INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-27 06:10 UTC

DOJ Seizes ~400 Domains Used for Illegal FIFA World Cup 2026 Streaming

THREAT CAMPAIGN | MEDIUM

SCC Item ID	SCC-CAM-2026-0585
Type	Threat Campaign
Severity	MEDIUM
Affected Products	End users visiting illegal streaming sites; FIFA World Cup 2026 broadcast rights holders
Published	2026-06-26
Discovery Source	Gemini

Executive Summary

The U.S. Department of Justice, coordinating with FIFA and international law enforcement, seized approximately 400 domains illegally streaming FIFA World Cup 2026 matches and removed over 27,000 unauthorized streaming URLs. Beyond copyright enforcement, these sites actively delivered malware, financial scams, and exposed visitors' personal and payment data. The primary business risk is to employees and consumers who may access these sites on corporate or personal devices, introducing malware into enterprise environments or suffering financial fraud.

Technical Analysis

This operation targeted piracy infrastructure supporting unauthorized redistribution of FIFA World Cup 2026 broadcast content. MITRE techniques observed include T1608.005 (Stage Capabilities: Link Target), T1204.001 (User Execution: Malicious Link), T1583.001 (Acquire Infrastructure: Domains), and T1566.002 (Phishing: Spearphishing Link). Threat actors registered or hijacked domains to simulate legitimate streaming services, then redirected visitors to scam pages, credential-harvesting forms, and malware delivery endpoints.

Related but distinct: A separate incident disclosed by a security researcher involved a vulnerability in FIFA's internal broadcast management systems that could have permitted unauthorized modification or takeover of World Cup TV streams; no CVE has been assigned and details remain limited to secondary reporting. No CVE or CVSS score applies to the domain seizure operation. No CWE identifiers are associated. Source quality score is 0.64; primary sourcing is Malwarebytes threat intelligence (June 2026) and secondary news reporting.

Action Checklist

1. Step 1: Containment. Block DNS resolution and outbound HTTP/HTTPS traffic to known illegal streaming domains at the perimeter firewall and DNS resolver. Apply category-based web filtering rules for 'streaming/piracy' and 'newly registered domains' to reduce exposure across corporate endpoints. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices).
2. Step 2: Detection. Query DNS logs and proxy logs for resolution or connection attempts to domains flagged in the DOJ seizure action or matching Malwarebytes IOC reporting. Search endpoint detection logs for T1204.001 (user clicked suspicious link) and T1566.002 (phishing link delivery) patterns. Review browser history and downloaded file telemetry on endpoints for accesses during World Cup match windows. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. Remove any malware artifacts identified on endpoints that accessed flagged domains. Rotate credentials for any user who submitted account or payment information on these sites. Revoke and reissue session tokens for affected accounts. Reference credential management and account monitoring controls.
4. Step 4: Recovery. Validate that endpoint protection tools have updated signatures covering malware families documented in the Malwarebytes June 2026 report. Re-scan affected endpoints post-remediation. Monitor outbound DNS and proxy logs for recurrence over the remainder of the World Cup tournament window. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and NIST SI-4 (System Monitoring).
5. Step 5: Post-Incident. Conduct user awareness communication specific to World Cup streaming risks, citing the DOJ seizure action as context. Review and update acceptable use policies to address unauthorized streaming services. Assess whether DNS-layer filtering and proxy-based web access controls are deployed and tuned for newly registered and high-risk content categories. Reference CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and NIST AU-2 (Event Logging) to ensure logging coverage includes DNS and proxy telemetry going forward.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal/privacy counsel and senior IR leadership if any confirmed endpoint shows successful malware execution post-visit to flagged streaming domains, or if any user is confirmed to have submitted payment card or credential data to these sites — triggering potential PCI-DSS breach notification obligations and applicable state breach notification laws.
Recovery Notes	After remediation, maintain heightened DNS and proxy log monitoring through the conclusion of the FIFA World Cup 2026 tournament window, as threat actors are highly likely to re-register new streaming domains following the DOJ seizure to resume operations before and during remaining matches. Validate that all endpoint protection signatures incorporate the malware families from the Malwarebytes June 2026 report before returning hosts to production. Conduct a follow-up sweep of browser extension inventories on all endpoints that accessed flagged domains, as drive-by malware from these sites has been associated with persistent browser extension implants that survive standard malware scans.

Forensic Artifacts	Sysmon Event ID 22 (DNS Query) logs filtered for DOJ-seized domain list and newly registered domain patterns during World Cup match broadcast windows — primary indicator of user exposure to flagged streaming infrastructure | Browser history and cookie databases (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History and Cookies; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite and cookies.sqlite) — evidence of direct site visits and any session/payment data submission to illegal streaming domains | Windows Prefetch directory (C:\Windows\Prefetch\) and Sysmon Event ID 1 (Process Creation) logs — identifies executables launched in the period immediately following a visit to a flagged streaming domain, consistent with drive-by malware delivery documented in the Malwarebytes June 2026 report | Browser extension directories (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\extensions) — malicious browser extensions are a documented payload from malware-laced streaming sites and persist post-reboot | Proxy/Squid or Windows DNS server access logs covering June–July 2026 match schedule windows — corroborates scope of corporate network exposure and identifies all endpoints that resolved or connected to flagged streaming domains, supporting both technical remediation scope and breach notification assessment

Per-Action IR Details

Step 1: Containment — Block DNS resolution and outbound HTTP/HTTPS traffic to known illegal streaming domains at the perimeter firewall and DNS resolver. Apply category-based web filtering rules for 'streaming/piracy' and 'newly registered domains' to reduce exposure across corporate endpoints. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices).

NIST Phase: Containment

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

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), NIST AC-4 (Information Flow Enforcement)

Compensating: On pfSense or OPNsense, import the DOJ-seized domain list as a URL table alias and apply a block rule on LAN-out for TCP/80 and TCP/443 to those destinations. For DNS sinkholes without enterprise tooling, deploy Pi-hole with a custom blocklist fed from the Malwarebytes June 2026 IOC feed; add regex blocklist entries matching the pattern of newly registered domains (e.g., *.fifa2026stream[.]*, *.wc26live[.]*).

Evidence: Before applying firewall and DNS block rules, export current DNS resolver cache (Windows: `ipconfig /displaydns > dns_cache_pre_block.txt`; Linux: `resolvectl statistics`) and capture a snapshot of active outbound connections (`Get-NetTCPConnection | Where-Object {$_.State -eq 'Established'} > active_conn_pre_block.txt` or `ss -tunap > active_conn_pre_block.txt`) to document any live sessions to flagged streaming domains prior to blocking.

Step 2: Detection — Query DNS logs and proxy logs for resolution or connection attempts to domains flagged in the DOJ seizure action or matching Malwarebytes IOC reporting. Search endpoint detection logs for T1204.001 (user clicked suspicious link) and T1566.002 (phishing link delivery) patterns. Review browser history and downloaded file telemetry on endpoints for accesses during World Cup match windows. 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 determine scope and identify affected endpoints

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following on Windows DNS server logs: `Select-String -Path 'C:\Windows\System32\dns\dns.log' -Pattern "`. For proxy logs (Squid), run: `grep -Ef doj_domains.txt

/var/log/squid/access.log | awk '{print $3, $7}'`. Use Sysmon Event ID 22 (DNS Query) logs via PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 22} | Select-Object TimeCreated, Message | Export-Csv sysmon_dns.csv`. Cross-reference results against match schedule windows (June–July 2026) to prioritize endpoints with hits during active broadcast hours.

Evidence: Capture volatile DNS query state before any endpoint isolation: export Sysmon Event ID 22 logs for the past 30 days, browser history files (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\History`, `%APPDATA%\Mozilla\Firefox\Profiles\*.default\places.sqlite`), and Windows prefetch artifacts (`C:\Windows\Prefetch\`) to identify executables launched after visiting flagged streaming domains. Collect proxy/squid access logs covering the full World Cup match window. Do NOT wipe browser caches or prefetch prior to collection.

Step 3: Eradication — Remove any malware artifacts identified on endpoints that accessed flagged domains. Rotate credentials for any user who submitted account or payment information on these sites. Revoke and reissue session tokens for affected accounts. Reference MITRE D3FEND D3-CRO (Credential Rotation) and D3-LAM (Local Account Monitoring).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove malware, unauthorized access mechanisms, and compromised credentials from the environment

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For malware removal without EDR, run ClamAV with updated definitions against the endpoint filesystem: `clamscan -r --remove=yes /home` (Linux) or `clamscan.exe -r --remove=yes C:\Users` (Windows via ClamWin). Apply YARA rules from the Malwarebytes June 2026 report against downloaded files directories. For credential rotation on systems without PAM tooling, force password reset via Active Directory: `Set-ADAccountPassword -Identity -Reset -NewPassword (Read-Host -AsSecureString)` and invalidate Kerberos tickets with `klist purge` on the affected host.

Evidence: BEFORE revoking credentials or killing sessions, capture: full RAM image using WinPmem (`winpmem.exe memdump.raw`) to preserve in-memory credential material and any injected code from drive-by malware delivered by the streaming sites; active session tokens from browser profile directories (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies`, `%APPDATA%\Mozilla\Firefox\Profiles\*.default\cookies.sqlite`); running process list with parent-child relationships (`Get-WmiObject Win32_Process | Select-Object ProcessId, ParentProcessId, Name, CommandLine > processes_pre_eradication.txt`); and scheduled tasks or persistence registry keys (`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`) that may have been set by malware dropped from the streaming sites.

Step 4: Recovery — Validate that endpoint protection tools have updated signatures covering malware families documented in the Malwarebytes June 2026 report. Re-scan affected endpoints post-remediation. Monitor outbound DNS and proxy logs for recurrence over the remainder of the World Cup tournament window. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and NIST SI-4 (no mapped control — SI-4 not present in the provided knowledge base; omitted per policy).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation, verify integrity, and confirm threat removal before returning to production

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without an enterprise AV management console, force ClamAV definition update and rescan on each remediated endpoint: `freshclam && clamscan -r /home` (Linux) or trigger ClamWin scheduled scan with latest definitions. For DNS monitoring without a SIEM, configure a cron job or Windows Scheduled Task to run every 6 hours during the World Cup window: parse Sysmon Event ID 22 logs and alert via email if any query matches the DOJ domain list or newly registered domain pattern. Use osquery with the query `SELECT name, query, type FROM

dns_resolvers` to validate no rogue DNS resolvers have been introduced post-remediation.

Evidence: Before returning any remediated endpoint to production, collect a post-remediation process snapshot and re-run Sysmon Event ID 1 (Process Creation) log export to confirm no persistence mechanisms remain active. Verify browser extension inventory has not been altered — malware from these streaming sites has been documented delivering malicious browser extensions; check `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions` and compare against a known-good baseline. Document the re-scan output and retain per AU-11 retention requirements.

Step 5: Post-Incident — Conduct user awareness communication specific to World Cup streaming risks, citing the DOJ seizure action as context. Review and update acceptable use policies to address unauthorized streaming services. Assess whether DNS-layer filtering (D3-PBWSAM, Proxy-based Web Server Access Mediation) is deployed and tuned for newly registered and high-risk content categories. Reference CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and NIST AU-2 (Event Logging) to ensure logging coverage includes DNS and proxy telemetry going forward.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, policy updates, detection improvement, and intelligence sharing

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AU-2 (Event Logging), NIST AC-8 (System Use Notification)

Compensating: Draft and distribute a targeted phishing-awareness email citing the DOJ seizure specifically — name the ~400 domains action and the Malwarebytes malware-delivery finding to make the risk concrete. Update the acceptable use policy to explicitly name unauthorized streaming services and link to the DOJ press release as reference. For DNS-layer filtering assessment without commercial tooling, validate Pi-hole or Windows DNS RPZ (Response Policy Zone) coverage by running a controlled test query against a known-seized domain and confirming NXDOMAIN is returned. Write and deploy a Sigma rule targeting Sysmon Event ID 22 for newly registered domain queries to catch recurrence during future high-interest sporting events.

Evidence: Compile the full incident artifact package for lessons-learned review: the initial DNS/proxy log exports showing scope of user access to flagged domains, the RAM captures and process snapshots from eradication, ClamAV re-scan outputs, and any credential rotation records. Document the total count of affected endpoints, users who accessed flagged sites during match windows, and any confirmed payment data submission to inform breach notification assessment under applicable state or GDPR obligations. Retain all artifacts per AU-11 organizational retention policy.

Detection Guidance

Monitor DNS resolver logs for queries to domains registered within 30 days of the World Cup tournament start, particularly those using tournament-related keywords (e.g., 'FIFA', 'worldcup', 'stream', 'live2026'). Query proxy and firewall logs for connections to domains flagged in the DOJ seizure list or Malwarebytes IOC feed from June 2026. Look for behavioral indicators consistent with T1204.001: users following links that resolve to redirect chains ending at non-broadcast-rights-holder domains during match broadcast windows. Flag downloads of executable or script content originating from these sessions. Cross-reference with file analysis and integrity monitoring to identify any persistence mechanisms dropped on endpoints that accessed flagged sites. DNS sinkholing of seized domains may already be in effect; outbound traffic to sinkholed IPs is itself a detection signal.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.malwarebytes.com/blog/threat-intel/2026/06/free-world-cup-stream-sites-are-serving-scams-not-football`	Malwarebytes June 2026 threat intelligence report documenting scam delivery via free World Cup stream sites; retrieve IOC list directly from this source	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1608.005** — Link Target
- **T1204.001** — Malicious Link
- **T1583.001** — Domains
- **T1566.002** — 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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1608.005	Link Target	Resource-Development
T1204.001	Malicious Link	Execution
T1583.001	Domains	Resource-Development
T1566.002	Spearphishing Link	Initial-Access

Sources

Source	URL	Tier
The FIFA World Cup 2026 is here! ■■ Whether you're travelling to ...	https://www.facebook.com/QUBelfast/posts/the-fifa-world-cup-2026-is...	T3

Source	URL	Tier
"Free World Cup stream" sites are serving scams, not football	https://www.malwarebytes.com/blog/threat-intel/2026/06/free-world-c...	T3
Authorities have removed more than 27000 illegal streaming URLs ...	https://www.instagram.com/p/DZah1h3kXOg/?hl=en	T3
A basic security flaw let a security researcher access internal FIFA ...	https://www.techradar.com/pro/security/a-basic-security-flaw-let-a-...	T3
Bug in FIFA World Cup internal system gave anyone ability to modify ...	https://www.reddit.com/r/soccer/comments/1ueotgj/bug_in_fifa_world_...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-27 06:10 UTC by TJS Security Command Center