to 1.13.0+.
CVE-2026-18844	Pulsetto Vagus Nerve Stimulator — ALL versions	Not published	CISA ICSMA-26-223-02	NO	Undisclosed BLE commands accepted without authentication permit disabling of electrical safety mechanisms. Vendor unresponsive to CISA; no fix exists. Patient counselling remains the only available control.
8 CVEs (CVE-2026-66875 et al.) / ICSMA-26-225-01	Mira Hormone Monitor and Android App (CVSS v3 9.8); Flow Neuroscience FL-100 tDCS headsets	9.8 / Not published	ICSMA-26-223-01 / -225-01	See advisory / Yes	Mira: missing authentication, authentication bypass by spoofing, hard-coded credentials and weak authentication permitting unauthorised access to health profiles, modification of health information, session token disclosure and account takeover. FL-100: hard-coded credential shared across all units — confirm firmware update via the Flow app.
CVE-2026-17583 / CVE-2026-17264	Thermo Fisher Applied Biosystems HID software; Medixant RadiAnt DICOM ≤ 2025.2	8.2 / 5.3 (v4.0)	ICSMA-26-216-01 / -218-01	Yes	Instrument output file tampering and heap out-of-bounds write via crafted DICOM pixel data. Update RadiAnt to 2026.1; three end-of-life Applied Biosystems products receive no update.



CVE / Advisory	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-50003 (+4) / CVE-2026-56445 / CVE-2026-3650	OFFIS DCMTK ≤ 3.7.0; pydicom / pynetdicom qrscp; Grassroots DICOM (GDCM) 3.2.2	9.8 / 9.1 / 7.5	ICSMA-26-181-01 / -176-01 / -083-01	Yes / NO / NO	DCMTK is patchable — deploy it. GDCM reaches week 29 and pynetdicom remains unfixed, both with maintainers CISA records as unresponsive. The shared DICOM control set covers all five affected product lines.
CVE-2026-12473 / CVE-2026-0257 / CVE-2025-53770	OHIF DICOM Web Viewer ≤ v3.12.0; Palo Alto GlobalProtect; Microsoft SharePoint	8.2 / 9.1 / see vendor	ICSMA-26-176-02; CISA KEV	Yes	OHIF: SSRF in default DicomWebProxy and DicomJSON data sources leaks the clinician's OIDC bearer token — upgrade to v3.12.2+ and remove unused data sources. GlobalProtect KEV deadline passed June 1.
CVE-2024-55591 / -24472 / CVE-2026-1731 / CVE-2025-10035	Fortinet FortiOS and FortiProxy; BeyondTrust RS/PRA; Fortra GoAnywhere	Various	AA26-222A; AA25-071A	Yes	Gunra and Medusa initial access vectors. Patch, then hunt for the forticloud-sync account and audit every RMM tool in the estate — directly relevant to this week's two RMM-abuse campaigns.
CVE-2025-66376 / -25089 / -39808 / -58644 / -48558 / CVE-2026-0611 / -43994	Zimbra; FortiSandbox; SharePoint; SimpleHelp RMM; Spacelabs Sentinel; coturn	Various	AA26-204A; CISA KEV; June briefs	Yes	Carried items — confirm remediation. Contec CMS8000 FDA disconnect recommendation also remains in force.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Microsoft Teams vishing plus Quick Assist as a full initial-access chain against healthcare ▲ UNC7072 CLOUDHAZE operational tempo: eight victim operations published at once, three in healthcare ▲ Legitimate remote tools as the persistence layer — Quick Assist, AnyDesk, GetScreen, DWAgent, ScreenConnect across two campaigns ▲ Cloud services as exfiltration infrastructure: AWS S3, Azure Blob Storage, SharePoint dead-drops, Dropbox ▲ EHR breach scale revision: a 2025 incident resolving to nearly 20 million individuals 18 months later ► No new CISA medical advisory; two September 10 advisories open for a fourth week	~20,000,000 individuals — reported scale of the Oracle Health / legacy Cerner breach (Texas AG via Bloomberg; not independently verified) 501 — the placeholder total still shown on the HHS OCR breach portal for that same incident 65 ATT&CK techniques mapped to CAMP.26.154, among the broadest in this series 8 UNC7072 operation records published together; 3 confirmed healthcare victims 69 new GTI-verified IOCs across 13 records CVE-2026-3650 (GDCM): NO PATCH — week 29; CVE-2026-56445 and CVE-2026-18844: NO PATCH

Sources: Google Threat Intelligence (GTI), CISA ICS Medical Advisory index and advisories ICSMA-26-253-01, -253-02, -225-01, -223-01, -223-02, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA ICS Advisories ICSA-26-279-01, -279-02, -281-03, CISA KEV Catalog, Citrix Security Bulletin CTX697096, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-237A, Bloomberg (via HIPAA Journal), Texas Attorney General, HIPAA Journal, HHS Office for Civil Rights breach portal, Oracle Health, The Register, Datatilsynet / Danish CPR administration (as reported), NVD / CVE Program / MITRE, NextGen Healthcare, Orthanc