Executive Summary

This edition covers active threat campaigns relevant to Healthcare and Technology sectors. Three campaigns are new this week and one (DPRK GitHub Tampering, CAMP.26.014) was first reported in the Feb 27 brief and continues to escalate. **The most critical new entry is the March 11 wiper attack on Stryker Corporation, attributed to Iran-linked group Handala (UNC5203), which disrupted EKG transmission systems and medical device operations globally. With U.S.-Iran military tensions ongoing, all Healthcare and Technology organizations should treat Iran-nexus threats as elevated.**

Active Threat Campaigns- Healthcare & Technology

> *Note: DPRK GitHub Code Tampering (CAMP.26.014) is highlighted in amber — it was first reported in the Feb 27 brief and is carried over due to continued escalation.*

Campaign	Type	Key Techniques	Targets	Priority Action
Stryker Wiper Attack (GLOBAL.26.002)	Destruction / Hacktivism	UNC5203 / Handala (Iran)	Healthcare, MedTech — US, EU	Wiper destroys Microsoft environment; Lifenet EKG system taken offline; device wipe across global fleet
DINODANCE Trojanized Installer (CAMP.26.023)	Espionage / Credential Theft	UNC6740	Technology, Manufacturing — US, UK, CH	Trojanized Tftpd64 GitHub installer drops DINODANCE via Deno runtime; fully in-memory; C2: serialmenot.com
macOS LotL Exfiltration (CAMP.26.025)	Espionage	Unknown	Technology — US, CH	curl/osascript LotL on macOS; AppleScript payload execution; chunked HTTP PUT data exfiltration
DPRK GitHub Code Tampering (CAMP.26.014) ↻ CARRIED OVER (first reported Feb 27)	Sabotage / Financial	DPRK-Nexus Actor	Technology, Education — US	Obfuscated Python backdoors on port 27017 (MongoDB masquerade); unauthorized force-push to GitHub main

Top 3 Actions This Week

1. [CRITICAL] Respond to Iran-Nexus Wiper Threat — Stryker / UNC5203

- Audit Microsoft 365 and Azure AD now — look for new OAuth grants, unfamiliar app registrations, or unauthorized admin activity
- Enforce Conditional Access policies and block all legacy authentication protocols
- Healthcare: confirm manual fallback procedures are in place for Stryker-dependent clinical systems (Lifenet, defibrillators, ambulance cots)
- Verify immutable or offline backups are accessible for all critical systems and test restoration procedures
- Report any mass file deletion, BitLocker key changes, or wipe-like behavior to your IR team immediately

2. [HIGH] Block DINODANCE — Trojanized GitHub Installer (UNC6740)

- Block or alert on deno.exe execution in environments where Deno is not a standard tool

- Enforce application allowlisting for MSI installers — prevent execution of unsigned or unverified packages
- Monitor RunMRU registry keys and scheduled tasks for obfuscated PowerShell one-liners
- Verify integrity of any network utility software downloaded from GitHub (check repo owner, stars, creation date)

3. [HIGH] Detect macOS Living-off-the-Land Exfiltration (CAMP.26.025)

- Ensure macOS endpoints are covered by EDR with LotL behavioral detection (curl, osascript, python abuse)
- Alert on outbound HTTP PUT requests with large chunked transfer encoding from macOS hosts
- Review MDM enrollment — all macOS devices should be managed and monitored
- Audit macOS devices in US and Switzerland environments first — confirmed targeting in those regions

4. [HIGH] Protect Source Code from DPRK GitHub Tampering (CAMP.26.014) — Ongoing

- Enable GitHub branch protection on all main/master branches — require PR reviews and passing status checks
- Block force-pushes to all protected branches
- Require MFA on all GitHub accounts, especially those with write access to production repositories
- Audit recent commit history for unexpected changes from accounts that don't normally commit to main
- Alert on outbound traffic to port 27017 from development machines

Threat Metrics

Activity Trends
▲ Iran-nexus wiper ops: significant escalation
▲ Developer/supply chain attacks: +40% vs. prior
▲ macOS-targeted LotL campaigns: emerging vector
▲ DPRK source code tampering: ongoing escalation
▼ Ransomware incidents: -12% vs. prior week

Cumulative IOC Count: 700+
File hashes: 69+
IP addresses: 6+
Domains: 590+ (driven by GLOBAL.26.002)
URLs: 37+

Resources: Google Threat Intelligence | MITRE ATT&CK (attack.mitre.org) | CISA Alerts (cisa.gov), CNN, Time, Cyberscurity Dive

Report suspicious calls or emails to your IT security team immediately.