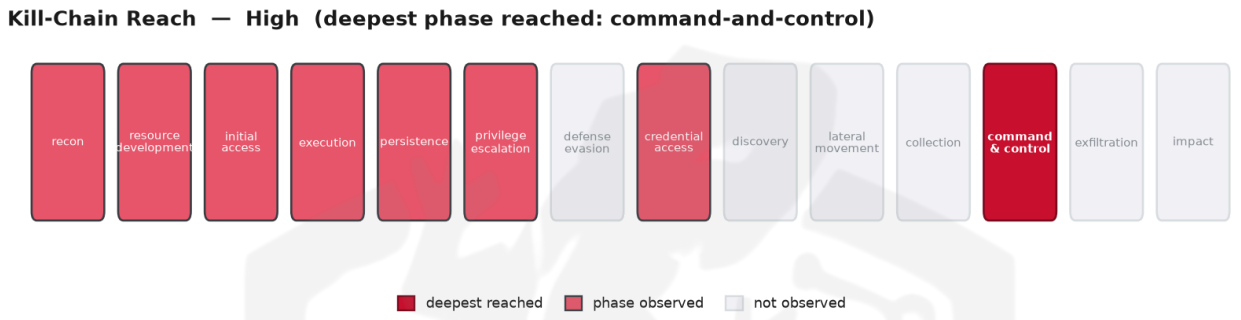
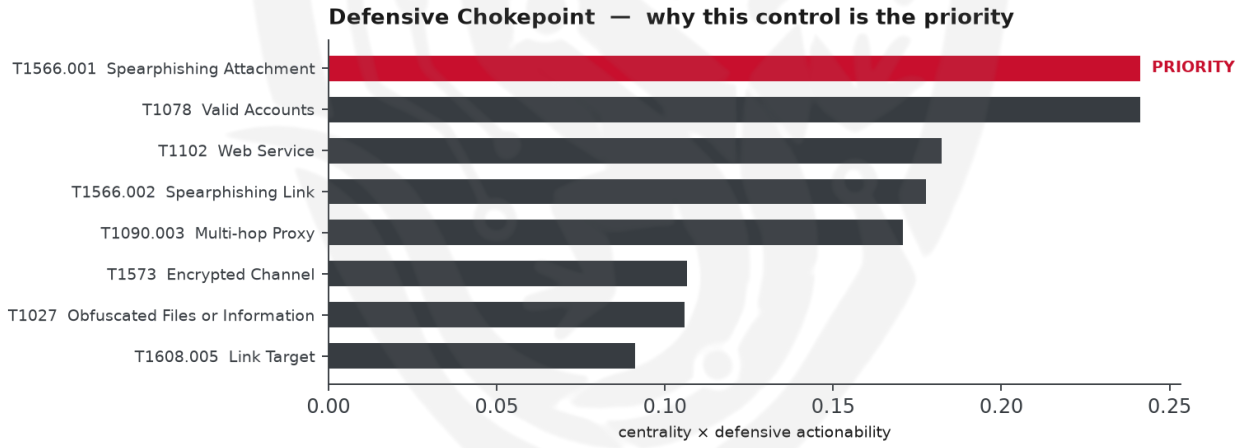
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 various sectors in multiple countries, including the United States of America, Argentina, Australia, Canada, and New Zealand. The threat actor is utilizing a range of techniques to compromise victims, with a focus on spearphishing and web-based attacks. Priority should be given to defending against spearphishing attachments, as this is the identified priority technique. The targeted sectors include Government, Finance, Healthcare, Education, and others, making this a high-priority threat.

Threat Overview

The threat actor, which remains unidentified, is using various techniques such as stealing web session cookies, uploading malware, and exploiting vulnerabilities to target victims. The actor is also utilizing

spearphishing links and attachments to compromise systems. The targeted countries and sectors suggest a widespread and coordinated effort.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving initial compromise through spearphishing, followed by malware upload and exploitation of vulnerabilities. The priority technique is T1566.001 Spearphishing Attachment, which is the identified graph chokepoint. To defend against this threat, the priority control is to: Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with high confidence 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)

- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1588.006 Vulnerabilities
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1608.004 Drive-by Target
- T1608.001 Upload Malware
- T1583.001 Domains
- T1102 Web Service
- T1608.005 Link Target
- T1583.006 Web Services
- T1090.003 Multi-hop Proxy
- T1584.006 Web Services
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1071.001 Web Protocols
- T1584.004 Server
- T1566.003 Spearphishing via Service

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2413).
- 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 0.4746; 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
LazyScripter	0.4746
BITTER	0.4734
CURIUM	0.4483
EXOTIC LILY	0.4355
Star Blizzard	0.4336

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	clintile[.]com
Domain	mypal[.]pro
Domain	lssc[.]ltd
Domain	forwarsprite[.]com
Domain	allegro-stroe[.]shop
Domain	allegrostroe[.]cc

Type	Indicator
Domain	allegro-stroe[.]cyou
Domain	allegro-stroe[.]cc
Domain	allegrostroe[.]shop
Domain	allegroau[.]com
Domain	g3user[.]com
Domain	usdtflow[.]net
Domain	allegrostroe[.]cyou
Domain	deepseekpg[.]bet
Domain	verify-what[.]com
Domain	lightacer[.]com
Domain	lssc-canada[.]ca
Domain	correoargentino-comarr[.]top
Domain	energy5[.]cyou
Domain	whats-zwp[.]vip
Domain	whats-zea[.]vip
Domain	whats-zei[.]vip
Domain	whats-zen[.]vip
Domain	whats-zef[.]vip
Domain	whats-zrs[.]vip
Domain	whats-zus[.]vip
Domain	m0vrsq6[.]top
Domain	polymk[.]com
Domain	bepviews[.]com
Domain	nasdaqpro[.]top
Domain	allegro-stroe[.]com

Type	Indicator
Domain	allegroau[.]cc
Domain	allegrostroe[.]com
Domain	datashareclub[.]com
Domain	faq-whatsapp-center[.]com
Domain	futureblockchain[.]net
Domain	hkxiu[.]com
Domain	inetcontrol[.]net
Domain	k-usdt[.]com
Domain	kirbycoco[.]cc

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:** T1566.001 Spearphishing Attachment (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 actor could pivot to using T1078 Valid Accounts by attempting to leverage existing credentials that were potentially compromised during the initial spearphishing campaign, which may allow them to maintain access to the network. They may try to use these valid accounts to blend in with normal user activity, potentially evading detection. The defensive countermeasure to mitigate 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