



Executive Summary

Three GTI-verified campaigns are reported this week, sourced from Google Threat Intelligence (GTI), CISA, Rapid7, Palo Alto Networks, and Cisco Talos. The most critical is CAMP.26.091, a suspected PRC-nexus espionage campaign conducting widespread exploitation of CVE-2026-0257 — an authentication bypass in the PAN-OS GlobalProtect portal and gateway that allows a remote, unauthenticated attacker to forge authentication cookies and establish VPN connections into the internal network. The vulnerability carries a CVSS base score of 9.1 (NVD), is rated P1 by GTI with confirmed in-the-wild exploitation since May 17, 2026 (Rapid7), has publicly available proof-of-concept exploit code, and was added to the CISA KEV catalog on May 29, 2026 with a federal deadline of June 1 — now passed. In victim environments where deep access was achieved, the actor unregistered Duo MFA modules and abused Active Directory Certificate Services to forge trusted certificates, ultimately gaining administrative control of Azure and Microsoft 365.

CAMP.26.090, a Vietnam-nexus financially motivated campaign active against U.S. healthcare through July 1, 2026, chaining phishing, legitimate RMM tools, and covert email inbox-rule modification to harvest credentials and sensitive data; and CAMP.26.092, a strategic web compromise campaign injecting the FLUTECLICK JavaScript profiler into compromised WordPress sites, with several June handoffs to a financially motivated actor holding historical RHYSIDA ransomware deployment ties — a group with an extensive hospital victim record.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Technique	Targets	Priority Action
PRC-Nexus GlobalProtect Exploitation — CVE-2026-0257 (CAMP.26.091)	Espionage / Vulnerability Exploitation	Widespread exploitation of CVE-2026-0257 authentication bypass in PAN-OS GlobalProtect portals/gateways beginning early June 2026 (forged authentication override cookies via /ssl-vpn/login.esp); post-compromise unregistering of Duo MFA modules and abuse of AD Certificate Services to forge trusted certificates, gaining administrative control of Azure and Microsoft 365; earlier March 2026 phase abused legitimate remote support tools to deploy the SNOWLIGHT downloader	Healthcare, Pharmaceuticals, Government, Financial Services + 9 other GTI-confirmed industries — US, UK, FR, ES, BR, IN + others	CRITICAL — Patch PAN-OS per PAN-SA advisory; CISA KEV deadline June 1 passed — verify compliance now; disable/rotate authentication override cookies; hunt for forged-cookie logins
Vietnam-Nexus Phishing → RMM Access & Credential Harvesting (CAMP.26.090)	Financial / Credential Theft	Phishing for initial access; installation of legitimate remote access/RMM tools for persistence; modification of victim email inbox rules to conceal activity; harvesting of credentials and sensitive data; GTI links eight malware families and 107 attack techniques to this activity; active through July 1, 2026	Healthcare, Manufacturing, Technology — US (GTI-confirmed)	HIGH — Audit mailbox inbox rules (forwarding/auto-delete); alert on unapproved RMM tool installation; enforce phishing-resistant MFA; review OAuth grants
FLUTECLICK WordPress Web Compromise → Ransomware-Linked Handoff (CAMP.26.092)	Initial Access / Reconnaissance / Ransomware Precursor	Strategic web compromise of public-facing WordPress sites (frequently exploiting the Divi theme); injection of the FLUTECLICK JavaScript profiler (generic filenames, e.g. file.js) hosted on newly registered .xyz/.lol domains; ClickFix social engineering; visitor profiling used to select targets, with several June 2026 handoffs to a	Industry targeting not yet confirmed in GTI; healthcare relevance driven by RHYSIDA's extensive hospital victim history and WordPress use in	HIGH — Scan all public WordPress properties for injected JavaScript; audit Divi theme versions; block newly registered .xyz/.lol domains; treat any FLUTECLICK detection as pre-



Campaign	Type	Key Technique	Targets	Priority Action
		financially motivated actor with historical RHYSIDA ransomware deployment ties	patient-facing portals	ransomware reconnaissance

Top 3 Priority Actions This Week

1. [CRITICAL] Patch PAN-OS GlobalProtect CVE-2026-0257 and Hunt for Forged-Cookie Access (CAMP.26.091)

CVE-2026-0257 is an authentication bypass (CWE-565 — reliance on cookies without validation and integrity checking) in the PAN-OS GlobalProtect portal and gateway. When authentication override cookies are enabled, an unauthenticated attacker can extract the public key from the appliance's TLS certificate, forge an encrypted authentication cookie, and submit it to the `/ssl-vpn/login.esp` endpoint to obtain a valid session and full VPN tunnel — no credentials required. Rapid7 confirmed successful exploitation across numerous customer environments beginning May 17, 2026, with a second wave on May 21; Palo Alto Networks acknowledged exploit attempts against unpatched devices on May 29, the same day CISA added the CVE to the KEV catalog with a June 1 federal deadline. Proof-of-concept exploit code is publicly available and GTI EPSS now sits at 0.87 (99.7th percentile). GTI attributes the June exploitation wave to a suspected PRC-nexus espionage actor that, in deep-access cases, unregistered Duo MFA modules and forged certificates via AD Certificate Services to seize Azure/M365 administrative control. Panorama and Cloud NGFW are not affected. Healthcare organizations widely use GlobalProtect for clinician and vendor remote access — a forged-cookie login lands an attacker directly inside the clinical network.

- Patch immediately per Palo Alto Networks advisory (security.paloaltonetworks.com/CVE-2026-0257); the KEV deadline has passed — verify compliance across every PA-Series, VM-Series, and Prisma Access deployment now
- If patching is delayed: disable authentication override cookies, or rotate the certificate used to encrypt them and ensure it is not reused for any other service (e.g., the HTTPS portal) — certificate reuse is what enables the forgery
- Hunt for exploitation: POST requests to `/ssl-vpn/login.esp` with cookie authentication from hosting providers (Vultr, Dromatics Systems); the spoofed MAC address `aa:bb:cc:dd:ee:ff`; and source IPs 104.207.144.154, 146.19.216.119, 146.19.216.120, 146.19.216.125 (Rapid7-reported)
- Audit Duo/MFA integration health — alert on unregistered or removed MFA modules — and review AD Certificate Services issuance logs for unexpected certificate templates or enrollments
- Review Azure AD / M365 for new admin role grants, unfamiliar app registrations, and unauthorized Conditional Access changes since mid-May
- **A special advisory was issued regarding this priority item last week to all Cloudwave customers.**

2. [HIGH] Counter Phishing → RMM → Inbox-Rule Credential Harvesting (CAMP.26.090)

Active since late November 2025 and observed through July 1, 2026, a Vietnam-nexus financially motivated actor is targeting U.S. healthcare, manufacturing, and technology organizations. The chain: phishing for initial access, installation of legitimate remote access/RMM tooling for hands-on persistence, covert modification of victim email inbox rules (to hide security alerts and conversation threads), and harvesting of credentials and



sensitive data. GTI associates eight malware families and 107 attack techniques with this campaign. Inbox-rule manipulation is a hallmark of business email compromise and payer/billing fraud in healthcare — rules that auto-delete or re-route messages are frequently the only early indicator.

- Audit mailbox inbox rules tenant-wide — flag rules that forward externally, move messages to RSS/archive folders, or delete based on security-related keywords
- Alert on installation or execution of RMM tools not on your approved list; enforce application allowlisting for remote access software
- Enforce phishing-resistant MFA (FIDO2) for email and VPN access, prioritizing finance, billing, and executive mailboxes
- Review recent OAuth application grants and revoke unrecognized mail-access permissions

3. [HIGH] Audit Public WordPress Properties for FLUTECLICK Injection (CAMP.26.092)

GTI is tracking a strategic web compromise campaign in which a financially motivated group systematically compromises public-facing WordPress sites — frequently exploiting the popular Divi theme — and injects the FLUTECLICK JavaScript profiler, typically delivered under generic filenames (e.g., file.js) from attacker-controlled, newly registered .xyz and .lol domains. FLUTECLICK profiles site visitors as a reconnaissance stage to select high-value targets for follow-on intrusion, and GTI documented several handoffs throughout June 2026 to a second financially motivated actor with historical RHYSIDA ransomware deployment ties. Note: GTI has not yet confirmed targeted industries for this campaign; it is included because RHYSIDA has one of the most extensive hospital victim records of any RaaS operation, and healthcare organizations commonly run WordPress for patient-facing portals and marketing sites. Activity was last observed July 1, 2026.

- Inventory and scan all public WordPress properties (marketing sites, foundation pages, patient education portals) for unauthorized injected JavaScript
- Update or remove the Divi theme where present; enforce automatic core/theme/plugin patching and file-integrity monitoring on WordPress hosts
- Block or alert on outbound requests to newly registered .xyz and .lol domains from corporate and clinical networks
- Treat any FLUTECLICK or ClickFix detection as pre-ransomware reconnaissance and escalate to priority incident handling — the handoff pattern mirrors the 22-second access-broker reality documented in M-Trends 2026

Medical Device and IoT Security

Two New DICOM Library Vulnerabilities This Week. CVE-2026-56445 (pydicom/pynetdicom, NEW): The qrscp application's C-STORE handler uses an attacker-supplied DICOM dataset instance directly in file path construction without sanitization, allowing arbitrary file writes via path traversal (CWE-22). CVSS 9.1 (v3.1) / 8.8 (v4.0). Disclosed June 25, 2026 in CISA medical advisory ICSMA-26-176-01 — the companion advisory to ICSMA-26-176-02 (OHIF, covered in the June 26 brief). A patch and workaround are available; no exploitation has been observed. pydicom/pynetdicom are foundational open-source libraries embedded across research imaging, PACS tooling, and DICOM routing scripts — inventory where they run, not just what's installed.

CVE-2026-22879 (vtk-dicom, NEW): A heap-based buffer overflow in the vtkDICOMItem data element handling of vtk-dicom 9.5.2 (CWE-129) allows a specially crafted DICOM file to corrupt memory, with potential arbitrary code execution. CVSS 8.1. Disclosed June 25, 2026 by Cisco Talos (TALOS-2026-2366) with fixes available; also tracked by Red Hat for



Fedora/ParaView packages. No exploitation observed. Applies to visualization and research pipelines built on VTK.

Both vulnerabilities are triggered by processing a malicious DICOM file — the same ingestion-path risk class as GDCM CVE-2026-3650. Compensating controls are shared: block DICOM ingestion from unauthenticated sources, segment imaging networks, and validate files at the boundary before library parsing.

CVE	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-56445 (NEW)	pydicom / pynetdicom qrsdp (DICOM C-STORE)	9.1	CISA ICSMA-26-176-01 (Jun 25)	Yes	Path traversal — unsanitized DICOM dataset instance used in file paths allows arbitrary file writes. No known exploitation. Apply patch; workaround and firewall guidance available in advisory.
CVE-2026-22879 (NEW)	vtk-dicom 9.5.2 (VTK DICOM toolkit)	8.1	Cisco Talos TALOS-2026-2366 (Jun 25)	Yes	Heap-based buffer overflow in vtkDICOMItem parsing; crafted DICOM file can enable code execution. No known exploitation. Patch imaging/research pipelines using vtk-dicom.
CVE-2026-3650	Grassroots DICOM (GDCM) 3.2.2	7.5	CISA ICSMA-26-083-01	NO	Week 15 with no patch — GDCM maintainer remains unresponsive to CISA. Maintain PACS segmentation, block unauthenticated DICOM ingestion, and continue escalating with imaging vendors.
CVE-2026-12473	OHIF DICOM Web Viewer	8.2	CISA ICSMA-26-176-02	Yes	SSRF; patched in OHIF v3.12.2 (added June 26 brief). Confirm the patch is deployed on all OHIF instances.
CVE-2026-0611	Spacelabs Sentinel cardiac monitoring	9.8	June 12 brief	Yes	Unauthenticated RCE; patched in v1l.6.0. Confirm deployment complete.
CVE-2026-43994	coturn TURN/STUN (telehealth WebRTC)	8.1	June 19 brief	Yes	Stack buffer overflow in OAuth token decoding; patch to coturn 4.10.0 across telehealth stacks.
CVE-2024-12248 / CVE-2025-0626	Contec CMS8000 patient monitors	9.8	FDA / CISA	N/A	FDA disconnect recommendation remains in force; no active exploitation observed.

CVE-2026-3650 status note: the CISA advisory (ICSMA-26-083-01) is now in its 15th week. CISA reports the GDCM maintainer has not responded to coordination requests, and downstream distributions (e.g., Debian) list the fix as postponed. Continue escalating with imaging vendors for a patched-library ETA and document all vendor responses for HIPAA risk-analysis records.

Activity Trends	Key Numbers This Week
▲ Edge/VPN authentication-bypass exploitation: CRITICAL — PRC-nexus, public PoC, CISA KEV deadline passed ▲ RMM tool abuse following phishing in healthcare: rising (CAMP.26.090 active through July 1) ▲ Strategic web compromise + ClickFix reconnaissance feeding ransomware handoffs: emerging ▲ Medical imaging (DICOM) library CVE disclosures: 2 new this week; 4 open in tracker ► Healthcare ransomware activity: sustained — no material change vs. prior week	CVE-2026-0257: CVSS 9.1 (NVD), GTI P1, EPSS 0.87 (99.7th percentile) — KEV deadline June 1 PASSED 44 new GTI-verified IOCs across 3 campaigns CVSS 9.1 — pydicom/pynetdicom path traversal (ICSMA-26-176-01) CVE-2026-3650 (GDCM): NO PATCH — week 15 of open advisory HIPAA Security Rule 90 FR 800: still a proposed rule as of July 3

Google (TALOS-2026-2366), NVD, Red Hat, Arctic Wolf, HIPAA Journal, Federal Register, Mandiant M-journal-2026-07-01, Rapid7, Palo Alto Networks PSIRT & Unit 42, Cisco Talos (TALOS-2026-2366)