INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-08 19:04 UTC

CallPhantom and GoldFactory: Play Store Fraud Campaigns Signal Escalating Mobile Subscription and RAT Threats in Asia-Pacific

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0293
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Android (Google Play Store), Google Pay, PhonePe, Paytm, WhatsApp, Indonesia CoreTax Platform
Published	2026-05-08T11:08:00
Discovery Source	Rss

Executive Summary

Two concurrent mobile fraud campaigns across Asia-Pacific have affected millions of users. The CallPhantom cluster placed 28 fraudulent apps on Google Play that accumulated 7.3 million downloads, charging subscription fees for fabricated data while collecting user information under false pretenses. GoldFactory, a threat actor associated with banking trojan and RAT deployment, has caused an estimated $2 million in losses from Indonesian users by impersonating the government's CoreTax tax platform and abusing 16 trusted brands to distribute malicious applications. Note: All cited sources are Tier 3 (vendor blogs, news outlets); claims should be corroborated against primary threat intelligence feeds before high-confidence decisions.

Technical Analysis

Two distinct mobile threat clusters are active across Asia-Pacific, both targeting Android users through a combination of official app store distribution and social engineering.

CallPhantom (Play Store Subscription Fraud):

- 28 fraudulent Android apps distributed via Google Play, accumulating 7.3 million downloads before removal
- Apps falsely advertised access to third-party call history, SMS records, and WhatsApp message logs
- No actual surveillance capability was present; output was randomly generated fabricated data

- Monetization relied entirely on deceptive subscription billing

- CWE-20 (Improper Input Validation), CWE-359 (Exposure of Private Information to Unauthorized Actor), CWE-451 (User Interface Misrepresentation of Critical Information)

- MITRE ATT&CK mobile techniques: T1660 (Phishing, Spearphishing via App Stores), T1661 (Masquerading), T1516 (Input Injection)

GoldFactory (Banking Trojan / RAT Campaign, Indonesia):

- Estimated $2 million in financial losses from Indonesian users

- Impersonated Indonesia's CoreTax tax platform to lend legitimacy to malicious app distribution

- Abused 16 trusted brand identities across social engineering and app delivery chains

- Associated with banking trojan and RAT deployments against Southeast Asian financial platforms, including Google Pay, PhonePe, and Paytm

- CWE-1021 (Improper Restriction of Rendered UI Layers, overlay abuse), CWE-20, CWE-359

- MITRE ATT&CK mobile techniques: T1417 (Input Capture, Keylogging), T1406 (Obfuscated Files or Information), T1437 (Standard Application Layer Protocol), T1444 (Masquerade as Legitimate Application), T1476 (Deliver Malicious App via Other Means), T1582 (SMS Control), T1627 (Execution Guardrails), T1636 (Protected User Data Access)

No CVE identifiers are present in this item. No vendor-issued patch is applicable to the subscription fraud campaign; the threat vector is app store policy and user deception. The GoldFactory RAT campaign requires device-level detection and remediation.

Action Checklist

1. Containment: If your organization operates a mobile device management (MDM) or enterprise mobility management (EMM) platform, query enrolled Android devices for applications matching the 28 CallPhantom app package names (package identifiers not confirmed in available Tier 3 sources; cross-reference Google Play enforcement notices, VirusTotal, and threat intelligence feeds for updated IOC sets). Block sideloading of unverified APKs via MDM policy. For GoldFactory, block known malicious domains and C2 infrastructure associated with the GoldFactory cluster through DNS filtering and proxy controls.
2. Detection: Review mobile application inventory logs from MDM platforms for applications with anomalous subscription billing behavior or apps requesting SMS, call log, or WhatsApp content access permissions without a clear business justification. For GoldFactory RAT indicators, monitor for anomalous outbound traffic patterns from Android endpoints to Southeast Asian infrastructure, overlay activity (T1021/T1417), and unexpected SMS control events (T1582). Consult threat intelligence platforms (e.g., MISP, VirusTotal, Recorded Future) for GoldFactory IOC sets.
3. Eradication: Remove any identified CallPhantom-affiliated applications from enrolled devices immediately. For GoldFactory-compromised devices, perform a full device wipe; banking trojans with RAT capabilities cannot be reliably remediated through app removal alone. Revoke any sessions or credentials (banking apps, UPI platforms including Google Pay, PhonePe, Paytm) that may have been exposed on compromised devices.
4. Recovery: After device remediation, require re-enrollment through MDM before restoring access to corporate resources. For users whose financial application credentials were potentially exposed,

coordinate with affected financial institutions (Google Pay, PhonePe, Paytm) to freeze accounts and re-issue credentials. Validate that no unauthorized transactions occurred during the exposure window. Monitor re-enrolled devices for 30 days for behavioral anomalies.

5. Post-Incident: This campaign exposes a gap in mobile application vetting for organizations that permit personal or corporate Android devices to access financial platforms. Review and update your mobile security policy to enforce app allowlisting, prohibit subscription apps with broad data access permissions, and require Play Protect attestation. Map identified control gaps to CIS Benchmark for Mobile Devices and NIST SP 800-124 (Guidelines for Managing the Security of Mobile Devices in the Enterprise). If users in your organization were affected by GoldFactory, this constitutes a social engineering failure; update security awareness training to address brand impersonation of government tax platforms.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if any GoldFactory-compromised device was used to access corporate financial systems, if confirmed unauthorized transactions exceed organizational fraud thresholds, if affected users are in jurisdictions with mandatory breach notification requirements for financial PII (e.g., PDPA in Thailand/Singapore, India DPDP Act), or if the GoldFactory CoreTax impersonator APK was distributed internally via corporate communication channels such as a company WhatsApp group.
Recovery Notes	Post-wipe device re-enrollment must be gated on MDM compliance policy confirmation that Google Play Protect attestation is active and no accessibility services are enabled beyond known enterprise applications, as GoldFactory RATs abuse Android Accessibility Services for persistence and overlay attacks. For users whose UPI-linked accounts (Google Pay, PhonePe, Paytm) were exposed, monitor linked bank account statements for a minimum of 90 days given that GoldFactory has demonstrated delayed fraudulent transaction patterns in prior Indonesian campaign reporting. Revalidate mobile security policy enforcement quarterly against the CIS Benchmark for Mobile Devices and NIST SP 800-124 Rev. 2 to prevent recurrence from the next wave of GoldFactory or CallPhantom infrastructure.

Forensic Artifacts	Android MDM application inventory export: package names, install sources (com.android.vending vs sideloaded), install timestamps, and declared permissions for all enrolled devices — primary artifact for identifying CallPhantom apps by their SMS/call log/WhatsApp permission profiles and GoldFactory APKs by sideload origin | ADB output of active Accessibility Services ('adb shell settings get secure enabled_accessibility_services') — GoldFactory banking trojans register as Accessibility Services to perform overlay attacks (MITRE T1417) and intercept OTP SMS (MITRE T1582); presence of an unrecognized accessibility service on a device with a financial app installed is a high-confidence GoldFactory compromise indicator | DNS resolver query logs filtered for Android device source IPs — GoldFactory C2 communication and CallPhantom subscription billing infrastructure will appear as recurring DNS queries to domains not matching known enterprise or Play Store infrastructure; Southeast Asian TLD patterns (.id, .xyz, .top) with high query frequency are particularly indicative | Google Play billing and subscription records from affected user Google accounts — accessible via Google Takeout (myaccount.google.com/data-and-privacy) — documents CallPhantom subscription charges for fabricated data services tied to specific app package names and charge dates, establishing financial harm timeline for each victim | Android logcat output captured via ADB ('adb logcat -d -v time') filtered for SMS, CALL_LOG, and WhatsApp content provider access events — surfaces GoldFactory RAT interception of banking OTPs and WhatsApp messages in the system log, with timestamps correlating to unauthorized transaction windows

Per-Action IR Details

Containment — If your organization operates a mobile device management (MDM) or enterprise mobility management (EMM) platform, query enrolled Android devices for applications matching the 28 CallPhantom app package names (specific package identifiers not confirmed in available sources — cross-reference threat intelligence feeds and Google Play enforcement notices). Block sideloading of unverified APKs via MDM policy. For GoldFactory, block known malicious domains and C2 infrastructure associated with the GoldFactory cluster through DNS filtering and proxy controls.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without MDM: use Android Debug Bridge (ADB) to enumerate installed packages across enrolled devices with 'adb shell pm list packages -f' and grep output against threat intel package name lists sourced from MISP or VirusTotal GoldFactory/CallPhantom tag searches. Block GoldFactory C2 domains at the DNS layer using Pi-hole with a blocklist derived from open-source GoldFactory IOC reports (search Malpedia actor 'GoldFactory' for domain indicators). For APK sideloading prevention without MDM, enforce Google Play Protect via policy reminder and audit 'Settings > Apps > Special App Access > Install Unknown Apps' manually on high-risk devices.

Evidence: Before blocking C2 or removing apps, capture: (1) DNS query logs from corporate resolver or Pi-hole showing any resolved GoldFactory-associated domains originating from Android device IPs; (2) proxy/firewall egress logs showing outbound connections from enrolled Android device IPs to Southeast Asian ASNs during the suspected exposure window; (3) MDM inventory snapshot listing all installed APKs on enrolled devices, including package name, version, install source (Play Store vs sideloaded), and install timestamp — sideloaded GoldFactory CoreTax impersonator APKs will show install source as 'unknown' rather than 'com.android.vending'; (4) full ADB package list output per device before any removal action, preserved as a timestamped flat file for chain of custody.

Detection — Review mobile application inventory logs from MDM platforms for applications with anomalous subscription billing behavior or apps requesting SMS, call log, or WhatsApp content access permissions without a clear business justification. For GoldFactory RAT indicators, monitor for anomalous outbound

traffic patterns from Android endpoints to Southeast Asian infrastructure, overlay activity (T1021/T1417), and unexpected SMS control events (T1582). Consult threat intelligence platforms (e.g., MISP, VirusTotal, Recorded Future) for GoldFactory IOC sets; no confirmed IOCs are available in the source material for this item.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM: export MDM application inventory reports (available natively in Microsoft Intune, Jamf, or VMware Workspace ONE) and parse with a PowerShell one-liner — 'Import-Csv mdm_inventory.csv | Where-Object { $_.Permissions -match "READ_SMS|READ_CALL_LOG|BIND_ACCESSIBILITY_SERVICE" } | Export-Csv flagged_apps.csv' — to surface CallPhantom-pattern apps requesting SMS/call log access. For GoldFactory overlay detection (MITRE T1417), use NetFlow or Wireshark packet captures on the corporate Wi-Fi SSID used by enrolled devices and filter for persistent long-duration TCP sessions to Indonesian or Southeast Asian IP ranges on non-standard ports. Search VirusTotal for GoldFactory tag and MalwareBazaar for 'GoldFactory' family tag to extract available APK hashes, then compare against MDM APK hash inventory.

Evidence: Before concluding detection phase: (1) MDM permission audit report — specifically flag any app holding RECEIVE_SMS, READ_SMS, BIND_ACCESSIBILITY_SERVICE, or READ_CONTACTS permissions that is not an enterprise-approved application; (2) Google Play Protect scan history logs from enrolled devices (accessible via MDM compliance reports) showing any flagged or suppressed warnings for CallPhantom app package names; (3) outbound network connection logs filtered for Android device MACs/IPs showing connections to IP ranges associated with GoldFactory C2 — cross-reference with known GoldFactory infrastructure reported in Malpedia or Group-IB GoldFactory reporting; (4) SMS and call log access events — on rooted or work-profile Android devices, retrieve logcat output ('adb logcat -d | grep -i "sms\|call_log\|whatsapp"') for evidence of GoldFactory RAT intercepting OTP or WhatsApp content (MITRE T1582, T1417).

Eradication — Remove any identified CallPhantom-affiliated applications from enrolled devices immediately. For GoldFactory-compromised devices, perform a full device wipe; banking trojans with RAT capabilities cannot be reliably remediated through app removal alone. Revoke any sessions or credentials (banking apps, UPI platforms including Google Pay, PhonePe, Paytm) that may have been exposed on compromised devices.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST AC-2 (Account Management), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts)

Compensating: For teams without centralized MDM wipe capability: issue step-by-step device factory reset instructions to affected users with documented confirmation checklist. Use ADB remote wipe command 'adb shell am broadcast -a android.intent.action.MASTER_CLEAR' only if physical access is available and lawful under your device policy. For credential revocation on Google Pay/PhonePe/Paytm without a dedicated IAM platform, contact each payment provider's enterprise or fraud team directly — Google Pay fraud reporting: pay.google.com/about/pay-later/fraud; PhonePe and Paytm each have documented merchant/enterprise fraud escalation paths. Document revocation timestamps per device per platform for breach notification records. Use ClamAV with an Android APK scanning profile on any APKs extracted pre-wipe to confirm GoldFactory family classification before closing the incident.

Evidence: Before wiping GoldFactory-compromised devices, capture the following forensic evidence as it will be destroyed by wipe: (1) full ADB backup of the device if lawful and policy-permitted — 'adb backup -apk -shared -all -f device_backup_[deviceID].ab' — to preserve GoldFactory APK and data artifacts for later analysis; (2) screenshot or logcat capture of active accessibility service registrations ('adb shell settings get secure enabled_accessibility_services') — GoldFactory RATs persist via Accessibility Services to survive app removal and this registry entry confirms active compromise; (3) network connection state at time of eradication — 'adb shell netstat -an' output to document active C2 sessions; (4) list of all accounts linked to affected Google Pay, PhonePe, and Paytm installations, captured from MDM app configuration logs or direct device export before wipe, to scope credential

revocation.

Recovery — After device remediation, require re-enrollment through MDM before restoring access to corporate resources. For users whose financial application credentials were potentially exposed, coordinate with affected financial institutions (Google Pay, PhonePe, Paytm) to freeze accounts and re-issue credentials. Validate that no unauthorized transactions occurred during the exposure window. Monitor re-enrolled devices for 30 days for behavioral anomalies.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST CP-10 (System Recovery and Reconstitution), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For teams without automated MDM compliance gate enforcement: implement a manual re-enrollment checklist requiring IT sign-off that includes: (1) factory reset verification (serial number confirmed wiped in MDM), (2) fresh OS install or factory image confirmed, (3) Google Play Protect re-enabled, (4) only allowlisted apps installed, (5) no 'Install Unknown Apps' permissions granted. For the 30-day monitoring period without EDR: schedule weekly ADB package inventory checks ('adb shell pm list packages -f > weekly_check_[date].txt') and diff against the post-wipe baseline to catch re-emergence of GoldFactory or CallPhantom packages. Use free network monitoring via Wireshark on corporate SSID to spot anomalous outbound Android traffic patterns.

Evidence: During recovery validation: (1) transaction logs from Google Pay, PhonePe, and Paytm accounts — request full transaction history for the exposure window (date of first app install through device wipe) from each financial institution's fraud team; document any transactions not initiated by the account holder as these constitute financial fraud evidence and may trigger regulatory reporting obligations depending on jurisdiction; (2) MDM re-enrollment audit log confirming device serial, enrollment timestamp, and compliance state at time of corporate resource access restoration; (3) Google Play Protect attestation status from MDM compliance report post-re-enrollment, confirming no harmful apps detected on the clean device; (4) network baseline capture from re-enrolled devices during first 72 hours to establish clean behavioral baseline for the 30-day anomaly monitoring period.

Post-Incident — This campaign exposes a gap in mobile application vetting for organizations that permit personal or corporate Android devices to access financial platforms. Review and update your mobile security policy to enforce app allowlisting, prohibit subscription apps with broad data access permissions, and require Play Protect attestation. Map identified control gaps to CIS Benchmark for Mobile Devices and NIST SP 800-124 (Guidelines for Managing the Security of Mobile Devices in the Enterprise). If users in your organization were affected by GoldFactory, this constitutes a social engineering failure — update security awareness training to address brand impersonation of government tax platforms.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For teams without a formal policy management platform: draft a one-page mobile security addendum to your acceptable use policy using NIST SP 800-124 Rev. 2 as the template baseline (available free at nvlpubs.nist.gov). For app allowlisting without enterprise MDM: publish an approved app list distributed via email policy, requiring users to self-certify compliance monthly. For GoldFactory social engineering training: create a 10-minute awareness module using free tools (Google Slides or Canva) showing side-by-side comparisons of the legitimate Indonesian CoreTax portal and GoldFactory's impersonation APK UI — source screenshots from public threat intelligence reports (Group-IB or Cyble GoldFactory coverage). Submit known GoldFactory IOCs and CallPhantom package names to MISP community instance for peer organization benefit.

Evidence: Post-incident documentation to compile for lessons-learned and potential regulatory reporting: (1) full timeline of CallPhantom app install dates vs. subscription charge dates per affected device, sourced from MDM inventory logs and user-reported billing statements — establishes financial harm scope; (2) GoldFactory social engineering delivery artifact, if recoverable — the CoreTax impersonator APK distributed via WhatsApp or direct link, preserved with hash values and VirusTotal submission receipt for threat intel sharing; (3) MDM policy configuration state at time of incident (specifically the 'Install Unknown Apps' and 'Google Play Protect' enforcement settings) to document the control gap; (4) user report log documenting which users self-reported suspicious subscription charges vs. those identified by MDM audit — gap between self-report rate and actual compromise rate informs future security awareness training effectiveness metrics.

Detection Guidance

No confirmed IOCs (hashes, domains, IPs, package names) are available from the cited Tier 3 sources for this item. The following behavioral indicators are derived from the MITRE ATT&CK techniques mapped to this campaign and should be treated as hunting hypotheses, not confirmed signatures.

CallPhantom indicators:

- Android apps requesting READ_CALL_LOG, READ_SMS, or WhatsApp content provider access without a verifiable business function

- Apps with active subscription billing that generate output with no verifiable data source (randomized or static output patterns)

- MDM logs showing installation of apps from Google Play categories associated with surveillance or call-history lookup utilities

GoldFactory indicators:

- Overlay UI activity on financial apps (Google Pay, PhonePe, Paytm); look for accessibility service abuse (T1021) or screen overlay permissions granted to non-system apps

- Keylogging artifacts: unexpected accessibility service registrations on Android devices (T1417)

- SMS control events: outbound SMS to unknown shortcodes or premium numbers (T1582)

- Obfuscated APK delivery: apps installed outside Play Store with certificate anomalies (T1406, T1476)

- Network traffic to unrecognized endpoints from financial app processes

- App masquerading as 'CoreTax' or Indonesian tax authority branding (T1444)

For confirmed IOC sets, query: VirusTotal, community threat intelligence platforms (AlienVault OTX if GoldFactory tag is available), and regional CERT feeds (ID-SIRTII/CC for Indonesia-specific GoldFactory infrastructure). Treat any IOC not confirmed by a primary source as indicative only.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	[not confirmed in available sources]	No specific IOC values are confirmed in the Tier 3 sources cited for this item. Consult VirusTotal, AlienVault OTX (GoldFactory), and ID-SIRTII/CC for current GoldFactory infrastructure indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1516** — Input Injection
- **T1636** — Protected User Data
- **T1444**
- **T1627** — Execution Guardrails
- **T1661** — Application Versioning
- **T1660** — Phishing
- **T1437** — Application Layer Protocol
- **T1476**
- **T1417** — Input Capture
- **T1406** — Obfuscated Files or Information
- **T1582** — SMS Control

OWASP-TOP10-2021

- **A03:2021** — Injection

NIST-800-53R5

- **SI-10** — Information Input Validation

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.26** — Application security requirements

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1516	Input Injection	Defense-Evasion
T1636	Protected User Data	Collection

Technique ID	Technique Name	Tactic
T1444		
T1627	Execution Guardrails	Defense-Evasion
T1661	Application Versioning	Initial-Access
T1660	Phishing	Initial-Access
T1437	Application Layer Protocol	Command-And-Control
T1476		
T1417	Input Capture	Collection
T1406	Obfuscated Files or Information	Defense-Evasion
T1582	SMS Control	Impact

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/fake-call-history-apps-stole-paym...	T3
New ZeroDayRAT Mobile Spyware Enables Real-Time Surveillance ...	https://thehackernews.com/2026/02/new-zerodayrat-mobile-spyware-ena...	T3
Critical Security Vulnerability in Paytm for Business Android App	https://www.linkedin.com/posts/kdmeena_responsibledisclosure-bugbou...	T3
How to Detect Fake PhonePe & GPay Apps - Cashfree Payments	https://www.cashfree.com/blog/spot-fake-upi-payment-app-scams/	T3
WhatsApp Confirms Update After Google Issues 'Attack Surface ...	https://www.forbes.com/sites/zakdoffman/2026/01/26/google-issues-wh...	T3

Generated 2026-05-08 19:04 UTC by TJS Security Command Center