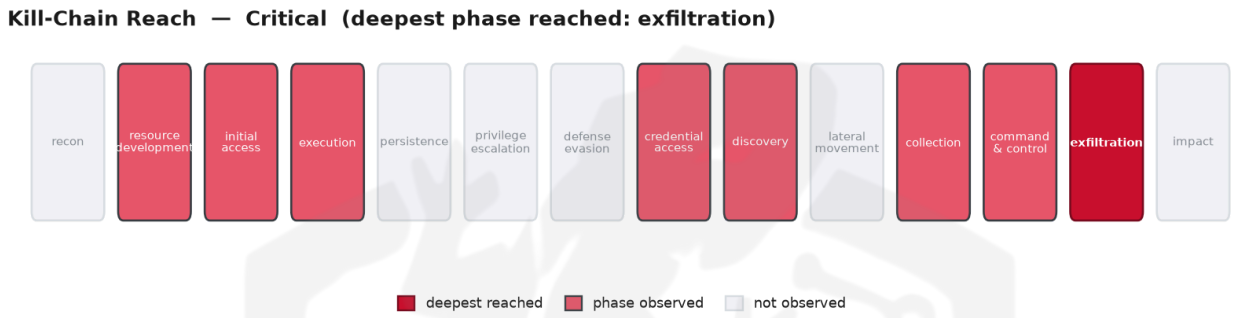
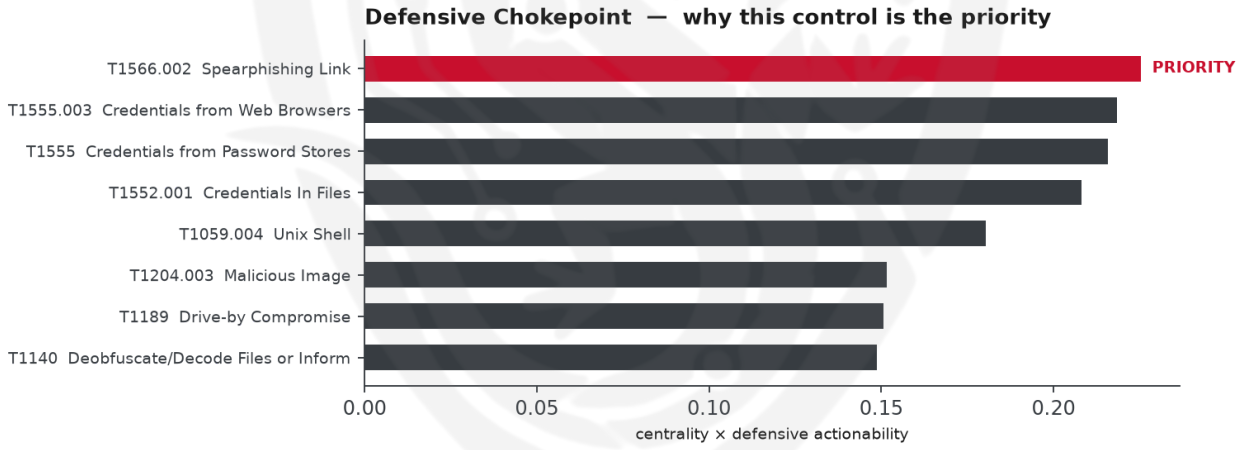
THREAT REPORT: UNKNOWN_ADVERSARY MALVERTISING CAMPAIGN

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 abusing the claude.ai shared chat for a ClickFix malvertising campaign, primarily targeting the technology sector in multiple countries, including British Indian Ocean Territory, France, and India. The campaign involves the MacSync malware family and exploits various techniques to compromise systems. Priority should be given to enabling defensive measures to prevent further attacks. The threat actor's tactics pose a critical operational risk due to the potential for exfiltration.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is utilizing the MacSync malware family to target victims. Although a central CVE is not specified, the actor employs a range of techniques,

including system owner/user discovery, stealing web session cookies, and spearphishing links. The targeted sectors are primarily technology-based, with a focus on countries such as Japan, Malaysia, Singapore, and Taiwan.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, starting with system information discovery and progressing through various tactics such as deobfuscating files, stealing credentials, and establishing a command and control channel. The priority technique identified is T1566.002 Spearphishing Link, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended 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

Although specific hosting providers or ASNs are not observed, third-party corroboration from abuse.ch indicates the presence of Unknown Stealer and Unknown malware families. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These findings provide additional context to the threat landscape but do not override the primary source information.

Technical Appendix

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

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

- T1033 System Owner/User Discovery
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1583.006 Web Services
- T1041 Exfiltration Over C2 Channel
- T1059.004 Unix Shell
- T1204.003 Malicious Image
- T1189 Drive-by Compromise

- T1105 Ingress Tool Transfer
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.2253).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4454; 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
ZIRCONIUM	0.4454
Mustard Tempest	0.4082
Evilnum	0.3974
Darkhotel	0.3961
Patchwork	0.3879

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Unknown Stealer, Unknown malware.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Domain	jerryshvac[.]com	
Domain	customroofingcontractors[.]com	Unknown malware

Type	Indicator	Context
Domain	a2abotnet[.]com	Unknown malware
Domain	claude-code[.]official-version[.]com	Unknown malware
Domain	isgilan[.]com	Unknown Stealer
Domain	plirepsijr74[.]com	
Domain	thnikagent[.]com	
Domain	babulikinet[.]com	
Domain	loserrq0j1sha8[.]com	
Domain	bernasibutuwqu2[.]com	malware_download
Domain	briskinternet[.]com	Unknown Stealer · malware_download
Domain	touristprogram[.]com	
Domain	homeinspectionnaperville[.]com	Unknown Stealer · malware_download
Domain	yoauction[.]com	
Domain	alabamarecoverycenter[.]com	
Domain	5x5web[.]com	
Domain	bewqslkslikrtjinfg9[.]com	
Domain	oaklandwaterdamage[.]com	

Type	Indicator	Context
Domain	peowqlauoshau8[.]com	
Domain	20claude[.]ai	
URL	hxxps://loserrq0j1sha8[.]com/debug/loader[.]sh?build=a39427f9d5bfda11277f1a58c89b7c2d	

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:** T1566.002 Spearphishing Link (initial-access)
- **Observed here:** the threat actor used T1189 Drive-by Compromise here as an alternative initial-access technique.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to T1189 Drive-by Compromise by exploiting vulnerabilities in software or plugins to compromise a user's system when they visit a malicious website, which may allow them to maintain their objective despite the block on spearphishing links. This technique may be used as an alternative means to gain initial access, and the actor would likely rely on unpatched vulnerabilities or user-enabled risky plugins to succeed. To counter this, the mandated defensive control of Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins should be implemented.

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.