Executive Summary

This week's brief covers 3 new threat campaigns sourced from Google Threat Intelligence (GTI), confirmed active through mid-to-late March 2026. The most time-critical entry is the Amatera Infostealer campaign (CAMP.26.032), which uses AI application lures to harvest credentials across Healthcare, Technology, and eight additional sectors — with activity confirmed as recently as March 19, 2026.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
CAMP.26.032 Amatera Infostealer via AI App Lure	Credential Theft / Espionage	AI app lure → MSHTA → Base64 PowerShell (HttpClient) → Amatera infostealer; RunMRU + Scheduled Task persistence	Healthcare, Tech, Mfg, Education — US, UK, CA, FR, KR, TW, CO, HK	HIGH — Block MSHTA remote payloads; alert on Base64 PS via HttpClient; audit Scheduled Tasks & RunMRU
CAMP.26.006 UNC6671 Cloud Extortion (BlackFile)	Financial / Data Theft Extortion	Social engineering bypasses MFA → pivots to M365 SharePoint/OneDrive; PowerShell/Python bulk exfil; BlackFile leak site	Technology, Finance, Manufacturing, Retail — US, CA, AU	HIGH — Audit MFA bypass vectors; alert on bulk SharePoint/OneDrive PS downloads; block 135 known C2 domains
CAMP.26.012 Agenda Ransomware via VPN (QILIN RaaS)	Financial/Ransomware	Compromised GlobalProtect VPN credentials → MeshAgent RMM for persistent C2 → AGENDA/QILIN ransomware	Healthcare, Retail — US, AE	HIGH — Rotate VPN credentials; block unapproved RMM tools (MeshAgent); verify offline backups & test restoration

Top 3 Actions This Week

1. [HIGH] Block Amatera Infostealer — AI App Lure (CAMP.26.032)

Active since early March 2026 and confirmed through March 19, this campaign delivers the Amatera credential stealer via fake AI application lures. MSHTA retrieves secondary components, which execute Base64-encoded PowerShell using System.Net.Http.HttpClient over port 443. Persistence uses Registry RunMRU and Scheduled Tasks. Confirmed in Healthcare, Technology, Manufacturing, Education, Legal, Automotive, Telecom, and Transportation sectors across 8 countries.

- Block MSHTA.exe making outbound connections; alert on Base64 PowerShell using HttpClient (MITRE T1059.001 + T1027.010)
- Audit Scheduled Tasks and Registry RunMRU keys for obfuscated or encoded command entries
- Train staff: be skeptical of browser prompts to install or 'update' AI applications
- Block IOC domains — see table; 4 C2 domains and 11 URLs tracked

2. [HIGH] Stop UNC6671 Cloud Extortion — MFA Bypass + M365 Exfil (CAMP.26.006)

Active since January 2026 through early March, UNC6671 uses social engineering to bypass MFA and access Microsoft 365. PowerShell and Python scripts mass-exfiltrate from SharePoint and OneDrive, followed by extortion threats via the BlackFile data leak site. TTPs overlap with ShinyHunters but use distinct infrastructure. Targets span Technology, Financial Services, Legal, Manufacturing, and Retail in US, Canada, and Australia.

- Implement phishing-resistant MFA (FIDO2/hardware keys) — social engineering MFA bypass is the primary entry vector
- Enable Unified Audit Logging in M365; alert on bulk SharePoint/OneDrive downloads via PowerShell or Python
- Block 135 known C2 domains and 38 IPs from the IOC list
- Establish an extortion response plan — include legal, HR, and communications in your IR playbook

3. [HIGH] Protect Against Agenda Ransomware via Compromised VPN (CAMP.26.012)

A QILIN/Agenda RaaS affiliate uses stolen GlobalProtect VPN credentials to enter environments, installs MeshAgent as a persistent backdoor, then deploys Agenda ransomware. Active since May 2025, last observed mid-February 2026. Healthcare is a primary target alongside Retail, with confirmed incidents in the US and UAE.

- Rotate GlobalProtect VPN credentials; enforce phishing-resistant MFA on all VPN access
- Block or alert on MeshAgent and other unapproved RMM tool execution
- Verify offline/immutable backups exist for all critical systems and test restoration procedures
- Cross-reference VPN logs against 8 known C2 IPs and 1 domain in the IOC list

Indicators of Compromise — Summary

Campaign	File Hashes	IP Addresses	Domains	URLs
Amatera / CAMP.26.032	3 files	—	4 domains	11 URLs
UNC6671 Cloud Extortion / CAMP.26.006	—	38 IPs	135 domains	—
Agenda Ransomware / CAMP.26.012	17 files	8 IPs	1 domain	—
TOTAL	20 files	46 IPs	140 domains	11 URLs

Threat Metrics

Activity Trends
▲ AI-themed social engineering: emerging vector
▲ MFA bypass / cloud exfil: +40% vs. prior
▲ RaaS VPN-entry ransomware: active and ongoing
▼ Wiper / destructive incidents: none this week

Cumulative IOC Count: 230+
File hashes: 20+
IP addresses: 46+
Domains: 140+ (led by UNC6671 C2)
URLs: 11+

Lessons Learned: Microsoft Intune Hardening from Handala / UNC5203 Wiper Exploits

The March 11, 2026 wiper attack by Handala (UNC5203/Cotton Sandstorm) against Stryker Corporation demonstrated the catastrophic potential when an Iran-linked threat actor gains footholds in a Microsoft cloud environment. Critically, the attack wiped devices across a global fleet — a capability only possible when endpoint management infrastructure (such as Microsoft Intune) is not hardened. The following lessons are drawn from post-incident analysis of that campaign.

What Went Wrong — Root Cause Analysis

Handala's wiper leveraged the Microsoft 365/Azure AD environment as its attack surface. Once administrative credentials or OAuth tokens were compromised, the actor was able to issue destructive device commands at scale. Intune, if improperly secured, becomes an adversary's weapon — turning every enrolled device into a potential wipe target.

Intune Hardening Recommendations

A. Restrict Intune Administrative Access

- Enforce Conditional Access on all Intune admin roles — require MFA, compliant devices, and named locations
- Apply Privileged Identity Management (PIM) for Intune Administrator and Global Administrator roles — no standing admin access
- Require phishing-resistant authentication (FIDO2 or Windows Hello for Business) for all accounts with Intune access
- Segregate Intune admin duties — separate accounts for policy authoring, device management, and device wipe actions

B. Limit and Monitor Device Wipe / Retire Capabilities

- Create a custom Intune RBAC role that explicitly removes Wipe and Remote Lock permissions from general IT staff
- Require a secondary approval workflow (Privileged Access Workstation + second admin sign-off) before any bulk wipe action can execute
- Alert immediately on any Remote Wipe or Retire Device action via Microsoft Sentinel or Defender for Cloud Apps
- Review and disable legacy device management protocols (e.g., basic auth MDM profiles) that could be leveraged to issue device commands

C. Monitor for Unauthorized Intune Configuration Changes

- Enable Intune Audit Logs and stream to your SIEM — alert on: new configuration profiles pushed, compliance policy changes, new admin accounts, and bulk device actions
- Alert on OAuth app registrations that request DeviceManagementManagedDevices.ReadWrite.All or similar Intune Graph API permissions
- Regularly review App Registrations and Enterprise Applications in Azure AD for unexpected Intune-scope grants
- Implement Microsoft Defender for Cloud Apps (MDCA) policies to flag anomalous Intune API calls, especially from unfamiliar IPs or at unusual hours

D. Reduce Blast Radius — Segment Device Groups

- Segment device groups by criticality — clinical/medical devices should be in isolated groups not manageable by general IT admin accounts
- Apply the principle of least privilege to all Intune RBAC roles — no admin should have scope over all device groups globally
- Tag clinical, OT, and high-criticality devices separately in Intune and restrict who can issue remote actions on those groups
- For healthcare: ensure Stryker Lifenet, defibrillators, and connected ambulance equipment are on a separate MDM scope with additional access controls

E. Prepare for Wiper Scenarios — Offline Recovery

- Maintain offline or immutable backups of all Intune configuration profiles, compliance policies, and enrollment configs — so you can rebuild your device management environment from scratch if wiped

- Document and test manual fallback procedures for all clinical workflows dependent on Intune-managed devices (e.g., paper-based protocols, manual EKG workflows)
- Establish a breakglass account procedure — a separate, tightly controlled admin account stored offline, usable only when primary admin access is lost
- Run a tabletop exercise simulating total loss of Intune environment: how long to restore enrollment, how to prioritize device re-provisioning, who authorizes manual clinical fallback?

⚠ Handala Threat Context

Handala (UNC5203 / Cotton Sandstorm / Haywire Kitten) is assessed to be linked to Iran's Ministry of Intelligen expansion to US healthcare. With ongoing US-Iran military tensions, continued retaliatory operations against V optional — it is a frontline defense.

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.