

The GHOST STADIUM Score: Billions At Stake At The World's Largest Football Tournament

Archived: 2026-06-04 02:00:20 UTC



Introduction

The 2026 FIFA World Cup is set to be the largest sporting event in history. Hosted across three nations — the United States, Canada, and Mexico — the tournament will take place from June 11 to July 19, 2026, featuring 104 matches played in 16 cities. The scale is unprecedented: FIFA estimates that more than six million fans will fill stadiums, with an average of 450,000 visitors per city. More than 150 million tickets were requested within the first 15 days of the sales window alone, making this edition approximately 30 times oversubscribed compared to previous tournaments. For context, the 2022 Qatar World Cup drew over 3.4 million in-stadium fans with an average attendance capacity of 96.3 per cent. The 2026 edition is expected to nearly double that figure.

This enormous demand — and the urgency it creates among fans desperate to secure tickets — has made the football tournament a magnet for fraud. Months before the opening whistle, Group-IB researchers have uncovered a sprawling ecosystem of fraud activity targeting the tournament and its global audience. The investigation identified more than 4,300 fraudulent domains impersonating FIFA's official web presence registered since August 2025, six distinct fraud schemes running in parallel, four independent threat actors, and over 2,500 FIFA account credential pairs already circulating in dark-web markets.

At the centre of this ecosystem sits a threat actor Group-IB has designated **GHOST STADIUM** — a Chinese-speaking, financially motivated operator running a sophisticated phishing campaign across more than 300 domains. GHOST STADIUM has built a pixel-perfect clone of the official FIFA website, complete with a replicated single sign-on (SSO) authentication flow, and multi-language support in 11 languages. A conservative estimate based on the campaign's observable infrastructure places the potential financial losses from premium ticket fraud alone (account for ~25% of 300+ phishing domains) at between \$71 million and \$474 million — and the total campaign losses across all tiers could reach into the billions.



Figure 1: Example of a fraudulent domain fifa-tickets[.]vip/tickets_shop, tracked under the GHOST STADIUM phishing campaign.

But GHOST STADIUM is not operating alone. Three additional threat actors — including a bulk domain squatter pre-positioning hundreds of typosquat domains, an industrialized infostealer ecosystem incidentally harvesting FIFA credentials at scale, and an underground supply chain of Phishing-as-a-Service (PhaaS) vendors lowering the barrier for new entrants — are exploiting the same event simultaneously. Together, they are running six parallel fraud schemes: credential phishing, fake ticket sales, counterfeit merchandise storefronts, fake streaming platforms, fraudulent betting and casino sites, and infostealer-driven credential theft.

This blog presents Group-IB’s research findings across the full fraud landscape, profiles the GHOST STADIUM threat actor, and introduces the Cyber Fraud Fusion (CFF) defence model — a coordinated framework that connects digital risk protection, threat intelligence, fraud prevention, cross-institutional intelligence sharing, and investigation services to predict and prevent fraud at the speed and scale of the campaign itself.

Key Discoveries

- **Over 4,300 fraudulent domains impersonating FIFA’s official web presence** have been registered since August 2025; more than 300 are confirmed actively running fraudulent infrastructure, more than 140 are flagged as suspicious, and approximately 3,800 are parked or dormant — pre-positioned for activation as the tournament approaches.
- **GHOST STADIUM**, a single Chinese-speaking threat actor, is operating a coordinated phishing campaign across 300+ domains using a shared phishing kit that exploits FIFA’s official PingIdentity SSO login flow by closing it with near pixel-perfect fidelity.
- **Six distinct fraud schemes** target football fans: credential phishing, fake ticket sales, counterfeit merchandise, fake streaming platforms, fraudulent betting sites, and infostealer-driven credential theft.
- **Financial losses** from premium and hospitality ticket fraud alone (~25% of all) are estimated at \$71 million to \$474 million across the campaign. Total phishing campaign losses operated by GHOST

STADIUM across all tiers may reach billions of dollars.

- **2,513 FIFA account credential pairs** (for fifa.com and fifa.org) are already circulating in dark-web markets, harvested incidentally by mass infostealer campaigns.
- **Four independent threat actors** have been identified, including a Phishing-as-a-Service supply chain that sells pre-built fraud kits, automated ticket-purchasing bots, and phishing templates to downstream operators.
- **Facebook Ads** serves as the primary paid traffic acquisition channel for the GHOST STADIUM campaign, with three Meta Pixel IDs embedded across the cluster, meaning the attacker is actively exploiting Meta's advertising platform to promote phishing pages to targeted victims.

Who May Find This Blog Interesting

- Cybersecurity analysts and corporate security teams
- Fraud prevention and anti-financial crime teams at banks, payment providers, and cryptocurrency exchanges
- Threat intelligence specialists
- Brand protection teams (sports organisations, ticketing platforms)
- Law enforcement investigators
- Computer Emergency Response Teams (CERT/CSIRT)

Group-IB Threat Intelligence Portal: GHOST STADIUM

Group-IB customers can access our Threat Intelligence and Fraud Protection portals for more information about GHOST STADIUM, the wider fraud ecosystem targeting the FIFA World Cup 2026, and the full indicators of compromise identified in this research:

- [GHOST STADIUM](#)
- [Fraud Intelligence Report](#)

Threat Actor Profile



Ghost Stadium

First seen
November 2025

Financially motivated Chinese-speaking threat actor operating a centrally managed phishing kit infrastructure targeting the global audience of the world's largest football tournament. The actor deploys a custom React-based phishing kit built with the Layui framework — a Chinese open-source UI library — cloning the official brand website and SSO login flow to harvest credentials and conduct fake ticket sales and payment fraud at scale.

Aliases

Dragon Ticket

Toolset

- Custom React.js phishing kit
- Layui 2.7.6 UI framework
- Cloned PingIdentity SSO
- Tawk.to live chat
- Meta Pixel IDs
- Cloudflare (per-domain zone isolation)
- ThinkPHP 5.0.28 backend
- Redis session store
- ChainUGO cryptocurrency payment gateway
- Snipcart custom payment gateways

Targeted Industries

- Entertainment & Sports
- Ticketing Platforms
- E-Commerce
- General Consumer Public

Targeted Countries

- United States
- Canada
- Mexico
- United Kingdom
- Germany
- France
- Portugal
- Spain
- Italy
- Brazil
- Argentina
- Colombia
- Australia
- China

Motivation

Financial Gain

Modus operandi

Exploiting legitimate operators and services such as bulk domain registration through GNAME.COM PTE. LTD.; automated kit deployment serving byte-identical HTML across all cluster domains; traffic acquisition via paid Meta (Facebook) advertising using three parallel ad accounts; credential capture via cloned PingIdentity SSO at /as/authorize; payment fraud via fake ticket storefront at /tickets_shop accepting cryptocurrency through ChainUGO; real-time victim engagement via Tawk.to live chat; search-engine concealment via noindex/nofollow meta tags on credential pages.

Group-IB, 2026

The GHOST STADIUM Campaign: How It Works

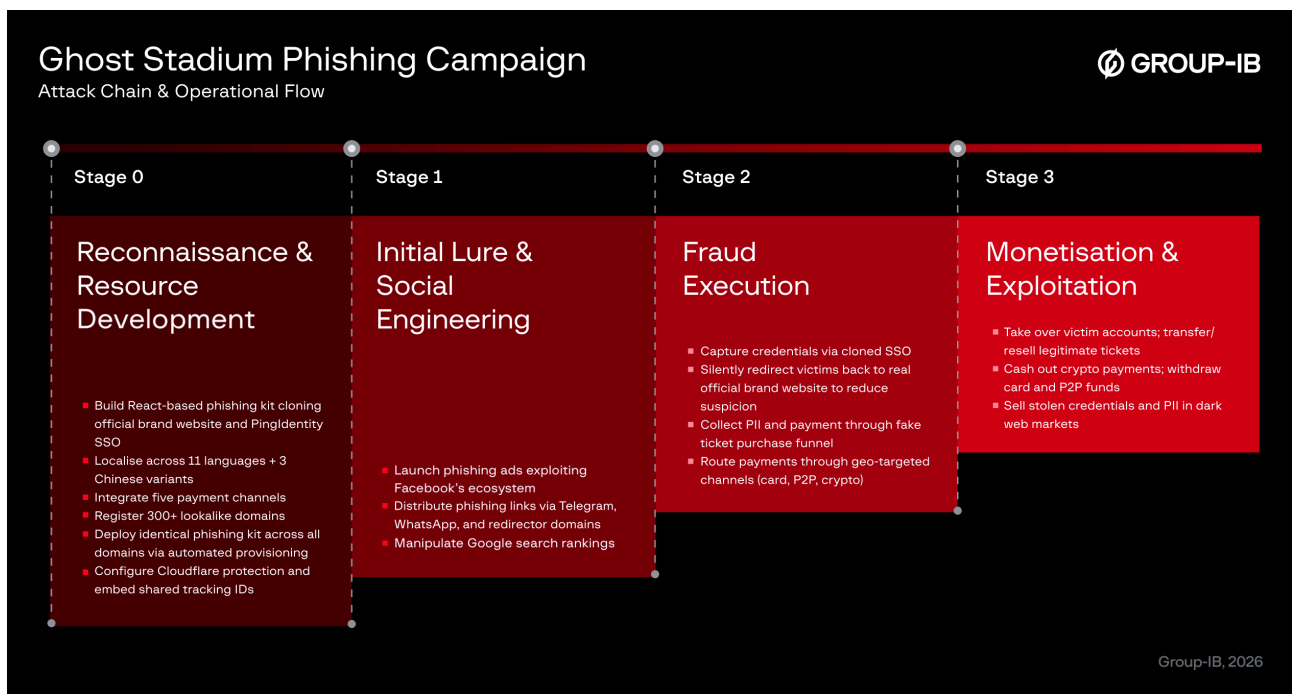


Figure 2: GHOST STADIUM phishing campaign attack chain and operational flow.

The Phishing Kit: A Pixel-perfect Clone

The GHOST STADIUM phishing kit is a custom React-based single-page application that clones the official fifa.com website to near pixel-perfect fidelity. The kit is built with the **Layui 2.7.6** UI framework, a Chinese open-source library virtually unknown outside the Chinese developer community. FIFA's legitimate single sign-on service is provided by PingIdentity, and the GHOST STADIUM phishing kit is even capable of replicating this using the actual `client_id` lifted from the real FIFA SSO.

The cloned flow is functionally indistinguishable from the legitimate login process as well including registration page and payment check out page. Critically, the phishing page scope parameters include `p1:reset:userPassword`, which authorises password reset — enabling the attacker to immediately lock legitimate users out of their accounts after capturing their credentials. The kit also requests email, address, and phone data, harvesting personal information beyond just login credentials. After capture, victims are silently redirected to the real <https://www.fifa.com/auth>, so the experience appears to be a successful login.

The phishing pages invest heavily in visual legitimacy. All product imagery and FIFA branding is loaded directly from FIFA's official digital hub Content Delivery Network (CDN), making the page visually authentic at zero infrastructure cost while bypassing content-similarity detection tools that compare hash signatures of hosted images. The footer carries authentic links to FIFA's real social media accounts and a Google Translate widget is embedded as an additional trust signal. This is not a crude phishing page — it is a meticulously engineered impersonation.

The kit auto-detects browser locale and switches its interface across **11 languages** plus three Chinese variants (Simplified, Traditional, and Hong Kong). The supported languages include English, German, French, Spanish, Portuguese, Italian, Arabic, Japanese, Korean, Indonesian, and Russian. The granular enumeration of three Chinese locales goes beyond what is necessary for global reach and is itself an attribution signal — Chinese-

speaking developers distinguish mainland, Taiwan, and Hong Kong locales because these are meaningful distinctions in their own linguistic environment.

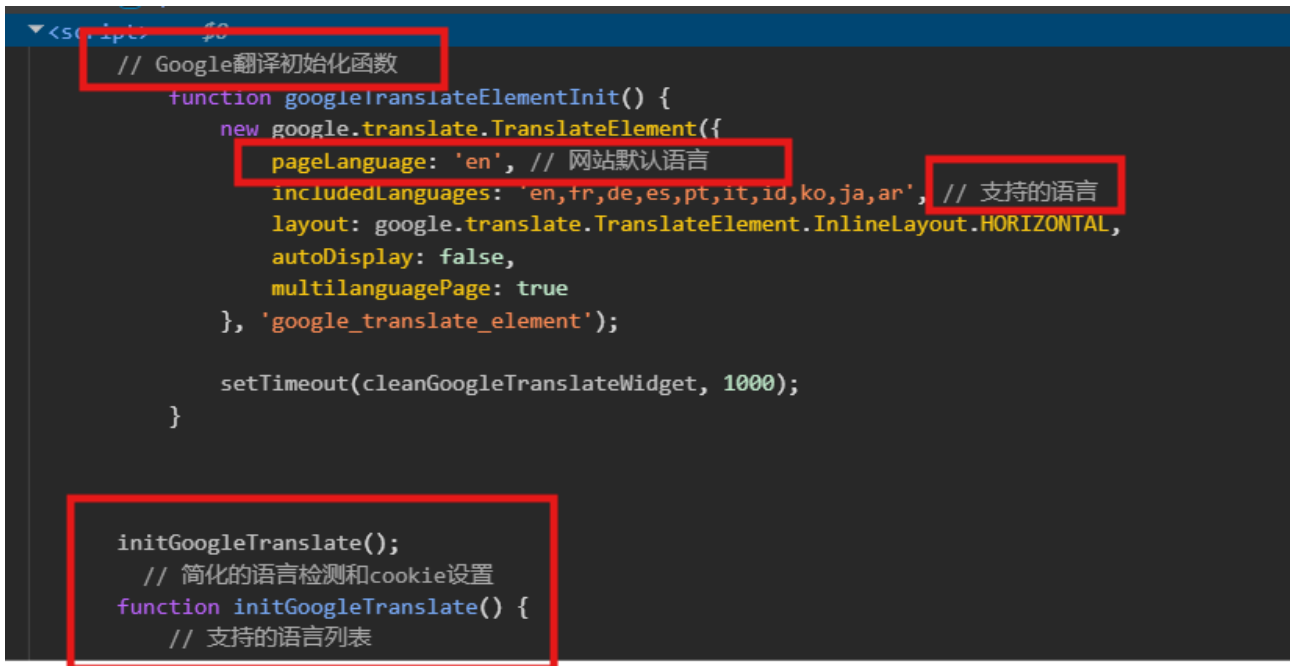


Figure 3: Chinese-language comments in the source code, a key attribution evidence linking the GHOST STADIUM phishing kit to a Chinese-speaking developer.

Infrastructure analysis further confirms single-operator control. Shared *SSL certificates* and Meta (Facebook) Pixel IDs are embedded identically across 300+ phishing domains, tying all domains to the same Facebook advertising accounts. The byte-for-byte identical 415 KB HTML pages and same Tawk[.]to live-chat Property ID were detected used across 79 domains selling premium and hospitality tickets, confirming automated multi-domain provisioning from a single source kit.

```

1209 <!-- Meta Pixel Code -->
1210 <script>
1211 !function(f,b,e,v,n,t,s)
1212 {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
1213 n.callMethod.apply(n,arguments):n.queue.push(arguments)};
1214 if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
1215 n.queue=[];t=b.createElement(e);t.async=!0;
1216 t.src=v;s=b.getElementsByTagName(e)[0];
1217 s.parentNode.insertBefore(t,s)}(window, document,'script',
1218 'static/js/fbevents.js');
1219 fbq('init', '1125427529712029');
1220 fbq('track', 'PageView');
1221 </script>
1222 <noscript></noscript>
1223 <!-- End Meta Pixel Code --> </div>

```

Figure 4: Shared Meta Pixel code observed across multiple phishing domains attributed to GHOST STADIUM.



Figure 5: Group-IB Graph shows connected SSL certificates across the GHOST STADIUM campaign domains.

How Victims Lose Credentials and Money



Figure 6: GHOST STADIUM victim journey.

The victim’s journey through the GHOST STADIUM campaign follows a carefully designed funnel. When a visitor arrives at any cluster domain, they are immediately presented with an aggressive fake popup mimicking official hospitality announcements, with a ‘BUY NOW’ call-to-action.

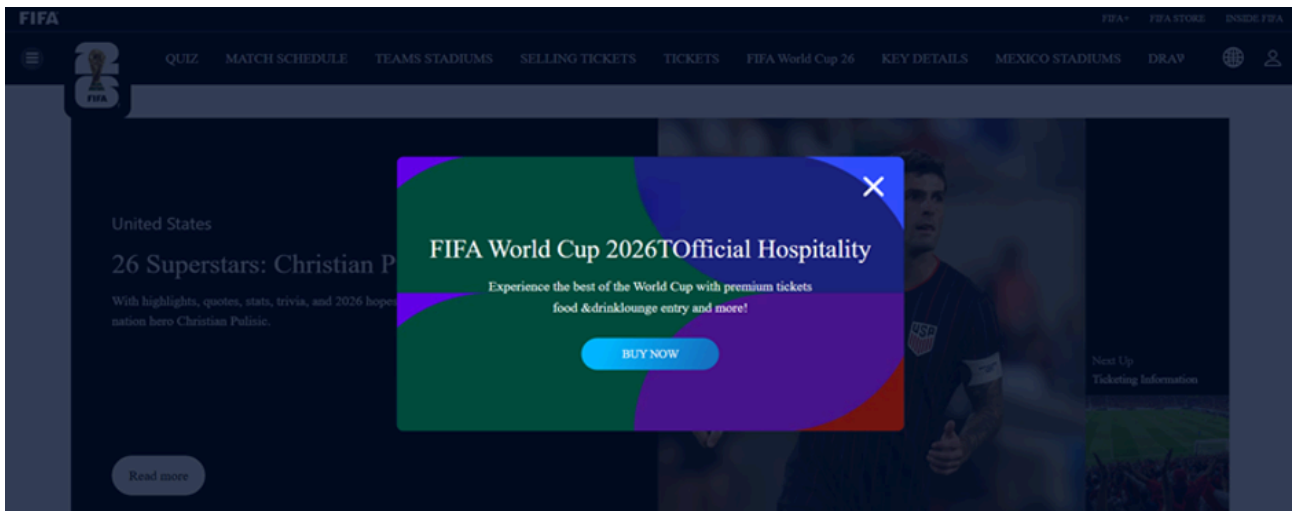


Figure 7: Example of a fake “BUY NOW” pop-up on a fraudulent domain (www-fifa[.]com[.]co) replicating the exact layout and branding of the legitimate site hospitality promotion used to lure victims.

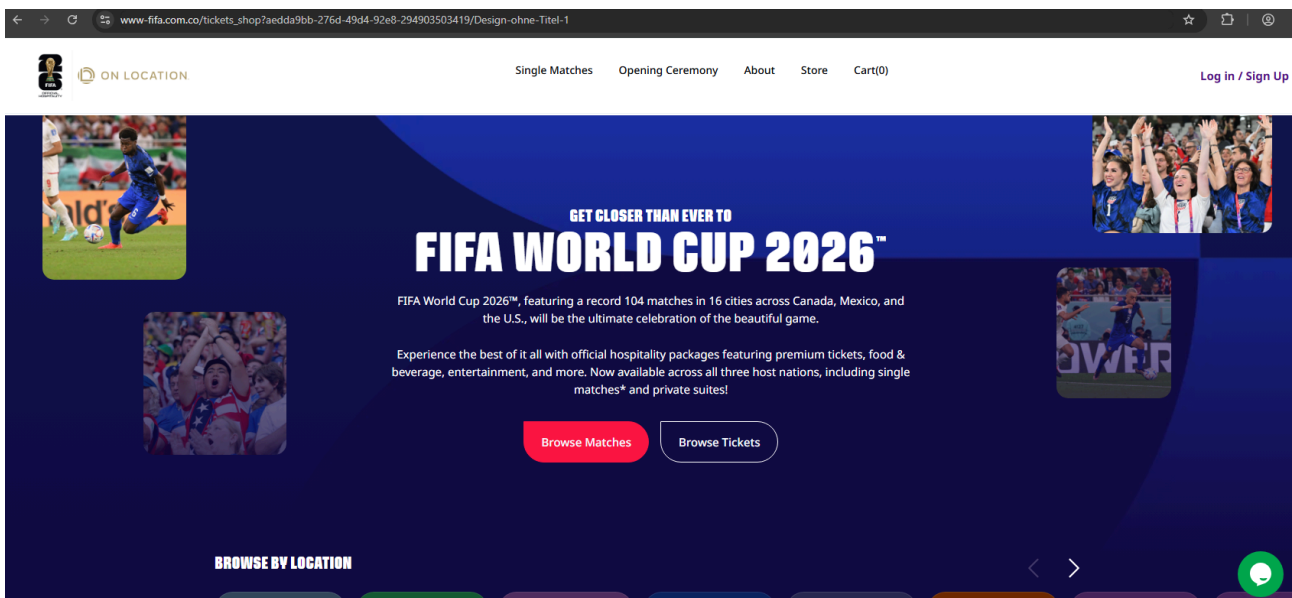


Figure 8: Example of a fraudulent ticketing page (www-fifa[.]com[.]co) that impersonates the official FIFA “On Location” hospitality site.

The function is structured as a pseudo-legitimate purchase flow: match selection, bundle selection (premium tiers), seating tier selection, cart review, and checkout. Victims who click “Browse Tickets” are redirected through a match selection interface to a fake “Log In / Sign Up” page that harvests credentials. Any credential pair with a valid email pattern is accepted, after which the account takeover process is complete. If the victim has legitimate tickets associated with their FIFA account, the attacker can change their credentials, lock them out, and resell the tickets. New users seeking to purchase tickets are redirected to a buying form and then a fake checkout page that collects extensive personal information via POST: first name, last name, email address, phone number, street address, city, state/province, ZIP/postal code, country, and delivery instructions.

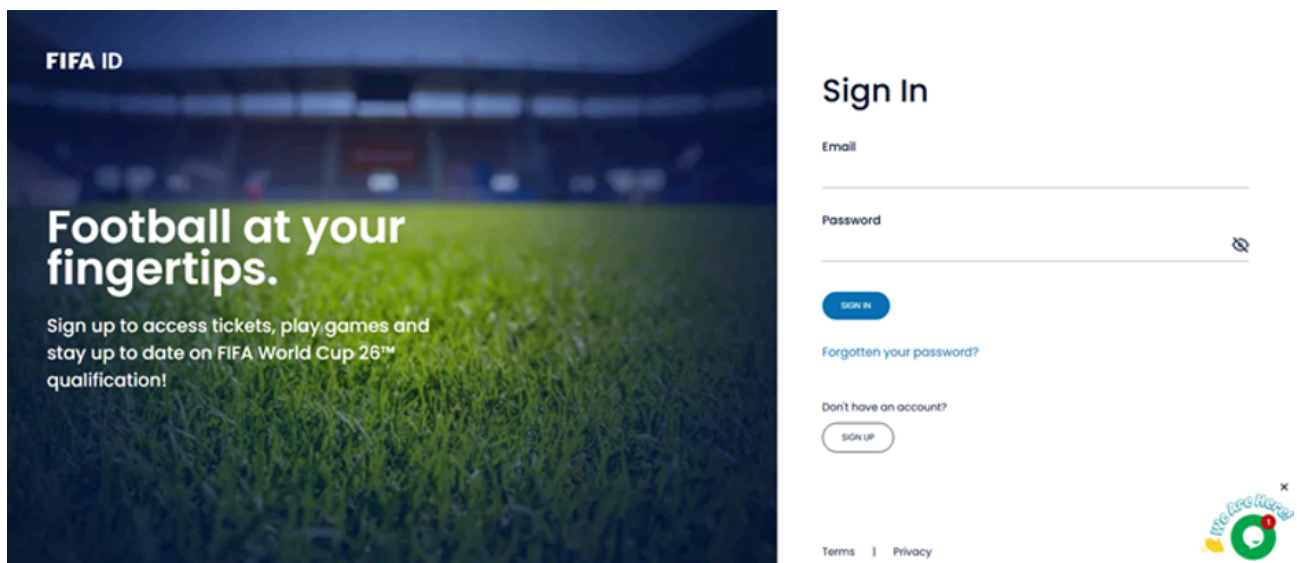


Figure 9: Example of a fake Log In / Sign Up page using the cloned PingIdentity SSO where credentials are captured.

A screenshot of a checkout page with a light blue and white color scheme. The top navigation bar includes the FIFA logo, an 'Account' link, and a 'Cart' icon showing 0 items. The main content area is divided into two columns. The left column, titled 'Shipping information', contains fields for 'First name' (John), 'Last name' (Doe), 'Email address' (john.doe@example.com), 'Phone number' (+1 (555) 123-4567), 'Street address' (1234 Main Street), 'City' (San Francisco), 'State / Province / Region' (California), 'ZIP / Postal code' (94107), and 'Country' (United States). There is also a text area for 'Delivery instructions (optional)' with the text 'Leave at front door, ring bell, etc.'. The right column contains an 'Order summary' section showing a 'Total' of '\$0.00' and an 'Estimated delivery' of '5-7 business days'. Below this is the 'Payment method' section, which states 'All transactions are secure and encrypted' and offers three options: 'Credit or debit card' (selected), 'Google Pay', and 'Apple Pay'. At the bottom of the right column is a large blue button labeled 'Pay \$0.00' with a lock icon, and a green 'checkout' button below it.

Figure 10: Example of a fake checkout page collecting PII and payment details.

After clicking “Pay”, the attacker accepts payments through at least **five distinct channels**, demonstrating a level of operational sophistication designed to maximise conversion across different victim profiles and geographies:

- 1. **Direct card capture:** Phishing forms on the attacker’s domain present a “Secure Payment” interface requesting cardholder name, card number, expiry, and CVV. Order IDs follow the format `FWC2026XXXXXXXX` , repeating across multiple domains and confirming a shared backend template.

The screenshot shows a web browser window with the address bar displaying `fifi emo.cc/pay/FWC2026050662D2B566`. The page has a dark blue header with a padlock icon and the text "Secure Payment". Below the header, the main content area is light blue and contains a white card with the following details:

- Order #FWC2026050662D2B566**
- Customer:** A [redacted]
- Email:** ok [redacted] gmail.com
- Items:** 1 item(s)
- Total: \$470.88 USD**
- Please complete payment within 14:38

Below the card, there is a payment form with the following fields:

- Payment logos: VISA, Mastercard, AMEX, DISCOVER
- Cardholder Name:** Name on card
- Card Number:** 1234 5678 9012 3456
- Expiry Date:** MM/YY
- CVV:** 123
- Pay \$470.88** (green button)

At the bottom of the form, there are two security assurances:

- Your payment information is encrypted and secure
- 256-bit SSL encryption

Figure 11: Example of card checkout pages with shared Order # formatting across phishing domains.

- 2. **Third-party payment gateways:** Some sites redirect victims to external processors such as `pay[.]zfxupi[.]net` , which offers Cash App and Chime as payment options. These gateways add a layer of perceived legitimacy and obscure the destination of funds.

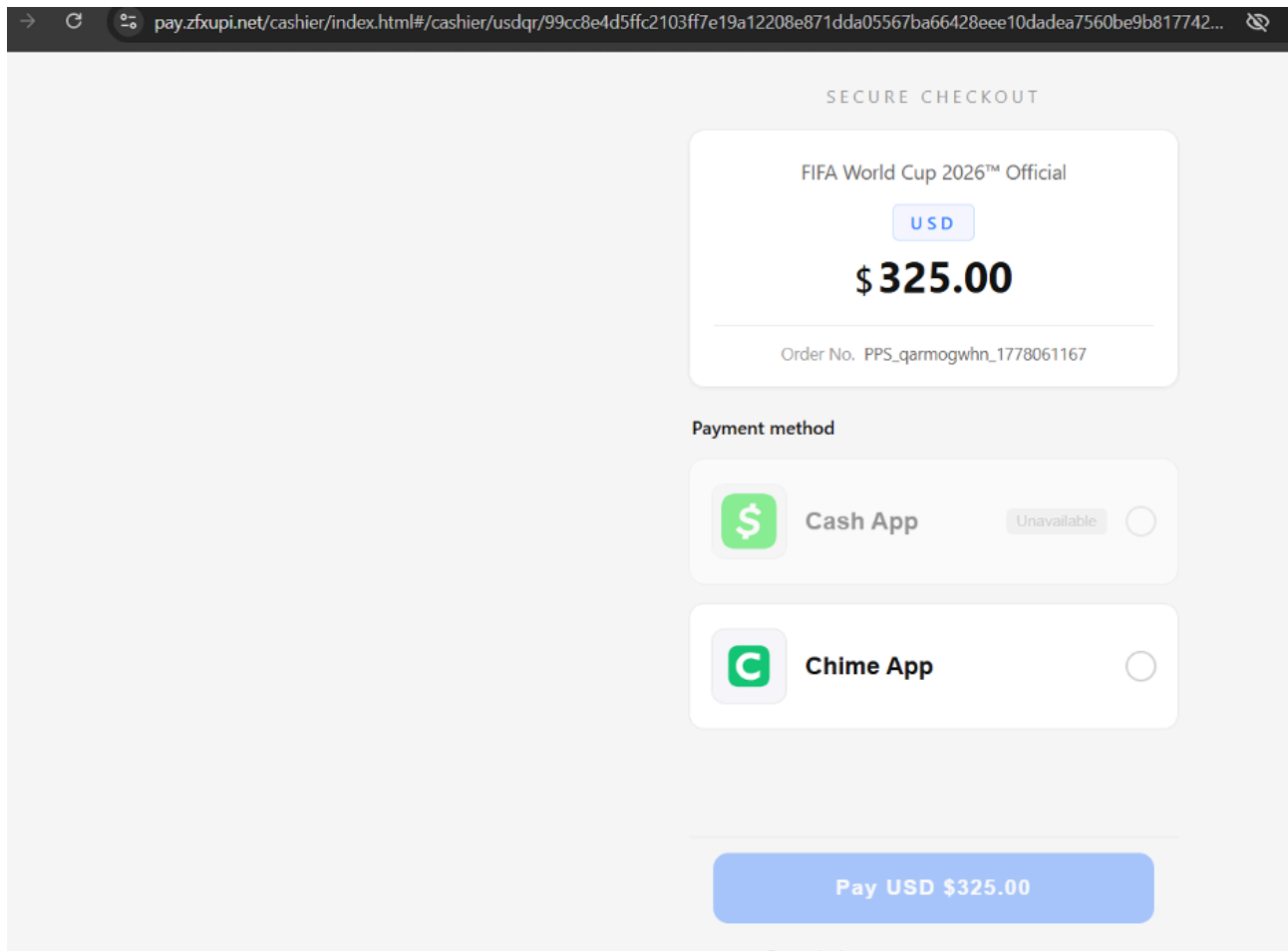


Figure 12: Example of redirection to external payment gateways.

- **3. Peer-to-peer money transfer apps:** Certain payment flows route through P2P platforms. Chime payments were observed routing to a specific cashtag, while Nequi, a Colombian P2P service, payments route to a specific account number. This indicates geo-targeting of payment channels by victim country.

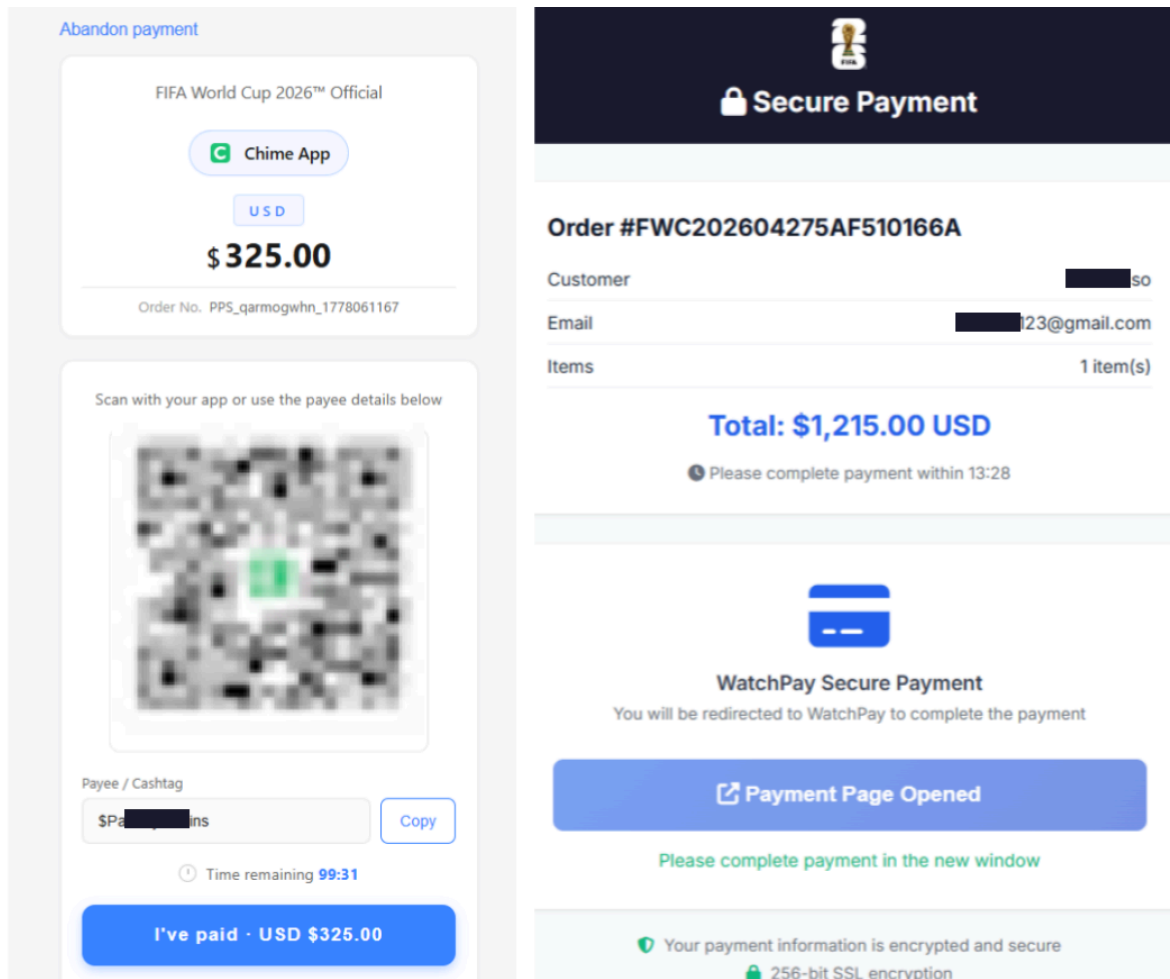


Figure 13: Examples of various peer-to-peer payment options.



Figure 13: Examples of various peer-to-peer payment options.

- **4. Region-specific payment rails:** One domain routes payments through “FIXYD — Mexico Payment”, confirming geographic targeting of victims based on country of origin.

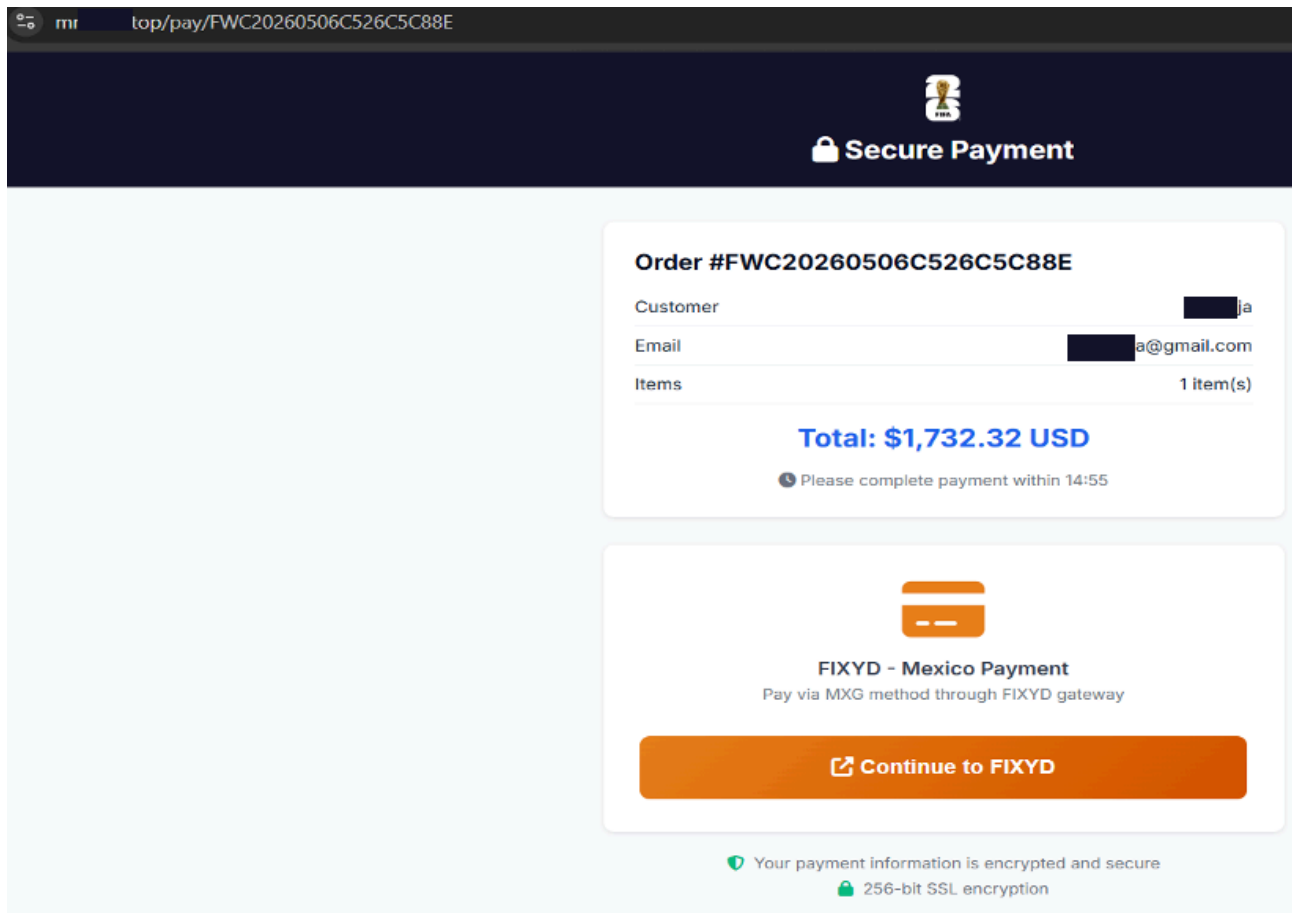


Figure 14: Example of geographic targeting with location-aware payment options.

- **5. Crypto on-ramp via legitimate processors:** Alchemy Pay converts \$195 USD card payments into approximately 185 USDT on Binance Smart Chain, giving the attacker irreversible cryptocurrency settlement under a regulated processor's branding.

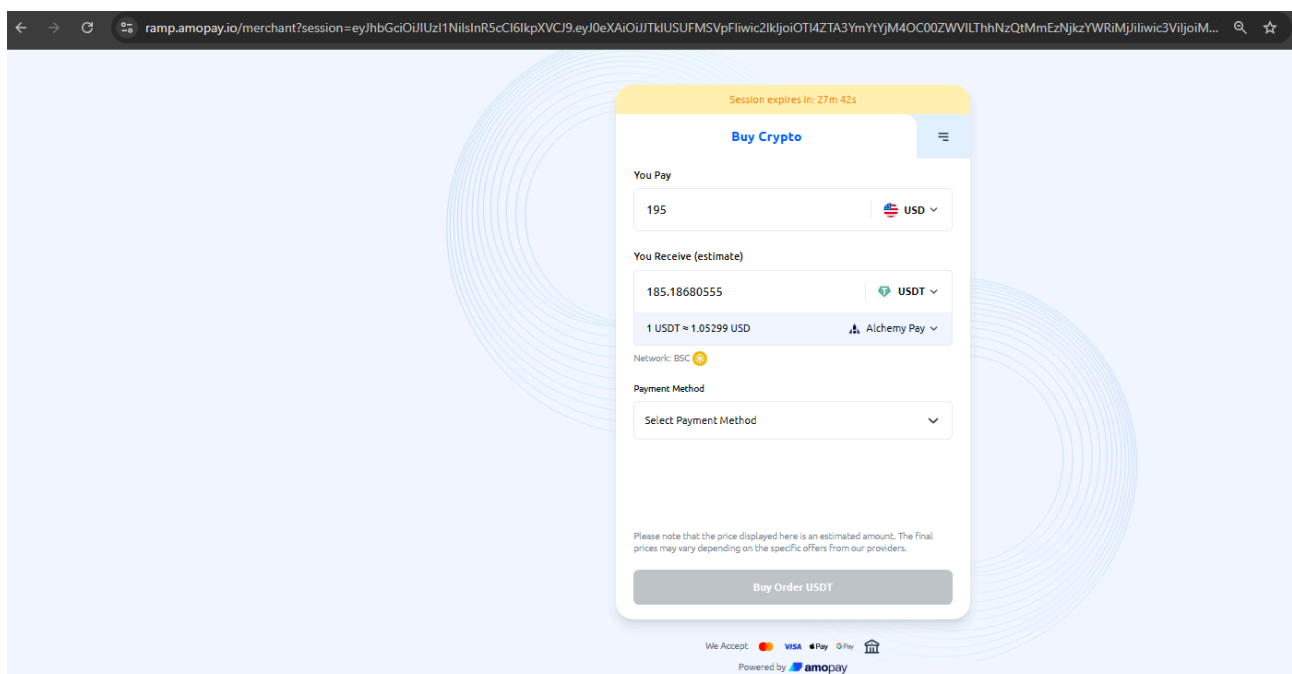


Figure 15: Example of crypto on-ramp payment options.

Regardless of which payment channel is used, the result is the same: money flows to the attacker and the victim receives no tickets.

Scale and Financial Impact

The observed fraud campaign targets the entire FIFA World Cup 2026 audience of over six million fans globally. Among the 300+ phishing sites, 79 were detected to provide only premium and hospitality tier tickets with pricing in the range of \$1,500 to \$10,000+. With more than 600 victims observed registering at a single domain, extrapolation across the 79 premium-focused sites suggests the victim count for premium and hospitality tier fraud alone may exceed 47,400 people, with financial losses ranging from approximately **\$71 million to \$474 million USD**.

These figures cover only the premium ticket fraud conducted by GHOST STADIUM. If one-quarter of the fake websites (79 out of 300+) can generate hundreds of millions of dollars in losses, the total profit from the entire campaign — including credential theft, lower-tier ticket fraud, and the broader ecosystem of downstream monetisation — could reasonably reach into the billions. Additionally, **2,513 confirmed FIFA credential pairs** are already listed for sale in dark-web markets at \$5 to \$50 per pair, feeding a separate account-takeover pipeline that operates independently of the phishing infrastructure.

How Phishing Sites Reach Victims

The GHOST STADIUM campaign uses multiple distribution channels to drive traffic to its phishing domains, with the exploitation of paid social media advertising serving as the primary acquisition engine.

- **Fake Facebook Ads:** Observed to be the main distribution channel, the attacker exploits Meta's advertising platform to promote the phishing pages directly to targeted users, significantly increasing both reach and perceived credibility. Three shared Meta Pixel IDs were detected across all 300+ domains, confirming that the same advertiser or group is behind the entire campaign. The ads deploy classic urgency tactics: displaying dramatically lower prices than official tickets (as low as \$60 for tickets officially priced at thousands) and using countdown timers with "first come, first served" messaging to pressure immediate action.

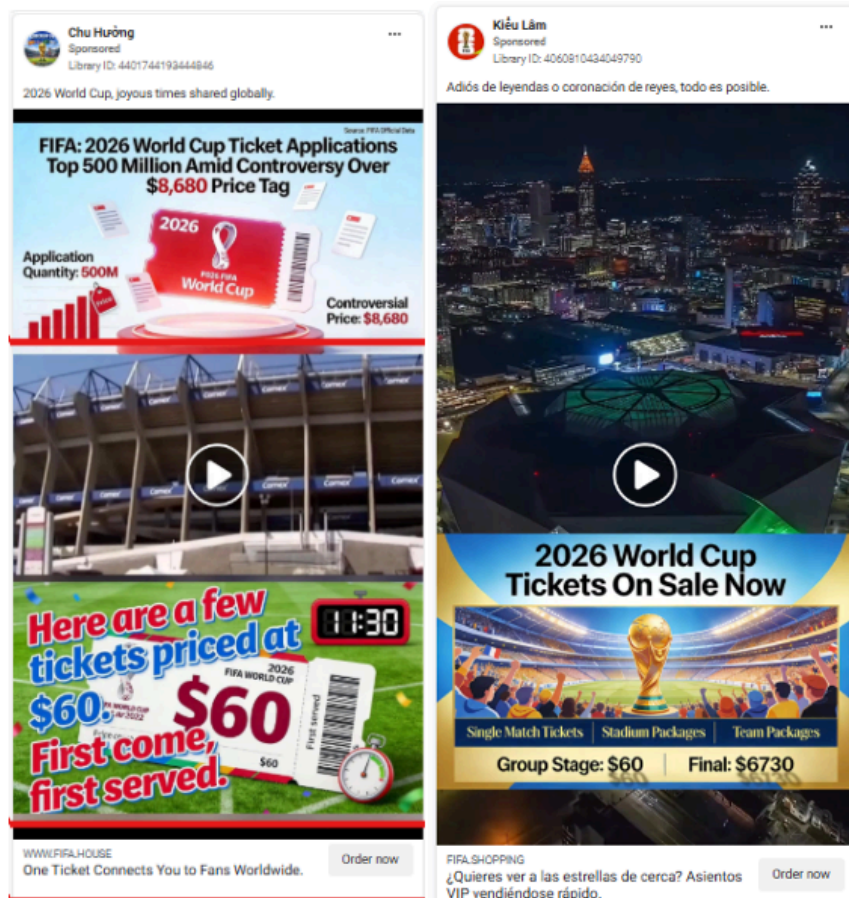


Figure 16: Examples of scam ads abusing Facebook’s advertising platform with fake urgency pricing and countdown timer.

Telegram and WhatsApp: Beyond web-based phishing, the campaign pushes victims toward direct communication channels. Some scam pages and fake Facebook ads display “Call now” or “Message” buttons, or list phone numbers directly on their profiles. Telegram channels are also abused to distribute phishing links with limited-time offers. This multi-channel approach ensures that victims who do not click on web ads can still be reached through direct messaging.

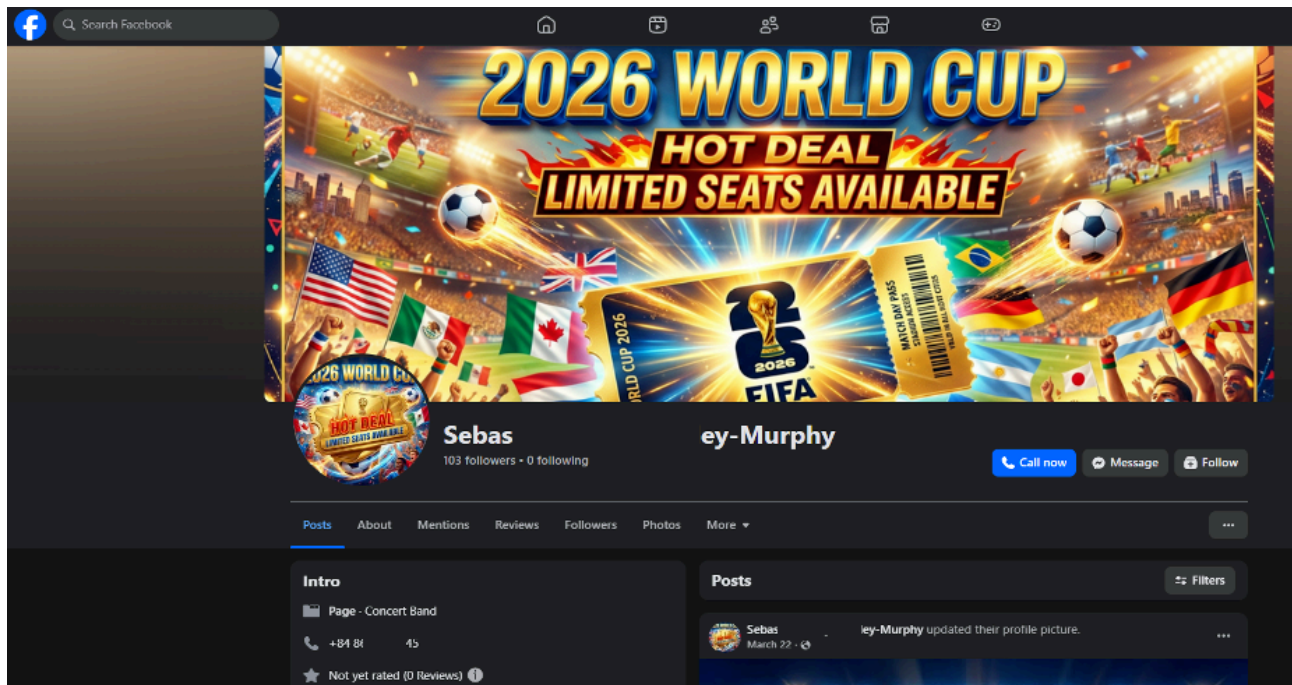


Figure 17: Example of a “Call Now” button on scam social media pages that direct victims toward direct communication with the fraudsters.

- **Search engines:** The malicious sites have also been observed to appear in Google search results for FIFA-related queries. Fraud domains such as fifa[.]tax, fifa[.]party, and fifa-web[.]co impersonate FIFA names and favicons, with copied content to mimic official ticketing sites and rank organically, with the possibility of reaching victims who never encountered a Facebook ad.

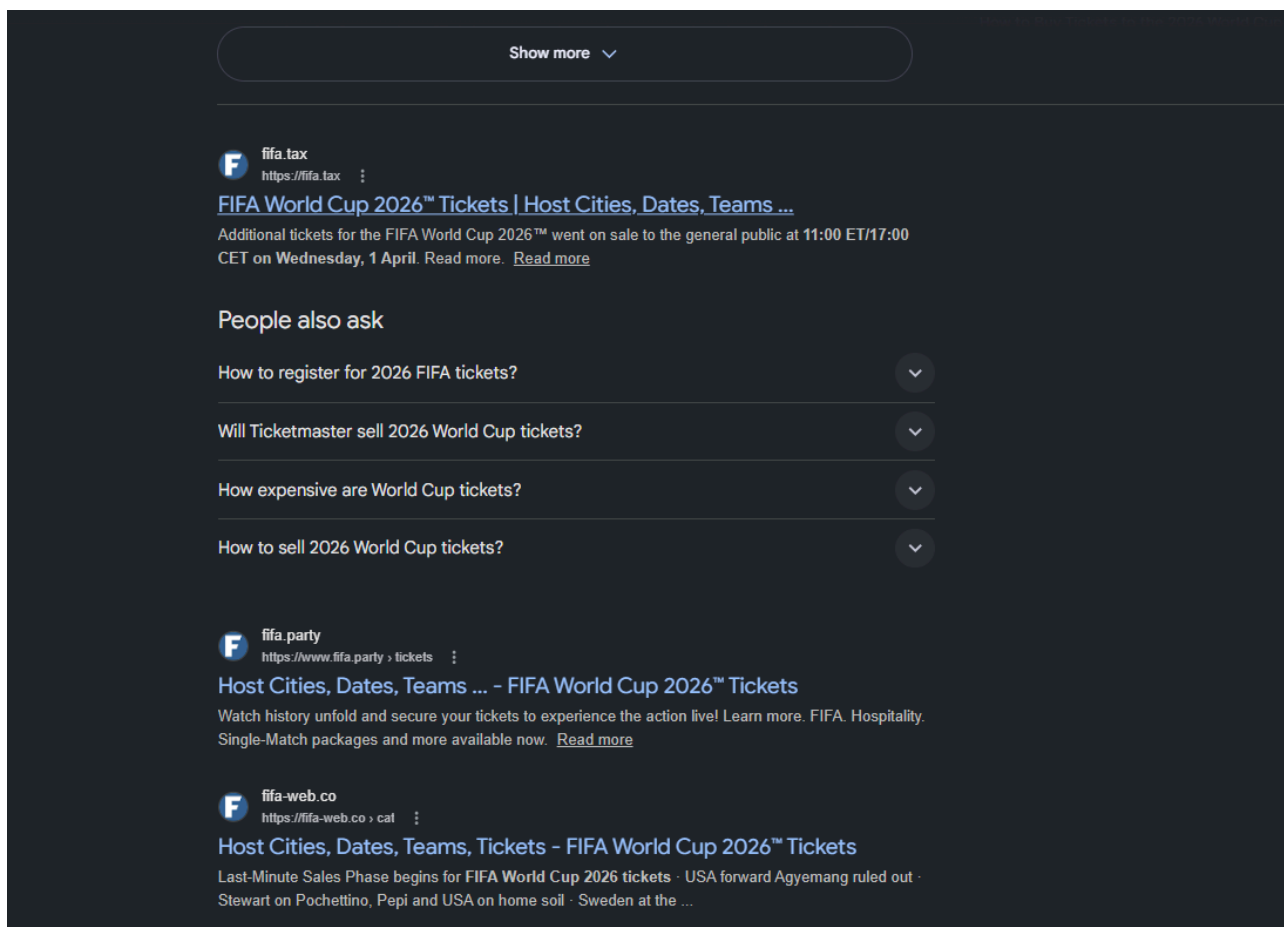


Figure 18: Google search results showing fraudulent domains impersonating FIFA’s official web presence ranking alongside legitimate results.

- **Redirector domains:** Four “football-” themed domains have been observed redirecting victims to these fraudulent domains impersonating FIFA’s official web presence. All four share the same origin IP (43.98.183[.]110) and were registered on the same date (April 27, 2026). These redirector domains can appear in any context related to FIFA and serve as resilient entry points if primary phishing domains are taken down.

```
football-ticket[.]top
football-ticket[.]shop
football-game[.]shop
football-tickets[.]top
```

The Fraud-as-a-Service Supply Chain

GHOST STADIUM does not operate in a vacuum. Investigations revealed a fourth threat actor category — **Dark Web Fraud Kit Sellers (TA-4)** — functioning as the supply-chain layer of the fraud ecosystem targeting the FIFA World Cup 2026. These underground vendors sell pre-built phishing kits , automated ticket-purchasing bots,

domain inventories, and email phishing templates through dark-web forums. Their activity has been observed since mid-2025, well before the phishing campaigns began active deployment.

The existence of this supply chain has three critical implications. First, it lowers the barrier to entry: any aspiring fraud operator may purchase a ready-made kit and deploy it without the technical capability to build one from scratch. Second, it means that taking down one operator does not eliminate the threat — the same kit (or its variants) may be deployed by new entrants who purchase it from the underground market.

As the tournament approaches, this supply chain is expected to accelerate: more kits will appear, more operators will enter the market, and the fraud surface will expand. Disruption of the supply chain itself — targeting kit sellers, bot distributors, and credential brokers — is a necessary complement to individual campaign takedowns.

Beyond Phishing — Four More Fraud Schemes Targeting Football Fans

While the GHOST STADIUM credential phishing and fake ticket sales operation represents the highest-confidence and most technically detailed finding, it is only part of a broader fraud ecosystem exploiting the FIFA World Cup 2026. Four additional fraud schemes were identified operating in parallel, each with distinct monetisation mechanics and victim flows.

Fake streaming platforms: Approximately 55 domains were observed promising “free” or “premium” live streaming of World Cup matches. These sites target fans who cannot attend matches in person and are seeking online streaming options. Victims are required to register and pay a subscription fee; in return, they receive either no content or, in more sophisticated variants, browser-based stealers or Remote Access Trojans (RATs) that silently compromise the victim’s device. The dual monetisation model — subscription fees plus downstream credential theft from malware infections — makes these sites particularly damaging. Domain templates such as `fifa2026tickets-streamlive[.]com` and `fifa-stream-*` are common, often featuring countdown timers and fake “Malware Scanned” trust badges.

Counterfeit merchandise storefronts: Approximately 56 domains plus dedicated Telegram channels were detected selling fake FIFA, national team, and player-branded merchandise. These storefronts use product imagery lifted directly from legitimate sources and are localised in Spanish and Portuguese, indicating strong targeting of Latin American markets — particularly Brazil, Argentina, Mexico, and Colombia. Victims complete purchases by providing card details and shipping information (PII), then receive goods that are either counterfeit, materially inferior to what was advertised, or never shipped at all. The harvested PII, including card details, shipping addresses, and phone numbers, is sold downstream to carding marketplaces and scam-targeting databases.

Fraudulent betting and casino sites: Approximately 32 domains were identified operating unlicensed sportsbook and casino platforms that misuse FIFA branding to appear authorised. A notable sub-cluster uses Chinese-language interfaces to target Asian audiences. Victims who create accounts and make initial deposits find that winnings are never paid out and their deposits are stolen outright. More insidiously, these sites require KYC verification — passport scans, selfie photographs, and proof-of-address documents — which are then harvested and sold on dark-web markets for use in synthetic-identity fraud and fraudulent account opening at financial institutions.

Infostealer credential pipeline: The most pervasive but least targeted threat comes from mass infostealer campaigns, dominated by the Vidar and Lumma malware families. These infections are delivered through

cracked-software lures, malvertising networks, Telegram cheat and mod channels. FIFA credentials are harvested as incidental collateral rather than as a targeted objective — the stealers copy all browser-stored credentials, cookies, autofill data, session tokens, and cryptocurrency wallet seeds from every infected device. Group-IB investigation identified approximately 130,000 infostealer logs containing FIFA references.

Fraud Schemes Summary and Impact

Scheme	Direct Losses	Secondary Losses	Scale
Credential Phishing (Fake SSO)	FIFA account credentials; session cookies	Account takeover; unauthorised ticket transfers; identity theft; credential reuse	300+ domains
Fake Ticket Sales	Crypto payment (\$1,500–\$10,000+ per ticket)	No chargeback; registration PII harvested	\$71M–\$474M estimated (premium tier, ~25% of campaign)
Fake Streaming	Subscription fees; card data	Malware infection; full browser-credential theft	~55 domains
Counterfeit Merchandise	Card data; payment for counterfeit or undelivered goods	PII sold to carding markets and scam-targeting lists	~56 domains + Telegram channels
Fraudulent Betting	Stolen deposits; winnings never paid	KYC documents (passport, selfie) sold for synthetic-identity fraud	~32 domains
Infostealer Pipeline	Passwords, autofill, cookies, session tokens, crypto-wallet seeds	Corporate account pivot via SSO; MFA bypass via stolen session cookies	~130,000 logs; 2,513 credential pairs

Four Independent Threat Actors

Group-IB investigation identified four distinct threat actors operating across the fraud ecosystem targeting the FIFA World Cup 2026. These are not a single coordinated campaign but a convergence of independent operators exploiting the same high-profile event across different fraud vectors and platforms.

Threat Actor	Type	Status	Scale	Primary Schemes
GHOST STADIUM (TA-1)	Phishing kit operator	Active	300+ domains	Credential phishing; fake ticket sales
Pre-Registration Wave (TA-2)	Bulk domain squatter	Active	~143 domains	Fake streaming; counterfeit merch; fraudulent betting

Infostealer Operators (TA-3)	Mass malware campaigns	Ongoing	~130,000 logs	Credential theft (FIFA incidental)
Dark Web Kit Sellers (TA-4)	PhaaS vendor	Active from mid-2025	Multiple forum listings	Supply chain — enables TA-1, TA-2, and new entrants

The Coordinated Defence — Cyber Fraud Fusion in Action

The fraud ecosystem targeting the FIFA World Cup 2026 exposes a fundamental weakness in the way organisations currently defend against large-scale fraud campaigns: **siloed response**. When one phishing website is taken down, hundreds more remain operational and thousands are parked awaiting activation. When one bank flags a suspicious cryptocurrency address, other payment channels remain untouched and other financial institutions remain unaware. Sporting organization brand protection teams, the banks and crypto exchanges processing payments, the social media platforms distributing the ads, and law enforcement agencies all hold fragments of the picture — but no single institution holds the complete view. The result is that response happens domain by domain, institution by institution, always behind the attacker’s deployment pace.

This is the problem that Cyber Fraud Fusion (CFF) is designed to solve. CFF is a unified framework that coordinates five interdependent capabilities — Digital Risk Protection, Threat Intelligence, Fraud Protection, the Cyber Fraud Intelligence Platform, and Investigation Services — into a single defence architecture that operates at the speed and scale of the campaign itself. Applied to the GHOST STADIUM operation, CFF transforms the defence from a sequence of isolated reactions into a coordinated, predictive response.

Scenario: Disrupting the GHOST STADIUM Campaign

Step 1: Detection — [Digital Risk Protection \(DRP\)](#)

The defence begins with the detection of a single GHOST STADIUM phishing domain. DRP’s continuous monitoring of social media, search engines, domain registrations, and web content identifies the fraudulent site through brand-impersonation signals. **Graph analysis** then expands this single detection into the full campaign infrastructure: one confirmed phishing domain reveals the 300+ connected domains through shared Meta Pixel IDs, the common Tawk.to Property ID, identical kit HTML fingerprints, and overlapping SSL certificates. DRP initiates automated takedown processes across the entire connected network while establishing ongoing monitoring of the approximately 3,800 parked domains for activation signals. Rather than playing whack-a-mole against individual domains, DRP maps and targets the infrastructure at the cluster level.

Step 2: Intelligence Enrichment — [Threat Intelligence \(TI\)](#)

TI enriches DRP’s detection with deep infrastructure analysis. The team profiles the GHOST STADIUM phishing kit — the Layui framework, the cloned PingIdentity SSO, the Chinese-language source code artefacts — and maps the full operational footprint. TI monitors dark-web markets for the 2,513 compromised FIFA credential pairs, tracking their availability and identifying downstream buyers. The team analyses the threat actor’s TTPs, maps the five payment channels to their financial endpoints, and monitors the Phishing-as-a-Service supply chain

for new kit variants or emerging operators. TI's intelligence output feeds directly into Fraud Protection and CFIP for operational action.

Step 3: Ecosystem Alert and Fund Interception — [Fraud Protection \(FP\)](#) and [CFIP](#)

The flagged indicators generated by DRP and enriched by TI are distributed to member institutions in real time through the **Cyber Fraud Intelligence Platform (CFIP)**. Cryptocurrency wallet addresses associated with ChainUGO payment flows are shared with member exchanges, enabling deposits to threat-actor wallets to be frozen before funds are moved. Payment channel indicators — the specific cashtags, Nequi account numbers, FIXYD payment rails, and Alchemy Pay endpoints identified in the research — are distributed to the relevant payment providers and banks. FIFA's account security team receives compromise signals for the 2,513 credential pairs identified in dark-web listings, enabling proactive account protection — forced password resets, session invalidation, and enhanced monitoring — before any buyer acts on the stolen credentials. CFIP's strength is its reach: a detection at one institution becomes an alert at all participating institutions simultaneously, closing the gaps that the attacker exploits when institutions work in silos.

Step 4: Attribution — Investigation

While DRP, TI, FP, and CFIP work to detect, prevent, and disrupt the campaign in real time, the Investigation team pursues the individuals behind GHOST STADIUM. The leaked ChainUGO API credentials, the Tawk.to operator account, the Meta Pixel advertising accounts, and the GNAME.COM registrar records all provide investigative starting points. Cryptocurrency tracing maps the flow of victim payments from ChainUGO through intermediary wallets to cash-out points at KYC-compliant exchanges, where account holder identities can be established. The evidence package — combining kit forensics, infrastructure mapping, financial flow analysis, and identity attribution — is built to a standard suitable for law enforcement referral and prosecution.

Outcome

With CFF, a single phishing detection triggers a cascade: 300+ connected domains identified and targeted for takedown; 3,800 parked domains under monitoring; cryptocurrency wallets flagged across member exchanges; payment channels disrupted across five identified rails; 2,513 compromised accounts proactively secured; and the operator's identity under active investigation. The campaign is disrupted at infrastructure, financial, and human levels simultaneously — not one domain at a time, but at the speed and scale of the campaign itself.

Why Fusion Matters

No single capability is sufficient against the scale of a fraud ecosystem such as the one targeting the FIFA World Cup 2026. DRP alone can take down domains, but cannot intercept payments or identify operators. TI alone can map infrastructure, but cannot freeze funds or alert financial institutions. FP alone can flag transactions, but cannot take down the phishing pages that drive them. Investigation alone can identify individuals, but cannot prevent losses in real time. It is only when these capabilities operate as a unified system — each team's output feeding the next team's input — that the defence matches the architecture of the attack. Four independent threat actors, six parallel fraud schemes, and over 4,300 domains demand a defence that is coordinated, predictive, and operates at ecosystem scale. That is what Cyber Fraud Fusion delivers.

Conclusion

The fraud ecosystem targeting the FIFA World Cup 2026 has already been fully operational months before the opening match. Four independent threat actors have deployed six distinct fraud schemes across more than 4,300 fraudulent domains impersonating FIFA's official web presence, with GHOST STADIUM's sophisticated phishing campaign at the centre. The scale of the infrastructure — 300+ active phishing domains, 3,800+ parked domains awaiting activation, 2,513 compromised credentials in dark-web circulation, and an underground supply chain feeding new operators into the ecosystem — means the threat will intensify as the tournament approaches and peak during the June 11 to July 19 match window.

The research demonstrates that this is not a problem that can be solved by any single institution working alone. Brand owners may struggle to take down every impersonated domain. Banks may not be able to freeze every payment channel. Law enforcement cannot investigate every operator. The speed, scale, and multi-channel nature of the campaign demand a coordinated response — a defence architecture that mirrors the scale and interconnection of the attack itself. The Cyber Fraud Fusion framework provides that architecture, connecting detection, intelligence, prevention, ecosystem-wide alerting, and investigation into a unified system that predicts and disrupts fraud before losses occur. The time to deploy that defence is now.

Recommendations

For End Users and Fans

- Purchase tickets **exclusively** through the official FIFA ticketing portal at fifa.com. Any ticket offer outside this portal should be treated with extreme caution.
- **Treat any FIFA ticket offer requiring cryptocurrency payment as fraud.** The official FIFA ticketing portal does not accept cryptocurrency.
- Verify the exact domain spelling before entering any credentials. The official domain is fifa.com — never fifa-com.*, www-fifa.*, or any hyphenated or alternative TLD variant.
- **Enable multi-factor authentication (MFA)** on your FIFA account immediately. If you have not changed your password recently, do so now.
- Do not click on FIFA ticket ads on Facebook, Instagram, Telegram, or WhatsApp. Legitimate ticket sales are conducted only through FIFA's official channels, not social media advertising.
- If you have already entered credentials on a suspicious site, change your FIFA account password immediately, review your account for unauthorised ticket transfers, and contact your bank or payment provider if you made a payment.

For Brand Protection Teams

- Request takedown of the identified domains through abuse channels at GNAME.COM PTE. LTD. (primary registrar, 57% of the cluster) and Cloudflare.
- Report the three Meta Pixel IDs (927432823410218, 1842358649811605, 1569148414168343) and the Tawk.to Property ID (6976ccbaba77e8198a866266) to Meta and Tawk.to respectively for account suspension.

- Monitor the approximately 3,800 parked domains for activation signals, particularly during the June–July tournament window.
- Proactively secure the 2,513 compromised FIFA account credential pairs identified in dark-web markets through forced password resets and enhanced monitoring.

For Financial Institutions, Payment Providers, and Crypto Exchanges

- Flag and monitor the cryptocurrency wallets, ChainUGO API endpoints, and payment channel identifiers listed in the IOC appendix.
- Integrate with the **Cyber Fraud Intelligence Platform (CFIP)** for real-time, cross-institutional sharing of fraud indicators tied to the fraud campaign targeting the FIFA World Cup 2026.
- Alert on transactions routed through the five identified payment channels (direct card capture, third-party gateways, P2P apps, region-specific rails, and crypto on-ramp processors).

For the Cybersecurity Ecosystem

- Deploy **Digital Risk Protection (DRP)** for continuous monitoring and automated takedown of brand-impersonation infrastructure at scale.
- Leverage **Threat Intelligence (TI)** for phishing kit fingerprinting, dark-web credential monitoring, and threat actor profiling.
- Adopt **CFIP** for privacy-preserving, real-time intelligence sharing across financial institutions, payment providers, and cryptocurrency exchanges.
- Engage **Investigation Services** to trace the financial flows and identify the individuals behind fraud operations such as GHOST STADIUM.

Acknowledgement of research support:

- Cristián Espinoza Sinsay – CERT Analyst
- Hans Figueroa – Senior CERT Analyst
- Julio David Trigo Medina – Junior CERT Analyst

Frequently Asked Questions (FAQ)

1. What are the six main fraud schemes observed in this blog?

arrow_drop_down

The six parallel fraud schemes targeting football fans are:

- [Credential phishing](#) (via fake Single Sign-On clones)
- Fake ticket sales (targeting premium and hospitality tiers)
- Counterfeit merchandise storefronts (selling fake branded gear)
- Fake streaming platforms (charging subscription fees or delivering malware)
- Fraudulent betting and casino sites (operating unlicensed sportsbooks)
- Infostealer-driven credential theft (harvesting account data via malware)

2. What tactics are used by the fraudsters?

arrow_drop_down

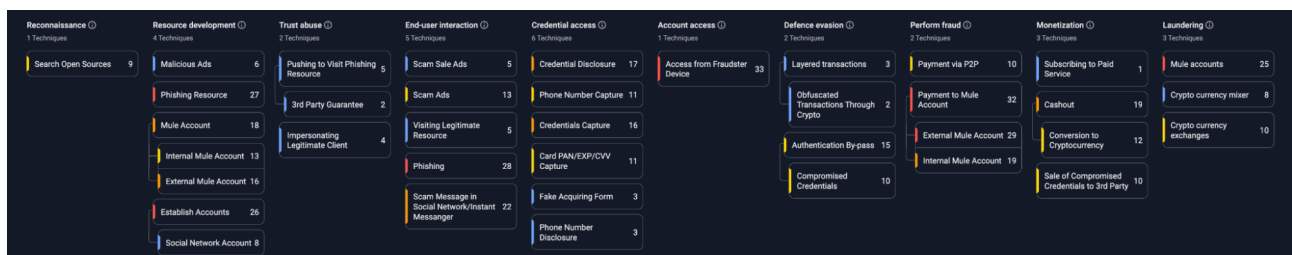
- [Brand Impersonation](#) through pixel-perfect web presence and SSO cloning.
- Social media (Facebook) ad network exploitation.
- Multi-channel communication through Telegram and WhatsApp channels, and embedded Tawk.to live chats on scam pages.
- Diverse payments using direct card capture, external third-party gateways, peer-to-peer apps (Chime, Nequi), region-specific payment rails (FIXYD), and crypto on-ramps (Alchemy Pay) to maximize conversion and obscure funds.
- Search engine poisoning by registering typosquat and themed domains to rank organically alongside legitimate listings.
- Underground supply chain with ready-made Phishing-as-a-Service (PhaaS) kits, automated bots, and templates from dark web forums to easily deploy fraud infrastructure.

3. How are victims affected?

arrow_drop_down

- Direct financial loss due to fake ticket sales, betting deposits, streaming subscriptions and counterfeit merchandise, with zero delivery and no recourse.
- [Account takeover](#) of legitimate FIFA credentials, which are then resold by the attackers.
- Identity theft from exposing sensitive PII on phishing sites and fake checkout process, which are then resold by fraudsters on the [dark web](#) and used in other fraud schemes.
- Device compromise with malicious infostealers or

Group-IB Fraud Matrix



Indicators of Compromise (IOCs)

Partial IOCs are listed in the blog; Group-IB customers can access the full list of IOCs from our complete [Fraud Intelligence report](#).

IOC-1: GHOST STADIUM — Credential Phishing + Fake Ticket Sales (Crypto)

Type	Value
------	-------

<i>Tawk.to live-chat property</i>	<i>6976ccbaba77e8198a866266</i>
<i>Meta Pixel #1</i>	<i>927432823410218</i>
<i>Meta Pixel #2</i>	<i>1842358649811605</i>
<i>Meta Pixel #3</i>	<i>1569148414168343</i>
<i>Cloned FIFA SSO client_id</i>	<i>35072598-fc20-4142-a469-1b940db47e6f</i>
<i>Crypto gateway</i>	<i>ChainUGO (testnet.chainugo.com)</i>
<i>Adjacent backend</i>	<i>www[.]fifa[.]show</i>
<i>Facebook Ad ID</i>	<i>1874578493179313</i>
<i>Facebook Ad ID</i>	<i>1214564190491246</i>
<i>Facebook Ad ID</i>	<i>929714589420716</i>

GHOST STADIUM Core Domains (representative sample of 79)

- *fifa[.]bio*
- *fifa[.]center*
- *fifa[.]gold*
- *fifa[.]red*
- *fifa[.]sale*
- *fifa[.]shopping*
- *fifa[.]show*
- *fifa[.]ski*
- *fifa[.]black*
- *Fifa[.]cafe*
- *fifa[.]fund*
- *fifa[.]market*
- *fifa[.]tax*
- *fifa[.]cash*
- *fifa[.]city*

- *Fifa[.]house*
- *fifa-com[.]co*
- *fifa-com[.]com*
- *fifa-com[.]shop*
- *fifa-com[.]site*
- *fifa-com[.]store*
- *fifa-com[.]website*
- *fifa-com[.]xyz*
- *fifa-com[.]vip*
- *fifa-com[.]top*
- *www-fifa[.]com*
- *www-fifa[.]co*
- *www-fifa[.]me*
- *www-fifaworldcup[.]com*
- *wc26-fifa[.]com*
- *fifa-26-worldcup[.]com*
- *fifaweb[.]com*

Hosting IPs (14 nodes)

- *148.178.18[.]23*
- *148.178.18[.]60*
- *154.86.0[.]33*
- *207.56.1[.]93*
- *66.112.212[.]25*
- *148.178.16[.]48*
- *148.178.16[.]5*
- *104.225.235[.]49*

- 89.208.250[.]38
- 65.49.223[.]138
- 148.178.22[.]16
- 85.121.242[.]41
- 216.189.149[.]193
- 137.220.224[.]67

IOC-2: Multi-Rail Fake Ticket Sales

Type	Value
Chime cashtag	\$Paramjit-Bains
Nequi account	3202059757
Regional rail domain	mm-fifa[.]top (FIXYD Mexico Payment)
Crypto on-ramp	Alchemy Pay
Redirector domain	football-ticket[.]top
Redirector domain	football-ticket[.]shop
Redirector domain	football-game[.]shop
Redirector domain	football-tickets[.]top
SSL fingerprint	3b8bb7631b39f455d31544b55ba97b49ab1888c1
SSL fingerprint	84ecdca915f1af822ccc8a04479f5179104f353c
SSL fingerprint	9bd164dd3f50d196c7dff4f6c1b0f1345ac96d9a

IOC-3: Real Payment Gateway Redirect (160+ Domains)

Type	Value
Entry domain	fifa-tickets[.]vip/tickets_shop
Login capture	fifa-tickets[.]vip/authorize[.]html
Payment order	fifa-tickets[.]vip/pay/FWC20260418A3230F12AC
Payment gateway abused	billplz[.]com
Example bill	www[.]billplz[.]com/bills/6e88393d1b82ede9

URL parameter signature	?aedda9bb-276d-49d4-92e8-294903503419/Design-ohne-Titel-1
-------------------------	---

Domain Naming Patterns to Avoid

Any domain matching these patterns and offering FIFA tickets, streaming, merchandise, or betting should be treated as potentially fraudulent:

- *fifa-com[.]{any TLD}*
- *www-fifa[.]{any TLD}*
- *www-fifaworldcup[.]{any TLD}*
- *fifa{word}[.]{any TLD}*
- *{word}fifa[.]{any TLD}*
- *vis-fifa[.]{any TLD}* (impersonates the real [vis.fifa.com](https://www.fifa.com))
- *fifa2026tickets{city}[.].com*
- *{city}unitycup2026[.].com*

Commonly abused TLDs: .com .online .shop .store .football .xyz .vip .top .icu .one .city .co .website .app

DISCLAIMERS:

The threat actor profile and attribution findings in this report are based on Group-IB technical analysis conducted between March 2026 to May 2026. All IOC data has been reviewed to protect the identities of victims; any remaining personal identifiers have been shared with law enforcement and are not reproduced here.

All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

This blog may reference legitimate third-party services such as Facebook, Telegram and others, solely to illustrate cases where threat actors have abused or misused these platforms.

This material is provided for informational purposes, prepared by Group-IB as part of its own analytical investigation, and reflects recently identified threat activity.

All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.