Executive Summary

Three GTI-verified campaigns are reported this week, sourced from Google Threat Intelligence (GTI), CISA, and Palo Alto Networks Unit 42. The most critical is CVE-2026-0300, a zero-day out-of-bounds write (CWE-787) in the Palo Alto Networks PAN-OS User-ID Authentication Portal (Captive Portal) — CISA added it to the KEV catalog on May 6 with a federal deadline of May 9, and no patch is yet available. GTI rates this P0 with a CVSS base score of 9.8. Also new this week: two linked campaigns directly targeting US healthcare organizations — CAMP.26.055, a ClickFix social engineering access-broker campaign active as recently as May 7, and CAMP.26.053, a heavily obfuscated PowerShell intrusion operation flagged by GTI as consistent with pre-ransomware activity, last observed May 1. The dominant theme this week: a no-patch critical network infrastructure zero-day under active state-sponsored exploitation, and a live access-broker-to-pre-ransomware chain actively targeting healthcare.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Technique	Targets	Priority Action
PAN-OS User-ID Auth Portal Zero-Day — CVE-2026-0300	Zero-Day / RCE (NO PATCH)	Out-of-bounds write (CWE-787) in PAN-OS Captive Portal / User-ID Authentication Portal; unauthenticated RCE with root privileges via crafted HTTP packets; CVSS 9.8 (GTI P0); affects PA-Series and VM-Series firewalls; Unit 42 attributes to likely state-sponsored cluster; first exploitation attempts observed April 9; NO PATCH until ~May 13	Healthcare, Government, Technology, Finance — Global (PA-Series/VM-Series with Captive Portal exposed)	CRITICAL — No patch yet: restrict Captive Portal to trusted zones only or DISABLE immediately; apply patches when released (~May 13); CISA KEV federal deadline May 9
ClickFix Social Engineering Initial Access — CAMP.26.055 (UNC6844)	Initial Access / Pre-Ransomware	UNC6844 lures victims via Microsoft Edge and Chrome to actor-controlled domains; ClickFix lures masquerade as technical support or system verification steps; victims manually execute malicious commands providing initial foothold; hands access directly to CAMP.26.053 secondary actor; 18 C2 domains, 30 IOCs; GTI last seen May 7, 2026	Healthcare, Education — US	HIGH — Block .js and script execution from browser download paths; train staff to recognize fake technical support/verification lures; treat any ClickFix detection as potential ransomware precursor
Obfuscated PowerShell Pre-Ransomware — CAMP.26.053 (Healthcare Direct Targeting)	Espionage / Pre-Ransomware	Heavily obfuscated Base64-encoded PowerShell downloads and executes secondary payloads in-memory; persistence via registry Run keys (ASEP); malicious DLL drops; CSC.EXE used to compile payloads on disk; post-exploitation SYSTEMINFO/IPCONFIG/NLTEST consistent with pre-ransomware reconnaissance; 117 IOCs; GTI last seen May 1, 2026; receives access from CAMP.26.055	Healthcare, Pharmaceuticals, Government, Education — US	HIGH — Alert on obfuscated Base64 PowerShell execution and in-memory payload activity; audit registry Run keys; ensure EDR behavioral coverage on clinical Windows endpoints; treat SYSTEMINFO/NLTEST bursts as imminent-ransomware indicator; verify offline backups

Top 2 Actions This Week

1. Critical Mitigate PAN-OS Zero-Day CVE-2026-0300 No Patch Yet

On May 6, 2026, CISA added CVE-2026-0300 to the Known Exploited Vulnerabilities catalog, setting a federal remediation deadline of May 9 — one of the shortest KEV windows seen this year. The vulnerability is an out-of-bounds write (CWE-787) in the PAN-OS User-ID Authentication Portal (Captive Portal), a feature used to authenticate users whose identities the firewall cannot automatically map. An unauthenticated attacker can send specially crafted HTTP packets to execute arbitrary code with root privileges on affected PA-Series and VM-Series firewalls. GTI rates this P0

with a CVSS base score of 9.8. As of publication, no patch exists: Palo Alto Networks expects to release fixes starting around May 13, 2026, for the most common maintenance branches. Palo Alto Networks Unit 42 attributes active exploitation to a likely state-sponsored cluster, with the first failed exploitation attempts logged on April 9, 2026. Incident response firms have reported spikes in related intrusion attempts since disclosure, and proof-of-concept exploit code has been observed circulating on underground forums. This vulnerability does not affect Cloud NGFW, Prisma Access, or Panorama appliances.

- Immediate mitigation — no patch available: navigate to Device > User Identification > Authentication Portal Settings and either restrict the portal to trusted internal zones only OR disable it entirely if Captive Portal is not required in your environment
- Identify all internet-exposed PA-Series and VM-Series firewalls using your asset inventory; use Palo Alto's advisory PAN-SA-2026-0012 to confirm whether your PAN-OS versions are in the affected ranges and prioritize those with the Captive Portal feature enabled
- Monitor for exploitation indicators: shellcode injection into nginx worker processes (as reported by Unit 42), unexpected outbound connections from firewall management interfaces, and new administrator accounts or SSH keys on affected devices
- Apply patches as soon as they are released (~May 13): the first wave covers PAN-OS 12.1.4-h5, 11.2.7-h13, 11.2.10-h6, 11.1.4-h33, 11.1.6-h32, 11.1.10-h25, 11.1.13-h5, 10.2.10-h36, and 10.2.18-h6; a second wave (~May 28) covers additional branches
- Healthcare organizations: Palo Alto firewalls are common perimeter and data center edge devices in clinical networks, a root-level compromise gives an attacker the ability to intercept all network traffic, modify routing, and pivot directly into clinical and medical device VLANs
- If you suspect exploitation prior to patching, treat the firewall as compromised and initiate an IR engagement: look for persistent backdoors, web shells, and unauthorized configuration changes

2. High Block ClickFix Initial Access Chain — CAMP.26.055 + CAMP.26.053

GTI has identified two linked campaigns actively targeting US healthcare and pharmaceutical organizations as of the week of May 8, 2026. CAMP.26.055 (GTI last seen May 7) is operated by UNC6844 and uses ClickFix-style browser lures to trick users into manually running malicious commands. The actor directs victims to actor-controlled domains via Microsoft Edge and Chrome, disguising the initial execution as a routine technical support or system verification step. Once the foothold is established, UNC6844 hands access directly to the secondary actor behind CAMP.26.053, which has been active since April 13 and was last observed May 1, 2026. CAMP.26.053 demonstrates advanced post-compromise capabilities on Windows endpoints: heavily obfuscated, Base64-encoded PowerShell commands download and execute secondary payloads entirely in memory to evade file-based detection. Persistence is established via registry Run keys (ASEP modification). The actor also drops malicious DLLs and uses the native C# compiler CSC.EXE to compile additional tooling directly on disk. Post-exploitation reconnaissance using SYSTEMINFO, IPCONFIG, and NLTEST is explicitly flagged by GTI as consistent with pre-ransomware staging. GTI confirms Healthcare, Pharmaceuticals, Government, and Education as targeted industries. 117 IOCs are on file.

- Block execution of .js files and script content downloaded via browser paths — this is the primary delivery mechanism for the CAMP.26.055 ClickFix lure; AppLocker or equivalent policy applied to browser download folders stops this chain at step one
- Train staff to recognize ClickFix lures — any browser prompt asking a user to manually copy and paste a command, open Run/PowerShell, or execute a "verification step" is an attack; this applies to clinical and administrative staff equally
- Alert on Base64-encoded PowerShell execution (powershell.exe -EncodedCommand) from any clinical endpoint — this is the CAMP.26.053 payload delivery mechanism and should never occur on a standard workstation or nursing terminal
- Alert on CSC.EXE (C# compiler) executing on non-developer endpoints — legitimate healthcare workstations have no reason to compile code on disk; this is a strong indicator of CAMP.26.053 activity

- If SYSTEMINFO, IPCONFIG, and NLTEST are observed running in rapid succession from the same host, treat this as an imminent-ransomware indicator and initiate IR immediately — GTI explicitly flags this reconnaissance pattern as pre-ransomware staging
- Audit registry Run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent) on all clinical Windows endpoints for unexpected entries — CAMP.26.053 establishes persistence here
- Verify offline, immutable backups for EHR, PACS, and pharmacy systems are current and tested — GTI's pre-ransomware classification means encryption may follow quickly if this campaign is not caught at the reconnaissance stage
- Block the 18 CAMP.26.055 C2/distribution domains and review the 117 CAMP.26.053 IOCs in the GTI portal; prioritize adding both sets to perimeter and endpoint controls

GTI Campaign IDs: CAMP.26.055 (first seen March 23, last seen May 7, 2026) and CAMP.26.053 (first seen April 13, last seen May 1, 2026). Both confirmed targeting Healthcare and Education, US-based.

Medical Device and IoT Security

- CVE-2026-3650 (GDCM DICOM Memory Leak), no patch available as of May 8, 2026; compensating controls remain in effect. Contec CMS8000 FDA disconnect recommendation unchanged. BeyondTrust CVE-2026-1731: confirm patching complete across all vendor remote-access platforms.

Sources: Google Threat Intelligence (GTI), CISA, Mandiant M-Trends 2026, Palo Alto Networks Unit 42 (PAN-SA-2026-0012), , Check Point Research, Shadowserver Foundation, MITRE ATT&CK,