



Executive Summary

Three GTI records with confirmed Healthcare targeting were created this week — the highest count in any single window in this series, and the third consecutive week in which GTI operation records have named US healthcare organizations as victims. The most actionable is CAMP.26.125, created September 14, which documents malvertising placed on invoice-related websites leading to deployment of the CLOUDHAZE malware family, with persistence via scheduled tasks and reconnaissance targeting system processes, security software status and browser profile data. Healthcare is GTI-confirmed alongside Education and Government across Canada, the United States and the United Kingdom. This was flagged as a forward notice in the September 11 brief, and the reason it matters is the linkage: GTI ties it to the same threat actor record as OP.26.1312, the UNC7072 operation against a US healthcare organization reported last week. The delivery mechanism and a confirmed healthcare victim are now both documented for the same actor, which makes the entry route — invoice-themed advertising, visited by finance and revenue-cycle staff — a specific thing to defend rather than a general warning.

Two further healthcare victim operations were documented. OP.26.1401 records UNC6971 executing a targeted operation against a US healthcare organization in June 2026, using the tool rel.curl to communicate with malicious infrastructure at sj98xe4.xyz; GTI associates this actor with the same records that appear in the NEONSLIDE framework reported on September 4. OP.25.1185 is different in character and worth reading carefully: it documents a UNC6394 operation against a US healthcare organization using the POUNDFALL malware family — in October 2025. GTI released five UNC6394 operation records together on September 17, covering victims from July 2025 through September 2026, which means a healthcare intrusion from eleven months ago is only now visible. That is a retrospective hunting task, not a current alert, and the brief treats it accordingly.

On breaches, the ShinyHunters extortion group reportedly published 7.1 million records from medical device manufacturer Baxter International, and reporting on the McKesson incident covered in the September 4 brief now puts the stolen dataset at 6.4 million unique email addresses. Cedar County Memorial Hospital in Missouri confirmed on September 10 that investigation into an August attack continues, with a relatively new extortion group calling itself Wallstreet claiming responsibility and threatening publication. CISA published no new medical advisory in this window — the two from September 10, covering Mirth Connect and Orthanc DICOM Server, remain open actions and are carried in the tracker as such.

Active Threat Campaigns- Healthcare & Technology

Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
CLOUDHAZE via Invoice-Themed Malvertising (CAMP.26.125)	Malvertising / Credential and host data theft (motivation unknown)	Malvertising placed on invoice-related websites ultimately leads to deployment of the CLOUDHAZE malware family. The actor establishes persistence via scheduled tasks and performs host reconnaissance targeting system processes, security software status, and browser profile data, exfiltrating collected data to actor-controlled command-and-control infrastructure. GTI links this campaign to the same threat actor record as OP.26.1312, the UNC7072 operation against a US healthcare organisation reported in the September 11 brief — which means the delivery mechanism and a confirmed healthcare victim are now both documented for the same actor. Activity observed August 5–11, 2026; 32 mapped ATT&CK techniques	Healthcare GTI-confirmed, alongside Education and Government — Canada, United States and United Kingdom	CRITICAL — Brief revenue cycle, accounts payable and procurement staff, who are the population that visits invoice-themed sites. Review web filtering coverage of advertising networks; alert on scheduled task creation followed by security software and browser profile enumeration
UNC6971 rel.curl Command Execution in Healthcare	Targeted intrusion operation	A single-victim operation record. GTI reports that UNC6971 executed a targeted operation against an organization in the healthcare subsector in June 2026, using the tool rel.curl to facilitate	Healthcare GTI-confirmed — United States. Activity	HIGH — Block and retro-hunt sj98xe4.xyz across DNS, proxy and firewall logs back to at



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
(OP.26.1401)	(motivation unknown)	network communications with malicious infrastructure at sj98xe4.xyz. GTI states the intrusion focused on establishing a presence within the environment to fulfil the actor's tactical objectives. The record is deliberately sparse — one indicator and two mapped techniques — which reflects limited observed activity rather than a limited threat. Notably, GTI associates UNC6971 with the same threat actor and malware records that appear in GLOBAL.26.006, the NEONSLIDE / ErrTraffic v3 framework reported in the September 4 brief	observed June 24, 2026	least May 2026. Alert on curl invoked from unusual parent processes on clinical and administrative endpoints
UNC6394 POUNDFALL Execution Targeting Healthcare (OP.25.1185, one of five UNC6394 records released together)	Targeted intrusion operation (motivation unknown)	GTI released five UNC6394 operation records on September 17, documenting a sustained campaign that had not previously been visible in this series. OP.25.1185 records that in October 2025 UNC6394 conducted an operation against a healthcare organization using the POUNDFALL malware family and related toolsets, deploying rel.poundfall to establish a foothold and facilitate further action. The other four records cover legal and professional services victims in the United Kingdom (July 2025), Canada (July 2025), the United States (September 2025) and the United Kingdom again in September 2026 — the last of these showing the actor is still operating. GTI describes the objective across the set as internal reconnaissance and strategic information exfiltration	Healthcare GTI-confirmed for OP.25.1185 — United States. The wider UNC6394 set is concentrated in Legal & Professional Services across the US, UK and Canada	HIGH — Note the timeframe: this healthcare intrusion occurred in October 2025 and is only now documented. Retro-hunt the POUNDFALL file hashes across historical EDR telemetry rather than treating this as a current-window alert
SANDWORM RELIC (APT44) — Health Ministry Impersonation Delivering FEEDUPDATE (CAMP.26.133)	Nation-state — Espionage and Attack / Destruction (Russia)	A phishing campaign using malicious links leading to ZIP archives that deploy VBScript loaders. The scripts deliver decoy documents and the FEEDUPDATE malware family. GTI notes specifically that the campaign involves masquerading as corporate AND HEALTH MINISTRY IDENTITIES to facilitate initial access and payload execution. GTI attributes the activity to SANDWORM RELIC (APT44), assessing motivations as both espionage and attack/destruction — the latter is significant, as APT44 is the actor group associated with destructive operations rather than collection alone. Activity observed April 20 – July 27, 2026	GTI-confirmed: Government — Ukraine only. NO healthcare targeting and no US targeting is confirmed. Carried solely because health ministry impersonation is the lure theme, which is directly relevant to how healthcare identity is being weaponized	MONITOR (US: low direct risk) — No action required for US healthcare beyond awareness. The transferable lesson is that public health authority identity is being used as a phishing lure by a destructive actor; brief staff that health ministry or public health agency branding is not a trust signal

Top 4 Priority Actions This Week

1. [CRITICAL] Defend the Invoice-Malvertising Route — Delivery and Healthcare Victim Now Both Confirmed

GTI created CAMP.26.125 on September 14, documenting a campaign in which malvertising on invoice-related websites ultimately leads to CLOUDHAZE deployment. The actor establishes persistence via scheduled tasks and performs host reconnaissance targeting system processes, security software status, and browser profile data, exfiltrating the collected data to actor-controlled command-and-control infrastructure. Healthcare is GTI-confirmed alongside Education and Government, with targeting confirmed in Canada, the United States and the United Kingdom, and



activity observed between August 5 and 11, 2026 across 32 mapped ATT&CK techniques. The significance is in the linkage rather than the volume. GTI associates this campaign with the same threat actor record as OP.26.1312, the operation reported in the September 11 brief in which UNC7072 targeted a US healthcare subsector organization with the CLOUDHAZE malware family using command-and-control domains including apexesmasters.com and familypenguins.com.

- Brief revenue cycle, accounts payable, procurement and practice management staff specifically, with the invoice-site lure described plainly; this is a different population from clinical staff and needs its own briefing
- Review web filtering coverage of advertising networks, and consider blocking ad-served executable downloads outright — this control has appeared repeatedly in this series and remains under-deployed
- Alert on scheduled task creation followed within a short window by enumeration of running processes, installed security products, and browser profile directories — that sequence is the documented CLOUDHAZE behavior and is high-fidelity
- Block and retro-hunt the previously reported UNC7072 domains apexesmasters.com and familypenguins.com alongside the three domains in this campaign record
- Because browser profile data is a collection target, treat any confirmed infection as a credential-compromise event: force password resets and revoke active sessions for the affected user rather than reimaging alone

2. [HIGH] Hunt Two Further Confirmed Healthcare Intrusions — One of Them Eleven Months Old

Two additional GTI operation records created this week confirm US healthcare victims, and they call for different responses. OP.26.1401 documents UNC6971 executing a targeted operation against a healthcare subsector organization in June 2026, using the tool rel.curl to facilitate network communications with malicious infrastructure at sj98xe4.xyz, with GTI stating the intrusion focused on establishing a presence to fulfil the actor's tactical objectives. GTI associates UNC6971 with the same threat actor and malware records that appear in GLOBAL.26.006, the NEONSLIDE and ErrTraffic v3 framework reported in the September 4 brief — which places this victim inside the same ecosystem as the largest campaign this series has covered. OP.25.1185 is the more unusual item. It documents a UNC6394 operation against a healthcare organization in October 2025, deploying rel.poundfall from the POUNDFALL malware family to establish a foothold. GTI released five UNC6394 operation records simultaneously on September 17, covering legal and professional services victims in the United Kingdom and Canada in July 2025, the United States in September 2025, the United Kingdom again in September 2026, and this healthcare victim in October 2025. GTI characterizes the objective across the set as internal reconnaissance and strategic information exfiltration.

The eleven-month gap between the healthcare intrusion and its documentation is the point worth carrying to leadership. It is a concrete illustration that absence of intelligence is not absence of intrusion, and that a healthcare organization compromised in October 2025 had no way to know from threat intelligence until now. The September 2026 record in the same set confirms UNC6394 is still operating, so this is not purely historical.

- Block and retro-hunt sj98xe4.xyz across DNS, proxy and firewall logs back to at least May 2026, and alert on curl invoked from unusual parent processes on clinical and administrative endpoints
- For POUNDFALL, retro-hunt the published file hashes across whatever historical EDR and endpoint telemetry you retain, targeting the October 2025 window specifically — this is a hunting exercise against archived data, not a live detection task
- Use the retention question as a governance finding: if your EDR telemetry does not reach back to October 2025, document that limitation, because it defines the ceiling on what retrospective hunting can ever tell you
- Treat both actors as active. UNC6971 is linked to the NEONSLIDE ecosystem covered on September 4, and UNC6394 has a confirmed September 2026 victim



3. [HIGH] Assess Exposure to the Baxter and McKesson Data Publications

Two developments concern data already stolen rather than new intrusions. The ShinyHunters extortion group reportedly published 7.1 million records from Baxter International, a major medical device manufacturer whose products include infusion pumps, IV solutions and surgical equipment used across virtually every US hospital. Reporting on the McKesson incident first covered in the September 4 brief now describes the stolen dataset, including 6.4 million unique email addresses; McKesson previously confirmed that intruders accessed several cloud-hosted accounts and exfiltrated data relating to its oncology, multispecialty and medical-surgical units. One caution on sourcing: the precise disclosure date of the Baxter publication was not confirmed in the sources reviewed for this brief, and the record counts in both cases derive from reporting and actor claims rather than company confirmation of a final figure. Treat them as reported figures with dates and attribution attached, not as established totals — the Conduent and Abbott cases earlier in this series both demonstrated how far initial claims can diverge from confirmed counts.

- If Baxter is a supplier to your organization, request written status on whether your organization's data, employee data, or patient-linked device data is within the published set
- For McKesson customers, the newly reported email-address volume raises the near-term risk of targeted phishing against your staff using genuine McKesson relationship context — brief pharmacy, supply chain and procurement teams that a convincing McKesson-themed email is now more likely, not less
- Record both as Business Associate or supplier events with the reported figures, their sources and their dates, and keep confirmed facts separate from actor claims in any internal or patient-facing communication
- Check whether either organization appears in your vendor register under a subsidiary or product name rather than the parent brand, which is a common reason exposure assessments miss a relationship

4. [HIGH] Close Out the Two Open Medical Advisories From September 10

With no new medical advisory published this window, the correct use of the week is to finish the two from September 10th advisory. ICSMA-26-253-01 covers three vulnerabilities in NextGen Healthcare Mirth Connect versions 4.7.1 and earlier, and remains the most consequential medical device advisory this series has covered: the CVE record for CVE-2026-82583 states that an authenticated user can execute arbitrary SQL through a Database Connector API, which could result in disclosure of stored credentials for connected systems, arbitrary file write, and denial of service, while CVE-2026-82578 requires no privileges at all. Mirth Connect is the HL7 integration engine holding connection credentials for the EHR, laboratory and radiology systems, PACS, pharmacy, scheduling and billing. ICSMA-26-253-02 covers CVE-2026-87020 in Orthanc DICOM Server versions earlier than 1.13.0, where an integer overflow allows an authenticated remote attacker to write past a heap allocation when decoding a crafted PNG or JPEG image. Both have vendor fixes available.

- Confirm Mirth Connect is at v4.7.2 or later everywhere it runs, including vendor-managed, embedded and inherited instances — it is frequently bundled inside integration products rather than separately procured
- Complete the credential rotation step for every downstream system credential stored in Mirth channel and connector configurations; this is the step most organizations will not do, and patching does not substitute for it
- Confirm Orthanc instances are at 1.13.0 or later, including research and teaching deployments stood up outside IT procurement
- Alert on the Mirth Connect Java process spawning a command shell or script interpreter — an integration engine has no legitimate reason to do this, making it a high-fidelity post-exploitation signal



Healthcare Sector Incident Watch

Smaller Providers Under Sustained Pressure

Alongside the large vendor incidents, a cluster of smaller provider breaches was reported this week and is worth noting as a pattern rather than individually. Cedar County Memorial Hospital in Missouri stated in a September 10 update that investigation and review of exposed data are continuing and that it has not yet confirmed the extent to which patient data was compromised; a relatively new cyber extortion and ransomware group calling itself Wallstreet claimed responsibility, added the hospital to its dark web leak site in late August, and threatened to publish stolen data. Hacking-related breaches were also reported by Next Level Medical in Texas and Grafton City Hospital in West Virginia, and separately by Hawaii Family Dental (approximately 46,000 individuals), Texas Hearing Institute (approximately 30,000 patients) and the Florida substance use disorder treatment provider Operation PAR (more than 145,700 individuals). None of these individually approaches the scale of the vendor breaches covered above, but collectively they describe the part of the sector with the least security resourcing absorbing steady pressure, including from newly formed extortion brands.

- If your organization is part of a health system with critical access or rural affiliates, review whether those sites have the same EDR coverage, backup validation and incident response access as the flagship facilities — in most systems they do not
- Track newly named extortion groups such as Wallstreet in your threat model; new brands frequently indicate affiliates migrating rather than new capability, which means established TTPs arriving under an unfamiliar name

Medical Device and IoT Security

CISA published no new ICS Medical Advisory between September 12 and 18, 2026. The agency did publish general ICS advisories on September 15 and 17, including ICSA-26-258-08 covering CareCam CM2507, which despite the product name is classified as an ICS Advisory rather than a medical advisory and sits outside medical device scope. The medical device workload is therefore unchanged and consists of two open patchable actions from September 10 — Mirth Connect and Orthanc, both covered in Priority Action 4 — plus the standing unpatched set.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Third consecutive week with GTI operation records confirming US healthcare victims — now three in a single week ▲ Historical intrusions surfacing: a healthcare compromise from October 2025 documented only now ▲ Medtech data exposure at scale: millions of records from a device manufacturer published by an extortion group ▲ Invoice-themed malvertising targeting finance and revenue-cycle staff as a healthcare entry route ▲ Public health authority identity used as a phishing lure by a destructive nation-state actor ► No new CISA medical advisory this window; two patchable advisories from September 10 remain open actions	3 GTI records with confirmed Healthcare targeting created this week — the highest count in any single window in this series 5 UNC6394 operation records released together on September 17, spanning July 2025 to September 2026 68 new GTI-verified IOCs across 8 records 7.1 million Baxter International records reportedly published by ShinyHunters 6.4 million unique email addresses reported in the McKesson stolen dataset CVE-2026-3650 (GDCM): NO PATCH — week 26; CVE-2026-56445 and CVE-2026-18844: NO PATCH

Sources: Google Threat Intelligence (GTI), CISA ICS Medical 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 Advisory index, CISA KEV Catalog, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-237A, HIPAA Journal, TechCrunch, BleepingComputer, HealthExec, Cedar County Memorial Hospital, McKesson, NVD / CVE Program / MITRE, NextGen Healthcare, Orthanc, Palo Alto Networks, Fortinet PSIRT