



Executive Summary

Two developments define this week. The first is a step change in scale. GTI released GLOBAL.26.006 on September 4, documenting a Malware-as-a-Service operator and multiple distribution clusters running the NEONSLIDE framework — identified as ErrTraffic version 3 — across globally compromised WordPress sites. Healthcare and Pharmaceuticals are both GTI-confirmed among nineteen industries across twenty-eight countries, and the record carries 3,722 indicators, by a wide margin the largest single-campaign indicator set this series has reported. The framework combines ClickFix social engineering overlays with EtherHiding: the stage-one downloader queries smart contracts across multiple EVM-compatible blockchains to resolve its command-and-control infrastructure dynamically, which means blocklists age faster than the campaign does. Execution runs entirely on native Windows binaries — headless PowerShell, curl.exe, cmd.exe and bitsadmin.exe staging into %TEMP%, %LOCALAPPDATA% and %PROGRAMDATA% — to bypass application whitelisting and egress monitoring, and stage-two commodity infostealers harvest browser credentials, cryptocurrency wallets and active session tokens.

The second is that the EtherHiding ecosystem this series has tracked since August has now produced a confirmed healthcare victim. GTI operation record OP.26.1183, created September 2, documents UNC7032 conducting a targeted intrusion against a US healthcare organisation in August 2026, deploying the SPINCHAIN malware family with command-and-control at timelevel12.com. GTI links that operation directly to CAMP.26.113, the SPINCHAIN EtherHiding campaign reported in the August 21 brief. Three parallel UNC7032 operations against government, legal and financial services targets were recorded in the same period using the same domain. This is the clearest confirmation yet that the ClickFix and EtherHiding delivery chains are reaching healthcare organizations, not merely listing healthcare among possible targets.

The breach picture is severe. Aesto Health confirmed a breach affecting 9.54 million people and at least 30 healthcare provider clients — reported as the second-largest confirmed healthcare data breach of 2026 to date — after attackers accessed its AWS environment and stole Social Security numbers, financial account information, medical histories, health records, insurance information, and claims and billing data. Luminis Health in Maryland was taken partly offline by a cyberattack, with patient portals down across its Annapolis and Lanham hospitals. Nutex Health, reported in the August 28 brief at initial disclosure, has now confirmed that attackers stole patient, employee and provider information alongside confidential business and financial data, and are threatening publication. McKesson confirmed that intruders accessed several cloud-hosted accounts and exfiltrated data relating to its oncology, multispecialty and medical-surgical units. CISA published no new medical advisory in this window.

Active Threat Campaigns- Healthcare & Technology

Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
NEONSLIDE / ErrTraffic v3 — ClickFix and EtherHiding at Industrial Scale (GLOBAL.26.006)	Malware-as-a-Service initial access — Financial Gain and Unknown (Russia source region)	GTIG is tracking widespread initial access operations by a Malware-as-a-Service operator and multiple distribution clusters running the NEONSLIDE (ErrTraffic v3) JavaScript framework across globally compromised WordPress sites. Since at least April 2026 it has used ClickFix overlays — deceptive Google Antigravity prompts, fake ChatGPT error messages, browser CAPTCHA verification failures and simulated BSOD screens — to induce users to paste and run command cradles in the Windows Run dialog. Execution is living-off-the-land: an obfuscated headless PowerShell process assesses environment compatibility, then abuses curl.exe and cmd.exe to stage configurations in %TEMP% and	Healthcare AND Pharmaceuticals both GTI-confirmed, among 19 confirmed industries — United States confirmed, plus 27 further countries	CRITICAL — 3,722 indicators, the largest set in this series. Alert on headless PowerShell with inline download cradles, on clipboard-pasted execution, on bitsadmin writing to %PROGRAMDATA%, and restrict outbound RPC to public blockchain endpoints



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
		%LOCALAPPDATA%, and bitsadmin.exe to pull secondary payloads into %PROGRAMDATA%, bypassing application whitelisting and egress monitoring. The stage-one downloader executes JSON-RPC queries against smart contracts on multiple EVM-compatible chains to resolve C2 dynamically. Stage-two payloads are commodity infostealers harvesting browser credentials, crypto wallets and active session tokens, persisting via HKCU Run keys masquerading as UpdateService, and exfiltrating compressed credential archives over HTTPS POST. Activity last observed September 3, 2026		
UNC7032 SPINCHAIN Command and Control in Healthcare (OP.26.1183)	Targeted intrusion operation (motivation unknown)	A discrete, single-victim operation record rather than a broad campaign. GTI reports that UNC7032 conducted a targeted operation against a healthcare organisation in August 2026 to facilitate unauthorised access and potential data acquisition, deploying the SPINCHAIN malware family with command-and-control at timelevel12.com. The initial attack vector was not determined. The adversary focused on maintaining a persistent foothold in the single targeted environment. GTI links this operation to CAMP.26.113 — the SPINCHAIN EtherHiding campaign reported in the August 21 brief — and to the same threat actor record, making this the first confirmed healthcare victim tied to that campaign	Healthcare GTI-confirmed — United States. Activity observed August 17, 2026. Parallel UNC7032 operations against Government (Philippines), Legal & Professional Services (France) and Financial Services (Canada) are recorded separately	HIGH — Block and hunt timelevel12.com across DNS and proxy logs immediately. Re-apply the CAMP.26.113 controls from the August 21 brief; this confirms the campaign reached a US healthcare organisation
AiTM Phishing and Stolen OAuth Tokens for Business Email Compromise (CAMP.26.120)	Business Email Compromise / Cloud tenant persistence	Since July 2026 a threat actor has run Business Email Compromise operations via adversary-in-the-middle phishing, using device code authentication lures and landing pages to harvest OAuth access tokens. After authentication the actor attempts persistence by registering unauthorised devices in identity management, routes traffic through attacker-controlled Proton VPN, and configures deceptive inbox rules to hide subsequent activity. GTI characterises this as an ongoing campaign to bypass authentication controls and maintain durable cloud tenant access. Activity observed to August 13, 2026	GTI-confirmed: Construction & Engineering, Education, Hospitality, Legal & Professional Services, Manufacturing, Technology — United States, United Kingdom, Australia, Singapore. Healthcare NOT confirmed. Carried because device code abuse is the same technique confirmed against healthcare in the CAMP.26.107 hospitality Wi-Fi	HIGH — Block device code authentication through Conditional Access where not required; alert on unauthorised device registration, on inbox rules that delete or move security notifications, and on sign-ins via consumer VPN providers



Campaign / Threat Activity	Type	Key Technique	Targets	Priority Action
			campaign (August 7 brief)	
China-Nexus TRACKSTOMP and EMPTYROAD Across Windows and Linux (CAMP.26.127)	Espionage (China-nexus)	Targeting of both Windows and Linux systems with TRACKSTOMP and EMPTYROAD payloads. On Windows the group establishes persistence via scheduled tasks and startup mechanisms while conducting internal network reconnaissance, credential harvesting via cmdkey, and browser data staging. On Linux the actor escalates privileges via sudo, retrieves second-stage binaries with wget and curl, performs shellcode extraction, modifies PAM authentication configuration for persistence, and uses timestomping to evade detection. GTI maps 80 ATT&CK techniques; activity observed to August 21, 2026	GTI-confirmed: Education, Government — United States and Brazil. Healthcare NOT confirmed. Carried because PAM authentication modification on Linux is a persistence technique that survives credential rotation, and healthcare runs substantial Linux estates under clinical and imaging workloads	HIGH — Alert on modification of PAM configuration files on Linux hosts, on cmdkey credential enumeration on Windows, and on timestomping. File integrity monitoring on /etc/pam.d is the highest-value control here

Top 4 Priority Actions This Week

1. [CRITICAL] Defend Against NEONSLIDE at Scale — 3,722 Indicators and Blockchain-Resolved C2

GLOBAL.26.006 is the largest campaign record this series has reported, and its architecture is specifically designed to defeat the controls most healthcare organisations rely on. Compromised WordPress sites worldwide serve ClickFix overlays using a rotating set of pretexts — deceptive Google Antigravity prompts, fake ChatGPT error messages, browser CAPTCHA verification failures, and simulated blue-screen-of-death displays — each designed to get a user to copy a command string and run it in the Windows Run dialog. Once pasted, an obfuscated headless PowerShell process checks environment compatibility, then stages configuration files in %TEMP% and %LOCALAPPDATA% using curl.exe and cmd.exe, and retrieves secondary payloads into %PROGRAMDATA% using bitsadmin.exe. GTIG notes explicitly that this sequence is chosen to bypass conventional application whitelisting and egress monitoring.

- Implement the detection GTIG recommends directly: endpoint rules identifying headless PowerShell executions containing inline network download cradles, and clipboard-pasted execution patterns
- Inspect or restrict outbound RPC traffic destined for public blockchain endpoints — for the overwhelming majority of healthcare networks there is no legitimate reason for a clinical or administrative endpoint to query an EVM smart contract
- Alert on bitsadmin.exe retrieving content into %PROGRAMDATA%, and on child processes spawned from the Windows Run dialog or shell dialogues
- Audit HKCU Run keys for entries masquerading as UpdateService or similar generic service names, and review hidden directories under %PROGRAMDATA% and %LOCALAPPDATA%
- Patch and access-control your web content management systems — the delivery layer for this entire framework is compromised WordPress sites, and any patient-facing WordPress property you run could become part of it



2. [HIGH] Hunt timelevel12.com — UNC7032 Has Reached a US Healthcare Organisation

GTI created operation record OP.26.1183 on September 2, documenting that UNC7032 conducted a targeted operation against a healthcare organisation in August 2026 to facilitate unauthorised access and potential data acquisition. The intrusion deployed the SPINCHAIN malware family, which established communications with command-and-control infrastructure at timelevel12.com. GTI states that the initial attack vector was not determined, and that the adversary focused on maintaining a persistent foothold within the single targeted environment. The significance is the linkage: GTI associates this operation with CAMP.26.113, the campaign reported in the August 21 brief in which the SPINCHAIN JavaScript downloader used EtherHiding to retrieve instructions from blockchain smart contracts and ClickFix prompts to induce execution, and with the same threat actor record. In the August 21 edition CAMP.26.113 carried Healthcare among thirteen GTI-confirmed industries; this operation record is the first confirmed healthcare victim attached to it. Three further UNC7032 operations using the same domain were recorded in the same period — against a government organisation in the Philippines (first seen August 16), a legal and professional services organisation in France (August 30), and a financial services organisation in Canada (September 3) — indicating sustained, multi-sector operational tempo rather than an isolated intrusion.

- Block timelevel12.com at DNS and proxy immediately, then retro-hunt across at least 90 days of DNS, proxy and firewall logs — a single resolution warrants full incident response
- Re-apply the CAMP.26.113 control set from the August 21 brief in full: alert on pcalua.exe or cmd.exe proxying PowerShell, on mshta.exe with remote arguments, on clipboard access by non-standard processes, and on WMIC execution outside administrative tooling
- Because the initial vector is undetermined, do not assume a specific entry point is closed — prioritise detection of the post-compromise behaviour over prevention of a single vector
- Review scheduled tasks and registry run keys created in the August window on any host that resolved the C2 domain

3. [HIGH] Respond to the Healthcare Breach Wave — Aesto, Luminis, Nutex and McKesson

Four healthcare breach developments landed in this window and they illustrate three distinct risk mechanisms. Aesto Health confirmed a breach affecting 9.54 million people and at least 30 healthcare provider clients, reported as the second-largest confirmed healthcare data breach of 2026 to date. Attackers accessed Aesto's AWS environment and stole information including Social Security numbers, financial account information, medical histories, health records, insurance information, and claims and billing data. This is aggregation risk: one vendor holding data for thirty provider organizations means a single cloud compromise produces a multi-organisation breach. Luminis Health, which operates hospitals in Annapolis and Lanham, Maryland, suffered a cyberattack that took patient portals and other systems offline; reporting indicates widespread outages began on August 31 with staff sent home before the health system publicly confirmed a cyber incident on September 2. The organization established a dedicated patient helpline, engaged legal counsel and third-party forensic specialists, and acknowledged that key questions including whether patient records were compromised remain unresolved. This is operational disruption risk. Nutex Health, whose initial disclosure was covered in the August 28 brief, has now confirmed that attackers stole patient, employee and healthcare provider information along with confidential business and financial data, and that the attackers are threatening to publish it — an escalation from exfiltration to active extortion. McKesson confirmed that hackers broke into several of its cloud-hosted accounts and exfiltrated data, with its chief technology officer stating the stolen data relates to its oncology and multispecialty and medical-surgical units, and the company expecting intermittent service degradation.

- Determine immediately whether Aesto Health is a vendor to your organization or to any of your provider partners, and request written confirmation of whether your patient population is within the 9.54 million



- For McKesson customers, note the newly specified scope — oncology, multispecialty and medical-surgical units — and ask directly whether your ordering and patient data falls within those units; plan for intermittent service degradation in pharmacy and supply workflows
- Use Luminis Health as a tabletop scenario this month: outages began a full day or more before public confirmation, which is the realistic shape of an incident — test whether your clinical downtime procedures activate on operational symptoms rather than waiting for a confirmed cyber determination
- For Nutex, note the progression from exfiltration to publication threat; if you are a partner organization, prepare for the possibility that your data appears in a leak regardless of your own security posture
- Record all four as Business Associate or partner events with confirmed facts and open questions separated, and diary follow-up rather than waiting for formal notification

4. [HIGH] Close Device Code and OAuth Token Abuse (CAMP.26.120)

Since July 2026 a threat actor has conducted Business Email Compromise operations using adversary-in-the-middle phishing built around device code authentication lures and landing pages designed to harvest OAuth access tokens. Following successful authentication the actor registers unauthorized devices in identity management to secure persistence, routes subsequent traffic through attacker-controlled Proton VPN infrastructure, and configures deceptive inbox rules — the standard technique for hiding security alerts and reply traffic from the legitimate mailbox owner. GTI describes this as an ongoing campaign specifically aimed at bypassing authentication controls and maintaining durable cloud tenant access, with activity observed to August 13, 2026 across the United States, United Kingdom, Australia and Singapore. Healthcare is not among the six GTI-confirmed industries. It is carried here because device code authentication abuse is not hypothetical for healthcare: the CAMP.26.107 hospitality Wi-Fi campaign in the August 7 brief, for which Healthcare is GTI-confirmed, used exactly this technique, redirecting victims into Microsoft's genuine device code flow so that the attacker received an MFA-satisfied session.

- Block device code authentication through Conditional Access for all users who do not have a documented need — this remains the single highest-value control against this technique and it is a policy change, not a project
- Alert on device registration events in Entra ID outside normal provisioning windows, and review all devices registered in the last 60 days against IT asset records
- Alert on inbox rule creation that deletes, marks read, or moves messages containing security or authentication keywords — this is the concealment step and it is highly detectable
- Flag authentication from consumer VPN provider address space for privileged, clinical and finance accounts

Medical Device and IoT Security

No New Advisory This Window

- CISA published no new ICS Medical Advisory between August 29 and September 4, 2026. The outstanding workload is unchanged from the August 28 brief and remains substantial. Three at-home Bluetooth Low Energy device advisories are open — Pulsetto Vagus Nerve Stimulator (no vendor fix, vendor unresponsive to CISA, undisclosed commands able to disable electrical safety mechanisms), Mira Hormone Monitor (eight CVEs, cleartext hormone data extraction and user tracking via a non-rotating BLE address), and Flow Neuroscience FL-100 (firmware update available via the Flow app). Four DICOM product advisories remain open, of which GDCM and pydicom/pynetdicom have no fix and unresponsive maintainers, while DCMTK and RadiAnt are patchable. GDCM reaches week 24 without a patch.
- The vendor-unresponsive pattern now spans three advisories in this tracker and is worth escalating as a governance matter rather than a technical one. Where CISA records that a maintainer or vendor has not responded, compensating controls are permanent rather than



temporary, and for patient-owned at-home devices those controls are limited to patient counselling. That belongs in a clinical risk register with a named owner, not in an IT backlog.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ EtherHiding industrialised: a MaaS operator now rents blockchain-resolved delivery chains at scale (GLOBAL.26.006) ▲ Healthcare victim confirmed for a campaign this series reported two weeks ago (UNC7032 SPINCHAIN) ▲ Mass-scale healthcare data exposure: a single vendor breach reaches 9.54 million individuals ▲ Hospital operational disruption: a Maryland health system taken partly offline with patient portals down ▲ ClickFix now spans Windows and macOS — four distinct ClickFix-linked records created this week alone ► No new CISA medical advisory in this window; the DICOM and BLE device backlog is unchanged	3,722 indicators in GLOBAL.26.006 alone — the largest single-campaign IOC set recorded in this series 9,540,000 individuals and 30+ provider clients affected by the Aesto Health breach 19 GTI-confirmed industries and 28 countries for GLOBAL.26.006, including Healthcare and Pharmaceuticals 3,781 new GTI-verified IOCs across 6 records 4 UNC7032 SPINCHAIN victim operations recorded across healthcare, government, legal and financial services CVE-2026-3650 (GDCM): NO PATCH — week 24; CVE-2026-56445 and CVE-2026-18844: NO PATCH

Sources: Google Threat Intelligence (GTI), CISA ICS Medical Advisories (ICSMA-26-225-01, -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, Aesto Health, Luminis Health, Nutex Health, McKesson (statement and customer notice), TechCrunch, BleepingComputer, HIPAA Journal, PrivacyGuides Data Breach Roundup, Hoodline, The IT Nerd, NVD / CVE Program / MITRE, Palo Alto Networks, Fortinet PSIRT