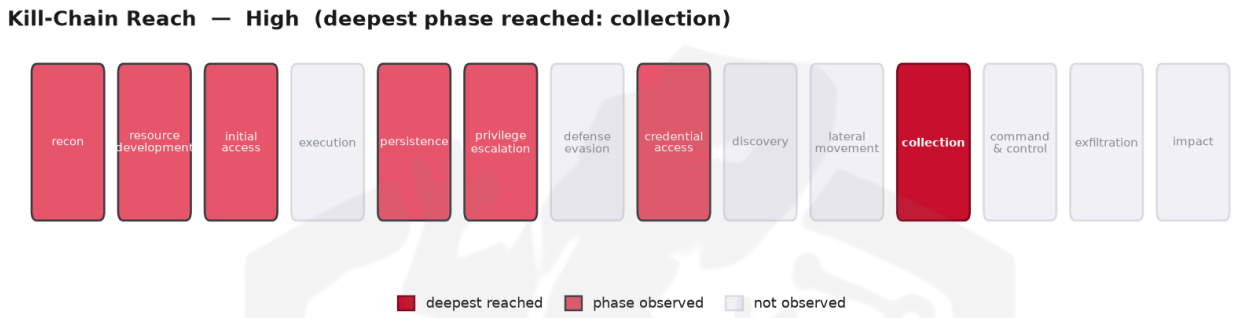
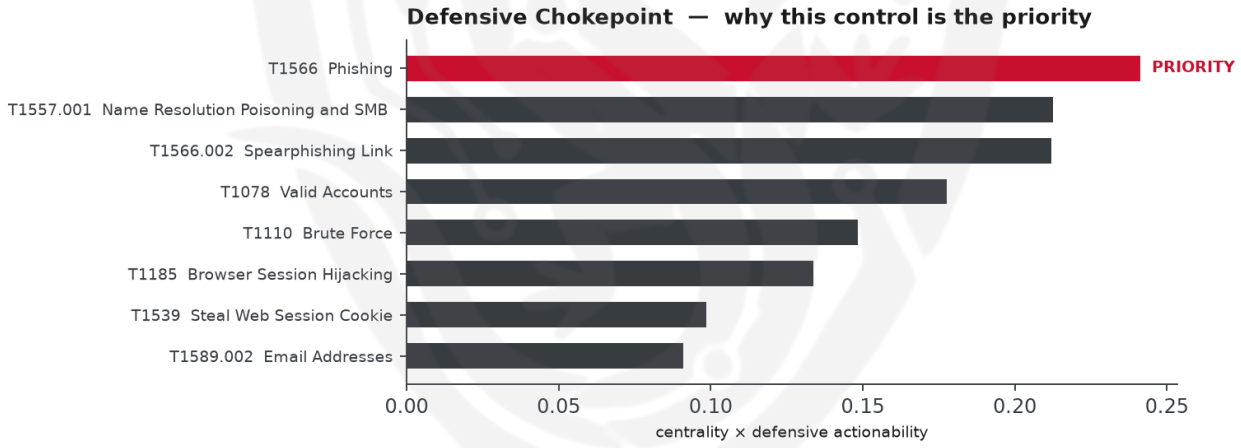
THREAT REPORT: UNKNOWN_ADVERSARY TARGETS FIFA WORLD CUP 2026

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity has been targeting entities related to the FIFA World Cup 2026, although specific details about the threat actor, malware families, and targeted countries are insufficient. The threat actor is exploiting various techniques to gain access to sensitive information. Priority should be given to defensive actions that mitigate phishing attacks. Enable attachment sandboxing and link rewriting to prevent potential breaches.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a range of techniques including Adversary-in-the-Middle, Acquire Infrastructure, Steal Web Session Cookie, and others to compromise victim systems and

gather sensitive information. The central vulnerability being exploited is not specified, but the actor's tactics involve phishing, email collection, and browser session hijacking.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, starting with initial access and progressing to credential theft, infrastructure compromise, and information gathering. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed in relation to this activity. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1557 Adversary-in-the-Middle
- T1583 Acquire Infrastructure
- T1539 Steal Web Session Cookie
- T1114 Email Collection
- T1566.002 Spearphishing Link
- T1586.002 Email Accounts
- T1583.001 Domains
- T1589 Gather Victim Identity Information
- T1185 Browser Session Hijacking
- T1557.001 Name Resolution Poisoning and SMB Relay
- T1589.002 Email Addresses
- T1584 Compromise Infrastructure
- T1586 Compromise Accounts
- T1590 Gather Victim Network Information
- T1566 Phishing
- T1110 Brute Force
- T1078 Valid Accounts
- T1589.001 Credentials
- T1598 Phishing for Information
- T1590.001 Domain Properties

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2413).
- Operational risk: High (score 0.604, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4016; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Star Blizzard	0.4016
Silent Librarian	0.4
IndigoZebra	0.3227
Magic Hound	0.2998
EXOTIC LILY	0.286

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator
Domain	fifa[.]gold
Domain	fifa-online[.]com
Domain	www-fifa[.]one
Domain	fifa[.]center
Domain	fifa[.]shopping
Domain	fifa[.]ski

Type	Indicator
Domain	fifaworldcup26[.]sale
Domain	ww-fifa[.]com
Domain	1346590[.]com
Domain	aa-fifa[.]shop
Domain	gx-fifa26[.]shop
Domain	sdf-26fifa[.]top
Domain	site-fifa[.]site
Domain	www-fifa[.]asia
Domain	www-fifa[.]bar
Domain	www-fifa[.]bio
Domain	www-fifa[.]biz[.]id
Domain	www-fifa[.]bond
Domain	www-fifa[.]cfd
Domain	www-fifa[.]click
Domain	www-fifa[.]club
Domain	www-fifa[.]cyou
Domain	www-fifa[.]digital
Domain	www-fifa[.]icu
Domain	www-fifa[.]info
Domain	www-fifa[.]lol
Domain	www-fifa[.]monster
Domain	www-fifa[.]my
Domain	www-fifa[.]my[.]id
Domain	www-fifa[.]qpon
Domain	www-fifa[.]sbs

Type	Indicator
Domain	www-fifa[.]web[.]id
Domain	www-fifa[.]work
Domain	www-fifa[.]xin
Domain	www-fifa[.]xyz
Domain	wz-fifa26[.]shop
Domain	fifa-rbi605[.]p[.]tawkto[.]email
Domain	admin-zone[.]tbpay[.]uk
Domain	www[.]fifaworldcup[.]one
Domain	www[.]ww-fifa[.]com

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1566 Phishing (initial-access)
- **Observed here:** the threat actor used T1078 Valid Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to using T1078 Valid Accounts by attempting to leverage compromised credentials or existing account access to maintain a foothold in the system, potentially exploiting weak password policies or unsecured account configurations. This approach may allow the actor to bypass the blocked phishing control and continue their campaign. To counter this, the mandated defensive control of Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively

    - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
    - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
    - Least-privilege review; separate admin from daily-driver accounts
    - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account