ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

GoldFactory / GoldPickaxe — Biometric-Stealing Mobile Banking Trojan Targeting e-KYC & Digital Identity Systems

TLP: CLEAR
Distribution: Public
Advisory on: GoldFactory / GoldPickaxe — Biometric-Stealing Mobile Banking Trojan Targeting e-KYC & Digital Identity Systems
Severity: High
Threat Type: Mobile Banking Trojan / Cybercrime-as-a-Service (Biometric-Enabled Fraud)
Affected Sectors: Mobile Financial Services (MFS), Banking, e-KYC / Digital Identity, Government Service Portals, Certificate Authorities / Registration Authorities
Date: 21 July 2026

Executive Summary

The **Cyber Threat Intelligence (CTI) Unit of BGD e-GOV CIRT** issues this advisory to alert government agencies, financial regulators, Mobile Financial Services (MFS) providers, banks, and digital identity operators about the active resurgence of the **GoldPickaxe** mobile banking Trojan, attributed to the **GoldFactory** cybercrime group.

First disclosed in 2024, GoldPickaxe is the first known iOS malware capable of stealing victims' facial biometric data to bypass facial-recognition-based e-KYC and banking authentication. Recent analysis reveals an advanced Android variant distributed through spoofed KuaiBo video-streaming phishing websites. Researchers identified 19 malware samples targeting users across multiple countries, with one variant configured to target 118 banking applications, demonstrating a strong focus on the financial sector.

The malware's most significant capability is the theft of facial biometrics, identity documents, and authentication data. Victims are tricked into recording facial videos and uploading identity cards, which are exfiltrated to attacker-controlled servers and used to generate AI-powered deepfakes capable of bypassing liveness verification and compromising banking and digital identity services. This evolving threat poses a significant risk to organizations relying on biometric authentication, e-KYC, and digital identity verification.

Relevance to Bangladesh

Open-source threat reporting has identified Bangladesh among the countries targeted by isolated GoldFactory impersonation attempts, indicating an expansion of the threat beyond its traditional regions. Bangladesh's reliance on mobile-based e-KYC, biometric National ID (NID) verification, Mobile Financial Services (MFS), OTP-based authentication, and digital citizen services makes the malware's biometric theft and e-KYC bypass capabilities particularly relevant. Accordingly, the threat to Bangladesh is assessed as HIGH. It should be noted that the July 2026 campaign primarily targets Android devices, while the iOS component relates to previously reported activity from 2024.

Threat Actor Profile — GoldFactory

Attribution & History

GoldFactory is a technically advanced cybercrime cluster — first discovered, named, and tracked by independent threat research — assessed to be a Chinese-speaking organised collective of cybercriminals with distinct development and operator groups dedicated to specific regions. It is distinct from nation-state APTs: its motive is financial fraud, executed through distribution of interconnected mobile malware families. Its preferred technologies include Aliyun Cloud, the Virbox Protector, and the ThinkPHP framework.

Milestone	Period	Significance
Cluster active since	Mid-2023	GoldFactory trojans in circulation
GoldDiggerPlus detected	September 2023	Extended GoldDigger variant with embedded second APK
GoldDigger reported	October 2023	Unknown Android trojan reported targeting 50+ Vietnamese financial institutions
GoldPickaxe earliest traces	Early October 2023	First biometric-harvesting variant observed
GoldFactory publicly disclosed	February 2024	First iOS trojan observed stealing facial-recognition data
Indonesia Coretax campaign	July 2025 – January 2026	16+ government and financial brands abused in a single operation, timed to national tax season
GoldPickaxe variant resurgence	July 2026	New evasive Android variant reported; 19 samples, impacted devices across 5 countries

Malware Family Ecosystem

The following families are attributed to GoldFactory by primary open-source research:

Family	Platform	Notable Capability
GoldDigger	Android	First known variant; targets 50+ Vietnamese apps; impersonates a Vietnamese government portal and a local electricity company; evades 40+ mobile antivirus products

GoldDiggerPlus	Android	Extended variant with embedded second APK (`b.apk`); works in tandem with GoldKefu; uses webfakes and targeted scam calls
GoldKefu	Android (embedded in GoldDiggerPlus)	Named for the Chinese word for "customer service" (客服); impersonates a Vietnamese messaging app; real-time voice/video calls, customer-service impersonation, fake bank alerts; integrates Agora SDK
GoldPickaxe	Android & iOS	Harvests facial-recognition data, identity documents, and SMS; proxies traffic through infected devices; uses AI-driven face-swapping to create deepfakes; exfiltrates to Alibaba cloud storage

Figure: GoldFactory Malware Family Ecosystem & Timeline

Adjacent / later campaign variants (reported in subsequent regional research)

Gigaflower: reported in later APAC campaign research as a newer variant shifting toward remote device control; regional analysis describes live screen streaming via WebRTC, reading of the Vietnamese national ID (CCCD), and QR-code extraction.

Coretax campaign/sample: Indonesian tax-season fraud-enablement tool with live operator support; linked in public reporting to the broader Indonesian GoldFactory ecosystem, though campaign-ecosystem names should not be treated as interchangeable malware-family names

***Android vs iOS note**: The July 2026 variant discussed in this advisory is Android-focused. The iOS dimension is historical: GoldPickaxe.iOS (2024) was distributed initially through Apple TestFlight and later via abused MDM profiles, communicates over websocket on port 8383, and starts a SOCKS5 proxy at 127.0.0.1:1081; it is more limited than its Android counterpart due to iOS platform restrictions.*

Operational Metrics

Threat-intelligence tracking quantifies GoldFactory's footprint

- ~15 infections per day across active campaigns
- 16+ trusted government and financial brands abused in a single campaign (Coretax)
- US$1,700 average financial loss per successful case
- US$3M+ minimum estimated annual regional losses (single region)

Campaign Overview — The July 2026 GoldPickaxe Variant

Distribution Vector

The current variant is distributed via a malicious domain spoofing KuaiBo, a prominent Chinese video-streaming and media-player application. Fake websites promise free access to KuaiBo and trick users into manually sideloading the malicious dropper APK. This pattern — distribution via phishing sites that impersonate legitimate consumer, government, or financial brands and induce APK sideloading — is the consistent GoldFactory hallmark. The Indonesian Coretax campaign abused more than 16 trusted government and financial-sector brands, timed precisely to Indonesia's national tax season to maximize victim volume.

Historically, GoldPickaxe.Android was disguised as over 20 different applications from Thailand's government, financial, and utility sectors.

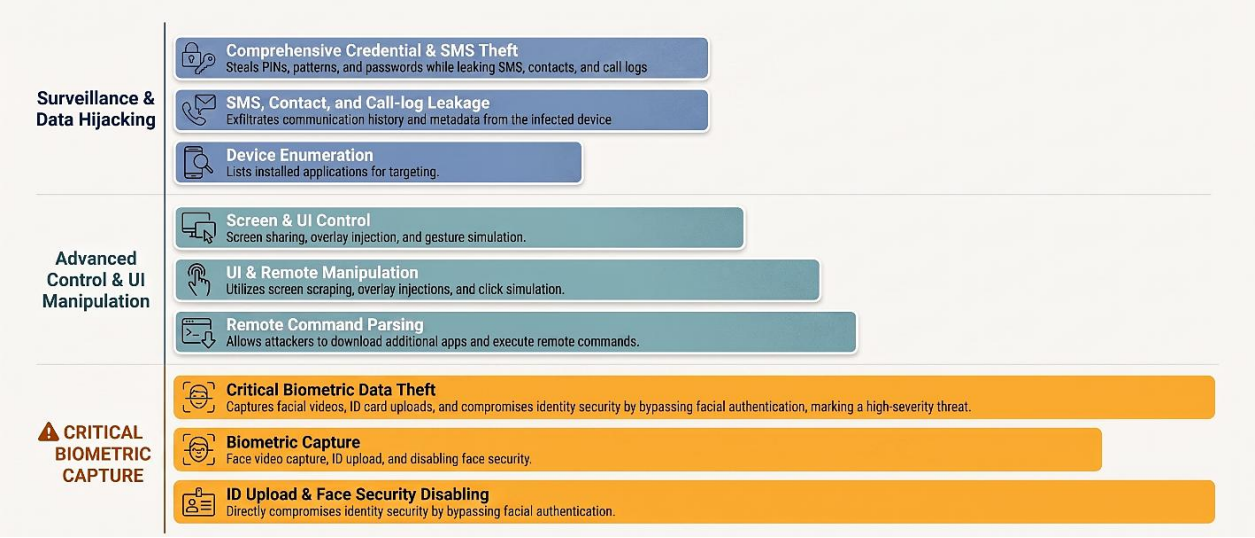

Figure: GoldPickaxe Capability Matrix

Targeting

- Primary focus: Southeast Asian market — mobile banking, e-wallets, and financial applications.
- Telemetry-observed impacted devices (5 countries): Indonesia, Malaysia, United States, Singapore, Saudi Arabia. Primary 2024 reporting confirms Vietnam and Thailand as the established target countries
- One Indonesia-focused sample contains a target list of 118 distinct banking applications.
- Open-source reporting additionally lists **Bangladesh** among outlier impersonation targets, signaling the group's awareness of South Asian MFS markets

Why Signature-Based Detection Fails

Independent analysis states that conventional signature-based detection is insufficient for this variant. The reasons are structural:

- The dropper is deliberately stripped of heavy malicious functionality to bypass static analysis
- Malicious logic is encrypted inside a packed binary and decrypted only at runtime
- The AndroidManifest is deliberately malformed to crash static-analysis tools (JADX, Apktool)
- C2 traffic is encrypted via a native library with per-request IVs derived from timestamps
- GoldDigger alone evades more than 40 mobile antivirus applications.

Technical Analysis

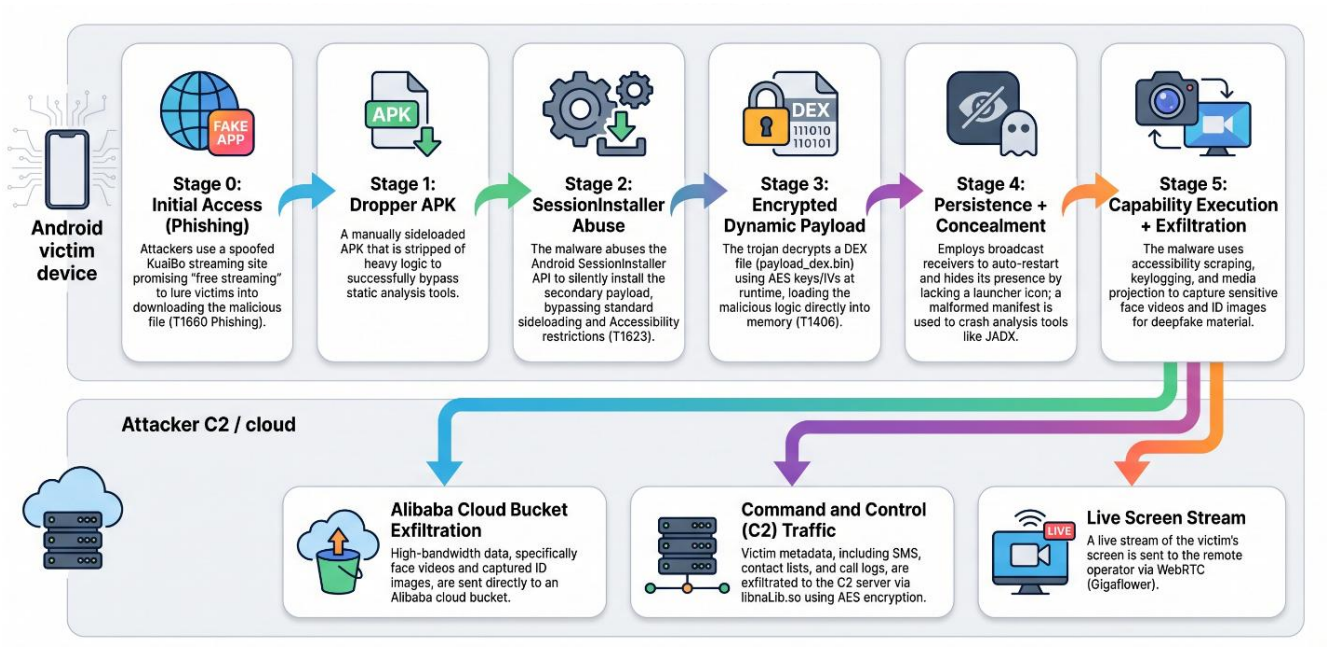

Figure: GoldPickaxe End-to-End Attack Chain

Attack Chain (Phase-by-Phase)

Phase	Activity	Technique
1. Initial ingress	User manually installs a "Dropper APK" disguised as KuaiBo	Phishing / social engineering (T1660)
2. Secondary deployment	Dropper uses the legitimate Android **SessionInstaller API** to silently install the payload, bypassing sideloading and Accessibility restrictions in recent Android versions	Command & scripting interpreter abuse (T1623, reported)
3. Evasion & dynamic loading	Payload decrypts an embedded `payload_dex.bin` using AES; IV and key are read from `dex_IV.bin` and `dex_key.bin`, then dynamically loaded into memory	Obfuscated Files or Information (T1406)
4. Persistence	Event-triggered broadcast receivers auto-initialise/restart the malware; no launcher icon is registered	Event-triggered execution (T1624.001); suppress app icon (T1628.001)
5. Capability execution	Accessibility-based screen scraping, Media Projection screen sharing, camera hijack, keylogging, overlay injection, gesture simulation	Multiple Collection / Credential Access / Impact techniques
6. C2 & exfiltration	All C2 traffic encrypted via native `libnaLib.so` (AES with timestamp-derived IVs); remote commands fetch secondary APKs	Encrypted channel (T1521.001); ingress tool transfer (T1544)

Persistence & Concealment

- Broadcast receivers registered against system events ensure the malware re-initialises or restarts without user interaction.
- The payload omits both `android.intent.action.MAIN` and `android.intent.category.LAUNCHER` intent filters, so no app icon appears on the home screen; manual removal requires navigating to Settings > Apps
- This also means sandbox environments may be unable to auto-launch the payload, hindering automated analysis.

Anti-Analysis & Defense Evasion

Technique	Mechanism
Packing	Both dropper and payload embed core logic inside an encrypted packed file using identical execution mechanics and the same filename (`payload_dex.bin`) — indicative of a shared packer
Manifest tampering	Deliberately malformed XML triggers parsing failures in JADX and Apktool, hiding requested permissions and background services

Runtime crypto extraction	IVs and AES keys were only recoverable via **dynamic binary instrumentation (DBI)** hooking of native routines
Native comms encryption	`libnaLib.so` encrypts all C2 traffic; IVs generated per-request from the request timestamp

C2 & Remote Command Handling

The malware parses remote commands containing a URL from the C2 server and can fetch and install secondary APK payloads, allowing dynamic deployment of additional functionality and resilience against C2 disruption. Historically, GoldPickaxe.Android communicates over websocket on port 8282 and starts a SOCKS5 proxy at 127.0.0.1:1081; data is exfiltrated via HTTP API plus Alibaba cloud storage.

Capability Matrix

Capability	Present	Command / Mechanism
Leak SMSs	✓	SMS interception (T1636.004)
Leak installed apps	✓	App enumeration (name, packageName, icon)
Leak Contacts	✓	(T1636.002)
Leak CallLog	✓	(T1636.003)
Camera surveillance	✓	Camera hijack
Simulate user gestures	✓	Accessibility-based gesture injection
Download other apps	✓	Remote APK fetch
Keylogging	✓	Active input capture
Screen Capture	✓	`enhance_display_true` — Accessibility scrape, JSON exfil
Screen Overlay	✓	Fake lock screens, fake system updates, fake ministry app
Steal PIN/pattern/password	✓	`four_password` fake lock-screen verification
Perform clicks	✓	Accessibility click injection
Leak device information	✓	Device profiling
Steal biometric data	✓	`face_video_judu`, `face_video_accept`, camera hijack
Steal ID	✓	`upload_idcard` via `IdentityVerifyPhotoActivity`

Biometric & Identity Theft — The Core Threat

This is the capability that elevates GoldPickaxe above ordinary banking trojans and makes it directly relevant to national digital-identity infrastructure:

- **Face-video capture** — The malware initiates an activity prompting the user to record a video of their face. The command face_video_judu makes the user believe facial recognition failed, re-prompting capture loops; face_video_accept simulates a successful verification. Documented capture instructions include "please hold the camera steady", "please blink", and Android prompts for blink, smile, head turns, nod, and open mouth — used to build a comprehensive facial biometric profile.
- **Disabling native biometrics** — disable_face_true disables facial recognition on the device, forcing a fallback to PIN/pattern authentication, which the malware then harvests via four_password.
- **Identity-card capture** — upload_idcard prompts the user to photograph their national ID, exfiltrating the image to the C2 server and cloud bucket.
- **Deepfake synthesis & liveness bypass** — Captured face videos and ID images are processed with AI-driven face-swapping services to create deepfakes, which are injected into banking/e-KYC liveness checks. Thai police confirmed that criminals install banking applications on their own Android devices and use captured face scans to bypass facial-recognition checks.

The standard injection toolkit involves virtual-camera software (VCAM, VCAMSX) to replace the camera feed, plus hooking frameworks (Frida, LSPosed, Objection) to tamper with session logic. Because liveness detection inspects the frame it receives — not how that frame arrived — an injected synthetic stream passes the check even with a high-quality liveness model. Regional cases confirm the pattern: in Indonesia, virtual-camera tooling was used to inject deepfakes into bank KYC flows; in Thailand, stolen photos were used to beat facial-biometric checks.

In the wider GoldFactory ecosystem, hooking frameworks including Frida Gadget, DobbyHook, and PineHook are used to interfere with system APIs, bypass anti-fraud mechanisms, and spoof application signatures.

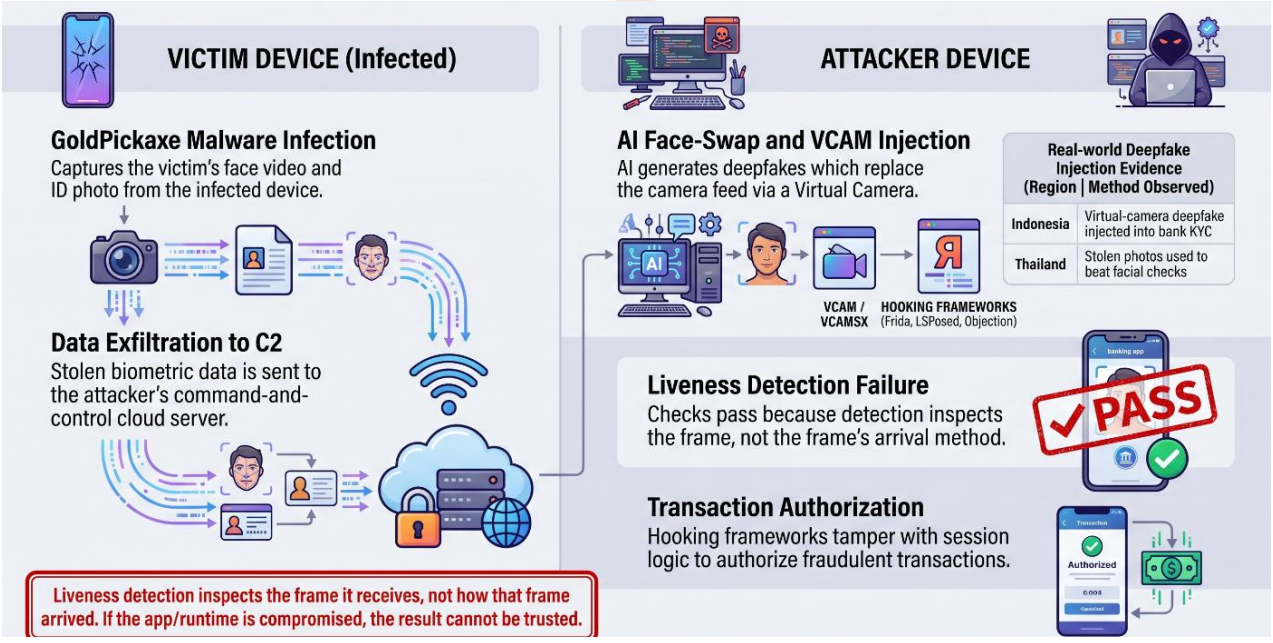

Figure: Biometric Deepfake Injection & Liveness Bypass

Screen Scraping & Live Screen Sharing

- Screen scraping (`enhance_display_true`) — abuses Android Accessibility Services to capture on-screen elements and transmit them to C2 in JSON
- Screen sharing (`screen_share_true`) — abuses the Media Projection API to provide unrestricted live visibility of the victim's UI

In the related Gigaflower variant, this evolves to live screen streaming via WebRTC, giving a remote operator real-time interactive control of the banking session.

Fake Overlays & Social Engineering

The malware deploys deceptive overlays: solid black screens, fake system-update interfaces, and fake biometric (fingerprint) prompts. A fake Indonesian ministry application harvests permissions; interaction triggers the `com.go.Permissions` activity-alias pointing to `com.sup.hop.ui.activity.PermissionsActivity`. A configurable injection_app command renders a spoofed AppDialog populated with a target app's real high-resolution icon (extracted as a Bitmap), redirecting the browser to a C2-specified malicious site after the victim clicks OK.

MITRE ATT&CK Mapping

Tactic	Technique ID	Name	GoldPickaxe Usage
Initial Access	T1660	Phishing	Spoofed KuaiBo sites deliver the Dropper APK
Execution	T1623 (reported)	Command and Scripting Interpreter	Abuses Android SessionInstaller API to install payload silently
Persistence	T1624.001	Event Triggered Execution: Broadcast Receivers	System-event receivers auto-initialise/restart the malware
Persistence	T1628.001	Hide Artifacts: Suppress Application Icon	Omits MAIN/LAUNCHER intent filters; no home-screen icon
Defense Evasion	T1406	Obfuscated Files or Information	Encrypted `payload_dex.bin` loaded at runtime via AES
Defense Evasion	T1629	Impair Defenses	Malformed manifest crashes JADX/Apktool; `disable_face_true` disables native facial recognition
Defense Evasion	T1655	Masquerading	activity-alias redirects and fake ministry/AppDialog overlays
Credential Access	T1417.002	Input Capture: GUI Input Capture	`four_password` fake lock screen + keylogging

Discovery	T1418	Software Discovery	Enumerates app name/packageName/icon; matches 118-app target list
Discovery	T1426	System Information Discovery	Device profiling
Collection	T1636.004	Protected User Data: SMS Messages	SMS interception
Collection	T1636.002	Protected User Data: Contacts List	Contacts exfiltration
Collection	T1636.003	Protected User Data: Call Logs	Call-log harvesting
Collection	T1453	Abuse Accessibility Features	`enhance_display_true` screen scraping
Collection	T1513	Screen Capture	`screen_share_true` via Media Projection
Collection	T1512	Video Capture	Camera hijack for face-video recording
Command and Control	T1521.001	Encrypted Channel	`libnaLib.so` AES with timestamp-derived IVs
Command and Control	T1544	Ingress Tool Transfer	Remote commands fetch secondary APKs
Exfiltration	T1646	Exfiltration Over C2 Channel	Sensitive data transmitted to GoldFactory infrastructure
Impact	T1516	Input Injection	Overlays mimic banking login; inject pattern locks and payloads

Indicators of Compromise (IoC)

Filenames / embedded artefacts

- `payload_dex.bin` (encrypted DEX payload, shared by dropper and payload)
- `dex_IV.bin` (AES initialisation vector)
- `dex_key.bin` (AES key)
- `libnaLib.so` (native C2-encryption library)

Android components / activity-aliases

- `com.go.control.IdentityVerifyPhotoActivity` (legacy alias) → `com.sup.hop.ui.activity.IdentityVerifyPhotoActivity`
- `com.go.Permissions` (alias) → `com.sup.hop.ui.activity.PermissionsActivity`

C2 command strings (high-fidelity behavioral IOCs)

`four_password, disable_face_true, enhance_display_true, screen_share_true, upload_idcard, face_video_judu, face_video_accept, injection_app.`

Distribution lure

Phishing domains spoofing **KuaiBo** (Chinese video-streaming app)

Sample hashes (SHA256)

Sample	SHA256
GoldPickaxe.iOS	`4571f8c8560a8a66a90763d7236f55273750cf8dd8f4fdf443b5a07d7a93a3df`
GoldPickaxe.Android	`b72d9a6bd2c350f47c06dfa443ff7baa59eed090ead34bd553c0298ad6631875`
GoldDigger	`d8834a21bc70fbe202cb7c865d97301540d4c27741380e877551e35be1b7276b`
GoldDiggerPlus	`b5dd9b71d2a359450d590bcd924ff3e52eb51916635f7731331ab7218b69f3b9`

Domains

`ms2ve[.]cc, hds6y[.]cc, smgeo[.]cc, www[.]dg1e[.]com, zu7kt[.]cc, ks8cb[.]cc, wbke[.]cc, t8bc[.]xyz, bv8k[.]xyz, hzc5[.]xyz, wsy6[.]xyz, r6go[.]xyz, msc4[.]xyz, wts3[.]xyz, qskm[.]xyz, tp7s[.]xyz, vki9[.]xyz, bgt6[.]xyz, gt6ss[.]xyz`

RTMP streaming endpoint

rtmp://18.142.163[.]73:1935/live/

Ports

GoldPickaxe.Android websocket	8282
GoldPickaxe.iOS websocket	8383
SOCKS5 proxy	127.0.0.1:1081

Detection Hunt Strings

Type	Hunt Query
Network (DNS/proxy)	Lookups/connections to KuaiBo-spoofing domains; traffic to hosts serving `payload_dex.bin` or APK downloads from non-Play-Store referrers; websocket traffic on ports 8282/8383 to non-corporate hosts; RTMP to `18.142.163.73`
Endpoint (Android MDM/EDR)	Apps with no launcher icon requesting Accessibility + Media Projection + camera + SMS + contacts; presence of `libnaLib.so`, `payload_dex.bin`, `dex_IV.bin`, `dex_key.bin`; SOCKS5 listener on 1081

App-store / package review	Package names containing `com.go.control, com.sup.hop`; activity-aliases redirecting `IdentityVerifyPhotoActivity / PermissionsActivity`
Behavioural	Device with Accessibility granted to a non-launcher app making AES-encrypted outbound traffic; rapid permission escalation to camera + screen capture after sideload

Impact Assessment for Bangladesh

Open-source reporting indicates that Bangladesh has been included among the countries targeted by isolated GoldFactory impersonation attempts, suggesting growing threat actor interest in the South Asian financial ecosystem. Although there is no evidence of compromise of any specific Bangladeshi system, the country's reliance on mobile financial services (MFS), biometric/NID verification, OTP-based authentication, and digital citizen services makes these attack techniques relevant. The following assessment provides a risk mapping to support defensive prioritization and preparedness.

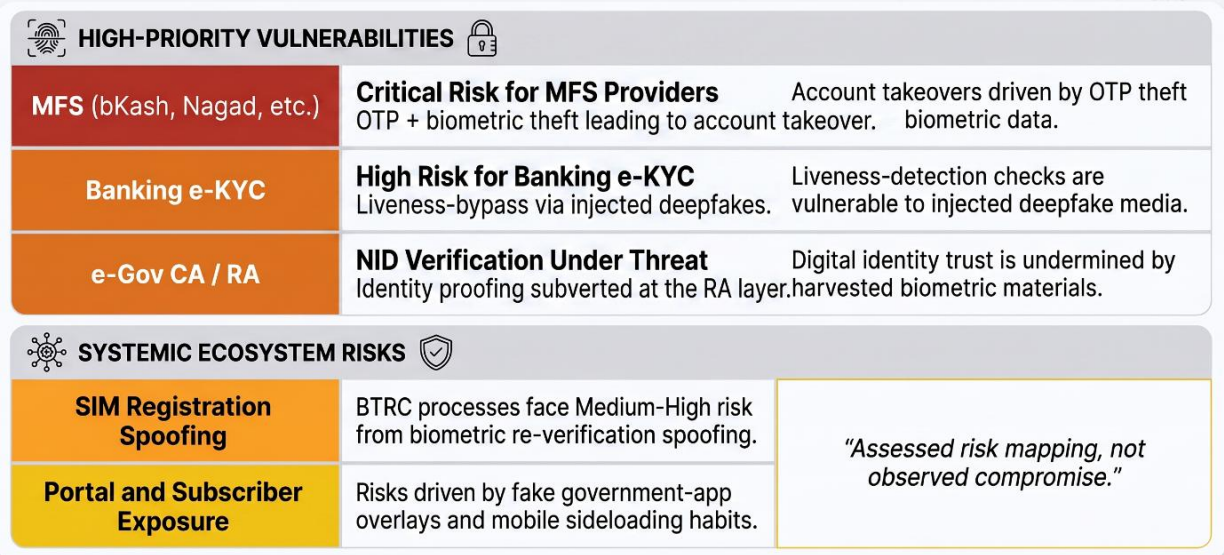

Figure: Bangladesh Sector Risk

Assessed Exposure of National Services

National Service Category	Assessed Exposure	Rationale
Mobile Financial Services (e.g., bKash, Nagad, Rocket)	CRITICAL	MFS account opening and reset flows that rely on mobile face/NID verification and OTP are the primary target profile; OTP interception + biometric theft enables account takeover

Banking e-KYC	HIGH	Banks performing remote video-KYC inherit the liveness-bypass weakness documented for Indonesia and Thailand
Biometric NID / digital-identity verification	HIGH	Services that trust NID-bound biometric verification could be targeted with harvested biometric material to impersonate legitimate citizens
e-Gov certificate authority / RA enrollment	HIGH	Remote identity-proofing at the Registration Authority layer could be subverted (see 6.2)
SIM / biometric registration	MEDIUM–HIGH	Biometric SIM registration and re-verification could be spoofed with harvested material
Government citizen-service portals	MEDIUM	Secondary targeting via fake government-app overlays (as seen with the fake Indonesian ministry app)

The PKI / Certificate-Authority Angle

GoldPickaxe does not directly target Bangladesh's e-Gov PKI cryptography; instead, it threatens the identity verification process. The primary risk lies at the Registration Authority (RA) layer, where certificate issuance depends on identity proofing. If remote enrollment relies on facial verification, NID validation, and OTP authentication, a compromised device could enable attackers to submit deepfake biometrics, stolen identity documents, and intercepted OTPs to obtain a fraudulent but cryptographically valid digital certificate. Therefore, organizations should prioritize strengthening identity assurance and enrollment verification controls rather than relying solely on cryptographic security.

Assessed Risk Matrix

Sector	Risk Level	Rationale
MFS providers	**CRITICAL**	Primary financial target profile; OTP + biometric theft enables full account takeover
Banks (mobile banking, e-KYC)	**HIGH**	Remote video-KYC exposed to deepfake liveness bypass
NID / digital-identity operators	**HIGH**	Services trusting NID-bound biometrics exposed to harvested-material impersonation
e-Gov certificate authority / RA	**HIGH**	Remote identity proofing could be subverted at enrollment
BTRC / SIM registration	**MEDIUM–HIGH**	Biometric re-verification spoofing

Government citizen-service portals	**MEDIUM**	Secondary targeting via fake government-app overlays
General mobile subscribers	**MEDIUM**	Sideloading culture and MFS reliance broaden victim pool

Defensive Recommendations

- **Block malicious infrastructure:** Block all identified phishing domains, malicious APK distribution sites, and GoldPickaxe IOCs (domains, IPs, hashes, package names, filenames, and command strings) across DNS, firewalls, web gateways, email gateways, EDR, MDM, and other security controls.
- **Enhance threat detection**: Deploy GoldPickaxe IOCs and behavioral indicators within SIEM, EDR, MDM, and Mobile Threat Defense (MTD) platforms, and continuously monitor for suspicious command execution and malware artifacts.
- **Identify compromised devices**: Scan managed mobile devices for sideloaded applications, hidden apps, and applications requesting excessive permissions such as Accessibility, Media Projection, Camera, SMS, and Contacts. Investigate and isolate suspected compromised devices.
- **Strengthen mobile security**: Enforce Mobile Device Management (MDM) policies by disabling APK sideloading, restricting Accessibility permissions, enabling Google Play Protect, and requiring device integrity verification (e.g., Play Integrity) for sensitive applications.
- **Harden e-KYC and biometric verification**: Implement advanced liveness detection, biometric injection detection, device attestation, behavioral analytics, and multi-factor identity verification to mitigate deepfake and virtual camera attacks. Do not rely solely on selfie- and ID-based verification.
- **Strengthen identity assurance**: Enhance Registration Authority (RA) enrollment and recovery procedures by requiring supervised or in-person identity proofing for high-assurance digital certificates and implementing additional fraud checks for remote enrollment.
- **Protect financial and government services**: Coordinate IOC sharing with Bangladesh Bank, Mobile Financial Service (MFS) providers, banks, and relevant stakeholders to improve fraud detection, transaction monitoring, and rapid response to emerging threats.
- **Deploy advanced application protection**: Integrate Runtime Application Self-Protection (RASP), anti-tampering, anti-hooking, overlay detection, and screen-sharing protection into government, banking, and MFS mobile applications.
- **Improve identity recovery and awareness**: Establish rapid credential and certificate revocation procedures for suspected biometric compromise, and conduct continuous public awareness campaigns on the risks of sideloaded applications, biometric theft, and verification of legitimate government and financial applications.

Detection Guidance

Network Detection

- Alert on DNS resolution or HTTPS connections to KuaiBo-impersonating domains and APK-hosting infrastructure referenced in the originating IOC repository.
- Alert on websocket traffic to non-corporate hosts on ports 8282 (Android) / 8383 (iOS); RTMP to 18.142.163[.]73.
- Detect AES-encrypted outbound traffic originating from Android processes with no launcher icon.
- Flag APK downloads from non-Play-Store referrers, especially following "free streaming" search results or messaging-app links.

Mobile Endpoint Detection

Behavioural Indicators (hunt):

- App with no launcher icon (no MAIN/LAUNCHER intent) requesting Accessibility Service
- App requesting the combination: Accessibility + Media Projection + Camera + SMS + Contacts + CallLog
- Presence of: payload_dex.bin, dex_IV.bin, dex_key.bin, libnaLib.so
- Activity-alias: com.go.control.* -> com.sup.hop.ui.activity.*
- Native library libnaLib.so generating per-request AES IVs from timestamps
- Manifest that fails to parse cleanly in JADX/Apktool
- SOCKS5 listener on 127.0.0.1:1081

Anti-Fraud / e-KYC Layer Detection

- Flag sessions where liveness check passes but device integrity attestation fails (root/emulator/virtual camera detected)
- Alert on rapid sequence: new device enrollment + biometric reset + OTP interception + credential change
- Alert on identical face-video/ID-image artefacts appearing across multiple accounts (synthetic-identity farming)
- Detect Frida/LSPosed/Objection and Frida Gadget / DobbyHook / PineHook hooking artefacts in app runtime.

References

- "GoldPickaxe Returns: When Your Biometric Information Is as Important as Your Money" (9 July 2026): https://zimperium.com/blog/goldpickaxe-returns-when-your-biometric-information-is-as-important-as-your-money
- "We identified iOS trojan stealing facial recognition data" (GoldFactory / GoldPickaxe primary research): https://www.group-ib.com/blog/goldfactory-ios-trojan/
- Top 10 Cyber Threat Actors (June 2026): https://www.group-ib.com/media-center/press-releases/top-10-cyber-threat-actors/
- GoldFactory author / campaign research (Ha Thi Thu Nguyen): https://www.group-ib.com/author/ha-thi-thu-nguyen/
- Mobile Deepfake Attack Playbook for Banks in Asia (2026): https://promon.io/resources/downloads/mobile-deepfake-attack-playbook-banks-asia
- App Threat Report Q2 2026: Coretax Android Banking Malware (7 July 2026): https://promon.io/security-news/app-threat-report-q2-2026-coretax-android-banking-malware
- GoldFactory threat bulletin, December 2025 (Vietnamese): https://cybersafe.vnu.edu.vn/news/thong-tin-cac-moi-de-doa-bao-mat-thang-122025
- Detect GoldPickaxe in iOS Mobile Apps: https://www.appdome.com/how-to/account-takeover-prevention/android-and-ios-trojans/detect-goldpickaxe-in-ios-mobile-apps/