



Executive Summary

Three new GTI-verified campaigns are reported this week with the most critical being CAMP.26.053, a targeted intrusion campaign deploying heavily obfuscated, Base64-encoded PowerShell against healthcare and pharmaceutical organizations in the United States. Active from April 13 through at least May 2026, the actor uses in-memory payload execution, registry Run key persistence, malicious DLL drops, and native C# compilation (CSC.EXE) to evade detection with TTPs consistent with pre-ransomware staging. Separately, CAMP.26.055 (UNC6844) delivers the initial foothold that feeds CAMP.26.053 via ClickFix social engineering lures distributed via Microsoft Edge and Chrome. And CAMP.26.064, a high-volume ClickFix campaign (173 IOCs) abusing the legacy `finger` utility to deploy NetSupport RAT targets healthcare organizations alongside government, education, and manufacturing globally, with last observed activity on May 26, 2026.

On the compliance front: the HIPAA Security Rule proposed rule (90 FR 800), the most significant update since 2003, has not yet been finalized as of June 5. The May 2026 OCR target passed without a final rule. A final rule is still listed on OCR's regulatory agenda; when published, organizations will have 180 to 240 days to comply. The direction is unambiguous: MFA, universal ePHI encryption, annual risk assessments, network segmentation, and vulnerability scanning are moving from optional to required. Begin implementation now — do not wait for the final rule.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Targets	Key Techniques	Priority Action
Obfuscated PowerShell & Registry Persistence Targeting HC/Pharma (CAMP.26.053)	Espionage / Ransomware Precursor	Healthcare, Pharma, Govt, Mfg, Education — US	Heavily obfuscated Base64 PowerShell; in-memory payload execution; ASEP registry Run keys; malicious DLL drops; native CSC.EXE C# compilation on disk; post-exploitation network discovery via SYSTEMINFO, IPCONFIG, NLTEST	HIGH — Alert on Base64 PowerShell executions; audit Run keys; enforce AppLocker; monitor CSC.EXE compilation; treat as ransomware precursor
UNC6844 ClickFix Initial Access for CAMP.26.053 (CAMP.26.055)	Initial Access / Social Engineering	Healthcare, Education — US	ClickFix lures via Microsoft Edge/Chrome; actor-controlled HTTPS domains; users tricked into manually executing malicious commands; hands off access to CAMP.26.053 operators as secondary actor	HIGH — Block ClickFix lure domains; train staff to recognize browser-delivered manual command execution prompts; alert on MSHTA and PowerShell from browser processes
ClickFix Finger-Protocol Lures Deploying NetSupport RAT (CAMP.26.064)	Espionage / Credential Theft	Healthcare, Govt, Education, Mfg, Retail, Transportation — US, IN, TW	ClickFix abuses legacy `finger` utility to download scripts; CURL retrieves renamed Python interpreter; in-memory stager; PowerShell compiles C# via CSC; NetSupport Manager RAT in hidden directories; 173 IOCs	HIGH — Block `finger.exe` outbound; alert on CURL → Python rename pattern; inspect CSC.EXE spawned from PowerShell; hunt NetSupport RAT installations in hidden directories

Top 3 Actions This Week

1. [HIGH] CAMP.26.053 — Obfuscated PowerShell Targeting Healthcare — Ransomware Pre-Staging

Between April 13 and at least May 1, 2026, GTI analysts observed a targeted intrusion operation against healthcare, pharmaceutical, government, manufacturing, and educational institutions in the United States. The actor enters via ClickFix social engineering (CAMP.26.055 / UNC6844 delivers the initial foothold), then transitions to advanced post-exploitation. The toolset relies on heavily obfuscated, Base64-encoded PowerShell commands to download secondary payloads and execute them entirely in memory, bypassing file-based antivirus. Persistence is established by adding Run keys to the registry (ASEP modification). The actor also drops malicious DLLs and invokes the native C# compiler CSC.EXE to compile payloads on disk. Post-exploitation activity follows a classic pre-ransomware pattern: SYSTEMINFO, IPCONFIG, and NLTEST commands enumerate the system and



Active Directory trusts, staging the environment for lateral movement and data exfiltration. GTI has confirmed Healthcare, Pharmaceuticals, Government, Manufacturing, and Education as targeted industries making this the most healthcare-relevant new campaign this week. IOC count: 3 files, 10 domains, 4 IPs, 100+ URLs (117 total).

- Alert immediately on Base64-encoded PowerShell executions, especially those using - EncodedCommand or HttpClient download cradles — these are the hallmark of CAMP.26.053 initial staging
- Audit HKCU\Software\Microsoft\Windows\CurrentVersion\Run and the equivalent HKLM key for unauthorized entries; CAMP.26.053 achieves persistence via Run key modification
- Block or alert on CSC.EXE (the native C# compiler) spawning from PowerShell or any non-development user context — this is highly anomalous in clinical environments
- Deploy or tune EDR to detect malicious DLL sideloading patterns; the actor drops DLLs alongside legitimate executables to establish persistence
- Treat any SYSTEMINFO or NLTEST execution from an endpoint where a PowerShell anomaly was detected as an active compromise indicator — escalate immediately and do not defer

2. [HIGH] CAMP.26.055 / CAMP.26.064 — Dual ClickFix Initial Access Campaigns — Healthcare Targeted

Two concurrent ClickFix campaigns are delivering initial access into healthcare environments. CAMP.26.055 (UNC6844, active since March 23, 2026, last seen May 7) specifically hands off to CAMP.26.053 operators and confirms Healthcare and Education as targeted industries. CAMP.26.064 (Eastern Europe-nexus, active since February 5, 2026, last seen May 26) is a higher-volume operation with 173 IOCs that abuses the legacy Windows `finger` command-line utility — rarely seen in the wild as an attack vector — to download malicious scripts without triggering standard web proxy detections. These scripts invoke CURL to retrieve a renamed Python interpreter, which then executes an in-memory stager that compiles and launches NetSupport Manager RAT hidden inside user directories. Healthcare is a confirmed targeted industry for CAMP.26.064 alongside government, education, manufacturing, retail, and transportation across the United States, India, and Taiwan.

- Block outbound connections from `finger.exe` (TCP port 79) at the perimeter — this port should have no legitimate use in any clinical or enterprise environment and is the unique delivery mechanism for CAMP.26.064
- Alert on CURL.EXE or curl spawned from PowerShell, cmd.exe, or any browser process, especially when the output is a renamed executable; this is the payload staging pattern for CAMP.26.064
- Train all staff, including clinical users, to recognize ClickFix lures: browser popups claiming a verification step is required, asking users to open Run, cmd, or PowerShell and paste a command — this is always malicious
- Alert on NetSupport Manager (nsm.exe, nscm.exe) processes running from AppData, Temp, or any hidden directory — legitimate NetSupport deployments are managed by IT and appear in approved system paths
- Correlate: if CAMP.26.055 ClickFix lure activity is detected on an endpoint, pivot to that host and check for CAMP.26.053 PowerShell staging activity immediately — these campaigns are linked

3. [HIGH] HIPAA Security Rule — Final Rule Not Yet Issued — Begin Implementation Now

OCR's proposed HIPAA Security Rule update (90 FR 800, published January 6, 2025) has not been finalized as of June 5, 2026. OCR's May 2026 target date passed without a final rule. The rule remains



listed on OCR's regulatory agenda, but no confirmed timeline has been provided by the Trump administration. When published, organizations will have 180-240 days to comply. The direction is unambiguous and organizations should not wait. The proposed rule eliminates the longstanding distinction between 'required' and 'addressable' implementation specifications — making effectively all controls mandatory. Key changes include: mandatory MFA across all ePHI-accessing systems; universal ePHI encryption at rest and in transit; annual security risk assessments (structured process: risk analysis, remediation plan, sanctions policy, activity review — all documented); network segmentation as a required control; regular technical vulnerability scanning; and substantially expanded business associate oversight requiring active verification of third-party safeguards (not just signed agreements). The rule also tightens incident response obligations and introduces interval-based testing requirements. Industry associations including CHIME have requested withdrawal citing cost burden (~\$9 billion projected year-one), but OCR has retained the finalization target. A phased, good-faith compliance approach is being credited by OCR in enforcement signaling.

- Conduct a gap assessment now against the proposed rule requirements — organizations that complete this before publication will have implementation runway; those that wait after publication will be compressed into 6-8 months
- Prioritize MFA deployment across all ePHI-accessing systems including EHR, PACS, pharmacy systems, and clinical portals — this is the single highest-leverage control and a confirmed mandatory requirement
- Begin universal ePHI encryption planning: both at rest (database and file-level) and in transit (TLS 1.2+ on all clinical communications) — audit existing encryption posture and identify gaps
- Conduct or commission a formal annual security risk analysis following the structured process: risk identification, likelihood/impact assessment, remediation plan, sanctions policy, and activity review procedures — all must be documented
- Inventory and assess all business associates for security posture — the proposed rule requires active verification of BA safeguards, not just BAA signatures; prioritize high-PHI-volume vendors
- Begin network segmentation audit: identify clinical, administrative, and IoMT network zones and confirm appropriate controls exist between them — this aligns with the HIPAA Security Rule proposed changes and is already required for NIST and CIRCIA readiness
- Review your HIPAA Notice of Privacy Practices for compliance with the Part 2 SUD records rule (compliance date February 16, 2026 — confirm this has been addressed)

Medical Device and IoT Security

No New Medical Device CVEs This Week. Everything from last week is still valid.

Regulatory and Compliance Update

OCR's proposed HIPAA Security Rule overhaul (90 FR 800, January 6, 2025) remains in proposed rulemaking status as of June 5, 2026. **The May 2026 finalization target was not met.** No final rule has been published. OCR has not confirmed a revised timeline. A final action is still listed on the HHS OCR regulatory agenda; the next update to that agenda is expected shortly. Given federal agency practice of routine deadline extension, legal counsel should be monitoring the Federal Register for the final rule publication date.

Key proposed changes that organizations should begin implementing now regardless of final rule timing:

- MFA across all ePHI-accessing systems — mandatory (not addressable) under the proposed rule



- Universal ePHI encryption at rest and in transit — mandatory
- Annual security risk assessments (risk analysis + remediation plan + sanctions policy + activity review), all documented
- Network segmentation as a required control — directly relevant to IoMT and clinical network architecture
- Regular technical vulnerability scanning at defined intervals
- Business associate security verification — active confirmation of safeguards, not just BAA signatures
- Expanded incident response obligations including defined response and recovery procedures

Compliance timeline when final rule publishes: 180-240 days from Federal Register publication date. OCR has signaled willingness to credit good-faith phased compliance plans, particularly for critical access hospitals and small-to-mid-size providers, but this is enforcement discretion and not a formal extension.

CIRCA — Healthcare Rulemaking

CIRCA mandatory cyber incident reporting rules for healthcare remain in finalization. Organizations should continue building the internal workflows needed to report covered cyber incidents within the required timeframes. CISA is the lead agency; the healthcare sector is specifically included in covered critical infrastructure.

42 CFR Part 2 (SUD Records) — Compliance Date Passed

The February 16, 2026 compliance deadline for the HIPAA Notice of Privacy Practices update under the revised Part 2 SUD records rules has passed. All HIPAA covered entities that receive, create, maintain, or transmit SUD treatment information should have updated their NPP. If this has not been confirmed complete in your organization, address it immediately.

Activity Trends	Key Numbers This Week
▲ ClickFix social engineering: sustained high — two concurrent HC-targeting campaigns ▲ Pre-ransomware obfuscated PowerShell staging: emerging priority vector in HC ▲ Legacy protocol abuse (finger.exe): novel delivery vector in CAMP.26.064 ▲ HIPAA compliance pressure: final rule imminent — organizations unprepared ▲ Healthcare ransomware (Lynx, SPHINXLOCKER, INC Ransom): sustained high ▲ IoMT / unmanaged endpoint risk: elevated — CAMP.26.053/064 target Windows endpoints ▲ PAN-OS CVE-2026-0300: patches available ~May 13; confirm deployment ▼ Email phishing as primary initial vector: continued sustained decline (M-Trends 2026)	● 3 new GTI-verified campaigns this week 223+ new IOCs across three campaigns 117 IOCs in CAMP.26.053 alone 173 IOCs in CAMP.26.064 (96 domains, 21 IPs) - HIPAA final rule: May 2026 target missed — no new date - CVE-2026-3650 (GDCM): NO PATCH — week 10+ of advisory 22 seconds — median access-broker handoff (M-Trends 2026, still operative) - Next brief: June 12, 2026

Sources: Google Threat Intelligence (GTI) | Palo Alto Networks / Unit 42; CISA KEV catalog; Mandiant M-Trends 2026; MITRE ATT&CK; National Vulnerability Database; Cybersecurity Dive; Bleeping Computer.