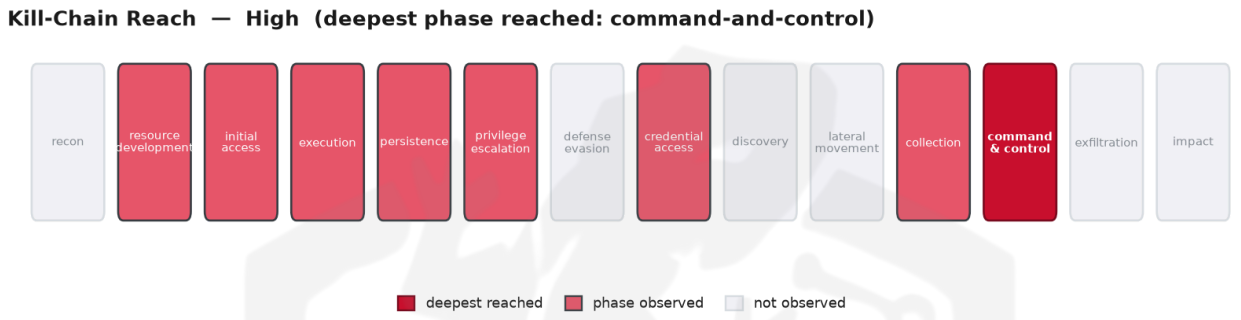
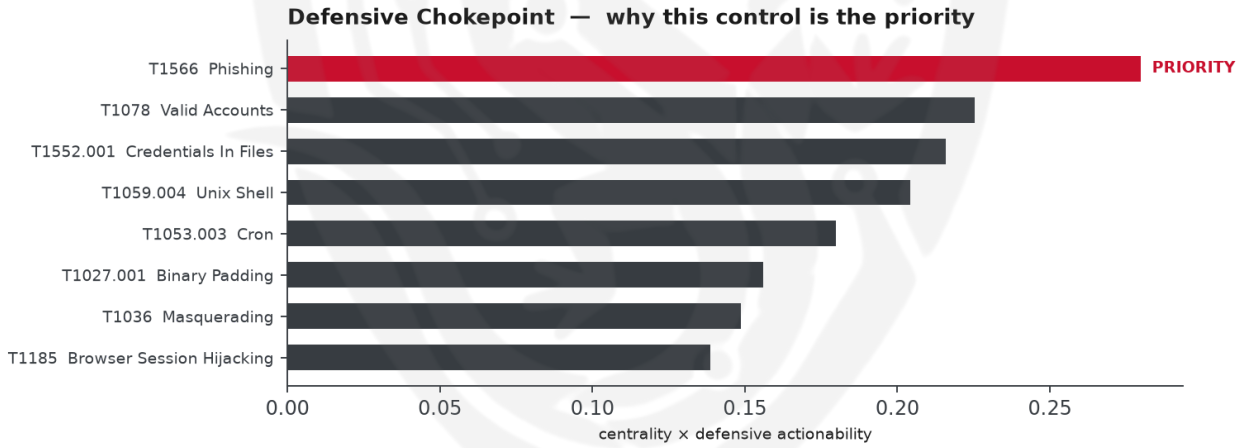
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 identified as a threat to the Finance and Technology sectors, utilizing various malware families including AMOS, ClawHavoc, and cluw. The threat actor's targets and motivations are not well understood due to insufficient data. Priority should be given to defensive actions that mitigate the threat of phishing and other social engineering tactics. Enable attachment sandboxing and link rewriting to prevent initial compromise.

Threat Overview

The threat actor, whose identity is unknown, is using a range of techniques to compromise targets, including Standard Encoding, Hide Artifacts, and Masquerading. The malware families AMOS, ClawHavoc, and cluw are being used, although the central vulnerability being exploited is not identified.

The threat actor is targeting the Finance and Technology sectors, but the specific countries being targeted are not known.

Attack Chain and Priority Control

The observed techniques suggest a complex attack chain, involving initial compromise through phishing or other means, followed by the use of various techniques to hide artifacts and maintain access. The priority technique is T1566 Phishing, which is the graph chokepoint. To mitigate this threat, 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

The malicious infrastructure is hosted on providers including Omegatech LTD and Emil Vitukhnovskii Trading As Great Flower, according to third-party observations. However, no malware families have been corroborated by abuse.ch, and indicators have low confidence ratings on AbuseIPDB, with the highest confidence seen being 14%.

Technical Appendix

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

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

- T1132.001 Standard Encoding
- T1564 Hide Artifacts
- T1204.002 Malicious File
- T1053.003 Cron
- T1071 Application Layer Protocol
- T1140 Deobfuscate/Decode Files or Information
- T1583.001 Domains
- T1036 Masquerading
- T1185 Browser Session Hijacking
- T1027.001 Binary Padding
- T1552.001 Credentials In Files
- T1583.006 Web Services
- T1566 Phishing
- T1059.004 Unix Shell
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2797).
- 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 0.4707; 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
BITTER	0.4707
TA551	0.4587
APT33	0.4376
Nomadic Octopus	0.4221
Higaisa	0.4061

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 14%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	91[.]92[.]242[.]30	AbuseIPDB 14% (NL) · AS202412 Omegatech LTD
IP	2[.]26[.]75[.]16	AbuseIPDB 0% (DE) · AS202226 Emil Vitukhnovskii Trading As Great Flower
Domain	laosji[.]net	
Domain	download[.]setup-service[.]com	

Type	Indicator	Context
URL	hxxp://glot[.]io/snippets/hfd3x9ueu5	
Hash	818aea6143282b352fdfdc0f3ebf77a36e54eb3befb5cad1a355a99ab97c6aa7	
Hash	881ce5cb124c4d2e814783724cc1388f6a1cbf6eee274c3f3366e77ba3503ad7	
Hash	b30eaed1f7478c28f4ec50d07ed5ef014ffbc4b2bc5a38d689ba9f7abb5e19c2	
Hash	b6c7e0bf573b1c7d9d3a05eb08d26579199515b847df984862805f44a7af8007	
Hash	ebb73dbb5aac1f6fe1a88e8f26126a1e1aa34c9f3345ad4345189b40d9bf1d1d	
Hash	f4e41aa269c88bf11a2022701a9cf41e9a186aa1b224d837c31bf34e0b875d0e	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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 actor could pivot to using T1078 Valid Accounts to maintain access and achieve their objectives, potentially by compromising or reusing existing credentials that were not affected by the phishing block. This technique may allow the actor to blend in with normal user activity, making it more challenging to detect their presence. The defender would likely counter this by enforcing the mandated defensive control: 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