INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-28 06:45 UTC

Grandoreiro and BTMOB RAT Campaigns Extend Banking Trojan Reach Across Windows and Android in Spain, Portugal, and Mexico

THREAT CAMPAIGN | HIGH | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0376
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Windows devices (Grandoreiro banking trojan), Android devices (BTMOB RAT); financial sector users and organizations in Spain, Portugal, and Mexico
Published	2026-05-27T12:10:21
Discovery Source	Rss

Executive Summary

Active campaigns are delivering the Grandoreiro banking trojan to Windows systems and the BTMOB remote access trojan to Android devices, targeting financial sector organizations and customers in Spain, Portugal, and Mexico. Attackers can steal banking credentials, intercept active banking sessions, and harvest mobile banking data, creating direct financial fraud exposure across both desktop and mobile channels. Organizations operating in affected regions with customer-facing banking services face elevated fraud liability and potential regulatory scrutiny under applicable data protection regimes.

Technical Analysis

Two concurrent campaigns target financial sector victims across Spain, Portugal, and Mexico using complementary malware families. Grandoreiro is a long-documented Windows banking trojan distributed via spear-phishing emails (T1566.001, T1566). Post-execution capabilities include keylogging (T1056.001), screen overlay attacks to intercept credentials (T1411), data collection from local systems (T1005), process injection (T1055), and adversary-in-the-middle positioning during live banking sessions (T1557). BTMOB RAT targets Android devices, enabling credential harvesting from mobile banking applications (T1417, T1417.001), contact and account data enumeration (T1432, T1435), location tracking (T1430), screen capture (T1513), and abuse of accessibility services (T1516). The dual-platform deployment eliminates the gap left when organizations harden only desktop banking channels. Grandoreiro operators are assessed as Brazilian-speaking (per WatchGuard threat report) and operate under a Malware-as-a-Service model. BTMOB RAT operator attribution is

unconfirmed. Relevant weaknesses include CWE-267 (privilege abuse), CWE-312 (cleartext storage of sensitive information), and CWE-359 (exposure of private personal information). No CVE identifier applies. Reporting originates from WatchGuard and ESET; the primary The Hacker News URL (2026-05-xx) was not actively verified and should be treated as unconfirmed until human validation.

Action Checklist

1. Containment: Block known Grandoreiro and BTMOB RAT distribution infrastructure at email gateway and web proxy. Apply phishing email controls aligned with NIST SI-3 (malware protection) and SC-7 (boundary protection) to flag messages with financial-lure subjects targeting Spain, Portugal, and Mexico regional themes. Enforce CIS 4.4 and CIS 4.5 host and server firewall rules to restrict unexpected outbound connections from endpoints where banking application access occurs.
2. Detection: Hunt for Grandoreiro indicators: unusual process injection activity (T1055), unexpected child processes spawned from email clients or browsers, keylogger artifacts, and overlay window creation events on Windows hosts. For Android environments, review mobile device management (MDM) logs for applications requesting accessibility service permissions (T1516), unexpected contact/account enumeration, or screen capture activity (T1513). Apply AU-6 (audit record review and analysis) cadence to SIEM logs for lateral movement and data staging (T1005). Validate against WatchGuard and ESET published IOCs once the primary reporting URL is human-verified.
3. Eradication: Remove confirmed malware infections using endpoint detection and response tooling. Revoke and rotate all credentials (NIST AC-2 account management, IA-4 identifier management) for accounts active on compromised Windows or Android devices. Disable and re-provision affected Android devices through MDM where BTMOB RAT infection is confirmed. Audit and enforce AC-6 (least privilege) on all accounts used to access banking platforms.
4. Recovery: Re-image confirmed Grandoreiro-infected Windows endpoints before returning to production. Verify integrity of system initialization configurations post-remediation (NIST CM-2 baseline configuration, SI-7 system monitoring). Confirm no persistence mechanisms remain via startup config and scheduled task review. Monitor recovered accounts for anomalous banking session activity for a minimum of 30 days. Apply AU-11 (audit record retention) to preserve forensic logs for post-incident review.
5. Post-Incident: Assess phishing resilience: review email filtering rules and user awareness training coverage for financial-lure themes (NIST SI-4, AU-2). Evaluate whether mobile device management policies enforce application allowlisting and restrict accessibility service grants on Android devices (CIS 2.3). Confirm MFA enrollment for all externally-exposed banking applications (CIS 6.3) and remote access (CIS 6.4). Document control gaps exposed by dual-platform delivery and update incident response playbooks to address simultaneous Windows and Android compromise scenarios.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if forensic evidence confirms banking credential exfiltration or active fraudulent transaction initiation from any compromised account, or if any regulated financial institution in the affected regions (Spain, Portugal, Mexico) has customer PII/account data exposed — triggering NIS2, CNBV, or Banco de España incident notification obligations within mandated timeframes.

Recovery Notes	Re-imaged Windows endpoints must not be returned to production until the banking application is reinstalled from vendor-verified media and post-imaging integrity checks (Sigcheck, scheduled task diff) are clean. Recovered Android devices must be re-enrolled through MDM with an explicit policy blocking non-system accessibility service grants before any banking application is installed. Monitor all recovered accounts for a minimum of 30 days for anomalous banking session indicators — specifically off-hours logins, session originating from new geolocations, and transaction velocity anomalies consistent with Grandoreiro's documented automated fraudulent transfer capability.
Forensic Artifacts	Windows AppData\Roaming and AppData\Local subdirectories: Grandoreiro stores encrypted configuration files and staging data in randomized-name folders within user profile AppData — collect full directory listings and file hashes from these paths on all suspect endpoints before eradication | Sysmon Event ID 8 (CreateRemoteThread) and Event ID 10 (ProcessAccess) logs: Grandoreiro's process injection routine (T1055) targeting browser and banking application processes leaves specific cross-process access records that identify both the injector and the injected target process by PID and image path | Windows Security Event Log Event ID 4688 (Process Creation) with full command-line logging: captures the execution chain from phishing lure document or fake installer through Grandoreiro's loader stages, revealing LOLBin abuse (mshta.exe, regsvr32.exe, or AutoIt interpreter) used in delivery | Android ADB output of 'dumpsys accessibility' and 'pm list packages -f': BTMOB RAT persists via accessibility service binding — this output captures the active service name, the APK path, and the package signing certificate hash, which are the primary forensic identifiers for the specific BTMOB RAT variant deployed | Email gateway message trace and raw headers for financial-lure phishing messages: preserves sender infrastructure (originating IP, SPF/DKIM pass-fail, sending domain registration date) and attachment/URL payload metadata specific to the Grandoreiro distribution campaign targeting Spanish, Portuguese, and Mexican financial institution branding

Per-Action IR Details

Containment — Block known Grandoreiro and BTMOB RAT distribution infrastructure at email gateway and web proxy. Apply phishing email controls aligned with NIST SI-4 (system monitoring) to flag messages with financial-lure subjects targeting Spain, Portugal, and Mexico regional themes. Enforce CIS 4.4 and CIS 4.5 host and server firewall rules to restrict unexpected outbound connections from endpoints where banking application access occurs.

NIST Phase: Containment

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

Controls: NIST SI-4 (System Monitoring), NIST SC-7 (Boundary Protection), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 3 (network connections) and Event ID 1 (process creation) on Windows endpoints accessing banking platforms. On the perimeter, use pi-hole or hosts-file-based DNS blocking for known Grandoreiro C2 domains published in ESET and WatchGuard advisories. For email, use free SpamAssassin rules or Microsoft Defender (free tier) with custom rules matching Spanish/Portuguese/Mexican financial-lure keyword patterns (e.g., 'BBVA', 'Santander', 'SAT Mexico', 'factura', 'comprobante'). On Android MDM (e.g., free tier of Miradore or manual ADB review), flag apps requesting BIND_ACCESSIBILITY_SERVICE.

Evidence: Before blocking, export the full email gateway message trace for the 30-day window preceding detection — capture sender domains, X-Originating-IP headers, and attachment/link metadata from phishing lures using Spanish, Portuguese, or Mexican financial institution branding. Capture DNS query logs from the recursive resolver showing lookups to Grandoreiro C2 infrastructure (typically rotating domains using DGA patterns documented in ESET's

Grandoreiro analyses). Export firewall netflow or proxy logs showing outbound HTTP/HTTPS to suspicious IPs on ports 443/80 originating from endpoints running banking applications. Preserve raw email headers of lure messages for sender policy framework (SPF/DKIM) forensic analysis.

Detection — Hunt for Grandoreiro indicators: unusual process injection activity (T1055), unexpected child processes spawned from email clients or browsers, keylogger artifacts, and overlay window creation events on Windows hosts. For Android environments, review mobile device management (MDM) logs for applications requesting accessibility service permissions (T1516), unexpected contact/account enumeration, or screen capture activity (T1513). Apply AU-6 (audit record review and analysis) cadence to SIEM logs for lateral movement and data staging (T1005). Validate against WatchGuard and ESET published IOCs once the primary reporting URL is human-verified.

NIST Phase: Detection Analysis

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

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

Compensating: On Windows: query Sysmon Event ID 1 (Process Create) for cmd.exe, powershell.exe, or mshta.exe spawned as children of Outlook.exe, Thunderbird.exe, or any browser process. Query Sysmon Event ID 8 (CreateRemoteThread) targeting banking application processes for T1055 injection evidence. Use the free Sigma rule 'proc_creation_win_grandoreiro' (available on SigmaHQ GitHub) converted to PowerShell Get-WinEvent queries. For overlay window detection (Grandoreiro's primary banking credential theft mechanism), run: Get-WinEvent -LogName 'Microsoft-Windows-Win32k/Operational' | Where-Object {$_.Id -eq 260} to identify topmost window creation events during banking app sessions. On Android via ADB: run 'adb shell dumpsys accessibility' to enumerate all apps with active accessibility service bindings — any non-system app listed is a high-priority IOC for BTMOB RAT T1516 abuse.

Evidence: Collect Windows Security Event Log Event ID 4688 (Process Creation with command-line auditing enabled) filtered on processes spawned by email clients or browsers during the period of suspected compromise. Capture Sysmon Event ID 10 (ProcessAccess) logs showing handles opened against banking application processes (e.g., the bank's desktop client or browser instances with banking URLs active). On Android, extract the accessibility service grant history via ADB ('adb shell settings get secure enabled_accessibility_services') and MDM enrollment logs showing app installation timestamps outside normal provisioning windows. Collect Windows prefetch files from %SystemRoot%\Prefetch for execution evidence of Grandoreiro loader components (typically disguised as PDF or document launchers). Preserve memory dump of any process exhibiting injection behavior before killing it — Grandoreiro uses in-memory execution that will not survive process termination.

Eradication — Remove confirmed malware infections using endpoint detection and response tooling. Revoke and rotate all credentials (D3-CRO) for accounts active on compromised Windows or Android devices. Disable and re-provision affected Android devices through MDM where BTMOB RAT infection is confirmed. Audit and enforce AC-6 (least privilege) on all accounts used to access banking platforms.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST IA-4 (Identifier Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without EDR: use Sysinternals Autoruns (free) to enumerate and remove Grandoreiro persistence entries across HKCU\Software\Microsoft\Windows\CurrentVersion\Run, scheduled tasks, and startup folders — export baseline before and after for diff comparison. Use ClamAV with the latest unofficial signature sets (including malwarebazaar-sourced Grandoreiro YARA rules) for filesystem scanning. For Android BTMOB RAT removal without MDM: perform factory reset via recovery mode — do not rely on in-OS uninstall given BTMOB RAT's documented use of accessibility services to resist removal. Credential rotation must cover: online banking portal passwords, any password manager credentials stored in the compromised browser profile, and any SMS-based OTP phone numbers tied to banking accounts on the compromised Android device.

Evidence: Before initiating removal, capture a full Autoruns export (autorunsc.exe -a * -c > autoruns_baseline.csv) from compromised Windows hosts to document all persistence mechanisms Grandoreiro may have installed. Extract the Windows registry hive HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent for offline analysis. On Android, use ADB to pull the app list ('adb shell pm list packages -f') and the accessibility service configuration before factory reset — this establishes which BTMOB RAT package names and signing certificates were active. Capture network connection state ('netstat -ano' on Windows, 'adb shell netstat' on Android) immediately before eradication to document active C2 connections with destination IPs and ports for IOC reporting.

Recovery — Re-image confirmed Grandoreiro-infected Windows endpoints before returning to production. Verify integrity of system initialization configurations post-remediation (D3-SICA). Confirm no persistence mechanisms remain via startup config and scheduled task review. Monitor recovered accounts for anomalous banking session activity for a minimum of 30 days. Apply AU-11 (audit record retention) to preserve forensic logs for post-incident review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), NIST CM-6 (Configuration Settings), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Verify post-reimaging integrity using Sysinternals Sigcheck (free) to validate digital signatures of all executables in %SystemRoot%\System32 and the banking application install directory — Grandoreiro has been documented replacing or side-loading legitimate DLLs. Run 'schtasks /query /fo LIST /v > scheduled_tasks_post_reimage.txt' and diff against a known-good baseline from a clean reference image. For the 30-day banking session monitoring without a SIEM, configure Windows Security Event Log audit policy for Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) on the endpoint and forward via Windows Event Forwarding (WEF) to a central Windows Event Collector at no cost. On Android, re-enroll through MDM and enforce a policy blocking accessibility service grants to non-system apps before the device handles any banking application.

Evidence: Preserve the forensic image (or at minimum a Velociraptor/KAPE triage collection) of the compromised Windows endpoint before reimaging — Grandoreiro artifacts including its loader, encrypted configuration files (typically stored in AppData\Roaming or AppData\Local under randomized folder names), and injected memory regions must be retained for threat intelligence and potential law enforcement referral. Archive all SIEM/WEF logs covering the incident window per AU-11 retention requirements, noting that Grandoreiro campaigns targeting Spanish and Portuguese banks have been subject to coordinated law enforcement action (Europol operations) where forensic evidence has investigative value beyond internal IR.

Post-Incident — Assess phishing resilience: review email filtering rules and user awareness training coverage for financial-lure themes (NIST SI-4, AU-2). Evaluate whether mobile device management policies enforce application allowlisting and restrict accessibility service grants on Android devices (CIS 2.3). Confirm MFA enrollment for all externally-exposed banking applications (CIS 6.3) and remote access (CIS 6.4). Document control gaps exposed by dual-platform delivery and update incident response playbooks to address simultaneous Windows and Android compromise scenarios.

NIST Phase: Post Incident

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

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 2.3 (Address Unauthorized Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct a tabletop exercise specifically modeling the Grandoreiro dual-channel attack path: phishing email delivers Windows loader while a smishing or social engineering vector delivers BTMOB RAT to the victim's registered mobile banking number — test whether your playbook handles credential theft from both channels simultaneously. For email filtering gap assessment without a commercial tool, export your email gateway's message disposition report for the 90 days prior to incident and run keyword frequency analysis (PowerShell or Python) against

subject lines for Spanish/Portuguese financial lure terms. Publish internal advisory to end users covering Grandoreiro's specific lure themes (fake tax authority notifications from Mexico's SAT, fake BBVA/Santander/CaixaBank alerts) using actual lure samples from the incident.

Evidence: Compile a lessons-learned artifact package including: the full IOC set (Grandoreiro C2 domains/IPs, BTMOB RAT package hashes, phishing sender domains) for submission to FS-ISAC or national CERTs (CCN-CERT for Spain, CNCS for Portugal, CERT-MX for Mexico) as these campaigns are actively tracked by regional authorities. Document which email filtering rules failed to catch the lure and which MDM policy gaps permitted the BTMOB RAT accessibility service grant — these become the measurable control improvements for the post-incident report. Retain all evidence per AU-11 retention policy with attention to potential regulatory notification obligations under Spain's NIS2 transposition, Portugal's Lei n.º 65/2021, or Mexico's CNBV cybersecurity regulations if banking customer data or credentials were confirmed exfiltrated.

Detection Guidance

Windows (Grandoreiro): Monitor for process injection (T1055) from browser or email client parent processes. Alert on creation of overlay windows during active browser sessions. Detect keylogger artifacts via file system monitoring of temp directories and unusual registry writes. Flag outbound connections to newly registered or low-reputation domains from financial workstations (NIST AU-2, AU-6). Use account management monitoring (NIST AC-2) to identify privilege escalation or unexpected local account activity post-infection. Android (BTMOB RAT): In MDM or mobile threat defense platforms, alert on applications granted accessibility service permissions outside of approved app inventory (CIS 2.1, CIS 2.3). Monitor for unexpected enumeration of contacts (T1435) or account data (T1432), screen capture API calls (T1513), and background location polling (T1430). Flag sideloaded applications not present in enterprise app catalog. Cross-platform: Correlate Windows and Android telemetry for the same user identity; simultaneous credential theft across both platforms is a strong indicator of this campaign's dual-deployment pattern. IOC validation: Confirm and operationalize specific hashes, domains, and IPs from WatchGuard and ESET advisories once the primary reporting URL is human-validated. Note: No verified IOC values are available in the current data set; do not deploy unverified indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not available — pending human validation of primary source URL]`	Grandoreiro C2 and BTMOB RAT distribution infrastructure — IOCs reported by WatchGuard and ESET but not extractable from unverified source. Obtain from WatchGuard and ESET advisories directly.	LOW

Framework Mappings

MITRE-ATTACK

- **T1516** — Input Injection
- **T1435**
- **T1582** — SMS Control
- **T1566.001** — Spearphishing Attachment

- **T1411**
- **T1432**
- **T1444**
- **T1417.001** — Keylogging
- **T1430** — Location Tracking
- **T1056.001** — Keylogging
- **T1005** — Data from Local System
- **T1417** — Input Capture
- **T1055** — Process Injection
- **T1557** — Adversary-in-the-Middle
- **T1513** — Screen Capture
- **T1566** — Phishing

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **CA-7** — Continuous Monitoring

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1516	Input Injection	Defense-Evasion
T1435		

Technique ID	Technique Name	Tactic
T1582	SMS Control	Impact
T1566.001	Spearphishing Attachment	Initial-Access
T1411		
T1432		
T1444		
T1417.001	Keylogging	Collection
T1430	Location Tracking	Collection
T1056.001	Keylogging	Collection
T1005	Data from Local System	Collection
T1417	Input Capture	Collection
T1055	Process Injection	Defense-Evasion
T1557	Adversary-in-the-Middle	Credential-Access
T1513	Screen Capture	Collection
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/grandoreiro-malware-and-btmob-rat...	T3
IT ServiSource (PTY) LTD's Post - LinkedIn	https://www.linkedin.com/posts/it-servisource_microsoft-third-party...	T3
Mobile Android Is an Even Bigger Opportunity for Attackers Than ...	https://www.paloaltonetworks.com/blog/2018/02/sp-mobile-android-eve...	T3
Mobile device security: Why protection is critical in the hybrid ... - IBM	https://www.ibm.com/think/insights/mobile-device-security-why-prote...	T3
Windows Trojan Targets Android, iOS Devices via USB Connection	https://www.securityweek.com/windows-trojan-targets-android-ios-dev...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-28 06:45 UTC by TJS Security Command Center