TICKET TO RIDE

Assaf Morag *investigates as mobile malware meets its newest hook, the World Cup*

Major global sporting events have long evolved far beyond moments of athletic excellence. Today, they represent massive digital ecosystems where commerce, entertainment and technology intersect at scale. With billions of viewers, intense emotional engagement, and urgent, time-sensitive demand for tickets, streams and betting opportunities, events like the FIFA World Cup 2026 create ideal conditions not only for legitimate business but also for cybercrime.

Attackers understand this dynamic well. They exploit the convergence of excitement, hype, scarcity, and trust to build highly effective campaigns that blur the line between legitimate services and malicious operations.

We recently carried out research focused on the lure infrastructure, which is a critical stage in the attack chain. It is structured from websites, landing pages and distribution mechanisms designed to attract users and guide them toward downloading mobile applications that may ultimately deliver malware, facilitate fraud or enable unauthorised data collection. While attention is often given to the malware itself, the infrastructure that precedes it is equally important. It is where psychological manipulation, branding abuse and technical evasion techniques come together to convert curiosity into compromise.

Our findings reveal a complex and evolving ecosystem of campaigns leveraging football-related themes, betting incentives and even emerging technologies like cryptocurrency. These campaigns range from regionally targeted operations to massive global infrastructures, which are designed with a common goal: to move users from relatively controlled web environments into mobile applications where attackers gain greater control and visibility.

One of the most prominent campaigns identified in the research is a large-scale APAC-focused operation consisting of dozens of distinct IP addresses, all geolocated in Hong Kong and hosting identical Chinese-language templates. At first glance, these sites appear simple, even unsophisticated. However, their design reflects a deep understanding of user behaviour and defensive mechanisms. Upon visiting the site, users are redirected to an intermediate page that immediately introduces a sense of urgency and control.

Attackers build highly effective campaigns that blur the line between legitimate services and malicious operations

The messaging on these pages is particularly telling. Users are warned about potential risks such as hijacking or losing access and are strongly encouraged to download a mobile application as a "protective" measure. Ironically, the very solution presented as a safeguard is the primary infection vector. The page also recommends saving screenshots of the domain for future access, subtly reinforcing persistence while acknowledging that domains may frequently change or be blocked.

This behaviour reveals the underlying resilience strategy of the infrastructure. Rather than relying on a single domain, the campaign uses rotating domains, disposable top-level domains such as .vip, and multiple entry points to ensure continued availability. Even if individual domains are taken down, the overall system remains operational. The inclusion of polished user interface elements, browser recommendations and even contact details contributes to the illusion of legitimacy, making it more likely that users will comply with the instructions.

As users progress through the flow, they encounter more refined and visually appealing landing pages. These pages are designed to resemble legitimate sports or betting applications, often incorporating recognisable football imagery and claims of official partnerships. The goal is not just to attract attention, but to establish trust quickly and push users toward immediate action.

The use of global football icons, combined with promises of high returns, bonuses and exclusive access, creates a powerful psychological trigger. Users are not just being offered an app. No… they are being invited into what appears to be a legitimate, high-reward ecosystem tied to a globally recognised event. This blending of emotional engagement and financial incentive is a hallmark of modern cybercriminal campaigns.

From a technical and operational perspective, these campaigns are highly scalable. While the language and certain elements target Chinese-speaking users, the core infrastructure can be easily adapted for different regions. By changing language packs, imagery and domain names, the same backend system can support campaigns across multiple geographies. Distribution channels such as piracy websites, messaging platforms and malvertising networks further amplify reach, creating a continuous funnel of potential victims.

In parallel, we identified another infrastructure consisting of a couple of dozen IP addresses associated with a newly registered domain, aiyouxisport[.]com[.]cn. Unlike the previous campaign, this one presents a more ambiguous case. The website uses a consistent Chinese-language template and appears to promote a sports-tech platform associated with AYX, a company positioned in the sports data and entertainment space.

At face value, the platform offers data-driven content such as match statistics and interactive features, which are common in legitimate sports-tech ecosystems. However, deeper inspection reveals strong overlaps with betting-related infrastructure. Domains linked to the same template often redirect users to gambling platforms, featuring typical incentive structures such as large bonuses and promotional offers tied to major tournaments like the UEFA Champions League.

The ambiguity of this infrastructure is precisely what makes it noteworthy. It sits at the intersection of legitimate business, gray-market activity, and potential cybercrime. The association with known football clubs through past partnerships adds a layer of credibility that can be exploited. Users encountering such platforms may not perceive them as suspicious, especially when the branding aligns with real-world entities.

Further analysis uncovered additional behaviours that raise concern. Some landing pages within this ecosystem encourage users to download mobile applications while explicitly advising them to use devices that do not have certain fraud prevention tools installed. In particular, references to avoiding China's National Anti-Fraud Center application suggest an intent to bypass security controls, whether for malware delivery or to facilitate access to restricted gambling services.

WITH THEIR GLOBAL REACH, SPORTING EVENTS PROVIDE ONE OF THE MOST EFFECTIVE HOOKS

These instructions are not accidental. They indicate a deliberate attempt to guide users around protective mechanisms, effectively lowering the barrier to compromise. In some cases, users are even provided with step-by-step guidance on how to disable network protections or installation restrictions. This level of detail reflects a mature operational model where user onboarding is carefully engineered to maximise success rates.

When analysing one of the distributed APK files, we found that there's a minimal detection across security engines, with only a single vendor flagging it as potentially malicious or unwanted. This highlights another important aspect of these campaigns: evasion. Whether through obfuscation, staged payload delivery or simply operating in a gray zone that avoids clear classification, these applications can remain undetected long enough to achieve their objectives.

Beyond regionally focused campaigns, the research also identified opportunistic infrastructures that leverage global narratives such as cryptocurrency and fan engagement. One notable example is a fake "FIFA Crypto" application promoted through a dedicated website.

This campaign takes advantage of the growing interest in digital assets and the perception that major organisations are entering the cryptocurrency space. While there have been discussions about potential blockchain initiatives in football, there is no officially launched FIFA cryptocurrency. This gap between expectation and reality creates an opportunity for attackers to introduce fraudulent or malicious offerings under the guise of innovation.

The analysed APK associated with this campaign showed multiple detections as a mobile trojan, confirming its malicious nature. However, the broader significance lies in the infrastructure supporting it. By pivoting from this single sample, we uncovered a vast network of more than 600 IP addresses and thousands of domains, all following similar patterns. This infrastructure is not limited to football-themed lures. It supports a wide range of applications, including games, productivity tools and betting platforms, with the World Cup serving as just one of many entry points.

The scale and flexibility of this infrastructure highlights the industrialisation of mobile malware

distribution. Attackers are no longer building isolated campaigns. Instead, they operate platforms capable of generating and distributing malicious applications across multiple verticals, adapting quickly to trends and user interests. Sporting events, with their global reach and emotional resonance, simply provide one of the most effective hooks.

THE FINDINGS REVEAL A COMPLEX ECOSYSTEM OF CAMPAIGNS OFTEN RELATED TO FOOTBALL

What emerges is a picture of malicious convergence. Traditional cybercrime elements such as phishing, malware distribution and credential harvesting are intertwined with gray-market activities like offshore betting and unregulated financial services. At the same time, legitimate branding is being leveraged, sometimes indirectly, to enhance credibility and reduce suspicion.

This development creates significant challenges for defenders. The boundary between legitimate and malicious becomes vague, making it harder to apply traditional detection and enforcement strategies. A platform that appears to provide sports data may also serve as a gateway to gambling or malware. A crypto-related application may combine elements of fraud, speculation and outright malicious activity.

The mobile ecosystem further complicates the situation. Unlike web environments, where security controls such as browser protections and domain filtering are more mature, mobile applications (primarily Android) operate with broader permissions and fewer visibility points. Once installed, they can often access sensitive data, interact with other applications and maintain persistence in ways that are difficult for users to monitor or control.

For organisations operating in sectors such as sports, media, finance and digital services, these findings carry important implications. Brand abuse, user trust exploitation and indirect association with malicious campaigns can all have reputational and financial consequences. Even when an organisation is not directly targeted, its imagery, partnerships or services may be used as part of a broader attack narrative.

With the FIFA World Cup 2026 over, attackers will continue to refine their methods, leveraging new technologies and narratives to stay relevant and effective. The combination of global attention, digital engagement and economic opportunity ensures that this environment will remain a prime target.

Ultimately, the challenge is not just to respond to individual campaigns, but to understand the ecosystem as a whole. By examining how these infrastructures are built, how they evolve, and how they interact with user behaviour, it becomes possible to anticipate and disrupt future operations. In a landscape where cybercrime is increasingly professionalised and scalable, this level of insight is essential for staying ahead ●

Assaf Morag is a cybersecurity researcher at Flare. The company investigates the cybercrime ecosystem to help global organisations detect high-risk exposures on the clear and dark web.

Malware campaigns are designed to move users from relatively controlled web environments into mobile applications where attackers gain greater control and visibility