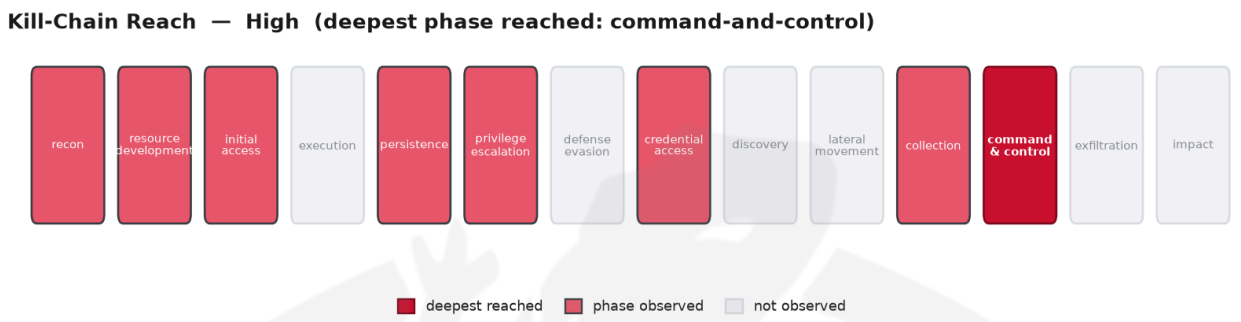
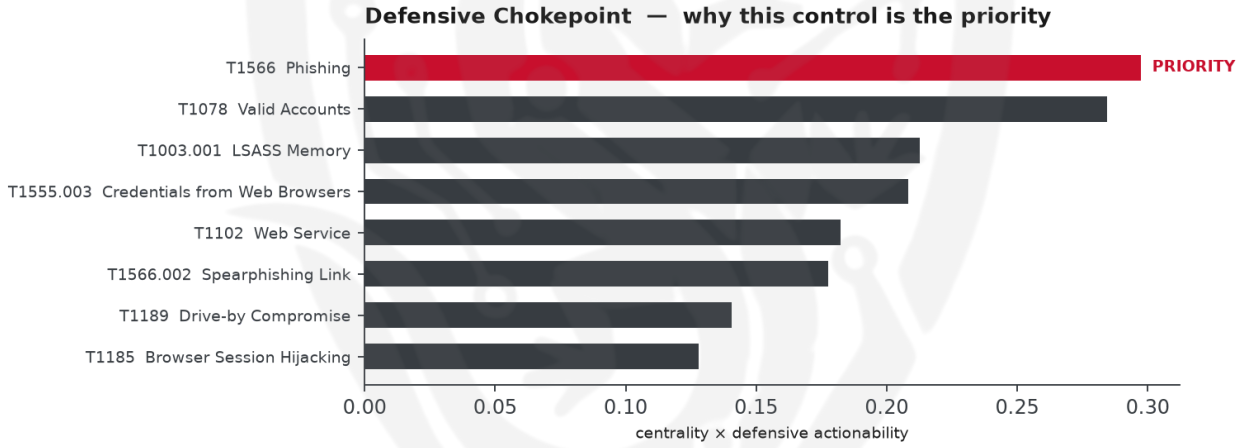
THREAT REPORT: GHOST STADIUM

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 source attributes this activity to GHOST STADIUM. This threat actor has been observed targeting the United States of America, Argentina, Brazil, Canada, Colombia, and Mexico, focusing on the hospitality, media, and finance sectors. The malware families Vidar and Lumma have been identified in this campaign. Priority should be given to defending against phishing attacks, as this is the identified chokepoint in the attack chain.

Threat Overview

GHOST STADIUM, the observed threat actor, has been associated with the malware families Vidar and Lumma. The targeted sectors include hospitality, media, and finance, across several countries. The victimology suggests a broad targeting strategy, affecting multiple industries and geographies.

Attack Chain and Priority Control

The attack chain involves a range of techniques, including keylogging, stealing web session cookies, and spearphishing. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended 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 specific information available on the hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher.

Technical Appendix

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

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

- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1588.004 Digital Certificates
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1586.002 Email Accounts
- T1583.001 Domains
- T1185 Browser Session Hijacking
- T1555.003 Credentials from Web Browsers
- T1003.001 LSASS Memory
- T1102 Web Service
- T1566 Phishing
- T1078 Valid Accounts
- T1585.001 Social Media Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1598 Phishing for Information
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1590.001 Domain Properties

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2973).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4269; 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
Sandworm Team	0.4269
Magic Hound	0.4091
APT42	0.4063
Star Blizzard	0.4002
Moonstone Sleet	0.3438

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[.]black
Domain	fifa[.]tax
Domain	fifaweb[.]com
Domain	fifa[.]red
Domain	fifa[.]fund
Domain	fifa-com[.]shop
Domain	fifa-com[.]site
Domain	fifa-com[.]store
Domain	fifa-com[.]website

Type	Indicator
Domain	fifa[.]city
Domain	fifa-com[.]vip
Domain	fifa-26-worldcup[.]com
Domain	fifa-com[.]co
Domain	fifa-com[.]com
Domain	fifa-com[.]top
Domain	fifa-com[.]xyz
Domain	fifa-tickets[.]vip
Domain	fifa-web[.]co
Domain	fifa[.]bio
Domain	fifa[.]cash
Domain	fifa[.]center
Domain	fifa[.]market
Domain	fifa[.]party
Domain	fifa[.]sale
Domain	fifa[.]shopping
Domain	fifa[.]show
Domain	fifa[.]ski
Domain	fifa2026tickets-streamlive[.]com
Domain	football-game[.]shop
Domain	football-ticket[.]shop
Domain	football-ticket[.]top
Domain	football-tickets[.]top
Domain	mm-fifa[.]top
Domain	unitycup2026[.]com

Type	Indicator
Domain	wc26-fifa[.]com
Domain	www-fifa[.]co
Domain	www-fifa[.]com
Domain	www-fifa[.]com[.]co
Domain	www-fifa[.]me

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:** GHOST STADIUM 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 GHOST STADIUM actor could pivot to using T1078 Valid Accounts if they have previously compromised credentials or have established a means to obtain them, which would likely allow them to maintain access to the target network. They may attempt to utilize existing accounts to blend in with normal activity and avoid detection. The defensive control to counter this would be to 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