Executive Summary

Two GTI-verified new campaigns are reported this week, sourced from Google Threat Intelligence (GTI) and CISA. The most operationally significant is CAMP.26.064, a new ClickFix-based campaign whose GTI narrative description states active since late March 2026 (GTI machine-recorded first activity: February 5, 2026) and last observed May 18, 2026, which abuses the legacy finger protocol to stealthily download and deploy persistent NetSupport RAT clients against confirmed Healthcare targets in the US, India, and Taiwan. Unlike prior ClickFix campaigns in this brief series, the finger-protocol delivery method is novel and distinct: it is specifically designed to bypass DNS-based web filtering by tunneling payloads over a legacy protocol that many security tools do not inspect.

Also new this week: a GTI-tracked campaign deploying XMRig cryptocurrency miners against Healthcare, Manufacturing, and Technology organizations via masqueraded PowerShell executables. The campaign uses BITSAdmin and trusted cloud services (GitHub, Google Drive) for stealthy ingress and establishes persistence through scheduled tasks disguised as Google Update processes.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Technique	Targets	Priority Action
NetSupport RAT via Finger Protocol + ClickFix Lures *GTI Campaign: CAMP.26.064 (NEW — first appearance in this brief series)*	Espionage / Remote Access Trojan	ClickFix social engineering lure directs victims to actor-controlled site; malicious command abuses legacy finger utility (finger.exe / finger@<actor-domain>) to download script over port 79; script invokes curl to retrieve a renamed Python executable; Python executes in-memory C# code compiled by CSC.EXE; NetSupport RAT client installed in hidden directory with persistence. Note: finger protocol bypasses many DNS/web filters as it is not HTTP/HTTPS.	Healthcare, Government, Education, Technology, Manufacturing, Legal, Retail, Transportation — US, India, Taiwan (GTI confirmed; active late March – May 18, 2026)	HIGH — Block finger.exe execution and outbound port 79; alert on CSC.EXE compiling code outside dev environments; detect NetSupport RAT IOCs; refresh ClickFix staff training
XMRig Cryptominer via Masqueraded PowerShell / BITSAdmin *GTI-tracked campaign (Healthcare-confirmed; NOTE: GTI internal ID conflicts with May 1 brief CAMP.26.058 — see analyst note in Action 2)*	Financial / Resource Hijacking	PowerShell executables masqueraded as svchost.exe to bypass Windows Defender and AMSI; BITSAdmin used to download 7Zip-archived payloads from GitHub and Google Drive (trusted cloud services bypass proxy/web filtering); archives extracted and XMRig miner executed; persistence via scheduled tasks disguised as 'Google Update' processes and WMI event consumer modifications	Healthcare, Manufacturing, Technology, Automotive, Transportation — US, Czech Republic, South Korea (GTI confirmed; active January – May 11, 2026)	HIGH — Alert on BITSAdmin downloading from GitHub/Google Drive; detect svchost.exe spawned outside System32; audit scheduled tasks named after Google products; investigate WMI event consumer modifications

Top 3 Actions This Week

1. [HIGH] Block NetSupport RAT via Finger Protocol — Legacy Protocol Abuse Bypasses Web Filtering

ClickFix social engineering is a continued, escalating reported in previous threat briefs.. This is a new campaign and distinct from the previous ones mentioned. Its differentiating characteristic is not the ClickFix lure itself but the payload delivery method: where prior campaigns used PowerShell with HTTPS, this campaign abuses the finger protocol which is an ancient UNIX/Windows lookup

utility that communicates over TCP port 79. Because most network security tools focus on HTTP/HTTPS and DNS, finger-based traffic is frequently uninspected and unblocked.

Healthcare relevance: NetSupport RAT provides attackers with full remote control of compromised endpoints, including keylogging, screen capture, file transfer, and lateral movement capabilities. Clinical workstations, pharmacy terminals, and nursing-station endpoints running Windows are all potential targets. The finger protocol delivery method is specifically dangerous because it does not generate the HTTP/HTTPS web requests that standard web content filters and DLP tools are configured to inspect.

Actions:

- Block outbound TCP port 79 at perimeter and internal firewalls immediately — finger protocol has no legitimate use in modern healthcare environments; blocking it is zero-impact and removes this delivery vector entirely
- Disable or block finger.exe execution on all Windows endpoints via AppLocker, Windows Defender Application Control, or Group Policy; verify this applies to clinical workstations and nursing terminals, not just corporate desktops
- Alert on CSC.EXE (C# compiler) executing in any context outside of known developer machines — legitimate clinical environments should never invoke the C# compiler at runtime
- Alert on curl or Invoke-WebRequest spawned from cmd.exe or PowerShell as a child of an interactive user session — particularly when the URL does not match approved software distribution servers
- Deploy NetSupport RAT behavioral detection signatures; obtain full IOC list from GTI portal under CAMP.26.064 (41 domains, 17 IPs, 29 URLs — counts verified live from GTI on May 22, 2026)
- Refresh ClickFix staff awareness training — this is the fourth distinct ClickFix campaign in 2026; ensure all clinical and administrative staff know that legitimate systems never ask users to copy and paste commands into a terminal or run window

2. [HIGH] Detect XMRig Cryptominer Abusing Trusted Cloud Ingress in Healthcare

Active since January 2026 and last confirmed May 11, 2026, this campaign targets Healthcare, Manufacturing, Technology, Automotive, and Transportation organizations in the US, Czech Republic, and South Korea. The attacker masquerades PowerShell executables as 'svchost.exe' to bypass Windows Defender and AMSI behavioral detection. Payload delivery uses BITSAdmin — a legitimate Windows Background Intelligent Transfer Service tool — to download password-protected 7Zip archives from GitHub repositories and Google Drive. By routing downloads through these trusted cloud platforms, the actor bypasses web proxies and URL filtering that would normally block downloads from unknown domains.

Once extracted, the XMRig cryptocurrency miner is executed, consuming clinical workstation and server CPU resources for cryptomining. Persistence is established via scheduled tasks with names mimicking Google Update processes, and through WMI event consumer modifications — a technique that survives reboots and is not visible in standard scheduled task enumeration. Healthcare relevance: while the immediate payload is a cryptominer rather than ransomware, the delivery infrastructure (trusted-cloud ingress, AMSI bypass, persistence via WMI) is identical to pre-ransomware staging techniques. A cryptominer deployment should be treated as evidence of a capable actor with persistent access, not a benign nuisance.

Actions:

- Alert on BITSAdmin (bitsadmin.exe) initiating transfers to GitHub.com or drive.google.com; while these platforms are legitimate, BITSAdmin downloading from them is an anomalous pattern in clinical environments

- Alert on svchost.exe processes not launched from C:\Windows\System32 or by the SYSTEM account; masqueraded svchost.exe copies are a reliable indicator of compromise
- Audit all scheduled tasks on clinical workstations and servers; any task referencing Google Update, GoogleUpdate.exe, or similar names that was not created by Google software (verify via signing certificate and file path) should be investigated
- Hunt for WMI event consumer modifications: query __EventFilter, __EventConsumer, and __FilterToConsumerBinding classes for unauthorized subscriptions
- Investigate anomalous CPU usage spikes on clinical workstations and servers — sustained high CPU from non-medical processes is a cryptominer indicator
- Check GitHub and Google Drive access logs (if available via proxy or CASB) for unusual BITSAdmin-sourced downloads; obtain IOC list from GTI portal for confirmed domains and URLs (3 domains, 5 URLs in GTI data)

3. [CRITICAL UPDATE] CVE-2026-0300 (PAN-OS Captive Portal) — Patches Now Available, Apply Immediately

CVE-2026-0300 was first reported in the May 8 brief as an unpatched zero-day. Palo Alto Networks has now released fixes starting the week of May 13, 2026. GTI confirms patch availability for the following branches: PAN-OS 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7, 10.2.18-h6, 11.1.4-h33, 11.1.6-h32, 11.1.7-h6, 11.1.10-h25, 11.1.13-h5, 11.2.4-h17, 11.2.7-h13, 11.2.10-h6, 11.2.12, 12.1.4-h5, and 12.1.7. A second wave covering additional branches is expected around May 28, 2026. CISA added this vulnerability to the KEV catalog on May 5, 2026 (GTI cisa_known_exploited.added_date: Unix timestamp 1778025600 = May 5, 2026 UTC) with a federal deadline of May 9, 2026 — both deadlines have now passed. If you have not yet patched, this is overdue.

GTI analysis from Palo Alto Networks Unit 42 confirms that the exploitation cluster CL-STA-1132 — assessed as likely state-sponsored with hallmarks of Chinese state hacking — escalated post-initial-access to AD enumeration, SAML flood-induced failover to secondary devices, and deployment of tunneling tools EarthWorm and ReverseSocks5. Any organization with an unpatched PAN-OS Captive Portal exposed to untrusted zones or the internet must assume compromise and initiate incident response in addition to patching.

Actions:

- Apply patches from the list above immediately; verify your PAN-OS branch against the fixed version list in Palo Alto advisory PAN-SA-2026-0012
- If your branch is in the second wave (~May 28): disable or restrict Captive Portal to trusted internal zones only as an interim mitigation
- If the portal was exposed prior to patching: treat the device as potentially compromised — hunt for new administrator accounts, unauthorized SSH keys, EarthWorm/ReverseSocks5 tunneling tools, and evidence of AD enumeration from firewall management interfaces
- Healthcare organizations: verify that clinical VLAN segmentation is enforced independently of PAN-OS policy so a compromised firewall cannot collapse network isolation between clinical and administrative environments

Medical Device and IoT Security

Finger Protocol and Legacy OT/IoT Risk

The finger protocol (TCP port 79) is not only present on Windows clinical workstations — it is also present in some legacy OT and embedded systems used in older clinical environments. Port 79 should be blocked at all network segments, including OT VLANs, building management system (BMS) segments, and any segments containing imaging or diagnostic equipment running Windows. Verify that your clinical VLAN firewall rules explicitly deny port 79 in both directions.

Persistent Medical Device Advisories (No New CVEs This Week)

CVE-2026-3650 (GDCM DICOM Memory Leak): No patch available as of May 22, 2026. CISA ICSMA-26-083-01 remains open. Compensating controls remain in effect: network segmentation of PACS and imaging systems, block unauthenticated DICOM connections, monitor for anomalous resource consumption on DICOM-processing hosts.

Contec CMS8000 / Epsimed MN-120 (CVE-2024-12248, CVE-2025-0626): GTI EPSS 0.0068, no active exploitation confirmed as of May 22. FDA disconnect recommendation unchanged.

BeyondTrust CVE-2026-1731: Confirm patching is complete across all vendor remote-access platforms. Any BeyondTrust appliance used for medical device vendor maintenance that remains unpatched should be treated as compromised.

Ivanti EPMM CVE-2026-38125: CISA KEV deadline April 29 has passed. Confirm all instances are patched to 12.4.0.1+.

Activity Trends	Key Numbers This Week
▲ Legacy-protocol abuse (finger/BITSAdmin): new delivery vector for healthcare targeting	CAMP.26.064 IOCs: 0 files | 17 IPs | 41 domains | 29 URLs (live GTI count May 22)
▲ Trusted-cloud-service ingress (GitHub, Google Drive): active bypass of web filtering	XMRig miner IOCs: 0 files | 0 IPs | 3 domains | 5 URLs
▲ ClickFix social engineering: sustained escalation — fourth distinct 2026 campaign	CVE-2026-20182 (Cisco SD-WAN): CVSS 10.0 — CISA KEV deadline May 21 PASSED
▲ Iran-nexus ops (UNC5203): sustained elevated threat to Western healthcare	CVE-2026-0300 (PAN-OS): CVSS 9.8 — patches now available; CISA KEV deadline May 9 PASSED
▲ Post-PAN-OS patch: CL-STA-1132 tunneling tools confirmed — treat unpatched devices as compromised	CVE-2026-3650 (GDCM DICOM): NO PATCH — week 8 of open advisory
▼ Ransomware new incidents: no new confirmed HC ransomware attack reported this week	22 seconds — median access-broker-to-ransomware handoff (M-Trends 2026, still operative)

Sources: Google Threat Intelligence (GTI) | Palo Alto Networks / Unit 42 | CISA — Known Exploited Vulnerabilities Catalog | MITRE ATT&CK | National Vulnerability Database | Bleeping Computer | The Hacker News | SecurityWeek | Rapid7 | Wiz | Arctic Wolf | Horizon3.ai | The Record from Recorded Future News | Cyber Security Agency of Singapore