Executive Summary

3 active threat campaigns are currently being tracked by the Google Threat Intelligence Group (GTIG), targeting organizations across Education, Healthcare, Technology, Legal & Professional Services, Manufacturing, Telecommunications, and Transportation sectors in the United States, United Kingdom, and Hong Kong. High priority: A North Korea-nexus actor has successfully tampered with GitHub source code repositories, representing an active supply chain risk. ClickFix-based social engineering lures continue to be leveraged across both Windows and macOS environments. Total IOC count: 128+ indicators

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
CAMP.26.017 · ClickFix Lures + Defender Evasion	Malware	Healthcare, Education, US, UK, HK	Fake browser update lures execute PowerShell; CFGHELPER scheduled task for persistence; Windows Defender exclusions for evasion; blockchain-based C2	Remove unauthorized Scheduled Tasks; audit Defender exclusion lists; restrict PowerShell execution policy
AI-Lure Malvertising → macOS Stealer	Malware/ Credential Theft	Technology — US, UK	AI-generated fake "how-to" ads instruct users to run cURL commands; ATOMICPROMPT stealer bypasses macOS Gatekeeper; elevates privileges via sudo	Train macOS users on terminal-based lures; enforce Gatekeeper; monitor unsigned binary execution
CAMP.26.014 · North Korea Python Backdoor + GitHub Tampering	Espionage/ Supply Chain	Technology - US	Obfuscated Python C2 masquerades as MongoDB traffic on port 27017; actor successfully force-pushed unauthorized code to victim GitHub repositories	Enforce GitHub branch protection and require PR reviews; block port 27017 from non-DB systems; audit repo push logs

Top 2 Actions This Week

1. **Enforce GitHub branch protection rules immediately.** The North Korea-nexus actor in CAMP.26.014 has successfully modified source code in victim repositories via unauthorized force-pushes. Require pull request reviews on all protected branches and enable audit logging for all push events without delay.

2. **Educate users on ClickFix and AI-generated social engineering lures.** Both CAMP.26.017 and CAMP.25.088 rely on convincing users to manually execute malicious commands — via fake browser updates on Windows and fake instructional ads on macOS. User awareness is the primary defensive layer against both campaigns.

Campaign Details

CAMP.26.017 — ClickFix Lures with Scheduled Task Persistence and Defender Evasion

Last Observed: Feb 26, 2026 | **IOCs:** 22 (12 files, 10 domains) | **MITRE Techniques:** 33

An unknown actor deployed fake browser update prompts (ClickFix lures) to execute obfuscated PowerShell and VBScript loaders entirely in-memory, evading file-based detection. Malware was silently installed via MSI packages. The actor established persistence via a Scheduled Task named

CFGHELPER and blinded Windows Defender by adding custom exclusions via Add-MpPreference. Late-stage C2 communications leveraged blockchain infrastructure as a dead drop resolver to obscure command-and-control addresses.

CAMP.25.088 — AI-Generated Malvertising Targeting macOS Systems

Last Observed: Feb 21, 2026 | **IOCs:** 99 (7 files, 52 domains, 1 IP, 39 URLs) | **MITRE Techniques:** 34

An unknown threat actor embedded AI-generated instructional content inside malicious advertisements — mimicking guides such as *"How to Install Google Drive on macOS"* — to deliver ClickFix instructions to macOS users. Victims were directed to run cURL commands that downloaded staging scripts. Those scripts then repeatedly prompted for the user's system password, escalated privileges via sudo, bypassed macOS Gatekeeper, removed quarantine attributes, and delivered the **ATOMICPROMPT** stealer as a final payload.

CAMP.26.014 — North Korea-Nexus Python Backdoor and GitHub Repository Tampering

Last Observed: Feb 18, 2026 | **IOCs:** 7 (1 file, 2 IPs, 4 URLs) | **MITRE Techniques:** 11 | **Origin:** KP North Korea (DPRK)

A DPRK-attributed actor used obfuscated Python scripts to establish in-memory C2, communicating over port 27017 to blend in with legitimate MongoDB database traffic. Secondary payloads were retrieved via custom HTTP headers containing large alphanumeric strings as a covert channel. The actor then escalated to directly targeting victim GitHub repositories, successfully executing an unauthorized force-push to the main branch and modifying the organization's source code — a significant supply chain risk.

Resources: Google Threat Intelligence | MITRE ATT&CK (attack.mitre.org) | CISA Alerts (cisa.gov)
Report suspicious calls or emails to your IT security team immediately.