



Executive Summary

The dominant story this week is the escalating Abbott incident, which moved from a brief disclosure to a detailed extortion claim inside this coverage window — and which, if the claims hold, would represent one of the most consequential healthcare data thefts of 2026. ShinyHunters extended its publication deadline from July 18 to July 21 and told BleepingComputer it obtained access through vishing attacks against Abbott employees in mid-June, compromising a Microsoft Entra single sign-on account and pulling data from connected SaaS applications including ServiceNow, SharePoint, Databricks, and Coupa. That tradecraft is a near-exact match for GTI campaign CAMP.26.094 reported in the July 10 brief. Critically, none of the volume claims have been substantiated: no data had been published as of July 20 reporting, and Abbott maintains there has been no impact to customers, operations, or finances. Full detail and the confirmed-versus-claimed split are in the dedicated section below.

Two new GTI-verified campaigns are reported, both released as GTI intelligence on July 19, 2026. CAMP.26.098 is a PRC-nexus espionage campaign delivering the custom HEAVYMETAL payload through weaponized PDF decoys containing nested archives, with Healthcare and Telecommunications both GTI-confirmed as targeted industries — though targeting is confirmed only in Vietnam, China, and the Philippines, making this a monitoring and hash-blocking item for US organizations rather than an active-defense priority. CAMP.26.101 is a suspected China-nexus supply chain compromise in which the actor tampered with AOMEI's software update servers so that client auto-updaters downloaded malicious loaders, side-loading DLLs through the anyviewer and nitro pro binaries to run a Python C2 engine deploying SHINYROAD and ADAPTIX. GTI confirms Education and Technology targeting; healthcare is not confirmed, but this campaign was last seen July 20 — inside this window — and the auto-update trust chain it attacks runs through every healthcare IT estate.

Sector data and regulatory: the Identity Theft Resource Center published its H1 2026 report on July 22, recording 281 healthcare data breaches in the first half of 2026 (up from 270 a year earlier) and flagging a sevenfold rise in malicious insider incidents nationwide. Three vulnerabilities were added to the CISA KEV catalog on July 16 — two actively exploited unauthenticated command-injection flaws in Fortinet FortiSandbox and a critical SharePoint deserialization flaw — all three carry direct healthcare exposure and are tracked below. Medical Device: CISA published no new ICS Medical Advisory for a second consecutive week; GDCM enters week 18 without a patch. Regulatory: the HIPAA Security Rule (90 FR 800, RIN 0945-AA22) delay to July 2027 is re-verified and unchanged.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Technique	Targets	Priority Action
HEAVYMETAL Delivery via Weaponized PDF Decoys (CAMP.26.098)	Espionage (PRC-nexus)	Weaponized PDF decoy documents containing nested archives that deliver custom HEAVYMETAL payloads disguised as system documents; the nested-archive structure defeats single-layer attachment scanning and the system-document masquerade evades casual file inspection; activity observed January 8 – May 28, 2026; intelligence released July 19, 2026; 45 GTI IOCs, the majority of them file hashes (41)	Healthcare and Telecommunications — both GTI-confirmed. Targeted regions are Vietnam, China, and the Philippines; NO US targeting is GTI-confirmed for this campaign	HIGH (US: MONITOR) — Ingest the 41 file hashes into EDR and mail-gateway blocklists; ensure attachment scanning recurses into nested archives; alert on executables extracted from PDF-adjacent archives; prioritize for organizations with APAC operations, research partners, or shared infrastructure
AOMEI Update Server Hijack → SHINYROAD / ADAPTIX (CAMP.26.101)	Supply Chain / Software Update Compromise (China-nexus)	Actor tampered with update servers for legitimate AOMEI software, altering server configuration files so client automatic updaters downloaded malicious second-stage loader	GTI-confirmed: Education and Technology — US, Spain, Switzerland. Healthcare NOT GTI-	HIGH — Inventory AOMEI products (Backupper, AnyViewer, Partition Assistant) across IT



Campaign	Type	Key Technique	Targets	Priority Action
		archives; loaders abused the anyviewer and nitro pro binaries for DLL side-loading to run a Python command-and-control engine deploying the SHINYROAD and ADAPTIX payloads; loaders enforced target locale whitelisting as an operational guardrail; first seen May 26, LAST SEEN JULY 20, 2026 — inside this coverage window; GTIG states it is continuing to monitor this emerging campaign	confirmed; included on technology-relevance grounds (auto-update trust chain; AOMEI backup and AnyViewer remote-access tooling appear in healthcare IT and vendor support estates)	and vendor-managed endpoints; disable automatic updates for these products pending vendor confirmation; alert on DLL side-loading from anyviewer/nitro pro and on unexpected Python C2 processes

Top 3 Priority Actions This Week

1. [CRITICAL] Close the Vishing → Entra ID → SaaS Exfiltration Path

This is the week's highest-value action because two independent threads now point at the same attack path. In the July 10 brief, GTI campaign CAMP.26.094 documented helpdesk phone impersonation driving a Self-Service Password Reset, rogue MFA device and passkey registration in Entra ID, Graph API reconnaissance, and SAML SSO pivots into Salesforce, ServiceNow, SharePoint Online, and OneDrive. This week, ShinyHunters described to BleepingComputer an Abbott intrusion that began with vishing against employees in mid-June, compromised a Microsoft Entra SSO account, and harvested data from ServiceNow, SharePoint, Databricks, and Coupa. GTI has not attributed the Abbott incident to CAMP.26.094 and this brief does not claim they are the same operation — but the pattern match is close enough that the CAMP.26.094 control set should be treated as the specific countermeasure for the specific threat now hitting healthcare organizations, not as generic identity hygiene. ShinyHunters has previously been linked to incidents at iRhythm and Stryker, both medical device firms, and its documented tradecraft centers on social engineering, SSO and MFA abuse, OAuth token abuse, and SaaS data theft.

- Require out-of-band manager callback verification for every helpdesk-assisted password reset, MFA enrollment, and passkey registration — the single control that breaks this chain at step one
- Remove SMS as a self-service reset factor for privileged, clinical, and finance accounts; require phishing-resistant factors for recovery
- Audit all MFA devices and passkeys registered in the last 60 days against IT asset and HR records; rogue passkey registration is rarely reviewed and is the persistence mechanism in both threads
- Inventory what your Entra ID SSO actually federates to — Databricks and Coupa are named in the Abbott claims and are exactly the kind of connected SaaS that falls outside clinical-system security reviews
- Alert on Graph API bulk export jobs, mass SharePoint/OneDrive downloads, and audit-log purge events; run tabletop exercises on a vishing scenario with your service desk this quarter

2. [HIGH] Patch the Three July 16 KEV Additions — FortiSandbox and SharePoint

CISA added three actively exploited vulnerabilities to the Known Exploited Vulnerabilities catalog on July 16, 2026, with a July 19 remediation deadline for federal civilian agencies under Binding Operational Directive 26-04. Two affect Fortinet FortiSandbox: CVE-2026-25089 (Fortinet CNA record CVSS 9.8; PSIRT advisory 9.1; NVD has not scored it independently) is an unauthenticated OS command injection in the web UI, reported against the start-VNC feature, allowing shell metacharacter injection through JSON payloads with no authentication and low attack complexity; CVE-2026-39808 (CVSS 9.1) is a second command injection in the same product. Fortinet shipped



fixes in April and June respectively and has not publicly marked either as exploited, but CISA has confirmed in-the-wild exploitation; the security firm Defused observed exploitation attempts in mid-June and characterized one public exploit as likely broken. This is the third FortiSandbox flaw exploited in the wild in 2026. The third addition, CVE-2026-58644 (CVSS 9.8), is a SharePoint Server deserialization flaw — note the discrepancy worth modeling around: CISA describes an unauthorized attacker executing code over a network, while Microsoft's FAQ states the attacker needs at least Site Owner rights. FortiSandbox matters disproportionately in healthcare because it feeds verdicts to FortiGate, FortiMail, and FortiWeb — compromising it does not just breach one appliance, it corrupts detection decisions across the security stack.

- Patch FortiSandbox to 4.4.9+ or 5.0.6+ (Cloud/PaaS 5.0.6+) immediately; the CNA record lists 4.2 as affected without remediation guidance — contact Fortinet for migration if you run 4.2
- Restrict FortiSandbox management interface exposure to trusted networks; these are unauthenticated flaws, so network reachability is the whole exposure
- Because exploitation predates the KEV listing by roughly a month, treat internet-exposed instances as potentially compromised: review HTTP logs for malformed requests, check for new admin accounts, unexpected command execution, and configuration changes before assuming patching is sufficient
- Apply the SharePoint update for CVE-2026-58644 and re-check Site Owner assignments on clinical policy libraries and vendor collaboration portals

3. [HIGH] Harden the Software Auto-Update Trust Chain (CAMP.26.101)

GTI released intelligence on July 19 on a suspected China-nexus supply chain compromise in which the actor altered configuration files on update servers for legitimate AOMEI software, causing client automatic updaters to fetch malicious second-stage loader archives. Those loaders abused the anyviewer and nitro pro binaries for DLL side-loading, executing a Python command-and-control engine that deployed the SHINYROAD and ADAPTIX payloads. The actor built locale whitelisting into the loaders as an operational guardrail — a deliberate targeting control that also suppresses detonation in sandboxes outside the intended geography. GTI confirms Education and Technology targeting in the United States, Spain, and Switzerland, and states it is continuing to monitor the campaign; healthcare is not a confirmed industry. It is included here because the mechanism generalizes: AOMEI's Backupper, Partition Assistant, and AnyViewer remote-access tools appear across small clinical practices, imaging workstations, and vendor support estates, and an auto-updater is a trusted, silent, privileged code-execution path that most healthcare asset inventories do not track.

- Inventory AOMEI products across clinical, administrative, and vendor-managed endpoints — AnyViewer in particular, since remote-access tooling is both widely installed and directly abused in this chain
- Disable automatic updates for AOMEI products pending vendor confirmation that update infrastructure has been remediated; apply updates manually from verified sources in the interim
- Alert on DLL side-loading from anyviewer.exe and nitro pro binaries, and on Python interpreter processes making outbound connections from endpoints where Python is not a sanctioned tool
- Broaden the lesson: identify every application in your estate with a silent auto-updater running at elevated privilege, and require that vendors disclose update-channel integrity controls (code signing, pinned certificates) in procurement and BAA reviews

Medical Device and IoT Security

No New Medical Device Advisories — Second Consecutive Week



CISA published no new ICS Medical Advisory during the July 18–24 window; the most recent remains ICSMA-26-181-01 (OFFIS DCMTK, June 30), covered in the July 10 brief. CISA did publish general ICS advisories during the week, but none in the medical category. Re-verified this cycle against the CISA advisory pages: the pynetdicom advisory still states that the maintainer has not responded to requests to work with CISA, and GDCM remains unpatched at week 18. Three open-source DICOM library advisories therefore remain concurrently open, and the shared compensating control set — blocking DICOM ingestion from unauthenticated sources, imaging network segmentation, and file validation at the boundary — covers all three simultaneously. DCMTK is still the only one of the three with a patch path, making its completion the fastest available risk reduction in the imaging ingestion chain.

Two cross-cutting items with a medical device dimension this week. First, the FortiSandbox KEV entries (Priority Action 2) matter for biomedical estates because security appliances often sit between clinical VLANs and the enterprise network; a compromised sandbox distorts the verdicts that segmentation policies depend on. Second, the AOMEI update hijack (Priority Action 3) is a reminder that imaging workstations and biomedical support laptops frequently run third-party backup and remote-access utilities outside the managed software catalogue — those auto-updaters are an unmonitored privileged code path into the clinical environment.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Vishing → Entra ID SSO → SaaS mass exfiltration: now the dominant healthcare data-theft pattern (Abbott claims; CAMP.26.094 pattern match) ▲ Software update / supply chain compromise: AOMEI update servers hijacked; auto-update trust chain under attack (CAMP.26.101) ▲ Malicious insider incidents: 21 in H1 2026 vs 3 in all of 2025 — a sevenfold rise (ITRC) ▲ Actively exploited security-appliance flaws: three new KEV entries July 16, two in FortiSandbox ► Medical device advisories: no new ICSMA for a second consecutive week; three DICOM library advisories still open ▼ Breach transparency: only 24% of H1 2026 notices disclosed how the breach occurred, down from 100% in 2020 (ITRC)	281 healthcare data breaches in H1 2026, up from 270 in H1 2025 (ITRC, published July 22) 11.7M healthcare victim notices in H1 2026 — below the 34.6M full-year 2025 pace 471.2M individuals affected across all US sectors in H1 2026 — already above all of 2025 (297.5M) 72 new GTI-verified IOCs across 2 campaigns Abbott / ShinyHunters: claims of 30M+ PII rows, 1M+ SSNs, 22M+ doctor-patient notes — ALL UNVERIFIED; no data published as of July 20 CVE-2026-3650 (GDCM): NO PATCH — week 18; CVE-2026-56445 (pynetdicom): NO PATCH

Sources: Google Threat Intelligence (GTI), CISA (KEV Catalog July 16 alert; ICS Medical Advisories ICSMA-26-181-01, -176-01, -176-02, -083-01; BOD 26-04), Abbott Newsroom (official statement), BleepingComputer, Cybernews, DataBreaches.net, HIPAA Journal, Malwarebytes, The Register, Identity Theft Resource Center (H1 2026 report), Becker's Hospital Review, Fortinet PSIRT, Microsoft Security Response Center, NVD / CVE Program, Davis Wright Tremaine, Clark Hill, Clearwater, Medcurity