CHECK POINT

EXPOSURE MANAGEMENT

FIFA WORLD CUP 2026 CYBER THREAT REPORT

By Cris Esparza, Manasa Pisipati, Ruty Davidson

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The FIFA World Cup 2026 is driving a clear escalation in cyber threat activity across Financial Services, Transportation & Hospitality, and Gambling, as attackers exploit high transaction volumes, global visibility, and compressed decision windows. Across all sectors, threat actors are expected to combine disruption (DDoS), fraud, and influence activity, often activated at peak visibility moments to maximize operational and reputational impact.

FINANCIAL SECTOR

Financial ecosystems are seeing early-stage exploitation of event-driven demand. Crypto scams (e.g., $WORLDCUP-type tokens) are leveraging hype and thin legitimacy signals to attract capital before potential loss events. In parallel, card-not-present fraud and social engineering campaigns are replicating prior World Cup patterns, targeting ticketing, travel, and hospitality flows.

Weak email authentication across parts of the ecosystem increases exposure to BEC within complex supplier and sponsorship chains, where payment redirection can occur with limited verification. Elevated AML pressure and human-trafficking risk further strain monitoring capabilities, particularly near host cities. The combined effect is sustained fraud exposure, increased reimbursement liability, and regulatory scrutiny across payment-driven organizations.

TRANSPORTATION & HOSPITALITY

These sectors face concentrated operational risk as ransomware, data extortion, and identity-based intrusions target systems with near-zero tolerance for downtime. Recent attacks on airlines, hotels, and airports demonstrate how attackers prioritize credential abuse and social engineering to bypass traditional controls.

At the same time, hacktivist groups have already demonstrated the ability to disrupt travel-related services through DDoS campaigns timed to major events. Fan-facing fraud, particularly lookalike booking domains, is scaling rapidly, exploiting trusted brands at the point of purchase. Even short disruptions in reservation, booking, or operational systems can cascade into traveler disruption, safety concerns, and immediate reputational damage at a global scale.

GAMBLING SECTOR

The gambling ecosystem is entering the tournament with threat infrastructure already active. Large-scale registration of lookalike domains, combined with a sharp rise in fake mobile apps and Telegram-driven betting schemes, shows coordinated pre-positioning ahead of peak betting activity.

The gambling ecosystem is entering the tournament with threat infrastructure already active. Large-scale registration of lookalike domains, combined with a sharp rise in fake mobile apps and Telegram-driven betting schemes, shows coordinated pre-positioning ahead of peak betting activity. Affiliate abuse and unregulated operators are exploiting regulatory gaps and acquisition channels to capture users and funds. This directly undermines legitimate operators, driving brand erosion, regulatory exposure, and increased post-event disputes and chargebacks, particularly as compromised credentials and fraudulent promotions intersect during high betting volume.

FINANCIAL SECTOR

Key Findings

This section assesses the cyber threat landscape facing the financial sector in the run-up to and during FIFA World Cup 2026. It is built on three evidence streams collected by Check Point Research and Check Point Exposure Management between May 2025 and May 2026.

The FIFA World Cup 2026 is creating conditions that financial-sector threat actors are already exploiting. Online and cross-border transactions are surging across ticketing, travel, hospitality, merchandise, sponsorship, sports betting, mobile payments, and cryptocurrency. Threat actors are mobilizing infrastructure to exploit that activity at scale.

Key findings drawn from activity observed in the run-up to the tournament:

- Event-themed crypto scams are scaling. Tokens such as $WORLDCUP exhibit hallmarks of rug-pull and Ponzi-style schemes including opportunistic event-driven hype timing, thin liquidity, no identifiable team behind the project, the absence of independent security audits and any verifiable affiliation with FIFA making it difficult for investors to assess the project's legitimacy accountability and long-term credibility.

- Card-not-present and social-engineering fraud are the most likely consumer-facing threats. Fraudulent ticketing, travel, and hospitality sites harvest payment cards and banking credentials, repeating patterns documented at the 2022 FIFA World Cup and Paris 2024 Olympics.

- Business Email Compromise (BEC) exposure is elevated. Pre-tournament research found more than one-third of official FIFA WC 2026 partners lack sufficiently strong DMARC enforcement to prevent domain spoofing of their procurement and sponsorship chains.

- AML and human-trafficking risk is flagged at the federal level. FinCEN has warned that the tournament's visitor influx and cross-border money movement could be exploited by trafficking networks, raising compliance pressure on banks, money transmitters, fintech platforms, and casinos near host cities.

- Russia-aligned actors are the most operationally relevant cluster. NoName057(16), Killnet, Anonymous Sudan, Storm-1679, Storm-1099, APT28, and Midnight Blizzard combine DDoS, espionage, and AI-enabled influence operations. Iranian, Chinese, and North Korean actors operate at lower intensity but remain credible across espionage and financially motivated activity.

Why the Financial Sector Is at Such High Risk

International sporting events such as the Olympics and FIFA World Cup create favorable conditions for financial-sector targeting because they generate a sharp increase in online, cross-border, and time-sensitive transactions across ticketing, travel, hospitality, merchandise, and sponsorship activity. Demand is concentrated in narrow purchasing windows, urgency suppresses normal verification behavior, and consumers transact with unfamiliar merchants under unfamiliar branding.

The cryptocurrency sector faces particularly high exposure because attackers exploit public interest in sports-related digital assets, fan tokens, and NFTs. Fraudulent "FIFA Coin" projects, fake crypto investment opportunities, and World Cup-themed NFT schemes are being used to lure users into downloading malicious apps and engaging in financial scams, though no official FIFA coin has been launched. These operations frequently promise guaranteed returns, referral rewards, and daily profits tied to sports-themed crypto ecosystems, resembling classic Ponzi-style investment schemes. The combination of emotional fan engagement and speculative investment behavior leaves inexperienced investors more vulnerable to fraud and social engineering.

Business-to-business exposure is also quite high. Large-scale events involve complex procurement, sponsorship, and payment chains across sponsors, vendors, logistics providers, hospitality partners, and service contractors. High transaction volumes, urgency, and operational complexity weaken standard payment-verification processes, increasing exposure to manipulated invoices, fraudulent wire transfers, beneficiary-account redirection, and payment-approval fraud.

Finally, the tournament creates compliance pressure. The U.S. Department of the Treasury's Financial Crimes Enforcement Network has warned that the visitor influx and cross-border money movement could be exploited by criminal networks involved in sex trafficking and labor trafficking. Banks, casinos, money transmitters, fintech platforms, and payment processors operating near host cities face elevated anti-money laundering workloads.

Observed Threats Around the the World Cup

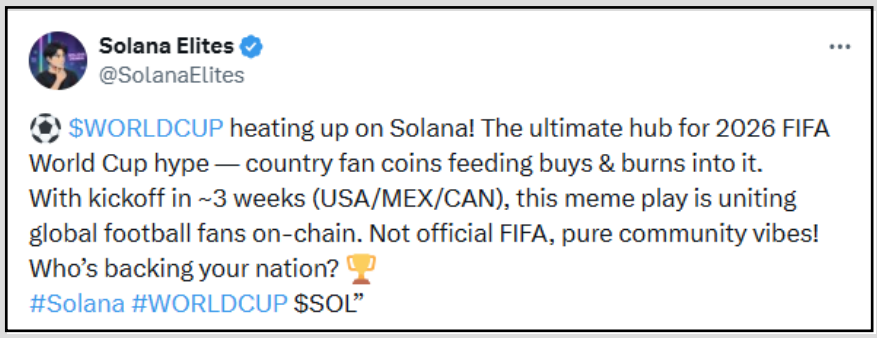
Crypto-themed scams

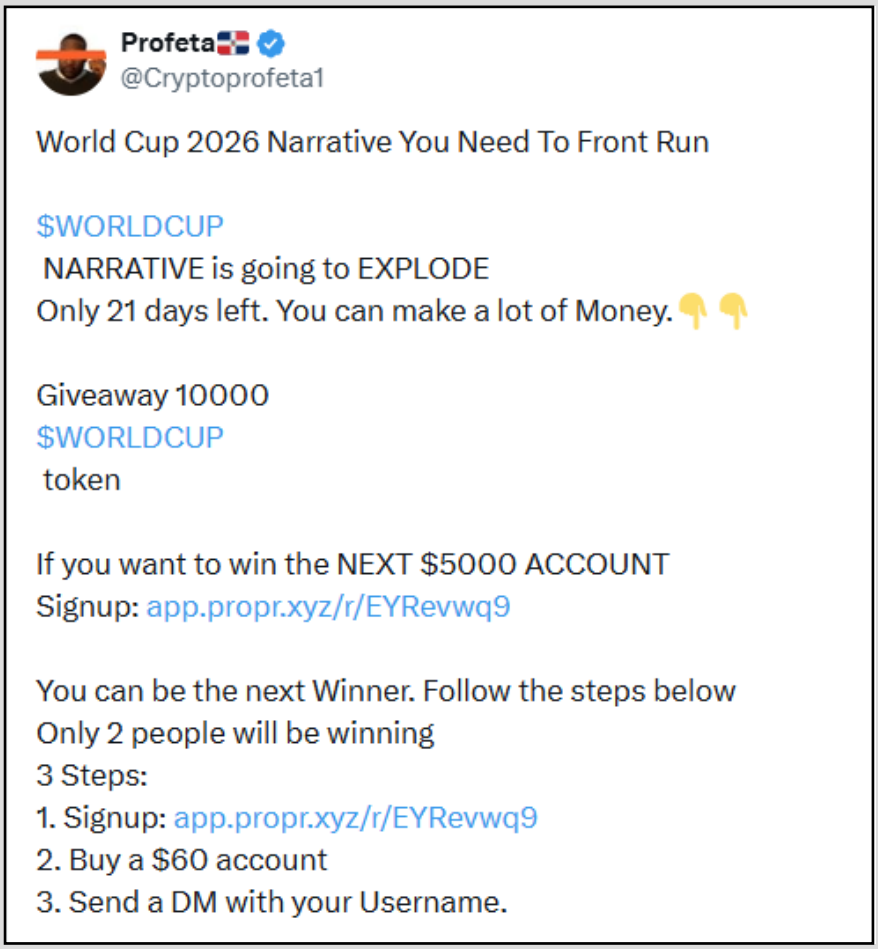
Event-themed cryptocurrency activity is one of the most visible financial threat categories in the lead-up to the World Cup. Promotional campaigns running on X and other social platforms heavily rely on urgency, exaggerated return projections, giveaways, and countdown narratives to pressure impulsive decisions. The pattern is well established at prior mega-events and has been observed to repeat in 2026.

$WORLDCUP

The $WORLDCUP token has generated significant discussion on X. It exhibits multiple characteristics commonly associated with high-risk speculative assets or potential fraudulent schemes rather than a legitimate investment vehicle and exemplifies the broader wave of meme coins seeking to capitalize on the excitement surrounding the tournament.

Launched in mid-May 2026, just weeks before the tournament, the project appears designed to exploit global event-driven hype. Such opportunistic timing is a recurring pattern in sports-related crypto scams, where rapid price inflation attracts retail investors before potential liquidity withdrawal or large-scale sell-offs occur, often resulting in substantial investor losses. Several X posts are seen promoting the $WORLDCUP token, although it is unclear whether the individuals promoting it are doing so knowingly or unknowingly.





Figures 1 and 2. X posts promoting the $WORLDCUP cryptocurrency, using language and messaging patterns commonly associated with crypto-scam campaigns (urgency, giveaway funnels, nation-themed FOMO).

$WORLDCUP

Market indicators indicate high risks: thin liquidity relative to peak market capitalization, which facilitates price manipulation; sharp, volume-driven price surges that appear engineered to trigger Fear of Missing Out among retail participants. Critically, $WORLDCUP lacks standard markers of legitimacy: no identifiable development team, no independent security audit, no clearly defined utility, no transparent roadmap, and no official connection to FIFA or the World Cup organizing bodies. The absence of institutional oversight increases vulnerability to fraud, including potential phishing through associated links.

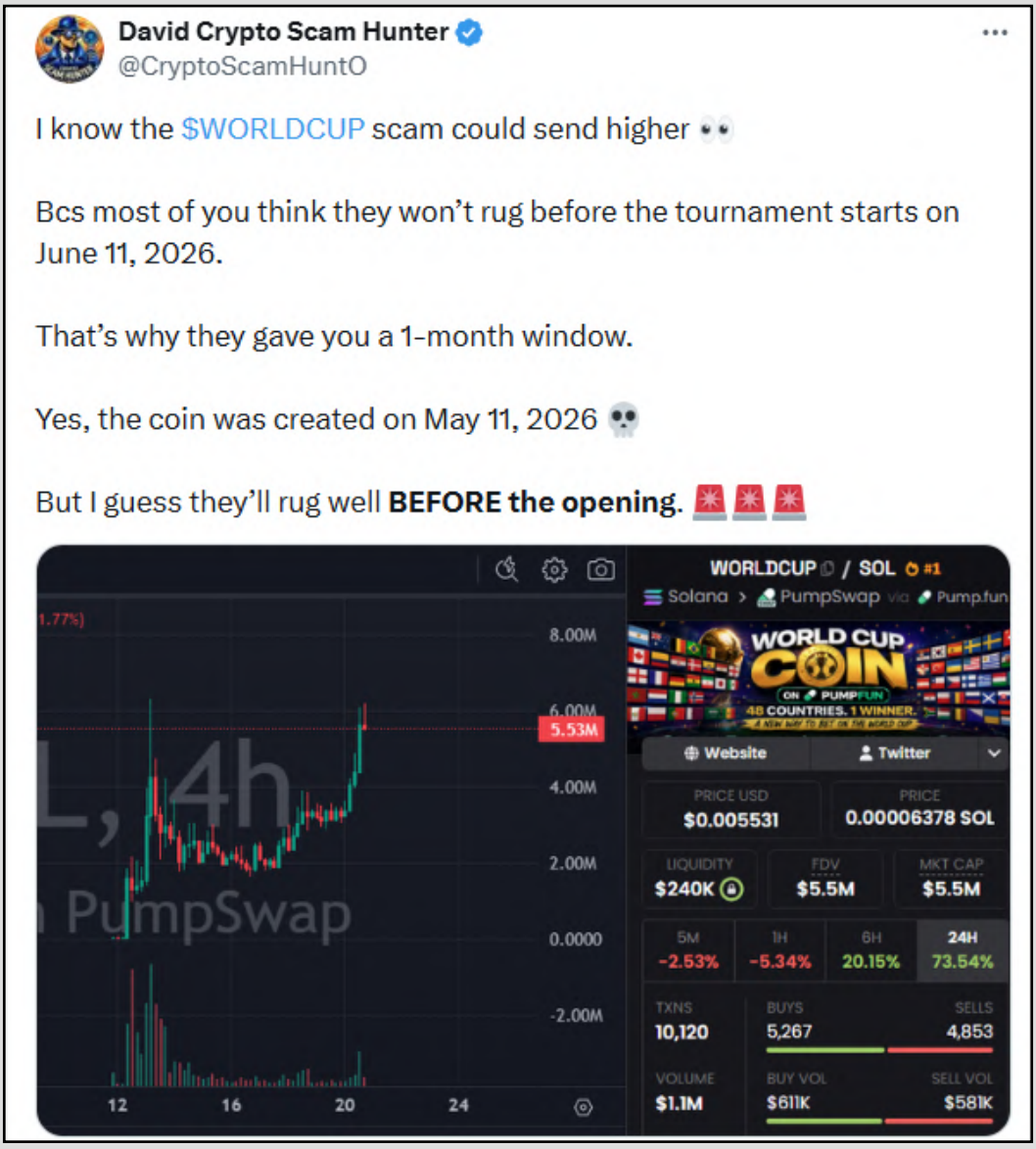


Figure 3. X post by a self-proclaimed "Scam Hunter" warning that the $WORLDCUP token is a coordinated scam, with price-chart context and project metadata visible on-screen.

Unofficial World Cup-themed tokens represent highly speculative assets with a substantial probability of total or near-total capital loss. Official FIFA digital initiatives, if any, are limited and clearly documented on verified channels.

Payment fraud - card-not-present and social engineering

One of the most common forms of fraud observed around international sporting events is card-not-present (CNP) fraud, in which victims unknowingly submit payment details to fraudulent websites impersonating official event organizers, ticketing providers, hospitality services, or travel agencies. Threat intelligence reporting around the 2022 FIFA World Cup identified phishing pages designed to imitate official services and harvest payment-card information and banking credentials, often exploiting urgency and scarcity to pressure rapid purchasing decisions.

Social engineering is the broader category that absorbs CNP fraud. Rather than relying solely on technical compromise, attackers impersonate official organizations, travel providers, sponsors, ticket resellers, hospitality vendors, or event-related service providers to deceive victims into voluntarily transferring funds or disclosing sensitive financial information. Research into cyber risks surrounding the Paris 2024 Olympics identified financially motivated cybercrime targeting hospitality, transportation, telecommunications, and sponsorship ecosystems as one of the most likely and persistent threats during the event period.

Figure 4. Example of a fraudulent ticketing website posing as an official FIFA World Cup 2026 platform; WHOIS records for thedomain returned a high malicious-risk score.

In many cases, victims either authorize payments themselves or unknowingly provide credentials through fraudulent portals, enabling subsequent account takeover, unauthorized purchases, fraudulent transfers, or identity-related financial crimes.

Business Email Compromise (BEC)

The financial impact of the World Cup extends beyond consumer fraud to significant business-to-business payment risks affecting sponsors, vendors, logistics providers, hospitality partners, and service contractors operating within the tournament ecosystem. Cyber criminals exploit complex procurement, sponsorship, and payment chains through supplier impersonation, invoice fraud, and BEC.

Figure 5. Pre-tournament research by Proofpoint found that one in three official FIFA World Cup 2026 partners lacked sufficiently strong DMARC enforcement to effectively prevent domain spoofing and email impersonation .[1]

Weak or non-enforced DMARC configurations increase opportunities for attackers to impersonate trusted organizations, spoof legitimate sender domains, and redirect payments through fraudulent invoices or altered beneficiary details. High transaction volumes, urgency, and operational complexity associated with global tournaments further weaken standard payment-verification processes, increasing exposure to manipulated invoices, fraudulent wire transfers, beneficiary-account redirection, and payment-approval fraud.

[1] https://www.proofpoint.com/uk/newsroom/press-releases/fifa-world-cup-2026-more-one-third-official-partners-expose-public-risk

Anti-Money Laundering (AML), human trafficking, and financial-crime compliance

The FIFA World Cup 2026 is expected to create significant financial crime and compliance challenges for banks, payment providers, and financial institutions because large international sporting events often increase opportunities for illicit financial activity, including human trafficking, money laundering, and exploitation-related transactions.

FinCEN has warned that the tournament's massive influx of visitors, rapid economic activity, and cross-border movement of people and money could be exploited by criminal networks involved in sex trafficking and labor trafficking. Financial institutions are being urged to strengthen AML monitoring systems, increase suspicious activity reporting, and improve transaction surveillance during the tournament period.

The financial sector plays a critical role because trafficking networks rely heavily on banking and payment systems to move and disguise illicit profits. Criminal activity associated with major events may involve unusual cash deposits, peer-to-peer payment transfers, prepaid cards, digital-asset transactions, and abnormal travel-related spending patterns. Traffickers may exploit increased demand for tourism, hospitality, transportation, and entertainment services during the World Cup to expand illegal operations, creating increased risk for banks, casinos, money transmitters, fintech platforms, and payment processors operating near host cities.

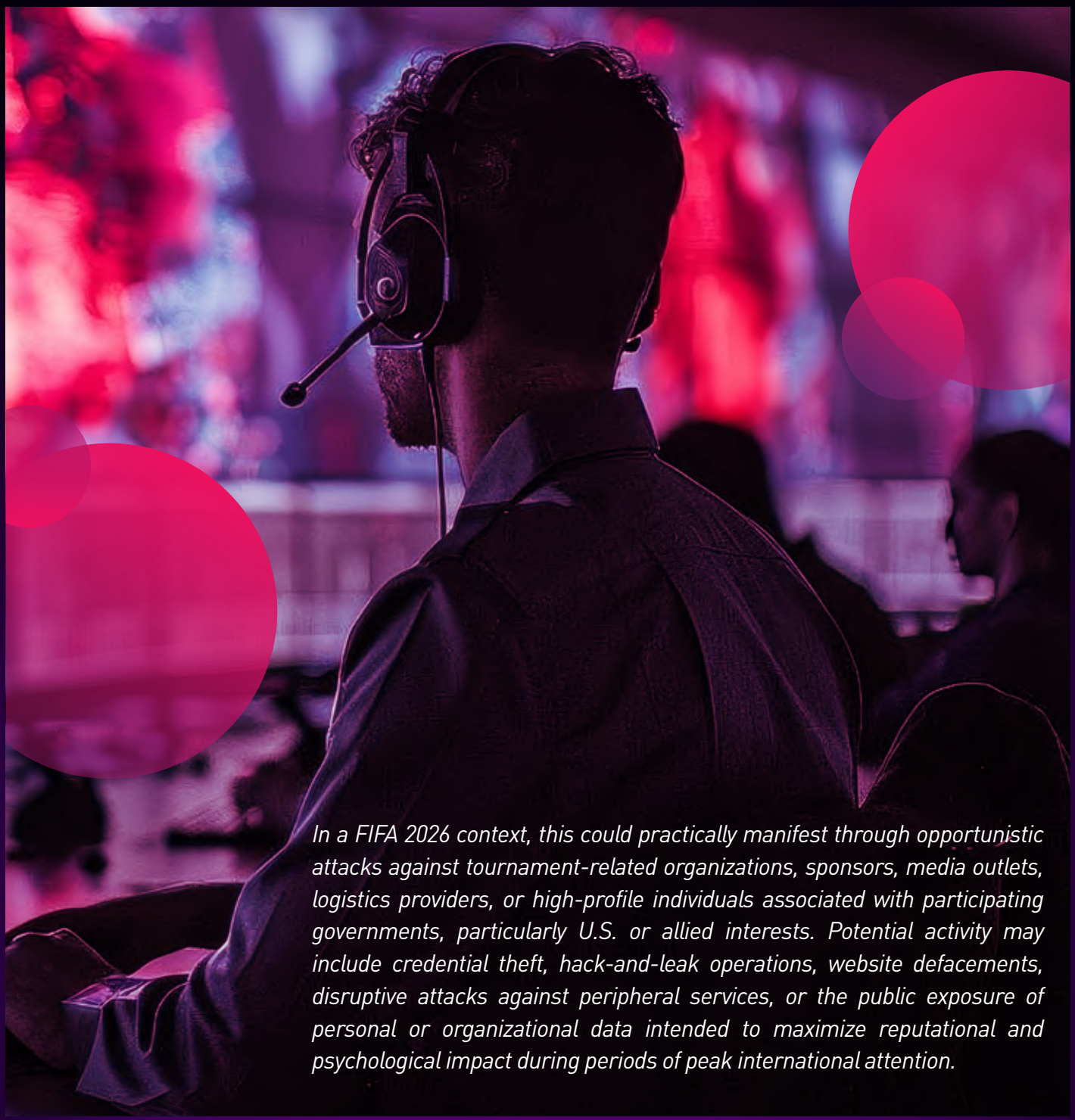
Impact and Risk

The financial impact of event-related fraud extends well beyond direct monetary loss. Banks and payment providers face chargebacks, reimbursement claims, fraud investigations, and operational strain on transaction-monitoring and dispute-resolution functions. BEC and supplier-impersonation activity drives wire-recovery requests, reimbursement disputes, and suspicious-transaction investigations. AML-related compliance activity (suspicious activity reporting, enhanced due diligence, and transaction surveillance) scales with the tournament's visitor and cash-flow volumes.

These pressures fall hardest on institutions operating near host cities and on entities exposed to high-volume consumer payment flows: card issuers, acquirers, e-commerce processors, money transmitters, fintech platforms, and casinos. Cryptocurrency exchanges and on-ramps face secondary exposure as event-themed tokens generate volume and as victims attempt to recover losses from scam projects.

Reputational impact is significant where customer accounts are drained or where fraud volumes overwhelm support functions. Regulatory scrutiny is also likely, particularly in jurisdictions with active fraud-reimbursement obligations and AML supervision.

Handala is particularly relevant to FIFA 2026 due to its demonstrated preference for high-visibility, psychologically impactful operations targeting politically symbolic entities and individuals. Rather than indiscriminate disruption, the group may seek to exploit the tournament's global visibility to amplify ideological messaging, embarrass perceived adversaries, or generate media attention through cyber-enabled influence operations.



In a FIFA 2026 context, this could practically manifest through opportunistic attacks against tournament-related organizations, sponsors, media outlets, logistics providers, or high-profile individuals associated with participating governments, particularly U.S. or allied interests. Potential activity may include credential theft, hack-and-leak operations, website defacements, disruptive attacks against peripheral services, or the public exposure of personal or organizational data intended to maximize reputational and psychological impact during periods of peak international attention.

Given Handala's pattern of combining cyber intrusions with public messaging and information exposure, the group may also attempt to leverage tournament-related incidents to shape narratives, signal political intent, or create disproportionate media amplification relative to the technical severity of an intrusion.

Chinese-aligned activity

China-linked cyber actors represent a lower-visibility but strategically significant threat category, primarily focused on long-term intelligence collection rather than overt disruption. Historical concerns surrounding major sporting events have included surveillance activity, data harvesting, and potential exploitation of official event platforms and digital ecosystems. In a FIFA 2026 context, China-aligned actors are more likely to leverage associated digital infrastructure to collect sensitive information relating to athletes, spectators, partner organizations, and host-nation systems, supporting broader strategic intelligence requirements rather than immediate operational disruption.

North Korea-aligned activity

North Korean cyber actors combine financially motivated cyber crime with strategic espionage. Their operations commonly involve phishing campaigns, credential theft, cryptocurrency-related theft, and targeted attacks against financial systems. In a major-event context, North Korea-linked groups may seek to exploit payment ecosystems, ticketing infrastructure, hospitality systems, or cryptocurrency services to generate financial gain. Although unlikely to emerge as primary disruptors of FIFA 2026 operations, their adaptability and focus on monetization position them as a persistent secondary threat.

Cross-cutting observations and threat prioritization

- Russia-aligned threat dominance. Russia-aligned actors represent the most capable and operationally relevant cluster identified across prior international sporting events, with demonstrated DDoS, disruption, espionage, and influence operations during Olympic-related activity.
- Hacktivist–APT convergence. Loosely affiliated collectives amplify geopolitical narratives through disruptive operations while advanced threat actors run parallel espionage and influence campaigns. The convergence increases both operational complexity and potential impact.
- AI-enabled influence operations. Recent sporting events have featured AI-assisted disinformation, including fabricated media content, manipulated narratives, and synthetic media designed to influence public perception, erode trust in organizers, or generate reputational damage.
- Coalition-based hacktivism. Hacktivist groups increasingly operate through informal coalitions, coordinating targets and campaigns through online platforms and messaging applications, enabling rapid mobilization and synchronized attacks during globally visible events.

Based on observed activity, the most operationally relevant threat actors for FIFA 2026 are concentrated within the Russia-aligned ecosystem, including NoName057(16), Killnet, Anonymous Sudan, Storm-1679, Storm-1099, APT28, and Midnight Blizzard. Secondary but relevant threats include Iran-aligned hacktivist actors, alongside Chinese and North Korean state-sponsored entities focused primarily on espionage, intelligence collection, and financial exploitation.

Historical Parallels

Activity observed at recent mega-events maps closely to the financial-sector threats now surfacing around FIFA 2026.

- 2022 FIFA World Cup (Qatar). Threat-intelligence reporting documented phishing campaigns disguised as ticketing and streaming services that harvested payment-card details, banking credentials, and identifying information for later exploitation.
- Paris 2024 Olympics. Research into cyber risks identified financially motivated cyber crime targeting hospitality, transportation, telecommunications, and sponsorship ecosystems as one of the most likely and persistent threats during the event period. Storm-1679 ran the fabricated "Olympics Has Fallen" disinformation campaign during the same Games.
- Milano–Cortina 2026 Winter Olympics. NoName057(16) ran DDoS campaigns against Italian officials, accommodation and hotel infrastructure, and public-administration domains, with peak activity coinciding with the opening ceremony.
- Olympic-related history. APT28 (Fancy Bear) has historically targeted Olympic-related organizations through phishing, credential theft, and strategic information disclosure; Midnight Blizzard has targeted diplomatic and governmental entities around major international events; the Matryoshka influence network has impersonated legitimate news outlets during Olympic-related campaigns.

Closing

Across crypto-themed scams, payment fraud, BEC, AML risk, and the broader hacktivist and state-linked threat landscape, the pattern around the FIFA World Cup 2026 is consistent with prior international sporting events: adversaries adapt their tactics to exploit the heightened pressure, connectivity, and trust that surround the tournament. Financial institutions, payment providers, fintech platforms, and cryptocurrency services positioned along the event's transaction flow are repeatedly targeted with similar techniques in rapid succession.

The cases documented in this report serve as both cautionary examples and strategic signals. Sustained vigilance through the end of the tournament, fraud-monitoring and AML capacity calibrated to the surge, and trusted information-sharing channels across private organizations and public-sector authorities are the conditions under which the financial sector enters the tournament with measured risk rather than accumulating exposure.

Introduction

The Transportation and Hospitality sector will play a foundational role in the successful execution of the FIFA World Cup 2026. The tournament's unprecedented scale places extraordinary operational demands on airlines, airports, public transit systems, hotels, and short term accommodation providers, all of which form the backbone of the World Cup experience.

Transportation and hospitality services are mission critical enablers. They connect teams, officials, media personnel, and millions of fans to venues, support last mile logistics from airports to stadiums, and underpin essential digital services such as ticketing, reservations, payments, and identity verification. Any significant disruption within these systems during match days could cascade rapidly, resulting in stranded travelers, public safety concerns, and reputational damage on a global stage watched by billions.

This report assesses the cyber threat landscape facing the Transportation and Hospitality sector in the run up to and during the FIFA World Cup 2026. It consolidates observed incidents, recurring threat patterns, fan targeted fraud activity, and historical precedent from prior World Cups and Olympic Games to brief sector stakeholders on the risks emerging ahead of the 11 June 2026 kickoff. The analysis is based on three evidence streams collected by Check Point Research and Check Point Exposure Management between May 2025 and May 2026.

Transportation and hospitality providers form the operational backbone of the tournament, moving teams, officials, media, and millions of fans across 16 host cities in three countries. The sector's near zero tolerance for downtime, expanded digital footprint, dense third party ecosystem, and high public visibility have made it a priority target for both financially motivated and ideologically motivated threat actors in the months preceding the tournament.

Key Findings

This report assesses the cyber threat landscape facing the Transportation and Hospitality sector in the run-up to and during FIFA World Cup 2026. It is built on three evidence streams collected by Check Point Research and Check Point Exposure Management between May 2025 and May 2026.

Transportation and hospitality providers form the operational backbone of the FIFA World Cup 2026, moving teams, officials, media, and millions of fans across 16 host cities in three countries. The sector's near-zero tolerance for downtime, expanded digital footprint, dense third-party ecosystem, and high public visibility have made it a priority target for financially motivated and ideologically motivated threat actors in the months preceding the tournament.

Key findings drawn from incidents observed between January and May 2026:

- Ransomware and data-extortion groups, including Qilin (Agenda), Clop, ShinyHunters, worldleaks, and Scattered LAPSUS$ Hunters, have hit airlines, airports, and global hotel brands, combining encryption with large-scale data theft.
- Identity abuse and social engineering (phishing, vishing, MFA fatigue, SIM-swapping) remain the most reliable intrusion paths, often producing no traditional malware indicators.
- Edge infrastructure exploitation, including vulnerabilities in F5 BIG-IP, BeyondTrust Remote Support, and Cisco SD-WAN, has driven industry-wide targeting campaigns.
- Pro-Russian hacktivist clusters such as NoName057(16) and Storm-1679 have run DDoS campaigns and blended cyber-physical disruption around the Milano–Cortina 2026 Winter Olympics.
- Fan-targeted fraud has scaled sharply: monthly registrations of FIFA-themed travel and hospitality lookalike domains peaked in April 2026, with hotel and lodging brands accounting for the majority of impersonation activity.
- Historical mega-events such as Brazil 2014, PyeongChang 2018, and Qatar 2022 show the same playbook: hacktivist disruption, destructive malware, and supply-chain pre-positioning timed to global visibility.

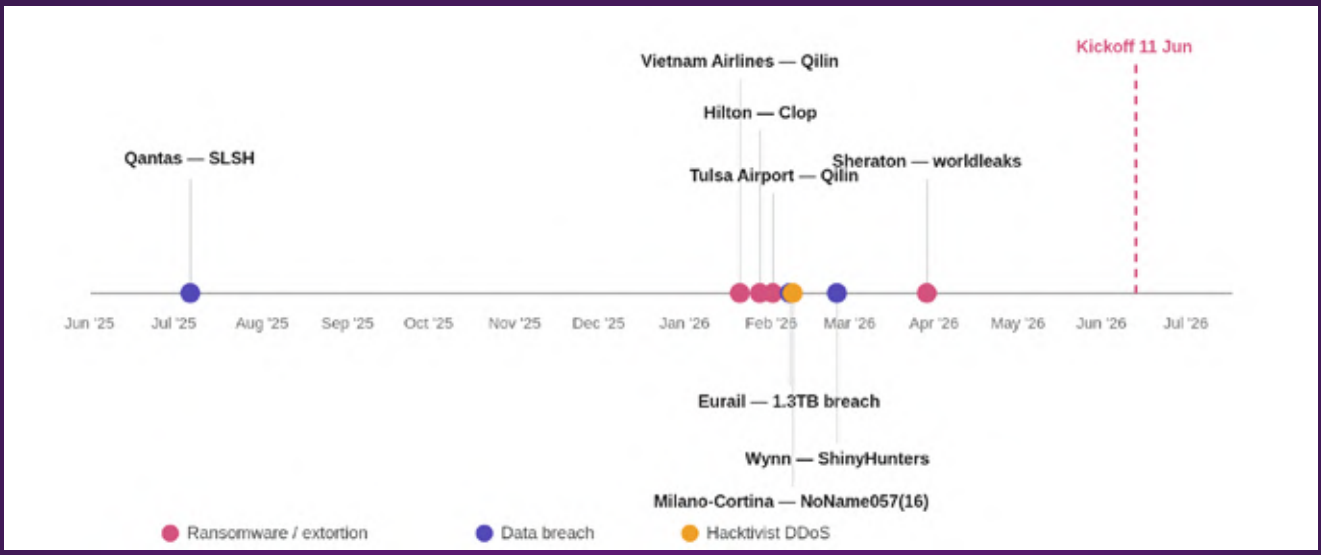


Figure 9. Timeline of notable cyber incidents affecting transportation and hospitality organizations in the months preceding the FIFA World Cup 2026 kickoff on 11 June 2026.

Why the Transportation & Hospitality Sector Is at Such High Risk

Operational pressure and near-zero tolerance for downtime

The operational pressure on this sector during the World Cup creates a near-zero tolerance for downtime. Airlines cannot afford booking or flight-operations outages during peak travel windows, and airports and public transit networks must maintain constant availability to manage crowd flows safely. Hotels and accommodation providers must sustain uninterrupted access to reservation systems, property-management platforms, and guest services while operating at or near full capacity. This environment significantly elevates risk, as threat actors are well aware that even brief service interruptions can create maximum leverage for extortion or disruption.

Expanded digital footprint and converged attack surface

The sector's digital footprint expands dramatically during a mega-event. Transportation and hospitality organizations rely on a dense ecosystem of interconnected technologies, including online booking engines, mobile applications, payment platforms, passenger screening systems, public Wi-Fi networks, and operational technology (OT) such as airport operations systems, rail signaling, and smart traffic infrastructure. The convergence of IT, OT, and consumer-facing digital services increases the overall attack surface, particularly as millions of travelers connect personal devices to unfamiliar networks in host cities and venues.

Third-party and supply-chain dependency

Compounding this exposure is the sector's heavy dependence on third-party vendors and supply chains. Airlines, hotels, and transit authorities integrate with online travel agencies, payment processors, identity verification providers, logistics subcontractors, and managed IT services. A compromise affecting a single upstream provider can therefore propagate across multiple organizations simultaneously, amplifying the potential impact. During large international events, these entities also coordinate closely with municipal services and national security bodies, meaning a cyber incident within transportation or hospitality systems may have downstream effects on broader public services.

Brand visibility as a targeting driver

Transportation and hospitality brands occupy a uniquely high-visibility position during the World Cup. Global airlines, hotel chains, and travel platforms often serve as official partners or sponsors, placing their names, logos, and digital assets directly in front of a worldwide audience. This visibility makes them attractive targets for financially motivated cyber criminals, hacktivist groups, and fraud actors seeking publicity, leverage, or scale. Domain impersonation, phishing campaigns, fraudulent booking platforms, and fake "official" mobile applications can all exploit the trust consumers place in well-known travel and hospitality brands.

Observed Threats Around the World Cup

Recent cyber incidents across the global transportation and hospitality sector reveal a clear escalation in threat activity in the lead-up to high-profile sporting events. These incidents demonstrate how threat actors deliberately exploit event-specific conditions such as heightened scrutiny, operational pressure, and public trust to maximize impact. Airlines, airports, hotels, and transit networks represent foundational infrastructure for the FIFA World Cup, and the cases examined here illustrate how adversaries increasingly target this ecosystem not only to disrupt operations, but also to undermine confidence, extract leverage, and generate strategic influence.

Hacktivist extortion and psychological pressure on airlines

In late 2025, the Scattered LAPSUS$ Hunters (SLSH), a data extortion group combining members and tactics associated with Scattered Spider, LAPSUS$, and ShinyHunters, targeted Qantas Airways, one of the world's largest international airlines. SLSH claimed unauthorized access to Qantas's network following a socially engineered intrusion and proceeded to exfiltrate sensitive data, including an estimated 5–6 million customer records. After ransom demands went unanswered, the group escalated the campaign by leaking approximately 153 GB of internal data on dark web platforms, exposing passenger names, contact information, and frequent flyer details. The extortion effort was reinforced through sustained psychological pressure, with SLSH publicly broadcasting Qantas's name across multiple channels and imposing a visible countdown deadline intended to coerce executive decision making under reputational and time based duress.

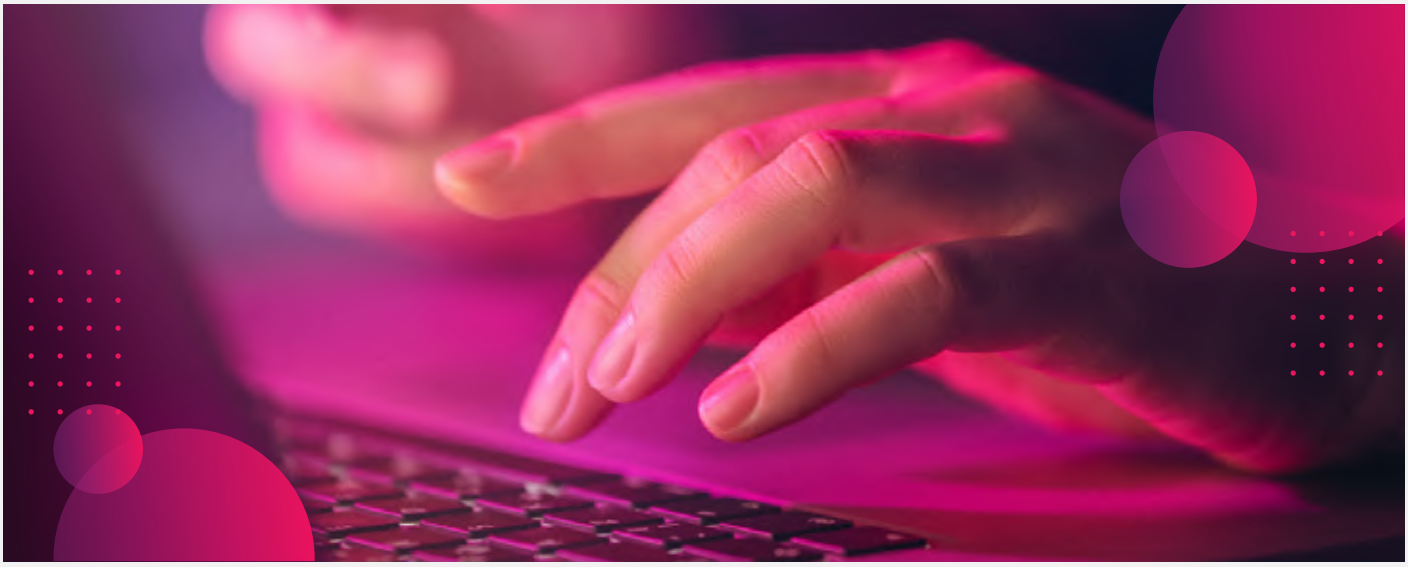
Available reporting indicates that SLSH's initial access relied on advanced social engineering and identity based techniques, rather than malware deployment. The group has a documented history of impersonating IT personnel during convincing voice phishing (vishing) calls, exploiting MFA push fatigue by overwhelming targets with authentication requests, and conducting SIM swapping to intercept mobile authentication codes. In the Qantas case, no zero day exploits or obvious malware artifacts were identified. Instead, the attackers likely manipulated a service provider or trusted employee into approving fraudulent access, enabling entry without triggering traditional antivirus or intrusion detection systems. This credentials based approach left limited forensic evidence, complicating detection and response. Initial containment reportedly depended on identifying anomalous login behavior, such as unusual access times or previously unseen devices, rather than signature based alerts.

A comparable breach affecting a major airline during a global tournament would carry immediate operational and reputational consequences. Disruption to airline systems at peak travel periods could delay flights, strand thousands of fans, and impede the movement of teams, officials, and staff en route to matches. As illustrated by the Qantas incident, a single airline compromise can rapidly cascade into broader travel disruption, potentially requiring host governments and FIFA to activate contingency transport measures under intense public scrutiny. Beyond logistics, the reputational impact would be acute. A public airline breach during the World Cup would amplify concerns around travel safety and tournament resilience on a global stage, increasing pressure on organizers to visibly demonstrate control over World Cup operations and passenger security.

Ransomware disruption targeting airport infrastructure

On January 30, 2026, the Qilin ransomware-as-a-service (RaaS) group launched a ransomware attack against Tulsa International Airport in Oklahoma, United States. Qilin, also tracked as Agenda, rose to prominence in 2025 by recruiting affiliates displaced by disruptions to larger RaaS programs. Known for double-extortion tactics, Qilin affiliates typically penetrate networks through unpatched Internet-facing systems or stolen credentials, then deploy custom ransomware to encrypt critical data while exfiltrating sensitive files for leverage. In Tulsa's case, the attackers infiltrated the airport's IT network, possibly via an unpatched system or a compromised remote-access account, and encrypted operational files relied upon for day-to-day activities. A ransom demand was subsequently issued in cryptocurrency under threat of data exposure and continued service disruption.

Ransomware deployment began rapidly once Qilin's affiliate established a foothold. The malware likely spread quickly across Windows systems, given Qilin's known use of cross-platform, Golang-based payloads, potentially appending a unique file extension to encrypted files. Previous Qilin variants have used extensions such as ".qilin" or ".agenda" as IoCs. While the precise initial access vector remains undisclosed, industry reporting in the first quarter of 2026 identified active exploitation of several network-device vulnerabilities that could align with this incident, including attacks against network-management platforms such as BeyondTrust and Cisco SD-WAN controllers. Qilin affiliates have also been observed exploiting common weaknesses such as exposed RDP services and misconfigured VPNs, often leaving behind IoCs including anomalous user accounts or suspicious new services established for persistence.



Swift containment by Tulsa's operations team limited immediate damage, allowing flights to continue without impact to aviation safety systems. Portions of the airport's business network, likely including administrative, scheduling, or baggage-handling subsystems, were taken offline or shifted to manual operations during incident response. This represents a best-case outcome in a worst-case scenario.

If a major host city airport were disrupted by ransomware during the tournament, the operational impact would extend well beyond the affected facility. Tens of thousands of fans, along with team staff and officials, could face delays or cancellations while traveling to scheduled matches. Such an incident would likely require coordinated intervention by local authorities and tournament organizers, including emergency ground transport measures or, in extreme cases, schedule adjustments to preserve match attendance. The public spectacle of a major aviation hub operating under duress during the World Cup would carry substantial reputational risk, intensifying scrutiny on FIFA and host governments to maintain operational stability under pressure.

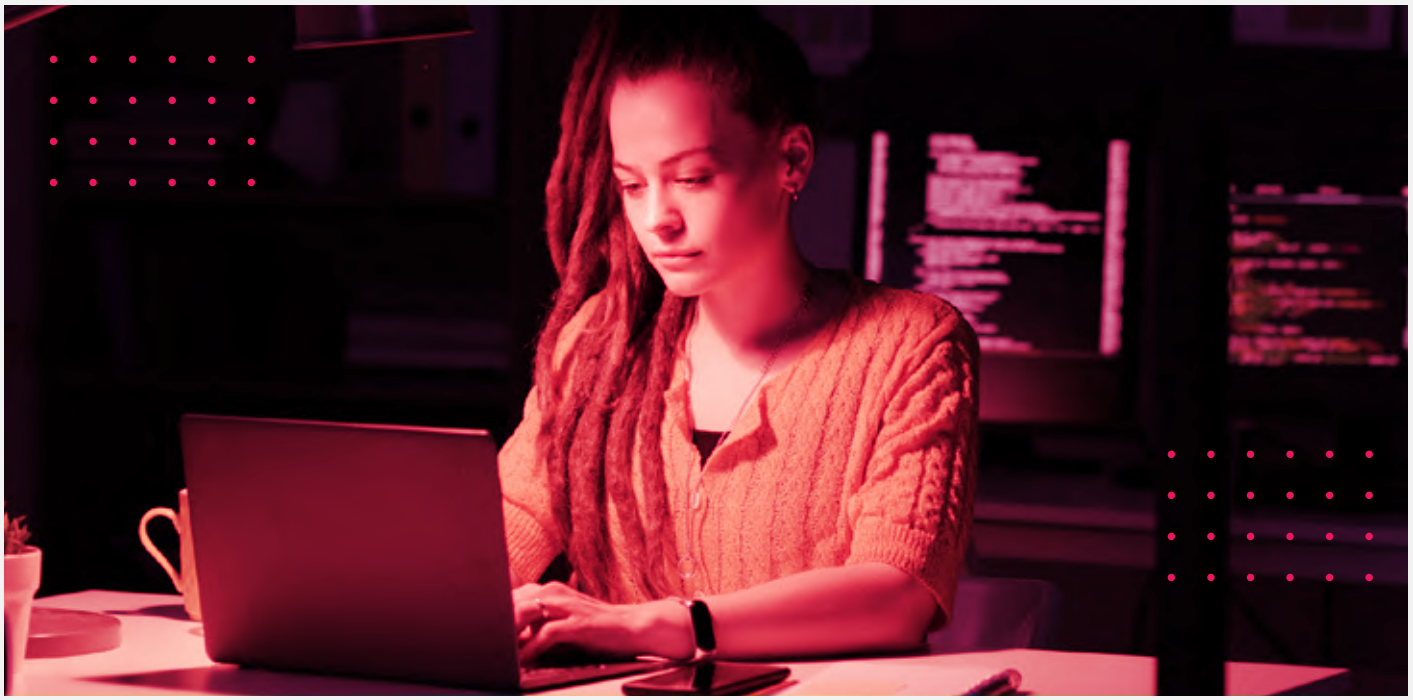
Ransomware and data extortion in global hospitality chains

In late January 2026, the Clop ransomware group (a seasoned Russia-linked criminal operation active since 2019) claimed a breach of Hilton Worldwide Holdings. Hilton, with thousands of properties globally, plays a critical role in large-scale event accommodation, including likely official lodging for World Cup teams and fans. On January 25, 2026, Clop added Hilton.com to its dark-web leak site, implying that the group had infiltrated Hilton's network, exfiltrated sensitive data, and potentially encrypted systems. The post accused Hilton of inadequate security practices and threatened public release of stolen data if negotiations were not initiated. This approach reflects Clop's established double-extortion playbook, which typically involves stealing large volumes of confidential data prior to, or even instead of, deploying ransomware.

Clop is notorious for exploiting newly disclosed or zero-day vulnerabilities in enterprise software to gain initial access at scale. Although Hilton has not publicly disclosed technical details of the intrusion, analysts noted contemporaneous exploitation of vulnerabilities in widely deployed infrastructure components, such as F5 BIG-IP devices, as a possible contributing factor. Indicators associated with Clop activity may include the appearance of a victim listing on the group's Tor-based leak site, signs of large-scale data staging or exfiltration, and, if ransomware was deployed, detection of known Clop binary patterns by advanced endpoint-detection tools. In this case, Clop appeared to prioritize data theft and leverage rather than immediate operational disruption, as guest-facing systems were reported to remain functional and the organization publicly downplayed the impact.

Hacktivist disruption and multi-vector attacks on event infrastructure

During the Milano–Cortina 2026 Winter Olympics in Italy, multiple pro-Russian hacktivist groups, including the KillNet-affiliated NoName057(16) and a cluster tracked as Storm-1679, conducted a coordinated campaign of cyber disruption. NoName057(16), known for high-visibility distributed denial-of-service attacks against European targets, directed traffic floods at Olympic-related hospitality and transit services. In parallel, Italian authorities disrupted a suspected attempt to compromise critical infrastructure in the days preceding the Opening Ceremony. As the Games commenced, Italy's transport network experienced physical sabotage, with unknown actors damaging railway signaling infrastructure, resulting in widespread high-speed train delays across northern Italy. The temporal alignment of these cyber and physical actions maximized confusion and media attention.



NoName057(16) and affiliated actors relied primarily on established DDoS techniques, coordinating botnets and volunteer participants through Telegram to overwhelm Olympic-related websites and services, including ticketing platforms, hotel booking systems, and transport information portals. IoCs included surges of traffic originating from compromised routers and Internet of Things devices, as well as the publication of target availability data on public monitoring platforms used by attackers to showcase impact. The thwarted pre-Opening infiltration suggests the potential use of custom malware or exploits targeting critical systems, possibly including industrial-control environments, although details remain undisclosed. The rail sabotage constituted a physical breach rather than a cyber intrusion, underscoring that infrastructure resilience depends on both digital and physical security controls.

In a World Cup scenario, a coordinated hacktivist campaign combining cyber disruption with physical interference in transportation or venue adjacent systems could paralyze host city mobility on match days. Such disruption would directly impede fan access to stadiums, elevate public safety concerns, and strain emergency response resources. The resulting impact could compel tournament officials and local authorities to delay matches or reroute large crowds to preserve safety and continuity. Visibly disrupted transport networks and defaced event related services would project a negative global image, requiring FIFA and host nations to publicly reaffirm control over World Cup security and operations in real time.

Impact and Risk

Taken together, these incidents reveal a consistent and concerning pattern. Transportation and hospitality providers face elevated and multifaceted threat exposure in the run-up to mega-events, driven by adversaries that deliberately exploit timing, visibility, and operational dependency. Financially motivated ransomware groups and ideologically driven hacktivists alike capitalize on the World Cup's high stakes to generate disproportionate impact, targeting systems where failure is unacceptable and trust is paramount.

Operational and business impact

Even short-duration outages can generate substantial losses as airlines, retailers, and service providers seek compensation and airport or hotel revenues decline. The potential consequences of an uncontained ransomware attack on a major airport include widespread flight delays or cancellations, passenger safety risks, and cascading disruptions across interconnected travel networks. Encryption of reservation and property-management platforms during peak demand could result in widespread check-in failures, overbooking, and payment-processing outages across hundreds of properties, a scenario especially disruptive during the World Cup.

Reputational and regulatory impact

Airlines and hotels are high-trust entities. Any hint of compromise, particularly in the pre-World Cup period, can erode public confidence in their safety and reliability. Even the perception of a hospitality compromise can be damaging, as guests entrust hotels with sensitive personal and payment information. Potential impacts include customer attrition, brand damage, and regulatory penalties under frameworks such as GDPR or PIPEDA. Regulatory scrutiny is also likely in aviation given stringent cyber-incident reporting requirements, and confirmed data breaches can prompt investigations across multiple jurisdictions.

Financial exposure

Financial exposure in such events can escalate rapidly, encompassing lost revenue, remediation costs, litigation, and extortion demands that, in similar cases, have reached eight-figure sums.

Safeguarding guidance

Treat the pre-event period as an elevated threat phase

Financial exposure in such events can escalate rapidly, encompassing lost revenue, remediation costs, litigation, and extortion demands that, in similar cases, have reached eight-figure sums.

Defend identity, access, and trust as primary attack surfaces

Recent incidents repeatedly demonstrate that attackers favor identity abuse over technical exploitation. Phishing, vishing, impersonation, and credential misuse remain the most reliable intrusion paths across airlines, airports, and hospitality providers. Organizations should treat identity protection as a mission-critical control by enforcing phishing-resistant authentication for event-relevant systems, monitoring continuously for exposed or reused credentials, and preparing staff for social-engineering scenarios that exploit the urgency and complexity of global events. Trusted access paths, particularly those involving partners and vendors, require the same level of scrutiny as internal systems.

Plan for disruption and prioritize operational resilience

Given the near-zero tolerance for downtime during the World Cup, resilience is as important as prevention. Organizations should operate under the assumption that some level of cyber disruption will occur and focus on limiting operational and reputational impact. Segmented networks, regularly tested offline backups, mature DDoS mitigation, and clearly defined incident-command structures are essential to maintaining continuity. Preparedness exercises should reflect real-world event conditions, including blended scenarios where cyber incidents coincide with physical disruption, reputational pressure, or public scrutiny, in order to reduce decision friction during live response.

Coordinate defense across the broader event ecosystem

Transportation and hospitality operations during the World Cup are deeply interconnected across organizations, jurisdictions, and service providers. Threat campaigns frequently exploit these seams by targeting multiple entities simultaneously or pivoting through third-party vendors. Effective defense depends on proactive coordination between private organizations, public-sector authorities, and event stakeholders. Establishing trusted information-sharing relationships, clear escalation paths, and shared situational awareness before the event begins is critical to avoiding fragmented responses when coordinated activity emerges.

Actively protect brand integrity and public confidence

During global events, transportation and hospitality brands function as trust anchors and are routinely exploited through impersonation, fraud, and disinformation. Protecting brand integrity is inseparable from operational security. Organizations should actively monitor for fraudulent domains, fake applications, and unauthorized use of brand assets, and be prepared to act quickly through takedowns and coordinated communication. Pre-approved messaging strategies and alignment between security, legal, and communications teams enable rapid counter-narratives and help preserve public confidence when false claims or scams surface at scale.

Key Examples

The following incidents illustrate how the threat patterns described above have materialized across transportation and hospitality organizations in the months leading up to the FIFA World Cup 2026. These cases highlight the operational, reputational, and systemic risks posed by ransomware, data extortion, and third-party compromise, particularly when timed to exploit periods of heightened scrutiny and demand.

Sheraton - worldleaks (March 2026)

In March 2026, the worldleaks extortion group carried out a ransomware attack against a large U.S. Sheraton hotel property, marking another example of financially motivated actors targeting globally recognized hospitality brands. The incident surfaced when worldleaks added the Sheraton parent network to its dark-web leak site, signaling both encryption activity and potential data theft. While business-continuity measures prevented widespread guest-facing outages, the incident created immediate concern around reservation systems, loyalty data, and internal operations.

Preliminary forensic findings suggested exploitation of a vulnerability in perimeter infrastructure as the most likely intrusion vector. At the time of the incident, security vendors were actively warning of exploitation attempts against a newly disclosed F5 BIG-IP remote code execution vulnerability, a technology commonly deployed across hotel and enterprise networks. Whether through this flaw or a similar edge-system weakness, the attack underscores a recurring hospitality risk: compromise of externally exposed infrastructure leading to rapid escalation into ransomware and data-extortion scenarios.

Within a World Cup environment, a ransomware incident affecting a major hotel chain such as Sheraton, particularly properties accommodating fans, teams, or officials, would create immediate logistical and safety challenges. Service outages or forced evacuations could displace thousands of guests during peak tournament demand, requiring host city authorities and event partners to coordinate alternative accommodations at short notice. Beyond the operational burden, such an incident would attract intense global attention during the competition, undermining confidence in event planning and placing pressure on FIFA and local organizers to demonstrate that the World Cup's hospitality infrastructure remains secure and effectively managed.

Wynn Resorts - ShinyHunters (February 2026)

A related pattern emerged in February 2026 when ShinyHunters targeted Wynn Resorts, a global hotel and casino operator. Unlike traditional ransomware campaigns, this intrusion focused primarily on data exfiltration rather than system encryption. Wynn disclosed that employee records were compromised following ShinyHunters' public extortion claim, while guest-facing systems remained operational. This tactic reflects a broader shift toward data-centric extortion, where threat actors monetize breaches through blackmail or resale of sensitive information without triggering obvious operational failures.

During a World Cup, a data extortion incident involving a prominent hospitality operator such as Wynn Resorts would introduce reputational and confidence risks even in the absence of operational outages. Disclosure of a breach affecting employee, guest, or VIP adjacent data during the tournament could heighten concern around personal data security among fans and stakeholders. While matches would proceed, the incident would divert attention from the sporting event itself and compel FIFA and host authorities to publicly address cybersecurity assurances, reinforcing the importance of robust data protection across tournament linked hospitality partners.

Vietnam Airlines - Qilin (January 2026)

In January 2026, the Qilin (Agenda) ransomware group targeted Vietnam Airlines, reinforcing the transportation sector's exposure to extortion campaigns that exploit the criticality of air travel. The attack involved encryption of administrative systems and the appearance of a corresponding leak-site entry, indicating concurrent data exfiltration. While flight safety was preserved through contingency procedures, even partial disruption to airline IT systems can have cascading effects across booking, scheduling, and partner integrations.

Threat intelligence from the same period pointed to active exploitation of vulnerabilities in remote access and network-management platforms, including flaws affecting BeyondTrust Remote Support and Cisco SD-WAN infrastructure. Airlines' reliance on these tools to manage globally distributed operations makes them attractive entry points for ransomware operators seeking privileged access with minimal friction.

In a global event dependent on tightly coordinated international travel, a ransomware attack disrupting a major airline would create immediate downstream effects for World Cup logistics. Fans, officials, and potentially team delegations could experience mass cancellations and missed connections, forcing organizers and host governments to activate contingency transport plans under significant time pressure. The cascading disruption would place added strain on tournament scheduling and public messaging, requiring FIFA and host nations to maintain confidence and continuity amid visible travel disruption during the competition.

Eurail - 1.3 TB data breach (February 2026)

In February 2026, Eurail, the consortium behind Interrail and Eurail travel passes, disclosed a massive data breach involving the exfiltration of approximately 1.3 terabytes of traveler information. The stolen dataset reportedly contained personal and travel details for millions of customers across Europe, making it one of the largest transportation-sector breaches in recent years. Although no threat group publicly claimed responsibility, the data quickly appeared for sale on underground forums, indicating financially motivated actors.

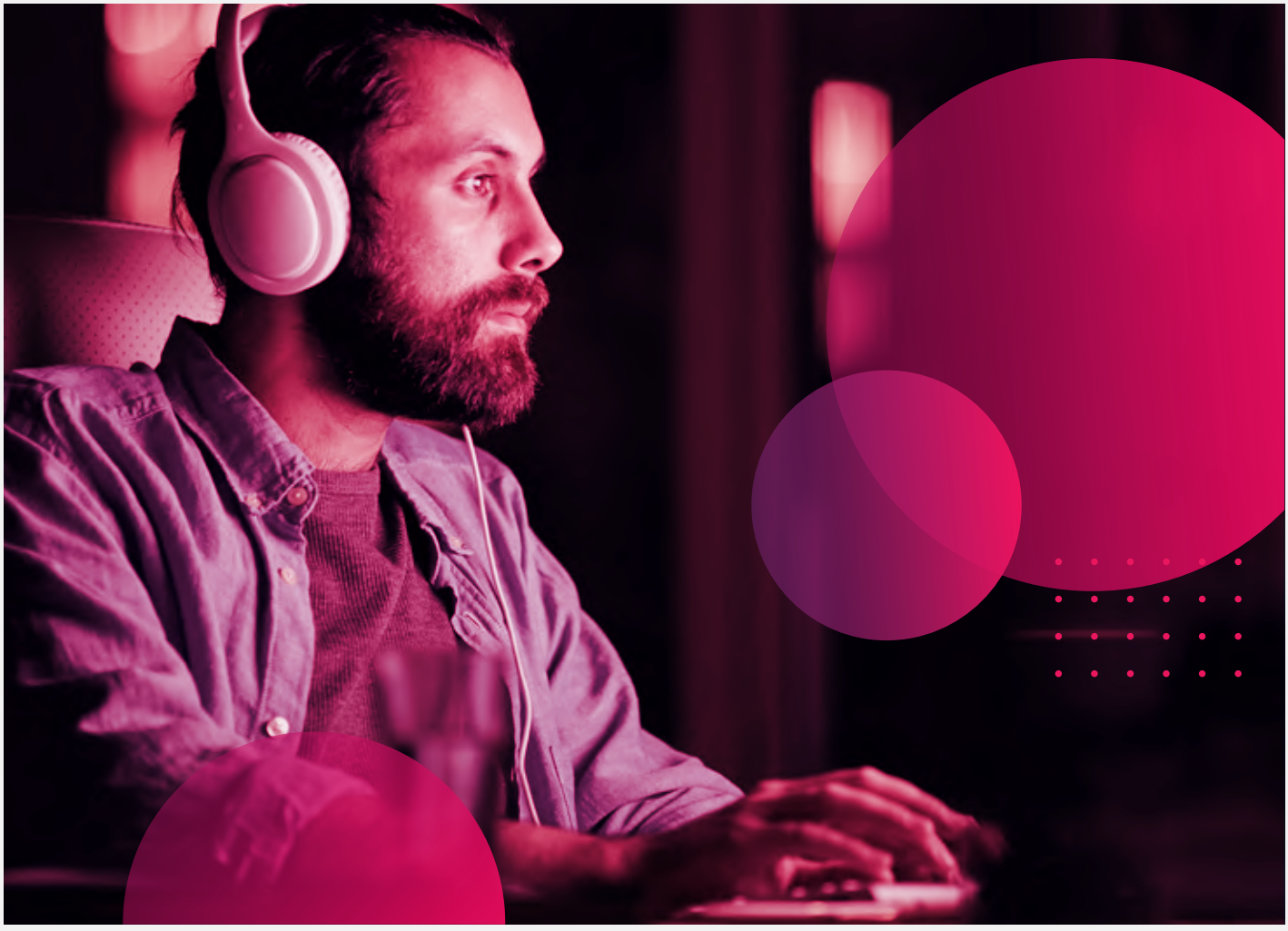
Investigators attributed the breach to an unpatched vulnerability in third-party software supporting Eurail's online booking infrastructure, enabling sustained unauthorized access. The scale and duration of data extraction suggest the attackers maintained persistence for an extended period, likely bypassing standard detection controls. Beyond immediate regulatory consequences, including GDPR investigations and potential fines, the breach introduced significant second-order risks. Exposed travelers may now be targeted with highly tailored phishing and fraud campaigns that leverage real itinerary and payment data, a particularly acute concern for individuals planning World Cup travel.

For a multi host World Cup spanning numerous cities and borders, a large scale travel data breach such as the Eurail incident would undermine both fan mobility and trust. Exposure of itinerary and identity data could fuel targeted fraud campaigns against attendees during the tournament, prompting authorities and FIFA to issue urgent advisories and reinforce verification processes at transit hubs. While match operations would continue, a high profile travel data compromise during the World Cup would erode confidence in the event's cybersecurity environment and reflect negatively on the perceived security oversight supporting tournament travel infrastructure.

Recurring patterns across the sector

Taken together, these incidents and numerous additional cases observed over the past year reveal several recurring threat patterns shaping the transportation and hospitality cyber-risk landscape ahead of the World Cup:

- Continued dominance of ransomware and extortion targeting globally recognized travel and hospitality brands, with established groups (Clop, LockBit, Qilin) and newer entrants (worldleaks) using double-extortion tactics to maximize pressure.
- Active exploitation of edge infrastructure and administrative platforms (VPN gateways, load balancers, identity providers, and remote support tools) as preferred intrusion vectors, with newly disclosed vulnerabilities driving industry-wide targeting.
- Convergence of data theft and operational disruption within single attack campaigns, extending the lifecycle of an incident from days into months of downstream regulatory, legal, and reputational exposure.
- Persistent hacktivist DDoS campaigns timed to geopolitical flashpoints and moments of maximum visibility, with cumulative impact even when individual attacks are mitigated.
- Exploitation of third-party and supply-chain weaknesses, such as booking platforms, payment processors, loyalty programs, and shared service providers, to access larger datasets or cascade impact across multiple organizations.



Fan-Targeted Fraud and Brand Impersonation

Across multiple World Cups and Olympic Games, fan-targeted phishing, impersonation, and fraud campaigns have remained one of the most consistent threat patterns. These schemes exploit surging demand for tickets, travel, accommodations, and event access by leveraging urgency and trust in official branding. The campaigns follow a repeatable model: threat actors rapidly clone legitimate branding, register lookalike domains, and reuse social-engineering templates proven effective in prior events. The impact extends beyond individual victims to legitimate airlines, hotels, and travel providers, which must manage reputational fallout and customer confusion caused by scams misusing their brands.

Domain registration trend

Open-source domain registration data covering November 2025 through May 2026 shows a clear escalation in FIFA-themed lookalike domains targeting travel and hospitality services as kickoff approaches.

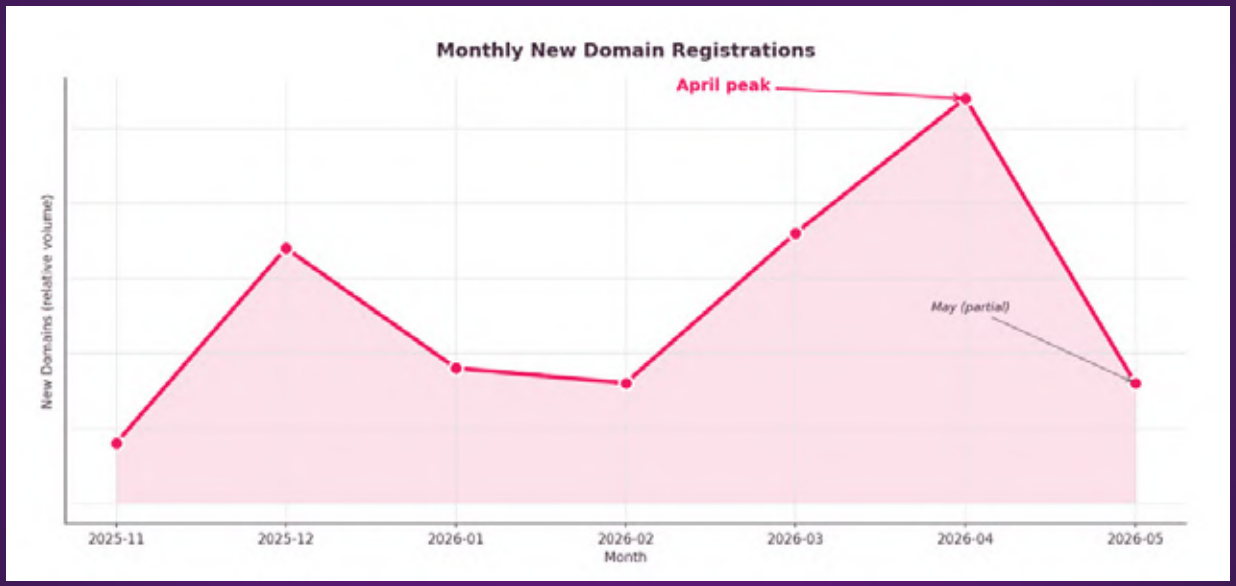


Figure 10. Monthly new registrations of FIFA-themed travel and hospitality lookalike domains, November 2025 – May 2026. Volumes climb steadily from late 2025 and peak in April 2026, ahead of the tournament. The May datapoint reflects a partial month.

Fraud target distribution

The same dataset shows that fraudulent domains concentrate overwhelmingly on accommodation and travel logistics rather than ticketing, reflecting where consumer purchasing activity is highest in the pre-event window.

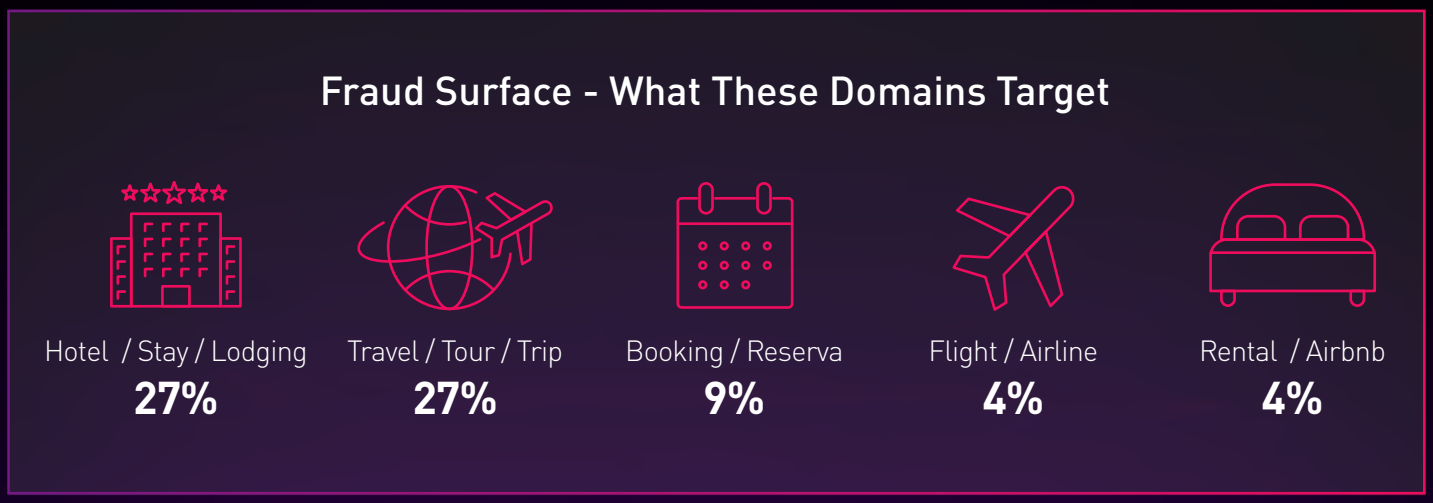


Figure 11. Distribution of FIFA-themed fraudulent domains by target category, November 2025 – May 2026. Hotel, stay, and lodging brands account for 56% of the corpus, followed by travel/tour/trip (27%) and booking/reservation (9%).

Registrar concentration

Registrar data points to a small number of providers carrying most of the fraudulent infrastructure, with a long tail of registrars hosting one or two domains.

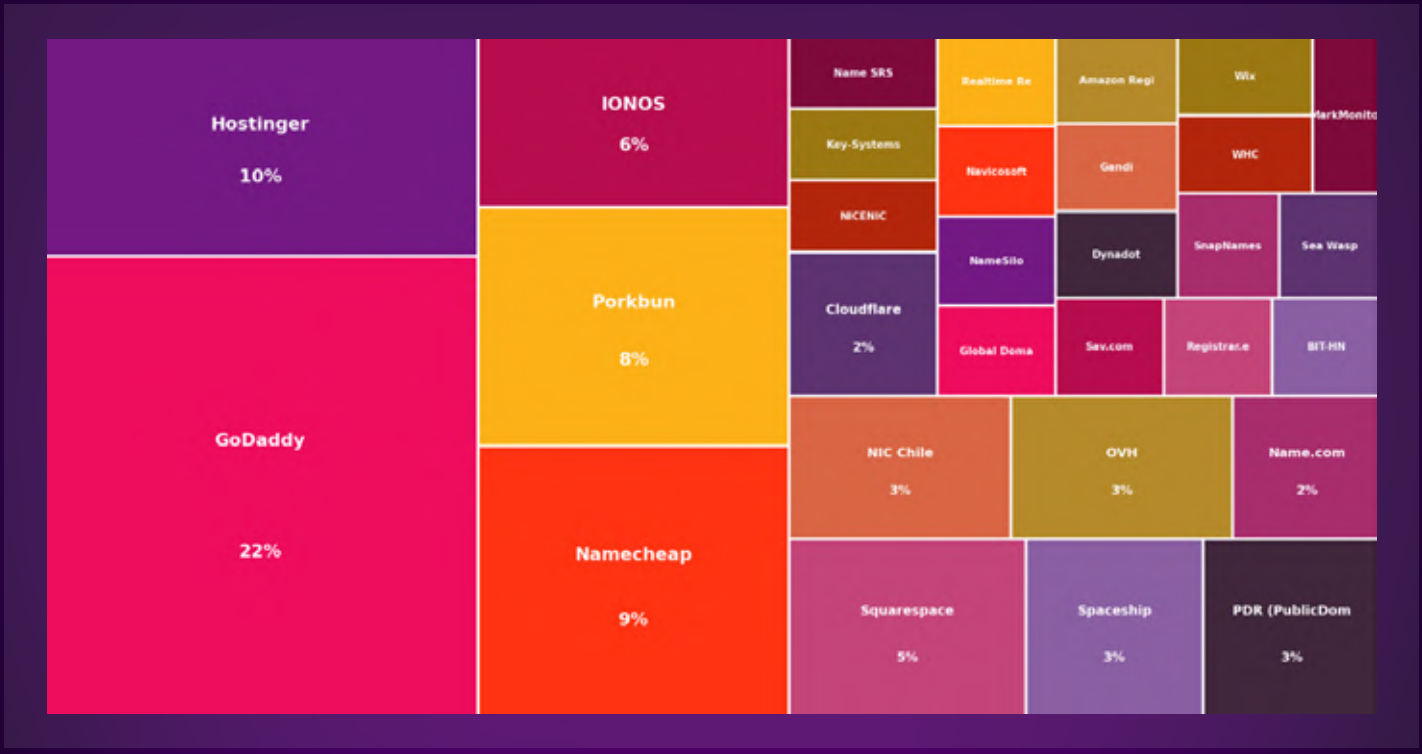


Figure 12. Registrar distribution across 30 registrars [AP1.1][MP1.2]hosting FIFA × travel and hospitality lookalike domains. GoDaddy (22%), Hostinger (10%), Namecheap (9%), Porkbun (8%), and IONOS (6%) together carry 56% of the corpus; 18 registrars host a single domain each.

Observed examples

The campaigns surfaced in this data follow patterns established at prior events. During the 2018 World Cup in Russia, spikes in phishing activity were observed whenever new ticket batches were released, with thousands of fake websites and emails impersonating FIFA and official sponsors. The same period saw the emergence of fake "World Cup livestreaming" mobile applications that delivered malware instead of video content. By the Qatar 2022 World Cup, these campaigns had become highly industrialized, with thousands of event-themed domains advertising fake entry permits, counterfeit tickets, bogus hotel bookings, and fraudulent flight deals through convincing websites and messaging platforms. The 2026 dataset reflects the same model at scale.

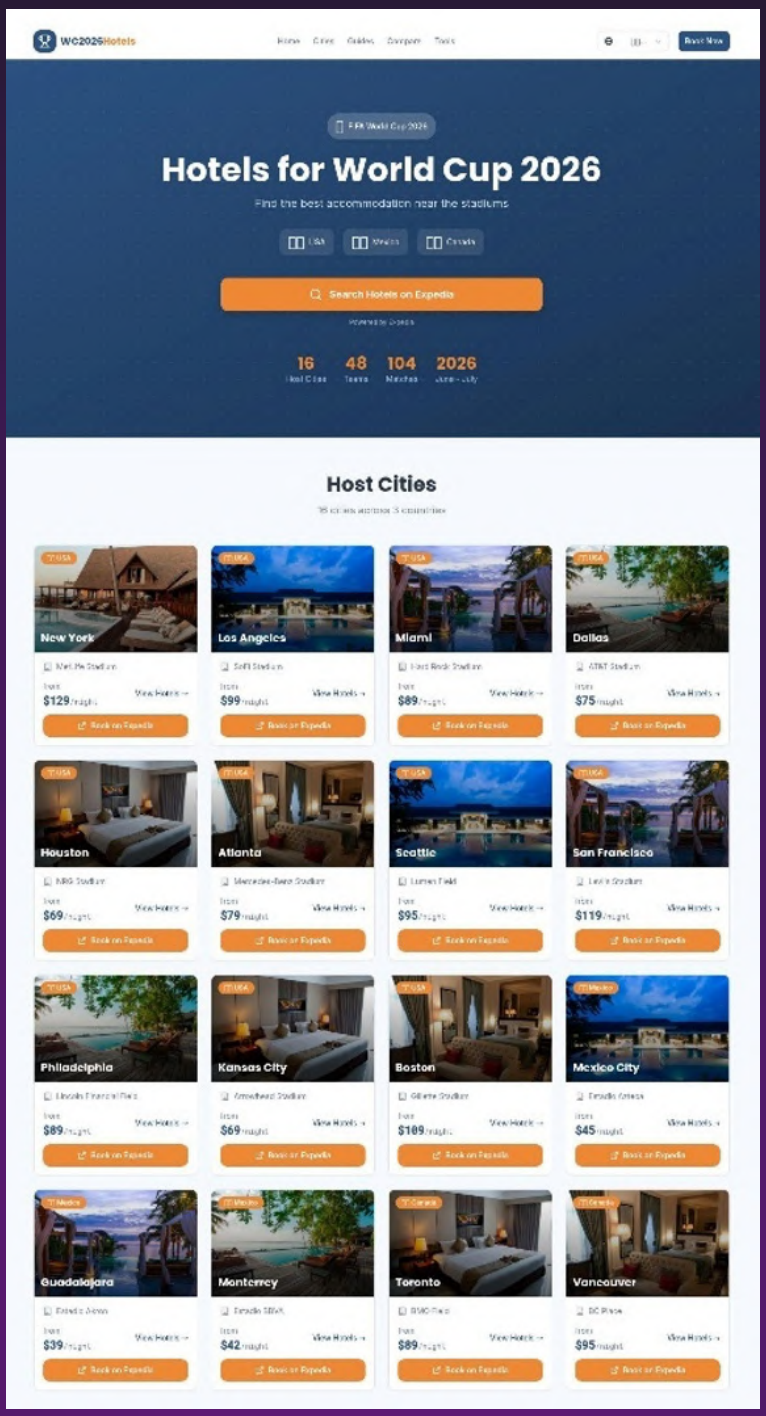


Figure 13. Screenshot of a fraudulent hotel booking site (WC2026Hotels) impersonating an official World Cup 2026 accommodation service, with listings for 16 host city locations across the USA, Mexico, and Canada.

Historical Parallels

Past World Cups and Olympic Games provide clear historical precedent for many of the threat patterns observed today. The incidents below illustrate how cyber adversaries have repeatedly exploited large-scale sporting events to target transportation, hospitality, and event-support ecosystems. Many of the risks facing the FIFA World Cup 2026 are evolutions of behaviors seen at previous mega-events, alongside a smaller number of genuinely new and escalating tactics.

Brazil 2014 - Operation Hacking Cup

During the June 2014 FIFA World Cup in Brazil, the hacktivist collective Anonymous launched a coordinated campaign known as Operation Hacking Cup (OpHackingCup). Framed as political protest, the campaign relied heavily on distributed denial-of-service attacks and website defacements aimed at World Cup-related digital infrastructure. Targets included the official tournament website, Brazilian government and law-enforcement portals, and high-profile corporate sponsors such as Emirates Airline and Hyundai.

Although core transportation and hospitality systems were not directly taken offline, the campaign demonstrated a recurring mega-event tactic that continues today: using DDoS attacks and public-facing disruptions to embarrass host nations and their corporate partners during moments of peak visibility. Anonymous amplified the campaign by leaking stolen credentials from Brazilian federal police systems, reinforcing its ability to penetrate sensitive environments even when the primary activity was disruptive rather than destructive.

PyeongChang 2018 - Olympic Destroyer

A significant escalation in event-related cyber activity occurred during the opening ceremony of the PyeongChang Winter Olympics on February 9, 2018, when a destructive malware strain later dubbed Olympic Destroyer was deployed against Olympic IT infrastructure. The attack caused widespread outages across internal networks and public-facing systems, including the official Olympics website, ticketing platforms, and stadium Wi-Fi services. Thousands of spectators were unable to print tickets, resulting in empty seats and operational disruption at a critical moment.

Widely attributed to Russia's GRU (Sandworm), Olympic Destroyer marked a departure from earlier hacktivist-style attacks. The malware combined worm-like propagation with wiper functionality disguised as ransomware, enabling rapid spread while complicating attribution. It relied on stolen credentials obtained earlier through targeted phishing of Olympic staff and leveraged legitimate Windows administration tools such as PsExec and WMI for lateral movement. The inclusion of deliberate false flags to mislead forensic analysis further distinguished this incident from prior event-related threats.

Qatar 2022 - BlackTech telecom intrusion

Approximately six months before the 2022 FIFA World Cup in Qatar, a China-linked advanced persistent threat group known as BlackTech conducted a covert intrusion into Qatar's primary telecommunications provider supporting World Cup operations. Rather than targeting visible event systems, the attackers compromised a configuration management database used to manage routers and network devices critical to broadcasting, communications, and vendor connectivity.

BlackTech deployed a sophisticated rootkit that granted persistent access to network infrastructure and allowed manipulation of router configurations. Evidence later revealed that the attackers altered DNS settings to redirect systems toward malicious updates, enabling downstream compromise of vendor environments. The intrusion remained undetected throughout the tournament and was uncovered only during post-event audits. While no disruption occurred, the incident represents a near-miss with severe implications, prepositioning the actor within the backbone of World Cup communications with the ability to disrupt broadcasts, ticketing systems, or public-safety communications at will.

Closing

Across all of these patterns, a common strategic theme emerges. Threat actors deliberately adapt their tactics to exploit the heightened pressure, connectivity, and trust that surround major international events. Transportation and hospitality organizations, by virtue of their operational centrality to the World Cup, are repeatedly targeted with similar techniques in rapid succession whether through coordinated vulnerability exploitation, concurrent extortion campaigns, or blended disruption efforts.

As the countdown to the FIFA World Cup 2026 continues, the cases in this report serve as both cautionary examples and strategic signals. Without robust preventive controls, rehearsed incident-response planning, and close collaboration with public-sector security and transportation authorities, organizations across the transportation and hospitality sector risk facing crises that compromise traveler safety, disrupt event logistics, and erode public confidence at a moment when global scrutiny is at its peak.

GAMBLING SECTOR

Introduction

This report assesses the cyber threat landscape facing the gambling sector in the run-up to and during FIFA World Cup 2026. It is built on three evidence streams collected by Check Point Research and Check Point Exposure Management between May 2025 and May 2026:[AP1.1] DNS intelligence tools for data on recent domain registrations , an Argos data-lake scan of mobile-app impersonation activity, and Check Point Exposure Management [AP2.1][GG2.2][MP2.3]deep-web and Telegram telemetry on bonus-abuse and tipster-channel chatter.

The scope is the gambling sector - specifically regulated online sports betting, iGaming, and the unregulated grey market that operates alongside them. The geographic focus is the three host nations, with secondary coverage of EU, LATAM, and MENA where the data signals reach. The timeframe is the full tournament lifecycle, with the weight of the analysis on the during-tournament window of June 11 to July 19, 2026.

Why is the Gambling Sector at High Risk

Why gambling is exposed at World Cup 2026

Three structural factors put the gambling sector in the top tier of exposure for this tournament.

First World Cup inside a mature regulated US sports betting market. Legal sports betting is live in the majority of US states and the District of Columbia as of mid-2026. The largest US operators have built tournament-ready promotional, payment, and KYC infrastructure across the 2024 and 2025 seasons. This is the first World Cup where the host nations include a fully regulated, scaled, mobile-first sports betting market alongside Ontario's regulated framework and Mexico's licensed operators. For context, previous tournaments in the Middle East (Qatar 2022) and Russia (2018) had heavily restricted or state-run monopolies on sports betting. The 2026 event will span host countries and regions with vastly different and highly regulated compliance environments. The state-by-state regulatory variance in the US creates a large attack surface: brand-abuse campaigns can exploit the gap between what a bettor in one state can legally do and what a bettor in another state expects to be able to do.

Parallel growth of the unregulated market

The dataset underlying this report shows the unregulated segment attracting the largest share of brand-impersonation infrastructure. Operators in the unregulated segment run aggressive paid-search, affiliate, and social-influencer campaigns timed to tournament windows. The unregulated market poses as a competitive issue, channel for brand abuse, a payment-fraud vector, and a regulatory-exposure risk all at once.

Multilingual targeting at scale

Crawled landing-page titles confirm campaign targeting across at least ten language communities, including English, Russian, Chinese (using the specific host-country phrase 美加墨世界杯 - "US-Canada-Mexico World Cup"), Turkish, Vietnamese, Thai, Indonesian, Spanish, Bengali, and Portuguese. This breadth indicates that the campaign is not regionally constrained.

Figure 13. Screenshot of a fraudulent hotel booking site (WC2026Hotels) impersonating an official World Cup 2026 accommodation service, with listings for 16 host city locations across the USA, Mexico, and Canada.

How the sector connects to the tournament

The gambling sector touches the World Cup at multiple milestones: ticket-adjacent fraud (ticket-and-bet bundles), broadcast and streaming overlays, the affiliate ecosystem that drives most operator acquisition, and the official sponsorship environment. FIFA does not currently maintain a global betting partner, which means any domain or page claiming to be an "official partner" or to offer "official odds" of teams, federations, or FIFA itself is, by definition, not authorized.

Observed Threats Around the FIFA World Cup 2026

This section is organized around the four threat clusters that the evidence base supports.

Brand impersonation and lookalike domain infrastructure

Pre-tournament registration acceleration

Monthly registrations of lookalike-domains volume within the sample rises sharply in the final pre-tournament window. April 2026 registrations totaled 21.9 percent of the annual sample in a single month, eight weeks before kickoff. March 2026 and April 2026 together represent 34 percent of the 12-month sample.

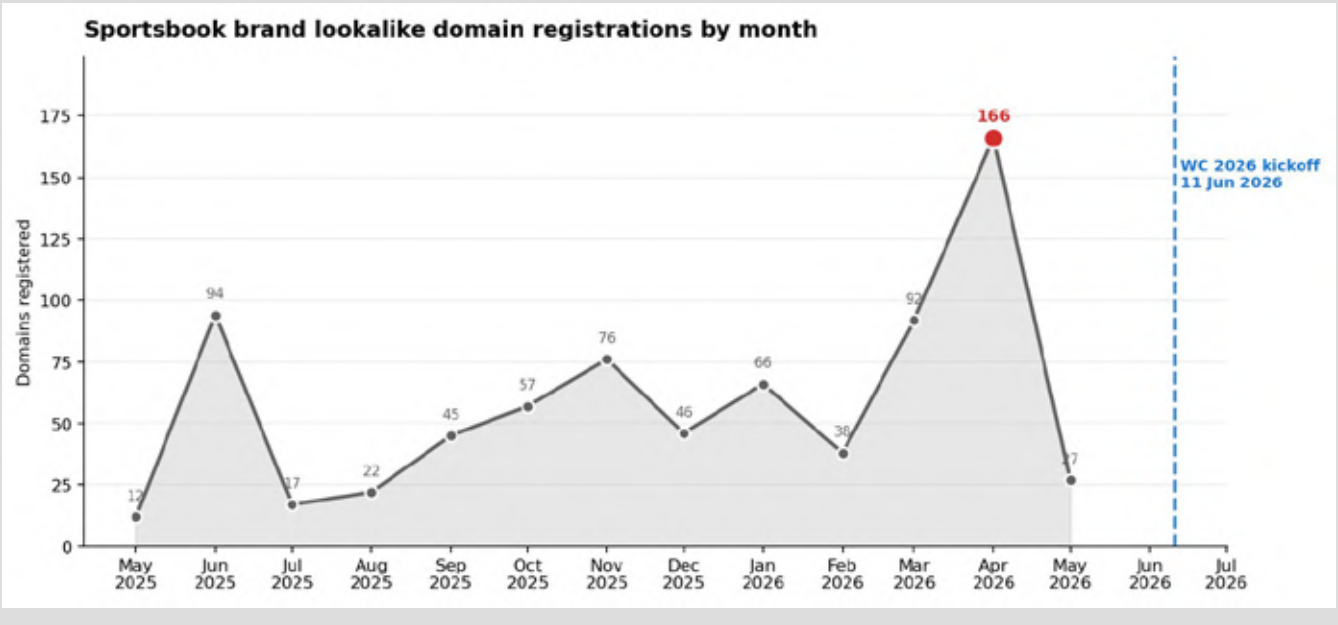


Figure 15. Sportsbook brand lookalike domain registrations by month, May 2025 – May 2026. The April 2026 peak of 166 domains is the largest monthly volume in the observation period and sits approximately eight weeks before the June 11, 2026 opening match. .

Registrar and TLD concentration

Dynadot accounts for 37.5 percent of the sample. The remaining registrar tail -Spaceship 5.9 percent, Dnsgulf 5.8 percent, Namecheap 4.2 percent, NameSilo 3.8 percent -represents smaller actors operating outside the main impersonation infrastructure. It is interesting to also note that there are three Singapore-registered registrars which make up 12.7% of the sample. (NameMart Pte. Ltd., Dnsgulf Pte. Ltd. and Gname.com Pte. Ltd.)

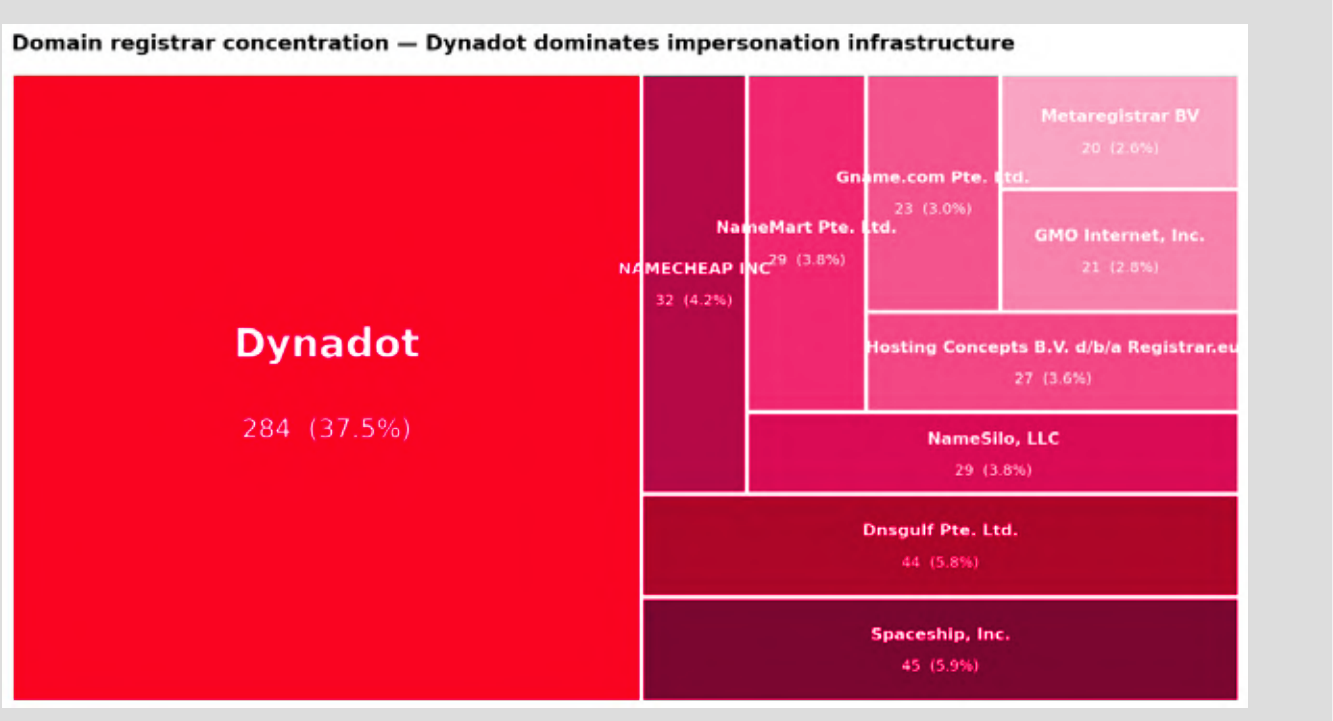


Figure 16. Domain registrar concentration across the 758-domain sample. Dynadot dominates at 37.5 percent.

TLD distribution shows .com leading at 41.6 percent, driven primarily by the April 2026 broader actor cluster, and .top at 28.4 percent. The .top concentration is particularly notable because .top is a phishing-favored generic TLD with consistently low abuse-response thresholds and registration costs.

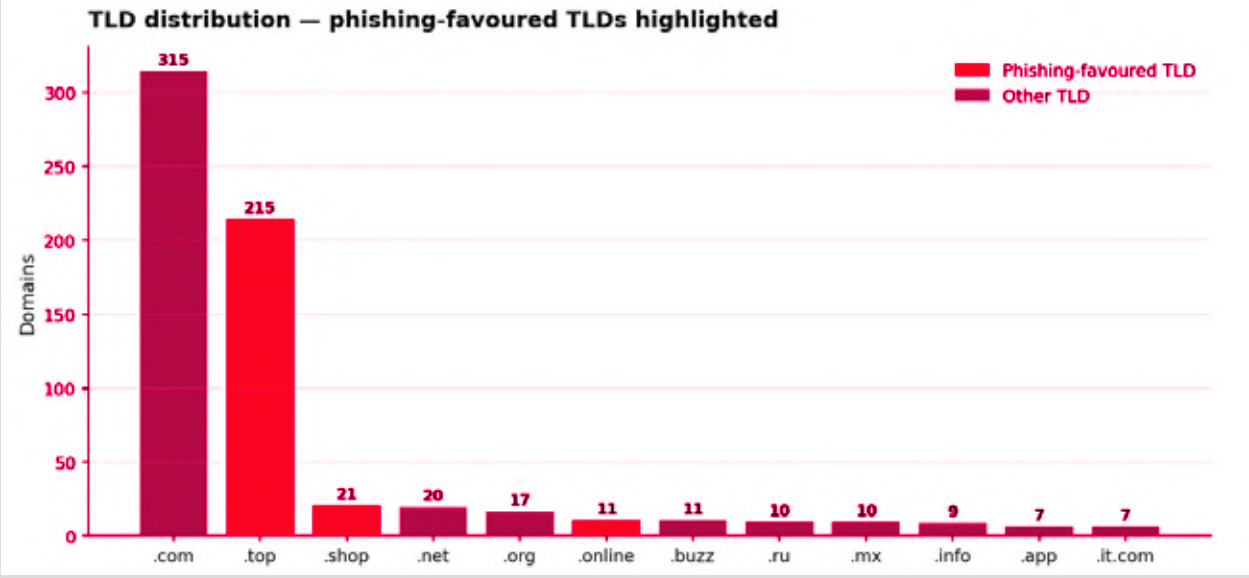


Figure 17. TLD distribution across the 758-domain sample. The .com TLD leads in absolute volume, but .top stands out at 215 domains. The .online TLD, also phishing-favored, appears at 11 domains.

Weaponization indicators

8.6 percent of sample domains have MX records configured. Domains without MX records cannot receive email and are typically used only for redirect or landing-page lures. Domains with MX records can receive password-reset and confirmation emails redirected from victim accounts, host attacker-controlled mailboxes for impersonation reply-paths, and deliver follow-on phishing from brand-lookalike addresses.

Staged but undeployed infrastructure

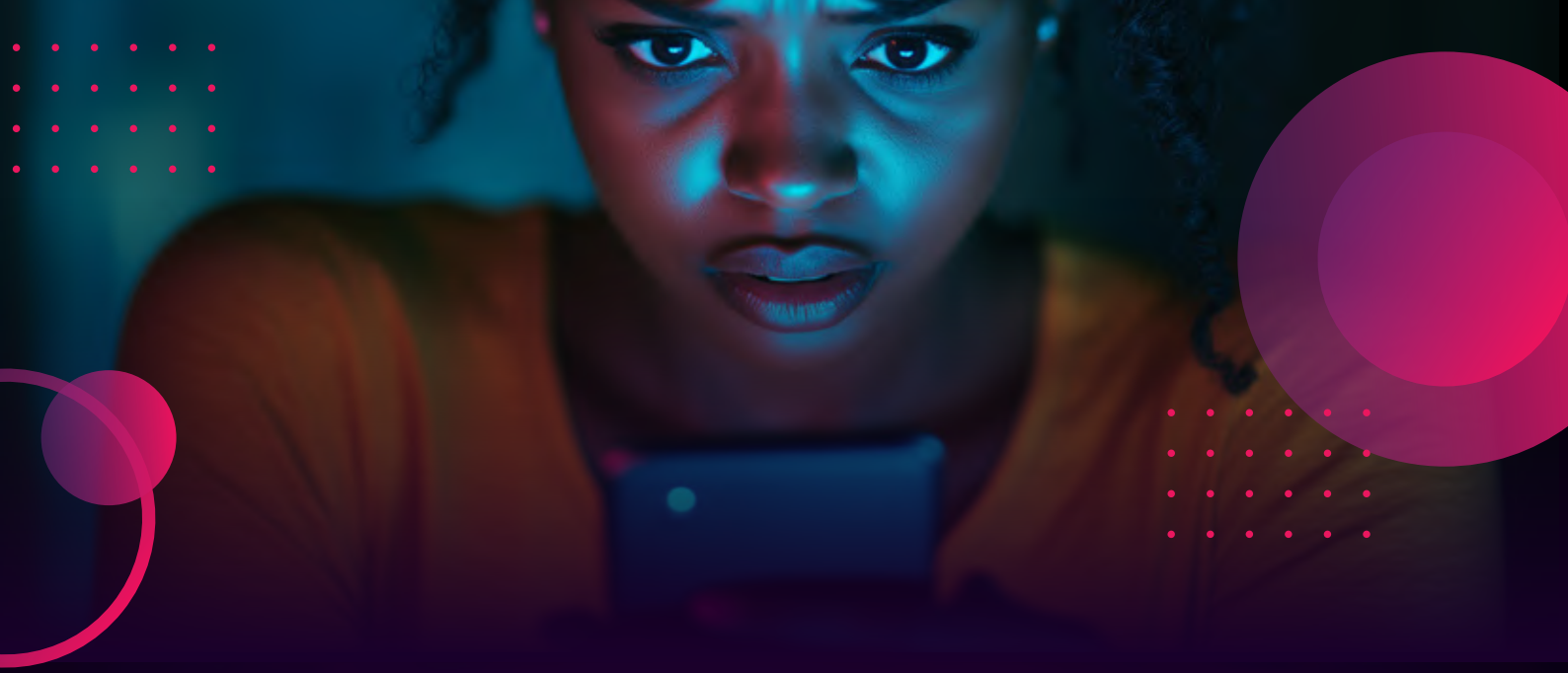
A subset of domains in the sample have no detectable FIFA reference in their crawled landing pages but carry sportsbook brand strings and registration patterns consistent with the broader infrastructure. Manual spot-check identified placeholder titles ("Hello World", "Website is ready"), Cloudflare error pages (525, 520), and generic gambling themes without explicit WC mention. This is consistent with the established pattern of registering and validating infrastructure weeks in advance, then deploying themed content closer to event milestones.

Affiliate and paid-search abuse

The gambling sector's affiliate ecosystem is its most structurally vulnerable customer-acquisition channel. Affiliates are paid on conversion. The result, observable across multiple regulated markets, is a surge in malicious affiliate activity in tournament windows.

Public CTI vendor publications cataloging World Cup 2026 phishing patterns (three independent vendors have published between March and May 2026) confirm the persistence of four affiliate-adjacent patterns:

- **Brand-bidding fraud.** Affiliates bid paid-search ads on the operator's own brand terms, often in violation of contract, redirecting traffic the operator would have acquired organically.
- **Cloaked redirects.** Affiliates route regulated-market traffic to offshore unregulated operators through a cloaked redirect that shows a compliant landing page to search crawlers and an unlicensed casino to the bettor.
- **Influencer impersonation.** Accounts impersonating sports influencers, ex-players, and tipsters promote referral codes for unregulated operators on TikTok, Instagram, and Telegram.
- **Traffic laundering.** Affiliates funnel traffic acquired through prohibited channels (banned ad networks, malware-adjacent placements, hijacked sports-streaming overlays) into legitimate operator funnels, creating regulatory exposure for the operator who accepts the conversion.



Mobile application impersonation

A coordinated mobile-app impersonation operation targeting major sportsbook brands is active in the pre-tournament window at approximately 60 times the rate observed in the equivalent non-tournament window twelve months prior. The operation runs alongside a separate population of 99 World Cup-themed apps from a mix of verified and unverified publishers, with both populations sharing back-end compliance infrastructure. Activity is concentrated on Google Play. Apple App Store exposure is limited to authorized regional licensees.

Sportsbook impersonation surge is event-driven, not background rate

A controlled comparison of two 60-day windows (March 24 – May 23, 2026 vs. the same range in 2025) using identical methodology across eight major sportsbook brands found 64 impersonator detections in the pre-tournament window against zero in the equivalent non-tournament baseline. Total app-store coverage for the same brands grew 2.5× across the two windows; impersonator detections grew by a factor of approximately 60×. None of the surge-window developer accounts appear in the baseline data.

Coordinated multi-brand operation

35+ confirmed impersonator apps have been published on Google Play in the broader six-month window, with publication density peaking April–May 2026. Each app exhibits title spoofing of a major sportsbook brand, a package name unrelated to the spoofed brand's official namespace, shell developer accounts, and listed category (arcade, puzzle, casual) inconsistent with the spoofed brand. At least five distinct developer accounts published apps spoofing two or more different sportsbook brands within hours or days of each other. Surge-window operator accounts carry mixed national naming conventions including Ukrainian/Russian, Indonesian, and generic-LLC formations. Two impersonation namespace strategies are observed: higher-sophistication actors borrow legitimate gambling-brand namespaces, exploiting reviewer practice of vetting namespace owner separately from app title whereas lower-sophistication actors use purpose-built nonsense namespaces.

World Cup–themed apps from unknown developers

99 World Cup–themed apps were published across Google Play, the Apple App Store, and 30+ third-party APK mirror sites in the December 2025 – May 2026 reporting window. Detection density peaked in the final three weeks before kickoff. A subset shows package-namespace geography inconsistent with title geography which is a known reviewer-evasion pattern.

Pre-existing customer harm independent of the impersonation surge

Domains belonging to the targeted sportsbook brands appear in Vidar stealer-log marketplace listings within the reporting window, indicating ongoing credential compromise of real customers of these brands. While this activity is not directly FIFA tournament-themed, it raises the consequence profile for the impersonation surge: compromised credentials are available to actors who may pivot into account takeover during peak betting volume.

Check Point Exposure Management identified multiple Russian-language Telegram operation in the past 30 days. On the victim-facing side the channels present as a betting tipster service, publishing high-stake "guaranteed pick" posts (e.g., "Ставка от 10к" - stakes from 10k) alongside screenshotted odds slips from FC 26 / United Esports Leagues fixtures such as Czech Republic vs. Portugal and England vs. Portugal.

Operations of this style consistently double as affiliate and promo-code abuse against the sportsbook itself: followers are funneled through referral links; the operator collects revenue-share or CPA payouts on every "new VIP deposit"; and the picks themselves are split across the audience with half the channel directed onto team A and the other half onto team B so that a portion of every fixture's followers always "wins" enough to keep depositing. The tipster then harvests affiliate commission on the resulting churn. This appears to be a direct exploitation of the bookmaker's promotional and affiliate ecosystem, financed by FIFA 2026 hype.

In parallel, Check Point Exposure Management surfaced FIFA 2026 chatter situated specifically inside the Bitcointalk Economy / Gambling discussion subforum, where threads frame FIFA 2026 ticketing, packaging, and pricing in a gambling-community context. Active underground recruitment for bonus-abuse schemes is also visible. The post below, dated May 14, 2026, illustrates the typical request:

Figure 18. Underground forum post requesting schemes to defeat anti-fraud systems and harvest multiple welcome bonuses from online casinos. Posted May 14, 2026 in an English-language black-hat subforum. Source: Check Point Exposure Management Argos.

Impact and Risk

Brand-trust erosion

When a fan loses money to a fake operator page, the fan associates that loss with the legitimate brand whose name appeared on the page. The FIFA-themed brand-impersonation domains in this report target a finite set of named operators (the sample is filtered against a tracked list of 18 sportsbook brand stems). Every one of those domains, if it reaches a fan and converts, is a unit of trust transferred away from the legitimate operator. Marketing leaders should treat brand-impersonation incidents as a customer-acquisition cost line item.

Regulatory exposure

Regulators across multiple markets have signaled tighter scrutiny in 2025 and into 2026:

- **US state regulators** (notably New York, New Jersey, Pennsylvania) have signaled heightened consumer-protection enforcement during the World Cup window, with explicit attention to deceptive promotional practices.
- **Ontario's iGaming regulator (AGCO)** published 2025 guidance specifically addressing impersonation and unregulated-operator advertising in the lead-up to the tournament.
- **Mexico's SEGOB** is the least mature regulator in the host region and the one most exposed to brand-impersonation complaints from fans.
- **The UK Gambling Commission and Malta Gaming Authority** have ongoing enforcement programs targeting affiliate compliance, with penalties extending to operators whose affiliates breach standards even when the operator was unaware.

Customer-facing and marketing teams should assume that any compliance failure visible to a regulator during the tournament window will receive higher penalty multiples than the same failure outside the window. Operators whose affiliates breach standards can be held accountable even when the operator was not directly aware of the breach.

Historical Parallels

Documented incidents at recent tournaments

Event window	Incident pattern
FIFA WC Qatar 2022 (Nov–Dec 2022)	Surge in gambling-themed phishing pages mimicking major European and Asian books, with cloned bonus pages using FIFA marks without authorization.
UEFA Euro 2024 (Jun–Jul 2024)	Sustained Layer 7 DDoS against multiple European sportsbooks during quarter-final and semi-final kickoffs.
Euro 2024	Affiliate-compliance pressure from the UK Gambling Commission and Germany's GGL on UK and German gambling operators during 2024, including against brand-bidding behavior.
Super Bowl LVIII (Feb 2024)	Reported uptick in sportsbook-themed mobile applications surfacing on Google Play and the App Store in the week of Super Bowl LVIII.
Super Bowl LIX (Feb 2025)	Coordinated paid-search campaign by unregulated operators targeting US state-licensed brand terms, observed across Google and Bing during game week.

Table 1. Documented gambling-sector cyber incidents at recent major sporting events. Sources cited inline.

Patterns by event

Event	Notable gambling-sector pattern	Relevance to 2026
FIFA WC Russia 2018	This WC saw a large-scale gambling-themed phishing localized into multiple languages. Russian-language criminal forums openly traded phishing kits keyed to the tournament.	Established the language-localized phishing pattern that will scale to Spanish, English, and Arabic at WC 2026.
FIFA WC Qatar 2022	Substantial lookalike-domain activity documented. Significant unregulated-operator activity in MENA targeting fans without local licensed alternatives.	Direct precedent for 2026 baseline projections.
UEFA Euro 2020 (held 2021)	Pandemic-era - large shift of betting volume into mobile and online channels, with corresponding spike in bot-driven abuse of sportsbook apps.	Mobile-app impersonation pattern matured during this window.
Super Bowl LVIII–LIX (2024–2025)	US market at scale.Unregulated-operator paid-search attacks on US state-licensed brand terms.	Direct precedent for NA host-region threats.
Paris Olympics 2024	Less betting-centric, but produceda large- scalebrand-impersonation campaigns against an event sponsor portfolio.	Establishes ceiling for sponsor-themed impersonation at a multi-week global event.
ICC Cricket WC 2023	Significant unregulated activity in South Asia; Telegram-based fake-operator networks observed promoting illicit-betting.	The structural conditions that produced the ICC 2023 illegal-operator surge are all present across LATAM, making a similar Spanish- and Portuguese-language pattern likely during WC 2026.

Table 2. Notable gambling-sector patterns at prior global sporting events, with their relevance as precedents for World Cup 2026.

Implications for Customer-Facing and Marketing Teams

Brand-monitoring posture should be live now

The data shows that 34 percent of annual brand-impersonation registration volume falls in the March–April 2026 window. By May 22, 2026, the bulk of the pre-tournament infrastructure has already been registered. Takedown workflows for lookalike domains, fake apps, and impersonated social accounts must be tested, staffed, and at agreed SLAs before the activation of staged content begins, which is expected in the 30 days before June 11, 2026.

Affiliate vetting must tighten before the window opens

Audit the affiliate roster. Document brand-bidding policies and enforce them. Affiliates that breach standards during the tournament window will damage the brand and the regulator relationship at the same time.

Customer-communication templates should be pre-built and pre-approved

Templates covering the likely incident types such as fake app, fake landing page, impersonated influencer, fake bonus claim should be drafted, legal-reviewed, and queued in CRM systems before the activation window opens.

Plan for the post-tournament tail

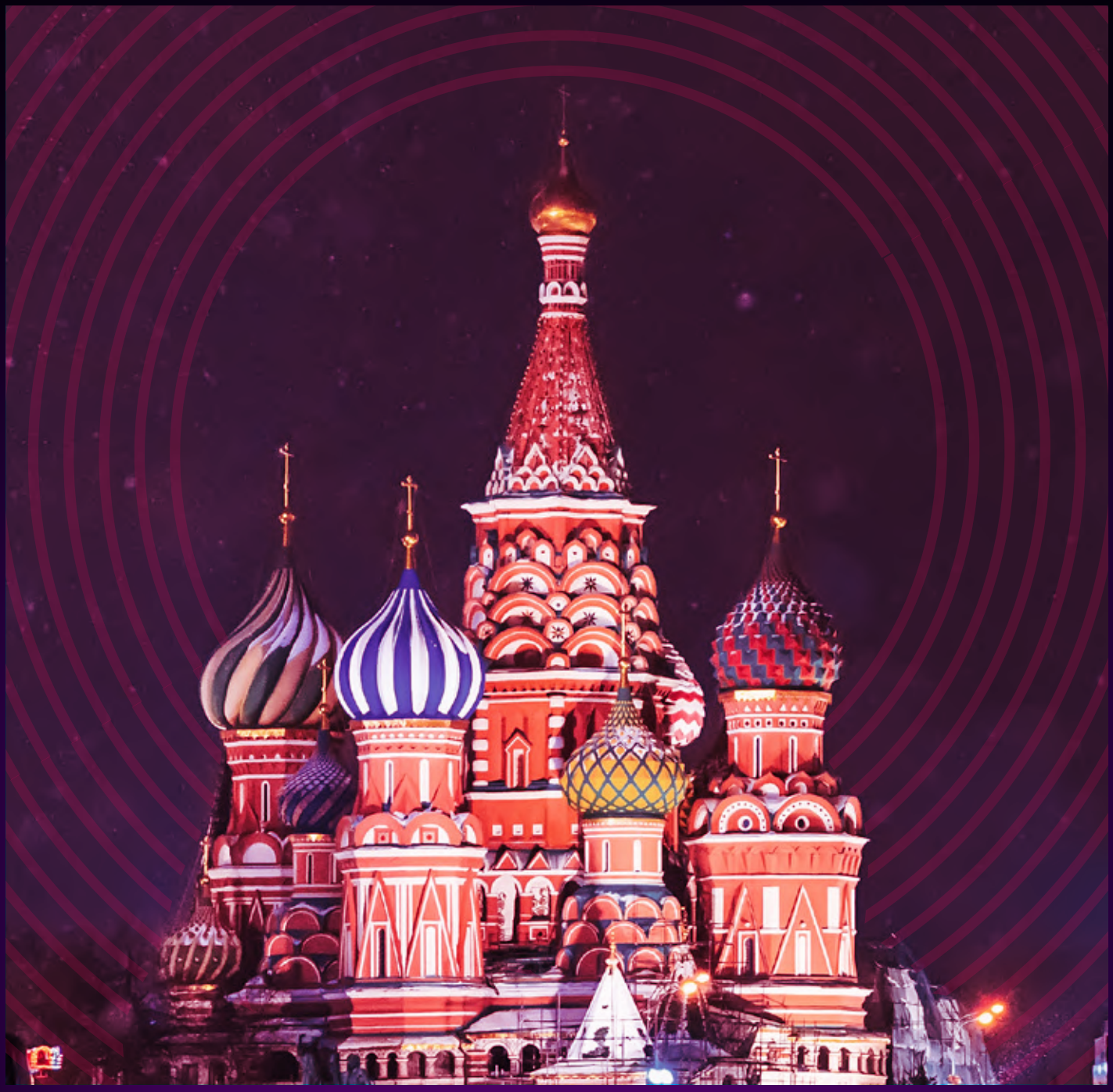
The dispute, chargeback, and complaint workload following the July 19, 2026 final will run through August. Staffing, communications posture, and senior-leadership availability should be planned accordingly.

Threat Actor Landscape

Beyond financially motivated cybercrime, the FIFA World Cup 2026 sits within a broader threat landscape shaped by ideologically motivated hacktivist collectives and state-linked actors. The following clusters and past attacks described are most operationally relevant based on activity observed during prior international sporting events that could potentially offer insight into the tactics, techniques and methods that could be re-used or adapted against the upcoming FIFA World Cup.

Russia-aligned ecosystem (primary cluster)

The Russia-aligned cyber ecosystem represents the most active and operationally disruptive threat cluster observed across recent international sporting events. Russia-affiliated hacktivist collectives have consistently demonstrated the capability to conduct coordinated disruptive operations targeting government institutions, event infrastructure, telecommunications providers, and transportation systems associated with high-profile events.



Groups including NoName057(16) have been linked to distributed denial-of-service (DDoS) campaigns against public-sector entities and event-related infrastructure, including activity targeting Italian officials and infrastructure during preparations for the Milano–Cortina 2026 Winter Olympics. Collectives such as Anonymous Sudan, HackNet, and People's Cyber Army have repeatedly targeted Western and pro-Ukraine countries through website defacements, service disruptions, and claimed data breaches, often prioritizing public-facing services and critical infrastructure.

The Russia-aligned cyber ecosystem represents the most active and operationally disruptive threat cluster observed across recent international sporting events. Russia-affiliated hacktivist collectives have consistently demonstrated the capability to conduct coordinated disruptive operations targeting government institutions, event infrastructure, telecommunications providers, and transportation systems associated with high-profile events.

Groups including NoName057(16) have been linked to distributed denial-of-service (DDoS) campaigns against public-sector entities and event-related infrastructure, including activity targeting Italian officials and infrastructure during preparations for the Milano–Cortina 2026 Winter Olympics. Collectives such as Anonymous Sudan, HackNet, and People's Cyber Army have repeatedly targeted Western and pro-Ukraine countries through website defacements, service disruptions, and claimed data breaches, often prioritizing public-facing services and critical infrastructure.

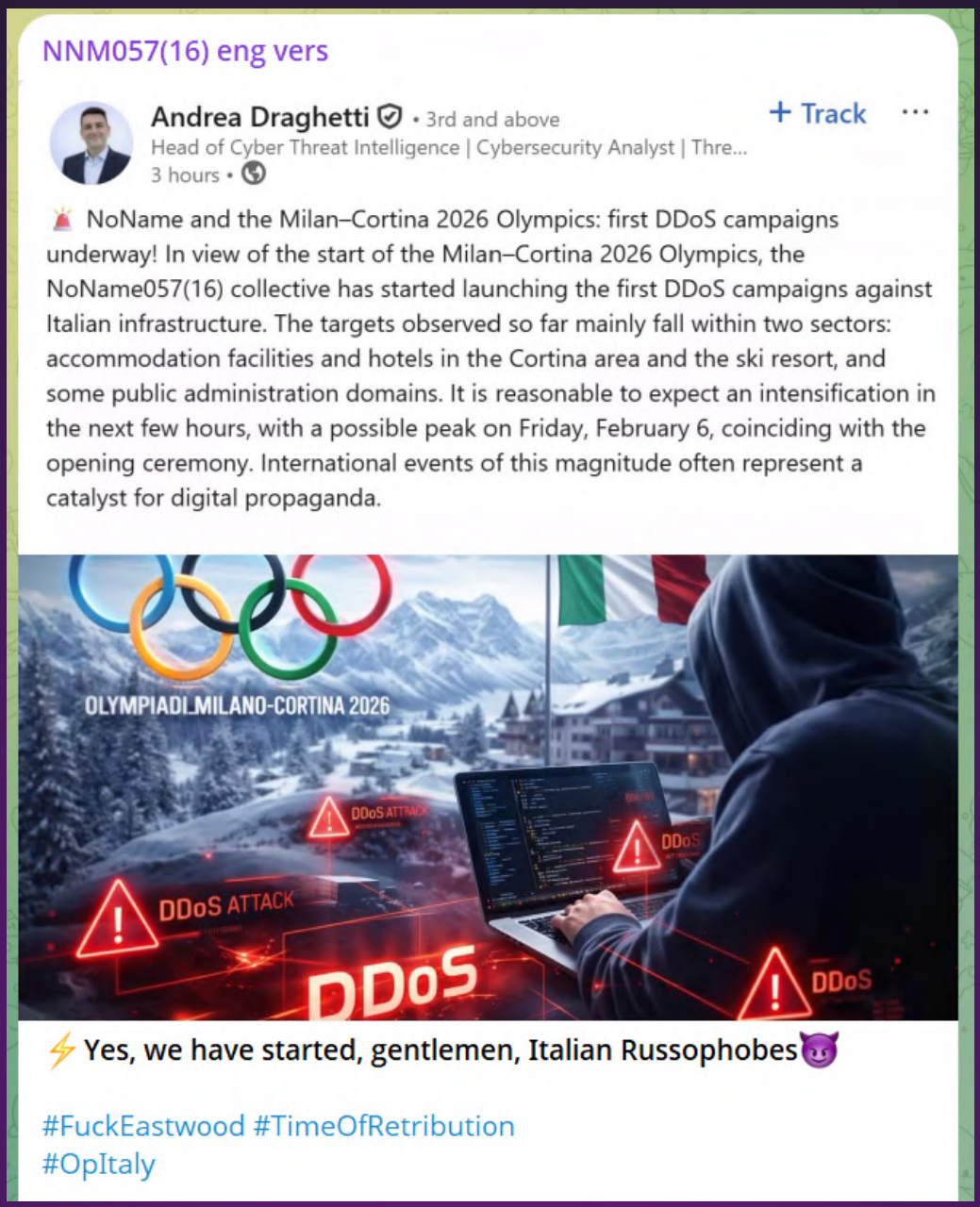


Figure 6. Telegram post by NoName057(16) showing a screenshot of a LinkedIn post by cyber threat intelligence analyst Andrea Draghetti, followed by the group's own claim of responsibility for a DDoS campaign targeting accommodation, hotel, and public administration domains during the Milano–Cortina 2026 Winter Olympics.

The broader Russia-aligned ecosystem is reinforced by actors such as Killnet and affiliated networks, which have previously coordinated disruptive campaigns against internationally visible events. These groups frequently coordinate activity through Telegram, enabling rapid mobilization, target sharing, and synchronized campaigns. Russia-aligned hacktivist networks represent a credible threat to FIFA 2026, particularly through disruptive attacks intended to generate media attention, undermine public confidence, and amplify geopolitical narratives.

Russia's state-linked cyber ecosystem combines cyber espionage, disruptive operations, and influence activity into a broader hybrid threat model. Threat actors including Storm-1679 and Storm-1099 have been associated with AI-enabled disinformation campaigns targeting international sporting events, including fabricated narratives concerning public safety, event logistics, and host-nation credibility. Similar activity was reported in relation to the Milano–Cortina 2026 Games.

Figure 7. Visual from the fabricated documentary "Olympics Has Fallen," produced by Storm-1679, which used the likeness of Tom Cruise to promote pro-Kremlin disinformation targeting the International Olympic Committee during the 2024 Paris Olympics.

Established cyber-espionage actors such as APT28 (Fancy Bear) have historically targeted Olympic-related organizations through phishing, credential theft, and strategic information disclosure. Midnight Blizzard has demonstrated sophisticated intelligence-collection capabilities targeting diplomatic and governmental entities surrounding major geopolitical and international events. These operations are further reinforced by coordinated influence ecosystems such as the Matryoshka network, associated with fabricated media content impersonating legitimate news outlets during Olympic-related campaigns.

Iran-aligned activity

Iran-aligned and pro-Palestinian hacktivist collectives represent an emerging but increasingly active threat layer, particularly during periods of heightened geopolitical tension. Groups such as GhostSec and revived derivatives of LulzSec have demonstrated capabilities spanning DDoS attacks, website defacements, data leakage operations, and ransomware deployment, including activity associated with the GhostLocker ransomware-as-a-service (RaaS) model. These operations are frequently ideologically motivated and disproportionately target Western governments, organizations, and entities perceived as aligned with Israel.

Iranian state-sponsored cyber actors are assessed as opportunistic but capable, with operational priorities centered on cyber espionage, credential harvesting, phishing, and intelligence collection. Iranian state-linked activity in the World Cup context would likely prioritize selective targeting aligned with political objectives (such as governmental, diplomatic, or organizational stakeholders) rather than broad disruptive operations.

In practical terms, this could manifest through targeted phishing or credential theft campaigns against FIFA-related stakeholders, tournament organizers, diplomatic missions, government agencies, transportation or border authorities, sponsors, media organizations, and hospitality providers supporting the event. Such activity may seek to obtain sensitive information, monitor diplomatic or security coordination, collect traveler or attendee-related intelligence, or gain access to communications involving politically relevant individuals or entities.

Given the high concentration of international officials, government representatives, and global media attention during FIFA 2026, the tournament environment may present an attractive opportunity for intelligence collection and influence-aligned cyber activity, particularly where geopolitical developments intersect with participating states or event-related diplomacy.

A relevant Iran-linked, pro-Palestinian hacker group is Handala, which has significantly increased operational activity since the onset of Operation Epic Fury, including notable attacks against U.S. targets such as the destructive cyber attack on Stryker Corporation and the compromise of personal data linked to FBI Director Kash Patel.

Figure 8. Section of Handala's leak site dedicated to data allegedly obtained from the cyber attack targeting Kash Patel.

Closing

Three weeks from kickoff, the brand-impersonation infrastructure targeting the gambling sector at FIFA World Cup 2026 is already built, staged, and partially activated. Two distinct actor profiles are operating in parallel mobile-app impersonation which has surged to roughly 60 times the non-tournament baseline. Telegram-based tipster and bonus-abuse operations are already live. The underground forum economy has not yet branded its fraud kits to the tournament; the evidence base is consistent with that branding usually observed to arrive in the final fortnight, after the staged infrastructure activates. Customer-facing and marketing teams have a short, measurable runway.

RECOMMENDATIONS

The FIFA World Cup 2026 is creating a high-risk operating environment driven by rapid transaction growth, global visibility, and compressed decision cycles. Threat actors are already positioned, with fraud infrastructure and intrusion campaigns active ahead of kickoff. Organizations should treat the current period as an elevated threat phase and act accordingly.

FINANCIAL SECTOR

The primary risk is the convergence of consumer fraud (CNP, scams), business payment compromise (BEC), and AML exposure within high-volume, cross-border transaction flows. Event-driven urgency and unfamiliar vendors reduce verification rigor, while weak email authentication across parts of the ecosystem increases exposure to payment redirection attacks. At the same time, crypto-related scams and illicit financial activity are scaling alongside fan engagement and cross-border movement.

Key recommendations:

- **Tighten payment verification controls** for vendor, sponsorship, and procurement flows.
- **Enforce strong email authentication (DMARC)** across partner ecosystems to reduce spoofing and impersonation risk.
- **Calibrate fraud and AML monitoring thresholds** for expected transaction spikes and atypical patterns tied to event activity.
- **Pre-align escalation paths** for fraud, AML, and law enforcement coordination to reduce response delays during peak periods.

TRANSPORTATION & HOSPITALITY

This sector faces a combination of ransomware, identity-based intrusion, DDoS disruption, and large-scale brand impersonation, all targeting systems with minimal tolerance for failure. Identity abuse- phishing, vishing, MFA fatigue remains the most effective entry vector, while third-party dependencies increase the likelihood of cascading impact. Fan-facing fraud campaigns are scaling rapidly, directly exploiting trusted airline and hotel brands.

Key recommendations:

- **Prioritize identity security** (phishing-resistant MFA, credential monitoring, employee readiness against social engineering).
- **Prepare for operational disruption, not just prevention,** including tested backups, segmentation, and incident command readiness.
- **Harden exposed infrastructure and third-party access points,** particularly remote access and edge systems.
- **Actively monitor and disrupt brand impersonation** (fraudulent domains, apps, and booking platforms) to limit downstream customer impact.

GAMBLING SECTOR

The main risk is pre-staged fraud infrastructure, including lookalike domains, fake apps, and affiliate abuse, actively positioned to intercept customers during peak betting activity. Regulatory complexity, especially across US state markets, creates exploitable gaps that unregulated operators and fraud actors are already leveraging. These risks directly intersect with customer acquisition channels, increasing both fraud exposure and regulatory scrutiny.

Key recommendations for Organizations:

- **Activate real-time brand monitoring and takedown workflows** for domains, apps, and impersonated social accounts.
- **Tighten affiliate governance and enforcement,** particularly around brand bidding, redirects, and third-party traffic sources.
- **Pre-build customer communication templates** (fraud alerts, fake apps, impersonation warnings) for rapid deployment.
- **Plan for post-event fraud and dispute volume,** including staffing and escalation capacity beyond the tournament window.

CONCLUSIONS

Between publication and the opening match, the threats this report describes will continue to develop along predictable lines, and the defender priorities outlined in the preceding chapters carry the most weight in the next ninety days. The Fan Safety Card on the following page is intended for redistribution. Check Point Research and Check Point Exposure Management will continue monitoring through the tournament and customers observing escalation should contact their Check Point account team.

The first World Cup hosted across three nations begins on June 11, 2026. We hope this report helps the people defending it - and the people enjoying it do both, well.

FAN SAFETY CARD

FIFA World Cup 2026: Stay Safe Online

The tournament will draw millions of fans across sixteen host cities in the United States, Canada, and Mexico, plus billions following online. As kickoff approaches, scammers, fraudsters, and threat actors are already in position. This page is a short, practical guide for fans on how to enjoy the tournament without losing money, data, or peace of mind.

Security teams at FIFA partners, host city institutions, and sector operators are welcome to reuse this content in their own customer communications.

1. Money, Tickets & Crypto

- **FIFA has not launched an official cryptocurrency.** Treat any "FIFA token" or "$WORLDCUP coin" as opportunistic at best, and likely fraudulent.
- **"You've won FIFA tickets" emails are nearly always phishing.** The official FIFA ticket portal is the only sanctioned channel for tournament tickets.
- **Verify the sender domain** on any email claiming to be from FIFA, Visa, Adidas, Coca Cola, Hyundai, or another tournament partner before clicking. Several partner domains lack strict anti spoofing controls.
- **Use credit cards** over debit cards or wire transfers for tournament related purchases. Chargeback rights are your strongest protection.
- **Be skeptical of "exclusive investment opportunities"** tied to the tournament. Legitimate sponsors do not pitch retail crypto.

2. Travel & Accommodation

- **Book accommodation through On Location** (FIFA's named hospitality partner) or directly with the hotel chain. Avoid unfamiliar aggregator sites.
- **Run a quick WHOIS or trust score check** on any booking site before payment. A domain registered in the last ninety days is a red flag.
- **Enable two factor authentication** on hotel loyalty accounts. Several major hospitality brands were breached in the months leading up to the tournament.
- **Do not post photos of boarding passes, tickets, or QR codes** on social media. Barcodes can be cloned.
- **Avoid public Wi Fi** for payment or account activity while travelling. Use cellular data or a trusted VPN.

3. Betting & Gambling

- **FIFA has no official betting partner.** Anyone presenting odds as "official FIFA sanctioned" is misrepresenting.
- **Stick to operators licensed in your jurisdiction:** state licensed in the US, provincially licensed in Canada, UKGC licensed in the UK, nationally licensed in EU member states.
- **Download betting apps only from official app stores** (Google Play, Apple App Store), and verify the developer name matches the licensed operator.
- **"Guaranteed pick" Telegram channels charging subscription fees** are nearly always tipster scams. Legitimate operators do not sell sure things.
- **Use a unique, strong password** on every sportsbook account. Credential reuse is the most common path into gambling account takeover.

4. Across the Tournament

- **Update your phone and key apps before travel.** Most attacks rely on unpatched software.
- **Treat unexpected QR codes with suspicion.** Confirm legitimacy with venue staff before scanning anything at hotels, restaurants, or stadium entrances.
- **Be wary of "support our team" donation appeals** on social media around match dates. Many will be fundraising scams.
- **Carry a backup means of communication** - a paper note with key contacts and your accommodation address - in case your phone is lost or compromised.
- **When in doubt, slow down.** Pressure to act fast is a hallmark of every type of fraud described in this report.

See something suspicious?

Report fraudulent sites, emails, apps, or social accounts claiming a FIFA connection to FIFA and to your local consumer protection authority. The faster fraudulent infrastructure is reported, the faster it can be taken down.

FIFA WORLD CUP 2026 CTI REVIEW

Check Point Research
Check Point Exposure Management

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management