



Executive Summary

Two GTI-verified campaigns are reported this week, both released as new GTI intelligence on July 10, 2026. CAMP.26.069 is a highly active, Russia-nexus initial access campaign using ClickFix social engineering to execute hidden-window PowerShell that delivers the NEONSLIDE downloader and the CURLYGATE and CURLYFENCE payloads — Healthcare is a GTI-confirmed targeted industry, and the campaign carries 354 IOCs, the largest single-campaign IOC set in this series since April. CAMP.26.094 is a financially motivated identity attack chaining helpdesk phone impersonation and Self-Service Password Reset (SSPR) abuse into full Entra ID account takeover — including rogue passkey registration for persistent MFA bypass — followed by Microsoft Graph API reconnaissance, bulk data exports with log purging, and SAML SSO pivots into Salesforce, ServiceNow, SharePoint Online, and OneDrive. GTI confirms Manufacturing, Retail, and Technology targeting; healthcare is not yet confirmed, but the tradecraft is a direct evolution of the hospital helpdesk attacks reported in the May 8 brief, and activity was last observed July 10.

Major breach development: the Conduent Business Services breach from 2025, a back-office vendor processing documents, claims, and payments for health plans and government agencies, has been confirmed on the HHS OCR breach portal at 62,224,658 affected individuals, making it the third-largest healthcare data breach on record behind Change Healthcare (192.7M) and Anthem (78.8M). The figure, reported to OCR on June 4 and widely covered through July 9, more than doubles the 25M estimate from February 2026 and is a defining case study in Business Associate concentration risk.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Technique	Targets	Priority Action
ClickFix → NEONSLIDE → CURLYGATE Initial Access (CAMP.26.069)	Initial Access / Financial (Russia-nexus)	ClickFix social engineering lures trick victims into running heavily obfuscated, hidden-window PowerShell; secondary payloads include a PowerShell downloader, CURLYGATE, CURLYFENCE, and the NEONSLIDE downloader; post-exploitation payload staging, dynamic code compilation via CSC.EXE to evade static signatures, and C2 beaconing; GTI describes this as a highly active initial access threat; activity observed April 15 – June 3, 2026; intelligence released July 10	Healthcare + 9 other GTI-confirmed industries (Financial Services, Technology, Manufacturing, Legal, Media, Automotive, others) — US, CA, FR, CH, KR + others	HIGH — Block/alert on hidden-window PowerShell spawned from browsers; alert on csc.exe compilation outside developer hosts; train staff on ClickFix CAPTCHA/verification lures; hunt the 354 GTI IOCs
Helpdesk Impersonation → SSPR Abuse → Entra ID / SaaS Mass Exfiltration (CAMP.26.094)	Credential Theft / Data Exfiltration	Phone impersonation of the IT helpdesk tricks an employee into a Self-Service Password Reset with SMS verification; actor hijacks the Entra ID identity, registers a rogue MFA device and rogue passkey for persistence; Microsoft Graph API used for directory reconnaissance and bulk data export jobs with log purging; Azure federated SAML SSO pivot into SaaS — Salesforce /aura report exports (customer/lead/opportunity data), ServiceNow user/computer lists, tens of thousands of SharePoint Online / OneDrive files downloaded; active June 7 – July 10, 2026	GTI-confirmed: Manufacturing, Retail, Technology — US. Healthcare NOT yet GTI-confirmed; included because the vector directly mirrors hospital helpdesk targeting (UNC3944, May 8 brief)	HIGH — Require out-of-band manager callback for all SSPR/MFA resets; disable SMS as an SSPR factor for privileged/clinical users; alert on new passkey and MFA device registrations; monitor Graph API bulk exports and audit-log purge events



Top 2 Priority Actions This Week

1. [HIGH] Defend Against ClickFix → NEONSLIDE → CURLYGATE Initial Access (CAMP.26.069)

GTI released intelligence on July 10 describing a highly active initial access campaign, attributed to a Russia-nexus, financially motivated actor, observed April 15 through June 3, 2026. ClickFix lures — fake verification prompts that instruct users to paste commands — trick victims into executing heavily obfuscated PowerShell with hidden windows, which retrieves a PowerShell downloader, CURLYGATE, CURLYFENCE, and NEONSLIDE. Post-exploitation activity includes payload staging, dynamic compilation of code using the native C# compiler CSC.EXE to evade static signatures, and C2 beaconing. Healthcare is a GTI-confirmed targeted industry among ten, with victims in the US and globally. The campaign carries 354 IOCs (9 files, 1 IP, 95 domains, 249 URLs). This is the third ClickFix-linked campaign relevant to this series (after CAMP.26.064's NetSupport chain and CAMP.26.059's VIDAR chain), confirming ClickFix as the dominant social engineering pattern of 2026: NEONSLIDE is shared with CAMP.26.059, but this is a distinct campaign with a different payload set.

- Alert on PowerShell launched with hidden-window/encoded-command parameters from browser or Explorer parent processes — the ClickFix execution signature
- Alert on csc.exe compilation events outside known developer workstations — dynamic compilation on clinical or business endpoints is a high-fidelity signal
- Ingest the 354 GTI IOCs (95 domains, 249 URLs) into web filtering and SIEM watchlists
- Refresh user training on ClickFix: no legitimate CAPTCHA or verification page ever asks users to copy commands into a terminal or the Run dialog

2. [HIGH] Harden Helpdesk SSPR and Passkey Registration Against Identity Takeover (CAMP.26.094)

GTI released intelligence on July 10 on a financially motivated campaign, active June 7 through July 10, 2026, that begins with a phone call impersonating the IT helpdesk. The actor talks an employee through a Self-Service Password Reset with SMS verification, hijacking the Entra ID identity, then registers both a rogue MFA device and a rogue passkey — a notable escalation, since passkeys are often treated as inherently trustworthy and are rarely audited. With persistent access secured, the actor conducts Microsoft Graph API reconnaissance (directory configuration, device counts, user privileges), initiates bulk data export jobs, and purges logs to evade detection, then pivots via Azure federated SAML SSO into connected SaaS: executing Salesforce /aura report exports of customer, lead, and opportunity data, pulling ServiceNow user and computer lists, and downloading tens of thousands of files from SharePoint Online and OneDrive. GTI confirms Manufacturing, Retail, and Technology targeting in the US; healthcare is not yet confirmed, but this is the same helpdesk-manipulation playbook UNC3944 used against hospital IT helpdesks (May 8 brief), now with SSPR abuse and passkey persistence added. Hospital helpdesks should treat it as directly applicable tradecraft.

- Require out-of-band manager callback verification for every SSPR-assisted reset and MFA/passkey enrollment — no exceptions for urgency claims
- Remove SMS as an SSPR verification factor for privileged, clinical, and finance accounts; require phishing-resistant factors
- Audit and alert on new passkey registrations — review all passkeys and MFA devices enrolled in the past 30 days against IT records
- Alert on Graph API bulk export jobs, mass SharePoint/OneDrive downloads, and audit-log deletion events; log purging is itself a detection
- Review Salesforce /aura endpoint activity and ServiceNow export logs if federated SSO connects them to Entra ID



Medical Device and IoT Security

Medical Device & Imaging: CISA published ICSMA-26-181-01 on June 30 covering five vulnerabilities in the OFFIS DCMTK Toolkit ($\leq 3.7.0$) — one critical (CVE-2026-50003, CVSS 9.8 path traversal) and four high. DCMTK is one of the most widely used DICOM implementations in the world (~100,000 downloads/year, embedded in commercial viewers, archives, and worklist/storage servers), making this the third open-source DICOM library advisory in three weeks after GDCM and pydicom/pynetdicom — unlike those two, DCMTK fixes ARE available.

Top Priority Action This Week

1. [CRITICAL] Patch OFFIS DCMTK Across the Imaging Estate — ICSMA-26-181-01

On June 30, 2026, CISA published medical advisory ICSMA-26-181-01 covering five vulnerabilities in the OFFIS DCMTK Toolkit, versions 3.7.0 and earlier. The critical flaw, CVE-2026-50003 (CVSS 9.8 v3.1 / 9.3 v4.0, CWE-22 path traversal), allows a malicious or compromised DICOM server to make a DCMTK client using bit-preserving C-GET storage mode write files outside the chosen output directory using `../` or absolute paths — a route to arbitrary file writes on imaging hosts. The four accompanying high-severity CVEs (CVE-2026-50254, CVE-2026-35505, CVE-2026-52868, CVE-2026-44628) enable unauthorized information access (including modality worklist data, which can contain PHI), memory exhaustion, and client/server crashes. No exploitation has been observed, and GTIG rates the practical priority of CVE-2026-50003 as P3/Medium because the vulnerable storage mode is not the default — but exposure is broad: DCMTK is one of the most widely used DICOM implementations in the world, downloaded roughly 100,000 times per year and embedded inside commercial viewers, archives, and worklist and storage servers. Unlike GDCM and pynetdicom, fixes exist: OFFIS has committed patches upstream, and CISA directs users to the latest patched GitHub snapshot.

- Update standalone DCMTK installations to the latest patched snapshot per the CISA advisory; Red Hat/Fedora and Debian are tracking distribution packages
- Inventory embedded DCMTK: query PACS, viewer, worklist, and storage-server vendors for DCMTK usage and their remediation timeline — embedded copies are the majority of real-world exposure
- Disable or avoid bit-preserving C-GET storage mode where not required — this removes the critical file-write path entirely
- Apply the standing DICOM ingestion-path controls: block DICOM from unauthenticated sources, segment imaging networks, and validate files at the boundary — the same control set already deployed for GDCM and pynetdicom
- Document vendor responses for HIPAA risk-analysis records, as with the two open no-patch DICOM advisories

Persistent CVE Tracker

CVE	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-50003 (NEW)	OFFIS DCMTK Toolkit $\leq 3.7.0$ (DICOM library)	9.8	CISA ICSMA-26-181-01 (Jun 30)	Yes	Path traversal (CWE-22): a malicious or compromised DICOM server can make a DCMTK client using bit-preserving C-GET storage mode write files outside the chosen output directory via <code>../</code> or absolute paths. No known exploitation; GTIG rates real-world priority P3/Medium because the vulnerable mode is non-default. OFFIS committed fixes upstream — update to the latest patched DCMTK snapshot per CISA; inventory embedded DCMTK in commercial viewers/archives.



CVE	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-50254 / -35505 / -52868 / -44628 (NEW)	OFFIS DCMTK Toolkit ≤3.7.0	High	CISA ICSMA-26-181-01 (Jun 30)	Yes	Four additional high-severity flaws in the same advisory: unauthorized information access (incl. worklist data that can contain PHI), memory exhaustion, and client/server process crashes. Same fix path as CVE-2026-50003.
CVE-2026-56445	pydicom / pynetdicom qrscp (DICOM C-STORE)	9.1	CISA ICSMA-26-176-01	NO	Unauthenticated path traversal / arbitrary file write. NO vendor fix — CISA reports the pynetdicom maintainer has not responded; releases through v3.0.4 affected. Restrict DICOM port access, segment, monitor the GitHub project for a fixed release.
CVE-2026-3650	Grassroots DICOM (GDCM) 3.2.2	7.5	CISA ICSMA-26-083-01	NO	Week 16 with no patch — maintainer remains unresponsive to CISA. Maintain PACS segmentation, block unauthenticated DICOM ingestion, continue escalating with imaging vendors.
CVE-2026-22879	vtk-dicom 9.5.2 (VTK DICOM toolkit)	8.1	Cisco Talos TALOS-2026-2366	Yes	Heap overflow via crafted DICOM file (June 25). Confirm your distribution/package has shipped the fix in imaging/research pipelines.
CVE-2026-12473	OHIF DICOM Web Viewer	8.2	CISA ICSMA-26-176-02	Yes	SSRF; patched in OHIF v3.12.2. Confirm deployment on all OHIF instances.
CVE-2026-0611	Spacelabs Sentinel cardiac monitoring	9.8	June 12 brief	Yes	Unauthenticated RCE; patched in v11.6.0. Confirm deployment complete.
CVE-2026-43994	coturn TURN/STUN (telehealth WebRTC)	8.1	June 19 brief	Yes	Stack buffer overflow in OAuth token decoding; patch to coturn 4.10.0 across 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.

HIPAA Security Rule Regulatory Update

90 FR 800 — MAJOR UPDATE: Final Action Delayed to At Least July 2027

A significant change this week. HHS's updated federal regulatory agenda, released the week of July 6–10, 2026, moves final action on the HIPAA Security Rule update (90 FR 800, NPRM published January 6, 2025) to at least July 2027 — a one-year slip from the previously targeted May 2026. The rulemaking's status has changed from 'final rule stage' to 'long term actions,' and it no longer appears on the 2026 Agency Rule List. Legal analysts note the new date signals HHS still intends to finalize at least some of the proposed amendments, with expectations that only a subset — likely the less controversial, highest-risk-reduction provisions — will survive. Separately, HHS is prioritizing HIPAA Privacy Rule amendments (care-coordination provisions), with a final rule expected as early as August 2026, and a proposed right-of-access rulemaking in November 2026.

What does not change: the current HIPAA Security Rule remains fully in effect and actively enforced. OCR has formally expanded its enforcement initiative beyond risk analysis to include risk



management — what organizations actually do about identified risks — and risk analysis failures remain the most-cited deficiency in OCR investigations. The delay is runway to build the program the proposed rule anticipates (encryption, MFA, segmentation, incident response), not a reason to pause. This item will continue to be re-verified each brief cycle.

Update on Conduent Confirmed at 62.2 Million from a breach that was discovered in Jan 2025

The HHS OCR breach portal now confirms that the Conduent Business Services breach affected 62,224,658 individuals which is the third-largest healthcare data breach ever recorded, behind only Change Healthcare (192.7M, 2024) and Anthem (78.8M, 2015). Conduent, a New Jersey-based business process outsourcing firm providing printing, mailing, document processing, payment integrity, and back-office support to health plans, government agencies, and large employers, discovered on January 13, 2025 that attackers had access to its network from October 21, 2024. The SafePay ransomware group claimed responsibility, asserting theft of multiple terabytes of data; exposed information includes Social Security numbers, medical information, and health insurance data. The total has climbed relentlessly — roughly 10.5M when first reported, 25M by February 2026 state disclosures (15.4M in Texas alone), and now 62.2M in the figure Conduent reported to federal regulators on June 4. Conduent reported \$25M in direct breach-response costs in Q1 2025 with a further \$16M anticipated, and state investigations remain active in Missouri and Texas. Determine exposure: if your organization or your health plan partners use Conduent for claims, printing/mailing, or payment integrity, request written notification-status confirmation now

Threat Metrics

Activity Trends	Key Numbers This Week
▲ ClickFix social engineering as initial access: highly active (CAMP.26.069 — 354 IOCs; third ClickFix-linked campaign in the series) ▲ Helpdesk/SSPR identity attacks pivoting into SaaS: escalating — now with rogue passkey registration for persistence ▲ Medical imaging (DICOM) library CVE disclosures: 5 new (DCMTK) — third open-source DICOM library advisory in three weeks ▲ Third-party/vendor breach totals: Conduent revised to 62.2M — 3rd-largest healthcare breach on record ► Healthcare ransomware activity: sustained — no material change vs. prior week ▼ HIPAA Security Rule finalization: delayed to at least July 2027	CVE-2026-50003 (DCMTK): CVSS 9.8 (v3.1) / 9.3 (v4.0) — patch available 358 new GTI-verified IOCs across 2 campaigns 62,224,658 individuals — Conduent breach total confirmed on the HHS OCR portal CVE-2026-3650 (GDCM): NO PATCH — week 16; CVE-2026-56445 (pynetdicom): NO PATCH CISA KEV addition June 29: CVE-2026-48558 (SimpleHelp RMM authentication bypass) — verify any SimpleHelp use by vendors/MSPs HIPAA Security Rule 90 FR 800: final action moved to ≥ July 2027

Source: Google Threat Intelligence (GTI), CISA (ICSMA-26-181-01; KEV Catalog), HHS OCR breach portal, OFFIS, NVD, MITRE / CVE Program, Red Hat, Debian, OSS-Sec, HIPAA Journal, GovInfoSecurity / BankInfoSecurity (ISMG), Davis Wright Tremaine, Paubox, Cybersecurity Dive, Becker's Hospital Review, Radiology Business