INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-29 14:00 UTC

BTMOB Android RAT Offered as Subscription MaaS with No-Code Phishing Builder Targeting Latin American Users

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0379
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Android devices (all versions supporting Accessibility Services); users targeted via fake Argentinian government agency lures and Google Play impersonation
Published	2026-05-28T17:10:11
Discovery Source	Rss

Executive Summary

BTMOB is a commercially sold Android remote access trojan operating on a subscription model, openly marketed at $700/month, that enables low-skill operators to deploy custom malicious apps targeting Android users, particularly in Latin America via fake government and Google Play lures. The platform abuses Android Accessibility Services to gain deep device control without rooting the device, allowing attackers to intercept credentials, monitor communications, and track location. Organizations with a mobile workforce operating in Latin America, or employees using personal Android devices for work, face elevated risk of credential theft and data exfiltration through this low-barrier, high-volume threat.

Technical Analysis

BTMOB is an Android RAT distributed as malware-as-a-service (MaaS), advertised on the clearweb and sold via Telegram. Pricing is $700/month or $5,000 lifetime. The platform provides a no-code APK builder, enabling rapid generation of custom phishing payloads without developer expertise. The malware abuses Android Accessibility Services - a legitimate Android feature - via CWE-693 (Protection Mechanism Failure) to achieve deep device control without requiring root access. Observed lure themes impersonate Argentinian government agencies and Google Play. BTMOB is linked to the SpySolr malware family as a predecessor. Mapped MITRE ATT&CK Mobile techniques include: T1476 (Deliver Malicious App via Other Means), T1418 (Software Discovery), T1417 (Input Capture), T1412 (Capture SMS Messages), T1444 (Masquerade as Legitimate Application), T1582 (SMS Control), T1406 (Obfuscated Files or Information), T1521 (Encrypted Channel),

T1430 (Location Tracking), T1513 (Screen Capture). No CVE is assigned. No vendor patch exists because the attack vector is not a software defect but intentional abuse of a legitimate Android design feature. Mitigation is defensive and behavioral, not patch-based.

Action Checklist

1. Step 1: Containment, Immediately audit which employees use personal Android devices for corporate email, VPN, or app access under any BYOD policy. Restrict corporate resource access from unmanaged Android devices pending a mobile device management (MDM) policy review. Per NIST AC-20 (Use of External Information Systems), enforce documented terms and conditions for BYOD device use before corporate access is permitted.
2. Step 2: Detection, Enroll managed Android devices in an MDM or mobile threat defense (MTD) solution capable of detecting Accessibility Service abuse. Query MDM telemetry for apps with active Accessibility Service permissions that are not on an approved list (CIS 2.1, Software Inventory; CIS 2.3, Address Unauthorized Software). Monitor for APKs sideloaded outside of approved app stores. Review endpoint logs for anomalous outbound encrypted channels from mobile devices (NIST AU-2, AU-6). Behavioral IOCs: apps requesting Accessibility Service permissions that were installed via sideload, apps impersonating government agencies or Google Play, unexpected SMS exfiltration activity, or abnormal location data egress.
3. Step 3: Eradication, Remove any identified BTMOB-infected devices from corporate network access immediately. Uninstall suspicious APKs and revoke any OAuth or corporate credentials that may have been accessed on the compromised device. Revoke and rotate all credentials the user authenticated with on the affected device per incident response credential rotation procedures. Enforce a policy requiring apps to be installed only from the official Google Play Store; disable sideloading (unknown sources) on all managed devices via MDM policy (NIST AC-3, Access Enforcement; CIS 4.6, Securely Manage Enterprise Assets and Software).
4. Step 4: Recovery, After credential rotation and device remediation, verify no residual Accessibility Service permissions remain active on managed devices. Confirm MDM enrollment and policy compliance before restoring corporate access. Re-validate MFA enrollment for affected accounts (CIS 6.3, 6.5). Monitor affected accounts for 30 days for signs of unauthorized access, credential reuse, or abnormal login patterns (NIST AU-6, Audit Record Review).
5. Step 5: Post-Incident, This campaign exposes gaps in mobile asset governance and BYOD policy enforcement. Conduct a mobile-specific risk assessment. Implement or review the mobile device acceptable use policy referencing NIST AC-19 (Access Control for Mobile Devices) and AC-20 (Use of External Systems). Establish a software inventory for mobile apps on managed devices (CIS 2.1). If Latin America is a significant operating region, add mobile-targeted MaaS threat tracking to the threat intelligence program. Evaluate whether current MDM tooling can detect Accessibility Service abuse; if not, this is a capability gap requiring remediation.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to legal and privacy counsel if forensic review confirms that BTMOB-infected devices had active access to applications containing PII, PHI, or financial data, as SMS interception and credential harvesting via Accessibility Service abuse may trigger breach notification obligations under GDPR, LGPD (Brazil), or applicable US state privacy laws; also escalate if more than one managed device is confirmed infected, indicating the BTMOB operator may have run a targeted campaign against the organization rather than opportunistic infection.
Recovery Notes	After device factory reset and credential rotation, verify that re-enrolled managed devices have MDM policy enforcement confirmed for three specific controls before restoring corporate access: sideloading disabled, Accessibility Service grant monitoring active, and SMS-based MFA replaced with authenticator-app or hardware token MFA for all affected accounts. Monitor affected user accounts in identity provider logs daily for the first 14 days and weekly for the subsequent 16 days (30 days total), specifically filtering for authentication events from unrecognized devices or geolocations inconsistent with the user's work location — BTMOB credential harvesting may enable delayed account takeover attempts by the MaaS operator or secondary purchasers of harvested credentials on criminal markets. If your organization operates in or serves users in Latin America, extend monitoring to corporate email and VPN accounts for all employees in that region, not just confirmed-infected devices, as the BTMOB subscription model means multiple operators may be running concurrent campaigns with the same tooling against the same target demographics.
Forensic Artifacts	Android Accessibility Service grant dump ('adb shell dumpsys accessibility') — captures every app with active Accessibility Service permissions at time of collection; BTMOB requires this permission to intercept keystrokes, read screen content, and simulate user actions without root, making this the primary persistence indicator specific to this RAT's operational mechanism | APK installer provenance records ('adb shell pm list packages -i') — identifies packages where the installer field is null or shows a sideload origin rather than 'com.android.vending', which is the delivery method for BTMOB since it cannot be distributed through the official Google Play Store; fake Argentinian government agency apps (targeting AFIP, ANSES, or similar) and fake Google Play update APKs are the specific lure formats documented in this campaign | Perimeter firewall and DNS logs filtered for mobile device IP ranges — BTMOB exfiltrates intercepted SMS messages, harvested credentials, and device location data to operator-controlled C2 servers over encrypted channels; DNS queries to newly registered or uncategorized domains from mobile device IPs, and periodic outbound HTTPS beacon patterns with consistent intervals, are the network-layer artifacts this RAT's C2 communication would produce | Identity provider and corporate email authentication logs for the full suspected infection window — BTMOB's Accessibility Service abuse enables it to read on-screen content including email, banking apps, and corporate applications, meaning the authentication log for any corporate app accessed while BTMOB was active represents the full scope of potentially harvested session tokens and credentials | Extracted BTMOB APK binary (preserved via 'adb pull /data/app//base.apk' before device wipe) — the APK's AndroidManifest.xml will contain the declared Accessibility Service configuration, required permissions (including RECEIVE_SMS, ACCESS_FINE_LOCATION, READ_CONTACTS, and BIND_ACCESSIBILITY_SERVICE), and C2 configuration strings; this artifact supports YARA rule development for detecting BTMOB variants and enables hash submission to threat intelligence sharing platforms to warn other organizations

Per-Action IR Details

Step 1: Containment — Immediately audit which employees use personal Android devices for corporate email, VPN, or app access under any BYOD policy. Restrict corporate resource access from unmanaged Android

devices pending a mobile device management (MDM) policy review. Per NIST AC-20, enforce documented terms and conditions for external system (personal device) use before corporate access is permitted.

NIST Phase: Containment

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

Controls: NIST AC-20 (Use of External Systems), NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without MDM, use your identity provider (Azure AD, Okta, or Google Workspace) to create a conditional access policy blocking authentication from non-compliant or unregistered device IDs. If no IdP conditional access is available, pull the VPN access log and manually cross-reference device IDs against your asset inventory — any Android device not in inventory gets its VPN certificate or account disabled immediately via your VPN admin console. Document each block with the device ID and user account affected.

Evidence: Before restricting access, capture the full corporate identity provider sign-in logs filtered for Android user-agent strings and mobile OS identifiers to establish a baseline of which personal devices have already authenticated to corporate resources. Export VPN gateway logs showing source IP, device fingerprint, and authentication timestamps for all Android sessions in the prior 30 days — BTMOB's credential interception via Accessibility Service abuse means any device that accessed corporate credentials in this window must be treated as potentially compromised.

Step 2: Detection — Enroll managed Android devices in an MDM or mobile threat defense (MTD) solution capable of detecting Accessibility Service abuse. Query MDM telemetry for apps with active Accessibility Service permissions that are not on an approved list (CIS 2.1 — Software Inventory; CIS 2.3 — Address Unauthorized Software). Monitor for APKs sideloaded outside of approved app stores. Review endpoint logs for anomalous outbound encrypted channels from mobile devices (NIST AU-2, AU-6). Behavioral IOCs: apps requesting Accessibility Service permissions that were installed via sideload, apps impersonating government agencies or Google Play, unexpected SMS exfiltration activity, or abnormal location data egress.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-3 (Malicious Code Protection), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 8.2 (Collect Audit Logs)

Compensating: On managed Android devices without MTD, use Android Debug Bridge (ADB) to run 'adb shell dumpsys accessibility' to list all apps with active Accessibility Service grants — compare output against your approved app whitelist and flag any sideloaded package names (non-Play Store installs appear without a com.android.vending installer record, verifiable via 'adb shell pm list packages -i' and grepping for installer fields that are null or show 'sideload'). For network detection on a budget, deploy Wireshark or tcpdump at the network egress point and filter for anomalous HTTPS beacon patterns originating from mobile device IP ranges — BTMOB C2 communications will appear as periodic encrypted outbound sessions to non-categorized IP ranges. Use osquery on any enrolled device capable of running it, or pivot to firewall/DNS logs to flag mobile device queries to newly registered or uncategorized domains.

Evidence: Capture the output of 'adb shell dumpsys accessibility' from each managed device before any remediation — this output records every app currently granted Accessibility Service permissions, which is the primary persistence and control mechanism BTMOB uses. Pull Android device package installation logs ('adb shell pm list packages -i -f') to identify APKs installed outside Google Play (installer field will not show 'com.android.vending'). Collect network flow logs from your perimeter firewall or proxy, filtering for outbound HTTPS sessions from mobile device IP ranges to uncategorized or newly registered domains — BTMOB exfiltrates intercepted SMS, credentials, and location data over encrypted channels to operator-controlled C2 infrastructure. Document any app with a package name impersonating Argentinian government agencies (e.g., AFIP, ANSES, Renaper) or Google-branded package names from non-Google publishers.

Step 3: Eradication — Remove any identified BTMOB-infected devices from corporate network access immediately. Uninstall suspicious APKs and revoke any OAuth or corporate credentials that may have been

accessed on the compromised device. Revoke and rotate all credentials the user authenticated with on the affected device per D3-CRO (Credential Rotation). Enforce a policy requiring apps to be installed only from the official Google Play Store; disable sideloading (unknown sources) on all managed devices via MDM policy (NIST AC-3 — Access Enforcement; CIS 4.6 — Securely Manage Enterprise Assets and Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For BYOD devices where you cannot remotely uninstall apps, require the user to perform a factory reset before re-enrollment — BTMOB's Accessibility Service persistence survives simple app uninstalls if the malicious APK has been granted device administrator rights. Verify Accessibility Service grants are cleared post-reset via 'adb shell dumpsys accessibility' before allowing corporate re-enrollment. For credential rotation without enterprise tooling, use your IdP admin console to immediately invalidate all active sessions and OAuth tokens for the affected user, force password reset, and re-enroll MFA tokens — assume BTMOB intercepted both the password and any SMS-based OTP codes the user received while the RAT was active, so SMS-based MFA must be replaced with authenticator-app or hardware token MFA for the affected account.

Evidence: Before wiping or factory resetting the device, capture a full backup of the device's app data using 'adb backup -all -apk -shared' if the device owner consents — this preserves the BTMOB APK, its configuration files, and any locally cached C2 communication artifacts for later analysis. Extract and preserve the malicious APK file ('adb pull /data/app//base.apk') for YARA-based signature development and submission to threat intelligence feeds. Document all Accessibility Service permissions granted, all accounts authenticated on the device (from browser saved credentials, email apps, and VPN client configs), and the device's full outbound network connection history from your firewall logs before eradication proceeds.

Step 4: Recovery — After credential rotation (D3-CRO) and device remediation, verify no residual Accessibility Service permissions remain active on managed devices. Confirm MDM enrollment and policy compliance before restoring corporate access. Re-validate MFA enrollment for affected accounts (CIS 6.3, 6.5; D3-MFA). Monitor affected accounts for 30 days for signs of unauthorized access, credential reuse, or abnormal login patterns (NIST AU-6 — Audit Record Review; D3-LAM — Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Without a SIEM, create a manual daily review process using identity provider sign-in logs — export CSV reports of authentication events for affected accounts and filter for: logins from new geographic locations, logins from device types not matching the re-enrolled managed device, logins occurring outside business hours, and any MFA bypass events. For the 30-day monitoring window, set up free alert rules in your IdP (Azure AD Free tier supports basic sign-in risk alerts; Google Workspace supports login challenge notifications) to trigger on impossible travel or new device logins for the flagged accounts. Re-validate that SMS-based MFA has been replaced for all affected accounts before re-granting corporate access — BTMOB intercepted SMS OTPs during the infection window, making SMS MFA an untrusted factor for these users going forward.

Evidence: Before restoring access, run 'adb shell dumpsys accessibility' one final time on the remediated device and confirm the output shows zero third-party app grants — document this output as your clean-state baseline for the device record. Pull the MDM compliance report confirming the device's enrollment status, OS patch level, and confirmation that 'Install Unknown Apps' (sideloading) is disabled. Preserve identity provider authentication logs for affected accounts covering the full suspected BTMOB infection window as forensic evidence of what credentials and sessions were potentially harvested — this establishes scope for any required breach notification assessment.

Step 5: Post-Incident — This campaign exposes gaps in mobile asset governance and BYOD policy enforcement. Conduct a mobile-specific risk assessment. Implement or review the mobile device acceptable use policy referencing NIST AC-19 (Access Control for Mobile Devices) and AC-20 (Use of External Systems). Establish a software inventory for mobile apps on managed devices (CIS 2.1). If Latin America is a significant operating region, add mobile-targeted MaaS threat tracking to the threat intelligence program. Evaluate whether current MDM tooling can detect Accessibility Service abuse — if not, this is a capability gap requiring remediation.

NIST Phase: Post Incident

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

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-20 (Use of External Systems), NIST RA-3 (Risk Assessment), NIST IR-4 (Incident Handling), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: To track BTMOB and similar Android MaaS campaigns without a commercial threat intelligence subscription, monitor MITRE ATT&CK for Mobile (specifically T1417 — Input Capture via Accessibility Service, T1582 — SMS Control, and T1430 — Location Tracking) for new technique updates. Subscribe to free threat feeds from MalwareBazaar and abuse.ch for newly submitted Android APK hashes associated with BTMOB infrastructure. Build a YARA rule from the extracted BTMOB APK (Step 3 evidence) targeting characteristic strings in the Accessibility Service declaration, C2 beacon format, or package naming conventions used in the fake Argentinian government lures, and deploy it via a free YARA scanner in your MDM app review pipeline or email gateway to catch future BTMOB-derived variants. Document the MDM Accessibility Service detection gap as a formal risk acceptance or remediation item in your risk register.

Evidence: Compile a full incident timeline from preserved artifacts — MDM enrollment logs, ADB accessibility dumps, network flow records, and IdP authentication logs — to establish the full scope of what credentials and corporate data were accessible on BTMOB-infected devices. This timeline is required input for the mobile-specific risk assessment and must document whether any regulated data (PII, PHI, financial records) was accessible via apps running on the infected device during the infection window, which determines breach notification obligations.

Detection Guidance

No CVE-specific signatures apply. Detection is behavioral. Primary signals: (1) Android apps with Accessibility Service permissions that are not pre-approved, query MDM for all devices with active Accessibility Service grants; flag any app not on an allowlist. (2) Sideloaded APKs, MDM telemetry should flag installs from unknown sources; enforce CIS 2.3 (Address Unauthorized Software). (3) Apps impersonating Argentinian government agencies (e.g., ANSES, AFIP, Migraciones) or Google Play, validate developer certificates and package names against official sources. (4) Anomalous encrypted outbound traffic from mobile devices to unfamiliar endpoints, consistent with BTMOB's use of encrypted command-and-control channels (T1521). (5) Unexpected SMS read/send activity or screen capture events from non-approved apps (T1412, T1513). NIST AU-2 and AU-6 apply; ensure mobile device activity logs are collected and reviewed. Monitor for ongoing suspicious Accessibility Service permission grants.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/btmob-android-malware-service-generates-custom-phishing-payloads/`	BleepingComputer reporting on BTMOB MaaS — primary news source; not a malicious IOC	LOW
DOMAIN	`zimperium.com/blog`	Zimperium research blog identified as a source for this campaign — no specific malicious IOCs were extractable from the provided source data	LOW

Framework Mappings

MITRE-ATTACK

- **T1476**
- **T1418** — Software Discovery
- **T1417** — Input Capture
- **T1412**
- **T1444**
- **T1582** — SMS Control
- **T1406** — Obfuscated Files or Information
- **T1521** — Encrypted Channel
- **T1430** — Location Tracking
- **T1513** — Screen Capture

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

NIST-800-53R5

- **AC-6** — Least Privilege
- **AT-2** — Literacy Training and Awareness
- **SI-4** — System Monitoring

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1476		
T1418	Software Discovery	Discovery
T1417	Input Capture	Collection
T1412		
T1444		
T1582	SMS Control	Impact
T1406	Obfuscated Files or Information	Defense-Evasion
T1521	Encrypted Channel	Command-And-Control
T1430	Location Tracking	Collection
T1513	Screen Capture	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/btmob-android-malwar...	T3
Researchers have found a new case where government authorities ...	https://www.facebook.com/techcrunch/posts/researchers-have-found-a-...	T3
Zimperium Blog	https://zimperium.com/blog	T3
Android security - TAdviser	https://tadviser.com/index.php/Article:Android_security	T3

Source	URL	Tier
Android "Fake ID" Vulnerability Lets Malicious Apps Impersonate ...	https://www.securityweek.com/android-fake-id-vulnerability-lets-mal...	**T3**

Generated 2026-05-29 14:00 UTC by TJS Security Command Center