BTMOB RAT – Malware Trends Tracker by ANY.RUN

By Stanislav Gayvoronsky

Archived: 2026-04-05 21:52:19 UTC

BTMOB RAT: The Android Phantom Hijacking Your Wallet

Key Takeaways

1. **Commercial-Grade Mobile Malware**: BTMOB RAT operates as Malware-as-a-Service with lifetime licenses selling for $5,000, representing a dangerous shift toward professionalized mobile threats with rapid development cycles.
2. **Beyond Traditional Mobile Malware**: This isn't just another Android trojan: it combines live screen control, banking overlay attacks, cryptocurrency theft, and comprehensive surveillance capabilities that rival desktop RATs.
3. **Accessibility Service Weaponization**: The malware exploits Android's accessibility features designed for disabled users, turning assistive technology into a powerful attack vector that bypasses most traditional mobile security measures.
4. **Financial Services in the Crosshairs**: With specialized capabilities targeting Alipay and banking apps through real-time overlay attacks, BTMOB RAT represents a new era of mobile financial fraud that threatens both personal and corporate banking security.
5. **Defense Strategies**: Detect via IOCs like specific domains and behavioral anomalies; prevent with app vetting, updates, and MTD tools; leverage threat intelligence for proactive blocking and variant tracking.

 BTMOB RAT IOCs in Interactive Sandbox *Gather BTMOB RAT IOCs in ANY.RUN's Interactive Sandbox*

What is BTMOB RAT Malware?

BTMOB RAT represents a significant evolution in Android malware, emerging as one of the most sophisticated Remote Access Trojans targeting mobile devices in 2025. This advanced malware evolved from the SpySolr family and has rapidly gained notoriety for its comprehensive data theft capabilities, remote control features, and ability to bypass modern Android security measures. With over 15 variants identified since December 2024, BTMOB RAT poses a serious threat to both individual users and organizations worldwide. The malware operates as a comprehensive Remote Access Trojan specifically designed for Android platforms, leveraging the operating system's Accessibility Service to gain extensive control over infected devices. Unlike traditional mobile malware that focuses on single attack vectors, BTMOB RAT combines multiple techniques including credential theft, remote device control, banking fraud, and data exfiltration capabilities.

What sets BTMOB RAT apart from other mobile threats is its sophisticated use of overlay attacks, particularly targeting financial applications like Alipay. The latest version (v2.5) incorporates advanced obfuscation techniques and can perform real-time screen manipulation.

The malware is distributed through a Malware-as-a-Service (MaaS) model, with cybercriminals advertising lifetime licenses for $5,000 through Telegram channels. This commercial approach has accelerated its adoption among threat actors and contributed to its rapid evolution and widespread distribution.

BTMOB RAT infiltrates via social engineering, primarily phishing sites masquerading as legitimate apps like iNat TV (e.g., tvipguncelpro.com) or fake WhatsApp mods (e.g., WhatsApp GB). Users are tricked into sideloading APKs, which prompt enabling Accessibility Service—framed as necessary for "enhanced features."

Spread occurs through:

- **Phishing Campaigns**: URLs distributed on forums, SMS, or search-engine-indexed fake sites (e.g., Argentine tax agency clones).
- **App Stores and Mods**: Malicious apps on Google Play or third-party stores.
- **MaaS Distribution**: Developers promote via Telegram, enabling affiliates to customize and deploy.

Post-infection, it self-propagates by exfiltrating contacts for SMS phishing or using infected devices to host phishing pages. Geographic targeting, like Morocco's 2025 alerts, shows adaptation to local lures.

BTMOB RAT Malware Victimology

BTMOB RAT predominantly targets Android users in emerging markets with high mobile banking adoption, where digital financial services are rapidly growing but security awareness lags. In Morocco, it has been a focal point of national alerts, affecting smartphone users who enable accessibility features for convenience, leading to widespread banking data theft. Morocco ranks third in Africa for web-based threats, with over 12.6 million attack attempts in 2024, amplifying BTMOB's impact.

Globally, victims include casual users of streaming or mining apps, as well as financial app users in China (e.g., Alipay targets). Recent campaigns have hit Latin America, such as Argentina via fake government sites impersonating tax agencies. Over 500,000 installations of similar accessibility-abusing malware were recorded in 2024, suggesting BTMOB's victim pool could number in the tens of thousands by September 2025. Businesses in retail and finance are indirect victims through employee devices, but primary targets remain individual consumers vulnerable to phishing.

How BTMOB RAT Functions

The trojan operates through several sophisticated mechanisms:

Accessibility Service Abuse:

It exploits Android's Accessibility Service, originally designed to help users with disabilities, to gain broad system permissions and control over user interface elements.

Overlay Attacks:

BTMOB RAT creates transparent or semi-transparent overlays on legitimate applications, particularly banking and payment apps, to capture user credentials and sensitive information without detection.

Remote Administration:

The malware establishes persistent command and control (C&C) communication channels, allowing attackers to remotely execute commands, update malware components, and extract data in real-time.

Dynamic Code Loading:

Advanced variants can download and execute additional malicious modules, expanding their capabilities based on specific attack objectives.

Anti-Detection Techniques:

The malware employs multiple evasion techniques including code obfuscation, runtime application self-protection (RASP), and behavioral analysis evasion to avoid detection by security solutions.

Data Exfiltration:

Stolen information is encrypted and transmitted to attacker-controlled servers through various channels, including HTTPS connections to legitimate-looking domains.

BTMOB RAT Attack Example and Technical Analysis

A dynamic analysis of a BTMOB sample in ANY.RUN's Interactive Sandbox reveals key operating mechanisms and network activity of the malware.

View analysis


BTMOB RAT analysis in Interactive Sandbox *BTMOB RAT sample analysis in the Interactive Sandbox*

Network Activity and Encryption

Analysis of network traffic revealed the malware's attempts to establish a connection with the command and control (C&C) server via hxxx [://] ip/yaarsa/private/yarsap_80541 [.] php. A characteristic sequence of requests is observed: an initial HEAD request, followed by a repeated HEAD after a pause, which is part of the handshake connection establishment mechanism and server availability check.


BTMOB RAT network connection attempts *BTMOB RAT sample analysis in the Interactive Sandbox*

All commands and data are transmitted through an encrypted channel, which complicates analysis of the payload. To protect its configuration and the collected data, the malware actively uses cryptographic APIs.


BTMOB RAT uses encryption technique *Encryption technique used by BTMOB RAT*

Configuration File and Management

BTMOB RAT stores its configuration in the system SharedPreferences storage in XML format. The configuration file contains a complex map of boolean values, where each parameter defines the malware's functionality.

 BTMOB RAT configuration file in Interactive Sandbox *BTMOB RAT configuration file contents visible in Interactive Sandbox*

Persistence and Privilege Escalation Mechanisms

Aggressive permission acquisition appears to be the key attack vector. The malware doesn't simply request access but manipulates the interface using Input Injection to automatically press the "Allow" button.

 BTMOB RAT uses input injection *BTMOB RAT detected to use Input Injection technique*

Once access is obtained, it gains control over the device, including implementing the Prevent Application Removal mechanism, intercepting events in Android Settings to block its own uninstallation.

To ensure continuous operation, the malware creates a background service immediately after launch and uses WakeLock, preventing the device from entering sleep mode. Additionally, it checks the lock screen state, which increases its stealth.

Data Collection and Malicious Activity

Before performing its main tasks, the malware conducts comprehensive reconnaissance: collects a list of installed applications, analyzes running processes, and obtains system data. This allows the operator to adapt the attack to the specific device.

Important malicious activity is conducting overlay attacks. The malware overlays phishing windows on legitimate applications, primarily banking and cryptocurrency ones, to steal credentials, PIN codes, and two-factor authentication.

You can view the succession of the above-mentioned processes in ANY.RUN's Sandbox as a process tree with every behavior's description.

 BTMOB RAT's malicious processes *BTMOB RAT's malicious processes*

Get started today for free

Analyze malware and phishing in a fully-interactive sandbox

Create free account

Notable BTMOB RAT Attacks

While specific large-scale BTMOB attacks are still emerging due to its recent discovery, several notable patterns have been identified:

Streaming Service Impersonation Campaigns:

Multiple campaigns have been observed where attackers created sophisticated fake websites mimicking popular streaming platforms, leading to thousands of downloads before detection.

Cryptocurrency Mining Fraud:

Significant campaigns targeting cryptocurrency enthusiasts through fake mining applications have resulted in substantial financial losses and credential theft.

Alipay PIN Theft Operations:

Recent versions specifically targeting Alipay users have demonstrated the malware's evolution toward financial fraud, with overlay attacks successfully capturing payment credentials.

Corporate Device Compromises:

Several incidents have been reported where employee devices were compromised through entertainment-focused phishing, leading to broader organizational security concerns.

These examples demonstrate the malware's versatility and the threat actors' ability to adapt their tactics based on current trends and user interests.

Gathering Threat Intelligence on BTMOB RAT Malware

Threat intelligence plays a crucial role in defending against BTMOB RAT:

- **Proactive Threat Detection**: Intelligence feeds provide early warning indicators of new BTMOB RAT campaigns, enabling organizations to implement protective measures before attacks reach their environments.
- **Attribution and Campaign Tracking**: Threat intelligence helps identify the tactics, techniques, and procedures (TTPs) used by BTMOB RAT operators, enabling better prediction and prevention of future attacks.
- **Contextual Analysis**: Intelligence provides crucial context about BTMOB RAT variants, helping security teams understand the specific threats relevant to their organization and user base.
- **Predictive Security**: Advanced threat intelligence can help predict likely evolution paths for BTMOB RAT, enabling proactive security measure implementation.

Start gathering intelligence by searching BTMOB in ANY.RUN's Threat Intelligence Lookup. View the RAT's fresh sample analyses to understand TTPs and harvest IOCs:

threatName:"btmob"


BTMOB RAT's samples found via Threat Intelligence Lookup *BTMOB RAT's samples found via Threat Intelligence Lookup*

Threat Intelligence Lookup is available for free: collect indicators, browse sandbox detonations quick and easy.

Integrate ANY.RUN's threat intelligence solutions in your company

Contact us

Conclusion

BTMOB RAT remains a versatile and dangerous remote access Trojan capable of damaging both individuals and enterprises. Its modular architecture, stealthy operations, and adaptability make it a prime tool for cybercriminals and APT actors alike. Proactive defense powered by advanced detection, prevention strategies, and real-time threat intelligence is essential to reduce risks and prevent devastating breaches.

Sign up to use ANY.RUN's TI Lookup for free: gather fresh actionable threat intelligence for timely detection and response.
