



THREAT ADVISORY

StreamRat Android Trojan Compromises Devices Via Social Media Ads

PREPARED BY

Drona Cyber solutions Pvt Ltd

DATE OF ISSUE

September 7,2026

CLASSIFICATION MATRIX

TLP : GREEN

1. Executive Summary

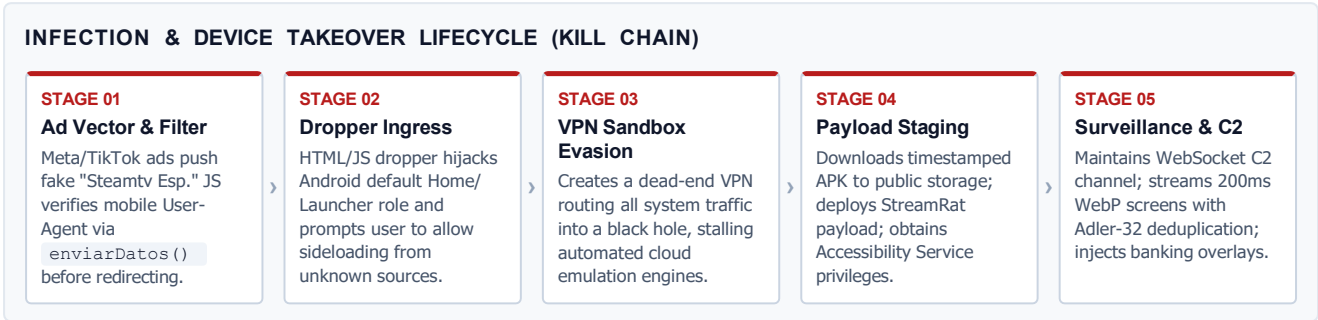
Drona Cyber Solutions has detected active dissemination of a highly sophisticated Android banking trojan tracked as **StreamRat**. Propagated through high-volume malvertising across Meta platforms (Facebook, Instagram) and TikTok under the promotional lure of "**SteamTV Esp.**", the malware targets Spanish-speaking users seeking gratis premium television streaming services.

The threat employs a multi-stage infection routine featuring an HTML/JS dropper lineage connected to historical *Mirax* banking campaigns. StreamRat achieves total device takeover by co-opting Android's Accessibility Services and the native MediaProjection framework. Crucially, it pioneers a novel sandbox evasion technique—initiating a localized non-functional VPN profile to temporarily sever internet egress and disrupt cloud automated sandboxes—prior to establishing WebSocket-driven remote access (RAT), Hidden VNC (HVNC), keylogging, dynamic HTML overlay injections, and automated UI node tree harvesting.

MALWARE FAMILY	StreamRat	CAMPAIGN ALIAS	SteamTV Esp.
MALWARE CLASSIFICATION	Android Banking Trojan / HVNC	PRIMARY VECTOR	Meta & TikTok Ad Campaigns
OPERATING MODEL	Malware-as-a-Service (MaaS)	TARGETED SECTOR	Banking, Financial Services & Insurance
GEOGRAPHIC SCOPE	Spain / Spanish-speaking Users	SEVERITY ASSESSMENT	CRITICAL (CVSS 8.8)
C2 PROTOCOL	WSS with Custom HTTP Headers	TOOLING OVERLAP	Shared Dropper Lineage with Mirax

2. Multi-Stage Compromise Lifecycle

The adversary executes a linear five-stage compromise workflow engineered to minimize user friction and evade automated behavioral telemetry:



3. Technical Analysis & Threat Mechanics

3.1 Initial Access, Fingerprinting & Launcher Hijacking

Victims clicking social media ads land on an adversary gateway executing `enviarDatos()`. The script validates that `navigator.userAgent` indicates an Android operating system, queries `api.ipify.org` to map user geography, and posts device details to `send_tg.php` to alert the actor's Telegram bot. Qualified targets receive `rledmi.html`, which instructs them how to enable installation from unknown sources.

Upon installation, the dropper prompts the user to grant default *Home Application (Launcher)* rights. Whenever the user attempts to navigate back using physical or gesture Home controls, Android routes directly back to the malware interface, effectively locking down device navigation.

Dead-End VPN Evasion: The dropper establishes a dummy VPN profile that acts as an intentional sinkhole. By routing all device egress through an unreachable interface while whitelisting only its own payload delivery threads, cloud dynamic sandboxes fail to detect outgoing malicious beacons and classify the file as benign.

3.2 Dual-Engine Screen Surveillance (VNC vs. HVNC)

Following sandbox evasion, the dropper downloads `update_{timestamp}.apk` to external public storage and completes installation via Android's session installer. Once initialized, the trojan revokes the dummy VPN, unregisters itself as launcher, and connects to its command server via encrypted WebSockets (WSS) using custom identity headers (`X-Device-Id` , `X-Device-Model` , `X-API-Level`).

Standard MediaProjection VNC

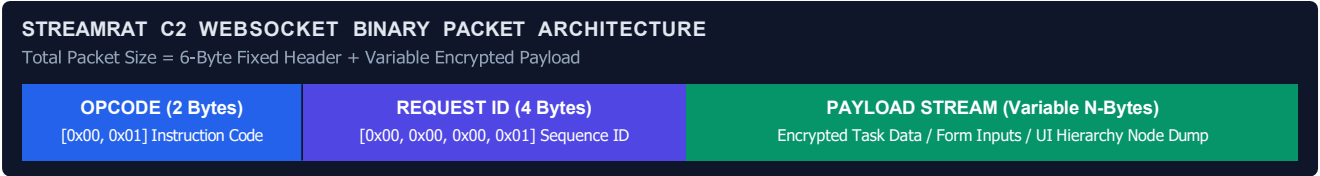
High Fidelity

Streams real-time raw frame buffers via Android's MediaProjection API for live operator control. System permission dialogues are automatically bypassed by injecting Accessibility clicks.

Covert Accessibility HVNC

Stealth Mode

Captures frames via `takeScreenshot()` every 200ms. Images are scaled to 35%, compressed to WebP at 40% quality, and deduplicated using **Adler-32 checksums** to eliminate identical frames.



3.3 Dynamic Overlay Injection & MaaS Platform Architecture

StreamRat utilizes two distinct overlay techniques to execute credential theft:

- Automatic Overlays:** Triggered when targeted banking applications enter the foreground. The bot queries the C2 via `maintenance_check` and `injection_check` , rendering HTML spoof forms via a local WebView to harvest online banking credentials.
- Immediate Overlays:** Displays black screens or fake "System Firmware Update" views to mask active background interactions executed through Accessibility APIs.

Infrastructure inspection reveals a dedicated management panel supporting three administrative tiers: *User* (operator), *Supervisor* (affiliate manager), and *Admin* (core author). Independent builders for droppers and payloads confirm StreamRat operates as a commercial Malware-as-a-Service (MaaS).

4. MITRE ATT&CK® Enterprise Matrix

TACTIC	TECHNIQUE ID	CONTEXTUAL APPLICATION IN STREAMRAT
Initial Access	T1566.002 / T1204.001	Spearphishing links distributed through sponsored social media advertisements on Meta and TikTok platforms.
Execution	T1059.007	Client-side JavaScript fingerprinting via <code>enviarDatos()</code> and IP verification on phishing landing pages.
Defense Evasion	T1562.001 / T1036.005	Disables network analysis via dummy VPN sinkhole; masquerades as "SteamTV Esp." entertainment utility.
Credential Access	T1056.001	Keylogging and financial credential harvesting via targeted HTML WebView overlays.
Collection	T1113 / T1115	Automated 200ms WebP screen captures and system clipboard monitoring.
Command & Control	T1071.001 / T1105	Bidirectional WebSocket (WSS) communications and session-based payload ingress transfer.
Exfiltration	T1041	Exfiltration of collected credentials, OTP tokens, and serialized UI hierarchy trees over C2.

THREAT ADVISORY: STREAMRAT ANDROID TROJAN

5. Indicators of Compromise (IOCs)

INDICATOR TYPE	OBSERVABLE VALUE	CLASSIFICATION / THREAT CONTEXT
IPv4 Address	45[.]147[.]28[.]59	StreamRat C2 WebSocket Server Node
IPv4 Address	193[.]32[.]2[.]245	Malicious Phishing & Dropper Hosting
File Hash (SHA-256)	e0714788b4e2518b0d9d4cbf18c7217bb97718e01689d77338f1cc4a230fcb6c	StreamRat HTML/JS Multi-Stage Dropper APK

INDICATOR TYPE	OBSERVABLE VALUE	CLASSIFICATION / THREAT CONTEXT
File Hash (SHA-256)	ba83cc3c9535690191018edf73ca5c6001609df9919462796aa2e551f142e4d3	StreamRat Core Android Banking Payload APK
Intelligence Source	threatfabric.com/blogs/...uncovering-streamrat	Primary Threat Research Telemetry Dossier

6. Strategic & Tactical Defense Recommendations

- Enforce Mobile Threat Defense (MTD) & Sandbox Evasion Detection**
Deploy enterprise MTD profiles capable of identifying unauthorized local VPN creations and immediately alerting administrators if unmanaged applications request Accessibility Service authorization.
- Perimeter Filtering & Network-Level IOC Ingestion**
Ingest identified C2 and staging IP addresses (45.147.28.59 , 193.32.2.245) into corporate firewalls, secure web gateways (SWG), and DNS sinkholes to intercept inbound and outbound traffic.
- Hardening BFSI Applications with Advanced RASP Controls**
Financial institutions should implement Runtime Application Self-Protection (RASP) with FLAG_SECURE to prevent screen streaming and detect active Accessibility overlays before accepting authentication credentials.
- Targeted Security Awareness on Sideloaded & Launcher Prompts**
Educate staff and consumers on mobile phishing lures offering gratis streaming entertainment, emphasizing that banking apps should never require setting third-party apps as the default Android Launcher.
- Periodic Audit of High-Privilege Mobile Authorizations**
Conduct regular security reviews on enterprise-enrolled Android endpoints to revoke dormant app permissions and eliminate software that requests unneeded Device Administrator or Accessibility privileges.

7. Conclusion & Analytical Outlook

StreamRat demonstrates the continuing professionalization of mobile threat actors. By leveraging commercial ad networks for precise regional targeting, employing dead-end VPN tunnels to defeat dynamic analysis, and engineering sub-200ms WebP frame transmission with Adler-32 deduplication, the operators have established a highly efficient, scalable Malware-as-a-Service model. Organizations operating within BFSI and mobile-centric sectors must anticipate further convergence between sophisticated evasion techniques and high-velocity social engineering lures.



**Securing Today,
Empowering Tomorrow**



Drona Cyber Sloutions



info@dronacybersolutions.com



+91 81609 68270



www.dronacybersolutions.com