



Executive Summary

Three new GTI-verified campaigns are reported this week, the most operationally urgent is CAMP.26.053 — an active targeted intrusion campaign against U.S. healthcare, pharmaceutical, and education institutions using heavily obfuscated PowerShell and in-memory C# compilation. Google Threat Intelligence Group (GTIG) explicitly characterizes the post-exploitation profile as consistent with pre-ransomware operations; healthcare CISOs should treat any detection of this TTP chain as a ransomware-in-progress event, not a low-severity alert. Also new: CAMP.26.064, a ClickFix-driven campaign deploying persistent NetSupport RAT clients via an unusual legacy finger protocol delivery chain — active to June 3, 2026, with 182 IOCs across 102 domains, and healthcare among its confirmed targeted industries. And CAMP.26.060 / GLOBAL.26.005 (TeamPCP / UNC6780) — a GitHub Actions supply chain attack now confirmed active through June 11, 2026, using OIDC token abuse to publish trojanized NPM and PyPI packages and deploy the FIRESALE credential stealer against 1Password and BitWarden vaults, with a built-in recursive wipe triggered on token revocation.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
Obfuscated PowerShell Pre-Ransomware — Healthcare & Education (CAMP.26.053)	Espionage / Ransomware Precursor	Heavily obfuscated Base64-encoded PowerShell → in-memory payload execution; CSC.EXE native C# compile on-disk; malicious DLL drops; ASEP Run-key persistence; SYSTEMINFO / IPCONFIG / NLTEST recon — GTI explicitly flags as pre-ransomware operations. First seen Apr 13, 2026. 117 IOCs.	Healthcare, Education, Govt, Pharmaceuticals — US (confirmed GTI)	HIGH — Re-rank obfuscated PS detections to Priority-1; alert on CSC.EXE from anomalous parents; audit Run-key ASEP modifications; isolate any host showing full TTP chain
ClickFix + Finger Protocol → NetSupport RAT (CAMP.26.064)	Initial Access / Remote Control	ClickFix lures via Edge/Chrome → finger.exe downloads scripts → curl retrieves renamed Python executable → in-memory C# stager via CSC → persistent NetSupport RAT in hidden directories. Eastern Europe nexus. Active late March – June 3, 2026. 182 IOCs: 102 domains, 21 IPs, 59 URLs.	Healthcare, Govt, Education, Mfg, Retail, Tech, Construction, Transport — US, IN, TW (confirmed GTI)	HIGH — Block finger.exe outbound; detect finger → curl → renamed-Python chain; alert on NetSupport from hidden directories; train staff on ClickFix browser prompt lures
GitHub Actions Cache Poisoning + FIRESALE Stealer — TeamPCP (CAMP.26.060 / GLOBAL.26.005*)	Financial / Supply Chain	UNC6780 (TeamPCP) poisons GitHub Actions caches via anonymizing-network repo scraping + rclone; harvests OIDC tokens; publishes trojanized NPM and PyPI packages; deploys FIRESALE to steal 1Password and BitWarden vaults; anti-forensic recursive wipe on token revocation. Targets Trivy, Bitwarden, Checkmarx KICS, LiteLLM pipelines. Active May–June 11, 2026. 16 IOCs.	Technology DevOps, Financial Services, Healthcare — Global (opportunistic; confirmed per parent GLOBAL.26.005)	HIGH — Rotate all GitHub OIDC and PAT tokens immediately; pin Actions to full SHA; audit NPM/PyPI installs; force-rotate 1Password/BitWarden master credentials on affected dev systems

Top 3 Priority Actions This Week

1. [HIGH] Treat CAMP.26.053 Detections as Ransomware-In-Progress

Since April 13, 2026, GTIG has tracked CAMP.26.053 targeting prominent healthcare and educational institutions in the US. The attacker uses heavily obfuscated, Base64-encoded PowerShell to download secondary payloads and execute them entirely in-memory, bypassing file-based antivirus. Persistence is established through Run-key modifications (ASEP). Malicious DLLs are dropped, and the native C# compiler (CSC.EXE) is invoked locally to compile payloads on-disk — a technique that circumvents allowlisting controls in environments that permit .NET framework use. Post-



exploitation activities include sequential SYSTEMINFO, IPCONFIG, and NLTEST execution — a reconnaissance pattern GTIG explicitly characterizes as consistent with pre-ransomware staging.

- Re-rank all obfuscated or Base64-encoded PowerShell detections with in-memory execution to Priority-1 in your SIEM — especially from clinical workstations, nursing stations, or administrative endpoints; this is a ransomware precursor timeline, not a medium-severity event
- Alert on CSC.EXE (Microsoft's native C# compiler, located at C:\Windows\Microsoft.NET\Framework\)\ spawning from PowerShell, cmd.exe, or user-initiated scripts; any CSC compilation outside of known developer endpoints is anomalous
- Monitor ASEP Run-key modifications via EDR (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) — flag any new entry added by processes other than your asset management tooling, particularly following PowerShell or unusual DLL activity on the same host
- SYSTEMINFO + IPCONFIG + NLTEST executing in sequence on a healthcare workstation within a short timeframe with no corresponding IT ticket or remote session should trigger immediate EDR isolation — do not wait for file-based confirmation; behavioral chain alone meets the GTIG pre-ransomware threshold
- Healthcare organizations: any host exhibiting the full CAMP.26.053 TTP chain (obfuscated PS → in-memory execution → CSC compile → Run-key persistence → discovery commands) should be isolated from the clinical network immediately and triaged as an active incident

2. [HIGH] Block the Finger Protocol — CAMP.26.064 NetSupport RAT Chain

Since late March 2026 and active through at least June 3, 2026 (per GTI last-seen), CAMP.26.064 — attributed by GTIG to an Eastern European nexus — has operated a ClickFix social engineering chain with a distinctive and rarely-seen delivery mechanism. Victims are directed to actor-controlled domains via Edge or Chrome and presented with a ClickFix prompt — a fake technical support or system verification step instructing manual command execution. The executed command invokes finger.exe, a legacy Windows network utility not present in most modern security monitoring baselines, to download malicious scripts. Subsequent stages use curl to retrieve a Python executable renamed to masquerade as a system binary, then invoke CSC to compile and deploy a NetSupport RAT client installed into a hidden directory for persistence.

- Block outbound execution of finger.exe entirely — this utility has no legitimate operational role in clinical or corporate environments; its execution is an unambiguous indicator of CAMP.26.064 activity and should trigger an immediate high-severity alert
- Detect the three-step delivery chain: finger.exe spawning curl, followed by a Python process renamed to a Windows system binary (e.g., svchost.exe, explorer.exe) — this sequence is unique to this campaign and distinguishable from legitimate Python activity
- Alert on NetSupport Manager (netsupport.exe or nsm.exe) executing from hidden directories, user profile subdirectories beginning with a dot, or AppData/Temp paths — legitimate enterprise NetSupport deployments do not install to concealed locations
- CSC.EXE execution on non-developer endpoints should now be treated as a shared indicator with CAMP.26.053 — apply the same Priority-1 treatment described in Action 1 above when finger.exe or curl precedes CSC activity on the same host
- Apply ClickFix user awareness training this week: staff should never execute commands delivered through a browser popup claiming to be a Windows update, CAPTCHA verification, or 'security check', particularly the 'Windows + R → paste → Enter' instruction pattern; include this scenario in your next phishing simulation



3. [HIGH] Rotate GitHub OIDC Tokens Now — CAMP.26.060 / GLOBAL.26.005 (TeamPCP / UNC6780)

Since May 10, 2026 (sub-campaign CAMP.26.060) and as far back as September 2025 (parent GLOBAL.26.005), UNC6780 — tracked by GTIG as the TeamPCP cluster — has operated a cascading software supply chain attack targeting developer CI/CD ecosystems. The actor uses anonymizing networks to scrape public GitHub repositories via rclone, then poisons GitHub Actions runner caches to harvest OpenID Connect (OIDC) tokens and Personal Access Tokens (PAT) from runner memory. Using those tokens, trojanized NPM and PyPI packages are published downstream — GTIG has confirmed compromise of Trivy, Bitwarden, Checkmarx KICS, TanStack, and LiteLLM pipelines. The FIRESALE credential stealer is deployed locally on developer endpoints to exfiltrate 1Password and BitWarden vault contents. A destructive anti-forensic mechanism recursively wipes compromised hosts if token revocation is detected, eliminating post-incident forensic evidence.

- Rotate all GitHub OIDC tokens and Personal Access Tokens (PATs) immediately — especially for any repositories with Actions workflows that ran in the past 60 days; the TeamPCP actor specifically harvests OIDC tokens from runner memory and uses them to publish to downstream package registries
- Pin all GitHub Actions to full commit SHAs in every workflow file — not branch names, not version tags; a poisoned cache entry on a non-SHA-pinned action is the primary mechanism CAMP.26.060 uses to inject into legitimate developer pipelines
- Audit Actions workflow files for permissions.id-token: write — restrict this to only workflows that explicitly require OIDC federation for cloud deployment; remove it from test, lint, and build workflows that have no cloud deployment function
- Force-rotate 1Password and BitWarden master credentials and all stored secrets for any developer with active GitHub Actions workflows in the past 60 days — the anti-forensic wipe makes post-compromise confirmation impossible; rotate preemptively rather than waiting for evidence of vault access
- Healthcare DevOps teams: any EHR integration API keys, HL7 endpoint credentials, FHIR server OAuth secrets, or cloud database passwords stored in developer password vaults or CI/CD secrets should be treated as potentially compromised and rotated immediately, with downstream service providers notified
- Rebuild any GitHub Actions runner caches that may have been active during May–June 2026 across affected pipelines; invalidate all cached artifacts from repositories that used dependency-scanning tools (Trivy, Checkmarx KICS) or ML/LLM libraries (LiteLLM) during this window

Medical Device and IoT Security

Persistent CVE Tracker — One New Advisory; No Active Medical Device Exploitation This Week

No new medical device CVEs with confirmed active exploitation were added by CISA or FDA for the week of June 19. One new GTI-flagged vulnerability with telehealth relevance is added to the tracker this week (CVE-2026-43994 / coturn). All prior open items remain in effect:

CVE	System	CVSS	CISA KEV Status	First Brief	Current Status
CVE-2026-3650	GDCM DICOM Library (PACS/Imaging)	7.5 / 8.7	ICSMA-26-083-01 open	Apr 3	⚠ NO PATCH — Week 13. Segment PACS. Block unauthenticated DICOM. Monitor imaging vendors for patch ETA.
CVE-2024-12248	Contec CMS8000 Patient Monitor	9.8	No active exploitation	Feb 9+	FDA disconnect recommendation in force. GTI EPSS 0.0068.
CVE-2025-0626	Contec CMS8000 Backdoor	—	No active exploitation	Feb 9+	FDA disconnect recommendation in force.



CVE	System	CVSS	CISA KEV Status	First Brief	Current Status
CVE-2026-32201	SharePoint 2016 / 2019 / Sub Ed	6.5	KEV deadline Apr 28 — PASSED	Apr 24	Patches KB5002861/54/53. Verify fully applied across all instances. Note: GTI GLOBAL.26.005 is the TeamPCP supply chain campaign, not this CVE.
CVE-2026-34197 + CVE-2026-40466	Apache ActiveMQ	8.8	KEV Apr 12 / Apr 20	Apr 24	Upgrade to 5.19.4 or 6.2.3 AND apply follow-on CVE-2026-40466 bypass patch.
CVE-2026-38125	Ivanti EPMM (MobileIron Core)	9.8	KEV Apr 29	May 1	Patch to 12.4.0.1+. Audit MDM logs for unauthorized enrollments.
CVE-2026-0300	PAN-OS User-ID Auth Portal	9.8	KEV May 9 — PASSED	May 8	Patches released ~May 13. Confirm all PA-Series/VM-Series updated. Treat unpatched as compromised.
CVE-2026-43994	Coturn TURN/STUN Server (WebRTC/Telehealth)	8.1	No active exploitation	NEW Jun 19	Stack buffer overflow in OAuth token path. Patch to coturn 4.10.0. Relevant for telehealth WebRTC relay infrastructure.

CVE-2026-3650 status note: This CISA advisory (ICSMA-26-083-01) has been open for 13 weeks. Grassroots DICOM remains unresponsive to CISA coordination. Healthcare organizations using GDCM-based imaging software from Dentsply Sirona, Zimmer Biomet, or others using GDCM 3.2.2 should escalate directly with their imaging vendors for a patched library ETA and log all vendor responses for HIPAA risk documentation.

CVE-2026-43994 (Coturn, NEW): A stack buffer overflow in the coturn TURN/STUN server's OAuth token decoding path (decode_oauth_token_gcm) allows up to 735 bytes of attacker-controlled data to be written past a 256-byte stack buffer before AES-GCM authentication is verified — no valid OAuth key needed. Coturn is widely deployed in telehealth platforms for WebRTC video relay. Patch to version 4.10.0 is available. GTI rates MEDIUM / P3 with no active exploitation confirmed. Apply if coturn is part of your telehealth infrastructure stack.

Activity Trends	Key Numbers This Week
▲ Pre-ransomware obfuscated PowerShell intrusions: escalating in healthcare and education ▲ ClickFix lure campaigns broadening: legacy protocol (finger) abuse as delivery vector ▲ GitHub Actions OIDC token abuse: supply chain credential theft escalating ▲ Developer password vault theft (FIRESALE): 1Password / BitWarden targets confirmed — Iran-nexus ops: sustained elevated posture vs. Western healthcare — Russia-nexus cloud intrusion (CAMP.26.081): continued activity through June 11 ▼ Email phishing as initial vector: continued sustained decline (M-Trends 2026)	3 new GTI-verified campaigns (CAMP.26.053 / .064 / .060) 319 total new IOCs across 3 campaigns this week 117 IOCs — CAMP.26.053 (Healthcare/Education pre-ransomware) 182 IOCs — CAMP.26.064 (ClickFix NetSupport, active to June 3) 16 IOCs — CAMP.26.060 (GitHub FIRESALE supply chain) 22 seconds — median access-broker handoff (M-Trends 2026) - CVE-2026-3650 (GDCM): NO PATCH — week 13 of open advisory

Sources: Google Threat Intelligence (GTI/GTIG) — all campaign and vulnerability claims verified via live GTI record lookup; CISA; FDA; NVD; MITRE ATT&CK; HIPAA Journal; Medcurity; Compliancy Group; HHS OCR (NPRM 90 FR 800); Alston & Bird.