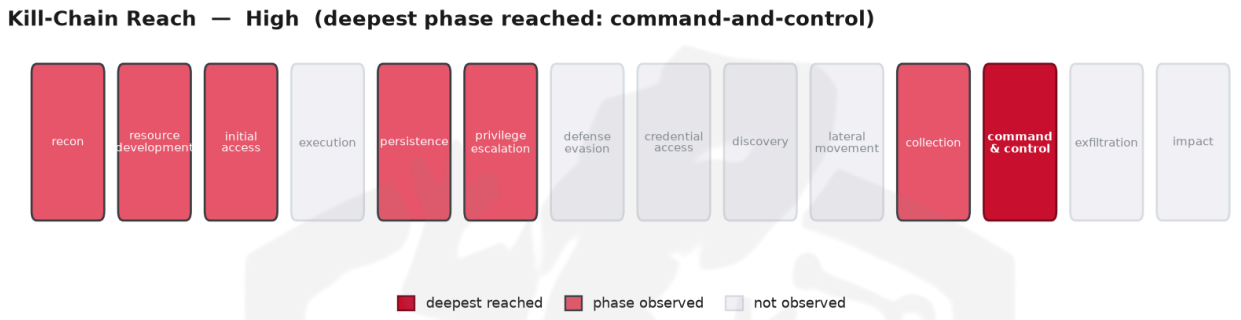
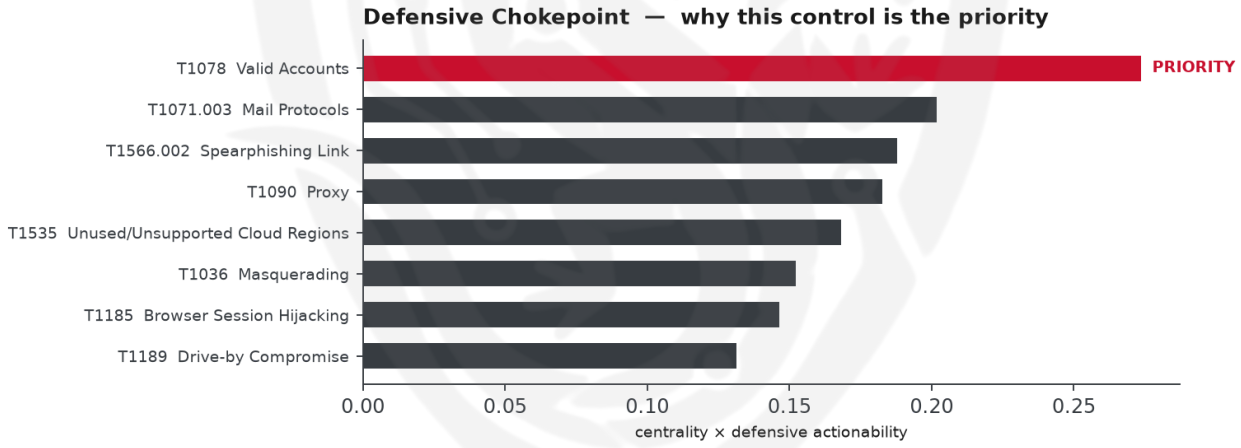
THREAT REPORT: PHISHING CAMPAIGN TARGETS RETAIL AND GOVERNMENT IN BOLIVIA AND THE UK

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 organizations in the retail and government sectors in Bolivia and the UK through a phishing campaign. The threat actor's tactics involve exploiting various techniques to gain access to sensitive information. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the risk. The campaign's impact is considered high, reaching command-and-control levels.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing a range of techniques including external remote services, email collection, and spearphishing links to target victims. The campaign's focus on retail and government sectors in Bolivia and the UK suggests a targeted approach. The techniques

used by the threat actor include masquerading, browser session hijacking, and mail protocols, among others.

Attack Chain and Priority Control

The observed techniques form a complex chain, with the threat actor using external remote services, email collection, and spearphishing links to gain initial access. The priority technique is T1078 Valid Accounts, which is the graph chokepoint. To counter this, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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)

- T1133 External Remote Services
- T1114 Email Collection
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1586.002 Email Accounts
- T1036 Masquerading
- T1185 Browser Session Hijacking
- T1071.003 Mail Protocols
- T1535 Unused/Unsupported Cloud Regions
- T1589.002 Email Addresses
- T1090 Proxy
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1132 Data Encoding
- T1189 Drive-by Compromise
- T1584.004 Server

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3206).
- 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 0.3344; 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	0.3344
Magic Hound	0.3344
TA577	0.329
TA551	0.3185
Star Blizzard	0.3135

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	boots-rewards-uk[.]xyz
URL	hxxps://ipelc[.]gob[.]bo/boots_store/
URL	hxxp://ipelc[.]gob[.]bo/boots_store/
Hash	13ac78f8f2ed76a03c85f0cdef07e5463aa64458303c0949090fcd81868ba8ca
Hash	375c2c84e2ca022c565507523b75c9c08a455479861ea41fc9b9ff74b3453445
Hash	5d2ad1795b0dfc4a58424b2fa2f002246f653b119d362954ae270b6998e9d575
Hash	6c428acbd91be85fedf9cbb334457ddea08ff624d4de88041749578e968d62a8
Hash	7fda5f10a2bc212daaa467484c56eb8abf3f3681f6405c5c2fac16d4124e44ca
Hash	95fc58dc321b07ecc99d95359bcdee08a5beb519ead8e70e40f33928533a1b14

Type	Indicator
Hash	c5ec55270af084d3c07d2918098d598bc2c5ca42f4189d69cdfcae2c958e5ec7

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows infrastructure to gather information and execute tasks, potentially exploiting the same level of access that was previously obtained through valid accounts. This technique may be particularly appealing to the actor because it enables them to interact with the system in a way that blends in with normal administrative activity, making it harder to distinguish from legitimate use. To counter this potential pivot, the defender would likely implement the mandated defensive control: Monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command