



Executive Summary

Two new GTI-verified campaigns are reported this week. The most directly healthcare-relevant is CAMP.26.102 (intelligence released July 23), a ClickFix social engineering cluster attempting to deploy the LUMMAC and VIDAR data theft tools. Both Healthcare and Pharmaceuticals are GTI-confirmed among thirteen targeted industries, and the United States is confirmed among six targeted regions — making this the clearest healthcare-confirmed record of the week. LUMMAC and VIDAR harvest browser-stored credentials, session cookies, and authentication tokens, which makes any detection a credential-compromise event rather than a malware-cleanup task.

The second new record, CAMP.26. is a stealth-oriented intrusion campaign that gains access through remote code execution against IIS web servers by exploiting deserialization vulnerabilities on a vulnerable ASP.NET endpoint, then persists through SLATEVINE, a custom C++ IIS backdoor module, alongside IRONBARK, a C-based kernel-level rootkit used to hide running processes and registry keys. GTI confirms Government as the only targeted industry, so healthcare targeting is not established — but IIS and ASP.NET host patient portals, PACS web front-ends, scheduling systems, and vendor integration endpoints across healthcare, and GTI maps an unusually broad 91 ATT&CK techniques to this campaign. The transferable concern is the persistence model: a kernel rootkit means on-host process and registry visibility can be defeated, so findings need corroboration from network and out-of-band telemetry.

The third item is advisory-sourced: joint Cybersecurity Advisory AA26-204A, published July 23 by CISA, the NSA, the FBI, the UK NCSC and agencies from more than a dozen allied nations, documents Russian state-supported actor LAUNDRY BEAR exploiting CVE-2025-66376 in Zimbra Collaboration Suite webmail — a zero-click flaw in which merely viewing a malicious email in a vulnerable version enables theft of email data, credentials, and two-factor authentication tokens. Healthcare and Public Health is not among the sectors named in the advisory, so it is carried here as an email-infrastructure action item for any organization running ZCS rather than as a healthcare-targeted campaign. Medical Device: CISA published no new ICS Medical Advisory for a third consecutive week, and GDCM reaches week 19 without a patch.

Active Threat Campaigns- Healthcare & Technology

Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
ClickFix Lures Delivering LUMMAC and VIDAR Infostealers (CAMP.26.102)	Credential / Data Theft (infostealer)	ClickFix social engineering lures used to attempt deployment of the LUMMAC and VIDAR data theft tools — commodity infostealers that harvest browser-stored credentials, session cookies, and authentication tokens. Short, sharp activity window: first observed July 8 and last observed July 15, 2026. GTI records only 8 associated ATT&CK techniques and a single IOC (one domain), indicating an early-stage or narrowly-observed cluster rather than a fully mapped operation; intelligence released July 23, 2026	Healthcare AND Pharmaceuticals both GTI-confirmed, among 13 confirmed industries — United States confirmed, plus Germany, France, India, South Korea, UAE	HIGH — Alert on hidden-window/encoded PowerShell from browser parents (the ClickFix signature); treat any LUMMAC or VIDAR detection as a credential-compromise event, not a cleanup task: force password resets and revoke sessions/tokens for the affected user immediately
IIS Exploitation → SLATEVINE Backdoor + IRONBARK Kernel Rootkit	Targeted Intrusion / Stealth Persistence	Initial access via remote code execution against Internet Information Services (IIS) web servers, exploiting deserialization vulnerabilities on a vulnerable ASP.NET endpoint (/Portal/FeedOrg.aspx). Post-	GTI-confirmed: Government — United States and Chile. Healthcare NOT GTI-confirmed; included on	HIGH — Inventory internet-facing IIS/ASP.NET applications and patch deserialization flaws; alert on



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
(CAMP.26.106)		exploitation: created local administrator accounts, enabled RDP, and used icacis to grant public permissions on IIS system files. Persistence via SLATEVINE, a custom C++ IIS backdoor module registered through appcmd, plus IRONBARK, a C-based kernel-level rootkit that hides running processes and registry keys. Credential harvesting via LSASS memory dumps and WDigest registry modification; WinRAR and Hidden.inf installers abused to stage tooling; C2 over encrypted TCP tunnels and DNS lookups to actor-controlled domains. Activity observed November 12, 2025 – June 26, 2026; 91 mapped ATT&CK techniques; intelligence released July 28, 2026	technology-relevance grounds: IIS/ASP.NET hosts patient portals, PACS web front-ends, and vendor integration endpoints across healthcare	appcmd module registration, new local admin accounts, RDP enablement, and icacis permission changes on IIS directories; a kernel rootkit means host-based tooling may be blinded — validate from network telemetry and out-of-band
LAUNDRY BEAR — Zimbra Zero-Click Email Exfiltration (Joint CSA AA26-204A, July 23)	Nation-State / Espionage (Russia)	Exploitation of CVE-2025-66376, a cross-site scripting flaw in the Zimbra Collaboration Suite Classic UI webmail arising from insufficient sanitization of CSS @import directives in email content. CISA describes the current campaign as a zero-click exploit requiring only that a user view a malicious email in a vulnerable webmail version (Proofpoint characterizes it as 'half-click'). Activity dates to at least July 2025 — Synacor patched in November 2025 and the flaw was publicly documented in January 2026, meaning it was a zero-day when first operationalized. More than 10 organizations were successfully targeted, with email addresses, passwords, and 2FA tokens exfiltrated or targeted for exfiltration	Sectors named in the advisory: Defense Industrial Base, federal and local government, law enforcement, technology, education, media, NGOs. Healthcare is NOT among the named sectors — included as an email-infrastructure action item for any organization running ZCS	HIGH (if ZCS in use) — Confirm Zimbra Collaboration Suite is patched past November 2025 for CVE-2025-66376; treat any unpatched Classic UI instance as compromised and hunt using the AA26-204A STIX IOC packages; force password resets and revoke 2FA tokens for affected mailboxes

Top 3 Priority Actions This Week

1. [HIGH] Patch and Hunt Zimbra Collaboration Suite — Zero-Click Exploitation (AA26-204A)

On July 23, 2026, CISA, the NSA, the FBI, the UK's National Cyber Security Centre and agencies from more than a dozen allied nations published joint Cybersecurity Advisory AA26-204A attributing a sustained espionage campaign to a Russian state-supported group tracked primarily as LAUNDRY BEAR — a designation originally coined by the Netherlands' AIVD and MIVD — and also as Void Blizzard, CL-STA-1114, and TA488. The group has exploited CVE-2025-66376, a cross-site scripting vulnerability in the Zimbra Collaboration Suite Classic UI arising from insufficient sanitization of CSS @import directives in email content, since at least July 2025. What makes this operationally unusual is the interaction model: CISA describes the current campaign as using a zero-click exploit that requires only that a user view a malicious email in a vulnerable webmail version, with no link to click and no attachment to open (Proofpoint, which published coordinated findings the same day, characterizes it as a half-click exploit). More than ten organizations were successfully targeted, with email addresses, passwords, and two-factor authentication tokens exfiltrated or targeted. Synacor patched the flaw in November 2025 and it was publicly documented in January 2026 — so it was a genuine zero-day when first operationalized, and victims continued to be compromised after a fix



existed. Healthcare and Public Health is not among the sectors named in the advisory; the sectors listed are Defense Industrial Base, federal and local government, law enforcement, technology, education, media, and non-governmental organizations. This is carried here because ZCS is a self-hosted webmail platform that does appear in healthcare and academic medical environments, and because the control lesson generalizes to any webmail platform.

- Determine whether Zimbra Collaboration Suite is running anywhere in your estate — including legacy, research, or acquired-entity environments; self-hosted webmail is a classic shadow-IT survivor
- Confirm patch level is past the November 2025 fix for CVE-2025-66376, and prioritize any instance still serving the Classic UI
- Retro-hunt using the STIX XML and STIX JSON IOC packages published with AA26-204A rather than assuming patching closes the exposure — exploitation predates the patch by months
- If compromise is suspected, force password resets and revoke 2FA tokens for affected mailboxes; stolen 2FA tokens survive a password change
- Generalize the lesson: a zero-click webmail exploit defeats user training entirely, so webmail platform patch cadence should be tracked with the same rigor as VPN and firewall patching

2. [HIGH] Prepare for Kernel-Level Persistence Behind Web-Facing Servers (CAMP.26.106)

GTI released intelligence on July 28 describing a stealth-oriented intrusion campaign against public sector infrastructure, observed from November 12, 2025 through June 26, 2026 in the United States and Chile. Initial access came via remote code execution against Internet Information Services web servers, exploiting deserialization vulnerabilities on a vulnerable ASP.NET endpoint (/Portal/FeedOrg.aspx). The actor then created local administrator accounts, enabled RDP, and used `icacls` to grant public permissions to IIS system files. Persistence was established through two custom capabilities. WinRAR and Hidden.inf installers were abused to stage tooling, and command and control ran over encrypted TCP tunnels and DNS lookups to actor-controlled domains. GTI maps 91 ATT&CK techniques to this campaign, an unusually broad footprint. GTI confirms Government as the only targeted industry, so healthcare targeting is not established — but IIS and ASP.NET host patient portals, PACS web front-ends, scheduling systems, and vendor integration endpoints throughout healthcare, and the persistence model here is the transferable concern.

- Inventory internet-facing IIS/ASP.NET applications, including vendor-supplied clinical web front-ends, and confirm deserialization vulnerabilities are patched — this class of flaw is a recurring initial-access vector
- Alert on IIS module registration via `appcmd`, new local administrator account creation, RDP enablement, and `icacls` permission changes against IIS directories; these are high-fidelity, low-noise signals
- Alert on WDigest registry modification (UseLogonCredential) — there is almost no legitimate reason to re-enable plaintext credential caching in a modern environment
- Assume host-based tooling can be blinded: where a kernel rootkit is plausible, validate findings from network telemetry, DNS logs, and out-of-band sources rather than trusting on-host process listings

3. [HIGH] Treat LUMMAC and VIDAR Detections as Credential Compromise (CAMP.26.102)

GTI released intelligence on July 23 on a ClickFix social engineering campaign attempting to deploy the LUMMAC and VIDAR data theft tools. Activity was observed between July 8 and July 15, 2026. GTI confirms thirteen targeted industries including both Healthcare and Pharmaceuticals, with targeting confirmed in the United States, Germany, France, India, South Korea, and the UAE. Two honest caveats: GTI has mapped only eight ATT&CK techniques and a single IOC (one domain) to this record, and no motivation is assigned — this is a thin, early-stage record rather than a fully characterized operation, so the behavioral guidance below carries far more defensive weight than the indicator. What justifies its priority is the payload class. LUMMAC and VIDAR are commodity infostealers that harvest browser-stored credentials, session cookies, and authentication tokens; a



successful execution means valid credentials and live sessions are already in an attacker's hands, and stolen session cookies bypass MFA on replay. In a healthcare context that means clinician EHR sessions, payer portals, and administrative SaaS access. This is the fourth distinct ClickFix-linked campaign tracked in this series since June — CAMP.26.069 (July 10 brief), CAMP.26.092 and CAMP.26.095 (July 3 and July 17), and now this one — which makes ClickFix the most persistent initial-access pattern of the period.

- Alert on PowerShell launched with hidden-window or encoded-command parameters from browser or Explorer parent processes — the consistent ClickFix execution signature across all four campaigns
- Treat any LUMMAC or VIDAR detection as a credential-compromise incident: force a password reset AND revoke all active sessions and refresh tokens for the affected user, because reimaging the endpoint alone leaves stolen cookies valid
- Prioritize browser credential hygiene on clinical and administrative endpoints — disable browser password managers where an enterprise vault is available, since browser-stored credentials are the primary target of both families
- Refresh ClickFix user training: no legitimate CAPTCHA, verification page, or system update ever asks a user to paste a command into the Run dialog or a terminal
- Pharmaceutical and research partners are in scope too — Pharmaceuticals is GTI-confirmed for this campaign, so extend the advisory to clinical trial and research collaborators

Medical Device and IoT Security

No New Medical Device Advisories — Third Consecutive Week

One adjacent OT item worth logging: CISA and international partners released an updated advisory on July 22 concerning Iranian-affiliated cyber actors targeting internet-connected programmable logic controllers. PLCs are not clinical devices, but they run building management, HVAC, and utility systems inside hospital campuses, and the OT-to-clinical lateral movement concern that has run through this series since the March 6 brief applies directly. Confirm that building-automation networks are segmented from clinical and medical device VLANs, and that internet-exposed PLCs in facilities estates are inventoried and access-controlled.

Persistent CVE and KEV Tracker

CVE	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2025-66376 (NEW)	Zimbra Collaboration Suite — Classic UI webmail	See note	Joint CSA AA26-204A (Jul 23)	Yes	Cross-site scripting via unsanitized CSS @import directives; exploited zero-click by LAUNDRY BEAR since at least July 2025 to steal email data, credentials, and 2FA tokens. Synacor patched November 2025. NOT currently listed in the CISA KEV catalog per this week's review — the authority here is the joint advisory. Confirm ZCS patch level; hunt with the advisory's STIX IOCs.
CVE-2026-25089 / CVE-2026-39808	Fortinet FortiSandbox (incl. Cloud and PaaS)	9.8 / 9.1	CISA KEV (Jul 16)	Yes	Two unauthenticated OS command injection flaws, actively exploited since mid-June; FCEB deadline was July 19. Fixed in 4.4.9+, 5.0.6+, Cloud/PaaS 5.0.6+. Because exploitation predates the KEV listing, treat internet-exposed instances as potentially compromised and hunt before assuming patching is sufficient.
CVE-2026-58644	Microsoft SharePoint Server	9.8	CISA KEV (Jul 16)	Yes	Deserialization of untrusted data. CISA describes network code execution; Microsoft's FAQ states the attacker needs at least Site Owner rights — model both. Re-check Site



CVE	System / Component	CVSS	Advisory	Patch	Status & Action
					Owner assignments on clinical policy libraries and vendor portals.
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. Still the ONLY open DICOM library advisory with a patch path — completing it (standalone plus vendor-embedded copies) remains the fastest available risk reduction in the imaging ingestion chain.
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. Re-verified against the CISA advisory this week: the maintainer has still not responded to requests to work with 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 19 with no patch. Memory leak when parsing malformed DICOM files with non-standard VR types in file meta information, leading to resource depletion and denial of service. Maintain PACS segmentation and block unauthenticated DICOM ingestion.
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. Confirm your distribution/package has shipped the fix in imaging and research pipelines.
CVE-2026-12473	OHIF DICOM Web Viewer	8.2	CISA ICSMA-26-176-02	Yes	SSRF; patched in v3.12.2. Also remove unused DicomWebProxy/DicomJSON data source configurations in authenticated deployments.
CVE-2026-48558	SimpleHelp RMM (vendor remote support)	KEV	CISA KEV (Jun 29)	Yes	Authentication bypass. Verify whether any vendor or MSP remote-access path into your environment uses SimpleHelp, and confirm patching.
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
▲ Infostealer delivery against healthcare and pharmaceuticals: LUMMAC and VIDAR via ClickFix (CAMP.26.102) ▲ Nation-state exploitation of email infrastructure: zero-click Zimbra webmail exploitation (AA26-204A)	13 GTI-confirmed targeted industries for CAMP.26.102 — including both Healthcare and Pharmaceuticals, with US targeting confirmed More than 10 organizations successfully targeted in the LAUNDRY BEAR ZCS campaign (AA26-204A)



Activity Trends	Key Numbers This Week
▲ Kernel-level persistence: IRONBARK rootkit + IIS backdoor module — host-based visibility can be defeated ▲ ClickFix as infostealer delivery: fourth distinct ClickFix-linked campaign tracked in this series since June ► Medical device advisories: no new ICSMA for a THIRD consecutive week; three DICOM library advisories still open	8 new GTI-verified IOCs across 2 campaigns — a deliberately low-IOC week; both records are thin on indicators 91 ATT&CK techniques mapped to CAMP.26.106 — an unusually broad tradecraft footprint CVE-2025-66376: exploited from at least July 2025; patched November 2025; publicly documented January 2026 CVE-2026-3650 (GDCM): NO PATCH — week 19; CVE-2026-56445 (pynetdicom): NO PATCH

Sector Baseline — GTI Healthcare Industry Snapshot

The following is drawn from the Google Threat Intelligence “Industry Snapshot: Healthcare” profile (collection industry-profile--healthcare). Read it as strategic context, not as this week’s telemetry: the profile covers a two-year observation window from March 1, 2024 to March 1, 2026, and the record was last modified June 8, 2026. GTI assigns “possible” confidence — not “confirmed” — to the industry and region attributions in this profile, so the figures below describe the shape of sector targeting rather than establishing specific victims. Two fields in the profile were empty when queried (the generated threat-activity-drivers text and the OSINT summary), so nothing is reported from them.

Threat Source Country	Actors / Campaigns	Targeted Country	Share of Observed Targeting
China	18	United States	7.2%
Russia	13	Canada	4.1%
North Korea	7	United Kingdom	3.4%
Brazil	5	Switzerland	2.8%
Mexico	4	France	2.6%
Iran	4	Australia	2.1%
Canada	2	Germany	1.5%
Vietnam	1	Singapore	1.5%
Italy	1	Hong Kong	1.4%

Source counts are GTI’s tally of distinct threat actors and campaigns attributed to each origin country across the window. Targeting shares are percentages of all observed targeting references; the profile lists overlapping region, sub-region, and country entries, so only country-level values are reproduced here and the column does not total 100%. Regional roll-ups for reference: Americas 7.4%, Europe 5.9%, Asia 3.9%, Oceania 2.3%, Africa 1.1%.

Sources

Nine origin countries account for the observed activity, and three dominate: China (18 actors/campaigns), Russia (13), and North Korea (7) together represent roughly two-thirds of the total. Iran contributes 4. The notable second tier is Latin American and financially driven rather than state-driven — Brazil (5) and Mexico (4) — which reflects regional cybercrime and banking-trojan ecosystems rather than espionage programs. Canada (2), Vietnam (1), and Italy (1) round out the list;



low counts from Western countries typically reflect criminal infrastructure or actor hosting rather than state sponsorship.

Destination Countries

Targeting is heavily concentrated in the English-speaking and Western European healthcare markets. The United States alone accounts for 7.2% of observed targeting references — more than the entire Europe roll-up minus its sub-regions — followed by Canada at 4.1% and the United Kingdom at 3.4%. Switzerland (2.8%) and France (2.6%) rank above Germany (1.5%), which is a reasonable proxy for pharmaceutical and research concentration rather than population. Asia-Pacific presence is real but thinner: Australia 2.1%, Singapore 1.5%, Hong Kong 1.4%. The full profile lists 68 targeted geographies including Africa, the Caribbean, and Central America, confirming the sector is targeted globally even though the volume sits in North America and Western Europe.

State of Affairs

GTI assigns healthcare an overall Cyber Threat Score of 4.6, and the component breakdown is the most useful part of the profile. Financially motivated activity scores 4.0 for frequency and 5.0 for magnitude — the highest value in the entire model — while state-sponsored activity scores 2.5 for frequency and 3.0 for magnitude, and information-operations/hacktivism scores 1.5 on both. The motivation tally reinforces it: Financial Gain appears 72 times against Espionage 32, Attack/Destruction 6, Notoriety 5, State Financial Gain 3, and Surveillance 1. The practical reading for a healthcare security program is that espionage is the more sophisticated threat but extortion and fraud are both more frequent and more damaging, so control investment should be weighted accordingly.

The tooling picture is conventional and commodity-heavy, which is good news for detection engineering. The most-used malware families across healthcare campaigns are BEACON (11 campaigns), MIMIKATZ (10), SHADOWLADDER.IDAT (8), PSEXEC (8), and FAKETREFF (6), followed by BLACKWIDOW, LUMMAC.V2, ADVIPSCAN, FAKEUPDATES, and SNOWLIGHT at 5 each. Note that LUMMAC.V2 appearing in the sector top ten independently corroborates the priority assigned to CAMP.26.102 in this brief, and FAKEUPDATES and SNOWLIGHT both featured in earlier editions of this series. On exploitation, the most-reused vulnerability is CVE-2025-59287 (Windows WSUS, 3 campaigns), followed by CVE-2023-38831, CVE-2024-9474, CVE-2025-53770 (SharePoint), CVE-2024-0012, and CVE-2021-21551 at 2 each — all previously disclosed and patchable, none novel. The most frequently observed actors by campaign count are UNC5518, UNC1543, and TEMP.Hex at 5 each, then UNC4984 and UNC4108 at 4.

Sources: Google Threat Intelligence (GTI), CISA / NSA / FBI / UK NCSC and international partners — Joint Cybersecurity Advisory AA26-204A and accompanying press release (cisa.gov), CISA KEV Catalog, CISA ICS Medical Advisories (ICSMA-26-181-01; -176-01; -176-02; -083-01), CISA ICS Advisories (ICSA-26-211 series), Google Threat Intelligence — Industry Snapshot: Healthcare (industry-profile--healthcare), Proofpoint, AIVD / MIVD, BleepingComputer, American Hospital Association, Fortinet PSIRT, Microsoft Security Response Center, NVD / CVE Program, Cisco Talos