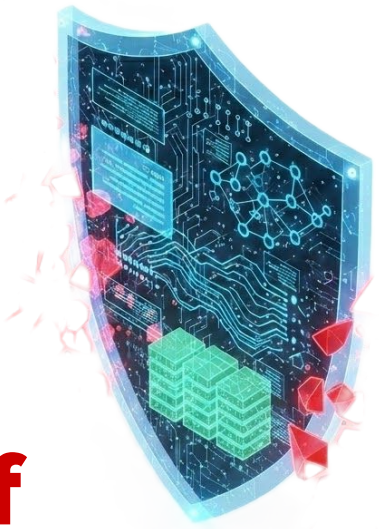
Report | April 2026



FEMITBOT: Abuse of Telegram Mini Apps for Large-Scale Fraud Campaigns

Analysis by CTM360

CTM360®

Industry	Country	Region
All	Global	Global

Overview:

Telegram Mini Apps are lightweight web applications within Telegram that enable seamless login, payments, and interaction. These features are increasingly abused to create convincing fraudulent environments.

CTM360 has identified a malicious infrastructure named **FEMITBOT,** which leverages the Telegram Mini App model to operate and scale multiple fraud campaigns globally. Various fraudulent scam cases were identified using FEMITBOT kit, where the fake telegram mini apps were pretending to be one of the following:

- Fake cryptocurrency platforms
- Illegal streaming service
- Fake Financial apps
- Fake AI platforms

Our analysis of multiple domains and Telegram MIni Apps associated with the FEMITBOT kit revealed a consistent API response containing the message **“Welcome to join the FEMITBOT platform.”** This recurring response across distinct domains indicates that they were all leveraging the same underlying FEMITBOT backend, linking the infrastructure together.

```
"data": {
  "content": "<p>Welcome to join the FEMITBOT platform</p>"
},
"msg": "ok"
```

In addition, Threat actors leveraging the **FEMITBOT kit** utilize Meta (Facebook/Instagram) pixels as a tracking mechanism to monitor user activity, measure engagement and optimize campaign performance in real time.

This analysis is based on CTM360’s previously documented **TRAP10 Mini App scam**, which outlines the abuse of Telegram Mini Apps for fraudulent, monetization-driven campaigns.

FEMITBOT KIT

CTM360 identified multiple scam campaigns leveraging the Telegram Mini Apps built on the **FEMITBOT kit infrastructure**, many of which **impersonate globally recognized brands such as BBC, Netflix, Binance, and Youku**. These brands are used to establish a false sense of legitimacy, increase user trust, and drive higher engagement across fraudulent workflows.

Streaming & Media	Crypto	AI & Computing	Financial Services	Mining Pools
BBC, Netflix, ABEMA, Youku, WeTV, CLARO	Bitget, OKX, Binance, Fragment, MoonPay	NVIDIA, CoreWeave, MetaPivot, AiLoop	StraitsX, Circle, Trade Exchange	SunDog, MiningDOGE, BTC Pool, Orepoo

Infrastructure Correlation Between Telegram Bots and Phishing Domains

Analysis of the campaigns reveals consistent linkage between Telegram bots and their associated phishing websites, demonstrating how the Telegram Mini App interface is directly connected to the underlying phishing and fraud infrastructure.

Each bot operates as a front-facing interaction layer, while the associated domain handles core backend functions such as user authentication, content delivery, payment processing, and data collection. This tight integration highlights a modular and reusable architecture, where multiple bots can be deployed using similar backend logic with minor variations in branding or theme.

Domains (Examples)	Telegram Bots (Examples)
zerocap[.]vip	@Zerocap01_bot
spiderpool[.]app	@SpiderPool01_bot
btcaimining[.]xyz	@AiSuperBtc
btcpoolok[.]cloud	@AiSuperBtcVIP01
cineotv[.]one	@BBC_Serve

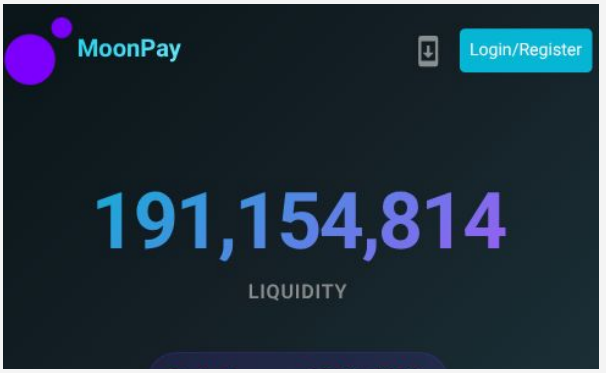
Note:
Additional use cases may exist beyond those identified. The observed campaigns are built on the FEMITBOT infrastructure, indicating a scalable framework capable of supporting further variants and themes.

Scam Use Cases

Fake websites impersonating various organization in multiple industries were identified on these malicious telegram mini app

Streaming & Media

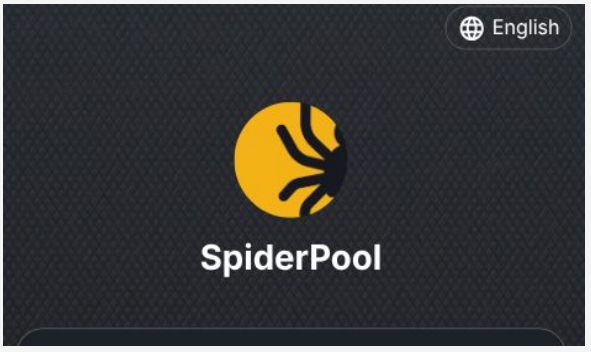
Crypto



AI & Computing

Financial Service

Crypto Mining Pool



Victim Flow

Phishing websites leveraging Telegram Mini Apps follow a **standardized** escalation model designed to build trust, gamify progress, and extract maximum financial value.

01

PRE-ACQUISITION

Luring & Social Engineering

Victims targeted via Meta Ads (Facebook/Instagram), or unsolicited Telegram invites promoting 'Passive Income'

02

ACQUISITION

Bot Interaction and a 'Launch App' button triggering

Target starts Telegram bot. Bot responds with customized welcome messahe Mini App environment.

03

ENTRY

Host Handshake & Exfiltration

The Telegram.WebApp.initData string (user ID, name, auth hash) is silently extracted and prepared for secondary auth flow.

04

Templates

Infrastructure Binding

Vue.js client calls /api/public/init. Receives 'skin_no' and 'setting' flags to render the correct brand impersonation (Netflix vs. BTC Mining skin).

05

AUTH

Session Hijacking

Client submits initData to /api/public/telegramLogin. Server issues a JWT (Gq cookie) with 10-day validity. Victim authenticated without entering a password.

06

ENGAGEMENT

Artificial Yield Generation

Dashboard displays fake 'Real-time Earnings'. Psychological pressure via 'Mining Speed' countdowns or 'Limited VIP Slots'.

07

QUALIFICATION

The 'Activation' Trap

To 'withdraw' fake earnings, victim is prompted to 'Activate' their account via a small initial deposit or by completing social tasks (inviting friends).

Modular Mini App Infrastructure - FEMITBOT

The identified infrastructure represents a modular ecosystem designed to support large-scale abuse operations through Telegram Mini Apps. Rather than relying on standalone setups, the platform operates on a template-driven, enabling rapid deployment and reuse across multiple campaigns.

Infrastructure Mapping

The observed infrastructure follows a structured and modular architecture, centered around Telegram bots and interconnected components that enable seamless deployment and operation of scam campaigns across Mini Apps and associated web infrastructure.

Frontend Layer

- Vue.js single-page application
- index-[HASH].js bundle
- Telegram WebApp SDK integrated
- Axios HTTP client with interceptor
- 15 skin variants (skin_no 1–15)
- 22+ pattern sub-variants
- 21+ theme color palettes
- Support for 22+ languages

API & Authentication

- /api/public/init — public endpoint
- Cookie-based JWT (js-cookie library)
- Bearer token on every request
- Telegram initData HMAC-SHA256 authentication
- Auto-login flow (tg_auto_login)
- Invitation code gating per operator

Operator Kit

- Unique API domain per deployment
- Tailored frontend skin + brand assets
- Dedicated Telegram bot configuration
- 5 crypto deposit networks supported
- MLM referral pyramid (up to 6 levels)
- Meta & TikTok pixel integration
- Android APK distribution
- Cloudflare CDN for origin masking

⚠️ **/api/public/init — Only unauthenticated endpoint. Returns full config: skin, registration, feature flags, malware URLs, tracking pixels — no auth required.**

FEMITBOT KIT Analysis

CTM360 conducted an analysis of the FEMITBOT kit and its associated infrastructure, examining backend responses, Telegram bot linkages, and frontend deployment patterns, and identified the following:

60+
Active Domains
Responding with valid JSON

146+
Telegram Bots
Incliding groups and channels

15+
Templates
Visual theme configuration

25+
JS Bundles
Visual theme configuration

100+
Pixel IDs
Meta conversion tracking

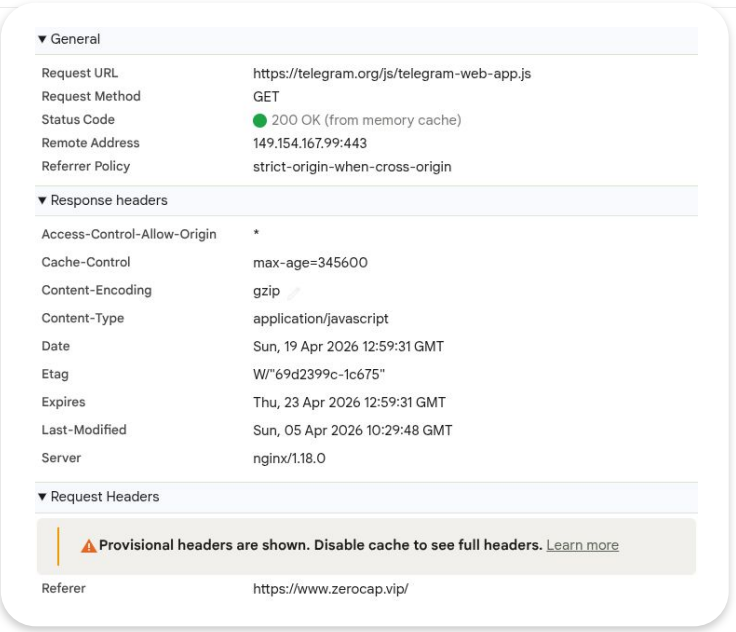
30+
Impersonated Brands
Brand Impersonation

Technical Infrastructure - FEMITBOT

WebView Integration and Trust Exploitation

The phishing site's HTML explicitly loads the Telegram WebApp SDK via a script tag in the document head src="https://telegram.org/js/telegram-web-app.js, which is the standard method for integrating with Telegram's Mini App framework.

This script allows the website to communicate with the Telegram app. When a user opens the Mini App through a bot, Telegram automatically opens the attacker's website inside an in-app browser (WebView), making it look like part of Telegram.

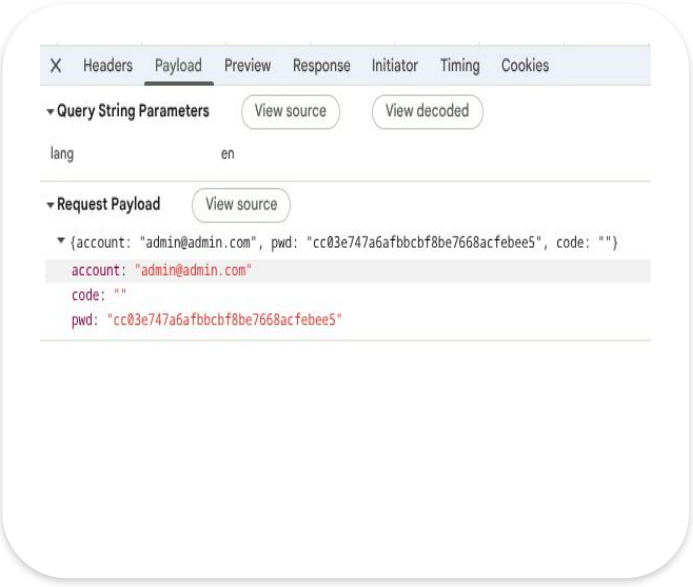


initData Authentication Flow

The Telegram WebApp SDK sends a piece of data (initData) that includes user details, a timestamp, and a secure signature.

The signature (hash) acts like a verification stamp. The server can use the bot's token to check this stamp and confirm that:

- The data really came from Telegram, and
- It hasn't been modified or tampered with.



Technical Infrastructure - FEMITBOT

Tracking Pixel Infrastructure

The observed infrastructure integrates conversion tracking mechanisms from Meta Platforms (Facebook/Instagram) and TikTok within its operations. These tracking pixels are triggered on key user interaction events, including account registration, initial deposit (mapped to “Purchase” events), subsequent deposits (custom “rePurchase” events), and other engagement milestones.

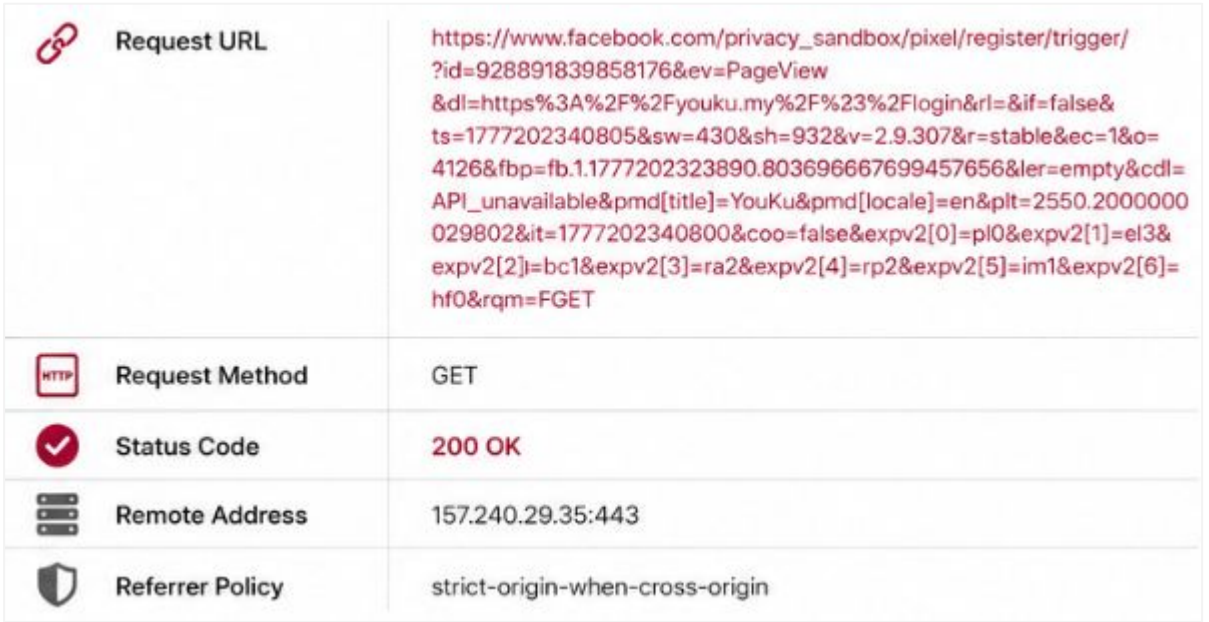
The systematic use of these technologies reflects a high level of operational maturity. Threat actors leverage digital marketing analytics to monitor user behavior, assess campaign performance, and optimize conversion funnels, enabling them to dynamically refine lures, adjust strategies, and allocate resources across multiple traffic sources to maximize returns.

Facebook Pixel Analysis

During analysis, a request was observed to the following endpoint:

- https://www.facebook.com/privacy_sandbox/pixel/register/trigger/

This request is associated with Meta (Facebook) Pixel tracking, specifically a PageView event, indicating that user activity on the page is being monitored and transmitted to Meta’s tracking infrastructure.



Request URL	https://www.facebook.com/privacy_sandbox/pixel/register/trigger/?id=928891839858176&ev=PageView&dl=https%3A%2F%2Fyouku.my%2F%23%2Flogin&rl=&if=false&ts=1777202340805&sw=430&sh=932&v=2.9.307&r=stable&ec=1&o=4126&fbp=fb.1.1777202323890.803696667699457656&ler=empty&cdl=API_unavailable&pmd[title]=YouKu&pmd[locale]=en&plt=2550.2000000029802&it=1777202340800&coo=false&expv2[0]=pl0&expv2[1]=el3&expv2[2]=bc1&expv2[3]=ra2&expv2[4]=rp2&expv2[5]=im1&expv2[6]=hf0&rqm=FGET
Request Method	GET
Status Code	200 OK
Remote Address	157.240.29.35:443
Referrer Policy	strict-origin-when-cross-origin

Malware Distrubution - FEMITBOT

The identified websites were observed to include a feature flag (app_download_show_switch) that, when enabled, facilitates the distribution of malicious payloads. In such cases, the sites provide Android APK files intended for sideloading onto victim devices. **Some examples are provided below.**

Android APK Distribution

The APK filenames are carefully chosen to resemble legitimate applications or use random-looking names that don't immediately trigger suspicion. The APKs are hosted on the same domain as the API, ensuring TLS certificate validity and avoiding mixed-content warnings in the browser.

The setting configuration includes android_app_type fields that control how the malware is delivered:

- **Type 1 (Direct download):**
  - The user clicks a button and the app file (APK) downloads immediately, like downloading a file from a website.
- **Type 2 (In-app browser):**
  - Instead of opening Chrome or Safari, the page opens inside the app itself, making it feel safer and more trusted while guiding the user to install or interact.
- **Type 3 (PWA prompt):**
  - The user sees a pop-up asking to “Add to Home Screen,” making the malicious site look like a normal app without needing a full download.

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence. CTM360 operates as an external CTEM technology platform outside an organization's perimeter. Seamless and turnkey, CTM360 requires no configuration, installation, or end-user input, with all data pre-populated and specific to your organization. All aspects are managed by CTM360.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

CTM360®