

Report | May 2026



FIFA World Cup 2026

Scams Surge as Fraud Networks Target Fans Worldwide

Analysis by CTM360



INDUSTRY
SportCOUNTRY
AllREGION
GlobalDATE
May, 2026

Key Findings



7,000+

FIFA World Cup 2026
themed domains
identified

1,000+

Malicious websites
have already been
activated

1,000+

Social media
impersonation accounts
observed across major
platforms

4,500+

Themed domains
registered in just the
last five months,
showing a sharp
pre-tournament surge

Observed Scams

Fake tickets, betting, and
streaming scams
consisting of bogus
platforms that may also
spread malware
applications to users

Overview

With the **FIFA World Cup 2026** set to begin on 11 June, **CTM360's** latest research reveals a sharp rise in digital fraud infrastructure targeting fans globally, as scammers continue building and activating a global fraud ecosystem around **fake tickets, streaming platforms, gambling and betting platforms, and social media impersonation campaigns**. With less than a month until the tournament kicks off, threat actors are increasingly leveraging lookalike domains, launching fraudulent websites, and amplifying scams through impersonation accounts across major social media platforms, all designed to exploit rising fan interest and urgency ahead of the event.

CTM360 identified more than **7,000 FIFA World Cup 2026-themed domains**, including over **4,500** newly registered themed domains observed in just the **last five months**, indicating a sharp rise in opportunistic and potentially malicious online activity as the tournament approaches closer. Of these, over **1,000 confirmed malicious or fraudulent websites** have already been activated, primarily leveraging fake ticketing platforms, deceptive streaming services, fraudulent betting and gambling schemes, and misleading promotional campaigns designed to target unsuspecting fans.

In addition, over **1,000 social media impersonation accounts** were identified across major platforms. These accounts use fake profiles, unauthorized branding, and deceptive promotional content to amplify scam operations and engage users seeking match tickets, streaming access, or tournament-related offers.

Observed Fraud & Scam Activities



Fake Ticket Sales & Hospitality Scams

Fraudulent sites offer fake match tickets, VIP packages, and hospitality experiences to steal payments and personal data.



Streaming Scams

Malicious platforms or mobile applications that promise free, early, or exclusive match streams, then trick them into giving personal information through fake subscriptions or malware downloads.



Fake Betting & Gambling Platforms

Scammers run fake betting sites and apps to steal deposits, harvest financial data, or manipulate outcomes through fraud.



Social Media Impersonation

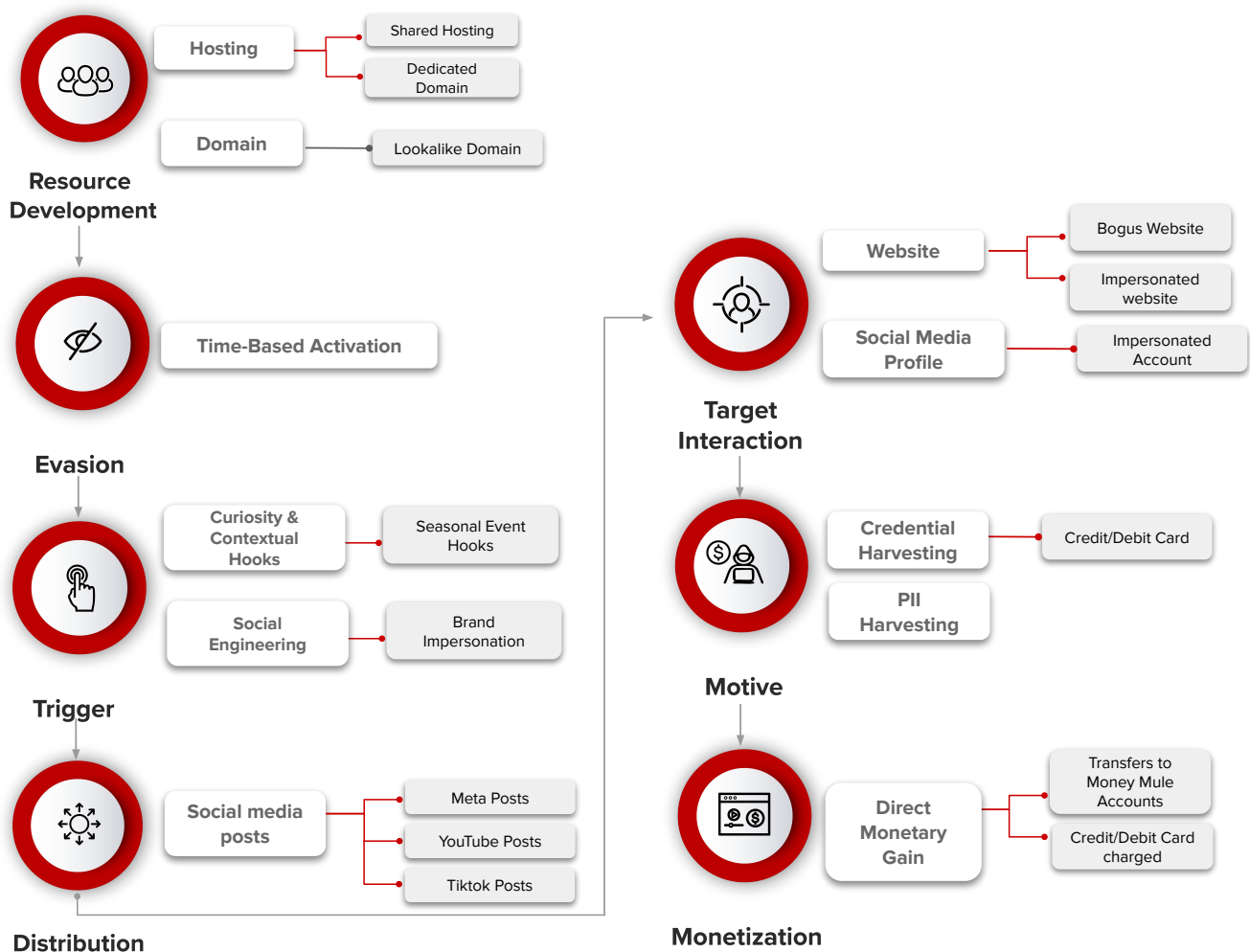
Fake accounts impersonate FIFA World Cup 2026 to promote scams and redirect users to malicious links.

FRAUD STAGES:

CTM360 Fraud Navigator

CTM360 Fraud Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the fraud. Fraud Navigator is a tool that categorizes common fraud techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies seven key stages in a fraud: resource development, evasion, trigger, distribution, target interaction, motive, and monetization. There are commonly 2 phases in the fraud, represented as Phase 1 (in white) & Phase 2 (in grey).

The Fraud Navigator framework has been mapped below to show how it aligns with each stage of the newly identified fraud variants. This highlights how the fraud evolved across both phases and how the campaign leveraged the FIFA World Cup theme to increase legitimacy, attract victims, and support social engineering efforts.



*Fraud Navigator Framework - FIFA WORLD CUP 2026 -
GLOBAL SCAM*

CTM360 Observations

2000+

fraudulent websites and social media accounts have been identified across platforms, with numbers **expected to increase** in the coming days.

Resource Development

Scammers rapidly deploy lookalike domains and simple, rapidly-built websites themed around the **FIFA World Cup 2026**, focusing on fake ticket sales and live streaming access. These sites mimic official FIFA platform and use urgency-driven messages like "Official FIFA World Cup 2026 tickets limited availability secure yours now." or "watch live now" to push users into quick payments or data entry on fraudulent pages.

On social media, attackers use low-activity or fake profiles to engage directly with users interested in tickets or streaming. Conversations are handled within the platform itself, where scammers impersonate sellers, negotiate prices, and request payments through multiple channels such as bank transfers, PayPal, and cryptocurrency, gradually guiding victims into completing fraudulent transactions.



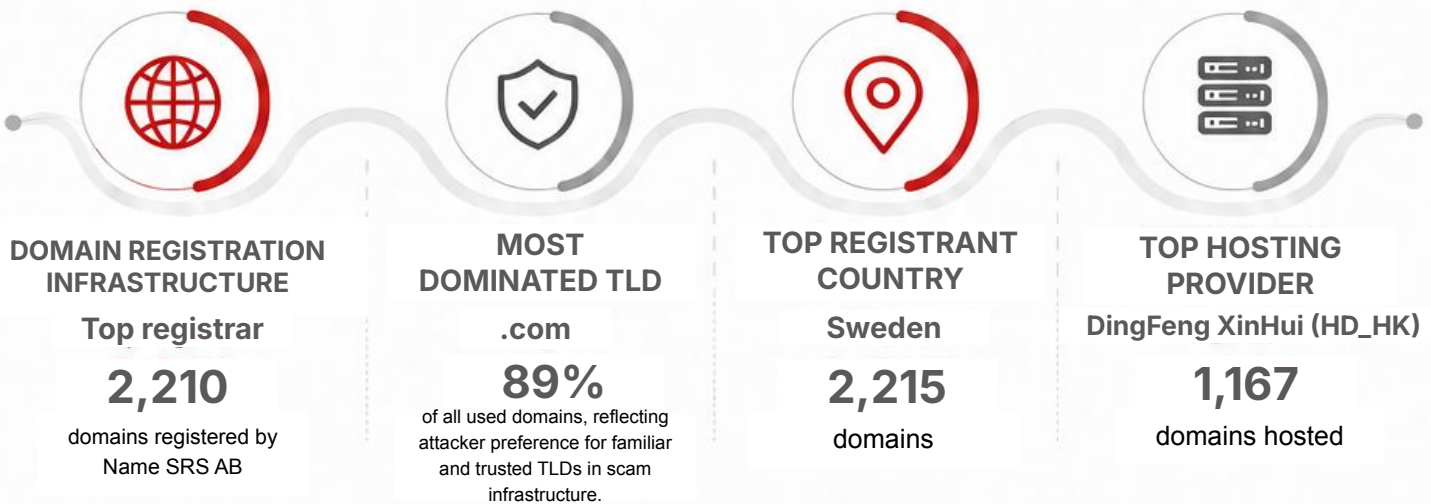
Trigger and Distribution

Scammers exploit high demand for **FIFA World Cup 2026 tickets and live streaming** by initiating direct engagement with users through social platforms and deceptive listings. The interaction is structured to build trust gradually, presenting itself as a legitimate opportunity to secure limited access or discounted tickets.

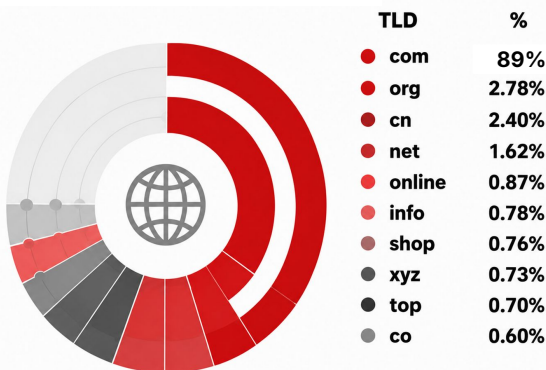
- **Social Media Profiles:** Fraudulent profiles circulates across social platforms promoting early ticket access, VIP packages, or free streaming platforms and mobile applications, often using FIFA branding, team logos, and host city references to appear legitimate.
- **Engagement Stage:** Users are engaged directly within social platforms or on fake contact channels where scammers respond as "sellers," discussing ticket availability, pricing, and match access in real-time conversations to build trust.
- **Fake Ticket / Streaming Platforms:** Victims are directed to counterfeit FIFA-themed websites that simulate official ticket booking or live streaming services, complete with fake seat selection, payment pages, and confirmation screens.

Technical Infrastructure Behind FIFA World Cup 2026 Lookalike Domain Registrations

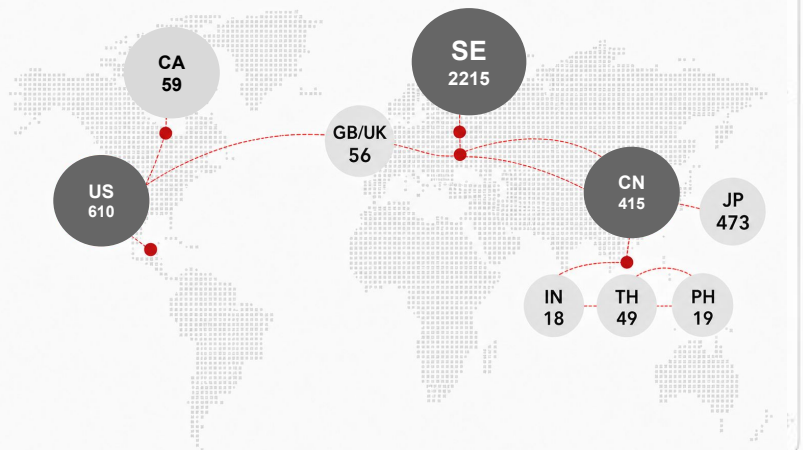
Infrastructure analysis of over **7,000+** domains associated with FIFA World Cup 2026 lookalike registrations reveals clear patterns across domain registrars, TLD usage, registrant locations, and hosting providers leveraged to deploy fraudulent and malicious web infrastructure.



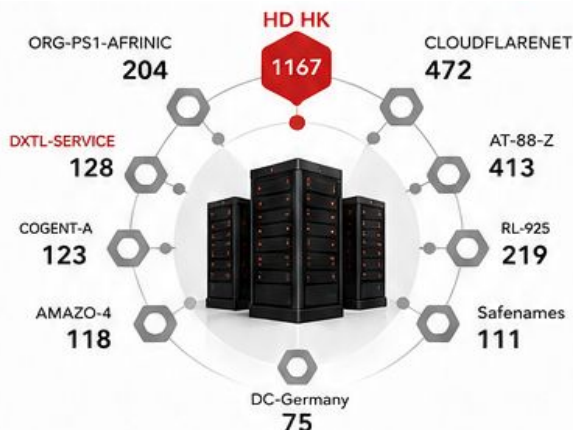
TLD USAGE DISTRIBUTION



TOP REGISTRANT COUNTRY DISTRIBUTION



TOP HOSTING INFRASTRUCTURE (ASN OVERVIEW)



TOP REGISTRAR DISTRIBUTION

Registrar	Count
Name SRS AB	2210
TuringSign Inc. d/b/a Cosmotown	686
GMO Internet, Inc.	473
GoDaddy.com, LLC	426
Gname.com Pte. Ltd.	323
Spaceship, Inc.	153
Metaregistrar BV	147
COSMOTOWN, INC.	127
NAMECHEAP INC	125
Web Commerce Communications Limited	79
Dynadot Inc	67

KEY TAKEAWAY



Attackers heavily rely on a small set of registrars, budget TLDs, and bulletproof hosting providers to scale phishing and impersonation campaigns around global events like FIFA World Cup 2026.



FIFA World Cup 2026 Themed Domains - IP to Domain Pattern Analysis

Overview

Analysis of top IP addresses hosting FIFA World Cup 2026 themed domains. The domains follow consistent patterns focused on ticketing, accommodation, travel, city targeting, fan engagement and event services.

Key Observations

Multiple IP addresses host large volumes of FIFA World Cup 2026 related domains.

Domains are highly consistent in pattern and theme across different IPs.

Common focus areas include: ticketing, hotels/apartments, travel, city targeting, fan engagement, live scores, guides, merchandise and event services.

City-specific targeting observed across host countries (USA, Canada, Mexico).

Top IPs Hosting FIFA World Cup 2026 Themed Domains

IP ADDRESS	DOMAIN PATTERN/CATEGORY	EXAMPLE DOMAINS (SAMPLE)
 3.33.130.190	 Accommodation, Hotels, Apartments & City Targeting	 - fifaworldcup2026apartments.com 2026fifaworldcupnewyork.com - welcometomexicofifaworldcup2026.com - fifaworldcup2026miamiapartments.com - fifaworldcup2026dallashotels.com
 15.197.148.33	 Ticketing, Hotels, Event Access & Festival Services	 - fifaworldcup2026tickets.com - fifaworldcup2026bostonhotels.com - fifaworldcupfestival.com 2026fifaworldcupnewjersey.org 2026fifaworldcupmerch.com
 13.248.243.5	 City Experience, Apps, Fan Engagement	 - fifaworldcupatlanta2026.com - fifaworldcupexperience.com - worldcupfan2026.com - metaworldcupsoccer.com - worldcupchat.com
 76.223.105.230	 Travel, Accommodation, Match Experience	 - fifaworldcup2026housing.com - fifaworldcuplivematchtoday.com - worldcupstayusa.com - fifaworldcup2026sanfran.com - worldcupvipsservices.com
 76.223.54.146	 Official-style Domains, Ticketing & Travel Services	 - usafifaworldcup2026.com - worldcupcanada26.com - worldcup2026travels.com - mexicofifaworldcup2026.com - fifaworldcupcanada2026.com
 13.248.169.48	 Tickets, Jerseys, Merch, Tournament Commercialization	 2026fifaworldcupshirts.com - buyworldcup2026tickets.info - cheapworldcup2026tickets.info - cheapworldcup2026tickets.com 2026fifaworldcupshirts.co
 2.57.91.91	 Travel, Tickets, Booking & Scheduling	 - fifaworldcuptickets.org - worldcuptravelpackages.com - worldcup2026bookings.com - worldcup26tickets.org 2026fifaworldcup.live

Legend



IP Address



Domain Pattern/Category



Example Domains (Sample)

--- Association

Summary



Multiple IPs are associated with large volumes of FIFA World Cup 2026 themed domains.



Domains follow consistent patterns including ticketing, accommodation, travel, city targeting, fan engagement and event services.



These domains pose risk of phishing, fraud, scams, misinformation and brand abuse targeting football fans worldwide.

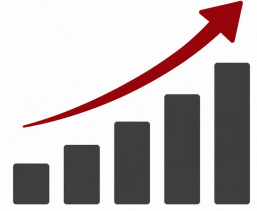
FIFA World Cup 2026 Themed Fraudulent Domains - Registration Surge Analysis



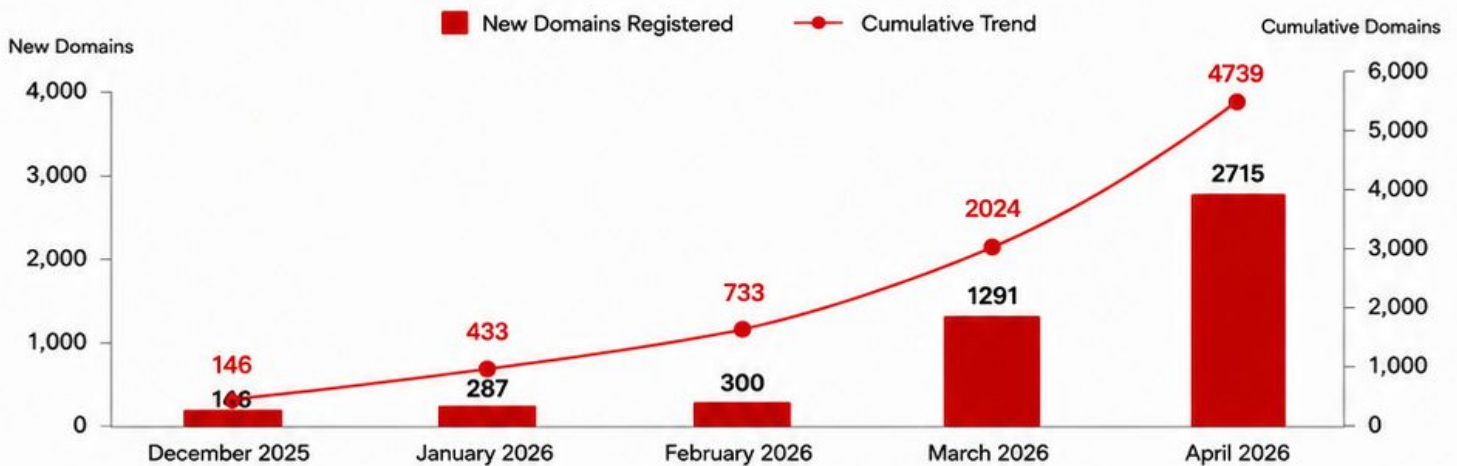
Real-Time Surge Alert

4500+

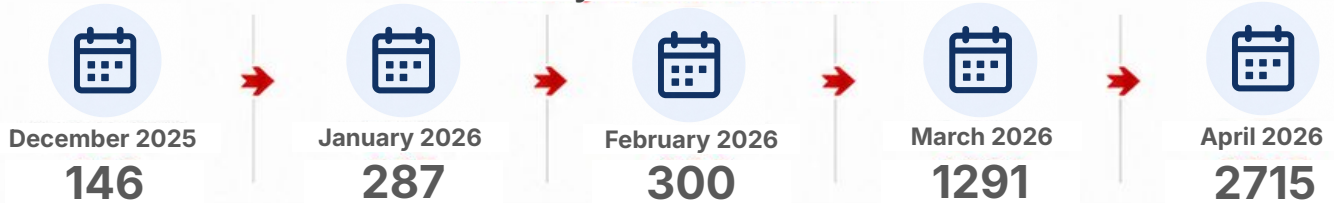
New Domains Registered
in Last 5 Months



Last 5 Months Registration Trend



Monthly Growth Breakdown



As the FIFA World Cup 2026 approaches, the number of themed fraudulent domains being registered continues to increase steadily.

Why This Matters



Global Impact

Attackers are exploiting the global excitement around FIFA World Cup 2026 to launch large-scale domain campaigns



Fan Targeting

Domains are crafted to target fans looking for tickets, travel, accommodation, merchandise and event information.



High-Risk Tactics

Lookalike domains, typosquatting and brand impersonation are being used to steal data and financial information.

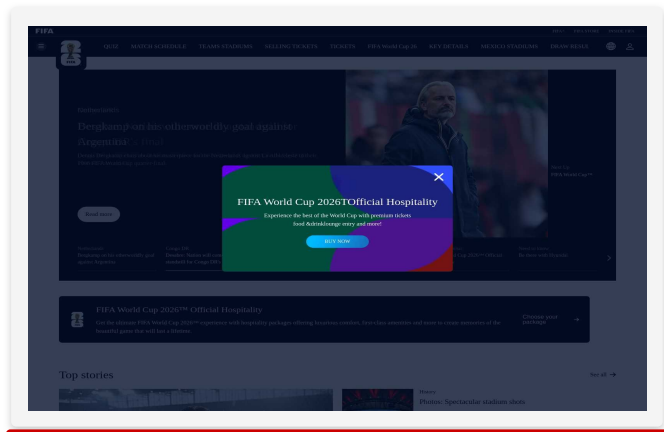


Act Now

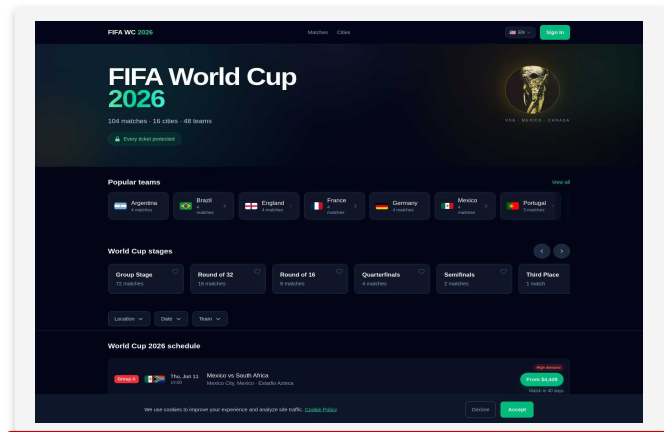
Organizations and fans must stay vigilant, verify domains and report suspicious activity immediately.

FIFA World Cup 2026-Themed Fraudulent Sites Templates

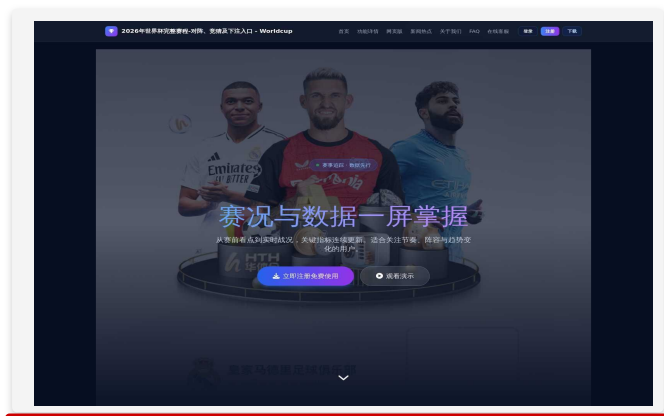
The screenshots below illustrate sample FIFA World Cup 2026-themed fraudulent **campaigns**, including fake ticket sales, deceptive streaming platforms, unauthorized betting and gambling websites, and promotional scams used to exploit fans and conduct online fraud under the guise of the tournament.



Ticket Scam



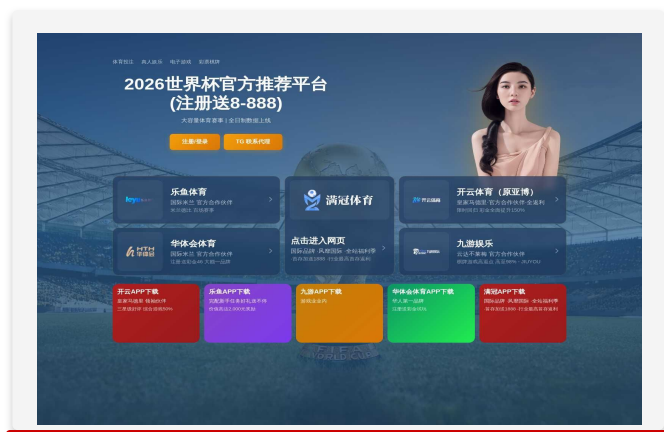
Ticket Scam



Streaming Scam (Bogus Website)



Streaming Scam (Malware Application)



Betting Scam



Betting Scam

FIFA World Cup 2026 – Streaming Scam: BTMOB Android Malware Campaign

Overview

CTM360 has identified a live streaming scam targeting fans searching for free or premium live streaming of FIFA World Cup 2026 matches. The scam uses fraudulent streaming websites to distribute malicious Android APKs powered by BTMOB (BeatBanker overlap) RAT and mining capabilities.

Although limited in scale at the moment, as the event is set to begin on June 11, the numbers are expected to increase significantly.

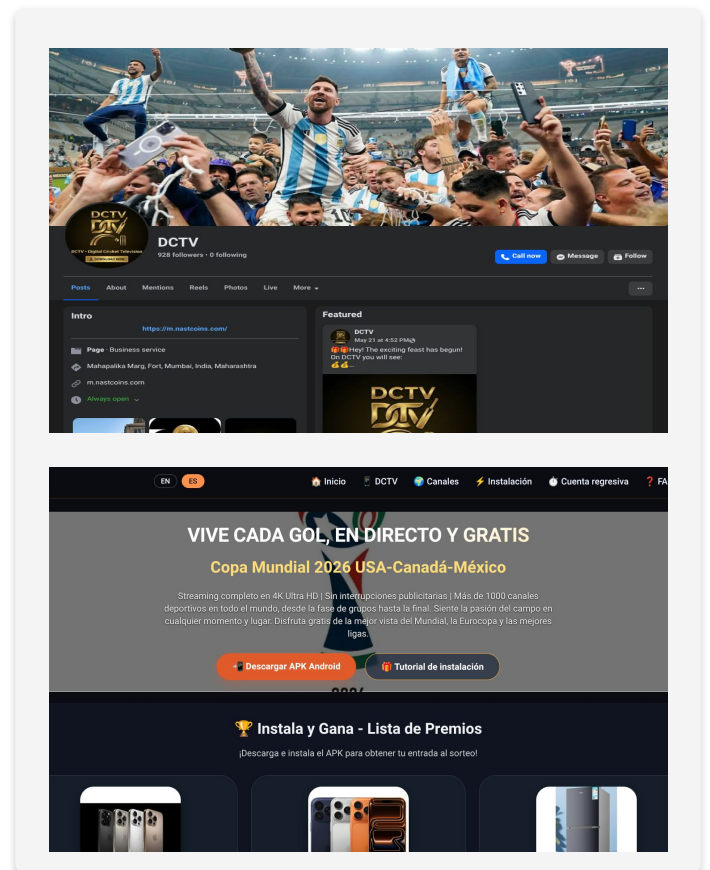
Campaign

Context

This malware campaign has been observed worldwide, masquerading as repackaged notes and IPTV-style Android applications that deliver remote access and crypto-mining capabilities. FIFA is one of the brands being targeted through a World Cup 2026 live-streaming theme designed to lure users seeking free or premium match access by exploiting sports enthusiasm and urgency.

Distribution Channels

- Meta ads & Fake Social Media Profiles
- Malicious APK promoted as streaming app/download



Malware Type

BTMOB is an Android RAT and crypto-mining malware that is often disguised as a legitimate notes or IPTV-style application.

Threat Actors Motive

The threat actors behind BTMOB are primarily motivated by financial gain through data theft and crypto-mining. Their activities include credential theft, OTP interception, user surveillance, and hijacking device resources for cryptocurrency mining.

Threat Actor Intent and Financial Motivation

Financial Gain: Scammers exploit the high global demand for FIFA World Cup tickets by creating fraudulent ticketing platforms, fake resale pages, and impersonating official ticket vendors to maximize financial profits and data collection.

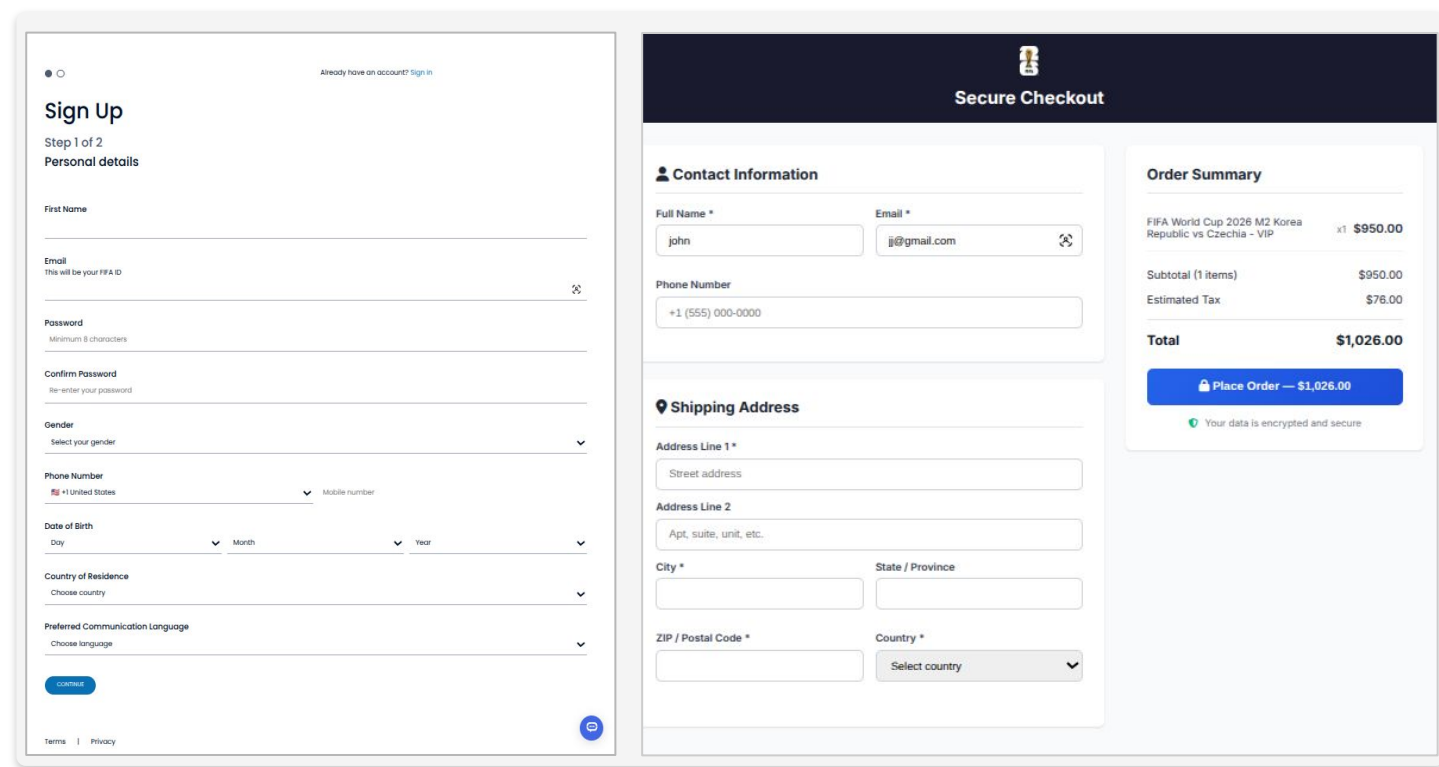
They set up convincing fake FIFA World Cup ticket portals and circulate urgent promotions through social media advertisements, or messaging applications, often referencing limited ticket availability, exclusive presales, or last-minute ticket releases. Victims are tricked into submitting personal information or making payments for non-existent tickets, resulting in direct financial loss. In many cases, scammers also:

- Operate across hundreds of domains
- Rebrand and relaunch new websites after takedowns
- Use mule accounts or cryptocurrency wallets to rapidly transfer or launder stolen funds

Harvesting Credentials & Sensitive Information: Before any payment is completed, scammers collect user information directly through their fraudulent websites, including:

- Personal details (name, email, phone number)
- Account credentials
- Delivery information
- Financial or contact data entered during checkout

This stolen information may later be used for dark-web resale, account takeover attempts, phishing campaigns, social-engineering attacks, identity theft, or financial fraud activities.



Sign Up
Step 1 of 2
Personal details

First Name *

Email *

Password *

Confirm Password *

Gender *

Phone Number *

Date of Birth *

Country of Residence *

Preferred Communication Language *

Secure Checkout

Contact Information

Full Name *

Email *

Phone Number *

Shipping Address

Address Line 1 *

Address Line 2 *

City *

State / Province *

ZIP / Postal Code *

Country *

Order Summary

FIFA World Cup 2026 M2 Korea Republic vs Czechia - VIP x1 \$950.00

Subtotal (1 items) \$950.00

Estimated Tax \$78.00

Total \$1,026.00

Place Order — \$1,026.00

Your data is encrypted and secure

FIFA World Cup 2026 Payment Fraud Workflow

Use Case 1: Fraudulent Ticket Selling Websites

Victims encounter fraudulent FIFA World Cup 2026 ticket-selling websites impersonating official ticketing platforms, hospitality vendors, or authorized resale services. The scam typically advertises:

- Discounted FIFA World Cup 2026 match tickets
- VIP or hospitality ticket packages
- Exclusive presale or priority-access tickets
- Last-minute ticket availability
- Limited-time promotional pricing

The fraudulent websites are designed to appear legitimate by using official FIFA-related branding, fake order confirmations, countdown timers, secure checkout interfaces, and QR-code or PIX payment options to pressure victims into completing payment quickly.

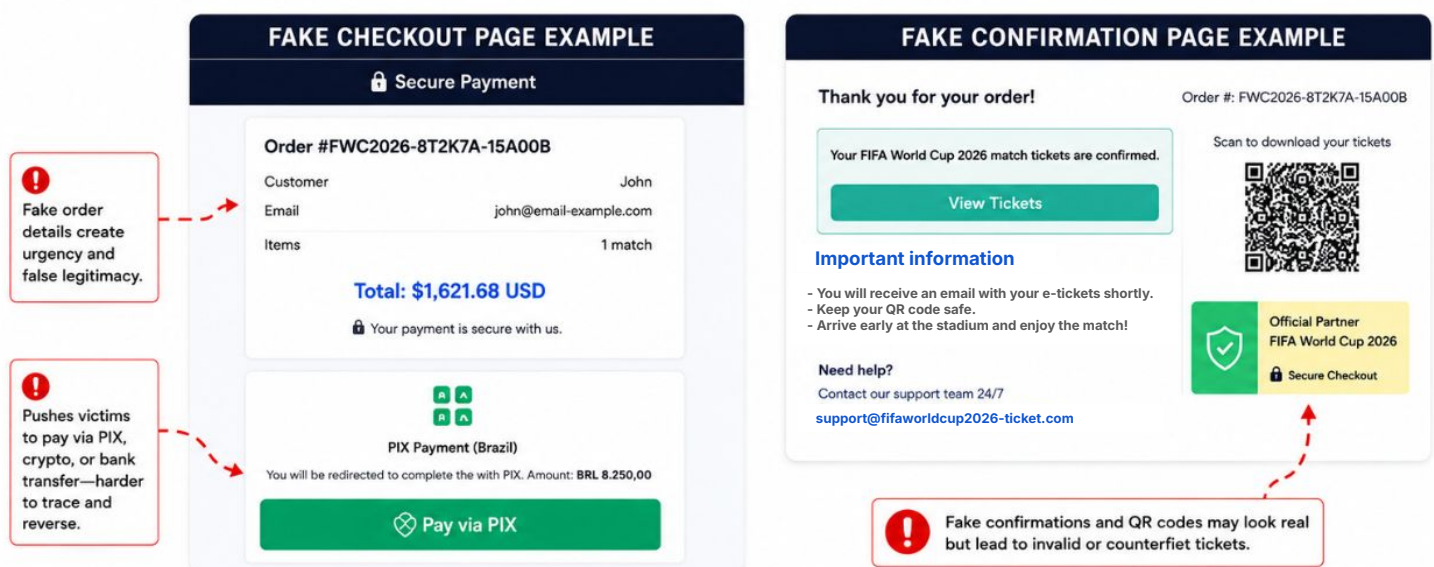
THE PAYMENT TRAP: HOW IT WORKS

Once the victim submits payment or enters their financial information, the scam enters a new phase:



HOW THE SCAM LOOKS

Fraudulent websites mimic legitimate platforms to gain your trust.



FIFA World Cup 2026 Payment Fraud Workflow

Use Case 2: Social Media Ticket Sale Scams

Victims encounter fake FIFA World Cup 2026 ticket sellers on social media, messaging apps, and online communities. These accounts advertise:

- Discounted tickets
- VIP or hospitality packages
- Last-minute availability
- Guaranteed seats for popular matches
- "Limited" or exclusive offers

Scammers build trust by chatting with victims, sharing fake screenshots, and pretending they have successfully sold tickets before. They often move the conversation to private messaging apps to complete the deal.



PAYMENT METHOD (IBAN BANK TRANSFER ONLY)

Once the victim agrees to buy tickets, the scam becomes a direct bank transfer fraud:



IBAN PAYMENT REQUESTS

Victims are asked to send money directly to an IBAN bank account provided by the scammer.



MONEY MULE ACCOUNTS

These bank accounts are usually controlled by money mules, meaning the real scammers stay hidden while others receive the money.



NO REFUNDS

Bank transfers are irreversible, so once the money is sent, it is very difficult to recover.



FAKE PROOF

Scammers may send fake payment confirmations or receipts to convince the victim everything is legitimate.



NO TICKETS DELIVERED

After payment, victims do not receive real tickets. Any QR codes or confirmations sent are fake and will not work at stadium entry.



The scam relies entirely on social media contact and direct IBAN bank transfers to trick victims into sending money that cannot be recovered.

HOW THE SCAM LOOKS (EXAMPLES)

Initial offer with attractive price and availability

Seller shares fake proof of previous sales

Uses fake samples to lock in trust

FifaTicket Serviceofficial
Active now

Hi! Do you have tickets for the World Cup?

Yes! I have great seats available
Category 1 - \$850 each
Limited offer for today only!

Just sold 4 tickets today ✓
Check my proof.

Great! How can I pay?

I will be sent to your mail with a valid QR code
To be scanned at the stadium entrance

Can u send me a sample please to make sure it is genuine

Best regards,
Elena Moreau
FIFA WORLD CUP TICKETING

716 716

This is a sample

FifaTicket Serviceofficial
Active now

what banks tell me

PayPal
Cash app
Chime
Zelle

All available

SOFI BANK
ACC NAME : Kimberly Singleton
Acc number:411007009661
Routing number : 031101334

Use this
And send the payment or receipt to our email

You are to pay \$2200
Best regards
Elena Moreau
FIFA World Cup ticketing

okay wait



IBAN bank details shared for payment



Fake tickets or screenshots are provided



After payment, seller disappears or blocks you

CTM360 Research Methodology

CTM360 identified and analyzed **FIFA World Cup 2026**-themed malicious and suspicious domains and accounts by leveraging the Fraud Navigator Framework to track scam progression across infrastructure setup, domain registration, brand impersonation, social media amplification, victim engagement, and monetization, enabling the identification of how threat actors weaponized FIFA World Cup 2026 themes to execute ticketing, streaming & betting scams across multiple online platforms.



Data Collection Period

The research and monitoring activities were conducted between January and May 2026.

The research and monitoring activities were conducted between **January and May 2026**. During this period, **CTM360** continuously tracked newly registered domains, suspicious social media activity, malicious infrastructure, and scam-related campaigns associated with **FIFA World Cup 2026** themes across multiple online platforms and channels.



Threat Classification

BTMOB is an Android RAT and crypto-mining malware that is often disguised as a legitimate notes or IPTV-style application.



Threat Actors Motive

After analyzing the social media accounts and the identified websites across multiple threat intelligence sources and verification tools, they were classified as **MALICIOUS** due to:

- Multiple users on social media reported that they were scammed by these websites or accounts after making payments.
- These findings were confirmed through multiple threat intel platforms, OSINT sources, and community reports.
- Malicious indicators such as suspicious domain names, unusual TLDs (e.g. **.xyz**, **.top**, **.online**), recently registered domains, poor language quality, and only accepting cryptocurrency as a payment option.



Keyword Patterns Used

FIFA, World Cup 2026, Worldcup2026, WC2026, FIFA2026, tickets, FIFA WC 2026, FIFA tickets, Coupe du Monde 2026, Copa Mundial 2026, Coppa del Mondo 2026, Copa do Mundo 2026, 2026 مونديال, 2026 كأس العالم



Used in multiple languages, including English, Spanish, French, Portuguese, Italian, Arabic, and others.



Social Media Scam Methodology

CTM360 followed a structured methodology to identify and analyze social media scams. Scammers create fake accounts, pages, or ads offering FIFA World Cup 2026 tickets at discounted prices to attract victims. They engage with users, respond to messages, and pretend to have tickets available to build trust. Victims are then asked to pay via bank transfer or cryptocurrency (IBAN), after which scammers either send fake tickets or stop responding, and no tickets are delivered.

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and fully managed unlimited takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

 +973 77 360 360

 info@ctm360.com

 www.ctm360.com

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

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents, or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential, or other damages or claims whatsoever including, but not limited to loss of data, loss in profits/business, network disruption...etc., arising out of or in connection with this advisory.

