Executive Summary

Three GTI-verified campaigns are reported as new this week, sourced from Google Threat Intelligence (GTI) and Mandiant. The most operationally urgent is CAMP.26.070 (Luna Moth), a financially motivated vishing and remote-access extortion operation that has been active January–May 2026, specifically targeting US organizations through IT help-desk impersonation over Zoom and Microsoft Teams, staging data to Google Drive and OneDrive, and issuing ransom demands exceeding $11 million — directly relevant to the Scattered Spider pattern already seen targeting hospital help desks. Also new: CAMP.26.060 (FIRESCALE), a GitHub Actions cache-poisoning and supply-chain attack that poisons npm and PyPI packages, deploys a credential stealer targeting 1Password and BitWarden vaults, and includes anti-forensic self-wipe capability — directly threatening healthcare DevOps and integration-engine pipelines. Finally, CAMP.26.038 receives an updated GTI profile this week confirming the use of Microsoft Teams as the initial access vector and GLASSTIDE backdoor in INC ransomware intrusions targeting healthcare organizations — adding specific Teams-channel context to the INC Ransom campaign first reported in the April 10 brief. The dominant theme this week: vishing and legitimate collaboration tool abuse are converging as the primary initial-access vector for both extortion and ransomware against healthcare, making technical perimeter controls alone insufficient.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Technique	Targets	Priority Action
Luna Moth — Vishing, Remote Access & Cloud Exfiltration (CAMP.26.070)	Financial / Extortion	Actors impersonate IT support via Zoom/Teams; manipulate staff into granting remote screen control or allowing physical workstation access; stage W-9, NDA, audit data to Google Drive / OneDrive; extortion demands exceeding $11M; East Europe source region	Technology, Legal & Professional Services — US	CRITICAL — Enforce mandatory out-of-band callback for any remote-access request initiated via Teams or Zoom; alert on bulk cloud upload activity to personal Google Drive or OneDrive from corporate endpoints; brief all help desk staff on Luna Moth lure scenarios
FIRESCALE — GitHub Actions Cache Poisoning & npm/PyPI Supply Chain (CAMP.26.060)	Financial / Supply Chain	Actor (South Africa nexus) uses rclone to scrape repos; poisons GitHub Actions OIDC token cache; publishes trojanized npm and PyPI packages; deploys FIRESCALE credential stealer targeting 1Password and BitWarden vaults; anti-forensic wipe triggered on token revocation	Technology, Healthcare DevOps — Global / Opportunistic	HIGH — Audit GitHub Actions workflows for cache poisoning; rotate all OIDC tokens; inspect npm and PyPI dependencies for newly published packages; verify 1Password and BitWarden vault access logs; confirm CI/CD pipeline secrets are isolated from production systems
INC Ransomware via Microsoft Teams — GLASSTIDE Backdoor (CAMP.26.038 — Updated GTI Profile)	Financial / Ransomware	Actors pose as IT support in Microsoft Teams; convince users to execute trojanized software updates using DLL hijacking; deploy GLASSTIDE custom backdoor; modify registry for persistent RDP access; harvest LSASS/AD credentials; exfiltrate via dual-use tools + cloud clients; mass file encryption with INC ransomware	Healthcare, Manufacturing, Technology — CA, IT	HIGH — Alert on software update execution initiated from Microsoft Teams processes; restrict DLL hijacking vectors via AppLocker; audit registry Run keys and RDP settings for unauthorized persistence; treat INC ransomware detections as full IR events

Top 3 Actions This Week

1. [CRITICAL] Defend Against Luna Moth Vishing & Remote-Access Extortion — CAMP.26.070

Between January and May 2026, GTIG tracked a multi-stage intrusion campaign operated by Luna Moth (CAMP.26.070), a financially motivated group with a confirmed Eastern Europe source region. The group's playbook is entirely social engineering-driven and requires no malware at the point of initial access. Actors contact employees by phone, posing as IT support staff and claiming an urgent issue requires immediate remote assistance. They then convince the target to either initiate a screen-

sharing session via Zoom or Microsoft Teams, or in cases where remote access is restricted, physically step away from their workstation to allow the actor to walk in and operate it directly. Once control is established, the actor methodically browses internal document repositories, identifying and staging high-value files including W-9 forms, NDAs, audit reports, legal documents, and financial records. Exfiltration runs silently through Google Drive or OneDrive, using legitimate cloud traffic that blends with normal business activity. The campaign culminates with extortion: executives receive ransom demands exceeding $11 million, and if unpaid, stolen data is published on dedicated leak sites. GTIG notes the campaign was active as recently as May 28, 2026. IOCs include 1 domain and 1 IP address on file in the GTI portal.

Why this matters for healthcare specifically: Hospital IT help desks handle urgent calls around the clock, often under staffing pressure with a culture of immediate patient-care support. Luna Moth's lures exploit exactly this environment. The Scattered Spider (UNC3944) hospital help-desk pattern first reported in the May 8 brief and Luna Moth now represent two distinct, concurrently active actor groups using the same fundamental technique. Healthcare organizations must treat all remote-access requests initiated via collaboration tools as requiring independent verification.

- Implement a mandatory out-of-band manager callback protocol for all requests to grant remote access, share screen, or accept remote assistance via any platform (Teams, Zoom, WebEx, Slack huddle) with no exceptions for urgency claims; the callback must go to a known number on HR/IT file, not a number provided by the caller
- Alert on bulk upload activity from corporate endpoints to personal Google Drive or consumer OneDrive accounts as this is the exfiltration channel; DLP tools should flag large outbound transfers to personal cloud storage domains
- Train all employees and not just IT staff on the Luna Moth scenario specifically: legitimate IT will never ask you to start a Zoom call to troubleshoot your computer, and will never ask you to step away from your workstation to let someone else operate it
- Restrict Teams external access: configure Teams to block direct messages and calls from external tenants unless explicitly allow-listed; Luna Moth and INC ransomware actors (CAMP.26.038) both abuse Teams external messaging to reach employees

2. [HIGH] Audit GitHub Actions and Package Dependencies for FIRESCALE Supply Chain Attack — CAMP.26.060

Since May 10, 2026, GTIG has tracked CAMP.26.060, a financially motivated supply-chain attack originating from a South Africa-nexus threat actor. The campaign exploits a specific weakness in GitHub Actions CI/CD pipelines: the actor uses anonymizing networks to scrape target repositories via *rclone*, then poisons GitHub Actions OIDC token caches. Using those harvested tokens, the actor publishes trojanized versions of legitimate npm and PyPI packages. When developers or automated build pipelines install these packages, the FIRESCALE credential stealer is deployed. FIRESCALE specifically targets password manager vaults — 1Password and BitWarden — to harvest all stored credentials in a single operation. Critically, the actor has implemented destructive anti-forensic safeguards: if token revocation is detected, the malware recursively wipes the compromised system to destroy evidence. For healthcare organizations, this campaign is directly relevant to any team running integration engines that use npm or Python package dependencies, or any DevOps pipeline deploying healthcare application code.

- Immediately audit all GitHub Actions workflows in your organization: look for unexpected cache read/write steps, newly added or modified workflow files, and any steps that publish to npm or PyPI registries as these are indicators of cache-poisoning activity
- Rotate all GitHub OIDC tokens and Personal Access Tokens (PATs) used in CI/CD pipelines, especially any with package-publish permissions
- Inspect recently installed npm and PyPI packages in your build pipelines against known-good checksums and focus on packages installed or updated between May 10–29
- Check 1Password and BitWarden access logs for any developer machines that ran affected pipelines — if FIRESCALE reached a vault, treat all stored credentials as compromised and rotate

- Pin npm and PyPI package versions in all package.json and requirements.txt files and use private registries or artifact proxies where possible to reduce exposure to upstream poisoning
- Be aware of the anti-forensic wipe: if you detect unusual file deletion activity or system wipe behavior on a developer or build machine, treat it as a FIRESCALE incident and begin forensics immediately before additional evidence is destroyed
- Healthcare-specific: integration engines and EHR build pipelines often run with elevated access to production HL7 routing and clinical databases — if a FIRESCALE-poisoned package was installed in one of these pipelines, the harvested vault credentials likely include database connection strings and API keys for clinical systems

3. [HIGH] Block INC Ransomware Teams Delivery Vector — GLASSTIDE Backdoor (CAMP.26.038 Updated)

GTIG has this week published an updated and expanded profile for CAMP.26.038, confirming that the INC ransomware operator targeting healthcare organizations uses Microsoft Teams as its primary initial-access channel which is detail not previously available in this brief series. Beginning earlier this year, the actor contacts employees via Microsoft Teams posing as IT support, convincing them to download and execute what appears to be a legitimate software update. The update uses DLL hijacking to silently load the GLASSTIDE custom backdoor while displaying a convincing progress bar. GLASSTIDE establishes a C2 channel, installs legitimate remote management software for persistent access, and modifies registry settings to enable RDP connectivity without relying solely on the backdoor. Post-access, the actor uses native tools (SYSTEMINFO, NLTEST, credential dumping from LSASS and NTDS) to enumerate the environment and harvest high-value credentials. After staging sensitive data on internal network shares, it uses legitimate dual-use administration tools and cloud storage clients for exfiltration, then deploys INC ransomware for mass file encryption. GTI confirms healthcare as a targeted industry. IOCs include 4 files, 1 domain, and 1 IP address.

- Configure Microsoft Teams to block or restrict external tenant messages and calls: go to Teams Admin Center > External Access and limit which external domains can contact your users — this removes the primary delivery channel for both Luna Moth and this campaign
- Alert on DLL hijacking patterns: specifically, alert on legitimate processes loading unsigned DLLs from non-standard paths, and on processes spawning cmd.exe or PowerShell following a software-update download initiated from a Teams conversation
- Block execution of software installers and update files that arrive via Teams file-sharing — legitimate enterprise software updates do not arrive as Teams attachments; add this to your security awareness training
- Alert on unusual registry modifications enabling RDP: monitor for changes to HKLM\System\CurrentControlSet\Control\Terminal Server and related keys, especially if made by non-standard processes

A notable breach: NYC Health + Hospitals (NYCHHC) Third-Party Vendor Breach — 1.8 Million Individuals Affected

Disclosed: May 19, 2026 | Reported to HHS: March 24, 2026 | Affected: ~1.8 million patients and employees | Sector: Public Healthcare (Largest US municipal health system)

- NYC Health + Hospitals Corporation (NYCHHC), the largest public health system in the United States serving over one million New Yorkers, confirmed on May 19, 2026 that an unauthorized third party accessed its network from approximately November 25, 2025 through February 11, 2026 — a period of 11 weeks — before being detected and removed. The intrusion originated through a security compromise at an unnamed third-party vendor with access to NYCHHC systems. During the access window, attackers exfiltrated files containing an unusually broad set of sensitive data: diagnoses, medications, test results and imaging, health insurance information, billing and payment records, Social Security numbers, passports and driver's licenses, precise geolocation data, and critically, biometric fingerprint and palm-print scans.

Biometric data cannot be changed, making this category of exposure a permanent, long-term risk for affected individuals. Investigators believe initial access was gained via the unnamed vendor, but the specific vulnerability has not been publicly disclosed.

Medical Device and IoT Security

No New Medical Device CVEs This Week

CVE-2026-3650 (GDCM DICOM Memory Leak): No patch available as of May 29, 2026. CISA advisory ICSMA-26-083-01 remains open; week 9 of unpatched critical advisory. Continue network segmentation of PACS and imaging systems, blocking unauthenticated DICOM, and monitoring for anomalous memory consumption on imaging hosts.

CVE-2026-0300 (PAN-OS Captive Portal Zero-Day): Wave 2 patches were expected around May 28, 2026, covering additional PAN-OS maintenance branches beyond the wave 1 release (~May 13). Confirm all PA-Series and VM-Series firewalls are now patched across both wave 1 and wave 2 branches. Any firewall not patched prior to May 8 disclosure should be treated as potentially compromised and an IR review initiated. Root-level firewall compromise provides full visibility into clinical VLAN traffic including medical device communications.

Contec CMS8000 / Epsimed MN-120 (CVE-2024-12248, CVE-2025-0626): GTI EPSS score 0.0068 — no known active exploitation as of May 29. FDA disconnect recommendation remains in force.

BeyondTrust CVE-2026-1731: Confirm patching is complete across all vendor remote-access platforms. Relevant to the FIRESCALE campaign this week: medical device vendor remote-access credentials stored in 1Password or BitWarden vaults are exactly the type of credential FIRESCALE targets; if any engineer with BeyondTrust access ran a compromised pipeline, treat those credentials as exposed.

Medtronic / ShinyHunters (from earlier brief): Medtronic's investigation is ongoing. Healthcare organizations should continue to verify that Medtronic device support connections are isolated from general corporate network paths, and audit any credentials shared with Medtronic vendor portals.

Activity Trends	Key Numbers This Week
▲ Vishing via Teams/Zoom: confirmed as primary initial-access vector for extortion and ransomware	**3 new GTI-verified campaigns | 2 directly relevant to healthcare**
▲ CI/CD supply chain attacks: FIRESCALE adds new anti-forensic wipe capability to npm/PyPI threat landscape	$11M+ — Luna Moth ransom demands against US organizations (confirmed)
▲ Password manager targeting: 1Password and BitWarden vaults now explicitly in attacker crosshairs	FIRESCALE: 2 GTI subscribers — supply chain campaign under active community tracking
▲ Healthcare ransomware (INC, SPHINXLOCKER, Lynx): sustained elevated posture	**CVE-2026-0300 (PAN-OS): wave 2 patches expected ~May 28 — verify all branches patched**
◀ ClickFix lure volume: declining from May 22 peak but still active (CAMP.26.064, CAMP.26.059)	**CVE-2026-3650 (GDCM): no patch — week 9 of open advisory**
▼ Email phishing as initial vector: continued sustained decline (M-Trends 2026)	CIRCIA rulemaking: finalization expected ~May–June 2026 — prepare mandatory incident reporting workflows now

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.