PLANET NINE

The FIFA Gold Rush: From Phishing to Gambling Across 8,832 Domains

June 2026

Important Notice

Planet-Nine Ltd. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any Planet-Nine product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any Planet-Nine products. Information in this document is subject to change without notice and does not represent a commitment on the part of Planet-Nine. The products and/or systems described in this document are furnished under a license agreement or non-disclosure agreement.

Table of Contents

1. Key Findings

THE FBI WARNING	ORION FINDINGS	THE REALITY	BEYOND PHISHING	THE UNKNOWN 60%
May 27, 2026: FBI warns of FIFA-themed phishing, fake ticketing sites, and domain impersonation. Roughly three dozen domains identified, with "many more" expected.	ORION, Planet Nine's AI-powered domain platform, scans new registrations in real time and scores each one for maliciousness in advance.	"Many more" was an understatement. In May 2026 alone, ORION identified 8,832 FIFA-themed domains.	ORION uncovered a diverse ecosystem of malicious FIFA-themed domains, including gambling networks, impersonation campaigns, ticketing scams, and recruitment fraud.	Nearly 60% of FIFA-themed domains remained inactive or unreachable. Some may prove benign, while others could be activated for fraud, impersonation, or other forms of abuse as the tournament approaches.

8,832 total FIFA-themed domains identified by ORION in May 2026

31%	**MALICIOUS**	≈ **2,700 domains** — actively malicious or tied to phishing, fraud, and other forms of abuse.
9%	**Safe**	≈ **800 domains** — appear legitimate, with no malicious indicators at registration.
60%	**Inactive / Unreachable**	≈ **5,300 domains** — insufficient data to classify. Many are inactive or under construction.

Nearly 60% of FIFA-themed domains remained unclassified. Many were inactive or under construction, highlighting the scale of World Cup-related infrastructure already in place. Dormant today does not mean safe tomorrow.

2. Overview

On May 27, the FBI's Internet Crime Complaint Center published PSA I-052726, warning that threat actors are spoofing the official FIFA website ahead of the 2026 World Cup – typosquats, alternative TLDs, fake ticket and hospitality sellers, and phishing pages built to harvest personal and banking data. The FBI named roughly three dozen domains and said to expect many more.[1]

"Many more" turned out to be an understatement. *ORION*, Planet Nine's AI-powered domain analysis platform, is built to get ahead of attacks at scale. It scans the global stream of newly registered domains the moment they appear and scores each one for maliciousness in advance – flagging threats across entire campaigns before they strike. In May 2026 alone, **ORION identified 8,832 FIFA-themed registrations. The FBI's list is only a small sample of the broader activity.**

The FBI's advisory highlights some of the most concerning risks associated with FIFA-themed domains, particularly phishing and fraud. ORION's broader dataset, however, shows that these domains are being used for a much wider range of activities. Across thousands of FIFA-themed registrations, we observed a large ecosystem of operators leveraging World Cup branding to drive traffic to gambling platforms, betting affiliates, promotional campaigns, and other forms of opportunistic monetization.

Of the 8,832 FIFA-themed domains identified by ORION during May 2026, 31% were classified as malicious, 9% as benign, and nearly 60% remained unclassified (OOD). A large portion of the OOD domains were inactive or under construction, highlighting the scale of World Cup-related infrastructure already registered ahead of the tournament.

[1] https://www.ic3.gov/PSA/2026/PSA260527

3. The Dominant Cluster: Chinese-Language Gambling

The largest category we observed consists of Chinese-language domains leveraging World Cup branding to drive traffic to gambling platforms, betting services, and livestreaming sites. The naming conventions are remarkably consistent: maiqiu (买球, football betting), jingcai (竞彩, sports lottery), shijiebei (世界杯, World Cup), peilv (赔率, odds), zhibo (直播, livestream), alongside countless combinations of terms such as “odds,” “bet,” “lottery,” “guess,” and “predictor.”

One brand appears frequently enough to warrant separate attention: *Kaiyun*, a brand referenced across numerous FIFA-themed registrations. We identified a domain cluster that impersonates both FIFA and Kaiyun directly, including fifa-kaiyungame[.]com[.]cn, kaiyun-fifa[.]com, main-kaiyun-fifa[.]com, and cn-fifa-kaiyunsports[.]com. Several of the live sites we reviewed also displayed what appeared to be impersonations of Kaiyun alongside FIFA-related imagery and trademarks.

A representative example is china-hans-2026fifa[.]com, a Chinese-language World Cup–themed portal promoting several unlicensed betting operators while prominently featuring impersonated Kaiyun branding and falsely claiming FIFA certification. We identified a gated JavaScript payload (link.js) on the domain that silently redirects visitors to gambling registration pages containing affiliate tracking codes, demonstrating that the site is actively monetizing World Cup-related traffic. Rather than appearing as an isolated registration, **the site forms part of a larger infrastructure cluster. Using ORION’s Domain Similarity Engine, we identified 52 additional FIFA-themed domains registered on May 2026 that share the same visual design and branding patterns. All 52 were independently classified as**

malicious by ORION, further supporting the assessment that these domains are part of a coordinated campaign.

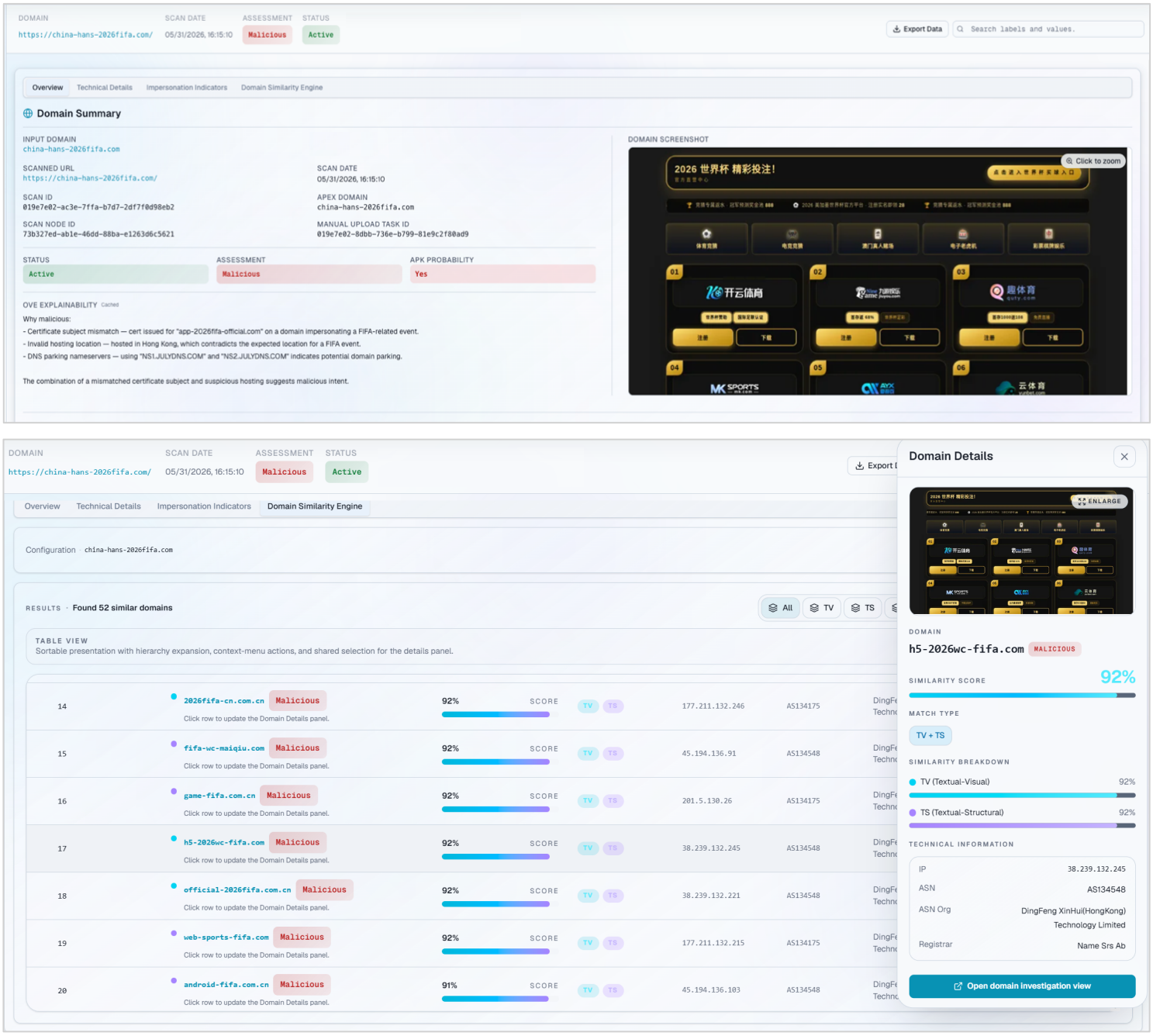

Figure 1: ORION investigation page for china-hans-2026fifa[.]com, showing a FIFA-themed betting portal and a cluster of visually similar domains identified by ORION's Domain Similarity Engine.

4. Fraudulent FIFA Services

The category most closely aligned with the FBI's warning involves domains masquerading as official FIFA properties. These registrations imitate ticket vendors, hospitality providers, merchandise stores, and other World Cup-related services in order to appear legitimate. The goal of such domains is typically to collect payments, personal information, and financial data from fans seeking official World Cup products and experiences. Examples in ORION's data include fifa-ticket[.]live, fifaworldcup26-hospitality[.]com, and mailticketsfifa[.]com.

A specific case is *fifatickets[.]vip*, a World Cup-themed ticketing website that prominently features FIFA 2026 branding alongside references to tournament venues, match schedules, and ticket availability. ORION flagged the site as malicious, illustrating how FIFA-related branding can be used to attract fans searching for tickets ahead of the tournament.

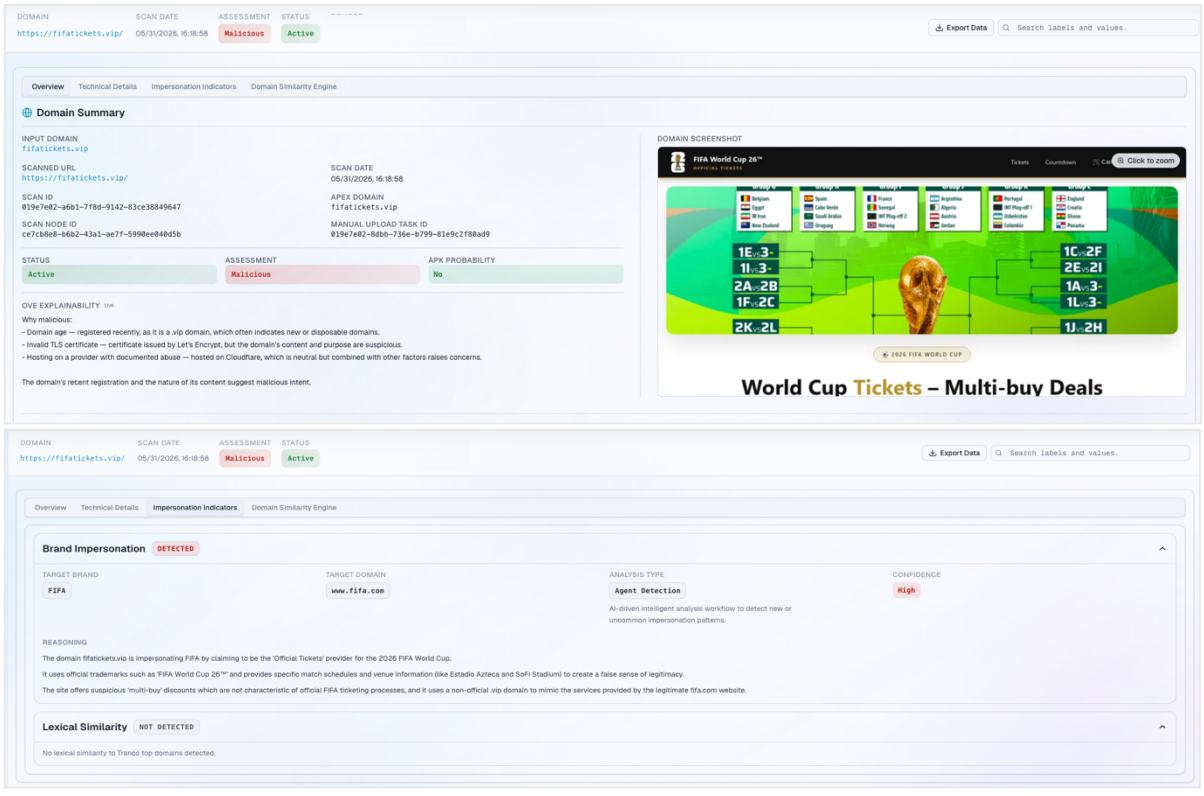

Figure 2: Snippet from ORION's investigation page for fifatickets[.]vip, including ORION's Brand Impersonation AI detection identifying the domain as a likely attempt to impersonate FIFA.

Another clear example is *fifagroup[.]shop*. This domain appears designed to mimic an official FIFA online store. ORION classified the domain as malicious at registration time, and the platform's Brand Impersonation AI model flagged it as a likely attempt to impersonate FIFA.

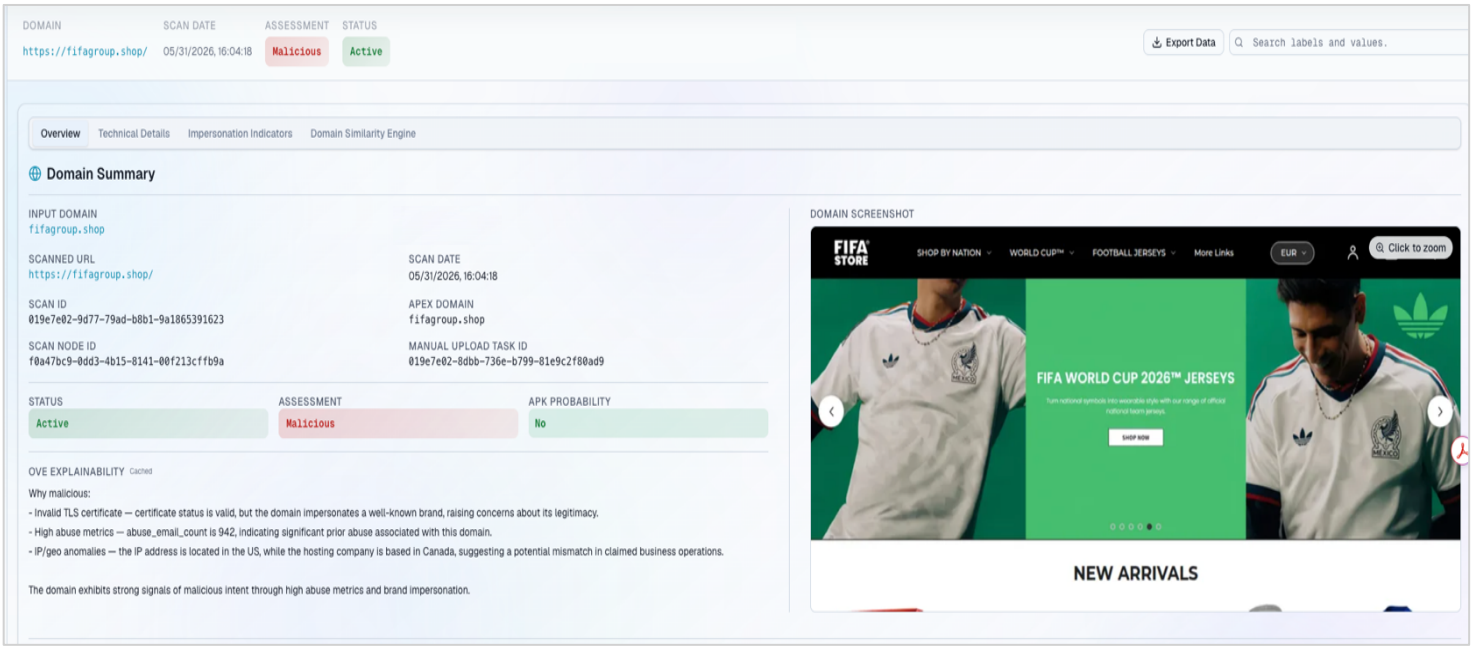

Figure 3: Snippet from ORION's investigation page for fifagroup[.]shop.

5. Recruitment Scams

ORION identified multiple FIFA-themed domains, including fifa-hr[.]com and fifa-careerhub[.]com, that appear designed to mimic official FIFA recruitment channels. In several cases, the sites displayed FIFA branding alongside scheduling pages inviting visitors to book meetings with purported recruiters. The combination of employment-related terminology, FIFA branding, and recruiter outreach appears intended to create the false impression of official FIFA or World Cup-related hiring opportunities. In one case, a purported recruiter whose details appeared on a FIFA-themed recruitment site publicly disclosed on LinkedIn that her identity had been

abused by threat actors as part of phishing activity. This suggests that at least some of these sites may be leveraging the identities of real individuals to enhance their credibility.

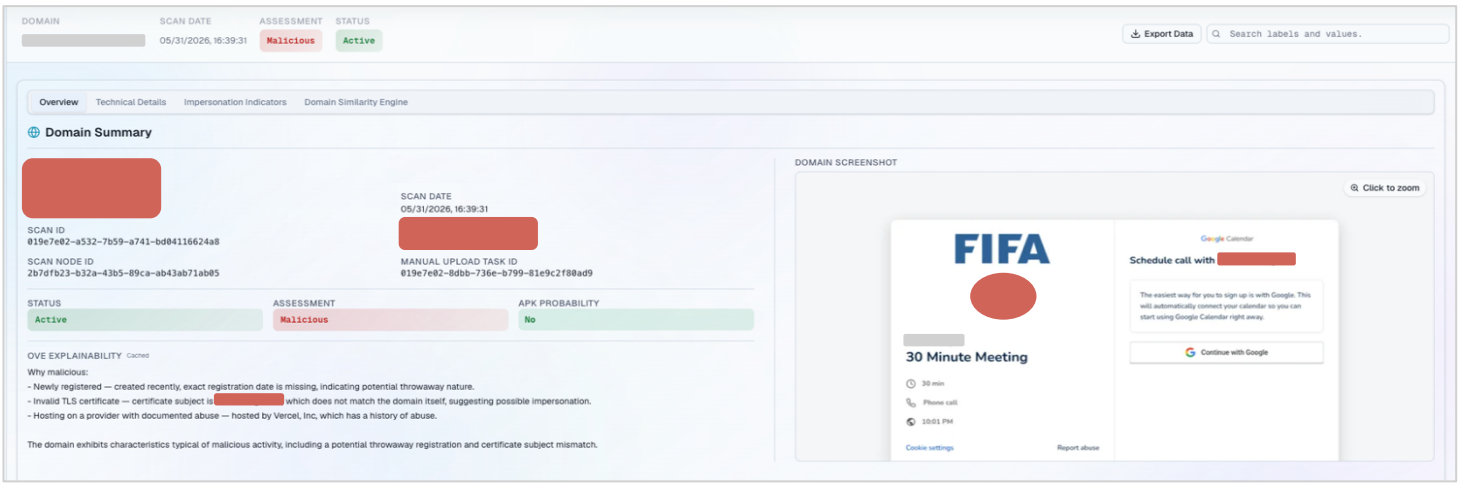

Figure 4: Snippet from ORION's investigation page for a FIFA-branded recruitment-themed website directing visitors to schedule a meeting with a purported recruiter.
Identifying information associated with the purported recruiter has been intentionally hidden for privacy reasons.

6. Typosquatting and Lookalikes

ORION also identified a collection of domains designed to exploit user mistakes and visual confusion. Examples such as fifah[.]top, fifa-com[.]org, and fifaiwoirlidcuip26[.]lol, mimic the FIFA brand through typographical variations, character substitutions, and deceptive naming patterns. The activity extends beyond traditional typosquatting into the use of alternative and uncommon TLDs, including .lol, .live, .store, .futbol, and others, that can lend an appearance of legitimacy while helping operators register large numbers of FIFA-themed domains. While the ultimate purpose of these registrations is not always apparent at registration time, such techniques are commonly used to capture traffic from users attempting to reach legitimate FIFA-related websites and services.

7. Most are Quiet – for Now

A large share of the FIFA-themed domains identified by ORION are currently inactive, parked, displaying maintenance pages, or sitting behind generic "under construction" placeholders. Nearly 60% of the 8,832 FIFA-themed registrations analyzed in May fell into ORION's Out-of-Distribution (OOD) category, indicating that their purpose could not yet be confidently determined. **That should not be mistaken for safety**. Dormant infrastructure is a common feature of event-driven campaigns, where domains are registered weeks or months in advance and activated only when public interest reaches its peak.

With the 2026 World Cup still weeks away, many operators have little incentive to deploy their infrastructure today. The closer the tournament gets – and the more fans begin searching for tickets, jobs, livestreams, betting platforms, and tournament information – the more valuable these domains become. History shows that major global events routinely attract waves of opportunistic registrations seeking to capitalize on that surge in attention.

Some of these domains may never become active. Others, however, could be repurposed for betting promotions, brand impersonation, fraudulent ticket sales, phishing campaigns, or other forms of abuse. **The key takeaway is that the threat is not limited to the domains already online. Thousands of FIFA-themed registrations are already in place, waiting for the moment when World Cup traffic begins to surge.**

8. Why this Matters Now

Major global events create a narrow window between the deployment of malicious infrastructure and the appearance of the first victims. The 8,832 FIFA-themed domains identified by ORION in May 2026 provide a view of that infrastructure before it becomes widely visible through user reports, takedown requests, or incident investigations.

Across the malicious set, ORION identified a clear concentration around gambling platforms, betting affiliates, and streaming services, alongside domains associated with brand impersonation, ticket sales, recruitment themes, and other forms of opportunistic monetization. With over 2,700 malicious domains registered in a single month, the findings illustrate the scale at which threat actors and opportunistic operators are already positioning themselves ahead of the 2026 World Cup.

For organizations responsible for protecting brands, customers, and users, including FIFA, sponsors, broadcasters, hospitality providers, and ticketing platforms, the most valuable signal is often found at the point of registration. By the time malicious domains surface in abuse reports or public investigations, the campaign is already underway.

ORION will continue monitoring the registration stream as the tournament approaches. If historical event-driven campaigns are any indication, this activity is unlikely to slow down.

Disclaimer: The findings in this post reflect ORION's automated analysis of newly registered domains as of May 2026. Classifications are based on signals available at the time of registration and may not reflect the current status, ownership, or intent of any domain referenced. Third-party brand names appear in this post solely to describe observed content on the analyzed domains; their inclusion does not imply that those brands are involved in, or responsible for, any of the activity described. Individuals whose identities appear to have been misused on the analyzed domains are referenced as victims of impersonation, not as participants.