INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-29 14:01 UTC

Ghost Stadium and Copycat Actors Deploy 300+ Fake FIFA Sites Ahead of 2026 World Cup

THREAT CAMPAIGN | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0380
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	General consumers; no specific software products, targets interact via fake FIFA web portals, Google Search ads, Facebook, Telegram, and WhatsApp
Published	2026-05-28T15:08:10
Discovery Source	Rss

Executive Summary

A coordinated fraud campaign attributed primarily to a Chinese threat actor called Ghost Stadium has deployed more than 300 cloned FIFA ticket portals targeting prospective 2026 World Cup attendees worldwide. The campaign harvests financial credentials and sells fraudulent tickets through typosquatting domains, paid Google Search ads, and social media channels including Facebook, Telegram, and WhatsApp. Organizations face reputational and financial risk if employees or customers interact with these sites; enterprise security teams should treat this as an active, ongoing campaign expected to intensify as the 2026 tournament approaches.

Technical Analysis

Ghost Stadium, a Chinese threat actor tracked by Group-IB, operates 300+ typosquatted and cloned domains impersonating official FIFA ticketing infrastructure. Copycat actors amplify reach through paid Google Search advertisements and social media distribution on Facebook, Telegram, and WhatsApp. The campaign relies entirely on social engineering and deceptive UI, no software CVEs are associated. Applicable weaknesses are CWE-345 (Insufficient Verification of Data Authenticity), exploited via brand impersonation and fake portal UIs, and CWE-1021 (Improper Restriction of Rendered UI Layers), exploited through deceptive overlays and iframe-based credential harvesting. MITRE ATT&CK techniques include T1656 (Impersonation), T1583.001 (Acquire Infrastructure: Domains), T1608.005 (Stage Capabilities: Link Target), T1566.002 (Phishing: Spearphishing Link), T1598.003 (Phishing for Information: Spearphishing Link), T1204.001 (User Execution: Malicious Link), and T1071.001 (Application Layer Protocol: Web Protocols). No patch exists, this is a campaign-level threat requiring DNS/web filtering, user awareness, and brand monitoring controls. The

campaign is active and assessed to intensify as the tournament approaches.

Action Checklist

1. Step 1: Containment. Push DNS/web filter block lists for known Ghost Stadium domains to all enterprise DNS resolvers and proxy layers immediately. Source blocklists from threat intelligence feeds and law enforcement advisories. Apply blocks organization-wide, including guest Wi-Fi and VPN exit nodes. Reference NIST SI-4 (System Monitoring) and CIS 4.4/4.5 (Firewall on Servers and End-User Devices).
2. Step 2: Detection. Query proxy and DNS logs for outbound connections to FIFA-themed domains registered after January 2025, particularly those with typosquatted patterns (e.g., fif4tickets[.]com, fifaworldcup2026[.]net variants). Flag traffic originating from Google Ads redirect chains to unknown FIFA-branded URLs. Monitor endpoint security logs for users who clicked links delivered via WhatsApp Web or Telegram Desktop clients. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. There is no patch; eradication is control-layer hardening. Update DNS resolver block lists and web content filtering categories to include newly registered FIFA-themed domains. Submit identified malicious URLs to Google Safe Browsing and platform abuse teams (Meta, Telegram) for takedown. Coordinate with brand protection or threat intelligence vendors to monitor for new domain registrations impersonating your organization's FIFA-adjacent communications. Reference NIST SC-7 (Boundary Protection) and D3FEND D3-PBWSAM (Proxy-based Web Server Access Mediation).
4. Step 4: Recovery. Verify block list deployment across all DNS resolvers and proxies; confirm no residual outbound connections to flagged domains in the 24 hours following block application. For any confirmed user interactions with a malicious portal, initiate credential reset workflows and review associated financial accounts for unauthorized transactions. Reference NIST IR-4 (Incident Handling) and CIS 6.2 (Establish an Access Revoking Process).
5. Step 5: Post-Incident. Conduct a user awareness campaign specific to FIFA 2026 fraud: distribute clear guidance on verifying the official FIFA ticketing URL, avoiding sponsored search results for event ticketing, and reporting suspicious communications. Review whether current security awareness training covers social engineering via paid ads and messaging apps, a gap this campaign commonly exploits. Reference NIST AT-2 (Literacy Training and Awareness) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process) for process improvements.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident commander and legal counsel if proxy or DNS logs confirm any corporate-device user submitted payment card data or credentials to a Ghost Stadium portal, as this may trigger PCI-DSS breach notification obligations or state-level consumer data breach reporting requirements; also escalate if Ghost Stadium domains are found impersonating your organization's own brand or communications rather than FIFA directly.

Recovery Notes	After block list deployment, run continuous DNS resolution checks against all known Ghost Stadium indicators for a minimum of 72 hours to confirm no resolver gaps, paying particular attention to guest Wi-Fi segments and split-tunnel VPN clients that may bypass corporate DNS. Monitor Windows Security Event IDs 4625 and 4648 for confirmed victim user accounts for 90 days, as Ghost Stadium harvested credentials may be used in delayed account takeover attempts long after the initial portal interaction. Given that Ghost Stadium is actively registering new domains and copycat actors are replicating the campaign, maintain weekly dnstwist sweeps on FIFA-adjacent keyword patterns through at least August 2026 to catch net-new infrastructure before employees encounter it.
Forensic Artifacts	DNS resolver query logs (Windows DNS debug log at %SystemRoot%\System32\dns\dns.log or BIND query log at /var/log/named/queries.log) filtered for FIFA-themed subdomain patterns registered after January 2025 — these show which internal hosts resolved Ghost Stadium typosquatted domains and establish the victim population scope | Proxy access logs (Squid /var/log/squid/access.log or equivalent) filtered for HTTP POST requests to FIFA-branded domains not matching the canonical fifa.com origin — POST requests indicate credential or payment data submission to a Ghost Stadium harvesting endpoint | Browser history SQLite databases (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite) on endpoints belonging to flagged users, queried for visit timestamps to typosquatted FIFA domains sourced via Google Ads redirect chains (identifiable by gclid= URL parameters) | WhatsApp Web Local Storage artifacts in browser profile (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Storage\leveldb\) and Telegram Desktop session cache (%APPDATA%\Telegram Desktop\tdata\) to identify users who received and acted on Ghost Stadium links distributed through these messaging channels — the primary social distribution vectors for this campaign | Google Ads redirect chain URLs preserved in proxy logs, specifically entries where the referrer header is googleadservices.com or doubleclick.net resolving to a FIFA-themed destination domain — these capture the paid search vector Ghost Stadium used to surface fraudulent portals above organic FIFA results and are actionable evidence for Google Ads abuse reporting

Per-Action IR Details

Step 1: Containment — Push DNS/web filter block lists for known Ghost Stadium domains to all enterprise DNS resolvers and proxy layers immediately. Source blocklists from Group-IB's published indicators and the FBI PSA. Apply blocks organization-wide, including guest Wi-Fi and VPN exit nodes. Reference NIST SI-4 (System Monitoring) and CIS 4.4/4.5 (Firewall on Servers and End-User Devices).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and prevent further exposure while preserving evidence

Controls: NIST SI-4 (System Monitoring), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Export Group-IB Ghost Stadium IOC domains and FBI PSA domain list into a flat text file; load into Pi-hole (free, DNS-layer sink) using the 'adlist' feature for immediate enterprise-wide blocking without SIEM. For proxy-layer blocking without a commercial tool, use Squid's 'dstdomain' ACL directive with the same domain list. Confirm block propagation by running: `for domain in $(cat ghost_stadium_iocs.txt); do dig @ $domain +short; done` — all entries should return NXDOMAIN or sinkhole IP within 15 minutes of deployment.

Evidence: Before applying blocks, export the current DNS resolver query logs (Windows DNS Server: %SystemRoot%\System32\dns\dns.log; BIND: /var/log/named/queries.log; pfSense/OPNsense: /var/log/resolver.log) covering the prior 30 days to capture any pre-block resolutions of Ghost Stadium typosquatted domains such as fif4tickets[.]com variants. Also export proxy access logs (Squid: /var/log/squid/access.log; Zscaler or Bluecoat: export

filtered by FIFA-themed URL patterns) before the block list is applied so that historical reach-back connections are preserved for victim identification.

Step 2: Detection — Query proxy and DNS logs for outbound connections to FIFA-themed domains registered after January 2025, particularly those with typosquatted patterns (e.g., fif4tickets[.]com, fifaworldcup2026[.]net variants). Flag traffic originating from Google Ads redirect chains to unknown FIFA-branded URLs. Monitor endpoint security logs for users who clicked links delivered via WhatsApp Web or Telegram Desktop clients. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources to scope victim population and confirm malicious activity

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, run this PowerShell one-liner against Windows DNS debug logs to surface Ghost Stadium-pattern resolutions: `Select-String -Path 'C:\Windows\System32\dns\dns.log' -Pattern '(?i)(fifa|worldcup|ticket).*(2026|wc26|cup26)' | Where-Object { $_ -match '\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}' } | Export-Csv ghost_stadium_dns_hits.csv`. For browser-delivered links from WhatsApp Web or Telegram Desktop, check Windows Security Event Log Event ID 4688 (Process Creation) for chrome.exe or msedge.exe with command-line arguments containing the suspicious domains: `Get-WinEvent -FilterHashtable @{LogName='Security';Id=4688} | Where-Object { $_.Message -match 'fif.*ticket|worldcup2026' }`. On Linux endpoints, grep Chrome history: `sqlite3 ~/.config/google-chrome/Default/History 'SELECT url, last_visit_time FROM urls WHERE url LIKE "%fifa%" OR url LIKE "%worldcup%"'`.

Evidence: Capture browser history artifacts before any user remediation: Chrome history at %LOCALAPPDATA%\Google\Chrome\User Data\Default\History (SQLite), Firefox places.sqlite at %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite, and Edge history at %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\History. Extract Telegram Desktop cache from %APPDATA%\Telegram Desktop\tdata\ and WhatsApp Web session artifacts from the browser profile's Local Storage (e.g., %LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Storage\leveldb\) to identify which users received and clicked Ghost Stadium phishing links via these messaging clients. Preserve Windows Security Event Log Event ID 4688 records showing browser process launches with suspicious URL arguments.

Step 3: Eradication — There is no patch; eradication is control-layer hardening. Update DNS resolver block lists and web content filtering categories to include newly registered FIFA-themed domains. Submit identified malicious URLs to Google Safe Browsing and platform abuse teams (Meta, Telegram) for takedown. Coordinate with brand protection or threat intelligence vendors to monitor for new domain registrations impersonating your organization's FIFA-adjacent communications. Reference NIST SC-7 (Boundary Protection) and D3FEND D3-PBWSAM (Proxy-based Web Server Access Mediation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat artifacts from the environment and harden controls to prevent reinfection; note that for fraud campaigns with no host-resident malware, eradication is achieved through control-layer blocking and upstream takedown

Controls: NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Use the free urlscan.io API to automate submission of newly identified Ghost Stadium URLs for public scanning and Google Safe Browsing flagging: `curl -X POST 'https://urlscan.io/api/v1/scan/' -H 'API-Key: ' -H 'Content-Type: application/json' -d '{"url": "http://fif4tickets[.]com", "visibility": "public"}'`. For continuous new-domain detection without a commercial brand protection vendor, set up a free account on WhoisFreaks or use the Python `dnstwist` tool (`pip install dnstwist; dnstwist --registered fifa2026tickets.com`) run as a nightly cron job to surface newly registered typosquats before users encounter them. Submit abuse reports directly to Google Ads at g.co/adsafety and

to Meta at facebook.com/help/reportlinks.

Evidence: Before submitting takedown requests, capture full screenshots and HTTP archive (HAR) files of each Ghost Stadium portal using browser developer tools (F12 > Network tab > Export HAR) to document the fraudulent payment flows and credential harvesting mechanisms — this evidence supports abuse reports and any downstream law enforcement referrals. Record WHOIS registration data for each Ghost Stadium domain using `whois > domain_whois_$(date +%Y%m%d).txt` before takedown actions alter registration records. Preserve any Google Ads creative IDs and advertiser IDs visible in the ad URL parameters (e.g., gclid= values in proxy logs) as these are actionable for Google's abuse team.

Step 4: Recovery — Verify block list deployment across all DNS resolvers and proxies; confirm no residual outbound connections to flagged domains in the 24 hours following block application. For any confirmed user interactions with a malicious portal, initiate credential reset workflows and review associated financial accounts for unauthorized transactions. Reference NIST IR-4 (Incident Handling) and CIS 6.2 (Establish an Access Revoking Process).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore normal operations, verify control effectiveness, and confirm no residual threat activity before declaring the incident closed

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 6.2 (Establish an Access Revoking Process), CIS 5.2 (Use Unique Passwords)

Compensating: Verify block list completeness without SIEM by running a 24-hour passive DNS query test: schedule a cron job every 30 minutes that attempts resolution of 5 known-bad Ghost Stadium domains against each internal resolver and logs the result to a CSV — any non-NXDOMAIN response indicates a resolver that missed the block push. For credential reset verification on affected users, use the free HaveIBeenPwned API to check whether the user's corporate email appears in breach datasets that Ghost Stadium may have cross-referenced: `curl 'https://haveibeenpwned.com/api/v3/breachedaccount/' -H 'hibp-api-key: '`. Document each affected user's confirmed interaction timestamp from proxy logs and open a 90-day monitoring window on their account for anomalous authentication events (Windows Security Event ID 4625 for failed logons, 4648 for explicit credential use).

Evidence: For each confirmed victim user, preserve the proxy or DNS log entry showing the exact timestamp and destination URL of the Ghost Stadium portal interaction, the source IP, and the authenticated username — this establishes the breach window for any regulatory notification clock. If the user entered payment card data on a Ghost Stadium portal, document this as a potential PCI-DSS reportable event; capture the HAR file showing the form submission endpoint. Check for any OAuth token grants or SSO session artifacts if the user navigated from a corporate device through a Google Ads redirect, as some Ghost Stadium portals have been observed attempting OAuth phishing alongside credential harvesting.

Step 5: Post-Incident — Conduct a user awareness campaign specific to FIFA 2026 fraud: distribute clear guidance on verifying the official FIFA ticketing URL, avoiding sponsored search results for event ticketing, and reporting suspicious communications. Review whether current security awareness training covers social engineering via paid ads and messaging apps — a gap this campaign commonly exploits. Reference NIST AT-2 (Literacy Training and Awareness) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process) for process improvements.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: document lessons learned, update detection and awareness capabilities, and share threat intelligence to improve organizational resilience against recurring campaign patterns

Controls: NIST AT-2 (Literacy Training and Awareness), NIST IR-3 (Incident Response Testing), NIST PM-16 (Threat Awareness Program), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a commercial awareness platform, create a one-page phishing bulletin using CISA's free Stop Ransomware and phishing awareness templates (available at cisa.gov/resources-tools/resources) customized to include: the official FIFA ticketing URL (fifa.com/tickets only), a visual example of a Ghost Stadium typosquatted domain versus the legitimate URL, and a screenshot-based guide to identifying Google Ads 'Sponsored' labels in

search results. Distribute via internal email and pin to Slack/Teams channels. For ongoing detection improvement, publish the Ghost Stadium domain patterns as a free Sigma rule (using the Sigma community repo at github.com/SigmaHQ/sigma) targeting proxy logs, and test detection coverage using atomic-red-team or manual simulation of a user browsing to a sinkholed Ghost Stadium domain.

Evidence: Compile a post-incident metrics report documenting: total number of users who resolved or accessed Ghost Stadium domains (from DNS/proxy logs), number of confirmed credential submissions (from portal interaction evidence), number of domains blocked, and time-to-block from first observed IOC — these metrics feed directly into the lessons-learned record required by NIST 800-61r3 §4 and demonstrate control effectiveness to leadership. Archive all Group-IB IOC feeds, FBI PSA indicators, and internal detection queries used during this incident in a case management record (even a shared folder with dated files) so that when Ghost Stadium or copycat actors resurface with new domains ahead of the July 2026 tournament, the response team has a ready baseline to diff against.

Detection Guidance

Primary detection surface is DNS and proxy logs. Query for outbound requests to domains matching FIFA-themed naming patterns registered within the past 12 months, focus on typosquats of 'fifa.com', 'fifatickets', 'worldcup2026', and related strings. Flag any domain with a newly registered certificate (check CT logs) and FIFA-adjacent branding. Secondary signal: endpoint browser history or proxy logs showing referral chains from Google Ads (ad click redirects) to unknown FIFA-branded destinations. Tertiary signal: user-reported suspicious messages received via WhatsApp Web or Telegram Desktop containing FIFA ticketing links. IOC enrichment: cross-reference outbound domains against threat intelligence feeds and law enforcement advisories on this campaign. Behavioral indicator: users submitting payment card data to non-fifa.com domains after clicking search ads. SIEM correlation rule suggestion, alert on: (DNS query contains 'fifa' OR 'worldcup2026') AND (domain registered within last 365 days) AND (domain NOT in allowlist of official FIFA properties). Reference NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`FIFA-themed typosquatted domains (300+ identified by Group-IB)`	Ghost Stadium infrastructure — exact domain list published by Group-IB; cross-reference their threat intelligence report for the full enumeration	HIGH
URL	`Google Search paid ad redirect chains to non-fifa.com destinations with FIFA branding`	Copycat actors purchasing sponsored search placement to direct users to fraudulent portals	MEDIUM
URL	`FIFA-branded links distributed via Facebook, Telegram, and WhatsApp`	Social media amplification vector identified by Group-IB and FBI PSA	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1656** — Impersonation

- **T1583.001** — Domains
- **T1071.001** — Web Protocols
- **T1204.001** — Malicious Link
- **T1608.005** — Link Target
- **T1566.002** — Spearphishing Link
- **T1598.003** — Spearphishing Link

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SI-7** — Software, Firmware, and Information Integrity

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1656	Impersonation	Defense-Evasion
T1583.001	Domains	Resource-Development
T1071.001	Web Protocols	Command-And-Control
T1204.001	Malicious Link	Execution

Technique ID	Technique Name	Tactic
T1608.005	Link Target	Resource-Development
T1566.002	Spearphishing Link	Initial-Access
T1598.003	Spearphishing Link	Reconnaissance

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fbi-warns-of-fake-fi...	T3
Qatar Tribune - Facebook	https://www.facebook.com/QatarTribune/posts/meta-the-owner-of-the-f...	T3
CISA Warns Threat Actors Are Using Commercial Spyware To ...	https://www.linkedin.com/pulse/cisa-warns-threat-actors-using-comme...	T3
Client Alert: Texas v. Meta and WhatsApp: A New Front in the Battle ...	https://www.shumaker.com/insight/texas-v-meta-and-whatsapp-a-new-fr...	T3
The Cyber Beat – your daily source for the best cybersecurity ...	https://thecyberbeat.com/	T3

Generated 2026-05-29 14:01 UTC by TJS Security Command Center